UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/011,022	07/21/2010	5623600	032468.0004-US01	3498

26853 7590 05/19/2011

COVINGTON & BURLING, LLP
ATTN: PATENT DOCKETING
1201 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20004-2401

EXAMINER	
ART UNIT	PAPER NUMBER

DATE MAILED: 05/19/2011

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Michael A. DeSanctis
Hamilton DeSantis & Cha LLP
225 Union Blvd, Suite 150
Lakewood, CO 80228

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. 90/011,022.

PATENT NO. 5623600.

ART UNIT 3992.

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Office Action in Ex Parte Reexamination	**Control No.** 90/011,022	**Patent Under Reexamination** 5623600
	Examiner MINH DIEU NGUYEN	**Art Unit** 3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

a☒ Responsive to the communication(s) filed on *04 March 2011* . b☒ This action is made FINAL.
c☒ A statement under 37 CFR 1.530 has not been received from the patent owner.

A shortened statutory period for response to this action is set to expire ___month(s) from the mailing date of this letter.
Failure to respond within the period for response will result in termination of the proceeding and issuance of an *ex parte* reexamination certificate in accordance with this action. 37 CFR 1.550(d). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).**
If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☒ Notice of References Cited by Examiner, PTO-892.
2. ☒ Information Disclosure Statement, PTO/SB/08.
3. ☐ Interview Summary, PTO-474.
4. ☐ ___.

Part II SUMMARY OF ACTION

1a. ☒ Claims *1-37* are subject to reexamination.

1b. ☐ Claims ___are not subject to reexamination.

2. ☐ Claims ___have been canceled in the present reexamination proceeding.

3. ☒ Claims *10 and 13* are patentable and/or confirmed.

4. ☒ Claims *1-9, 11-12, 14-37* are rejected.

5. ☐ Claims ___are objected to.

6. ☐ The drawings, filed on ___are acceptable.

7. ☐ The proposed drawing correction, filed on ___has been (7a) ☐ approved (7b)☐ disapproved.

8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All b)☐ Some* c)☐ None of the certified copies have

   1☐ been received.

   2☐ not been received.

   3☐ been filed in Application No. ___.

   4☐ been filed in reexamination Control No. ___.

   5☐ been received by the International Bureau in PCT application No. ___.

   * See the attached detailed Office action for a list of the certified copies not received.

9. ☐ Since the proceeding appears to be in condition for issuance of an *ex parte* reexamination certificate except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte* Quayle, 1935 C.D. 11, 453 O.G. 213.

10. ☐ Other: _____

cc: Requester (if third party requester)

DETAILED ACTION

This final office action on the merit is in response to the Patent Owner's amendment and response filed 3/4/2011. The amendment, introduced 15 new claims, 8 of which claims 23-24, 27-28, 31, 34 and 35-36 were new independent claims, for total of 37 claims, (13 independent claims). The amendment also presented various arguments. The Amendment has been duly considered. Claims 10, 13 are patentable, claims 1-9, 11-12, 14-22 are not deemed persuasive to overcome the prior rejections. See the "Response to Arguments" section for additional details. Thus, the rejections, set for the in the non-final office action, mailed 1/6/2011, is repeated below. Accordingly, this office action is made final. See MPEP 706.07 and 2271.

I. Procedures Governing Reexamination

THIS ACTION IS MADE FINAL.

A shortened statutory period for response to this action is set to expire 2 months from the mailing date of this action.

Extensions of Time

Extensions of time under 37 CFR 1.136(a) do not apply in reexamination proceedings. The provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Further, in 35 U.S.C. 305 and in 37 CFR

1.550(a), it is required that reexamination proceedings "will be conducted with special dispatch within the Office".

Extensions of time in reexamination proceedings are provided for in 37 CFR 1.550(c). A request for extension of time must be filed on or before the day on which a response to this action is due, and it must be accompanied by the petition fee set forth in 37 CFR 1.17(g). The mere filing of a request will not effect any extension of time. An extension of time will be granted only for sufficient cause, and for a reasonable time specified.

The filing of a timely first response to this final rejection will be construed as including a request to extend the shortened statutory period for an additional month, which will be granted even if previous extensions have been granted. In no event, however, will the statutory period for response expire later than SIX MONTHS from the mailing date of the final action. See MPEP § 2265.

