IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|---|---|---|
| In re *Ex Parte* Reexamination of: | § | |
| | § | |
| | § | |
| **U.S. Patent Number 5,623,600** | § | Control No.: Not Yet Assigned |
| | § | |
| Issued: April 22, 1997 | § | Group Art Unit: Not Yet Assigned |
| | § | |
| For: Virus Detection and Removal for Computer Networks | § | Examiner: Not Yet Assigned |
| | § | |
| | § | Attorney Docket No.: FORT-000013L |

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**REQUEST FOR *EX PARTE* REEXAMINATION UNDER 35 U.S.C. §§ 302-307**

Dear Sir:

Fortinet, Inc., by and through its undersigned attorneys respectfully requests reexamination under 35 U.S.C. §§ 302-307 and 37 C.F.R. § 1.510 of U. S. Patent No. 5,623,600 ("the '600 patent") attached hereto as Exhibit A. The '600 patent issued on April 22, 1997 to Eva Chen and Shuang Ji. Trend Micro, Incorporated ("Trend Micro") is listed as the assignee of the '600 patent. Eva Chen, Trend Micro's co-founder and current Chief Executive Officer, along with Trend Micro, will hereinafter be referred to by name or as "applicant" or "patentee". This reexamination is requested because a review of existing prior art reveals that, contrary to Ms. Chen's assertion that the '600 patent is a primary example of Trend Micro's innovation and industry firsts, the technology underlying the purported inventive systems and methods of the '600 patent was neither novel nor innovative, but rather was obvious in light of multiple printed publications prior to September 26, 1994 (the "Critical Date").

This Request for *Ex Parte* Reexamination ("Request") is not being served on the correspondent of record for the '600 patent as such service is believed to be futile in view of the fact that the Skjerven Morrill law firm dissolved on or about March 1, 2003. Pursuant to 37 C.F.R. §1.510(b)(5), a duplicate copy of this Request is being supplied to the Office on CD-ROM.

For the convenience of the Examiner, following is a table of contents for this Request:

## Contents

## I. NOTIFICATION OF CONCURRENT PROCEEDINGS PURSUANT TO 37 C.F.R. § 1.565

Requestor, Fortinet, Inc. ("Fortinet" or "requestor") and the patentee, are currently involved in litigation involving, *inter alia,* the above referenced '600 patent (stemming from a "parent" application) and related U.S. Patent No. 5,889,943 (the "'943 patent", stemming from a "child" application). The patent litigation is in the U.S. District Court, Northern District California (Civil Action No. CV 10-0048 MMC). A related state court contract action involving the '600 patent and the '943 patent is also pending in California Superior Court of Santa Clara (Case No. 1:09−CV-149262). Copies of the federal and state court complaints are submitted herewith as Exhibit B1 and Exhibit B2, respectively.

Pursuant to 35 U.S.C. § 305, Requester respectfully urges that this Request be granted and the reexamination be conducted not only with "special dispatch", but also with "priority over all other cases" in accordance with MPEP § 2261, due to the ongoing nature of the underlying litigation.

Reexamination is requested in view of the substantial new questions of patentability presented herein. Requestor reserves all rights and defenses available including, without limitation, defenses as to invalidity and unenforceability. By filing this Request in compliance with the Patent Rules, Requester does not represent, agree or concur that the '600 patent is enforceable, and by asserting the substantial new questions of patentability herein, Requester specifically asserts that claims 1-22 (all claims) of the '600 patent are in fact not patentable and as such the United States Patent and Trademark Office (USPTO) should reexamine and find claims 1-22 unpatentable and cancel such claims of the '600 patent, rendering the '600 patent null, void and otherwise unenforceable.

## II. CITATION OF CLAIMS FOR WHICH REEXAMINATION IS REQUESTED AND CITATION OF PATENTS AND PRINTED PUBLICATIONS PRESENTED TO PROVIDE A SUBSTANTIAL NEW QUESTION OF PATENTABILITY

In accordance with 37 C.F.R. §§ 1.510(b)(1) and (b)(2), reexamination of claims 1-22 (all issued claims) of the '600 patent is requested in view of the following references:

**Exhibit C** "The Design of a Secure Internet Gateway", by Bill Cheswick, USENIX Summer Conference June 11-15, 1990 ("Cheswick") — Not previously considered during examination.

**Exhibit D** "Firewalls and Internet Security – Repelling the Wily Hacker", by William R. Cheswick and Steven M. Bellovin, Copyright 1994 ("Cheswick and Bellovin") — Not previously considered during examination.

**Exhibit E** "A Gateway to Internet Health and Happiness", by Robin Layland, published September 21,1994 in Data Communications, Internetworking Views ("Layland") — Not previously considered during examination.

**Exhibit F** Intel LANProtect Product Documentation (together, Intel LANProtect Product Overview and Intel LANProtect Software Users Guide), copyright 1992, by Intel Corporation ("LANProtect") — Not previously considered during examination.

**Exhibit G** "SPECIAL REPORT: Secure Computing Corporation And Network Security", published December 1994, the LOCALNetter Newsletter, vol. 14, No. 12 ("Sidewinder") — Not previously considered during examination.

**Exhibit H** "TIS Firewall Toolkit Overview", published June 30, 1994, by Trusted Information Systems, Inc. and USENIX Association, Proceedings of the Summer 1994 USENIX Conference, June 6-10, 1994 (collectively, "TIS Firewall") — Not previously considered during examination.

**Exhibit I** U.S. Patent No. 5,319,776, issued to Hile *et al.*, filed in September 1992 and issued June 1994 ("Hile") — Previously considered during examination.

**Exhibit J** "TFS gateway", by TenFour Sweden AB ("TFS Manual") — Not previously considered during examination.

**Exhibit K** "MIMEsweeper administrator guide" ("MIMEsweeper")-published by Integralis Ltd Copyright 1995. — Not previously considered during examination.

**Exhibit L** "MpScan-Email Security" ("MpScan") — Published by Cybersoft- Not previously considered during examination.

**Exhibit M** "Network security SunScreen SPF-100" ("SunScreen SPF-100") - Not previously considered during examination.

The combination of Hile with newly cited art presents a substantial new question of patentability. Although Hile was cited during prosecution of the '600 patent and considered in combination with another prior art reference, the Examiner did not substantively consider Hile in combination with Cheswick, the Cheswick and Bellovin reference, the Layland reference, the LANProtect reference, the Sidewinder reference, the TIS Firewall reference, the MpScan reference or the SunScreen SPF-100 reference. These references present new, non-cumulative technological teachings that would have been considered important to a reasonable examiner at the time of prosecution as is shown by a consideration of the prosecution history and reasons for allowance. Accordingly, in light of the new, non-cumulative technological teachings of these references as discussed in detail below, the combination of newly cited art presented herein in combination with Hile presents a substantial new question of patentability as to claims 1-22 (all claims) of the '600 patent.

The highly relevant Hile reference previously applied by during prosecution of the '600 patent should be carefully reconsidered in combination with the prior art references provided herewith. Under 35 U.S.C. § 303(a), as amended in 2002 "[t]he existence of a substantial new question of patentability is not precluded by the fact that a patent or printed publication was previously cited by or to the Office or considered by the Office." In so amending, Congress specifically stated that the amendment "overturns the holding of In re Portola Packaging Inc." Rather than a strict prohibition against reexamination of a patent based on a publication that had been considered during the initial examination of a patent, "the appropriate test . . . should not

merely look at the number of references or whether they were previously considered or cited but their combination in the appropriate context of a new light as it bears on the question of the validity of the patent." A complete listing of all the Exhibits, including relevant publications and patents, is provided at the end of this Request.

The following other written evidence is also made of record, solely to help explain the content of certain of the references listed above. *See* MPEP § 2205.

**Exhibit N** "An Introduction to the Norman Firewall: The secure way to connect to the Internet and other TCP/IP-based networks" ("Norman Firewall") - published by Norman Data Defense, Inc. Copyright November 1995.

**Exhibit O** Robert McMillan, "Trend Micro: Barracuda Suit Not About Open Source," PC World, PCW Business Center, June 13, 2008 ("McMillan").

**Exhibit P** Steve Chang and Jenny Chang, "Trend Micro: History of the Global No. 1 Internet Security Company," Trend Micro, Copyright 2002 ("Trend Micro History").

## III. INTRODUCTION

Claims 1-22 (all claims) of the '600 patent are invalid under 35 U.S.C. § 103(a) in view of the previously cited and uncited prior art references listed above. The references cited in this Request demonstrate the lack of novelty and the obviousness of all claims (i.e., claims 1-22) of the '600 patent, thereby raising a number of substantial new questions of patentability which merit consideration by way of reexamination.

The '600 patent issued from an application filed on September 26, 1995. The '600 patent broadly claims a system, an apparatus and methods for detecting computer viruses during transmission over a network.[1] The specification of the '600 patent describes a gateway computer

[1] '600 patent, col. 1, ll. 10-13

consisting of: a prior art computer system,[2] running a prior art operating system, such as Berkeley Software Distribution (BSD) UNIX,[3] connecting two networks using prior art connection methods,[4] providing prior art data transfer services, such as FTP and SMTP,[5] via prior art proxy servers modified according to the teaching of the patent.[6] In other words, the patent describes a basic and entirely routine network implementation. The specification also describes scanning for viruses, which was also in the prior art, at an intermediary node between computers or computer networks.[7] The purportedly novel teaching of the patent application was simply the combination of a rudimentary and well known network implementation, with the addition of equally rudimentary and well known anti-virus scanning on a network gateway.

Independent claim 1 of the '600 patent is representative and instructive – demonstrating the obviousness over the prior art systems and publications presented herewith. Claim 1 broadly claims a system implemented on a proxy server for detecting viruses in data transfers—a system which performs the obvious steps of checking data to be transferred for the presence of a virus and performing various equally obvious actions depending on the result of the virus check. In a nutshell, this claim under the broadest reasonable construction arguably covers any anti-virus scanning performed by any network device. In fact, such a broad construction of the '600 patent has been openly adopted by applicant as part of its aggressive licensing program and associated litigation ("We [Trend] are litigating [with] Barracuda, who are selling a ***gateway*** and putting ***whatever type of AV***, whether it's ClamAV or Shophos [*sic*] of whomever's AV, on there.[8] "In the ['600] patent, we are not claiming that we invented the antivirus scanner. We are not claiming that

[2] '600 patent at col. 3, l. 66 – col. 4, l. 17
[3] '600 patent at col. 5, ll. 10-16
[4] '600 patent at col. 4, ll. 36-45
[5] '600 patent at col. 7, ll. 2-9
[6] '600 patent at col. 5, l. 60 - col. 6, l. 3
[7] '600 patent at col. 4, l. 63 - col. 5, l. 26
[8] McMillan at p. 1 (emphasis added).

we invented the proxy server. But the ***concept*** of using these two together so that you can stop the virus during the transition [*sic:* transmission] is new."[9]).

The other independent claims of the '600 patent are similarly broad and equally invalid and unpatentable over the prior art. In addition, the dependent claims offer no real discernable differences over the broad and overreaching independent claims. For example, dependent claim 2 specifies the proxy server as an FTP proxy server (one of the most prolific proxy servers at the time of the '600 patent was filed), while dependent claim 3 specifies the proxy server as an SMTP proxy server (arguably the other most prolific proxy server in existence at the time). Because SMTP and FTP were so wide spread (essentially standard network elements on virtually every network of the time) these dependent claims add no meaningful limitations to the already overly broad base claims. Cheswick and Bellovin notes the ubiquitous nature of SMTP and FTP at pg. 29 and 41 ("If you are talking mail transport on the Internet, you are usually talking about the *Simple Mail Transport Protocol (SMTP)*" and "anonymous FTP has become a principal standard on the Internet for publishing software, papers, pictures, etc. Most major sites need to have a publicly accessible anonymous FTP repository somewhere. Whether you want it or not, you most likely need it.")

This Request demonstrates that scanning for viruses on network devices was not novel as of the Critical Date. The prior art printed publications submitted herewith would be considered important to a reasonable examiner, and thus raise substantial new questions of patentabilty that render claims 1-22 (all the issued claims) of the '600 patent invalid. These materials should have been—but were not—raised and considered during prosecution of the '600 patent. Had the examiner been properly made aware of these references and the obvious patentability issues stemming therefrom, the claims of the '600 patent would never have issued.

[9] McMillan at p. 2 (emphasis added).

**Historical Context Prior To Prosecution**

Desktop virus scanning programs became publicly available and widely publicized by the mid-to-late 1980's.[10] Network-based virus scanning also became widely-known, implemented and publicized shortly thereafter.

By the late 1980's, people had begun connecting individual desktop computers together, so the need arose for something more than ordinary desktop antivirus scanning. U.S. Patent No. 5,319,776 to Hile *et al.*, filed in September 1992 and issued June 1994 is entitled, "In Transit Detection of Computer Virus With Safeguard."[11] Hile, which was cited by the applicant and considered by the examiner, describes an improvement to a personal computer data transfer program that scans data for computer viruses during the data transfer "on the fly" and before the data is stored on a destination storage medium so as to prevent computer viruses from infecting the computer. Hile then automatically inhibits virus-infected data from being stored.[12]

Figure 1 of Hile shows a first computer system 12 and a second computer system 14 connected over a telecommunication link 26 using modems 28, which are connected to the respective serial ports 22. The first computer system transmits data over telecommunication link 26 to the second computer system.[13] Figure 1 is as follows:

[10] *See*, e.g., "An Overview of 18 Virus Protection Products, Computers and Security", by Dr. Harold Joseph Highland FICS, Vol. 7, No. 2, 1988
[11] Hile
[12] Hile at col. 1, ll. 55-62
[13] Hile at col. 3, ll. 18-38

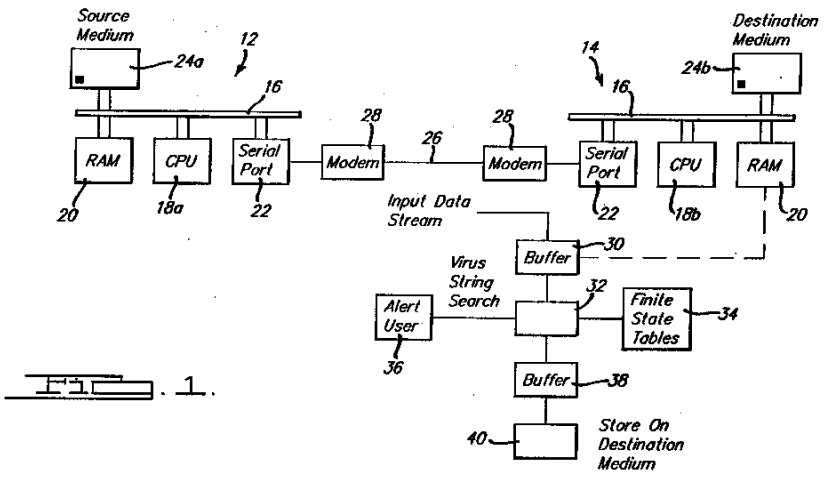



Fig. 1.

Hile notes the problem of copying a file from one computer system to another where the integrity of a remote computer system is not known, thus making it desirable to scan for viruses while a file is "in transit" from one computer to another:

> In a telecommunications system, often the user of the second computer system 14 will have no direct control over the integrity of files stored on the source medium 24a. A file on source medium 24a may be corrupted by a virus, for example. Assuming the user of computer system 14 has been careful, the destination medium can be characterized as a known secure storage medium. From the computer system 14 user's standpoint, the source medium may be considered an insecure storage medium, since the user of system 14 does not control what is stored on the source medium. [14]

Additionally, well before the Critical Date, commercially available programs had already been developed to protect servers behind a network gateway. Server-based antivirus programs were typically installed on a server and automatically scanned any file that was sent into, or out of, that server.[15] The Intel LANProtect system (later renamed LanDesk Virus Protect) was a file server-based system that could selectively scan files that were attempted to be saved on, or accessed from, a Novell file server. Like the prior art desktop virus scanners, the LANProtect system also selectively scanned only certain types of files likely to contain viruses. The specific files to be scanned, and the actions taken if a virus was found, were user-configurable. The LANProtect

[14] Hile at col. 3, ll. 45-55
[15] LANProtect

system and other similar systems were not disclosed to the examiner and/or considered by the examiner during the prosecution of the '600 patent. The LANProtect reference teaches facilitating the selective transfer of data using a server arranged to scan the data for a virus and the software disclosed includes data handling actions dependent upon the existence of a virus. Indeed, this is not surprising, given that the product referred to by the LANProtect reference was jointly developed and marketed by Intel and Trend Micro beginning in 1992.[16]

In fact, not only did the LANProtect reference contain the obvious combination of features Trend disingenuously argued was novel (i.e., the use of antivirus scanning by a proxy server) when it filed its Petition to Make Special, which is discussed further below, but multiple other well-publicized products of the time also contained this simple and obvious combination of features. For example, the Norman Firewall (which was demonstrated and offered for sale at a Federal Office Systems Expo (FOSE) trade show that began on March 21, 1995) implemented virus scanning at the firewall. Also, the TFS (Transfer File System) Gateway, developed by TenFour Sweden AB, was a series of gateway products that acted as a link between local and global mail systems.[17] According to the TFS Manual, the TFS Gateway acted as a link or "common denominator" between different email systems, such as a (local) LAN email system and a global email system, like the Internet. The TFS Gateway was able to handle multiple email systems by providing its own translations for each such system. In doing so, it allowed third parties to link to the TFS Gateway directly. The TFS Gateway provided for virus scanning at the gateway.

Moreover, like the TFS Gateway, MIMEsweeper 1.0, developed by Integralis, also implemented virus scanning at the gateway.

> MIMEsweeper sits between organisations' mail systems, whether internal or external, and scans the contents of all mail for any undesirable attributes. If

[16] Trend Micro History pages 7, 53-57 (showing Eva's involvement with the Intel LANProtect product).
[17] TFS Gateway at TFS00123; TFS00640-719

> detected, the complete mail item will be quarantined. The initial definition of undesirable contents will be anything identified as a Virus, but it is intended to leave the classification of undesirables open and extensible.[18]
>
> MIMEsweeper incorporates store and forward technology, diverting incoming files to a mail box where they can be scanned for unidentifiable attachments or viruses. Messages containing an undesirable attribute are quarantined, allowing virus protection tools to be used.[19]

MIMEsweeper described itself as an email router which automatically and transparently scanned both incoming and outgoing email for the presence of viruses or macro bombs within attachments. It provided "recursive dismantling and analysis of a wide range of file types including: MIME and "unlocks hidden viruses and macro bombs from nested compressed files (*e.g.*, '.ZIP' within '.ZIP'), self exploding ZIP, auto-start macros, … etc."[20]

MIMEsweeper handled mail message attachments by extracting and unbundling messages and all attachments from the mail system and repeating identification and unbundling of composite attachments until all data was identified and unpackaged. It scanned for undesirable attributes, e.g., viruses or other hazardous files. *Id.* It would attempt to unravel all mail attachments to their lowest components, e.g., uncompressing ZIP archives. *Id.* It identified text, executable files, binary data and UUencoded data.[21]

MIMEsweeper supported virus scanning by enabling the execution of third party virus packages, using those packages to scan for viruses, and quarantining any undesirable mail messages. When detected, the undesirable mail message was moved to a holding location and the administrator was notified. Mail message attachments were then reconstructed for scanning or behavior checking, depending on the virus protection technology used. MIMEsweeper provided

[18] MIMEsweeper at CLSW-00003
[19] MIMEsweeper at CLSW-00723
[20] MIMEsweeper at CLSW-00690-91
[21] MIMEsweeper at CLSW-00726-27

built-in interfaces for the majority of then existing virus protection packages, including ThunderByte, F-Prot, Dr Solomon's, and Sophos. [22]

Examples of well-publicized and commercially available products on the market prior to the Critical Date include, (1) the TFS Gateway, a commercially available secure mail gateway developed and distributed by TenFour Sweden AB, which included virus scanning capabilities and makes obvious the claims of the '600 patent,[23] (2) the Norman Firewall, a commercially available secure firewall with virus scanning capabilities developed and distributed by Norman Defense Data Systems, that makes obvious most, if not all, of the claims of the '600 patent,[24] (3) MIMEsweeper, a commercially available email gateway with antivirus scanning from Integralis Corporation, that makes obvious the claims of the '600 patent,[25] (4) Sidewinder, a firewall with antivirus scanning developed and promoted by Secure Computing Corporation, that makes obvious the claims of the '600 patent,[26] and (5) TIS Firewall, a firewall with flexible threat prevention facilities, that in combination with common antivirus scanning techniques makes obvious all of the claims of the '600 patent.[27]

In addition to the well-publicized prior art products that were not presented to, or considered by, the examiner, there were also numerous highly relevant texts and articles on the subject of virus scanning including network-based virus scanning – none of which were presented to, or considered by, the examiner during prosecution of the '600 patent. For example, the 1994 book, "*Firewall and Internet Security – Repelling the Wily Hacker*", by Cheswick and Bellovin,[28] was considered the definitive text on firewalls at the time, but was not made of record during prosecution of the '600

[22] MIMEsweeper at CLSW-00724, 00727-28
[23] TFS Gateway
[24] Norman Firewall
[25] MIMEsweeper
[26] Sidewinder
[27] TIS Firewall
[28] Cheswick and Bellovin at 70, 76 and chapter 6

patent. Moreover, Cheswick and Bellovin explicitly discusses all of the major concepts and components described in the '600 patent, including scanning files for viruses on a network device, such as a gateway or a file server. Cheswick and Bellovin states that the firewall can control all incoming and outgoing traffic, and in this context "control" means selectively forwarding traffic when certain conditions (such as no viruses) are met. As virus scanning was widely known, and the ability to control traffic was disclosed in this book, anyone of ordinary skill in the art reading Cheswick and Bellovin would have been readily able to construct the simple system, apparatus and methods claimed by the '600 patent.

Cheswick and Bellovin further teaches a firewall that includes filters and a gateway. The filter blocks transmission of certain classes of data and the gateway provides relay services. The application gateway described by Cheswick and Bellovin includes the ability to scan for viruses.

> An application-level gateway represents the opposite extreme in firewall design. Rather than using a general-purpose mechanism to allow many different kinds of traffic to flow, special-purpose code can be used for each desired application.... [I]t is easy to log and control *all* incoming traffic and outgoing traffic. The SEAL package [Ranum, 1992] from Digital Equipment Corporation takes advantage of this.... It is equally valuable to route incoming mail through a gateway.... Application gateways are often used in conjunction with the other gateway designs, packet filters, and circuit-level relays.... The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions.... The type of filtering depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.[29]

From the above historical context, it is clear that all of the following had been developed, commercially deployed and well-known prior to the Critical Date:

- Virus detection by signature scanning;
- Selective scanning of only file types likely to contain a virus, including the obvious consideration of file name extensions;
- Scanning at a desktop;
- Scanning a file in transit between two computers;

[29] Cheswick and Bellovin at 75-76.

- Scanning at a file server;
- Scanning at an internet gateway or firewall – including on proxy servers, and scanning FTP and SMTP traffic;
- Scanning encoded portions of email messages; and
- Taking certain preset actions once a virus was detected.

The references relied upon in this Request, including Cheswick, Cheswick and Bellovin, Layland, LANProtect, Sidewinder, TIS Firewall, TFS Manual, MIMEsweeper, MpScan and SunScreen SPF-100, were not considered during prosecution of the '600 patent. And, while Hile was considered during prosecution, it was not considered in the manner presented here and in light of the new, non-cumulative technological teachings contained in the prior art publications presented herewith. As discussed below, each of these prior art publications alone or in combination contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent, and properly considered, these references raise a number of substantial new questions of patentability with respect to claims 1-22 (all claims) of the '600 patent as pointed out in more detail below.

## IV. REQUIREMENTS FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510

Requester has satisfied each requirement for *ex parte* reexamination of the '600 patent.

### A. 37 C.F.R. § 1.510(b)(1) and (b)(2): Statement Pointing Out Each Substantial New Question of Patentability

A statement pointing out each substantial new question of patentability based on the cited patents and printed publications, and a detailed explanation of the pertinence and manner of applying the patents and printed publications to claims 1-22 (all claims) of the '600 patent is presented in Sections VI-VIII below in accordance with C.F.R. §

1.510(b)(1) and (b)(2).

### B. 37 C.F.R. § 1.510(b)(3): Copy of Every Patent or Printed Publication Relied Upon To Present a Substantial New Question of Patentability

A copy of every patent or printed publication relied upon to present a substantial new question of patentability is submitted herewith, pursuant to C.F.R. § 1.510(b)(3), as **Exhibits C through M**. Each of these cited prior art publications constitutes effective prior art as to the claims of the '600 patent under 35 U.S.C. § 103(a). Each of the relied upon prior art publications contains a new, non-cumulative technological teaching not present during the prosecution of the '600 patent. In general, no prior art was considered during prosecution of the '600 patent teaching or suggesting the use of a proxy server and a proxy daemon in connection with detecting a virus during data transfer and also selectively removing the virus based on determining whether the data is of type that is likely to contain a virus and performing a preset action based on results of virus scanning, whereas each of the relied upon prior art publications includes teaching regarding one or more of the foregoing limitations. Consequently, a reasonable examiner would consider these teachings as contained in Cheswick, Cheswick and Bellovin, the Layland reference, the LANProtect reference, the Sidewinder reference, the TIS Firewall reference, the MpScan reference or the SunScreen SPF-100 reference and Hile important in determining whether claims 1-22 are patentable.

### C. 37 C.F.R. § 1.510(b)(4): Copy of The Entire Patent For Which Reexamination is Requested

In accordance with 37 C.F.R. § 1.510(b)(4), a copy of the '600 patent is attached as Exhibit A.

### D. 37 C.F.R. § 1.510(b)(5): Certification That A Copy of the Request Has Been Served In Its Entirety On The Patent Owner

This Request is not being served on the correspondent of record for the '600 patent

as such service is believed to be futile in view of the fact that the Skjerven Morrill law firm dissolved on or about March 1, 2003. Pursuant to 37 C.F.R. §1.510(b)(5), a duplicate copy of this Request is being supplied to the Office on CD-ROM.

### E. 37 C.F.R. § 1.510(A): Fee For Requesting Reexamination

In accordance with 37 C.F.R. § 1.510(a), $2,520.00 is being submitted concurrently herewith via EFS-Web to cover the fee for reexamination.

## IV. OVERVIEW OF THE '600 PATENT AND ITS PROSECUTION HISTORY

### The Patent Claims

Claims 1-22 (all claims) of the '600 patent are invalid under 35 U.S.C. § 103(a) in view of the previously cited[30] and uncited prior art references listed above[31]. In considering the claims of the '600 patent, the claims must be "given their broadest reasonable interpretation consistent with the specification."[32] Relevant to the broadest-reasonable-construction analysis, please consider that applicant has published its position that any antivirus (AV) scanning on any network device infringes the claims of the '600 patent:

---

[30] Under 35 U.S.C. § 303(a), as amended in 2002 "[t]he existence of a substantial new question of patentability is not precluded by the fact that a patent or printed publication was previously cited by or to the Office or considered by the Office."

[31] Notably, the '600 patent was actively prosecuted during a period in which examiners where handcuffed by the "teaching, suggestion, motivation" (TSM) test in making obviousness rejections of pending claims. Pursuant to the TSM test, an examiner was constrained as to the prior art that he/she could use in putting forth an obviousness rejection. In view of the new obviousness standard articulated by the Supreme Court in KSR International Co. v. Teleflex Inc., 127 S. Ct. 1727, 2007 WL 1237837, which rejected the rigid and formalistic TSM approach of the Court of Appeals for the Federal Circuit, it is respectfully submitted the existence of a substantial new question of patentability can be made out in view of prior art patents and/or printed publications, which were considered by an examiner under the now rejected TSM test, when (1) a previously cited/considered reference is presented in a new light or a different way that escaped review during earlier examination or (2) a previously cited/considered reference is combined with one or more other prior art patents and/or printed publications which were not cited/considered during prosecution of the patent at issue (*See*, e.g., Manual of Patent Examining Procedure (8th ed., rev. 7, 2008) (hereafter "MPEP") §§ 2216, 2242 and 2258.01.

[32] The Federal Circuit's en banc decision in Phillips v. AWH Corp., 415 F.3d 1303 (Fed. Cir. 2005) expressly recognized that the USPTO employs the "broadest reasonable interpretation" standard.

> We are litigating [against] Barracuda, who are selling a ***gateway*** and putting ***whatever type of AV***, whether it's ClamAV or Shophos [*sic*] of whomever's AV, on there. [33]
>
> In the ['600] patent, we are not claiming that we invented the antivirus scanner. We are not claiming that we invented the proxy server. But the ***concept*** of using these two together so that you can stop the virus during the transition is new."[34]

The '600 patent issued from an application filed on September 26, 1995. The '600 patent claims a system and method for detecting computer viruses during FTP (File Transfer Protocol) and/or SMTP (Simple Mail Transfer Protocol) transfers at a server.[35] The specification of the '600 patent describes a gateway computer consisting of: a prior art computer system,[36] running a prior art operating system, such as BSD UNIX,[37] connecting two networks using prior art connection methods,[38] providing prior art data transfer services such as FTP and SMTP,[39] via prior art proxy servers modified according to the teaching of the patent.[40] The specification further describes scanning for viruses, which was also in the prior art, at an intermediary node between computers or computer networks.[41]

**Claim 1** recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:", and includes:

- a memory for storing data and routines,….. the memory including a server for scanning data for a virus..
- a communications unit for receiving and sending data in response to control signals,

[33] McMillan at p. 1 (emphasis added).
[34] McMillan at p. 2 (emphasis added).
[35] '600 patent, col. 1, ll. 10-13
[36] '600 patent at col. 3, l. 66 - col. 4, l. 17
[37] '600 patent at col. 5, ll. 10-16
[38] '600 patent at col. 4, ll. 36-45
[39] '600 patent at col. 7, ll. 2-9
[40] '600 patent at col. 5, l. 60 - col. 6, l. 3
[41] '600 patent at col. 4, l. 63 – col. 5, l. 26

- a processing unit for receiving signals from the memory and the communications unit…
- a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses….
- a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input,…

Claim 1 claims a computer-implemented method for detecting viruses on a proxy server. It includes steps for checking for the presence of a virus in the data and performing data handling actions depending on the result of the virus check. Because most of the specific verbiage of claim 1 simply recites common elements of computer systems and computer networks, consistent with applicant's stated construction of the scope of the claims of the '600 patent, claim 1 should be construed for purpose of this reexamination request to cover any system that performs anti-virus scanning on a network gateway (e.g., a proxy server).

Dependent **claim 2** adds the obvious limitation that the proxy server be a common (standard in the industry) "FTP proxy server". Similarly, dependent **claim 3** specifies the proxy server be a common (equally standard in the industry) SMTP proxy server.

Paralleling the claim 1 system, independent **claim 4** broadly claims a computer-implemented method for detecting viruses at a server. It includes steps for checking for the presence of a virus in the data and transferring the data depending on the result of the virus check. Distinct from claim 1, claim 4 includes the trivial and obvious step of determining whether the data is of a type that is likely to contain a virus and only checking for viruses if the data is of a type that is likely to contain a virus. **Claim 5** depends on claim 4 and adds the illusory limitation of storing the data in a temporary file at the server after the step of electronically transmitting. **Claim 6**

depends on claim 5 and adds the illusory limitation of scanning for viruses using signature scanning (the common industry-standard method for checking for viruses).

**Claim 7** depends on claim 4 and purports to add limitations to the various preset actions to be performed on the data. These obvious limitations include transmitting the data unchanged, not transmitting the data, storing the data in a file, and notifying the intended recipient of the new file. **Claim 8** depends on claim 4 and adds the trivial and obvious limitation of looking at the file extension to determine if the data is of a type likely to contain a virus.

Like claim 2, dependent **claims 9** and **10** restrict the steps of claim 4 to data transfers that are FTP transfers. Claims 9 and 10 further include the use of an FTP proxy server and an FTP daemon; while claim 9 refers to outbound transfers, and claim 10 describes inbound transfers.

**Claim 11** recycles obvious elements from prior claims but in the context of email messages (i.e., the network data to be inspected is email). The determination of whether the mail contains a virus is done by first determining whether the mail contain any encoded portion (i.e., the type of data commonly known at the time that may contain a virus). The step would further include storing each encoded portion of the mail message in a temporary file, decoding the encoded portions of the mail message to produced decoded portions of the mail message, scanning each of the decoded portions for a virus and testing whether the scanning step found any viruses. A preset action is performed on the mail message if the mail contains the virus. **Claim 12** depends on claim 11 and adds the illusory limitation of determining whether the mail message includes any encoded portions by looking for uuencoded (the most common industry standard email encoding scheme) portions.

Independent **claim 13** relates to a method for scanning a mail message transferred using an SMTP proxy server for viruses. As discussed above, given the ubiquitous nature of SMTP proxy servers, claim 13 is indistinguishable from claim 12. However, the scope of claim 13 under the

broadest reasonable construction standard is difficult to determine because the claim is inherently ambiguous as it fails to claim the subject matter that the applicants regarded as their invention. Specifically, claim 13 claims the opposite of what is disclosed in the specification. The specification describes the alleged invention as a system that conditionally checks an email for a virus – depending on whether it contains encoded portions (i.e., attachments). As shown in Figure 8B of the '600 patent, the system only checks for viruses in emails that have encoded portions. Email messages without encoded portions are allowed to pass through the system unchecked. Such a system is designed to conserve resources by not checking emails that are unlikely to contain a virus (i.e., emails without encoded portions). In contrast to the alleged invention described and disclosed in the specification, claim 13 recites a method for scanning emails for encoded portions, then unconditionally checking all emails for viruses – including emails without encoded portions. In any event, although somewhat ambiguous, the entire set of elements, is inherently obvious in view of the prior art.

Dependent **claim 14** is another recycled claim, as it purports to restrict the steps of claim 11 to require that the mail message be temporarily stored at the server and scanned for a virus. Dependent **claim 15** adds to the steps of claim 11 the illusory limitation that the scanning step be performed using a signature scanning process. **Claims 16** and **Claim 17** adds the recycled preset steps to be performed on the data based on the result of virus determining step.

The elements of independent **claim 18** are drafted in "means plus function" format. Claim 18 relates to an apparatus for detecting viruses in data transfers. The apparatus comprising the means for receiving a data transfer request including a destination address; means for electronically receiving data at a server; means for determining whether the data contains a virus at the server; means for performing a preset action on the data using the server if the data contains a virus; and

means for sending the data to the destination address if the data does not contain a virus. Dependent **claim 19** restricts claim 18 so that the means for determining the presence of a virus includes means for scanning the data using a signature scanning process. Dependent **claim 21** restricts claim 18 to include a "second means" to detect if the data is of a type likely to contain a virus and means to take specific actions depending on whether the data is of a type that is likely to contain a virus. Claim 21 is invalid because it is indefinite. Independent claim 18 recites an apparatus with a series of means-plus-function elements. Claim 21 depends from claim 18. The disputed language in claim 21 is a negative limitation that requires that certain steps recited in claim 18 not be performed on data that is unlikely to contain a virus. However, one of the steps that claim 21 purports to preclude — the "scanning" step —appears nowhere in claims 18 or 21. It is therefore impossible to determine what claim 21 prohibits. Because it is impossible to determine the scope of claim 21's negative limitation, the claim's scope is somewhat ambiguous and indefinite. Claim 21 seeks to address the selective scanning of the data for virus wherein the whole of the data passing between through the network is not scanned. In spite of claim 21 being indefinite, the aspect purported to be claimed in Claim 21 is obvious in light of the references presented below. Dependent **claim 22** restricts claim 18 to include a "second means" to qualify the destination address of the server.

**Prosecution of the '600 Patent Considering Prior Art Not Presented or Considered**

Herein Requester provides summaries of pertinent portions of the prosecution history, the specification and claims of the '600 patent to assist in giving the claims under reexamination their "broadest reasonable interpretation"[42] for purposes of reexamination. Requester notes, however, that the claim construction in reexamination is broader than claim construction in litigation. *See In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984). The summaries of the specification and

[42] The Federal Circuit's en banc decision in Phillips v. AWH Corp., 415 F.3d 1303 (Fed. Cir. 2005) expressly recognized that the USPTO employs the "broadest reasonable interpretation" standard.

claims provided herein and the following explanation regarding the prosecution history, therefore, are not intended to be an assertion regarding how the claims should be construed in litigation. Moreover, nothing in this Request should be construed as expressing any position as to whether the claims of the '600 patent would survive scrutiny under the patent-eligible subject matter analysis of *In re Bilski*, 545 F.3d 943 (Fed. Cir. 2008) (*en banc*) or whether the '600 patent satisfies the definiteness, enablement, best mode, or written description requirements of 35 U.S.C. § 112, since these grounds of invalidity cannot properly be raised in a request for reexamination. *See* MPEP § 2216 ("Questions relating to grounds of rejection other than those based on prior art patents or printed publications should not be included in the request and will not be considered by the examiner if included.").

The '600 patent was issued on April 22, 1997 from U.S. Application No. 08/533,706 (the "'706 application"), which was filed on September 26, 1995. As originally filed, the '706 application laid claim to a system, an apparatus and methods broadly directed at the concept of performing antivirus scanning on data being transmitted through an intermediate system (e.g., a proxy server) and selectively transferring the data depending on the existence of viruses in the data.

These broad claims were presented to the USPTO despite the fact that prior to the Critical Date, Trend Micro and Eva Chen where directly involved in product development and distribution of a prior art product, Intel's LANProtect product, upon which these broad claims read and which was commercially available and well publicized in 1992.[43]

In any event, on July 2, 1996, the applicant filed a Petition to Make Special ("Petition") based on a pre-examination search allegedly conducted by a professional searcher. The applicant

[43] LANProtect and Trend Micro History pages 7, 53-57 (showing Eva's involvement with the Intel LANProtect product).

provided a discussion of each of ten US patent documents allegedly identified during the pre-examination search. The applicant also pointed out alleged distinctions of the pending claims over each of the ten identified US patent documents. In the Petition, the applicant distinguished the purported "invention" over US Patent No. 5,511,163 of Lerche et al. ("Lerche") by virtue of the fact that allegedly Lerche "observes local network traffic and ***reacts only to viruses which have already entered the network***." See Petition at pg. 11. In contrast, the applicant explained since the "claimed invention prevents the spread of viruses in data transferred through the server, it can ***prevent the virus from ever penetrating the network***." Emphasis added. See Petition at pg. 11. Notably, no limitations existed in the pending claims to support this alleged distinction.

In the Petition, the applicant also presented alleged claim distinctions over Hile as follows:

> By contrast, Applicant's claimed invention facilitates the selective transfer of data using a server which is arranged to scan the data for a virus and, additionally, specify data handling actions dependent upon the existence of a virus. By including such ***virus scanning and data handling actions in a server***, Applicants' claimed invention prevents the spread of viruses in data transfers which are routed through the server such as those between a first computer outside of a network and a second computer within the network. Hile et al., however, merely scans data strings in the memory buffer of a computer which is the source or destination for data.
> Emphasis added. See Petition at pg. 4.

The applicant inexplicably made the above arguments despite being involved in the LANProtect product development and distribution. Meanwhile, the applicant never properly brought the LANProtect reference to the attention of the Examiner despite its inclusion of teachings regarding all or most of the purportedly novel aspects argued in the Petition. This Request seeks to remedy that oversight by providing this and other highly relevant references for proper consideration by the USPTO.

On August 27, 1996, Examiner Albert Decady, apparently unaware of the well publicized state of the art in commercial available antivirus systems of the time, issued a first substantive

Office action ("First Office Action"), which concluded that many of the claimed concepts were novel. The First Office Action indicated original dependent claims 2-4, 9-12, 16, 18, 19, 21 and 23 were allowable if rewritten in independent form and that original independent claim 22 and its dependents, i.e., claims 24, 25 and 26 were allowed.

With respect to original dependent claims 2-4, 11 and 12, the Examiner indicated they were allowable because:

> … the prior arts [*sic*] do not teach, singly or in combination, that the server is a ***proxy server*** nor do they teach a [*sic*] FTP or SMTP proxy server to handle evaluation and transfer of data files. The prior arts [*sic*] also fail to teach a daemon for transferring data from the proxy server wherein the daemon is an ***FTP or SMTP daemon***. (Emphasis added. See First Office Action at pg. 3)

With respect to original dependent claims 9 and 10, the Examiner indicated they were allowable because:

> … the prior arts [*sic*] fail to teach, singly or in combination, the step of ***determining whether the data is of a type [that is likely to contain a virus]*** and ***transmitting*** the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus. (Emphasis added. See First Office Action at pg. 3)

With respect to original dependent claim 16, the Examiner indicated it was allowable because:

> … the prior arts [*sic*] fail to teach, singly or in combination, that the server includes a ***SMTP proxy server*** and a ***SMTP daemon***. (Emphasis added. See First Office Action at pg. 3)

With respect to original dependent claims 18, 19 and 21, the Examiner indicated they were allowable because:

> … the prior arts [*sic*] fail to teach, singly or in combination, the steps of ***storing*** each encoded portion of the mail message (data) in a separate file; ***decoding*** the encoded

> portions of the data (mail message) to product decoded portions of the mail message; and ***scanning each of the decoded portions for a virus***.
> (Emphasis added. See First Office Action at pg. 4)

With respect to original independent claims 22, the Examiner indicated it was allowable because:

> … the prior arts [*sic*] taken singly or in combination fail to teach equivalent means, as disclosed in the application at bar, to carry out the claimed invention. For example … the present invention calls for a means for determining whether the data contains a virus at the server. This means, as disclosed in the specification, is the ***FTP proxy server*** or the ***SMTP proxy server***. The prior arts [*sic*] fail to teach these particular means or equivalent means to do the same [function]; therefore, the examiner favors the allowance of these claims (id). (Emphasis added. See First Office Action at pg. 4)

The remaining original claims (i.e., claims 1, 5-8, 13-15, 17 and 20 were rejected as being obvious. Claim 1 was rejected as being obvious over Lerche in view of Hile. The Examiner correctly noted that Hile taught selectively transferring a file based on the existence of a virus within the file; however, despite the teachings of Hile regarding other elements of the claim, the Examiner relied on Lerche for such teachings. Claims 5-8, 13-15, 17 and 20 were rejected as being obvious over Hile in view of Lerche.

On September 5, 1996, the USPTO granted the applicant's Petition and was thereafter acknowledged by the Examiner on September 18, 1996.

The applicant submitted a response to the First Office Action on September 24, 1996 ("First Amendment and Response"). In the First Amendment and Response, the applicant cancelled claims 2, 9, 14 and 18 and amended claims 1, 3, 4, 5, 7, 10, 13, 15, 16, 19-21 and 23. The applicant amended independent claim 1 (which issued as claim 1) to incorporate the proxy server and daemon limitations of former claim 2. The applicant amended independent claim 5 (which issued as claim 4) to incorporate the determining and transmitting steps of former dependent claim 9. The

applicant amended independent claim 13 (which issued as claim 11) to incorporate the storing, decoding and scanning steps of former dependent claim 18. The applicant rewrote dependent claim 16 (which issued as claim 13) in independent form by incorporating the limitations of claims 13 and 14. Notwithstanding Trend's direct involvement and knowledge regarding the LANProtect reference and its disclosure of most if not all the purportedly novel aspects, Trend did not cite the LANProtect reference to the examiner during prosecution.

On October 22, 1996, the USPTO mailed a Notice of Allowability indicating claims 1, 3-8, 10-13, 15-17 and 19-26 (later renumbered as 1, 2-7, 8-11, 12-14 and 15-22, respectively) were allowed with various changes made by way of an Examiner's Amendment.

The applicant paid the issue fee as a small entity and submitted formal drawings on November 20, 1996 and the '600 patent issued on April 22, 1997. After the '600 patent issued, on or about February 20, 1998, it allegedly came "to the attention of the patent owner that small entity status may not have been appropriate" and the applicant submitted a Letter under Rule 28 and Conditional Petition under Rule 137 for Delayed Payment of Balance of the Issue Fee under Rule 317 on February 20, 1998 concurrently with authorization to charge the issue fee deficiency to the deposit account of the applicant's representative.

## V. STATEMENT UNDER 37 C.F.R. § 1.510(B)(1) OF EACH SUBSTANTIAL NEW QUESTION OF PATENTABILITY BASED UPON PREVIOUSLY UNCITED PRIOR ART, INCLUDING DETAILED EXPLANATIONS FOR PERTINENCE AND MANNER OF APPLYING PRIOR ART UNDER 35 U.S.C. § 103

The claims of the '600 patent are unpatentable under 35 U.S.C. §103(a) in view of the prior art references provided herewith, which were not previously presented during the examination of the patent. As the following discussion demonstrates, claims 1-22 (all of the claims) of the '600

patent are invalid under 35 U.S.C. § 103(a) in view of the previously uncited prior art references under any reasonable interpretation of the claims.

The following is a list of each substantial new question of patentability based on prior patents and printed publications pursuant to 37 C.F.R. § 1.510(b)(1). References below are to claims in the '600 patent.

A. Whether claim 1 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference, the TIS Firewall reference, the TFS Manual reference and the MIMEsweeper reference;

B. Whether claim 1 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference, the TIS Firewall reference, the TFS Manual reference and the MIMEsweeper reference in combination with one or more admission by the patentee in the '600 patent, the '600 patent file wrapper, or in combination with the previously considered Hile reference;

C. Whether claim 2 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference and the TIS Firewall reference;

D. Whether claim 2 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference and the TIS Firewall reference, in combination with one or more admission by the patentee in the '600 patent, the '600 patent file wrapper, or in combination with the previously considered Hile reference;

E. Whether claim 3 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference, the TIS Firewall reference, the TFS Manual and the MIMEsweeper reference;

F. Whether claim 3 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference, the TIS Firewall reference, the TFS Manual reference and the MIMEsweeper reference in combination with one or more admission by the patentees in the '600 patent, the '600 patent file wrapper, or in combination with the previously considered Hile reference;

G. Whether claim 4 is obvious in view of the LANProtect reference, TIS Firewall reference and the TFS Manual reference;

H. Whether claim 4 is obvious in view the Cheswick and Bellovin reference, TIS Firewall reference and the Sidewinder reference;

I. Whether claim 5 is obvious in view of the LANProtect reference;

J. Whether claim 5 is obvious in view of the TIS Firewall reference, the Sidewinder reference and the MIMEsweeper reference;

K. Whether claim 6 is obvious in view of the LANProtect reference and the TIS Firewall reference;

L. Whether claim 6 is obvious in view of the Cheswick and Bellovin reference, the Sidewinder reference and the MpScan reference;

M. Whether claim 7 is obvious in view of the LANProtect reference and the TFS Manual reference;

N. Whether claim 7 is obvious in view of the Cheswick and Bellovin reference, the Sidewinder reference and the TIS Firewall references;

O. Whether claim 8 is obvious in view of the LANProtect reference and the TFS Manual reference;

P. Whether claim 8 is obvious in view of the Cheswick and Bellovin reference, the Sidewinder reference and the MIMEsweeper reference;

Q. Whether claim 9 is obvious in view of the TIS Firewall reference;

R. Whether claim 9 is obvious in view of the LANProtect reference and the Sidewinder reference;

S. Whether claim 10 is obvious in view of the TIS Firewall reference;

T. Whether claim 10 is obvious in view of the combination of the LANProtect reference and the Sidewinder reference;

U. Whether claim 11 is obvious in view of the LANProtect reference and the MIMEsweeper reference;

V. Whether claim 11 is obvious in view the LANProtect reference, the MIMEsweeper reference, the Sidewinder reference and the MpScan reference;

W. Whether claim 12 is obvious in view of the MpScan reference and the MIMEsweeper reference;

X. Whether claim 12 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference and the TIS Firewall reference, in combination with one or more admission by the patentees in the '600 patent or in combination with the previously considered Hile reference;

Y. Whether claim 13 is obvious in view of the LANProtect reference and the MIMEsweeper reference;

Z. Whether claim 13 is obvious in view of the LANProtect reference, the MIMEsweeper reference, the MpScan reference, the Sidewinder reference, the

Cheswick reference, the Cheswick and Bellovin reference, the TIS Firewall reference and the TFS Manual reference;

AA. Whether claim 14 is obvious in view of the LANProtect reference and the MIMEsweeper reference;

BB. Whether claim 14 is obvious in view of the LANProtect reference, the MIMEsweeper reference, the TIS Firewall reference, the Sidewinder reference, the MpScan reference and the Layland reference in combination with the previously considered Hile reference;

CC. Whether claim 15 is obvious in view of the LANProtect reference and the TIS Firewall reference;

DD. Whether claim 15 is obvious in view of the Cheswick and Bellovin reference, the Sidewinder reference and the MpScan reference;

EE. Whether claim 16 is obvious in view of the LANProtect reference and the MIMEsweeper reference;

FF. Whether claim 16 is obvious in view of the LANProtect reference, the MIMEsweeper reference, the Sidewinder reference, the TIS Firewall reference, the Layland reference and the SunScreen SPF-100 reference;

GG. Whether claim 17 is obvious in view of the LANProtect reference and the MIMEsweeper reference;

HH. Whether claim 17 is obvious in view of the LANProtect reference, the MIMEsweeper reference, the Sidewinder reference, the TIS Firewall reference, the Layland reference and the SunScreen SPF-100 reference;

II. Whether claim 18 is obvious in view of the TFS Manual reference, the LANProtect reference, the Cheswick and Bellovin reference and the TIS Firewall reference;

JJ. Whether claim 18 is obvious in view of the TFS Manual reference, the LANProtect reference, the Cheswick and Bellovin reference and the TIS Firewall reference in combination with the previously considered Hile reference;

KK. Whether claim 19 is obvious in view of the LANProtect reference and the TIS Firewall reference;

LL. Whether claim 19 is obvious in view of the Cheswick and Bellovin reference, the Sidewinder reference and the MpScan reference;

MM. Whether claim 20 is obvious in view of the LANProtect reference and the MIMEsweeper reference;

NN. Whether claim 20 is obvious in view of the LANProtect reference, the MIMEsweeper reference, the Sidewinder reference, the TIS Firewall reference, the Layland reference and the SunScreen SPF-100 reference;

OO. Whether claim 21 is obvious in view of the TFS Manual reference and the LANProtect reference;

PP. Whether claim 21 is obvious in view of the TFS Manual reference, the LANProtect reference and the Sidewinder reference;

QQ. Whether claim 22 is obvious in view of the TFS Manual reference, the LANProtect reference, the MIMEsweeper reference and the Cheswick and Bellovin reference; and

RR. Whether claim 22 is obvious in view of the TFS Manual reference, the LANProtect reference, the MIMEsweeper reference, the Cheswick and Bellovin reference, the MpScan reference and the TIS Firewall reference.

## VI. PERTINENCE AND MANNER OF APPLYING PRIOR ART UNDER 35 U.S.C. § 103

Claims 1-22 of the '600 patent are obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the Layland reference, the LANProtect reference, the Sidewinder reference, the TIS Firewall reference, Hile, TFS Manual, MIMEsweeper, MpScan and/or SunScreen SPF-100, individually, or in combination.

### Motivation to Combine

The articulated KSR obviousness standard[44] dictates that all of the highly relevant and related teachings and technology relating to virus scanning in Cheswick, Cheswick and Bellovin, Layland, LANProtect, Sidewinder, TIS Firewall, TFS Manual, MIMEsweeper, MpScan and SunScreen SPF-100 and Hile are clearly properly combinable and are representative of the obvious body of knowledge well within the grasp of the average practitioner skilled in the art of virus detection. Meanwhile, various of these references explicitly cite or refer to other of these references. For example, Cheswick and Bellovin includes a discussion of the TIS Firewall Toolkit (see, e.g., Cheswick and Bellovin at pg. 115) and SunScreen SPF-100 cites to Cheskwick and Bellovin (see, e.g., SunScreen SPF-100 at pg. 30).

The discussion below presents the pertinence and manner of applying the prior art under 35 U.S.C. § 103(a). The references are to the respective claims, Claims 1-22, in the '600 patent.

[44] In KSR International Co. v. Teleflex Inc., 127 S. Ct. 1727 (2007), the Supreme Court "beg[a]n by rejecting the rigid approach of the Court of Appeals" (i.e., requiring satisfaction of the "teaching, suggestion, motivation" (TSM) test) to show an invention would have been obvious (and is therefore unpatentable). Returning to its own nonobviousness cases, the Court held that "the [nonobviousness] analysis **need not seek out precise teachings directed to the *specific subject matter* of the challenged claim**, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ."

**A. Whether claim 1 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference, the TIS Firewall reference, the TFS Manual reference and the MIMEsweeper reference**

The teachings relating to use of proxy server and proxy daemons in connection with removing a virus during data transfers as contained in the references presented below were not present during the prior examination of the '600 patent. A reasonable examiner would consider these teachings important in determining whether claim 1 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 1 of the '600 patent.

**I. The Cheswick Reference**

The Cheswick reference was not considered during the prosecution of the '600 patent. It was published in June 1990 and discusses a secure network configuration involving a pair of machines (i) a trusted internal machine (AT&T's secure Internet gateway) and (ii) an untrusted external gateway. The Internet gateway passes mail and other common Internet services between AT&T's internal machines and the Internet, but protects the internal network even if the external machine is fully compromised.

**Cheswick makes obvious Claim 1 Under § 103(a)**

**Claim 1: "A system for"**

**(1) "...detecting and selectively removing viruses in data transfers..."**

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

Cheswick teaches the use and construction of a firewall or other system that can detect and deter various threats including viruses in data transfers. See Cheswick at 236 (Many Internet sites

use a gateway machine like a Sun. These machines forward IP packets in both directions, and provide a mail gateway service. The packet flow is still dangerous, though filtering is available).

**(2) "...a memory for storing data and routines, the memory having inputs and outputs, the memory including a server..."**

Claim 1 further recites "a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus." As the memory, routines, inputs and outputs are inherent in any computer-implemented virus scanning system, the only real limitations of any substance in the foregoing element are the common sense and obvious data handling actions.

Cheswick discloses memory, inputs and outputs, a server for scanning data as well as actions to be performed on finding a virus. See Cheswick at 234 ("Our new gateway machine, named inet, is a MIPS M/120 running System V with Berkeley enhancements. Various daemons and critical programs have been obtained from other sources, checked and installed.") Because Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

**(3) "...a communications unit for receiving and sending data in response to control signals..."**

Claim 1 further recites "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output." This element requires no more than that which would be inherently present in any system for transferring data – a communications unit for receiving and sending data.

Cheswick discloses network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, Cheswick discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals. See e.g., Cheswick at 235 (describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router).

**(4) "...a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit..."**

Claim 1 further recites "a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted." While stated quite verbosely, this element boils down to the simple detection of viruses in data and the selective transfer of such data based on the existence of viruses within such data.

Cheswick discloses and describes network systems, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of network virus

scanning. See Cheswick at 235(describing the use of an MIPS M/120 processor on the gateway, the base UNIX operating system, and the inclusion of an Ethernet board to connect to a router). The inclusion of memory and the attachment of memory to a communications process is inherent and obvious in the context of Cheswick. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick. As indicated above, since Cheswick clearly contemplates inet (AT&T's gateway) would be a convenient place to perform certain checks relating to inbound mail, inherently action would be taken by the gateway based on the results of the checks (e.g., the existence or non-existence of a virus in the data being transferred). See Cheswick at pg. 235.

**(5) "...a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses..."**

Claim 1 further recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred." In simple terms, a proxy server can be conceptually thought of as an intermediary that forwards IP traffic on behalf of the originator and then appears to be the origin of the IP traffic.

As evidenced by Cheswick, firewalls and gateways routinely and customarily implement proxy servers. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services); and the Abstract of Cheswick at pg. 233 ("This paper describes out Internet gateway. It is an application-level gateway that passes mail and many of the common Internet services between our internal machines and the internet). Despite the fact that the Examiner cited the proxy server as a point of

novelty when he allowed claim 1 during the original examination of the '600 patent, it should now be appreciated that proxy servers are a well-known and common mechanism for providing a layer of mediation between a private network and the Internet.

**(6) "...a daemon for transferring data from the proxy server in response to control signals from the proxy server..."**

Claim 1 further recites "a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred." Notwithstanding the Examiner's identification of a daemon as a point of novelty during the original examination of the '600 patent, this Request attempts to make it clear that daemons were well-known and widely used at the time the '600 patent was filed. Daemons are simply processes that run in the background (rather than under the direct control of a user) in the context of a multitasking operating system, such as the UNIX operating system. Prior to the filing of the '600 patent, there were and there remain many common daemons in the UNIX operating system, including, but not limited to, *syslogd* (a daemon that handles the system log), *sshd* (a daemon that handles incoming SSH connections), *ftpd* (a daemon that handles authentication and transfer of files for client processes), *smtpd* (a daemon that talks the SMTP with other SMTP daemons to receive mail from them and saves the mail into a spool directory for later processing).

While non-essential network daemons were removed from the Internet gateway described in Cheswick, the essential network daemons remained. Firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See

e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

Cheswick was not considered during prosecution of the '600 patent. Cheswick contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggested or taught use of a proxy server and a daemon in connection with removing a virus during data transfers. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 1 as pointed out above.

## II. The Cheswick and Bellovin Reference

The Cheswick and Bellovin reference was not considered during prosecution of the '600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers.

**Cheswick and Bellovin makes obvious Claim 1 Under § 103(a)**
**Claim 1: "A system for"**

**(1) "...detecting and selectively removing viruses in data transfers..."**

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. See Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. See Cheswick and Bellovin at 70. Cheswick and Bellovin also describes implementing various security operations at the gateway, including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76 ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

**(2) "...a memory for storing data and routines, the memory having inputs and outputs, the memory including a server..."**

Claim 1 further recites "a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus." As indicated above, since the memory,

routines, inputs and outputs are inherent in any computer-implemented virus scanning system, the only apparent limitations of any substance in the foregoing element are the common sense and obvious data handling actions.

Cheswick and Bellovin disclose memory, inputs and outputs, a server for scanning data and inherently disclose actions to be performed on finding a virus. As discussed further below, quarantining and/or deletion are typical and common sense actions.

**(3) "...a communications unit for receiving and sending data in response to control signals..."**

Claim 1 further recites "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output." As noted earlier, this element, a communications unit, would be inherently present in any system for transferring data.