Proposed Amendments, Affidavits, or Declarations

Patent owner is notified that any proposed amendment to the specification and/or claims in this reexamination proceeding must comply with 37 CFR 1.530(d)-(j), must be formally presented pursuant to 37 CFR 1.52(a) and (b), and must contain any fees required by 37 CFR 1.20(c).

Submissions

Submissions after the final Office action on the merits will be governed by the requirements of 37 CFR 1.116, after final rejection and by 37 CFR 41.33 after appeal, which will be strictly enforced. Any amendment after a Final Action must include "a showing of good and sufficient reasons why the amendment is necessary and was not earlier presented" in order to be considered. See MPEP § 2260.

Concurrent Litigation

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the patent at issue in this reexamination proceeding throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

II. Grounds of Rejection

Claim Rejection – 35 U.S.C § 305

The following is a quotation of the first and second paragraphs of 35 U.S.C. 305:

> After the times for filing the statement and reply provided for by section 304 of this title have expired, reexamination will be conducted according to the procedures established for initial examination under the provisions of sections 132 and 133 of this title. In any reexamination proceeding under this chapter, the patent owner will be permitted to propose any amendment to his patent and a new Claim or claims thereto, in order to distinguish the invention as claimed from the prior art cited under the provisions of section 301 of this title, or in response to a decision adverse to the patentability of a claim of a patent. No proposed amended or new claim enlarging the scope of a claim of the patent will be permitted in a reexamination proceeding under this chapter. All reexamination proceedings under this section, including any appeal to the Board of Patent Appeals and Interferences, will be conducted with special dispatch within the Office.

Claims 24-26, 28-30, 31-33 and 34 are rejected under 35 U.S.C. 305 as enlarging the scope of the claims of the patent being reexamined. In 35 U.S.C. 305, it is stated that "[n]o proposed amended or new claim enlarging the scope of a claim of the patent will be permitted in a reexamination proceeding..." A claim presented in a reexamination "enlarges the scope" of the patent claims where the claim is broader than any claim of the patent. A claim is broader in scope than the original claims if it contains within its scope any conceivable product or process which would not have infringed the original patent. A claim is broadened if it is broader in any one respect, even though it may be narrower in other respects.

Claim 24 is broader than the original claim to which it is most similar, original claim 11, in that claim 24 recites performing one of i)..., ii)...and iii)...It is interpreted that any one of the steps i), ii) and iii) can be performed. As such, claim 24 does not recite "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 contain a virus".

Claims 25-26 depends from rejected claim 23 and includes all the limitations of that claim, thereby rendering that dependent claims as being of enlarged scope insofar as they depends on that claim.

Claim 28 is broader than the original claim to which it is most similar, original claim 11, in that claim 28 recites performing at least one of i)..., ii)...and iii)...It is interpreted that any one of the steps i), ii) and iii) can be performed. As such, claim 28 does not recite "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 contain a virus".

Claims 29-30 depends from rejected claim 28 and includes all the limitations of that claim, thereby rendering that dependent claims as being of enlarged scope insofar as they depends on that claim.

Claim 31 is broader than the original claim to which it is most similar, original claim 13, in that claim 31 recites performing at least one of i)..., ii)...and iii)...It is interpreted that any one of the steps i), ii) and iii) can be performed. As such, claim 31 does not recite "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 contain a virus".

Claims 32-33 depends from rejected claim 31 and includes all the limitations of that claim, thereby rendering that dependent claims as being of enlarged scope insofar as they depends on that claim.

Claim 34 is broader than the original claim to which it is most similar, original claim 13, in that claim 34 recites sending the mail message to the destination address if either the mail message does not contain a virus **or** the mail message does not contain any encoded portions. It is understood that the sending step is performed if either the message does not contain a virus **or** any encoded portions. As such, claim 34 does not recite "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 following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 18-20 and 22 are rejected under 35 U.S.C. 102(a) as being anticipated by **Norman Data Defense Systems, Inc., June 1995 (hereafter Norman)** (An Introduction to the Norman Firewall).