Cheswick and Bellovin describe network systems, which when implemented as disclosed, necessarily have communications units to send and receive data in response to control signals as indicated by this element. For example, all of these references discuss handling network traffic, which is comprised of various network protocols such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals.

**(4) "...a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit..."**

Claim 1 further recites "a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to

the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted." Again, while there is quite a bit of verbiage present in this element, it essentially boils down to the simple detection of viruses in data and the selective transfer of such data based on the existence of viruses within such data.

Cheswick and Bellovin discloses and describes network systems, and as such necessarily have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of network virus scanning. The inclusion of memory and the attachment of memory to a communications process are inherent and obvious in any and all of the references cited herein. That virus scanning and selective data transfer utilizes the processor, memory, and communications unit is equally inherent and obvious in Cheswick and Bellovin. As indicated above, since Cheswick and Bellovin suggests scanning of incoming files by an application gateway, common sense requires selective transfer of the data based on whether a virus is detected.

**(5) "...a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses..."**

Claim 1 further recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred." As indicated above, a proxy server certainly was not a novel component at the time

of filing of the '600 patent. Rather, a proxy server was a common mechanism used to forward IP traffic and creating the appearance of the proxy server being the origin of the IP traffic.

Cheswick and Bellovin further illustrates the routine and customary implementation of proxy servers in the context of firewalls and gateways. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus). Consequently, this element is clearly taught by Cheswick and Bellovin.

**(6) "...a daemon for transferring data from the proxy server in response to control signals from the proxy server..."**

Claim 1 further recites "a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred." As indicated above, daemons were well-known and widely used at the time the '600 patent was filed. Daemons are simply processes that run in the background (rather than under the direct control of a user) in the context of a multitasking operating system, such as the UNIX operating system.

Cheswick and Bellovin describes firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network

security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

Cheswick and Bellovin was not considered during prosecution of the '600 patent. Cheswick and Bellovin contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches use of proxy server and proxy daemons in connection with removing a virus during data transfers. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 1 as pointed out above.

## III. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious Claim 1 Under § 103(a)**
**Claim 1: "A system for"**

**(1) "...detecting and selectively removing viruses in data transfers..."**

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

LANProtect teaches the use and construction of a network server that can detect and handle viruses in data transfers. See LANProtect at 1 ("Intel has taken a unique approach [with LANProtect], implementing virus protection as a network service rather than as a network application. Intel has done so by basing LANProtect on a network architecture that ***provides protection at the server*** without impacting performance—an architecture that will become the model for network-based virus protection in the future." Emphasis Added.); and LANProtect at 7 ("All information from the scan is stored in the LProtect log file at the file server. If a virus is detected, PCScan notifies the workstation user with options for handling the infection.")

**(2) "...a memory for storing data and routines, the memory having inputs and outputs, the memory including a server..."**

Claim 1 further recites "a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus."

LANProtect discloses memory, inputs and outputs, a server for scanning data and actions to be performed on finding a virus. See LANProtect at 7 ("All information from the scan is stored in the LProtect log file at the file server. If a virus is detected, PCScan notifies the workstation user with options for handling the infection.")

**(3) "...a communications unit for receiving and sending data in response to control signals..."**

Claim 1 further recites "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output;

LANProtect necessarily includes communications units to send and receive data in response to control signals as indicated by this element. LANProtect discusses handling network traffic, which is comprised of various network protocols, such as X11, UDP, FTP, Telnet and SNMP. Each of these protocols includes the handling of data traffic and associated control signals.

**(4) "...a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit..."**

Claim 1 further recites "a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted."

LANProtect discloses and describes network systems, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in each of these systems, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of network virus scanning

**(5) "...a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses..."**

Claim 1 further recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be

transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred."

LANProtect includes proxy servers by virtue of the fact that it runs in concert with the Netware operating system, and by virtue of its LProtect module. See LANProtect at 2 ("LANProtect vl.5 is a 100% server-based virus protection software product. The program utilizes a common set of files on a NetWare 3.1x file server and is comprised of the following key modules: LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses. LProtect is also WAN-compatible, offering automatic updates from one file server to any other file server across a backbone that may be running LProtect.").

**(6) "...a daemon for transferring data from the proxy server in response to control signals from the proxy server..."**

Claim 1 further recites "a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred."

LANProtect discloses and describes network communications systems, which when implemented as disclosed, necessarily have communications units to send and receive data as

indicated by this element. Firewalls, gateways and network mail servers routinely and customarily implement and include daemons that interact with proxy servers.

LANProtect was not considered during prosecution of the '600 patent. LANProtect contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches use of proxy server and proxy daemons in removing a virus during data transfers. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 1 as pointed out above.

## IV. The TFS Manual Reference

The TFS Manual reference was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network.

**TFS Manual makes obvious Claim 1 Under § 103(a)**
**Claim 1: "A system for"**

**(1) "...detecting and selectively removing viruses in data transfers..."**

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

TFS Manual discloses a method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. See, e.g., TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems.") and TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

**(2) "...a memory for storing data and routines, the memory having inputs and outputs, the memory including a server..."**

Claim 1 further recites "a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus." As noted above, in view of the fact that memory, routines, inputs and outputs are inherent in any computer-implemented virus scanning system, the only real limitations of any substance in the foregoing element are the common sense and obvious data handling actions.

The TFS Gateway as described by the TFS Manual has memory, inputs and outputs, a server for scanning data and actions to be performed on finding a virus. The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and the recipient will be notified. Requirements: To use this feature you need a Virus program, e.g. Dr Salomon's Antivirus.")

**(3) "...a communications unit for receiving and sending data in response to control signals..."**

Claim 1 further recites "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output."

TFS Manual discloses a series of gateway products that acts as a link between local as well as global mail systems. A gateway system as disclosed in the TFS Manual necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art.

**(4) "...a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit..."**

Claim 1 further recites "a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted." As a processing unit, the communications unit and memory are inherent in any computer-implemented virus scanning system, the only real limitations of any substance in the foregoing element are the common sense and obvious steps of detecting viruses and selectively transferring the data depending upon the existence of viruses.

TFS Manual discloses and describes a gateway system, and as such have communications units to send and receive data as indicated by this element. The inclusion of security features, including virus scanning in this system, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of gateway virus scanning. Meanwhile, it is inherent and common sense to make a decision based on a check being performed. Therefore, in view of the fact that TFS Manual expressly teaches checking for viruses in all incoming attachments, common sense suggests attachments confirmed to have a virus would not be forwarded to the intended destination and that attachments confirmed not to have a virus would be safe to pass. See TFS Manual at pg. 77.

**(5) "...a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses..."**

Claim 1 further recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred." During the prior examination, the only limitation of substance in this element was considered to be the proxy server; however, as noted above, proxy servers were pervasive.

TFS Manual discloses a gateway system that handled SMTP traffic and acts as a proxy server. See TFS Manual at 37 ("A unique quality with TFS is that it supports MIME both for sending and receiving mail. When TFS receives the message, it will scan the message. If it finds that the message is sent with MIME, it will convert it into proper format for the PC client to read. The same applies when sending messages. When sending a message, specify which character set

the recipient is using. If the recipient is using MIME, you can send the message with MIME.") Virtually all manually generated Internet e-mail is transmitted via SMTP in MIME format.

**(6) "...a daemon for transferring data from the proxy server in response to control signals from the proxy server..."**

Claim 1 further recites "a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred."

TFS Manual discloses a gateway system for sending and receiving e-mail messages across different networks. The TFS gateway uses an SMTP daemon. The SMTP daemon in the TFS Gateway was used to handle SMTP communication, both sending and receiving e-mail messages, including receiving the TCP/IP information and translating it into text files and then taking these files and translating them out to the recipient node. See TFS Manual at 37 ("A unique quality with TFS is that it supports MIME both for sending and receiving mail. When TFS receives the message, it will scan the message. If it finds that the message is sent with MIME, it will convert it into proper format for the PC client to read. The same applies when sending messages. When sending a message, specify which character set the recipient is using. If the recipient is using MIME, you can send the message with MIME.")

TFS Manual was not considered during prosecution of the '600 patent. TFS Manual contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches use of proxy server and proxy daemons in connection with

removing a virus during data transfers. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 1 as pointed out above.

## V. The TIS Firewall Reference

The TIS Firewall reference was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls.

**TIS Firewall makes obvious Claim 1 Under § 103(a)**
**Claim 1: "A system for"**

**(1) "...detecting and selectively removing viruses in data transfers..."**

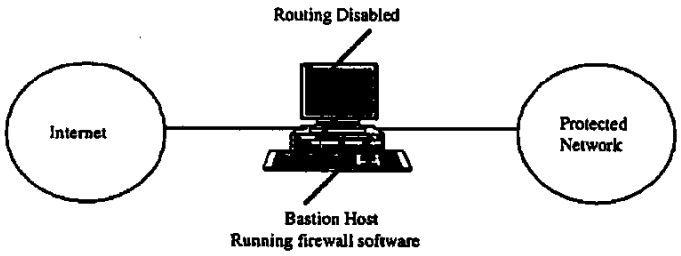
Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

TIS Firewall is an application-level firewall. As part of transferring messages, it checked for the presence of specific message features that were associated with known worms. Cheswick and Bellovin note that the TIS Firewall Toolkit can monitor incoming SMTP traffic, and "provides a hook for any necessary prefiltering of letter bombs." Cheswick and Bellovin at pg. 115. TIS Firewall also checked for the presence of certain keywords in the message. As scanning for

keywords representative of harmful content is equivalent to scanning for viruses, this element is taught by TIS Firewall.

**(2) "...a memory for storing data and routines, the memory having inputs and outputs, the memory including a server..."**

Claim 1 further recites "a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus."




TIS Firewall discloses memory, inputs and outputs, a server for scanning data and actions to be performed on finding a suspicious message feature. The Bastion host that runs the firewall software necessarily has a memory unit and any person skilled in the art would recognize the memory as an inherent feature of the TIS Firewall.

**(3) "...a communications unit for receiving and sending data in response to control signals..."**

Claim 1 further recites "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output."

TIS Firewall discloses a firewall system that provides secure access to the outside network. A firewall system as disclosed in TIS Firewall necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art.

**(4) "...a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit..."**

Claim 1 further recites "a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted."

TIS Firewall discloses a firewall system that provides a secure access to the outside network. A Firewall system as disclosed in TIS Firewall necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art.

The inclusion of security features, including checking for presence of specific message features, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of gateway virus scanning.

**(5) "...a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses..."**

Claim 1 further recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred."

TIS Firewall discloses a firewall system that handled SMTP and FTP traffic and acts as a proxy server. See TIS Firewall at 4 ("The toolkit software provides proxy services for common applications like FTP and TELNET, and security for SMTP mail. Since the bastion host is a security-critical network strong point, it is important that the configuration of the software on that system be as secure as possible.")

**(6) "...a daemon for transferring data from the proxy server in response to control signals from the proxy server..."**

Claim 1 further recites "a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred."

TIS Firewall discloses a firewall system for secure connection across different networks. TIS firewall uses an SMTP/FTP daemon. The FTP daemon in TIS Firewall was used to handle FTP communication. See TIS Firewall at 10 ("The toolkit includes source code for a modified version of the FTP daemon which permits an administrator to provide both FTP service and FTP proxy service on the same system.")

TIS Firewall was not considered during prosecution of the '600 patent. TIS Firewall contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches use of proxy server and proxy daemons in connection with removing a virus during data transfers. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP

§2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 1 as pointed out above.

## VI. The MIMEsweeper Reference

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email.

**MIMEsweeper makes obvious Claim 1 Under § 103(a)**
**Claim 1: "A system for"**

**(1) "...detecting and selectively removing viruses in data transfers..."**

Claim 1 recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

MIMEsweeper sits between organisations' mail systems, whether internal or external, and scans the contents of all mail for any undesirable attributes. See MIMEsweeper at 10. ("MIMEsweeper was conceived out of a requirement to scan incoming Email attachments for computer viruses").

**(2) "...a memory for storing data and routines, the memory having inputs and outputs, the memory including a server..."**

Claim 1 further recites "a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus."

MIMEsweeper discloses memory, inputs and outputs, a server for scanning data and actions to be performed on finding a suspicious message feature. See MIMEsweeper at 13 ("The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery."); MIMEsweeper at 7 ("Any mail message found to contain a virus … is 'quarantined'. The configurable nature of MIMEsweeper also allows the quarantining of other user-specified filetypes.") and MIMEsweeper at 9 ("Once in quarantine, MIMEsweeper provides a management tool for … [r]eleasing messages … [d]eletion of messages … [c]opying of quarantined messages … [a]rchiving of MIMEsweeper log files").

**(3) "…a communications unit for receiving and sending data in response to control signals..."**

Claim 1 further recites "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output."

MIMEsweeper discloses an email gateway system that provides a secure transfer of emails within a network from the outside network. A mail gateway system as disclosed in MIMEsweeper necessarily has a communication system for receiving and sending data and would be obvious to a person skilled in the art.

**(4) "…a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit..."**

Claim 1 further recites "a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted."

MIMEsweeper discloses an email gateway system that provides a secure transfer of emails within a network from the outside network. The inclusion of security features, including checking for presence of specific message features, necessarily incorporates a processor and communications controller claimed in this element, as these are fundamental and routine part of gateway virus scanning.

**(5) "...a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses..."**

Claim 1 further recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred."

MIMEsweeper discloses a mail gateway system that handled SMTP traffic and incorporates the features of a proxy server. See MIMEsweeper at 9 ("The pre-existing mail PO is typically duplicated, leaving the MIMEsweeper functionality and the new externally-facing Post Office

invisible to corporate users. The MIMEsweeper functionality and the internal PO(s) are similarly invisible to users outside the organisation.")

**(6) "...a daemon for transferring data from the proxy server in response to control signals from the proxy server..."**

Claim 1 further recites "a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred." As indicated above, a daemon is simply a process that runs in the background (rather than under the direct control of a user) in the context of a multitasking operating system, such as the UNIX operating system.

MIMEsweeper discloses an email gateway system for secure mail exchange across networks. MIMEsweeper utilizes a daemon that is used to handle mail communication. See MIMEsweeper at 75 ("A transfer agent moves data between message stores, normally without examining or modifying it"). See MIMEsweeper at 13 ("The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.").

MIMEsweeper was not considered during prosecution of the '600 patent. MIMEsweeper contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches use of proxy server and proxy daemons in connection with removing a virus during data transfers. As such, the substantial new question of patentability (SNQ)

presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 1 as pointed out above.

**B. Whether claim 1 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference, the TIS Firewall reference, the TFS Manual reference and the MIMEsweeper reference in combination with one or more admission by the patentee in the '600 patent, the '600 patent file wrapper, or in combination with the previously considered Hile reference**

None of Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS manual, and MIMEsweeper were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of proxy servers and proxy daemons in connection with removing a virus in data transfers was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the

patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and proxy daemons in connection with removing a virus during data transfers, raise a substantial new question of patentability with respect to claim 1 as pointed out in more detail below.

**Claim 1** recites "A system for detecting and selectively removing viruses in data transfers, the system comprising:"

- a memory for storing data and routines,….. the memory including a server for scanning data for a virus..
- a communications unit for receiving and sending data in response to control signals,
- a processing unit for receiving signals from the memory and the communications unit…
- a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses….
- a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input,…

In total, claim 1 claims a system for detecting and selectively removing viruses in data transfers. It should be noted that the memory unit, processing unit and communication unit, are all routine components, exceptionally well known in the art, and add nothing to support this claim being novel or non-obvious. The Hile reference, which was considered during the prosecution of the '600 patent, discloses these elements as detailed below.

Following is a discussion of how Cheswick, Cheswick and Bellovin, LANProtect reference, TIS Firewall, TFS manual and MIMEsweeper reference together in view of the previously considered Hile reference disclose (either expressly or inherently) and render obvious each limitation of claim 1.

Cheswick describes implementations of network systems utilizing firewall and gateways. Firewalls and gateways routinely and customarily implement proxy servers. It also mentions the use of daemons in scanning services. See e.g., Cheswick at 234-235 (discussing the implementation of a gateway and use of a proxy and various daemons in the context of providing scanning and security services).

In addition, Cheswick and Bellovin reference describe firewalls and gateways routinely and customarily implement proxy servers. See Cheswick and Bellovin at Chapter 6 ("Gateway tools", discussing the use of proxies and daemons as fundamental gateway components to manage network communications and provide network security services, including scanning for viruses and operations to deal with security threats, such as an included virus).

LANprotect also describes the claimed aspect of using a proxy server in connection with scanning for viruses at the gateway. See LANProtect at 2 ("LANProtect v1.5 is a 100% server-based virus protection software product. The program utilizes a common set of files on a NetWare 3.1x file server and is comprised of the following key modules: LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses. LProtect is also WAN-compatible, offering automatic updates from one file server to any other file server across a backbone that may be running LProtect.").

Furthermore TFS manual discloses a proxy server in context of email transfers. Here, the proxy server handles SMTP traffic. See TFS Manual at 37 ("A unique quality with TFS is that it supports MIME both for sending and receiving mail. When TFS receives the message, it will scan

the message. If it finds that the message is sent with MIME, it will convert it into proper format for the PC client to read. The same applies when sending messages. When sending a message, specify which character set the recipient is using. If the recipient is using MIME, you can send the message with MIME.")

TIS Firewall specifically and clearly discloses the use of an FTP/SMTP daemon for ensuring secure connection across different networks. See TIS Firewall at 10 ("The toolkit includes source code for a modified version of the FTP daemon which permits an administrator to provide both FTP service and FTP proxy service on the same system.")

MIMEsweeper discloses a mail gateway system that handled SMTP traffic and incorporates the feature of a proxy server. See MIMEsweeper at 9 ("The pre-existing mail PO is typically duplicated, leaving the MIMEsweeper functionality and the new externally-facing Post Office invisible to corporate users. The MIMEsweeper functionality and the internal PO(s) are similarly invisible to users outside the organisation."). MIMEsweeper utilizes a daemon that is used to handle mail communication. See MIMEsweeper at 75 ("A transfer agent moves data between message stores, normally without examining or modifying it"). See MIMEsweeper at 13 ("The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.").

The teachings as contained in Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS manual and MIMEsweeper were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination. As described above, a reasonable examiner would consider these combined teachings important in determining whether

claim 1 is patentable. For this reason, the teachings of Hile in combination with the teachings by Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS manual and MIMEsweeper raise a substantial new question of patentability with respect to at least claim 1 of the '600 patent.

### C. Whether claim 2 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference and the TIS Firewall reference

Claim 2 adds as the specific proxy server type, "a FTP proxy server". However, the restriction on the proxy server element to an FTP proxy server is a meaningless restriction because the FTP proxy server is, and was, a very common (if not the most common) proxy server, included on virtually every file server and electronic mail system as of the Critical Date.

None of Cheswick, Cheswick and Bellovin, LANProtect and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of proxy servers and proxy daemons in connection with removing a virus during data transfers, wherein the proxy server is an FTP proxy server and the proxy daemon is an FTP daemon was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith,

which include materials describing the use of proxy servers and proxy daemons in connection with removing a virus during data transfers, wherein the proxy server is an FTP proxy server and the proxy daemon is an FTP daemon, raise a substantial new question of patentability with respect to claim 2 as pointed out in more detail below.

## I. The Cheswick Reference

The Cheswick reference was not considered during the prosecution of the '600 patent. It was published in June 1990 and discusses a secure network configuration involving a pair of machines (i) a trusted internal machine (AT&T's secure Internet gateway) and (ii) an untrusted external gateway. The Internet gateway passes mail and other common Internet services between AT&T's internal machines and the Internet, but protects the internal network even if the external machine is fully compromised.

**Cheswick makes obvious Claim 2 Under § 103(a)**

**Claim 2: "wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files"**

Claim 2 recites "The system of claim 1, wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files, and the daemon is an FTP daemon that communicates with a recipient node and transfers data files to the recipient node."

Cheswick discloses the use of an FTP proxy server. See Cheswick at 234 ("*Pftp* provides FTP access in a similar manner." "We provide incoming login and mail service. For incoming file transfer, inet provides an anonymous FTP service").

## II. The Cheswick and Bellovin Reference

The Cheswick and Bellovin reference was not considered during prosecution of the '600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers.

**Cheswick and Bellovin makes obvious Claim 2 Under § 103(a)**

**Claim 2: "wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files"**

Claim 2 recites "The system of claim 1, wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files, and the daemon is an FTP daemon that communicates with a recipient node and transfers data files to the recipient node."

Cheswick and Bellovin discloses the use of an FTP proxy server. See e.g., Firewalls and Internet Security, Cheswick and Bellovin (1994) at 94 ("As we have described, outgoing FTP sessions normally require an incoming TCP call. To support this, our proxy service can listen on a newly created socket. The port number is passed back to the caller, which generates the appropriate FTP PORT command. The call is thus outgoing from the user's machine to the firewall, but incoming from the FTP server.").

## III. The TIS Firewall Reference

The TIS Firewall reference was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls.

**TIS Firewall makes obvious Claim 2 Under § 103(a)**

**Claim 2: "wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files"**

Claim 2 recites "The system of claim 1, wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files, and the daemon is an FTP daemon that communicates with a recipient node and transfers data files to the recipient node."

TIS Firewall utilizes an FTP proxy server that handles evaluation and transfer of data files and an FTP daemon that communicates with a recipient node and transfers data to the recipient node. See TIS Firewall at 10 ("In order to permit file transfer through the firewall without risking compromising the firewall's security an FTP proxy server is provided.")

## IV. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious Claim 2 Under § 103(a)**

**Claim 2: "wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files"**

Claim 2 recites "The system of claim 1, wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files, and the daemon is an FTP daemon that communicates with a recipient node and transfers data files to the recipient node."

It would have been obvious to use the Intel Products LANProtect at an FTP proxy server and to utilize an FTP daemon. LANProtect was designed to be installed and run on a NetWare server, which is a computer that has a Novell loadable module running on it. The NetWare server receives a request from a user on the local area network. The NetWare server then determines whether to send the requested information to the user. If the NetWare server decides to send the information to the user, the file is transmitted electronically in units called packets. Each packet includes a header, and part of the information included in the header is the destination address

where the information is being sent. See LANProtect at 5 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail me transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses."). In addition, it would have been obvious to use the network file server/scanning system disclosed by LANProtect at a mail server, and implementing an FTP proxy server and an FTP daemon.

**D. Whether claim 2 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference and the TIS Firewall reference, in combination with one or more admission by the patentee in the '600 patent, the '600 patent file wrapper, or in combination with the previously considered Hile reference**

None of Cheswick, Cheswick and Bellovin, LANProtect and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of proxy servers and proxy daemons in connection with removing a virus during data transfers, wherein the proxy server is an FTP proxy server and the proxy daemon is an FTP daemon was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith,

which include materials describing the use of proxy servers and proxy daemons in connection with removing a virus during data transfers, wherein the proxy server is an FTP proxy server and the proxy daemon is an FTP daemon, raise a substantial new question of patentability with respect to claim 2 as pointed out in more detail below.

**Claim 2** recites "the proxy server is a FTP proxy server that handles evaluation and transfer of data files, and the daemon is an FTP daemon that communicates with a recipient node and transfers data files to the recipient node."

In total, Claim 2 adds as the specific proxy server type, "a FTP proxy server". However, the restriction on the proxy server element to an FTP proxy server is a meaningless restriction because the FTP proxy server is, and was, a very common (if not the most common) proxy server, included on virtually every file server and electronic mail system as of the Critical Date.

Following is a discussion of how Cheswick, Cheswick and Bellovin, LANProtect and TIS Firewall together in view of the previously considered Hile reference disclose (either expressly or inherently) and render obvious each limitation of claim 2.

Cheswick discloses the use of an FTP proxy server. See Cheswick at 234 ("*Pftp* provides FTP access in a similar manner." "We provide incoming login and mail service. For incoming file transfer, inet provides an anonymous FTP service").

In addition, Cheswick and Bellovin also discloses the use of an FTP proxy server. See e.g., Firewalls and Internet Security, Cheswick and Bellovin (1994) at 94 ("As we have described, outgoing FTP sessions normally require an incoming TCP call. To support this, our proxy service can listen on a newly created socket. The port number is passed back to the caller, which generates the appropriate FTP PORT command. The call is thus outgoing from the user's machine to the firewall, but incoming from the FTP server.").

Furthermore, it would have been obvious to use the Intel Products LANProtect at an FTP proxy server and to utilize an FTP daemon. LANProtect was designed to be installed and run on a NetWare server, which is a computer that has a Novell loadable module running on it. The NetWare server receives a request from a user on the local area network. The NetWare server then determines whether to send the requested information to the user. If the NetWare server decides to send the information to the user, the file is transmitted electronically in units called packets. Each packet includes a header, and part of the information included in the header is the destination address where the information is being sent. See LANProtect at 5 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail me transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses."). In addition, it would have been obvious to use the network file server/scanning system disclosed by the LANProtect at a mail server, and implementing an FTP proxy server and an FTP daemon.

Additionally, TIS Firewall utilizes an FTP proxy server that handles evaluation and transfer of data files and an FTP daemon that communicates with a recipient node and transfers data to the recipient node. See TIS Firewall at 10 ("In order to permit file transfer through the firewall without risking compromising the firewall's security an FTP proxy server is provided.")

The teachings as contained in Cheswick, Cheswick and Bellovin, LANProtect and TIS Firewall were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination. As described above, a reasonable examiner would consider these combined teachings important in determining whether

claim 2 is patentable. For this reason, the teachings of Hile in combination with the teachings by Cheswick, Cheswick and Bellovin, LANProtect and TIS Firewall raise a substantial new question of patentability with respect to at least claim 2 of the '600 patent.

**E. Whether claim 3 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference, the TIS Firewall reference, the TFS Manual and the MIMEsweeper reference**

Claim 3 adds the specific daemon type, an "SMTP daemon". However, the restriction on the daemon to an SMTP daemon is a hollow restriction as the SMTP daemon is, and was, a very common daemon, included on virtually every electronic mail system as of the Critical Date.

None of Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of proxy servers and proxy daemons in connection with removing a virus during data transfers, wherein the proxy server is an SMTP proxy server and the proxy daemon is an SMTP daemon was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and proxy daemons in connection with

removing a virus during data transfers, wherein the proxy server is an SMTP proxy server and the proxy daemon is an SMTP daemon, raise a substantial new question of patentability with respect to claim 3 as pointed out in more detail below.

## I. The Cheswick Reference

The Cheswick reference was not considered during the prosecution of the '600 patent. It was published in June 1990 and discusses a secure network configuration involving a pair of machines (i) a trusted internal machine (AT&T's secure Internet gateway) and (ii) an untrusted external gateway. The Internet gateway passes mail and other common Internet services between AT&T's internal machines and the Internet, but protects the internal network even if the external machine is fully compromised.

**Cheswick makes obvious Claim 3 Under § 103(a)**

**Claim 3: "wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages"**

Claim 3 recites "The system of claim 1, wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node."

The Cheswick reference discloses the use of SMTP proxy server that handles mail communication. See Cheswick at 234 ("Outgoing mail is sent to inet via SMTP over either Datakit or the internal Internet. It is stored and forwarded from there. Upas performs the mail gateway functions."). Cheswick also disclose the use of a server daemon in a gateway system. See Cheswick at 234 ("Our new gateway machine, named inet, is a MIPS M/120 running System V with Berkeley-enhancements. Various daemons and critical programs have been obtained from other sources, checked, and installed.")

## II. The Cheswick and Bellovin Reference

The Cheswick and Bellovin reference was not considered during prosecution of the '600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers.

**Cheswick and Bellovin makes obvious Claim 3 Under § 103(a)**

**Claim 3: "wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages"**

Claim 3 recites "The system of claim 1, wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node."

Cheswick and Bellovin discusses SMTP as a common proxy type necessary for the prolific Sendmail program, and discusses the SMTP proxy in the context of security and filtering. *See* Cheswick and Bellovin at 189 ("A summary of the most common proxy connections [including SMTP] is shown in Table 11.1."). *See also* Cheswick and Bellovin at 242 (disclosing sources for a variety of network daemons, including sites and code bases that contained SMTP daemons such as the source site for BSD UNIX source code Version 4.2).

## III. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious Claim 3 Under § 103(a)**

**Claim 3: "wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages"**

Claim 3 recites "The system of claim 1, wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node."

LANProtect specifically notes scanning network traffic of any type. *See e.g.*, LANProtect at 5 ("All network traffic originating outside the file server (e.g., from workstations, modem servers, email file transfer etc.) and all network traffic originating at the file server is scanned for virus infections."). In addition, it would have been obvious to use the network file server/scanning system disclosed by the LANProtect reference at a mail server, and implementing a SMTP proxy server and an SMTP daemon.

## IV. The TIS Firewall Reference

The TIS Firewall reference was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls.

**TIS Firewall makes obvious Claim 3 Under § 103(a)**
**Claim 3: "wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages"**

Claim 3 recites "The system of claim 1, wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node."

TIS Firewall reference discloses the TIS Firewall Toolkit included an SMTP proxy server called "smap," which stands for "Simple Mail Access Protocol." See TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to

users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

## V. The TFS Manual Reference

The TFS Manual reference was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network.

**TFS Manual makes obvious Claim 3 Under § 103(a)**
**Claim 3: "wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages"**

Claim 3 recites "The system of claim 1, wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node."

TFS Manual contained an SMTP proxy server and an SMTP daemon to perform mail communication across networks. See TFS Manual at 28. TFS Manual also mentions the message server software. See TFS Manual at 35. ("TFS requires both the Message Server software and API software to be active.")

## VI. The MIMEsweeper Reference

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email.

**MIMEsweeper makes obvious Claim 3 Under § 103(a)**
**Claim 3: "wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages"**

Claim 3 recites "The system of claim 1, wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node."

MIMEsweeper discloses the use of an SMTP proxy server and an SMTP daemon to perform mail communication across networks. See MIMEsweeper at 13 ("The client server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery. The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.")

**F. Whether claim 3 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference, the TIS Firewall reference, the TFS Manual reference and the MIMEsweeper reference in combination with one or more admission by the patentees in the '600 patent, the '600 patent file wrapper, or in combination with the previously considered Hile reference**

None of Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of proxy servers and proxy daemons in connection with removing a virus during data transfers, wherein the proxy server is an SMTP proxy server and the proxy daemon is an SMTP daemon was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on

the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and proxy daemons in connection with removing a virus during data transfers, wherein the proxy server is an SMTP proxy server and the proxy daemon is an SMTP daemon, raise a substantial new question of patentability with respect to claim 2 as pointed out in more detail below.

**Claim 3** recites "the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node."

In total, Claim 3 adds as the specific proxy server type, "a SMTP proxy server". However, the restriction on the proxy server element to an SMTP proxy server is a meaningless restriction because the SMTP proxy server is, and was, a very common (if not the most common) proxy server, included on virtually every electronic mail system as of the Critical Date.

Following is a discussion of how Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper together in view of the previously considered Hile reference disclose (either expressly or inherently) and render obvious each limitation of claim 3.

Cheswick discloses the use of SMTP proxy server that handles mail communication. See Cheswick at 234 ("Outgoing mail is sent to inet via SMTP over either Datakit or the internal Internet. It is stored and forwarded from there. Upas performs the mail gateway functions."). Cheswick also disclose the use of a server daemon in a gateway system. See Cheswick at 234 ("Our new gateway machine, named inet, is a MIPS M/120 running System V with Berkeley-

enhancements. Various daemons and critical programs have been obtained from other sources, checked, and installed.")

In addition, Cheswick and Bellovin discusses SMTP as a common proxy type necessary for the prolific Sendmail program, and discusses the SMTP proxy in the context of security and filtering. *See* Cheswick and Bellovin at 189 ("A summary of the most common proxy connections [including SMTP] is shown in Table 11.1."). *See also* Cheswick and Bellovin at 242 (disclosing sources for a variety of network daemons, including sites and code bases that contained SMTP daemons such as the source site for BSD UNIX source code Version 4.2).

Furthermore, LANProtect specifically notes scanning network traffic of any type. *See e.g.*, LANProtect at 5 ("All network traffic originating outside the file server (e.g., from workstations, modem servers, email file transfer etc.) and all network traffic originating at the file server is scanned for virus infections."). In addition, it would have been obvious to use the network file server/scanning system disclosed by LANProtect at a mail server, and implementing a SMTP proxy server and an SMTP daemon.

Additionally, TIS Firewall discloses the TIS Firewall Toolkit included an SMTP proxy server called "smap," which stands for "Simple Mail Access Protocol." See TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

In addition, TFS Manual contained an SMTP proxy server and an SMTP daemon to perform mail communication across networks. See TFS Manual at 28. TFS Manual also mentions the

message server software. See TFS Manual at 35 ("TFS requires both the Message Server software and API software to be active.")

Finally, MIMEsweeper discloses the use of an SMTP proxy server and an SMTP daemon to perform mail communication across networks. See MIMEsweeper at 13 ("The client server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery. The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.")

The teachings as contained in Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination. As described above, a reasonable examiner would consider these combined teachings important in determining whether claim 3 is patentable. For this reason, the teachings of Hile in combination with the teachings by Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall, TFS Manual and MIMEsweeper raise a substantial new question of patentability with respect to at least claim 3 of the '600 patent.

### G. Whether claim 4 is obvious in view of the LANProtect reference, TIS Firewall reference and the TFS Manual reference

Independent claim 4 relates to a computer-implemented method for detecting viruses at a server. It includes steps for checking for the presence of a virus in the data and transferring the data depending on the result of the virus check. Claim 4 also includes steps for determining whether the

data is of a type that is likely to contain a virus and only determining whether a virus is present if the data is of a type that is likely to contain a virus. The steps of claim 4 are obvious in view of one or more references as discussed below:

## I. The TFS Manual Reference

The TFS Manual reference was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network.

**TFS Manual makes obvious Claim 4 Under § 103(a)**
**Claim 4: "A computer implemented method"**

**(1) "...for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:....."**

Claim 4 recites "A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:"

TFS Manual discloses a gateway having a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. See, e.g., TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

**(2) "...receiving at a server a data transfer request including a destination address;"**

Claim 4 further recites "receiving at a server a data transfer request including a destination address."

TFS Manual discloses a gateway that receives mail message requests using SMTP, and other protocols. *See, e.g.*, TFS Manual, Chapter on "Receiving Mail from Internet Mail" (TFS "will send any outgoing messages and receive any incoming messages."); An incoming message directed to a recipient will have a destination address and this would be obvious to any person skilled in the art. The limitation of the data transfer request containing a destination address in inherent in the TFS Manual.

**(3) "…electronically receiving data at the server;..."**

Claim 4 further recites "electronically receiving data at the server."

TFS Manual discloses a gateway wherein the mail message would necessarily be electronically received at the server.

**(4) "…determining whether the data contains a virus at the server;"**

Claim 4 further recites "determining whether the data contains a virus at the server."

TFS Manual discloses a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. See, e.g., See, e.g., TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming

attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

**(5) "...performing a preset action on the data using the server if the data contains a virus;"**

Claim 4 further recites "performing a preset action on the data using the server if the data contains a virus."

TFS Manual teaches the gateway would perform different actions depending on the results of the virus scanning. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

**(6) "...sending the data to the destination address if the data does not contain a virus;"**

Claim 4 further recites "sending the data to the destination address if the data does not contain a virus."

TFS Manual teaches the gateway would perform different actions depending on the results of the virus scanning. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

**(7) "...determining whether the data is of a type that is likely to contain a virus; and;"**

Claim 4 further recites "determining whether the data is of a type that is likely to contain a virus."

TFS Manual discloses this claim element. The TFS Gateway described in TFS Manual would not scan the inline part of the message or text-only attachments because there was no risk that text files would create any damage. See TFS Manual at pg. 77 (example contents of a VIRUS.BAT file are shown in which only executable files are scanned). Additionally, the TFS Gateway could be used with commercially available antivirus scanners at the time, such as McAfee's VirusScan, Dr Solomon's and IBM Antivirus, which would only scan files likely to contain a virus. See TFS Manual at 77. These antivirus scanners could also compare the extension type of the file to be scanned with extension types known to be able to contain a virus.

**(8) "...transmitting the data from the server to the destination without performing the steps of determining....."**

Claim 4 further recites "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus."

TFS Manual discloses this claim element. If a mail message does not have any encoded portions, the TFS Gateway sends it to the destination address without first scanning it for viruses. Therefore, it was not scanned and no preset action was taken. The mail message was simply forwarded to its destination. In addition, as discussed above, if the commercially available antivirus scanner determined a file was not of a type likely to contain a virus, that file would not be scanned, and the TFS Gateway would transmit the file to its destination.

TFS Manual was not considered during prosecution of the '600 patent. TFS Manual contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus.". As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 4 as pointed out above.

## II. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious Claim 4 Under § 103(a)**
**Claim 4: "A computer implemented method"**

**(1) "...for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:"**

Claim 4 recites "A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:"

LANProtect discloses detecting viruses during file transfers between computers. *See, e.g.*, LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library … to scan those files for known viruses.").

**(2) "…receiving at a server a data transfer request including a destination address;"**

Claim 4 further recites "receiving at a server a data transfer request including a destination address."

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

**(3) "…electronically receiving data at the server;"**

Claim 4 further recites "electronically receiving data at the server."

LANProtect discloses electronically receiving data at the server. See e.g., LANProtect at pg. 27 ("Scan both incoming and outgoing files on the server with the Real Time scan"). The receiving of data (incoming and outgoing files) electronically is an inherent and fundamental aspect

of any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

**(4) "...determining whether the data contains a virus at the server;"**

Claim 1 further recites "determining whether the data contains a virus at the server."

LANProtect product literature expressly teaches this step. *See, e.g.*, LANProtect at pp. 3, 6 and 11 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v.1.5 has additional virus detection technology to effectively handle these types of viruses .... LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (*e.g.*, from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).

**(5) "...performing a preset action on the data using the server if the data contains a virus;"**

Claim 1 further recites "performing a preset action on the data using the server if the data contains a virus."

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving

the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

**(6) "...sending the data to the destination address if the data does not contain a virus;"**

Claim 1 further recites "sending the data to the destination address if the data does not contain a virus."

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

**(7) "...determining whether the data is of a type that is likely to contain a virus; and;"**

Claim 1 further recites "determining whether the data is of a type that is likely to contain a virus."

LANProtect permits the program, user, or administrator to identify the types of files to be scanned for viruses (*e.g.*, DOS files with ".EXE" extension). *See, e.g.*, LANProtect at p. 6 ("The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).")

**(8) "...transmitting the data from the server to the destination without performing the steps of determining....."**

Claim 1 further recites "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus."

LANProtect discloses that this step is performed by the LANProtect product. When the LANProtect product is configured to scan only those file types likely to contain a virus (e.g., DOS files with ".EXE" extension as configured by the user or administrator), LANProtect does not scan other file types or take any of the preset actions described above on the other file types, thereby meeting this limitation.

LANProtect was not considered during prosecution of the '600 patent. LANProtect contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus." As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 4 as pointed out above.

### H. Whether claim 4 is obvious in view the Cheswick and Bellovin reference, TIS Firewall reference and the Sidewinder reference

None of Cheswick and Bellovin, TIS Firewall and Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art considered during prosecution of the '600 patent taught or suggested "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus."

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith raise a substantial new question of patentability with respect to claim 4 as pointed out in more detail below.

**Claim 4** recites "A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:"

- receiving at a server a data transfer request including a destination address;
- electronically receiving data at the server;
- determining whether the data contains a virus at the server;
- performing a preset action on the data using the server if the data contains a virus;

- sending the data to the destination address if the data d determining whether the data is of a type that is likely to contain a virus; and does not contain a virus;
- determining whether the data is of a type that is likely to contain a virus; and
- transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus.

### I. Cheswick and Bellovin in view of Sidewinder renders obvious Claim 4 Under § 103(a)

The Cheswick and Bellovin reference was not considered during the prosecution of the '600 patent. It was published in 1994, to discuss a new paradigm in firewall and internet security.

Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. See Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. See Cheswick and Bellovin at 70. Cheswick and Bellovin also describes implementing various security operations at the gateway including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76. ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned

on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

Cheswick and Bellovin describes a system that receives data transfer requests with a destination address at a server. See e.g., Cheswick and Bellovin at pg. 66-69 and 74-75.

Cheswick and Bellovin describes that the incoming files are scanned for virus therefore the data is received electronically. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

Cheswick and Bellovin describes scanning for viruses at a server. See e.g., Cheswick and Bellovin at pg. 76 ("A location with many PC users might wish to scan incoming files for viruses.").

Cheswick and Bellovin describes filtering files that do not meet the criteria of the gateway and thus would filter a file containing a virus in a preset manner. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

Cheswick and Bellovin teaches that the firewall can log and control all incoming and outgoing traffic. Controlling all traffic includes sending the data to the destination address if the data meets the criteria of the gateway, or for example, does not contain a virus. *See e.g.*, Cheswick and Bellovin at pg. 74-75.

To the extent the aspect of "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus." is not taught or suggested by Cheswick and Bellovin, this element is disclosed or suggested by Sidewinder as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations. MPEP § 2143. Motivation to

combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses the element of determining whether the data is of a type that is likely to contain virus. See Sidewinder at SR-454.10 ("Sidewinder can detect and block messages that are not English language text and that therefore could contain viruses"). Sidewinder also discloses the element of transmitting the data without performing the determination step. See Sidewinder at SR-454.4 (indicating certain classes of data can be selectively prohibited from passing to and from the external network).

So, a person having ordinary skill in the art can easily use the teachings of Cheswick and Bellovin in combination with the teachings of Sidewinder to come up with a computer implemented method of virus detection at the server wherein the virus detection is selectively done by determining whether the data is of type that is likely to contain a virus and transmitting the data if the data is not of type that is likely to contain a virus.

Neither Cheswick and Bellovin nor Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects of determining whether the file is of type that is likely to contain virus, transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and

taking a preset action if the data contains a virus. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 4 as pointed out above.

## II. TIS Firewall in view of Sidewinder renders obvious Claim 4 Under § 103(a)

The TIS Firewall reference was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls.

TIS Firewall is a computer firewall system that is capable of detecting and selectively removing worms and viruses, as evidenced by the fact that it detected the Internet Worm, which exploited a well-known hole in the standard UNIX SMTP server, sendmail. *See e.g.*, TIS Firewall at pg. 10, FN 3 ("The Morris Internet worm took advantage of a loophole in fingerd to compromise some systems").

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called

smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm. *See e.g.*, TIS Firewall at pg. 41 (since many attacks "have a distinctive signature, smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

TIS Firewall performs preset actions based on the content of the message, including the presence of a virus.

TIS Firewall discloses the element of sending the data to the destination if the data does not contain a virus. If an attack signature is not detected, a daemon process passes the message to the mail handler, which is a daemon itself and which in turn forwards the message ultimately to the destination address.

To the extent the aspect of "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus." is not taught or suggested by TIS Firewall, this element is disclosed or suggested by Sidewinder as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations. MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having

ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses the element of determining whether the data is of a type that is likely to contain virus. See Sidewinder at SR-454.10 ("Sidewinder can detect and block messages that are not English language text and that therefore could contain viruses"). Sidewinder also discloses the element of transmitting the data without performing the determination step. See Sidewinder at SR-454.4 (indicating certain classes of data can be selectively prohibited from passing to and from the external network).

So, a person having ordinary skill in the art can easily use the teachings of Cheswick and Bellovin in combination with the teachings of Sidewinder to come up with a computer implemented method of virus detection at the server wherein the virus detection is selectively done by determining whether the data is of type that is likely to contain virus and transmitting the data if the data is not of type that is likely to contain virus.

Neither TIS Firewall nor Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects of determination whether the file is of type that is likely to contain virus, transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and taking a preset action if the data contains a virus. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a

proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 4 as pointed out above.

**I. Whether claim 5 is obvious in view of the LANProtect reference**

Claim 5 adds the limitation of storing the data in a temporary file to claim 4. The storing of data at the server is not a new feature and inherent in virus scanning gateway systems as discussed below.

**I. The LANProtect Reference**

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious Claim 5 Under § 103(a)**
**Claim 5: "storing the data in a temporary file at the server after the step of electronically transmitting;"**

Claim 5 recites "The method of claim 4, further comprising the steps of storing the data in a temporary file at the server after the step of electronically transmitting; and wherein the step of determining includes scanning the data for a virus using the server."

LANProtect reference discloses the element of storage of the data in a temporary file at the server after the step of electronically transmitting and the step of determining by scanning the data for a virus using the server.

*See e.g.,* LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses.... LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).").

LANProtect was not considered during prosecution of the '600 patent. This prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects of determination whether the file is of type that is likely to contain virus, transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and taking a preset action if the data contains a virus. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 4 as pointed out above.

### J. Whether claim 5 is obvious in view of the TIS Firewall reference, the Sidewinder reference and the MIMEsweeper reference

Claim 5 adds the limitation of storing the data in a temporary file to claim 4. The storing of data at the server is not a new feature and inherent in virus scanning gateway systems. Claim 4 is rendered obvious by the combination of TIS Firewall with Sidewinder. The aspect of storing data in a temporary file at the server is disclosed by MIMEsweeper. See MIMEsweeper at 13 ("The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery.")

So, a person having ordinary skill in the art can easily use the teachings of TIS Firewall in combination with the teachings of Sidewinder and further in view of MIMEsweeper to come up with a computer implemented method of virus detection at the server wherein the virus detection is selectively done by determining whether the data is of type that is likely to contain virus and transmitting the data if the data is not of type that is likely to contain virus and otherwise storing the data in a temporary file at the server.

None of TIS Firewall, Sidewinder and MIMEsweeper were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects scanning for the virus at the server and storing the data in a temporary file at the server. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is

requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 5 as pointed out above.

### K. Whether claim 6 is obvious in view of the LANProtect reference and the TIS Firewall reference

Claim 6 adds a further limitation to claim 5 by claiming that the virus scanning is carried out by signature scanning process. One or more references discussed below disclose the aspect of signature scanning process of virus detection.

#### I. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious Claim 6 Under § 103(a)**
**Claim 6: "scanning is performed using a signature scanning process"**

Claim 6 recites "The method of claim 5, wherein the step of scanning is performed using a signature scanning process."

LANProtect reference discloses the element of signature scanning. The Intel Products performed a signature scanning process when scanning for viruses.

#### II. The TIS Firewall Reference

The TIS Firewall reference was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls.

**TIS Firewall makes obvious Claim 6 Under § 103(a)**
**Claim 6: "scanning is performed using a signature scanning process"**

Claim 6 recites "The method of claim 5, wherein the step of scanning is performed using a signature scanning process."

TIS Firewall discloses the element of signature scanning process of virus scanning. The TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm using signature scanning. *See e.g.*, TIS Firewall at pg. 41 (since many attacks "have a distinctive signature, smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

Neither LANProtect nor TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects scanning for the virus at the server and storing the data in a temporary file at the server and wherein the scanning is done via signature analysis. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 6 as pointed out above.

### L. Whether claim 6 is obvious in view of the Cheswick and Bellovin reference, the Sidewinder reference and the MpScan reference

Claim 6 purports to add a further limitation to claim 5 by simply indicating the virus scanning is carried out by signature scanning process – the primary method of virus scanning at the time of filing of the '600 patent. Claim 6 is rendered obvious by the combination of Cheswick and Bellovin with Sidewinder in view of MpScan.

The aspect of signature scanning is suggested by the MpScan reference, which renders obvious every limitation of claim 6 in combination with Cheswick and Bellovin and Sidewinder. See MpScan at 2 ("Performs pattern matching of outgoing email for words, phrases or any other defined data delivery.")

So, a person having ordinary skill in the art can easily use the teachings of Cheswick and Bellovin in combination with the teachings of Sidewinder and further in view of MpScan to come up with a computer implemented method of virus detection at the server wherein the virus detection is selectively done by determining whether the data is of type that is likely to contain virus and transmitting the data if the data is not of type that is likely to contain virus and storing the data in a temporary file at the server and wherein the scanning is done using signature analysis.

None of Cheswick and Bellovin, Sidewinder and MpScan were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects scanning for the virus at the server and storing the data in a temporary file at the server. As such, the substantial new questions of patentability (SNQs) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record

during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 6 as pointed out above.

### M. Whether claim 7 is obvious in view of the LANProtect reference and the TFS Manual reference

Dependent claim 7 further limits independent claim 4 by defining the preset steps that need to be taken to be one of a group including "Transmitting the data unchanged; Not transmitting the data; Storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name". The preset steps of claim 7 are obvious in view of by one or more references as discussed below:

#### I. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discusses aspects of new software that provides total LAN protection.

**LANProtect makes obvious Claim 7 Under § 103(a)**
**Claim 7: "preset action on the data using the server comprises performing one step from the group of"**

Claim 7 recites "The method of claim 4, wherein the step of performing a preset action on the data using the server comprises performing one step from the group of: Transmitting the data unchanged; Not transmitting the data; Storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name"

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving

the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

LANProtect was not considered during prosecution of the '600 patent. LANProtect contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches the preset step of "Transmitting the data unchanged; Not transmitting the data; Storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name." As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 7 as pointed out above.

## II. The TFS Manual Reference

The TFS Manual reference was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network.

**TFS Manual makes obvious Claim 7 Under § 103(a)**
**Claim 7: "preset action on the data using the server comprises performing one step from the group of"**

Claim 7 recites "The method of claim 4, wherein the step of performing a preset action on the data using the server comprises performing one step from the group of: Transmitting the data

unchanged; Not transmitting the data; Storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name."

TFS Manual discloses a Gateway that would perform different actions depending on the results of the virus scanning. See TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

TFS Manual was not considered during prosecution of the '600 patent. TFS Manual contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches the preset step of "Transmitting the data unchanged; Not transmitting the data; Storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name." As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 7 as pointed out above.

**N. Whether claim 7 is obvious in view of the Cheswick and Bellovin reference, the Sidewinder reference and the TIS Firewall references;**

**Claim 7** limits the types of actions that can represent the preset action of claim 4, reciting "The method of claim 4, wherein the step of performing a preset action on the data using the server comprises performing one step from the group of:"

- Transmitting the data unchanged;
- Not transmitting the data; and
- Storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name.

### I. Cheswick and Bellovin in view of Sidewinder renders obvious Claim 7 Under § 103(a)

Cheswick and Bellovin in view of Sidewinder discloses every limitation of claim 4. The discussion of claim 4 is incorporated herein by reference. The further refinement of the "performing a preset action" step of claim 4 required by claim 7 is disclosed by Sidewinder.

Sidewinder discusses performing preset actions based on the content of the message, including the presence of a virus. In Sidewinder, messages which fail to pass the filter are passed to the System Administrator for action. Rejected mail may be discarded or kept in a 'trash' folder for later examination. Outgoing data which has been blocked by the filter is forwarded to the System Administrator for disposition. Incoming data which has been blocked by the filter is discarded (i.e., not transmitted).

*See e.g.*, Sidewinder at SR-454.8 – SR-454.12 ("Messages which fail to pass the filter are forwarded to the System Administrator for action" and [the] System Administrator can block files or messages that don't pass the filter.)

So, a person having ordinary skill in the art can easily use the teachings of Cheswick and Bellovin in combination with the teachings of Sidewinder to come up with a computer implemented

method of virus detection at the server wherein the virus detection is selectively done and a preset action is performed based on the result of the detection.

Neither Cheswick and Bellovin nor Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects scanning for the virus at the server and storing the data in a temporary file at the server. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 7 as pointed out above.

## II. Cheswick and Bellovin in combination with TIS Firewall renders obvious Claim 7 Under § 103(a)

Cheswick and Bellovin discloses every limitation of claim 4. The discussion on claim 4 is incorporated herein by reference. The limitation recited by claim 7, i.e., performing one of a group of identified preset actions, is disclosed by the TIS Firewall.

TIS Firewall performs preset actions based on the content of the message, including the presence of a virus.

So, a person having ordinary skill in the art can easily use the teachings of Cheswick and Bellovin in combination with the teachings of TIS Firewall to come up with a computer implemented method of virus detection at the server wherein the virus detection is selectively done and a preset action is performed based on the result of the detection.

Neither Cheswick and Bellovin nor TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects scanning for the virus at the server and storing the data in a temporary file at the server. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 7 as pointed out above.

### O. Whether claim 8 is obvious in view of the LANProtect reference and the TFS Manual reference

Dependent claim 8 further limits independent claim 4 by defining the determining step to include comparing an extension type of a file name for the data to a group or known extension types. The determining step of claim 8 is obvious in view of one or more references as discussed below:

## I. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious Claim 8 Under § 103(a)**
**Claim 8: "comparing an extension type of a file name for the data to a group or known extension types"**

Claim 8 recites "The method of claim 4, wherein the step of determining whether the data is of a type that is likely to contain a virus is performed by comparing an extension type of a file name for the data to a group or known extension types."

LANProtect discloses determining whether the data is of a type that is likely to contain a virus by comparing an extension type of a file name for the data to a group of known extension types. *See e.g.*, LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses…. LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension)."

LANProtect was not considered during prosecution of the '600 patent. LANProtect contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches the determining step consisting of comparing extension type of

a file name for the data to a group or known extension types. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raises a substantial new question of patentability with respect to claim 8 as pointed out above.

## II. The TFS Manual Reference

The TFS Manual reference was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network.

**TFS Manual makes obvious Claim 8 Under § 103(a)**
**Claim 8: "comparing an extension type of a file name for the data to a group or known extension types"**

Claim 8 recites "The method of claim 4, wherein the step of determining whether the data is of a type that is likely to contain a virus is performed by comparing an extension type of a file name for the data to a group or known extension types."

TFS Manual discloses this claim element. The TFS Gateway described in TFS Manual would not scan the inline part of the message or text-only attachments because there was no risk that text files would create any damage. Additionally, the TFS Gateway could be used with commercially available antivirus scanners at the time, such as McAfee's VirusScan, Dr Solomon's and IBM Antivirus, which would only scan files likely to contain a virus. See TFS Manual at 77.

These antivirus scanners could also compare the extension type of the file to be scanned with extension types known to be able to contain a virus.

TFS Manual was not considered during prosecution of the '600 patent. TFS Manual contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches the determining step consisting of comparing extension type of a file name for the data to a group or known extension types. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 8 as pointed out above.

**P. Whether claim 8 is obvious in view of the Cheswick and Bellovin reference, the Sidewinder reference and the MIMEsweeper reference**

Dependent claim 8 further limits independent claim 4 by defining the determining step to include comparing an extension type of a file name for the data to a group or known extension types. Each element of claim 4 is disclosed by the combination of Cheswick and Bellovin and Sidewinder. The discussion of Claim 4 is incorporated herein by reference. The limitation of claim 8 is further rendered obvious by Sidewinder and MIMEsweeper as discussed below.

Sidewinder determines whether the data is of a type that the program, user, or administrator believes is likely to contain a virus. *See e.g.*, Sidewinder at SR-454.9 - SR-454.10

("The System Administrator also has the option to block all mail which does not fit the statistical properties of English-language plaintext. Such filtering effectively stops the use of the mail service as a means of sending or receiving dangerous, offensive, or illegal material such as virus-containing object code, personal encrypted messages, or pornographic pictures.").

MIMEsweeper determines whether the data is of a type that the program, user, or administrator believes is likely to contain a virus, see, e.g., MIMEsweeper at pg. 49 ("The way a file is scanned depends on the type of file … to be scanned and the validator employed.)

So, a person having ordinary skill in the art can easily use the teachings of Cheswick and Bellovin in combination with the teachings of TIS Firewall to come up with a computer implemented method of virus detection at the server wherein the virus detection is selectively done and the virus detection step consisting of comparing extension type of a file name for the data to a group or known extension types.

None of Cheswick and Bellovin, Sidewinder and MIMEsweeper were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects of comparing the extension type of the file name for the data to a group or known extension types. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the

patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 8 as pointed out above.

### Q. Whether claim 9 is obvious in view of the TIS Firewall reference

Dependent claim 9 restricts the steps of claim 4 to data transfers that are FTP transfers to the outbound transfers. The steps as recited by claim 9 are made obvious by TIS Firewall as discussed below:

### I. The TIS Firewall Reference

The TIS Firewall reference was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls.

**TIS Firewall makes obvious Claim 9 Under § 103(a)**
**Claim 9: "The method of claim 4, further comprising the steps of:"**

**(1) "...determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;"**

Claim 9 recites "The method of claim 4, further comprising the steps of: determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;"

TIS Firewall determines whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.")

**(2) "...wherein the server is a FTP proxy server;"**

Claim 9 further recites "wherein the server is a FTP proxy server."

TIS Firewall discloses the use of an FTP server. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

**(3) "...wherein the step of electronically receiving data comprises the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network; and;"**

Claim 9 further recites "wherein the step of electronically receiving data comprises the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network."

TIS Firewall discloses this element. The step of electronically receiving data at the TIS Firewall includes the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks;" "Routers can control traffic at an IP level, by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level, forcing traffic to move out of the protocol layer for more detailed examination.").

**(4) "...wherein the step of electronically receiving data comprises the steps of transferring the data from a server task to a FTP daemon and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network;"**

Claim 9 further recites "wherein the step of electronically receiving data comprises the steps of transferring the data from a server task to a FTP daemon and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network."

TIS Firewall discloses this element. The step of electronically receiving data at the TIS Firewall comprised the steps of transferring the data from a server task to an FTP daemon and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks;" "Routers can control traffic at an IP level, by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level, forcing traffic to move out of the protocol layer for more detailed examination;" "As an example, the FTP proxy can block FTP export of files while permitting import of files, representing a granularity of control that router-based firewalls cannot presently achieve.").

TIS Firewall was not considered during prosecution of the '600 patent. TIS Firewall contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches steps of determining whether the data transfer that are FTP transfers is an outbound data transfer and steps of proceeding with the outbound transfer. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is

requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 9 as pointed out above.

### R. Whether claim 9 is obvious in view of the LANProtect reference and the Sidewinder reference

Dependent claim 9 restricts the steps of claim 4 to data transfers that are FTP transfers to the outbound transfers. The discussion regarding obviousness of claim 4 as discussed above is incorporated herein by reference. The steps recited by claim 9 are rendered obvious under 35 U.S.C. § 103(a) by LANProtect in view of Sidewinder as discussed below:

**Claim 9** recites "The method of claim 4, further comprising the steps of:"

- determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;
- wherein the server is a FTP proxy server;
- wherein the step of electronically receiving data comprises the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network; and
- wherein the step of electronically receiving data comprises the steps of transferring the data from a server task to a FTP daemon and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network

LANProtect discloses each limitation of claim 4. Additionally the Sidewinder reference discloses each limitation of claim 9 as discussed below.