a) As to claim 18, Norman discloses an apparatus for detecting viruses in data transfers between a first computer and a second computer (Norman, page 4 – the firewall includes a fully configured secure computer system and virus detection capability), the apparatus comprising: means for receiving a data transfer request including a destination address (Norman, page 1 - With a proxy server between an internal network and external connections, "IP packets will not pass directly from the input to the output network interfaces", because "the proxy server runs two separate connections with the proxy as the carrier in between". Page 7, the firewall of Norman "uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly." Such a proxy server necessarily receives data transfer requests from internal network nodes. Page 8 - With respect to outgoing transfers, the firewall "log[s] into the workstation on the secure network to transfer the requested file". Page 5 - The firewall "can identify the packets' destination"); means for electronically receiving data at a server (Norman describes a firewall having a proxy server; server that receives incoming data. The proxy server stands "between the [internal] network and any external connections .... IP packets will not pass directly from the input to the output network interfaces in the proxy server environment." (Norman, p. 1.); means for determining whether the data contains a virus at the server (The firewall of Norman "uses a proxy server" (Norman, p. 1) which "automatically checks every incoming file for viruses before letting the file through" (Norman, p. 5); means for performing a preset action on the data using the server if the data contains a virus (The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman, p. 5). "When a virus is located [by the firewall], the file transaction is blocked and logged."(Norman, p. 9.) The firewall "can be made to notify a network management station on the internal net through SNMP traps. If a virus.., is discovered, traps can be sent to one or several machines on the secure network." (Norman, p.20); and means for sending the data to the destination address if the data does not contain a virus (Traffic that is due to be checked for viruses..[is] queued, and the [antivirus] module will then scan and give clearances for each file. When a file is cleared, it is then passed on by the proxy process." (Norman, p. 9.)

b) **As to claim 19**, Norman discloses wherein means for determining includes a means for scanning that scans the data using a signature scanning process (Norman, page 9, states that "[a]s new viruses are discovered and analyzed, their 'signatures' are included in the virus definition file (NVC.DEF)", a files that is updated regularly).

c) **As to claim 20**, Norman discloses wherein the means for performing a preset action comprises: means for transmitting the data unchanged (Transmitting data unchanged, even if it contains a virus, simply represents the ordinary operation of prior art network gateways which performed no antivirus scanning); means for not transmitting the data (The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman, p. 5). "When a virus is located [by the firewall], the file transaction is blocked and logged." (Norman, p. 9); 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.

d) **As to claim 22**, Norman discloses 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 (Norman teaches a firewall that "can identify the packets' destination" (Norman, p. 5). Moreover, conventional network security products "'read' the address information in packets and direct each to its intended destination" (Norman, p. 5). For example, a screening router applies rules that "rely on the origin and destination IP-addresses to decide if a packet is 'good' or 'bad' " (Norman, p. 3).

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3 are rejected under 35 U.S.C. 103(a) as being obvious over **Cheswick** (The Design of a Secure Internet Gateway) in view of **Cheswick and Bellovin (hereafter CB)** (Firewalls and Internet Security) and further in view of **TIS Firewall** (TIS Firewall Toolkit Overview).

a) **As to claim 1,** Cheswick discloses a system for detecting and selectively removing viruses in data transfers (Cheswick, page 233-234 - The New Gateway, named inet, is used so the internal machines are protected even if an invader breaks into the gateway machine, becomes root and creates and runs a new kernel), the system comprising: 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 (Cheswick, page 234 – The Inet gateway 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, page 235 – Inbound mail is delivered directly to Inet. Inet checks the destination. If it is a trusted machine (i.e. its smtp is trusted), a connection request is sent to r70 (a single internal machine that provides a limited set of services to Inet for reaching internal machines). If not, the mail is relayed through an accessible internal machine); a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output (Cheswick, page 234 – Cheswick discloses the design of a secure internet gateway for providing incoming login and mail service and outgoing mail, so a communications unit is inherently present in any system for transferring data); 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 (Cheswick, page 234 – the Inet uses a 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 communication process is inherent and obvious in the context of Cheswick).

Cheswick discloses inbound mail is delivered directly to Inet. Inet checks the destination. If it is a trusted machine (i.e. its smtp is trusted), a connection request is sent to r70 (a single internal machine that provides a limited set of services to Inet for reaching internal machines). If not, the mail is relayed through an accessible internal machine (page 235).

Cheswick does not explicitly disclose, however CB discloses 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 (CB discloses the use of firewalls to significantly increase security on network computers. Chapter 3, pages 51, 70, 75-76 – Packet filtering, circuit gateways, and application gateways are discussed. Commonly, more than one of these is used at the same time to log and control all incoming and outgoing traffic to scan for viruses).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having 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 in the system of Cheswick, as CB discloses, so as to increase security on network computers.

Cheswick and CB disclose a proxy server and a daemon (Cheswick, pages 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. CB, 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).