Sidewinder was capable of determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network.

Sidewinder could be configured as an FTP proxy server

The step of electronically receiving data at the Sidewinder comprised the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network.

The step of electronically receiving data at the Sidewinder comprised the steps of transferring the data from a server task to an FTP daemon and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network.

So, a person having ordinary skill in the art can easily use the teachings of LANProtect in view of Sidewinder to come up steps of determining whether the data transfer that are FTP transfers is an outbound data transfer and steps of proceeding with the outbound transfer.

Neither LANProtect nor Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches steps of determining whether the data transfer that are FTP transfers is an outbound data transfer and steps of proceeding with the outbound transfer. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 9 as pointed out above.

## S. Whether claim 10 is obvious in view of the TIS Firewall reference

Dependent claim 10 restricts the steps of claim 4 to data transfers that are FTP transfers to the inbound transfers. The steps recited by claim 9 are obvious in view of the TIS Firewall reference as discussed below:

### I. The TIS Firewall Reference

The TIS Firewall reference was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls.

**TIS Firewall makes obvious Claim 10 Under § 103(a)**
**Claim 10: "The method of claim 4, further comprising the steps of:"**

**(1) "...determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;"**

Claim 10 recites "The method of claim 4, further comprising the steps of: determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;"

TIS Firewall determines whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.")

**(2) "...wherein the server is a FTP proxy server;"**

Claim 10 further recites "wherein the server is a FTP proxy server."

TIS Firewall reference discloses the use of an FTP server. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

**(3) "…Wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a node having the destination address, if the data is being transferred into the first network; and"**

Claim 10 further recites "Wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a node having the destination address, if the data is being transferred into the first network."

TIS Firewall discloses this element. The step of sending the data in the TIS Firewall comprises transferring the data from the FTP proxy server to a node having the destination address, if the data is being transferred into the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks;" "Routers can control traffic at an IP level, by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level, forcing traffic to move out of the protocol layer for more detailed examination.").

**(4) "…Wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network."**

Claim 10 further recites "wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network."

TIS Firewall discloses this element. The step of sending the data in the TIS Firewall comprised the steps of transferring the data from the FTP proxy server to an FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network. *See e.g.,* TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks;" "Routers can control traffic at an IP level, by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level, forcing traffic to move out of the protocol layer for more detailed examination;" "As an example, the FTP proxy can block FTP export of files while permitting import of files, representing a granularity of control that router-based firewalls cannot presently achieve.")

TIS Firewall was not considered during prosecution of the '600 patent. TIS Firewall contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches steps of determining whether the data transfer that are FTP transfers is an inbound data transfer and steps of proceeding with the inbound transfer. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record

during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 9 as pointed out above.

### T. Whether claim 10 is obvious in view of the combination of the LANProtect reference and the Sidewinder reference

Dependent claim 10 restricts the steps of claim 4 to data transfers that are FTP transfers to the inbound transfers. The discussion regarding obviousness of claim 4 as discussed above is incorporated herein by reference. The steps recited by claim 10 are rendered obvious under 35 U.S.C. § 103(a) by LANProtect in view of Sidewinder as discussed below:

**Claim 10** recites "The method of claim 4, further comprising the steps of:"

- determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;
- wherein the server is a FTP proxy server;
- Wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a node having the destination address, if the data is being transferred into the first network; and
- Wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network.

LANProtect discloses each limitation of claim 4. Additionally the Sidewinder reference discloses each limitation of claim 10 as discussed below.

Sidewinder was capable of determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network.

Sidewinder could be configured as an FTP proxy server.

The step of sending data at the Sidewinder comprised transferring the data from the FTP proxy server to a client node, if the data is being transferred into the first network.

The step of sending the data at the Sidewinder comprised transferring the data from the FTP proxy server to an FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network.

So, a person having ordinary skill in the art can easily use the teachings of LANProtect in view of Sidewinder to come up steps of determining whether the data transfer that are FTP transfers is an inbound data transfer and steps of proceeding with the inbound transfer.

Neither LANProtect nor Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches steps of determining whether the data transfer that are FTP transfers is an inbound data transfer and steps of proceeding with the inbound transfer. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 9 as pointed out above.

### U. Whether claim 11 is obvious in view of the LANProtect reference and the MIMEsweeper reference

The teaching related to the scanning of the mail messages for the presence of encoded portions, then storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus as contained in the references presented below was not present during the prior examination of the '600 patent. A reasonable examiner would consider this teaching important in determining whether claim 11 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 11 of the '600 patent.

## I. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious claim 11 under § 103(a)**

**Claim11: "A computer implemented method"**

**(1) "...for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:"**

Claim 11 recites "A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:"

LANProtect discloses detecting viruses in data transfers between computers. *See e.g.*, LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity."). *See e.g.*, LANProtect at pg. 16 ("Direction of I/O to scan- LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.").

**(2) "…receiving a mail message request including a destination address;"**

Claim 11 further recites "receiving at a server a data transfer request including a destination address."

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

**(3) "…electronically receiving data at the server;"**

Claim 11 further recites "electronically receiving data at the server."

LANProtect discloses electronically receiving data at the server. See e.g., LANProtect at pg. 27 ("Scan both incoming and outgoing files on the server with the Real Time scan"). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

**(4) "…determining whether the mail message contains a virus, the determination of whether the mail message contains a virus comprising determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produced decoded portions of the**

**mail message, scanning each of the decoded portions for a virus and testing whether the scanning step found any viruses;"**

Claim 11 further recites "whether the mail message contains a virus…"

LANProtect discloses checking incoming executables for viruses at the server. *See e.g.*, LANProtect User's Guide at pg. ii ("Rather than scanning the file server, the Real Time File looks at files going into and/or out of the file server. Using the Real Time File scan, LANProtect begins looking for viruses when the NLM is loaded and continues scanning until the NLM is loaded").

LANProtect discloses a preconfigured scanning process that can be customized. For example, LANProtect teaches a user can specify the type of files that need to be checked at the server. *See e.g.*, LANProtect at pg. 2-8 ("All the server scans are preconfigured to reflect maximum security. However, you may change each configuration and customize the scan. Configuration impacts security level, which files will be scanned, who will be notified when infected files are found, and how infected files handled.").

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

**(5) "…performing a preset action on the mail message if the mail message contains a virus; and"**

Claim 11 further recites "performing a preset action on the data using the server if the data contains a virus."

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

**(6) "…sending the mail message to the destination address if the mail message does not contain a virus."**

Claim 11 further recites "sending the data to the destination address if the data does not contain a virus."

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

## II. The MIMEsweeper Reference

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses.

**MIMEsweeper makes obvious claim 11 under § 103(a)**

**Claim11: "A computer implemented method"**

**(1) "…for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:"**

Claim 11 recites "A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:"

MIMEsweeper reference discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 ("MIMEsweeper is an enabling technology which facilitates the implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments.").

**(2) "…receiving a mail message request including a destination address;"**

Claim 11 further recites "receiving at a server a data transfer request including a destination address."

MIMEsweeper receives a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the

MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination. Since the SMTP server involved receives requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

**(3) "...electronically receiving data at the server;"**

Claim 11 further recites "electronically receiving data at the server;"

MIMEsweeper electronically receives mail messages at the server. *See e.g.,* MIMEsweeper at pg. 13 ("It is assumed that MIMEsweeper is being installed in an environment where electronic mail is already in use."). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

MIMEsweeper checks the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

**(4) "…determining whether the mail message contains a virus, the determination of whether the mail message contains a virus comprising determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produced decoded portions of the mail message, scanning each of the decoded portions for a virus and testing whether the scanning step found any viruses;"**

Claim 11 further recites "whether the mail message contains a virus……;"

MIMEsweeper teaches a scanning process that is preconfigured and that can be customized. The way a file is scanned by MIMEsweeper depends on the type of file to be scanned and the 'Validator' employed. *See e.g.,* MIMEsweeper at pg. 49.

MIMEsweeper teaches scanning the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper 'quarantines' any mail message found to contain a virus or unidentifiable attachment based on the assumption that viruses can be in any part of an attachment. *See e.g.,* MIMEsweeper at pg. 7 ("MIMEsweeper takes a holistic approach in that it assumes viruses can be in any part of an attachment. Any mail message found to contain a virus or unidentifiable

attachment is 'quarantined'. The configurable nature of MIMEsweeper also allows the quarantining of other user-specified file types.").

MIMEsweeper discloses a total E-mail content management tool. It breaks the message into its constituent elements and then subjects each of those components to different checks depending on the content. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper provides a framework for total Email content management. Once MIMEsweeper is configured into Email routing it can analyze the content of each message. MIMEsweeper breaks the messages into its constituent elements and then subjects each of those components to different checks depending on content."). The MIMEsweeper extracts the elements from the mail messages and then presents all the extracted elements to external programs for analysis. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper is recursive in its analysis; so it will find a ZIP file within a ZIP file and a uuencoded component of that file. In other words the analysis continues until MIMEsweeper cannot break the message down further."). *See e.g.,* MIMEsweeper at pg. 9 ("The rationale behind this is that Email borne threats might not be recognized by checks if they are compressed or encoded."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper checks viruses within itself, presenting all the extracted elements of the Email message to external programs (called Validators) and reacts in a user-configurable manner according to return codes."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper's container handling architecture allows decompression of Email message attachment contents."). Since, the Minesweeper extracts all the elements of the email message before presenting them to external programs called "Validators" for virus scanning, the storing of these extracted elements in separate temporary files would be obvious to any person skilled in the art.

**(5) "...performing a preset action on the mail message if the mail message contains a virus; and"**

Claim 11 further recites "performing a preset action on the data using the server if the data contains a virus."

MIMEsweeper discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**(6) "...sending the mail message to the destination address if the mail message does not contain a virus."**

Claim 11 further recites "sending the data to the destination address if the data does not contain a virus."

Further, if a file does not contain a virus, the MIMEsweeper teaches allowing transfer of the data to the destination address. The MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

## V. Whether claim 11 is obvious in view the LANProtect reference, the MIMEsweeper reference, the Sidewinder reference and the MpScan reference

None of LANProtect, MIMEsweeper, MpScan and Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600

patent. As shown above, no prior art concerning the scanning of the mail messages for the presence of encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the scanning of the mail messages for the presence encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus raise a substantial new question of patentability with respect to claim 11 as pointed out in more detail below.

**Claim 11** recites "A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer", the method comprising the steps of:

- receiving a mail message request including a destination address;
- electronically receiving the mail message at a server;
- determining whether the mail message contains a virus, the determination of whether the mail message contains a virus comprising determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produced decoded portions of the mail message, scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses;

- performing a preset action on the mail message if the mail message contains a virus; and
- sending the mail message to the destination address if the mail message does not contains a virus.

### I. LANProtect in view of MpScan and Sidewinder renders obvious Claim 11 Under § 103(a):

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

LANProtect discloses detecting viruses in data transfers between computers. *See e.g.*, LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity."). *See e.g.*, LANProtect at 16 ("Direction of I/O to scan- LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.").

LANProtect discloses receiving a data transfer request including a destination address. As LANProtect runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the data file.

LANProtect discloses electronically receiving data at the server. See e.g., LANProtect at pg. 27 ("Scan both incoming and outgoing files on the server with the Real Time scan"). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

LANProtect discloses checking incoming executables for viruses at the server. *See e.g.*, LANProtect User's Guide at pg. ii ("Rather than scanning the file server, the Real Time File looks

at files going into and/or out of the file server. Using the Real Time File scan, LANProtect begins looking for viruses when the NLM is loaded and continues scanning until the NLM is loaded").

LANProtect discloses a preconfigured scanning process that can be customized. For example, LANProtect teaches a user can specify the type of files that need to be checked at the server. *See e.g.*, LANProtect at pg. 2-8 ("All the server scans are preconfigured to reflect maximum security. However, you may change each configuration and customize the scan. Configuration impacts security level, which files will be scanned, who will be notified when infected files are found, and how infected files handled.").

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

However if the aspect of "the determination of whether the mail message contains a virus comprising determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produced decoded portions of the mail message, scanning each of the decoded portions for a virus and testing whether the scanning step found any viruses;" was somehow construed so that LANProtect did not practice this aspect, the following references combined with LANProtect would render claim 11 obvious.

This element is disclosed or suggested by MpScan and Sidewinder as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

MpScan reference discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized. MpScan deals with compressed, uuencoded and "other" data formats and is capable of blocking the binary, graphic and encrypted data. *See e.g.,* MpScan pg. 1-2.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder indicates the product incorporates the patented Type Enforcement mechanism that prevents an outside attacker from "breaking out" and either gaining control of the server or bypassing any of the inbound or outbound data filtering. *See e.g.,* Sidewinder at SR-454.5. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. Data may be filtered on the basis of content as well as source or destination. *See e.g.,* Sidewinder at SR-454.8 ("The System Administrator is able to set-up mail filtering for both inbound and outbound messages. Inbound mail can be filtered on the basis of destination. In addition, the System Administrator can prohibit the mailing of messages which are not comprised of English-language plaintext. This latter form of filtering prevents users from avoiding accountability through the use of encryption, or from sending or receiving potentially dangerous, offensive, or illegal material, such as Object code containing Viruses or pornographic pictures.").

In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). The Sidewinder reference clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

So, a person having ordinary skill in the art can easily use the teachings of LANProtect in combination with the teachings of MpScan or Sidewinder to come up with a computer implemented

method for detecting viruses in a mail message transferred between a first computer and a second computer wherein the virus detection is selectively done by determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produce decoded portions of the mail message, scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses; performing a preset action on the mail message if the mail message contains a virus; and sending the mail message to the destination address if the mail message does not contains a virus.

None of LANProtect, MpScan and Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the scanning of the mail messages for the presence of encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 11 as pointed out above.

## II. MIMEsweeper in view of MpScan and Sidewinder renders obvious Claim 11 Under § 103(a)

MIMEsweeper was not considered during the prosecution of the '600 patent. It was released in September of 1995, to protect networks from virus infection via E-mail. MIMEsweeper was conceived out of a requirement to scan incoming E-mails and their attachments for computer viruses.

MIMEsweeper discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 ("MIMEsweeper is an enabling technology which facilitates the implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments.").

MIMEsweeper receives a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination. Since SMTP server involved receives requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MIMEsweeper electronically receives mail messages at the server. *See e.g.,* B MIMEsweeper at pg. 13 ("It is assumed that MIMEsweeper is being installed in an environment where electronic mail is already in use."). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

MIMEsweeper checks the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MIMEsweeper scanning process is preconfigured and can be customized. The way a file is scanned by MIMEsweeper depends on the type of file to be scanned and the 'Validator' employed. *See e.g.,* MIMEsweeper at pg. 49.

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper 'quarantines' any mail message found to contain a virus or unidentifiable attachment based on the assumption that viruses can be in any part of an attachment. *See e.g.,*

MIMEsweeper at pg. 7 ("MIMEsweeper takes a holistic approach in that it assumes viruses can be in any part of an attachment. Any mail message found to contain a virus or unidentifiable attachment is 'quarantined'. The configurable nature of MIMEsweeper also allows the quarantining of other user-specified file types.").

MIMEsweeper discloses a total E-mail content management tool. It breaks the message into its constituent elements and then subjects each of those components to different checks depending on the content. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper provides a framework for total Email content management. Once MIMEsweeper is configured into Email routing it can analyze the content of each message. MIMEsweeper breaks the messages into its constituent elements and then subjects each of those components to different checks depending on content."). The MIMEsweeper extracts the elements from the mail messages and then presents all the extracted elements to external programs for analysis. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper is recursive in its analysis; so it will find a ZIP file within a ZIP file and a uuencoded component of that file. In other words the analysis continues until MIMEsweeper cannot break the message down further."). *See e.g.,* MIMEsweeper at pg. 9 ("The rationale behind this is that Email borne threats might not be recognized by checks if they are compressed or encoded."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper checks viruses within itself, presenting all the extracted elements of the Email message to external programs (called Validators) and reacts in a user-configurable manner according to return codes."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper's container handling architecture allows decompression of Email message attachment contents."). Since, the Minesweeper extracts all the elements of the email message before presenting them to external programs called "Validators" for virus scanning, the storing of these extracted elements in separate temporary files would be obvious to any person skilled in the art.

MIMEsweeper discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

Further, if a file does not contain a virus, the MIMEsweeper allows transfer of the data to the destination address. The MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

However if the aspect of "the determination of whether the mail message contains a virus comprising determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produced decoded portions of the mail message, scanning each of the decoded portions for a virus and testing whether the scanning step found any viruses;" was somehow construed so that MIMEsweeper did not practice this aspect, the following references combined with MIMEsweeper would render claim 11 obvious.

This element is disclosed or suggested by MpScan and Sidewinder as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143.

Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized. MpScan deals with compressed, uuencoded and "other" data formats and is capable of blocking the binary, graphic and encrypted data. *See e.g.,* MpScan pg. 1-2.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder indicates the product incorporates the patented Type Enforcement mechanism that prevents an outside attacker from "breaking out" and either gaining control of the server or bypassing any of the inbound or outbound data filtering. *See e.g.,* Sidewinder at SR-454.5. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. Data may be filtered on the basis of content as well as source or destination. *See e.g.,* Sidewinder at SR-454.8 ("The System Administrator is able to set-up mail filtering for both inbound and outbound messages. Inbound mail can be filtered on the basis of destination. In addition, the System Administrator can prohibit the mailing of messages which are not comprised of English-language plaintext. This latter form of filtering prevents users from

avoiding accountability through the use of encryption, or from sending or receiving potentially dangerous, offensive, or illegal material, such as Object code containing Viruses or pornographic pictures.").

In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). The Sidewinder reference clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

So, a person having ordinary skill in the art can easily use the teachings of the MIMEsweeper in combination with the teachings of MpScan or Sidewinder to come up with a computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer wherein the virus detection is selectively done by determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produce decoded portions of the mail message, scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses; performing a preset action on the mail message if the mail message contains a virus; and sending the mail message to the destination address if the mail message does not contains a virus.

None of MIMEsweeper, MpScan and Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological

teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the scanning of the mail messages for the presence of encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus. As such, the substantial new question of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 11 as pointed out above.

### W. Whether claim 12 is obvious in view of the MpScan reference and the MIMEsweeper reference

The teaching related to the scanning of the mail messages for the presence of "uuencoded" portions as contained in the references presented below was not present during the prior examination of the '600 patent. A reasonable examiner would consider this teaching important in determining whether claim 12 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 12 of the '600 patent.

#### I. The MpScan Reference

The MpScan reference was not considered during the prosecution of the '600 patent. MpScan discloses an e-mail content scanning firewall available prior to January 1994.

**MpScan makes obvious claim 12 under § 103(a)**

**Claim12: "The method of claim 11, wherein the step of determining whether the mail message includes any encoded portions searches for uuencoded portions."**

Claim 12 recites "the method of claim 11, wherein the step of determining whether the mail message includes any encoded portions searches for uuencoded portions."

MpScan describes the aspect of receiving a mail message request including a destination address. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/or are transmitted to and from competitor's addresses, except as authorized. MpScan deals with compressed, uuencoded and "other" data formats and is capable of blocking the binary, graphic and encrypted data. *See e.g.,* MpScan pg. 1-2.

## II. The MIMEsweeper Reference

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses.

**MIMEsweeper makes obvious claim 12 under § 103(a)**

**Claim12: "The method of claim 11, wherein the step of determining whether the mail message includes any encoded portions searches for uuencoded portions."**

MIMEsweeper reference discloses a total E-mail content management tool. It breaks the message into its constituent elements and then subjects each of those components to different checks depending on the content. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper provides a

framework for total Email content management. Once MIMEsweeper is configured into Email routing it can analyze the content of each message. MIMEsweeper breaks the messages into its constituent elements and then subjects each of those components to different checks depending on content."). The MIMEsweeper extracts the elements from the mail messages and then presents all the extracted elements to external programs for analysis. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper is recursive in its analysis; so it will find a ZIP file within a ZIP file and a uuencoded component of that file. In other words the analysis continues until MIMEsweeper cannot break the message down further."). *See e.g.,* MIMEsweeper at pg. 9 ("The rationale behind this is that Email borne threats might not be recognized by checks if they are compressed or encoded."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper checks viruses within itself, presenting all the extracted elements of the Email message to external programs (called Validators) and reacts in a user-configurable manner according to return codes.").

### X. Whether claim 12 is obvious in view of the Cheswick reference, the Cheswick and Bellovin reference, the LANProtect reference and the TIS Firewall reference, in combination with one or more admission by the patentees in the '600 patent or in combination with the previously considered Hile reference

None of Cheswick, Cheswick and Bellovin, LANProtect and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the use of proxy servers and proxy daemons in connection with removing a virus during data transfers, wherein the proxy server is an FTP proxy server and the proxy daemon is an FTP daemon was considered during prosecution of the '600 patent.

As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents

a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the use of proxy servers and proxy daemons in connection with removing a virus during data transfers, wherein the proxy server is an FTP proxy server and proxy daemon is an FTP daemon, raise a substantial new question of patentability with respect to claim 12 as pointed out in more detail below.

**Claim 12** recites "the proxy server is a FTP proxy server that handles evaluation and transfer of data files, and the daemon is an FTP daemon that communicates with a recipient node and transfers data files to the recipient node."

In total, Claim 12 adds as the specific proxy server type, "a FTP proxy server". However, the restriction on the proxy server element to an FTP proxy server is a meaningless restriction because the FTP proxy server is, and was, a very common (if not the most common) type of proxy server, included on virtually every file server and electronic mail system as of the Critical Date.

Following is a discussion of how Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall together in view of the previously considered Hile reference disclose (either expressly or inherently) and render obvious each limitation of claim 12.

Cheswick discloses the use of an FTP proxy server. See Cheswick at 234 ("*Pftp* provides FTP access in a similar manner." "We provide incoming login and mail service. For incoming file transfer, inet provides an anonymous FTP service").

In addition, Cheswick and Bellovin also discloses the use of an FTP proxy server. See e.g., Firewalls and Internet Security, Cheswick and Bellovin (1994) at 94 ("As we have described,

outgoing FTP sessions normally require an incoming TCP call. To support this, our proxy service can listen on a newly created socket. The port number is passed back to the caller, which generates the appropriate FTP PORT command. The call is thus outgoing from the user's machine to the firewall, but incoming from the FTP server.").

Furthermore, it would have been obvious to use the Intel Products LANProtect at an FTP proxy server and to utilize an FTP daemon. LANProtect was designed to be installed and run on a NetWare server, which is a computer that has a Novell loadable module running on it. The NetWare server receives a request from a user on the local area network. The NetWare server then determines whether to send the requested information to the user. If the NetWare server decides to send the information to the user, the file is transmitted electronically in units called packets. Each packet includes a header, and part of the information included in the header is the destination address where the information is being sent. See LANProtect at 5 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail me transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library (see below) to scan those files for known viruses."). In addition, it would have been obvious to use the network file server/scanning system disclosed by the LANProtect reference at a mail server, and implementing an FTP proxy server and an FTP daemon.

Additionally, TIS Firewall utilizes an FTP proxy server that handles evaluation and transfer of data files and an FTP daemon that communicates with a recipient node and transfers data to the recipient node. See TIS Firewall at 10 ("In order to permit file transfer through the firewall without risking compromising the firewall's security an FTP proxy server is provided.")

The teachings as contained in Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination. As described above, a reasonable examiner would consider these combined teachings important in determining whether claim 12 is patentable. For this reason, the teachings of Hile in combination with the teachings by Cheswick, Cheswick and Bellovin, LANProtect, TIS Firewall raise a substantial new question of patentability with respect to at least claim 12 of the '600 patent.

### Y. Whether claim 13 is obvious in view of the LANProtect reference and the MIMEsweeper reference

The teaching related to electronically receiving the mail messages including the destination address at the server, then scanning the messages for the presence of encoded portions and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination address as contained in the references presented below was not present during the prior examination of the '600 patent. A reasonable examiner would consider this teaching important in determining whether claim 13 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 13 of the '600 patent.

#### I. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious claim 13 under § 103(a)**

**Claim13: "A computer implemented method"**

**(1) "...for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:"**

Claim 13 recites "A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:"

LANProtect discloses detecting viruses in data transfers between computers. *See e.g.,* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity."). *See e.g.,* LANProtect at pg. 16 ("Direction of I/O to scan- LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.").

**(2) "...receiving a mail message request including a destination address;"**

Claim 13 further recites "receiving at a server a mail message request including a destination address."

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a

destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

**(3) "…electronically receiving the mail message at the server;"**

Claim 13 further recites "electronically receiving the mail message at the server."

LANProtect discloses electronically receiving data at the server. See e.g., LANProtect at pg. 27 ("Scan both incoming and outgoing files on the server with the Real Time scan"). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

**(4) "…scanning the mail message for encoded portions;**

**determining whether the mail message contains a virus;"**

Claim 13 further recites "whether the mail message contains a virus…"

LANProtect discloses checking incoming executables for viruses at the server. *See e.g.*, LANProtect User's Guide at pg. ii ("Rather than scanning the file server, the Real Time File looks at files going into and/or out of the file server. Using the Real Time File scan, LANProtect begins looking for viruses when the NLM is loaded and continues scanning until the NLM is loaded").

LANProtect discloses a preconfigured scanning process that can be customized. For example, LANProtect teaches a user can specify the type of files that need to be checked at the server. *See e.g.*, LANProtect at pg. 2-8 ("All the server scans are preconfigured to reflect maximum security. However, you may change each configuration and customize the scan. Configuration impacts security level, which files will be scanned, who will be notified when infected files are found, and how infected files handled.").

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

**(5) "...performing a preset action on the mail message if the mail message contains a virus;"**

Claim 13 further recites "performing a preset action on the data using the server if the data contains a virus."

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect

places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

**(6) "…sending the mail message to the destination address if the mail message does not contain a virus; and"**

Claim 13 further recites "sending the data to the destination address if the data does not contain a virus."

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

**(7) "…wherein the step of sending the mail message to the destination address is performed if the mail message does not contain any encoded portions; the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address."**

Claim 13 further recites "sending the data to the destination address if the data does not contain any encoded portions; the server includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message to its destination involves transferring of mail message from

the SMTP proxy server to the SMTP daemon and thereafter transferring the message from SMTP daemon to its final destination."

LANProtect specifically discloses the scanning of the network traffic of any type. *See e.g.,* LANProtect at pg. 6 ("All network traffic originating outside the file server (e.g. from workstations, modem servers, email file transfer etc.) and all network traffic originating at the file server is scanned for virus infections."). In addition, it would have been obvious to use the network file server system/scanning system disclosed by the LANProtect reference at the mail server and in addition implementing a SMTP proxy server and an SMTP daemon.

## II. The MIMEsweeper Reference

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses.

**MIMEsweeper makes obvious claim 13 under § 103(a)**

**Claim13: "A computer implemented method"**

**(1) "...for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:"**

Claim 13 recites "A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:"

MIMEsweeper discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 ("MIMEsweeper is an enabling technology which facilitates the

implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments.").

**(2) "…receiving a mail message request including a destination address;"**

Claim 13 further recites "receiving at a server a data transfer request including a destination address."

MIMEsweeper teaches receiving a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination. Since SMTP server involved receives requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

**(3) "…electronically receiving the mail message at the server;"**

Claim 13 further recites "electronically receiving the data at the server."

MIMEsweeper teaches electronically receiving mail messages at the server. *See e.g.,* MIMEsweeper at pg. 13 ("It is assumed that MIMEsweeper is being installed in an environment

where electronic mail is already in use."). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

MIMEsweeper checks the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

**(4) "…scanning the mail message for encoded portions; determining whether the mail message contains a virus;"**

Claim 13 further recites "whether the mail message contains a virus…"

MIMEsweeper teaches a scanning process that is preconfigured and that can be customized. The way a file is scanned by MIMEsweeper depends on the type of file to be scanned and the 'Validator' employed. *See e.g.,* MIMEsweeper at pg. 49.

MIMEsweeper teaches scanning the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper 'quarantines' any mail message found to contain a virus or unidentifiable attachment based on the assumption that viruses can be in any part of an attachment. *See e.g.,* MIMEsweeper at pg. 7 ("MIMEsweeper takes a holistic approach in that it assumes viruses can be in any part of an attachment. Any mail message found to contain a virus or unidentifiable attachment is 'quarantined'. The configurable nature of MIMEsweeper also allows the quarantining of other user-specified file types.").

MIMEsweeper discloses a total E-mail content management tool. It breaks the message into its constituent elements and then subjects each of those components to different checks depending on the content. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper provides a framework for total Email content management. Once MIMEsweeper is configured into Email routing it can analyze the content of each message. MIMEsweeper breaks the messages into its constituent elements and then subjects each of those components to different checks depending on content."). The MIMEsweeper extracts the elements from the mail messages and then presents all the extracted elements to external programs for analysis. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper is recursive in its analysis; so it will find a ZIP file within a ZIP file and a uuencoded component of that file. In other words the analysis continues until MIMEsweeper cannot break the message down further."). *See e.g.,* MIMEsweeper at pg. 9 ("The rationale behind this is that Email borne threats might not be recognized by checks if they are compressed or encoded."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper checks viruses within itself, presenting all the extracted elements of the Email message to external programs (called Validators) and reacts in a user-configurable manner according to return codes.").

**(5) "…performing a preset action on the mail message if the mail message contains a virus; and"**

Claim 13 further recites "performing a preset action on the data using the server if the data contains a virus."

MIMEsweeper discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**(6) "...sending the mail message to the destination address if the mail message does not contain a virus."**

Claim 13 further recites "sending the data to the destination address if the data does not contain a virus."

Further, if a file does not contain a virus, the MIMEsweeper allows transfer of the data to the destination address. MIMEsweeper teaches examining the messages and based upon the results of the analysis, submitting the message for onward transmission, or diverting it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

**(7) "...wherein the step of sending the mail message to the destination address is performed if the mail message does not contain any encoded portions; the server includes a SMTP proxy**

**server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address."**

Claim 13 further recites "sending the data to the destination address if the data does not contain any encoded portions; the server includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message to its destination involves transferring of mail message from the SMTP proxy server to the SMTP daemon and thereafter transferring the message from SMTP daemon to its final destination."

MIMEsweeper discloses the use of an SMTP proxy server and an SMTP daemon to perform mail communication across networks. *See e.g.,* MIMEsweeper at pg. 13 ("The client server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery. The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.")

**Z. Whether claim 13 is obvious in view of the LANProtect reference, the MIMEsweeper reference, the MpScan reference, the Sidewinder reference, the Cheswick reference, the Cheswick and Bellovin reference, the TIS Firewall reference and the TFS Manual reference**

None of LANProtect, MIMEsweeper, MpScan, Sidewinder, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual were considered during prosecution of the '600 patent.

Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the scanning of the electronically received mail messages for the presence of encoded portions and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination address was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the scanning of the electronically received mail messages for the presence of encoded portions and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination raise a

substantial new question of patentability with respect to claim 13 as pointed out in more detail below.

**Claim13:** "A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:"

- receiving a mail message request including a destination address;
- electronically receiving the mail message at the server;
- scanning the mail message for encoded portions; determining whether the mail message contains a virus;
- performing a preset action on the mail message if the mail message contains a virus;
- sending the mail message to the destination address if the mail message does not contain a virus; and
- wherein the step of sending the mail message to the destination address is performed if the mail message does not contain any encoded portions; the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address."

## I. LANProtect in view of MpScan, the Sidewinder reference, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual renders obvious Claim 13 Under § 103(a);

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

LANProtect discloses detecting viruses in data transfers between computers. *See e.g.,* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity."). *See e.g.,* LANProtect at pg. 16 ("Direction

of I/O to scan- LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.").

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

LANProtect discloses electronically receiving data at the server. See e.g., LANProtect at pg. 27 ("Scan both incoming and outgoing files on the server with the Real Time scan"). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

LANProtect discloses checking incoming executables for viruses at the server. *See e.g.*, LANProtect User's Guide at pg. ii ("Rather than scanning the file server, the Real Time File looks at files going into and/or out of the file server. Using the Real Time File scan, LANProtect begins looking for viruses when the NLM is loaded and continues scanning until the NLM is loaded").

LANProtect discloses a preconfigured scanning process that can be customized. For example, LANProtect teaches a user can specify the type of files that need to be checked at the server. *See e.g.*, LANProtect at pg. 2-8 ("All the server scans are preconfigured to reflect maximum security. However, you may change each configuration and customize the scan. Configuration impacts security level, which files will be scanned, who will be notified when infected files are found, and how infected files handled.").

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

LANProtect specifically discloses the scanning of the network traffic of any type. *See e.g.,* LANProtect at pg. 6 ("All network traffic originating outside the file server (e.g. from workstations, modem servers, email file transfer etc.) and all network traffic originating at the file server is scanned for virus infections."). In addition, it would have been obvious to use the network file server system/scanning system disclosed by the LANProtect reference at the mail server and in addition implementing a SMTP proxy server and an SMTP daemon.

However if the aspect of "scanning of the electronically received mail messages for the presence of encoded portions and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail

message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination" was somehow construed so that LANProtect did not practice this aspect, the following references combined with LANProtect would render claim 13 obvious.

This element is disclosed or suggested by a set of prior art including MpScan, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized. MpScan deals with compressed, uuencoded and "other" data formats and is capable of blocking the binary, graphic and encrypted data. *See e.g.,* MpScan pg. 1-2.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder indicates the product incorporates the patented

Type Enforcement mechanism that prevents an outside attacker from "breaking out" and either gaining control of the server or bypassing any of the inbound or outbound data filtering. *See e.g.,* Sidewinder at SR-454.5. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. Data may be filtered on the basis of content as well as source or destination. *See e.g.,* Sidewinder at SR-454.8 ("The System Administrator is able to set-up mail filtering for both inbound and outbound messages. Inbound mail can be filtered on the basis of destination. In addition, the System Administrator can prohibit the mailing of messages which are not comprised of English-language plaintext. This latter form of filtering prevents users from avoiding accountability through the use of encryption, or from sending or receiving potentially dangerous, offensive, or illegal material, such as Object code containing Viruses or pornographic pictures.").

In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). The Sidewinder reference clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

Cheswick discloses the use of SMTP proxy server that handles the mail communication. *See e.g.,* Cheswick at 234 ("Outgoing mail is sent to inet via SMTP over either Data kit or the internal Internet. It is stored and forwarded from there. Upas performs the mail gateway functions."). Cheswick also discloses the use of a server daemon in a gateway system. *See e.g.,*

Cheswick at 234 ("Our new gateway machine named inet, is a MIPS M/120 running System V with Berkeley-enhancements. Various daemons and critical programs have been obtained from other sources, checked and installed.")

In addition, Cheswick and Bellovin discusses SMTP as a common proxy type necessary for the prolific Send-mail program, and discusses the SMTP proxy in the context of security and filtering. *See e.g.,* Cheswick and Bellovin at 189 ("A summary of the most common proxy connections [including SMTP] is shown in Table 11.1."). *See also* Cheswick and Bellovin at 242 (disclosing sources for a variety of network daemons, including sites and code bases that contained SMTP daemons such as the source site for BSD UNIX source code Version 4.2).

Additionally, TIS Firewall discloses the TIS Firewall Toolkit included an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

In addition, the TFS Manual contained an SMTP proxy server and an SMTP daemon to perform mail communication across networks. *See e.g.,* TFS Manual at 28. TFS Manual also discloses the message server software. *See e.g.,* TFS Manual at 35. ("TFS requires both the Message Server software and API software to be active.")

So, a person having ordinary skill in the art can easily use the teachings of LANProtect in combination with the teachings of the MpScan, Sidewinder, Cheswick, Cheswick and Bellovin, TIS Firewall or TFS Manual to come up with a computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer; by scanning the

received mail messages for the presence of encoded portions at the sever and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination.

None of LANProtect, MpScan, Sidewinder, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual as discussed below were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent.

As described herein, no prior art considered during prosecution of the '600 patent concerns the scanning of the received mail messages for the presence of encoded portions at the sever and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the

references presented herewith, raise a substantial new question of patentability with respect to claim 13 as pointed out above.

## II. MIMEsweeper in view of MpScan, Sidewinder, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual renders obvious Claim 13 Under § 103(a);

MIMEsweeper was not considered during the prosecution of the '600 patent. It was released in Sept, 1995, to protect networks from virus infection via E-mail. MIMEsweeper was conceived out of a requirement to scan incoming E-mails and their attachments for computer viruses.

MIMEsweeper discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 ("MIMEsweeper is an enabling technology which facilitates the implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments.").

MIMEsweeper receives a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination. Since SMTP server involved receives requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also

store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MIMEsweeper electronically receives mail messages at the server. *See e.g.,* MIMEsweeper at pg. 13 ("It is assumed that MIMEsweeper is being installed in an environment where electronic mail is already in use."). The receiving of data (incoming and outgoing files) electronically is inherent in any data transfer system utilizing a server and as such would be obvious to any person skilled in the art.

MIMEsweeper checks the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MIMEsweeper scanning process is preconfigured and can be customized. The way a file is scanned by MIMEsweeper depends on the type of file to be scanned and the 'Validator' employed. *See e.g.,* MIMEsweeper at pg. 49.

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper 'quarantines' any mail message found to contain a virus or unidentifiable attachment based on the assumption that viruses can be in any part of an attachment. *See e.g.,* MIMEsweeper at pg. 7 ("MIMEsweeper takes a holistic approach in that it assumes viruses can be in any part of an attachment. Any mail message found to contain a virus or unidentifiable attachment is 'quarantined'. The configurable nature of MIMEsweeper also allows the quarantining of other user-specified file types.").

MIMEsweeper reference discloses a total E-mail content management tool. It breaks the message into its constituent elements and then subjects each of those components to different checks depending on the content. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper provides a framework for total Email content management. Once MIMEsweeper is configured into Email routing it can analyze the content of each message. MIMEsweeper breaks the messages into its constituent elements and then subjects each of those components to different checks depending on content."). The MIMEsweeper extracts the elements from the mail messages and then presents all the extracted elements to external programs for analysis. *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper is recursive in its analysis; so it will find a ZIP file within a ZIP file and a uuencoded component of that file. In other words the analysis continues until MIMEsweeper cannot break the message down further."). *See e.g.,* MIMEsweeper at pg. 9 ("The rationale behind this is that Email borne threats might not be recognized by checks if they are compressed or encoded."). *See e.g.,* MIMEsweeper at pg. 9 ("MIMEsweeper checks viruses within itself, presenting all the extracted elements of the Email message to external programs (called Validators) and reacts in a user-configurable manner according to return codes.").

MIMEsweeper reference discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken

can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

Further, if a file does not contain a virus, MIMEsweeper allows transfer of the data to the destination address. MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

MIMEsweeper discloses the use of an SMTP proxy server and an SMTP daemon to perform mail communication across networks. *See e.g.,* MIMEsweeper at pg. 13 ("The client server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery. The MIMEsweeper SMTP server consists of two mail handling agents. The receiving agent stores incoming Email in a dedicated directory, and then moves it to a second directory from where it is picked up at timed intervals by the delivery agent.")

However if the aspect of "scanning of the electronically received mail messages for the presence of encoded portions and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail

message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination" was somehow construed so that MIMEsweeper did not practice this aspect, the following references combined with MIMEsweeper would render claim 13 obvious.

This element is disclosed or suggested by a set of prior art including MpScan, Sidewinder, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized. MpScan deals with compressed, uuencoded and "other" data formats and is capable of blocking the binary, graphic and encrypted data. *See e.g.,* MpScan pg. 1-2.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder indicates the product incorporates the patented

Type Enforcement mechanism that prevents an outside attacker from "breaking out" and either gaining control of the server or bypassing any of the inbound or outbound data filtering. *See e.g.,* Sidewinder at SR-454.5. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. Data may be filtered on the basis of content as well as source or destination. *See e.g.,* Sidewinder at SR-454.8 ("The System Administrator is able to set-up mail filtering for both inbound and outbound messages. Inbound mail can be filtered on the basis of destination. In addition, the System Administrator can prohibit the mailing of messages which are not comprised of English-language plaintext. This latter form of filtering prevents users from avoiding accountability through the use of encryption, or from sending or receiving potentially dangerous, offensive, or illegal material, such as Object code containing Viruses or pornographic pictures.").

In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). The Sidewinder reference clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

Cheswick discloses the use of SMTP proxy server that handles the mail communication. *See e.g.,* Cheswick at 234 ("Outgoing mail is sent to inet via SMTP over either Data kit or the internal Internet. It is stored and forwarded from there. Upas performs the mail gateway functions."). Cheswick also disclose the use of a server daemon in a gateway system. *See e.g.,*

Cheswick at 234 ("Our new gateway machine named inet, is a MIPS M/120 running System V with Berkeley-enhancements. Various daemons and critical programs have been obtained from other sources, checked and installed.")

In addition, Cheswick and Bellovin discusses SMTP as a common proxy type necessary for the prolific Send-mail program, and discusses the SMTP proxy in the context of security and filtering. *See e.g.,* Cheswick and Bellovin at 189 ("A summary of the most common proxy connections [including SMTP] is shown in Table 11.1."). *See also* Cheswick and Bellovin at 242 (disclosing sources for a variety of network daemons, including sites and code bases that contained SMTP daemons such as the source site for BSD UNIX source code Version 4.2).

Additionally, TIS Firewall discloses the TIS Firewall Toolkit included an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

In addition, TFS Manual contained an SMTP proxy server and an SMTP daemon to perform mail communication across networks. *See e.g.,* TFS Manual at 28. TFS Manual also discloses the message server software. *See e.g.,* TFS Manual at 35. ("TFS requires both the Message Server software and API software to be active.")

So, a person having ordinary skill in the art can easily use the teachings of MIMEsweeper in combination with the teachings of MpScan, Sidewinder, Cheswick, Cheswick and Bellovin, TIS Firewall or TFS Manual to come up with a computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer by scanning the received

mail messages for the presence of encoded portions at the sever and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination.

None of MIMEsweeper, MpScan, Sidewinder, Cheswick, Cheswick and Bellovin, TIS Firewall and TFS Manual as discussed below were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent.

As described herein, no prior art considered during prosecution of the '600 patent concerns the scanning of the received mail messages for the presence of encoded portions at the sever and thereafter performing the preset action or sending the mail messages to its destination depending on whether it contains virus or not, wherein the server involved includes a SMTP proxy server and a SMTP daemon and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to its destination. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim

13 as pointed out above.

### AA. Whether claim 14 is obvious in view of the LANProtect reference and the MIMEsweeper reference

The teaching related to the storing the mail messages in a temporary file and thereafter scanning the temporary file for the presence of viruses as contained in the references presented below was not present during the prior examination of the '600 patent. A reasonable examiner would consider this teaching important in determining whether claim 14 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 14 of the '600 patent.

### I. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious claim 14 under § 103(a)**

**Claim14: "The method of claim 11,"**

**(1) "...wherein the step of determining whether the mail message contains a virus, further comprises the steps of:"**

Claim 14 recites "the method of claim 11, wherein the step of determining whether the mail message contains a virus, further comprises the steps of:"

LANProtect discloses detecting viruses in data transfers between computers. *See e.g.,* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity."). *See e.g.,* LANProtect at pg. 16 ("Direction of I/O to scan- LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.").

**(2) "…storing the message in a temporary file;"**

Claim 14 further recites "storing the message in a temporary file."

LANProtect discloses the element of storage of data in a temporary file at the server and thereafter scanning the file for the presence of the viruses. *See e.g.,* LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses…. LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files specified as 'all' or by specific file extension).").

**(3) "…scanning the temporary file for viruses; and testing whether the scanning step found a virus.'**

Claim 14 further recites "scanning the temporary file for viruses and testing whether the scanning step found a virus."

LANProtect discloses the element of storage of data in a temporary file at the server and thereafter scanning the data for a virus using the server. *See e.g.,* LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses…. LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic

originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).").

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

## II. The MIMEsweeper Reference

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses.

**The MIMEsweeper Reference makes obvious claim 14 under § 103(a)**

**Claim14: "The method of claim 11,"**

**(1) "…wherein the step of determining whether the mail message contains a virus, further comprises the steps of:"**

Claim 14 recites "the method of claim 11, wherein the step of determining whether the mail message contains a virus, further comprises the steps of:"

MIMEsweeper discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 ("MIMEsweeper is an enabling technology which facilitates the implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments.").

**(2) "…storing the message in a temporary file;"**

Claim 14 further recites "storing the message in a temporary file;"

The aspect of storing data in a temporary file at the server is disclosed by MIMEsweeper. *See e.g.,* MIMEsweeper at pg. 13 ("The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery.")

**(3) "…scanning the temporary file for viruses; and testing whether the scanning step found a virus.'**

Claim 14 further recites "scanning the temporary file for viruses and testing whether the scanning step found a virus."

MIMEsweeper teaches checking the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

**BB. Whether claim 14 is obvious in view of the LANProtect reference, the MIMEsweeper reference, the TIS Firewall reference, the Sidewinder reference, the MpScan reference and the Layland reference in combination with the previously considered Hile reference**

None of MIMEsweeper, TIS Firewall, Sidewinder, MpScan, Layland were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the storing of the messages in temporary files and thereafter scanning the messages for the presence of the viruses was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the storage of the messages in the temporary files and thereafter

scanning the temporary files for the presence of the viruses raise a substantial new question of patentability with respect to claim 14 as pointed out in more detail below.

**Claim 14** recites "The method of claim 11, wherein the step of determining whether the mail message contains a virus, further comprises the steps of:

- storing the message in a temporary file;
- scanning the temporary file for viruses; and
- testing whether the scanning step found a virus."

Claim 14 adds the limitation of storing the data in a temporary file to claim 11. The storing of data at the server is not a new feature and inherent in virus scanning gateway systems. Claim 14 is rendered obvious by the combinations of LANProtect and/or MIMEsweeper and/or the TIS Firewall and/or Sidewinder and/or MpScan and/or the Layland and/or in combination with the previously considered Hile reference.

### I. LANProtect in view of TIS Firewall and/or Sidewinder and/or MpScan and/or Layland renders obvious Claim 14 Under § 103(a);

LANProtect was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

LANProtect discloses detecting viruses in data transfers between computers. *See e.g.,* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file server from inbound and outbound virus activity."). *See e.g.,* LANProtect at pg. 16 ("Direction of I/O to scan- LANProtect has the capability to scan files as they enter the server or as they enter and exit the server.").

LANProtect discloses the element of storage of the data in a temporary file at the server and thereafter scanning the file for the presence of the viruses. See e.g., LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines

infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses.... LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files specified as 'all' or by specific file extension).").

LANProtect discloses the element of storage of the data in a temporary file at the server and thereafter scanning the data for a virus using the server. *See e.g.,* LANProtect at pg. 11 and 14 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v. 1.5 has additional virus detection technology to effectively handle these types of viruses.... LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (e.g., from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).").

LANProtect discloses detecting polymorphic viruses, such as those that utilize mutation engine code to encrypt various portions of the virus with different encryption keys for each new instance of the virus, with the help of a rule-oriented analyzer. As such, LANProtect discloses the steps of detecting encoded portions of a mail message, decoding the encoded portions and scanning the encoded portions for viruses. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it,

examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it.").

However if the aspect of "storing the messages in temporary files and thereafter scanning the temporary files for the presence of the viruses" was somehow construed so that LANProtect did not practice this aspect, the following references combined with LANProtect would render claim 14 obvious.

This element is disclosed or suggested by a set of prior art including TIS Firewall, the Sidewinder, MpScan, Layland as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Following is a discussion of how TIS Firewall, Sidewinder, MpScan and Layland together in view of the previously considered Hile reference disclose (either expressly or inherently) and render obvious each limitation of claim 14.

In the TIS Firewall, the encoded portion is stored in separate temporary storage. The "?" character is decoded by replacement with a "#" character and the following address site is scanned for other "?" characters. Based on the test of whether any other "?" characters are found, further replacements are made. *See e.g.,* TIS Firewall at pg. 10, FN 3 ("The Morris Internet worm took

advantage of a loophole in fingerd to compromise some systems"), TIS Firewall at pg. 10 ("if there is a security hole in fingerd, it cannot be effectively exploited, since no file system or executables will be available to the attacker").

In addition, Sidewinder teaches routines that can store mail messages in storage based on content or presence of object code containing viruses and then scan those messages for viruses. *See e.g.,* Sidewinder at SR-454.1 – SR-454.2 ("Sidewinder is an application-level secure gateway between TCP/IP networks and incorporates the patented Type Enforcement mechanism"), 2858 (discusses Type Enforcement and data filtering), SR-454.9 – SR-454.11 (the Sidewinder System Administrator can filter mail based on destination or content).

Furthermore, MpScan describes the aspect of receiving a mail message and performing the pattern matching of the outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/or are transmitted to and from competitor's addresses, except as authorized. To the extent the reference doesn't explicitly disclose whether the mail messages are stored in temporary files or in some other form of storage, in order to perform the pattern matching of outgoing email, it would have been obvious to use a temporary file to store messages temporarily. *See e.g.,* MpScan pg. 1-2.

Layland was not considered during prosecution of the '600 patent. Layland suggests use of an Internet gateway that subjects all incoming files to a virus scan by storing mail messages, for example, in temporary files or in some other form of storage prior to the scanning of the data for the presence of the viruses. *See e.g.,* Layland at pg. 23-24 ("The router would send all traffic to and from the Internet to the gateway for approval and processing before routing the traffic to its destination.... The Internet Gateway would subject all incoming files to a virus scan.") In order to

scan the incoming files, it would have been obvious to use the temporary files or some other means of storage for storing or buffering the incoming files.

The teachings as contained in TIS Firewall, Sidewinder, MpScan and Layland were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination. Hile teaches storing of data in a temporary file, scanning the temporary file for virus, and determining if a virus is present or not. *See e.g.,* col. 4, ll. 7-26.

As described above, a reasonable examiner would consider these combined teachings important in determining whether claim 14 is patentable. For this reason, the teachings of Hile in combination with the teachings of TIS Firewall, Sidewinder, MpScan and Layland raise a substantial new question of patentability with respect to at least claim 14 of the '600 patent.

### II. MIMEsweeper in view of TIS Firewall and/or Sidewinder and/or MpScan and/or Layland renders obvious Claim 14 Under § 103(a);

MIMEsweeper was not considered during the prosecution of the '600 patent. It was released in Sept, 1995, to protect networks from virus infection via E-mail. The MIMEsweeper was conceived out of a requirement to scan incoming E-mails and their attachments for computer viruses.

MIMEsweeper discloses a mail gateway system that handles SMTP traffic and incorporates the functionality of scanning the E-mail attachments for the presence of virus. *See e.g.,* MIMEsweeper at pg. 5 ("MIMEsweeper is an enabling technology which facilitates the implementation of various functionality and applications at the important Email gateway to external or internal networks. It is envisaged that the most common such functionality will be virus scanning of Email attachments.").

The aspect of storing the data in a temporary file at the server is disclosed by MIMEsweeper reference. *See e.g.,* MIMEsweeper at pg. 13 ("The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyse, and then collect cleared messages for onward delivery.")

MIMEsweeper checks the incoming email attachments for viruses at the server. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

However if the aspect of "storing the messages in temporary files and thereafter scanning the temporary files for the presence of the viruses" was somehow construed so that MIMEsweeper did not practice this aspect, the following references combined with MIMEsweeper would render claim 14 obvious.

This element is disclosed or suggested by a set of prior art including TIS Firewall, Sidewinder, MpScan and Layland as discussed below. A *prima facie* case of obviousness is

established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Following is a discussion of how TIS Firewall, Sidewinder, MpScan and Layland together in view of the previously considered Hile disclose (either expressly or inherently) and render obvious each limitation of claim 14.

In the TIS Firewall, the encoded portion is stored in separate temporary storage. The "?" character is decoded by replacement with a "#" character and the following address site is scanned for other "?" characters. Based on the test of whether any other "?" characters are found, further replacements are made. *See e.g.,* TIS Firewall at pg. 10, FN 3 ("The Morris Internet worm took advantage of a loophole in fingerd to compromise some systems"), TIS Firewall at pg. 10 ("if there is a security hole in fingerd, it cannot be effectively exploited, since no file system or executables will be available to the attacker").

In addition, Sidewinder teaches routines that can store mail messages in storage based on content or presence of object code containing viruses and then scan those messages for viruses. *See e.g.,* Sidewinder at SR-454.1 – SR-454.2 ("Sidewinder is an application-level secure gateway between TCP/IP networks and incorporates the patented Type Enforcement mechanism"), 2858

(discusses Type Enforcement and data filtering), SR-454.9 – SR-454.11 (the Sidewinder System Administrator can filter mail based on destination or content).

Furthermore, MpScan describes the aspect of receiving a mail message and performing the pattern matching of the outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/or are transmitted to and from competitor's addresses, except as authorized. To the extent the reference doesn't explicitly disclose whether the mail messages are stored in temporary files or in some other form of storage, in order to perform the pattern matching of outgoing email, it would have been obvious to use a temporary file to store messages temporarily. *See e.g.,* MpScan pg. 1-2.

Layland indicates the storage of mail messages in temporary files or in some other form of storage prior to the scanning of the data for the presence of the viruses. *See e.g.,* Layland at pg. 23-24 ("The router would send all traffic to and from the Internet to the gateway for approval and processing before routing the traffic to its destination.... The Internet Gateway would subject all incoming files to a virus scan.") In order to scan the incoming files, it would have been obvious to use the temporary files or some other means of storage for storing or buffering the incoming files.

The teachings as contained in TIS Firewall, Sidewinder, MpScan and Layland were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination. Hile teaches storing of data in a temporary file, scanning the temporary file for viruses, and determining if a virus is present or not. *See e.g.,* col. 4, ll. 7-26.

As described above, a reasonable examiner would consider these combined teachings important in determining whether claim 14 is patentable. For this reason, the teachings of Hile in

combination with the teachings by MIMEsweeper, TIS Firewall, Sidewinder, MpScan and Layland raise a substantial new question of patentability with respect to at least claim 14 of the '600 patent.

### CC. Whether claim 15 is obvious in view of the LANProtect reference and the TIS Firewall reference

Claim 15 adds a further limitation to claim 11 by claiming that the virus scanning is carried out by signature scanning process. One or more references discussed below disclose the aspect of signature scanning process of virus detection.

#### I. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious Claim 15 Under § 103(a)**

**Claim 15: "scanning is performed using a signature scanning process"**

Claim 15 recites "The method of claim 11, wherein the step of scanning is performed using a signature scanning process."

LANProtect discloses the element of signature scanning. The Intel Products performed the signature scanning process while scanning for viruses. See, e.g., LANProtect at pg. 4-10.

#### II. The TIS Firewall Reference

The TIS Firewall reference was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls.

**TIS Firewall makes obvious Claim 6 Under § 103(a)**

**Claim 15: "scanning is performed using a signature scanning process"**

Claim 15 recites "The method of claim 11, wherein the step of scanning is performed using a signature scanning process."

TIS Firewall discloses the element of signature scanning process of virus scanning. The TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm using signature scanning.

*See e.g.*, TIS Firewall at pg. 41 (since many attacks "have a distinctive signature, smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

Neither LANProtect nor TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspect of scanning the mail messages for the presence of encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus wherein the scanning for virus is done via signature analysis. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 15 as pointed out above.

**DD. Whether claim 15 is obvious in view of the Cheswick and Bellovin reference, the Sidewinder reference and the MpScan reference**

Claim 15 adds a further limitation to claim 11 by claiming that the virus scanning is carried out by signature scanning process. Claim 15 is rendered obvious by the combination of Cheswick and Bellovin with Sidewinder in view of MpScan.

The aspect signature scanning is suggested by MpScan and renders every limitation of claim 15 obvious in combination with Cheswick and Bellovin or Sidewinder. See MpScan at 2 ("Performs pattern matching of outgoing email for words, phrases or any other defined data delivery.")

So, a person having ordinary skill in the art can easily use the teachings of Cheswick and Bellovin in combination with the teachings of Sidewinder and further in view of MpScan to come up with a computer implemented method of virus detection at the server wherein the virus detection is selectively done by scanning the mail messages for the presence of encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus wherein the scanning for virus is done via signature analysis.

None of Cheswick and Bellovin, Sidewinder and MpScan were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspect of scanning the mail messages for the presence of encoded portions, storing the encoded portions in separate temporary files and thereafter decoding the stored encoded portions to detect the presence of the virus wherein the scanning for virus is done via signature analysis. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or

printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 15 as pointed out above.

### EE. Whether claim 16 is obvious in view of the LANProtect reference and the MIMEsweeper reference

The teaching related to the step of performing a preset action on the mail message comprising one of transferring the mail message unchanged, not transferring the mail message, storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address as contained in the references presented below was not present during the prior examination of the '600 patent. A reasonable examiner would consider this teaching important in determining whether claim 16 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 16 of the '600 patent.

#### I. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious claim 16 under § 103(a)**

**Claim16: "The method of claim 11, wherein**

**(2) …the step of performing a preset action on the mail message comprises performing one step from the group of:"**

Claim 16 recites "The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:"

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

**(2) "…transferring the mail message unchanged;"**

Claim 16 further recites "transferring the mail message unchanged."

In LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone or moving the virus infected file to a special directory. *See e.g.,* LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented

analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.,* LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory.").

**(3) "...not transferring the mail message;"**

Claim 16 further recites "not transferring the mail message."

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

**(4) "...storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name; and"**

Claim 16 further recites "storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name."

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

**(5) "…creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address."**

Claim 16 further recites "creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address."

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

## II. The MIMEsweeper Reference

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses.

**MIMEsweeper makes obvious claim 16 under § 103(a)**

**Claim16: "The method of claim 11, wherein**

**(1) …the step of performing a preset action on the mail message comprises performing one step from the group of:"**

Claim 16 recites "The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:"

MIMEsweeper teaches scanning the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper further discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**(2) "…transferring the mail message unchanged;"**

Claim 16 further recites "transferring the mail message unchanged."