Cheswick and CB do not explicitly disclose, however TIS Firewall discloses 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, pages 3-4 – The toolkit software provides proxy services for common applications like FTP and TELNET, and security for SMTP mail, the toolkit software is configured to address "that which is not expressly permitted is denied);

and 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, page 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).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having 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 and 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 in the system of Cheswick and CB, as TIS Firewall discloses, so as to achieve all different levels of security from the basic to the most rigorous security configurations (TIS Firewall, page 1).

b) **As to claim 2,** the combination of Cheswick, CB and TIS Firewall discloses 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, page 10 - A proxy server for FTP).

c) **As to claim 3,** combination of Cheswick, CB and TIS Firewall discloses 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,.page 8 – SMTP service).

Claims 4 and 7 are rejected under 35 U.S.C. 103(a) as being obvious over **Cheswick and Bellovin (hereafter CB)** (Firewalls and Internet Security) and in view of **Sidewinder** (Special Report: Secure Computing Corporation and Network Security).

a) **As to claim 4,** CB discloses 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 (CB, pages 66-69, 74-75 – CB describes a system that receives data transfer requests with a destination address at a server); electronically receiving data at the server;

determining whether the data contains a virus at the server (CB, page 76 – a location with many PC users might wish to scan incoming files for viruses, Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules and filter placement; also, protocol specific filtering to detect viruses in data transfers); performing a preset action on the data using the server if the data contains a virus (CB, page 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).

CB does not explicitly disclose, however Sidewinder discloses certain types of data can be selectively prohibited from passing to and from the external network, by sending the data to the destination address if the data 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 (Sidewinder, pages SR-454.9, SR-454-10 – block all incoming and outgoing news which does not fit the statistical properties of English-language plaintext, filter incoming and outgoing news on the basis of content similarity to postings deemed to be in violation of the site's policy. Page SR-454.4 - certain classes of data may be prohibited from passing to and from the external network).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teaching of selectively transfer data based on the existence of viruses within such data by sending the data to the destination address if the data 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 in the system of CB, as Sidewinder teaches so as to avoid downstream virus infection.

b) **As to claim 7**, the combination of CB and Sidewinder discloses 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 (Sidewinder, SR-454.8 – SR-454-12 - 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).

Claims 5, 8, 11-12, 14 and 16-17 are rejected under 35 U.S.C. 103(a) as being obvious over **Cheswick and Bellovin (hereafter CB)** (Firewalls and Internet Security) in view of **Sidewinder** (Special Report: Secure Computing Corporation and Network Security) and further in view of **MIMEsweeper** (MIMEsweeper administrator guide).

a) As to claim 5, the combination of CB and Sidewinder discloses the step of determining includes scanning the data for a virus using the server (CB, page 76 – a location with many PC users might wish to scan incoming files for viruses, Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules and filter placement; also, protocol specific filtering to detect viruses in data transfers).

The combination of CB and Sidewinder does not explicitly disclose, however MIMEsweeper discloses the steps of storing the data in a temporary file at the server after the step of electronically transmitting (MIMEsweeper, page 13 – "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).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of storing the data in a temporary file at the server after the step of electronically transmitting in the system of CB and Sidewinder, as MIMEsweeper discloses, so as to allow a network administrator or the like to later review and evaluate the transmitted data.

b) As to claim 8, the combination of CB, Sidewinder and MIMEsweeper discloses 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 (MIMEsweeper, page 49 – "The way a file is scanned depends on the type of file…to be scanned and the validator employed").

c) As to claim 11, CB discloses a computer implemented method for detecting viruses in a mail message transfers between a first computer and a second computer, the method comprising the steps of: receiving a mail message request including a destination address (CB, pages 66-69, 74-75 – CB describes a system that receives data transfer requests with a destination address at a server); electronically receiving the mail message at a server; determining whether the mail message contains a virus (CB, page 76 – a location with many PC users might wish to scan incoming files for viruses, Chapter 3 "Firewall Gateways" including a discussion of packet filtering, filtering rules and filter placement; also, protocol specific filtering to detect viruses in data transfers); performing a preset action on the mail message if the mail message contains a virus (CB, page 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).