MIMEsweeper discloses the transfer of the mail message unchanged depending on the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages,

(iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

**(3) "…not transferring the mail message;"**

Claim 16 further recites "not transferring the mail message."

MIMEsweeper discloses the aspect of not transferring the transfer of the mail message unchanged depending on the return codes from the Virus checking packages called 'Validators'. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**(4) "…storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name; and"**

Claim 16 further recites "storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name."

MIMEsweeper discloses the storage of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called 'Validators'. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of

quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**(5) "...creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address."**

Claim 16 further recites "creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address."

MIMEsweeper discloses the storage of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called 'Validators' and further archiving log files to the removable media which contain the output of the determining step. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**FF. Whether claim 16 is obvious in view of the LANProtect reference, the MIMEsweeper reference, the Sidewinder reference, the TIS Firewall reference, the Layland reference and the SunScreen SPF-100 reference**

None of LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with

a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address raise a substantial new question of patentability with respect to claim 16 as pointed out in more detail below.

**Claim 16** recites "The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:

- transferring the mail message unchanged;
- not transferring the mail message;

- storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name; and
- creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address.

**I. LANProtect in view of Sidewinder and/or TIS Firewall and/or Layland and/or SunScreen SPF-100 renders obvious Claim 16 Under § 103(a):**

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

The SunScreen SPF-100 reference was developed in 1995 to provide broader, more robust and more flexible network security. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF 100 was also designed to provide administrators with the necessary tools to flexibly and intuitively manage their gateway access to public networks. Employing a dedicated administration station, the SunScreen SPF 100 system ensures absolute administration privacy and easy to-use rule-based controls to ensure that internal corporate networks and intercompany communications are safeguarded.

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file

containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

However if the aspect of "the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message

request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address;" was somehow construed so that LANProtect did not practice this aspect, the following references combined with LANProtect would render claim 16 obvious.

This element is disclosed or suggested by a set of prior art including the Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). The Sidewinder reference clearly teaches the storage of the rejected messages

for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its destination. *See e.g.,* TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. It suggests the Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a

log detailing any incidence of corrupted files and also the sources of those files. *See e.g.,* Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

Furthermore, SunScreen SPF-100 discloses some of the aspects of claim 16. The SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

So, a person having ordinary skill in the art can easily use the teachings of the LANProtect in combination with the teachings of Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 to come up with a computer implemented method for detecting viruses in a mail message transferred

between a first computer and a second computer wherein the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address.

None of LANProtect, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 16 as pointed out above.

**II. MIMEsweeper in view of Sidewinder and/or TIS Firewall and/or the Layland and/or SunScreen SPF-100 renders obvious Claim 16 Under § 103(a):**

MIMEsweeper was not considered during the prosecution of the '600 patent. It was released in Sept, 1995, to protect networks from virus infection via E-mail. MIMEsweeper was conceived out of a requirement to scan incoming E-mails and their attachments for computer viruses.

SunScreen SPF-100 was developed in 1995 to provide broader, more robust and more flexible network security. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 was also designed to provide administrators with the necessary tools to flexibly and intuitively manage their gateway access to public networks. Employing a dedicated administration station, the SunScreen SPF-100 system ensures absolute administration privacy and easy to-use rule-based controls to ensure that internal corporate networks and intercompany communications are safeguarded.

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper further discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include:

(i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

MIMEsweeper further discloses the storage of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called 'Validators' and in addition archiving log files to the removable media which contain the output of the determining step. *See e.g.,* MIMEsweeper at pg. 9.

However if the aspect of "the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address;" was somehow construed so that MIMEsweeper did not practice this aspect, the following references combined with MIMEsweeper would render claim 16 obvious.

This element is disclosed or suggested by a set of prior art including the Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to

interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). The Sidewinder reference clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its

destination. *See e.g.,* TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. Layland suggests an Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a log detailing any incidence of corrupted files and also the sources of those files. *See e.g.,* Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

Furthermore, SunScreen SPF-100 discloses some of the aspects of claim 16. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the

inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

So, a person having ordinary skill in the art can easily use the teachings of the MIMEsweeper in combination with the teachings of Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 reference to come up with a computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer wherein the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address.

None of MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent

concerns the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or not transferring the mail message, or storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name or creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 16 as pointed out above.

### GG. Whether claim 17 is obvious in view of the LANProtect reference and the MIMEsweeper reference

The teaching related to the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message as contained in the references presented below was not present during the prior examination of the '600 patent. A reasonable examiner would consider this teaching important in determining whether claim 17 is

patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 17 of the '600 patent.

## I. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious claim 17 under § 103(a)**

**Claim17: "The method of claim 11, wherein**

**(1) …the step of performing a preset action on the mail message comprises performing one step from the group of:"**

Claim 17 recites "The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:"

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect

places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

**(2) "...transferring the mail message unchanged;"**

Claim 17 further recites "transferring the mail message unchanged."

In LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone or moving the virus infected file to a special directory. *See e.g.,* LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.,* LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory.").

**(3) "...transferring the mail message with the encoded portions having a virus deleted;"**

Claim 17 further recites "transferring the mail message with the encoded portions having a virus deleted."

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection

determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

**(4) "…renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory; and"**

Claim 17 further recites "renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory."

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in

the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

**(5) "....writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message."**

Claim 17 further recites "writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message."

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and

immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

## II. The MIMEsweeper Reference

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses.

**MIMEsweeper makes obvious claim 17 under § 103(a)**

**Claim17: "The method of claim 11, wherein**

**(1) ...the step of performing a preset action on the mail message comprises performing one step from the group of:"**

Claim 17 recites "The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:"

MIMEsweeper teaches scanning the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper further discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail

administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**(2) "…transferring the mail message unchanged;"**

Claim 17 further recites "transferring the mail message unchanged."

MIMEsweeper discloses the transfer of the mail message unchanged depending on the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

**(3) "…transferring the mail message with the encoded portions having a virus deleted;"**

Claim 17 further recites "transferring the mail message with the encoded portions having a virus deleted."

To the extent MIMEsweeper doesn't explicitly disclose the aspect of transferring the mail message with the encoded portions having viruses deleted, this aspect would have been obvious to any person skilled in the art.

**(4) "...renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory; and"**

Claim 17 further recites "renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory."

MIMEsweeper discloses the copying of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called 'Validators'. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**(5) "....writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message."**

Claim 17 further recites "writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message."

MIMEsweeper discloses the copying of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called 'Validators' and further archiving log files to the removable media which contain the output of the determining step. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**HH. Whether claim 17 is obvious in view of the LANProtect reference, the MIMEsweeper reference, the Sidewinder reference, the TIS Firewall reference, the Layland reference and the SunScreen SPF-100 reference**

None of LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents

a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message raise a substantial new question of patentability with respect to claim 17 as pointed out in more detail below.

**Claim 17** recites "The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:

- transferring the mail message unchanged;
- transferring the mail message with the encoded portions having a virus deleted; and
- renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory; and
- writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message.

**I. <u>LANProtect</u> in view of <u>Sidewinder</u> and/or <u>TIS Firewall</u> and/or <u>Layland</u> and/or <u>SunScreen SPF-100</u> renders obvious Claim 17 Under § 103(a):**

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

SunScreen SPF 100 was developed in 1995 to provide broader, more robust and more flexible network security. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 was also designed to provide administrators with the necessary tools to flexibly and intuitively manage their gateway access to public networks. Employing a dedicated administration station, the SunScreen SPF-100 system ensures absolute administration privacy and easy to-use rule-based controls to ensure that internal corporate networks and intercompany communications are safeguarded.

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

However if the aspect of "the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message;" was somehow construed so that LANProtect did not practice this aspect, the following references combined with LANProtect would render claim 17 obvious.

This element is disclosed or suggested by a set of prior art including the Sidewinder, the TIS Firewall, Layland and SunScreen SPF-100 as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). The Sidewinder reference clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP

mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its destination. *See e.g.,* TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. Layland suggests an Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a log detailing any incidence of corrupted files and also the sources of those files. *See e.g.,* Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user

could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

Furthermore, SunScreen SPF-100 discloses some of the aspects of claim 17. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

So, a person having ordinary skill in the art can easily use the teachings of the LANProtect in combination with the teachings of Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 to come up with a computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer wherein the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified

directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message.

None of LANProtect, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 17 as pointed out above.

## II. MIMEsweeper in view of Sidewinder and/or TIS Firewall and/or Layland and/or SunScreen SPF-100 renders obvious Claim 17 Under § 103(a):

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses.

SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 was also designed to provide administrators with the necessary tools to flexibly and intuitively manage their gateway access to public networks. Employing a dedicated administration station, the SunScreen SPF-100 system ensures absolute administration privacy and easy to-use rule-based controls to ensure that internal corporate networks and intercompany communications are safeguarded.

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper further discloses the steps of performing a preset action on the messages according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages,

(iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

MIMEsweeper further discloses the copying of the corrupt mail messages to removable area depending on the return codes from the Virus checking packages called 'Validators' and in addition archiving log files to the removable media which contain the output of the determining step. *See e.g.,* MIMEsweeper at pg. 9.

However if the aspect of "the step of performing a preset action on the mail message comprising of either of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message." was somehow construed so that MIMEsweeper did not practice this aspect, the following references combined with MIMEsweeper would render claim 17 obvious.

This element is disclosed or suggested by a set of prior art including the Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be

provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). The Sidewinder reference clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "Simple Mail Access Protocol." *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its destination. *See e.g.,* TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. Layland suggests an Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a log detailing any incidence of corrupted files and also the sources of those files. *See e.g.,* Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

Furthermore, SunScreen SPF-100 discloses some of the aspects of claim 17. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across

public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

So, a person having ordinary skill in the art can easily use the teachings of the MIMEsweeper in combination with the teachings of Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 to come up with a computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer wherein the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message.

None of MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the step of performing a preset action on the mail message comprising of either transferring the mail message unchanged, or transferring the mail message with the encoded portions having a virus deleted, or renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory or writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 17 as pointed out above.

### II. Whether claim 18 is obvious in view of the TFS Manual reference, the LANProtect reference, the Cheswick and Bellovin reference and the TIS Firewall reference

Independent claim 18 relates to an apparatus for detecting viruses in the data transfers between two computers at a server. It includes steps for checking for the presence of a virus in the

data and transferring the data depending on the result of the virus check. Claim 18 also includes steps for performing preset action on the data if the data contains virus. The steps of claim 18 are obvious in view of one or more references as discussed below:

## I. The TFS Manual Reference

The TFS Manual reference was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network.

**TFS Manual makes obvious Claim 18 Under § 103(a)**

**Claim 18: "An apparatus"**

**(1) "...for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:"**

Claim 18 recites "An apparatus for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:"

TFS Manual discloses a gateway having a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. See, e.g., TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

**(2) "...means for receiving a data transfer request including a destination address;"**

Claim 18 further recites "means for receiving a data transfer request including a destination address."

TFS Manual discloses a gateway that receives mail message requests using SMTP, and other protocols. *See, e.g.* TFS Manual, Chapter on "Receiving Mail from Internet Mail" (TFS "will send any outgoing messages and receive any incoming messages.");

**(3) "...means for electronically receiving data at a server;"**

Claim 18 further recites "means for electronically receiving data at a server."

The TFS Manual discloses a gateway wherein the mail message would be electronically received at the server.

**(4) "...means for determining whether the data contains a virus at the server;"**

Claim 18 further recites "means for determining whether the data contains a virus at the server."

TFS Manual discloses a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. *See e.g.,* TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

**(5) "...means for performing a preset action on the data using the server if the data contains a virus; and"**

Claim 18 further recites "means for performing a preset action on the data using the server if the data contains a virus."

TFS Gateway would perform different actions depending on the results of the virus scanning. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

**(6) "...means for sending the data to the destination address if the data does not contain a virus."**

Claim 18 further recites "means for sending the data to the destination address if the data does not contain a virus."

TFS Manual teaches the gateway would perform different actions depending on the results of the virus scanning. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

## II. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious Claim 18 Under § 103(b)**

**Claim 18: "An apparatus"**

**(1) "...for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:"**

Claim 18 recites "An apparatus for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:"

LANProtect can detect viruses during file transfers between computers. *See, e.g.* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN NLM to intercept file activities and then draws on the virus pattern library … to scan those files for known viruses.").

**(2) "…means for receiving a data transfer request including a destination address;"**

Claim 18 further recites "means for receiving a data transfer request including a destination address."

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

**(3) "…means for electronically receiving data at a server;"**

Claim 18 further recites "means for electronically receiving data at a server;"

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address and data being received electronically adds a meaningless limitation to claim 18. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

**(4) "...means for determining whether the data contains a virus at the server;"**

Claim 18 further recites "means for determining whether the data contains a virus at the server."

LANProtect product literature confirms that LANProtect performed this step. *See, e.g.* LANProtect at pg. 3, 6 and 11 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v.1.5 has additional virus detection technology to effectively handle these types of viruses .... LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (*e.g.*, from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).

**(5) "...means for performing a preset action on the data using the server if the data contains a virus; and"**

Claim 18 further recites "means for performing a preset action on the data using the server if the data contains a virus."

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

**(6) "...means for sending the data to the destination address if the data does not contain a virus;"**

Claim 18 further recites "means for sending the data to the destination address if the data does not contain a virus."

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

## III. The Cheswick and Bellovin Reference

The Cheswick and Bellovin reference was not considered during prosecution of the '600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers.

**Cheswick and Bellovin makes obvious Claim 18 Under § 103(a)**

**Claim 18: "An apparatus"**

**(1) "...for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:"**

Claim 18 recites "An apparatus for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:"

Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. *See e.g.,* Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. *See e.g.,* Cheswick and Bellovin at 70. Cheswick and Bellovin also describes implementing various security operations at the gateway including selective scanning and potential operations that could be performed in the event a threat is found. *See e.g.,* Cheswick and Bellovin at 76. ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

**(2) "...means for receiving a data transfer request including a destination address;"**

Claim 18 further recites "means for receiving a data transfer request including a destination address."

Cheswick and Bellovin describes a system that receives data transfer requests with a destination address at a server. *See e.g.,* Cheswick and Bellovin at pg. 66-69 and 74-75.

**(3) "...means for electronically receiving data at a server;"**

Claim 18 further recites "means for electronically receiving data at a server;"

Cheswick and Bellovin describes that the incoming files are scanned for virus therefore the data is received electronically. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

**(4) "...means for determining whether the data contains a virus at the server;"**

Claim 18 further recites "means for determining whether the data contains a virus at the server."

Cheswick and Bellovin describes scanning for viruses at a server. See e.g., Cheswick and Bellovin at pg. 76 ("A location with many PC users might wish to scan incoming files for viruses.").

**(5) "...means for performing a preset action on the data using the server if the data contains a virus; and"**

Claim 18 further recites "means for performing a preset action on the data using the server if the data contains a virus."

Cheswick and Bellovin describes filtering files that do not meet the criteria of the gateway and thus would filter a file containing a virus in a preset manner. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

Cheswick and Bellovin teaches that the firewall can log and control all incoming and outgoing traffic. Controlling all traffic includes sending the data to the destination address if the data meets the criteria of the gateway, or for example, does not contain a virus. *See e.g.*, Cheswick and Bellovin at pg. 74-75.

**(6) "...means for sending the data to the destination address if the data does not contain a virus."**

Claim 18 further recites "means for sending the data to the destination address if the data does not contain a virus."

Cheswick and Bellovin teaches that the firewall can log and control all incoming and outgoing traffic. Controlling all traffic includes sending the data to the destination address if the data meets the criteria of the gateway, or for example, does not contain a virus. *See e.g.*, Cheswick and Bellovin at pg. 74-75.

## IV. The TIS Firewall Reference

The TIS Firewall reference was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls.

**TIS Firewall makes obvious Claim 18 Under § 103(a)**

**Claim 18: "An apparatus"**

**(1) "...for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:"**

Claim 18 recites "An apparatus for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:"

TIS Firewall is a computer firewall system that is capable of detecting and selectively removing worms and viruses, as evidenced by the fact that it detected the Internet Worm, which exploited a well-known hole in the standard UNIX SMTP server, sendmail. *See e.g.*, TIS Firewall at pg. 10, FN 3 ("The Morris Internet worm took advantage of a loophole in fingerd to compromise some systems").

**(2) "...means for receiving a data transfer request including a destination address;"**

Claim 18 further recites "means for receiving a data transfer request including a destination address."

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

**(3) "...means for electronically receiving data at a server;"**

Claim 18 further recites "means for electronically receiving data at a server."

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP

protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

**(4) "...means for determining whether the data contains a virus at the server;"**

Claim 18 further recites "means for determining whether the data contains a virus at the server."

TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm. *See e.g.*, TIS Firewall at pg. 41 (since many attacks "have a distinctive signature, smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

**(5) "...means for performing a preset action on the data using the server if the data contains a virus; and"**

Claim 18 further recites "means for performing a preset action on the data using the server if the data contains a virus."

TIS Firewall teaches performing preset actions based on the content of the message, including the presence of a virus.

**(6) "...means for sending the data to the destination address if the data does not contain a virus."**

Claim 18 further recites "means for sending the data to the destination address if the data does not contain a virus."

TIS Firewall discloses the element of sending the data to the destination if the data does not contain a virus. If an attack signature is not detected, a daemon process passes the message to the mail handler, which is a daemon itself and which in turn forwards the message ultimately to the destination address.

### JJ. Whether claim 18 is obvious in view of the TFS Manual reference, the LANProtect reference, the Cheswick and Bellovin reference and the TIS Firewall reference in combination with the previously considered Hile reference

None of TFS Manual, LANProtect, Cheswick and Bellovin and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, while Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith raise a substantial new question of patentability with respect to claim 18 as pointed out in more detail below.

**Claim 18** recites "An apparatus for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:

- means for receiving a data transfer request including a destination address;

- means for electronically receiving data at a server; means for determining whether the data contains a virus at the server;
- means for performing a preset action on the data using the server if the data contains a virus; and
- means for sending the data to the destination address if the data does not contain a virus.

Following is a discussion of how the TFS Manual, LANProtect, Cheswick and Bellovin, TIS Firewall together in view of the previously considered Hile reference disclose (either expressly or inherently) and render obvious each limitation of claim 18.

TFS Manual discloses a gateway having a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. See, e.g., TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

TFS Manual discloses a gateway that receives mail message requests using SMTP, and other protocols. *See, e.g.* TFS Manual, Chapter on "Receiving Mail from Internet Mail" (TFS "will send any outgoing messages and receive any incoming messages.");

The TFS Manual discloses a gateway wherein the mail message would be electronically received at the server.

TFS Manual discloses a computer-implemented method for detecting viruses in data transfers, specifically mail messages, between a first computer and a second computer. *See e.g.,* TFS Manual at 1 ("TFS is a series of gateway products that acts as a link between local as well as global mail systems."). The user's manual explicitly instructed users how to write a "VIRUS.BAT" file to be invoked by the TFS Gateway so that all incoming mail message attachments could be scanned for viruses with a commercially available antivirus scanner. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified.")

TFS Gateway would perform different actions depending on the results of the virus scanning. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

TFS Manual teaches the gateway would perform different actions depending on the results of the virus scanning. *See e.g.,* TFS Manual at 77 ("With version 2.1 of TFS it is possible to check files for viruses on all incoming attachments. If the file contains a known virus the file will be automatically deleted and the sender and recipient will be notified."). On the other hand, if no virus was detected, the data or mail message would be sent to its destination.

Furthermore, LANProtect can detect viruses during file transfers between computers. *See, e.g.* LANProtect at pg. 2 ("LProtect is a NetWare Loadable Module (NLM) that continuously shields file servers from inbound and outbound virus activity. Regardless of file source (e.g., workstation, modem server, e-mail file transfer, etc.), the LProtect NLM uses the Intel PSCAN

NLM to intercept file activities and then draws on the virus pattern library … to scan those files for known viruses.").

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address and data being received electronically adds a meaningless limitation to claim 18. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

LANProtect product literature confirms that LANProtect performed this step. *See, e.g.* LANProtect at pg. 3, 6 and 11 ("LANProtect prevents viruses from being introduced onto the network and quarantines infected files so they do not contaminate other files;" "LANProtect v.1.5 has additional virus detection technology to effectively handle these types of viruses …. LANProtect draws on a virus pattern library to detect common known viruses;" "Real-Time Scanning: All network traffic originating outside the file server (*e.g.*, from workstations, modem servers, etc.) and all network traffic originating at the file server is scanned for virus infections. The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving

the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

LANProtect discloses the step of performing a preset action on the data. LANProtect teaches various configuration options upon detecting a virus, including (i) notifying the user if there is a virus, (ii) renaming the file, (iii) deleting the file, (iv) leaving the file unchanged, or (v) moving the file. LANProtect at pg. 2-29 and 2-34). Further, if a file does not contain a virus, LANProtect teaches allowing transfer of the data to the destination address.

Cheswick and Bellovin extensively teaches and describes the use and construction of a firewall or other system that can detect viruses in data transfers. See Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules, and filter placement; also, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. See Cheswick and Bellovin at 70. Cheswick and Bellovin also describes implementing various security operations at the gateway including selective scanning and potential operations that could be performed in the event a threat is found. See Cheswick and Bellovin at 76. ("Application gateways are often used in conjunction with the other gateway designs, packet filters and circuit-level relays. As we show later [], an application gateway can be used to pass X11 [a type of network traffic] through a firewall with reasonable security. The semantic knowledge inherent in the design of an application gateway can be used in more sophisticated fashions. As described earlier, gopher servers can specify that a file is in the format used by the uuencode program. But that format includes a file name and mode. A clever gateway could examine or even rewrite this line, thus blocking attempts to force the installation of bogus .rhosts files or shells with the setuid bit turned on. The type of filtering used depends on local needs and customs. A location with many PC users might wish to scan incoming files for viruses.")

Cheswick and Bellovin describes a system that receives data transfer requests with a destination address at a server. See e.g., Cheswick and Bellovin at pg. 66-69 and 74-75.

Cheswick and Bellovin describes that the incoming files are scanned for virus therefore the data is received electronically. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

Cheswick and Bellovin describes scanning for viruses at a server. See e.g., Cheswick and Bellovin at pg. 76 ("A location with many PC users might wish to scan incoming files for viruses.").

Cheswick and Bellovin describes filtering files that do not meet the criteria of the gateway and thus would filter a file containing a virus in a preset manner. *See e.g.*, Cheswick and Bellovin at pg. 76-77.

Cheswick and Bellovin teaches that the firewall can log and control all incoming and outgoing traffic. Controlling all traffic includes sending the data to the destination address if the data meets the criteria of the gateway, or for example, does not contain a virus. *See e.g.*, Cheswick and Bellovin at pg. 74-75.

In addition, the TIS Firewall is a computer firewall system that is capable of detecting and selectively removing worms and viruses, as evidenced by the fact that it detected the Internet Worm, which exploited a well-known hole in the standard UNIX SMTP server, sendmail. *See e.g.*, TIS Firewall at pg. 10, FN 3 ("The Morris Internet worm took advantage of a loophole in fingerd to compromise some systems").

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9(smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP

protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm. *See e.g.*, TIS Firewall at pg. 41 (since many attacks "have a distinctive signature, smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

TIS Firewall performs preset actions based on the content of the message, including the presence of a virus. The TIS Firewall replaces the "|" character with a "#" character (modify), writes the file to a holding area (sequester) and logs the event (alert), only if the address portion of the mail message contains a "|" character.

TIS Firewall reference discloses the element of sending the data to the destination if the data does not contain a virus. If an attack signature is not detected, a daemon process passes the message to the mail handler, which is a daemon itself and which in turn forwards the message ultimately to the destination address.

The teachings as contained in TFS Manual, LANProtect, Cheswick and Bellovin, TIS Firewall were not present during the prior examination of the '600 patent.

While Hile was cited during examination of the '600 patent, the teachings of Hile in view of the prior art presented herewith was not present during examination. As described above, a reasonable examiner would consider these combined teachings important in determining whether claim 18 is patentable. For this reason, the teachings of Hile in combination with the teachings by

TFS Manual, LANProtect, Cheswick and Bellovin, TIS Firewall raise a substantial new question of patentability with respect to at least claim 18 of the '600 patent.

So, a person having ordinary skill in the art can easily use the teachings of the previously considered Hile reference in combination with the teachings of TFS Manual or LANProtect or the teachings of Cheswick and Bellovin or TIS Firewall to come up with an apparatus for detecting viruses in data transfers between a first computer and a second computer, wherein the apparatus is capable of electronically receiving data transfer request including a destination address, capable of determining whether the data contains a virus at the server and further capable of performing a preset action or directly sending the data to the destination address depending on whether the data contains virus or not.

### KK. Whether claim 19 is obvious in view of the LANProtect reference and the TIS Firewall reference

Claim 19 adds a further limitation to claim 18 by claiming that the virus scanning is carried out by signature scanning process. One or more references discussed below disclose the aspect of signature scanning process of virus detection.

#### I. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious Claim 19 Under § 103(b)**

**Claim 19: "scanning is performed using a signature scanning process"**

Claim 19 recites "The apparatus of claim 18, wherein means for determining includes a means for scanning that scans the data using a signature scanning process."

LANProtect discloses the element of signature scanning. The Intel Products performed the signature scanning process while scanning for viruses. See, e.g., LANProtect at pg. 4-10.

## II. The TIS Firewall Reference

The TIS Firewall reference was not considered during the prosecution of the '600 patent. It was published in June 30, 1994 and describes a set of programs and configuration practices designed to facilitate the building of network firewalls.

### TIS Firewall makes obvious Claim 19 Under § 103(a)

**Claim 19: "scanning is performed using a signature scanning process"**

Claim 19 recites "The apparatus of claim 18, wherein means for determining includes a means for scanning that scans the data using a signature scanning process."

TIS Firewall discloses the element of signature scanning process of virus scanning. The TIS Firewall includes a server that scans content for the presence of special characters indicating a virus or worm using signature scanning. *See e.g.,* TIS Firewall at pg. 41 (since many attacks "have a distinctive signature smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

Neither LANProtect nor TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspect of scanning the data for the presence of the viruses at the server wherein the scanning for virus is done via signature analysis. As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents

a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 19 as pointed out above.

### LL. Whether claim 19 is obvious in view of the Cheswick and Bellovin reference, the Sidewinder reference and the MpScan reference

Claim 19 adds a further limitation to claim 18 by claiming that the virus scanning is carried out by signature scanning process. Claim 19 is rendered obvious by the combination of Cheswick and Bellovin with Sidewinder in view of MpScan.

The aspect signature scanning is suggested by MpScan and renders every limitation of claim 19 obvious in combination with Cheswick and Bellovin and/or Sidewinder. *See e.g.,* MpScan pg. 2 ("Performs pattern matching of outgoing email for words, phrases or any other defined data delivery.")

So, a person having ordinary skill in the art can easily use the teachings of Cheswick and Bellovin in combination with the teachings of Sidewinder and further in view of MpScan to come up with a computer implemented method of virus detection at the server wherein the scanning for virus is done via signature analysis.

None of Cheswick and Bellovin, Sidewinder and MpScan were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspect of scanning the data for the presence of the viruses wherein the scanning for virus is done via

signature analysis. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 19 as pointed out above.

### MM. Whether claim 20 is obvious in view of the LANProtect reference and the MIMEsweeper reference

The teaching related to the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name as contained in the references presented below was not present during the prior examination of the '600 patent. A reasonable examiner would consider this teaching important in determining whether claim 20 is patentable. For this reason, the teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 20 of the '600 patent.

#### I. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious claim 20 under § 103(a)**

**Claim20: "The apparatus of claim 18, wherein**

**(1) … the means for performing a preset action comprises:"**

Claim 20 recites "The apparatus of claim 18, wherein the means for performing a preset action comprises:"

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

**(2) "…means for transmitting the data unchanged;"**

Claim 20 further recites "means for transmitting the data unchanged;"

In LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone or moving the virus infected file to a special directory. *See e.g.,* LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus

content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.,* LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory.").

**(3) "...means for transmitting the data unchanged;'**

Claim 20 further recites "means for transmitting the data unchanged;"

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

**(4) "...means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name."**

Claim 20 further recites "means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name."

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

**II. The MIMEsweeper Reference**

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses.

**MIMEsweeper makes obvious claim 20 under § 103(a)**

**Claim 20: "The apparatus of claim 18, wherein**

**(1) … the means for performing a preset action comprises:"**

Claim 20 recites "The apparatus of claim 18, wherein the means for performing a preset action comprises:"

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper further discloses the steps of performing a preset action on the messages/data according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**(2) "…means for transmitting the data unchanged;"**

Claim 20 further recites "means for transmitting the data unchanged;"

MIMEsweeper discloses the transfer of the data/ mail messages unchanged depending on the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages,

(iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

**(3) "…means for not transmitting the data; and"**

Claim 20 further recites "means for not transmitting the data."

MIMEsweeper discloses the aspect of not transferring the infected mail message/ data depending on the return codes from the Virus checking packages called 'Validators'. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**(4) "…means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name."**

Claim 20 further recites "means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name."

MIMEsweeper discloses the storage of the corrupt mail messages or the data in removable area depending on the return codes from the Virus checking packages called 'Validators'. The reference discloses that the actions which can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii)

copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

(iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

**NN. Whether claim 20 is obvious in view of the LANProtect reference, the MIMEsweeper reference, the Sidewinder reference, the TIS Firewall reference, the Layland reference and the SunScreen SPF-100 reference**

None of LANProtect, MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the

new file name raise a substantial new question of patentability with respect to claim 20 as pointed out in more detail below.