CB does not explicitly disclose, however Sidewinder discloses sending the mail message to the destination address if the mail message does not contain a virus; (Sidewinder, pages SR-454.9, SR-454-10 – block all incoming and outgoing news which does not fit the statistical properties of English-language plaintext, filter incoming and outgoing news on the basis of content similarity to postings deemed to be in violation of the site's policy. Page SR-454.4 - certain classes of data may be prohibited from passing to and from the external network).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ sending the mail message to the destination address if the mail message does not contain a virus in the system of CB, as Sidewinder teaches so as to avoid downstream virus infection.

The combination of CB and Sidewinder does not disclose, however MIMEsweeper discloses 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 (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. Page 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. 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". "The rationale behind this is that Email borne threats might not be recognized by checks if they are compressed or encoded".

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of 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 in the system of CB and Sidewinder, as

MIMEsweeper discloses so as to selectively transfer data based on the existence of viruses in order to avoid downstream virus infection.

d) **As to claim 12**, the combination of CB, Sidewinder and MIMEsweeper discloses wherein the step of determining whether the mail message includes any encoded portions searches for uuencoded portions (MIMEsweeper, page 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).

e) **As to claim 14,** the combination of CB, Sidewinder and MIMEsweeper discloses 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.

f) **As to claim 16**, the combination of CB, Sidewinder and MIMEsweper discloses wherein the step of performing a preset action on the mail message using the server comprises performing one step from the group of: transmitting 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 (Sidewinder, SR-454.8 – SR-454-12 - 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).

g) **As to claim 17**, the combination of CB, Sidewinder and MIMEsweper discloses 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 (Sidewinder, SR-454.8 – SR-454-12 - 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).

Claims 6 and 15 are rejected under 35 U.S.C. 103(a) as being obvious over **Cheswick and Bellovin (hereafter CB)** (Firewalls and Internet Security) in view of **Sidewinder** (Special Report: Secure Computing Corporation and Network Security) in view of **MIMEsweeper** (MIMEsweeper administrator guide) and further in view of **TIS Firewall** (TIS Firewall Toolkit Overview).

The combination of CB, Sidewinder and MIMEsweeper does not disclose, however TIS Firewall discloses the step of scanning is performed using a signature scanning process (TIS Firewall, page 41 – since many attacks "have a distinctive signature, smap or the firewall's mailer can be configured to attempt to identify these letterbombs").

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the step of scanning is performed using a signature scanning process in the system of CB, Sidewinder and MIMEsweeper, as TIS Firewall discloses so as to identify the existence of viruses.

Claim 9 is rejected under 35 U.S.C. 103(a) as being obvious over **Cheswick and Bellovin (hereafter CB)** (Firewalls and Internet Security) in view of **Sidewinder** (Special Report: Secure Computing Corporation and Network Security) and further in view of **TIS Firewall** (TIS Firewall Toolkit Overview).

The combination of CB and Sidewinder does not disclose, however TIS Firewall discloses 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 (TIS Firewall, page 41 - The FTP application gateway is a single process that mediates FTP connections between two networks); 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, page 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); and wherein the step of electronically receiving data comprises 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 (TIS Firewall, page 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).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use 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 an FTP daemon, and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network in the system of CB and Sidewinder, as TIS Firewall teaches so as to facilitate secure outbound and inbound file transfers using a common file transfer mechanism.

Claims 1-3 are rejected under 35 U.S.C. 103(a) as being obvious over **Norman Data Defense Systems, Inc., June 1995 (hereafter Norman)** (An Introduction to the Norman Firewall) in view of **TIS Firewall** (TIS Firewall Toolkit Overview).