**Claim 20** recites "The apparatus of claim 18, wherein the means for performing a preset action comprises:

- means for transmitting the data unchanged;
- means for not transmitting the data; and
- means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name.

**I. LANProtect in view of Sidewinder and/or TIS Firewall and/or Layland and/or SunScreen SPF-100 renders obvious Claim 20 Under § 103(a):**

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

SunScreen SPF-100 was developed in 1995 to provide broader, more robust and more flexible network security. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 was also designed to provide administrators with the necessary tools to flexibly and intuitively manage their gateway access to public networks. Employing a dedicated administration station, the SunScreen SPF-100 system ensures absolute administration privacy and easy to-use rule-based controls to ensure that internal corporate networks and intercompany communications are safeguarded.

LANProtect discloses performing preset actions based on the content of the message, including the presence of a virus. According to LANProtect, when a virus infected message is detected, preset actions are taken, such as renaming the file, deleting the file, leaving the file alone, or moving the virus infected file to a special directory. *See e.g.*, LANProtect at pg. 5 ("LANProtect now contains

a special rules-oriented analyzer that can detect the mutation engine as it enters the system, decrypt it, examines its virus content, notify the system administrator, and quarantine or wipe out the file containing it."). *See e.g.*, LANProtect at pg. 15 ("Actions on virus detection determine how viruses will be handled upon detection. Once a virus is detected on the server, you may determine the action to take. You may rename, delete, leave alone, or move the virus to a special directory."). See e.g., LANProtect at pg. 11 ("When an infected file is found, LANProtect places information about the file and the virus in a log file and then acts on the in the infected file. The action taken on an infected file is determined when you configure the scans.").

LANProtect further discloses the aspect of renaming the infected files with new name and storing them and informing the system administrator when virus is found. *See e.g.,* LANProtect at pg. 28 ("This level of security relates to a more relaxed detection and remedial environment. The following is a list of the configurations and options selected for moderate security: Scan selected files intermittently with the manual server and prescheduled Server scans, Scan only incoming files with the real time scan, Rename infected files, Generate report and send it to printer, Notify only system administrator when a virus is found."). See also LANProtect at pg. 2-4 ("The infected file directory defaults to a subdirectory called VIRUS under the directory where LANProtect was installed. When viruses are detected, all of the scans that are configured to move infected files upon virus detection will use this directory to quarantine infected files. The infected file retains its original file name in the virus directory. If an infected file has the same name as a file existing in the virus directory, LANProtect renames the newly infected file with the .VIR extension and immediately renames any subsequent file name extensions (.V01, .V02 etc.) LANProtect also keeps track of the infected files original path in VIRUS.ID file.").

However if the aspect of "the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name" was somehow construed so that LANProtect did not practice this aspect, the following references combined with LANProtect would render claim 20 obvious.

This element is disclosed or suggested by a set of prior art including the Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). The Sidewinder reference clearly teaches the storage of the rejected messages

for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "SMTP `. *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its destination. *See e.g.,* TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. Layland suggests an Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a

log detailing any incidence of corrupted files and also the sources of those files. *See e.g.,* Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

Furthermore, SunScreen SPF-100 discloses some of the aspects of claim 20. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

So, a person having ordinary skill in the art can easily use the teachings of the LANProtect in combination with the teachings of Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 to come up an apparatus as disclosed in claim 18 further being capable of performing a preset action

comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name.

None of LANProtect, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 20 as pointed out above.

## II. MIMEsweeper in view of Sidewinder and/or TIS Firewall and/or the Layland and/or SunScreen SPF-100 renders obvious Claim 20 Under § 103(a):

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that

protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses.

SunScreen SPF-100 was developed in 1995 to provide broader, more robust and more flexible network security. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 was also designed to provide administrators with the necessary tools to flexibly and intuitively manage their gateway access to public networks. Employing a dedicated administration station, the SunScreen SPF-100 system ensures absolute administration privacy and easy to-use rule-based controls to ensure that internal corporate networks and intercompany communications are safeguarded.

MIMEsweeper scans the incoming email attachments for the presence of computer viruses. The architecture involved incorporates a message store for storing the messages temporarily. The MIMEsweeper operates while transferring the data between the message stores. *See e.g.,* MIMEsweeper at pg. 10 ("MIMEsweeper as mail transfer agent"). The MIMEsweeper firstly reads a waiting message from the database, analyzes its contents, and then depending on the analysis, it submits the message for onward transmission or diverts it according to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10.

MIMEsweeper further discloses the steps of performing a preset action on the messages or the data according to the return codes from the Virus checking packages called 'Validators'. Actions taken can be to quarantine the message and send full logs from virus checking packages to the E-mail administrator. The further possible actions that can be taken on the quarantined messages include: (i) release of the messages for forwarding to their intended destination, (ii) deletion of messages, (iii) copying of quarantined messages to removable area, (iv) archiving of MIMEsweeper log files to removable media. *See e.g.,* MIMEsweeper at pg. 9.

MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

MIMEsweeper further discloses the copying of the corrupt mail messages/data to removable area depending on the return codes from the Virus checking packages called 'Validators' and in addition archiving log files to the removable media which contain the output of the determining step. *See e.g.,* MIMEsweeper at pg. 9.

However if the aspect of "the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name" was somehow construed so that MIMEsweeper did not practice this aspect, the following references combined with MIMEsweeper would render claim 20 obvious.

This element is disclosed or suggested by a set of prior art including the Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses an application level secure gateway between TCP/IP networks which guards the connection to the Internet. Sidewinder discloses filtering of data (e.g., mail messages) that cross the network boundary in either direction. In Sidewinder the messages which fail to pass the filter are forwarded to the System Administrator for action. *See e.g.,* Sidewinder at SR-454.9 ("The Mail Service provides the following capabilities to users: The ability to screen mail and assign priorities to incoming messages, the ability to send and receive mail via the Internet in a controlled fashion, the user interface is graphical, with "point and click" and "drag and drop" logic used throughout."). The Sidewinder reference clearly teaches the storage of the rejected messages for later reviewing. *See e.g.,* Sidewinder at SR-454.9 ("Rejected messages may be discarded or kept in a "trash" folder for later examination.").

In addition TIS Firewall discloses the TIS Firewall Toolkit including an SMTP proxy server called "smap" which stands for "SMTP `. *See e.g.,* TIS Firewall at 8, ("SMTP is implemented using a pair of software tools called smap and smapd. Generally, SMTP mail poses a threat to the system, since mailers run with systems-level permissions in order to deliver mail to users' mailboxes. Smap and smapd address this concern by isolating the mailer so that it runs in a restricted directory via chroot, as an unprivileged user.")

TIS Firewall accepts all the incoming messages and writes them to disk in a 'spool area' and then scans the spool area and delivers the messages to the real send mail for the delivery to its destination. *See e.g.,* TIS Firewall at 5 ("To help secure mail service direct network access to send mail is prevented. A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap, is small enough to be subjected to a code review for correctness (unlike sendmail) and simply accepts all incoming messages and writes them to disk in a spool area. Rather than running with permissions, the proxy

runs with a restricted set of permissions and runs "chrooted" to the spool area. A second process is responsible for scanning the spool area and delivering the mail messages to the real send mail for delivery - a mode of operation in which send mail can operate with reduced permission."

Layland discloses the steps of performing a preset action on the data. Layland suggests an Internet gateway should subject all the incoming files to a virus scan. Layland further discloses the user has the option of either accepting the delivery of a particular message or rejecting it or blocking any particular source by telling the gateway not to forward any messages from that source. The Internet gateway disclosed in Layland immediately discards any suspected file and maintains a log detailing any incidence of corrupted files and also the sources of those files. *See e.g.,* Layland at pg. 24 ("The internet gateway would subject all the incoming files to a virus scan, with any suspect file immediately discarded. The gateway also would keep a log detailing any incidence of corrupted files, and the sources of those files.") *See also* Layland at pg. 24 ("at that point, user could (a) accept delivery of that particular message, (b) reject delivery or (c) reject delivery and tell the gateway not to forward any messages from that source.")

Furthermore, SunScreen SPF-100 discloses some of the aspects of claim 20. SunScreen SPF-100 was designed to deliver firewall protection and virtual private network support across public networks. SunScreen SPF-100 teaches the aspect of storing the information of the packets. *See e.g.,* SunScreen SPF-100 at pg. 11 ("A significant drawback of many packet screens is the inability to retain detailed information (known as context or state information) about packets that have passed through. If information can be recorded and maintained about the packets, such as where the packets came from, where they were going, and what they were doing, more powerful and secure screening can be performed."). SunScreen SPF-100 also indicates the preset actions that can be taken after screening the traffic coming into and leaving the trusted network. The actions

that can be taken include pass, reject or reject with notification to the sender. *See e.g.,* SunScreen SPF-100 at pg. 20 ("The SunScreen packet screening engine screens traffic coming into and leaving the trusted network. It can extract and examine any portion of the packets, allowing for powerful rules and decision making. Actions that may be taken on packets include pass, reject, reject with a notification to the sender, encrypt, decrypt, alert, and log.")

So, a person having ordinary skill in the art can easily use the teachings of the MIMEsweeper in combination with the teachings of Sidewinder , TIS Firewall, Layland and SunScreen SPF-100 to come up with an apparatus as disclosed in claim 18 further being capable of performing a preset action comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name.

None of MIMEsweeper, Sidewinder, TIS Firewall, Layland and SunScreen SPF-100 were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the step of performing a preset action as disclosed in claim 18 comprising of either transmitting the data unchanged, or not transmitting the data, or means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is

requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 20 as pointed out above.

### OO. Whether claim 21 is obvious in view of the TFS Manual reference and the LANProtect reference

Claim 21 further adds the limitation to claim 18 of the subject patent that the apparatus is further capable of performing the steps for determining whether the data is of a type that is likely to contain a virus and capable of transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus. The steps of claim 21 are made obvious in view of one or more references as discussed below:

#### I. The TFS Manual Reference

The TFS Manual reference was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network.

**TFS Manual makes obvious Claim 21 Under § 103(a)**

**Claim 21: "The apparatus of claim 18 further comprising:"**

**(1) "...a second means for determining whether the data is of a type that is likely to contain a virus; and"**

Claim 21 further recites "a second means for determining whether the data is of a type that is likely to contain a virus."

TFS Manual discloses this claim element. As discussed in TFS Manual, the TFS Gateway would not scan the inline part of the message or text-only attachments because there was no risk

that text files would create any damage. Additionally, the TFS Gateway could be used with commercially available antivirus scanners at the time, such as McAfee's VirusScan, Dr Solomon's and IBM Antivirus, which would only scan files likely to contain a virus. See TFS Manual at 77. These antivirus scanners could also compare the extension type of the file to be scanned with extension types known to be able to contain a virus.

**(2) "…means for transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus."**

Claim 21 further recites "means for transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus."

TFS Manual discloses this claim element. If a mail message does not have any encoded portions, the TFS Gateway sends it to the destination address without first scanning it for viruses. Therefore it was not scanned and no preset action was taken. The mail message was simply forwarded to its destination. In addition, as discussed above, if the commercially available antivirus scanner determined a file was not of a type likely to contain a virus, that file would not be scanned, and the TFS Gateway would transmit the file to its destination.

TFS Manual was not considered during prosecution of the '600 patent. TFS Manual contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches "determining whether the data is of a type that is likely to

contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus.". As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raise a substantial new question of patentability with respect to claim 21 as pointed out above.

## II. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious Claim 21 Under § 103(a)**

**Claim 21: "The apparatus of claim 18; further comprising:"**

**(1) "…a second means for determining whether the data is of a type that is likely to contain a virus; and"**

Claim 21 further recites "a second means for determining whether the data is of a type that is likely to contain a virus."

LANProtect permits the program, user, or administrator to identify the types of files to be scanned for viruses (*e.g.*, DOS files with ".EXE" extension). *See, e.g.* LANProtect at pg. 6 ("The

LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).")

**(2) "...means for transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus."**

Claim 21 further recites "means for transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus."

LANProtect discloses that this step is performed by the LANProtect product. When LANProtect is configured to scan only those file types likely to contain a virus, they do not scan at all other file types or take any of the preset actions.

LANProtect was not considered during prosecution of the '600 patent. LANProtect contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent suggests or teaches "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus." As such, the substantial new question of patentability (SNQ) presented herein meets the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that

resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the reference presented herewith, raise a substantial new question of patentability with respect to claim 21 as pointed out above.

**PP. Whether claim 21 is obvious in view of the TFS Manual reference, the LANProtect reference and the Sidewinder reference**

None of TFS Manual, LANProtect and Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As shown above, no prior art that suggests or teaches "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus." was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith raise a substantial new question of patentability with respect to claim 21 as pointed out in more detail below.

**Claim 21** recites "The apparatus of claim 18; further comprising:"

- a second means for determining whether the data is of a type that is likely to contain a virus; and
- means for transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus.

**I. TFS Manual in view of Sidewinder renders obvious Claim 21 Under § 103(a).**

The TFS Manual reference was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different network.

TFS Manual indicates that the TFS Gateway would not scan the inline part of the message or text-only attachments because there was no risk that text files would create any damage. Additionally, the TFS Gateway could be used with commercially available antivirus scanners at the time, such as McAfee's VirusScan, Dr Solomon's and IBM Antivirus, which would only scan files likely to contain a virus. See TFS Manual at 77. These antivirus scanners could also compare the extension type of the file to be scanned with extension types known to be able to contain a virus.

In addition, TFS Manual discloses if a mail message does not have any encoded portions, the TFS Gateway sends it to the destination address without first scanning it for viruses. Therefore it was not scanned and no preset action was taken. The mail message was simply forwarded to its destination. In addition, as discussed above, if the commercially available antivirus scanner determined a file was not of a type likely to contain a virus, that file would not be scanned, and the TFS Gateway would transmit the file to its destination.

However the aspect of "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a

type that is likely to contain a virus." was somehow construed so that TFS Manual did not practice this aspect, the following references combined with TFS Manual would render claim 21 obvious.

This element is disclosed or suggested by Sidewinder as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses the element of determining whether the data is of a type that is likely to contain virus. See Sidewinder at SR-454.10 ("Sidewinder can detect and block messages that are not English language text and that therefore could contain viruses"). Sidewinder also discloses the element of transmitting the data without performing the determination step. See Sidewinder at SR-454.4 (indicating certain classes of data can be selectively prohibited from passing to and from the external network).

So, a person having ordinary skill in the art can easily use the teachings of the TFS Manual reference in combination with the teachings of the Sidewinder reference to come up with an apparatus capable of virus detection at the server wherein the virus detection is selectively done by determining whether the data is of type that is likely to contain virus and transmitting the data if the data is not of type that is likely to contain virus.

Neither TFS Manual nor Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects of determination whether the file is of type that is likely to contain virus, transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 21 as pointed out above.

## II. LANProtect in view of Sidewinder renders obvious Claim 21 Under § 103(a).

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

LANProtect permits the program, user, or administrator to identify the types of files to be scanned for viruses (*e.g.*, DOS files with ".EXE" extension). *See, e.g.* LANProtect at pg. 6 ("The LProtect NLM scans the following types of files: DOS (all files that originate on any computer capable of handling DOS files, specified as 'all' or by specific file extension).")

LANProtect discloses that this step is performed by the LANProtect product. When LANProtect is configured to scan only those file types likely to contain a virus, they do not scan at all other file types or take any of the preset actions.

However the aspect of "determining whether the data is of a type that is likely to contain a virus" and "transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus." was somehow construed so that LANProtect did not practice this aspect, the following references combined with the LANProtect reference would render claim 21 obvious.

This element is disclosed or suggested by Sidewinder as discussed below. A *prima facie* case of obviousness is established if there is a motivation to combine two or more references and the references together teach or suggest all of the claim limitations MPEP § 2143. Motivation to combine need not be provided on the face of the references themselves. "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41 (2007); *see also* MPEP § 2143.01.

Sidewinder discloses the element of determining whether the data is of a type that is likely to contain virus. See Sidewinder at SR-454.10 ("Sidewinder can detect and block messages that are not English language text and that therefore could contain viruses"). Sidewinder also discloses the element of transmitting the data without performing the determination step. See Sidewinder at SR-

454.4 (indicating certain classes of data can be selectively prohibited from passing to and from the external network).

So, a person having ordinary skill in the art can easily use the teachings of the LANProtect reference in combination with the teachings of the Sidewinder reference to come up with an apparatus capable of virus detection at the server wherein the virus detection is selectively done by determining whether the data is of type that is likely to contain virus and transmitting the data if the data is not of type that is likely to contain virus.

Neither LANProtect nor Sidewinder were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the aspects of determination whether the file is of type that is likely to contain virus, transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 21 as pointed out above.

**QQ. Whether claim 22 is obvious in view of the TFS Manual reference, the LANProtect reference, the MIMEsweeper reference and the Cheswick and Bellovin reference**

Claim 22 further adds the limitation to claim 18 of the subject patent that the apparatus further comprises of means for comparison of the destination address to valid addresses for the first network. The teachings contained in the references presented below raise a substantial new question of patentability with respect to claim 22 of the '600 patent. The steps of claim 22 are obvious in view of one or more references as discussed below:

## I. The TFS Manual Reference

The TFS Manual reference was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different networks.

**TFS Manual makes obvious claim 22 under § 103(a)**

**Claim22: "means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network."**

Claim 22 recites "The apparatus of claim 18, further comprising means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network"

TFS Manual discloses a gateway that receives mail message requests using SMTP, and other protocols. *See e.g.,* TFS Manual, Chapter on "Receiving Mail from Internet Mail" (TFS "will send any outgoing messages and receive any incoming messages.");

## II. The LANProtect Reference

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

**LANProtect makes obvious claim 22 under § 103(a)**

**Claim22: "means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network."**

Claim 22 recites "The apparatus of claim 18, further comprising means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network."

LANProtect inherently discloses receiving a data transfer request including a destination address. LANProtect software runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. The aspect of data transfer request including a destination address is an inherent and fundamental aspect of data transfer utilizing a server and hence would be obvious to a person skilled in the art.

## III. The MIMEsweeper Reference

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses.

**MIMEsweeper makes obvious claim 22 under § 103(a)**

**Claim 22: "means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network"**

Claim 22 recites "The apparatus of claim 18, further comprising means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network."

MIMEsweeper receives a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination. Since SMTP server involved receives requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

The MIMEsweeper examines the messages and based upon the results of the analysis, submit the message for onward transmission, or divert it to a quarantine policy. *See e.g.,* MIMEsweeper at pg. 10 ("Unlike a standard transfer agent, MIMEsweeper examines the messages that it moves, and may redirect or modify them based upon the result of the examination.").

## IV. The Cheswick and Bellovin Reference

The Cheswick and Bellovin reference was not considered during prosecution of the '600 patent. It was published in 1994 and discusses proper use of firewalls to significantly increase security on networked computers.

**Cheswick and Bellovin makes obvious claim 22 under § 103(a)**

**Claim 22: "means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network"**

Claim 22 recites "The apparatus of claim 18, further comprising means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network."

Cheswick and Bellovin describes a system that receives data transfer requests with a destination address at a server. See e.g., Cheswick and Bellovin at pg. 66-69 and 74-75.

**RR. Whether claim 22 is obvious in view of the TFS Manual reference, the LANProtect reference, the MIMEsweeper reference, the Cheswick and Bellovin reference, the MpScan reference and the TIS Firewall reference**

None of TFS Manual, LANProtect, MIMEsweeper, Cheswick and Bellovin, MpScan and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching or suggestion specifically not present during the prosecution of the '600 patent. As shown above, no prior art concerning the virus scanning apparatus further comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network was considered during prosecution of the '600 patent.

As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which

reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, which include materials describing the virus scanning apparatus comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first raise a substantial new question of patentability with respect to claim 12 as pointed out in more detail below.

**Claim 22** recites "The apparatus of claim 18, further comprising means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network."

In total, Claim 22 adds to claim 18 that the apparatus disclosed is further capable of determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first.

### I. TFS Manual in view of MpScan or TIS Firewall renders obvious Claim 22 Under § 103(a):

The TFS Manual reference was not considered during the prosecution of the '600 patent. It was published in 1995, to discuss the data transfer across different networks.

TFS Manual discloses a gateway that receives mail message requests using SMTP, and other protocols. *See e.g.,* TFS Manual, Chapter on "Receiving Mail from Internet Mail" (TFS "will send any outgoing messages and receive any incoming messages.");

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail

transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized.

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

So, a person having ordinary skill in the art can easily use the teachings of the TFS Manual in combination with the teachings of MpScan or TIS Firewall to come up with the virus scanning apparatus as disclosed in claim 18 further comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network.

None of TFS Manual, MpScan and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the virus scanning apparatus as disclosed in claim 18 further comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be

demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 22 as pointed out above.

## II. LANProtect in view of MpScan or TIS Firewall renders obvious Claim 22 Under § 103(a):

The LANProtect reference was not considered during the prosecution of the '600 patent. It was published in 1992 and discloses server-based virus protection software that provides total LAN protection.

LANProtect teaches receiving a data transfer request including a destination address. As LANProtect runs on servers servicing clients on a LAN, when it receives requests for transferring data to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the data file.

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized.

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would

be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

So, a person having ordinary skill in the art can easily use the teachings of the LANProtect in combination with the teachings of MpScan or TIS Firewall to come up with the virus scanning apparatus as disclosed in claim 18 further comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network.

None of LANProtect, MpScan and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the virus scanning apparatus as disclosed in claim 18 further comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the

patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 22 as pointed out above.

### III. MIMEsweeper in view of MpScan or TIS Firewall renders obvious Claim 22 Under § 103(a):

The MIMEsweeper reference was not considered during the prosecution of the '600 patent. It was published in September 1995 and documents a mail filtering product for email gateways that protects networks from virus infection via email. MIMEsweeper was conceived out of a requirement to scan incoming emails and their attachments for computer viruses.

MIMEsweeper receives a data transfer request including a destination address. In SMTP versions of MIMEsweeper, the forwarders are built into MIMEsweeper functionality. Once the MIMEsweeper has analyzed the messages, the cleared messages are routed to their destination. Since SMTP server involved receives requests for transferring Email messages to a given client, the request must include the destination address of the client seeking to have the data sent to it. Otherwise, the server will have no way of knowing to which client to send the email after analyzing it. *See e.g.,* MIMEsweeper at pg. 13 ("The client-server architecture of SMTP mail means that a fully functional SMTP server is required to handle the receipt of Email items from the Internet, and their delivery to local or remote users after MIMEsweeper checking. The SMTP server must also store messages, on receipt, in a form and location suitable for MIMEsweeper to read and analyze, and then collect cleared messages for onward delivery.").

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized.

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41) ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

So, a person having ordinary skill in the art can easily use the teachings of MIMEsweeper in combination with the teachings of MpScan or TIS Firewall to come up with the virus scanning apparatus as disclosed in claim 18 further comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network.

None of MIMEsweeper, MpScan and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the virus scanning apparatus as disclosed in claim 18 further comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on

the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 22 as pointed out above.

## IV. Cheswick and Bellovin in view of MpScan or TIS Firewall renders obvious Claim 22 Under § 103(a):

The Cheswick and Bellovin reference was not considered during the prosecution of the '600 patent. It was published in 1994, to discuss a new paradigm in firewall and Internet security.

Cheswick and Bellovin describes a system that receives data transfer requests with a destination address at a server. See e.g., Cheswick and Bellovin at pg. 66-69 and 74-75.

MpScan discloses an e-mail content scanning firewall. It describes the aspect of receiving a mail message request including a destination address and uuencoded, compressed or "other" formats. MpScan describes performing pattern matching on the outgoing e-mail and blocks the e-mail transmissions if they contain company classified material and/ or are transmitted to and from competitor's addresses, except as authorized.

TIS Firewall discloses a proxy server which receives data transfer requests via TCP/IP which include destination addresses. Herein, data transfer being electronic is inherent and would be obvious to any person skilled in the art. *See e.g.*, TIS Firewall at pg. 8-9 (smap receives mail messages); TIS Firewall at pg. 41 ("A simple program that implements a skeleton of the SMTP protocol is presented on the SMTP port on the mail server. This SMTP proxy, called smap,...simply accepts all incoming messages and writes them to disk in a spool area."); TIS Firewall at pg. 41 ("The FTP application gateway is a single process that mediates FTP connections between two networks.").

So, a person having ordinary skill in the art can easily use the teachings of Cheswick and Bellovin in combination with the teachings of MpScan or TIS Firewall to come up with a virus scanning apparatus as recited by claim 18 further comprising a means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network.

None of Cheswick and Bellovin, MpScan and TIS Firewall were considered during prosecution of the '600 patent. Each of these prior art publications contains a new, non-cumulative technological teaching specifically not present during the prosecution of the '600 patent. As described herein, no prior art considered during prosecution of the '600 patent concerns the virus scanning apparatus as disclosed in claim 18 further comprising of means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network. As such, the substantial new questions of patentability (SNQs) presented herein meet the legal standard for ordering *ex parte* re-examination as set forth in MPEP §2216 ("It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.") And, as a result, the references presented herewith, raise a substantial new question of patentability with respect to claim 22 as pointed out above.

## VII. LIST OF EXHIBITS

**Exhibit A** U.S. Patent No. 5,623,600 – Issued April 22, 1997 ("the '600 patent").

**Exhibit B1** *Fortinet, Inc. v. Trend Micro Incorporated et al.*, Civil Action No. 10-048 (N.D. Cal.)

**Exhibit B2** *Trend Micro Incorporated. v. Fortinet, Inc.*, Civil Case No. 1-09-CV-149262 (Santa Clara Sup. Ct., Cal.)

**Exhibit C** "The Design of a Secure Internet Gateway", by Bill Cheswick, USENIX Summer Conference June 11-15, 1990 ("Cheswick") — Not previously considered during examination.

**Exhibit D** "Firewalls and Internet Security – Repelling the Wily Hacker", by William R. Cheswick and Steven M. Bellovin, Copyright 1994 ("Cheswick and Bellovin") — Not previously considered during examination.

**Exhibit E** "A Gateway to Internet Health and Happiness", by Robin Layland, published September 21,1994 in Data Communications, Internetworking Views ("Layland") — Not previously considered during examination.

**Exhibit F** Intel LANProtect Product Documentation (together, Intel LANProtect Product Overview and Intel LANProtect Software Users Guide), copyright 1992, by Intel Corporation ("LANProtect") — Not previously considered during examination.

**Exhibit G** "SPECIAL REPORT: Secure Computing Corporation And Network Security", published December 1994, the LOCALNetter Newsletter, vol. 14, No. 12 ("Sidewinder") — Not previously considered during examination.

**Exhibit H** "TIS Firewall Toolkit Overview", published June 30, 1994, by Trusted Information Systems, Inc. and USENIX Association, Proceedings of the Summer 1994 USENIX Conference, June 6-10, 1994 (collectively, "TIS Firewall") — Not previously considered during examination.

**Exhibit I** U.S. Patent No. 5,319,776, issued to Hile *et al.*, filed in September 1992 and issued June 1994 ("Hile") — Previously considered during examination.

**Exhibit J** "TFS gateway," by TenFour Sweden AB ("TFS Manual") — Not previously considered during examination.

**Exhibit K** "MIMEsweeper administrator guide" ("MIMEsweeper")-published by Integralis Ltd Copyright 1995. — Not previously considered during examination.

**Exhibit L** "MpScan-Email Security" ("MpScan") — Published by Cybersoft- Not previously considered during examination.

**Exhibit M** "Network security SunScreen SPF 100" ("SunScreen SPF-100") - Not previously considered during examination.

**Exhibit N** "An Introduction to the Norman Firewall: The secure way to connect to the Internet and other TCP/IP-based networks" ("Norman Firewall") - published by Norman Data Defense, Inc. Copyright November 1995.

**Exhibit O** Robert McMillan, "Trend Micro: Barracuda Suit Not About Open Source," PC World, PCW Business Center, June 13, 2008 ("McMillan").

**Exhibit P** Steve Chang and Jenny Chang, "Trend Micro: History of the Global No. 1 Internet Security Company," Trend Micro, Copyright 2002 ("Trend Micro History").

## VIII. CONCLUSION

For at least the reasons set forth above, it is clear that a new question of patentability is raised in connection with claims 1-22 (all of the claims) of the '600 patent by this Request for *Ex Parte* Reexamination because claims 1-22 are rendered obvious in view of the previously uncited prior art. Therefore, it is requested that reexamination be granted and all claims 1-22 be finally rejected.

As identified in the attached Certificate of Service, and in accordance with 37 C.F.R. §1.510(b)(5), a duplicate copy of this Request, in its entirety, is being supplied to the Office on CD-ROM as service on the patentee via the address of the attorney or agent of record is believed to be futile in view of the fact that the Skjerven Morrill law firm dissolved on or about March 1, 2003.

Please direct all correspondence to the undersigned.

Respectfully submitted,
Hamilton, DeSanctis & Cha LLP

Date: June 1, 2010

By /Michael A. DeSanctis/
Michael A. DeSanctis, Esq.
Reg. No. 39,957
Customer No. 064128
Ph: (303) 856-7155