a) As to claim 1, Norman discloses a system for detecting and selectively removing viruses in data transfers (Norman, page 4 – Norman teaches a firewall that "include[es] a fully configured secure computer system and virus detection capability" and "provides a single, highly secured route for data to travel between your network and the internet), the system comprising: 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 (The firewall of Norman is a computing device with memory (RAM); it uses a proxy server, necessarily loaded in memory while running (Norman, pp. 1, 7, 11). "The default configuration is a 100 MHz Intel 486 with 16 MB of RAM and a 1 GB SCSI disk subsystem that is running the SecureWare OS with the firewall software. The other CPU, the front end server, is by default a 66 MHz Intel 486 with 8 MB of RAM and a 500MB hard drive." (Norman, p. 7.) The firewall "has been equipped with an antivirus scanner" that "utilizes the well-known NORMAN Anti-Virus scanner engine, which scans for more then 7100 known viruses ....When a virus is located, the file transaction is blocked and logged." (Norman, p. 9.) The firewall "automatically checks every incoming file for viruses before letting the file through"; it "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman, p. 5); a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output ("Nearly all [internet security products] perform addressing, routing and filtering of data packets. They 'read' the address information in packets output; and direct each to the intended destination." (Norman, p. 5.) For example, a screening router "filter[s] packets using a pre-defined set of rules .... The router then determines whether or not a packet is allowed to pass .... [R]ules can be applied to the source and destination ports.... One can also specify separate sets of rules on incoming and outgoing connections." (Norman, p. 3.) " [A] packet filtering router controls packets at a low level .... Each packet resides on the system for a short moment while the header information is analyzed against the pre-determined rules." (Norman, p. 4.) The firewall of Norman "[a]ttaches LANs to intemet via dial-up or dedicated 56 KB or T1 facilities" (Norman, p. 11). "Not merely a packet filter or a router, [it] combines multiple secure computing and communications devices in a single package .... This fully configurable system is tunable to provide the functionality your work demands and the security your organization needs." (Norman, p. 4.); 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 ("Up to four separate CPUs can be accommodated on the bus. In the basic configuration, two CPUs are supplied. One processor runs the SecureWare operating system. This platform also runs the proxy processes and the anti-virus module. The other processor acts as the un-secure front-end server, and can be configured by the customer." (Norman, p. 6.) "The default configuration is a 100 MHz Intel 486 with 16 MB of RAM and a 1 GB SCSI disk subsystem that is running the SecureWare OS with the firewall software. The other CPU, the front end server, is by default a 66 MHz Intel 486 with 8 MB of RAM and a 500 MB hard drive." (Norman, p. 7.) "A separate Anti-Virus/Hotword process runs on the SecureWare platform. Traffic that is due to be checked for viruses and hotwords are queued, and the module will then scan and give clearances for each file. When a file is cleared, it is then passed on by the proxy process. (Norman, p. 9.); 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 ("A superior way of securing an IP network is to apply a so-called proxy server between the network and any external connections ....[T]he proxy machine runs two separate connections with the proxy as a carrier in between. This means that IP packets will not pass directly from the input to the output network interfaces in the proxy server environment:" (Norman, p. 1.) "A more secure approach than packet filtering and routing is the use of so-called proxy processes to convey the traffic between the inside and the outside net. All traffic will then be divided into two separate sessions. One session is established between the internal user and the firewall, and one session is established between the firewall and the external host." (Norman, p. 4.) The firewall of Norman "uses a proxy server" (Norman, p. 1); it "uses nothing but proxy services to pass traffic from one network to the other" (Norman, p. 7)).

Norman does not explicitly disclose, however TIS Firewall discloses 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 teaches a firewall design in which a sendmail proxy communicates with the SMTP daemon (sendmail server), in order to prevent direct network access to sendmail. "This sendmail-proxy, called smap,.., simply accepts all incoming messages and writes them to disk in a spool area .... A second process is responsible for scanning the spool area and delivering the mail messages to the real sendmail for delivery .... Smap preserves sendmail's functionality, while preventing an arbitrary user on the network from communicating directly with it." (TIS Firewall, p. 41). TIS Firewall also discloses more generally that "[a] proxy forwarder for a network protocol is an application that runs on a firewall host and connects specific service requests across the firewall, acting as a gateway .... Proxies can give the illusion to the software on both sides of a direct point-to-point connection." (TIS Firewall, page 37). The diagram of a telnet application proxy on page 38 of TIS Firewall shows that an application proxy is distinct from, and communicates with, an application daemon (telnetd server).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having 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 in the system of Norman, as TIS Firewall discloses, so as to allow secure network protocol services as well as reuse of existing facilities for data transfer.

b) **As to claim 2,** the combination of Norman and TIS Firewall discloses 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 Norman describes a proxy server that includes server is a FTP proxy server that handles proxy services for FTP (Norman, pp. 8, 11). The evaluation and transfer of data files, and the figure in Norman, page 8, illustrates an FTP daemon is an FTP daemon that communicates transaction handled by the firewall. The two-way arrow between the workstation in the protected LAN and the proxy, and the two-way arrow between the proxy and the remote host, demonstrate FTP communication with, and transfers of files to, a recipient node. TIS Firewall teaches a host-based application-level firewall design in which an FTP proxy controls the transfer of data files between an FTP daemon and a recipient node. A "bastion host provides application-level control" (TIS Firewall, p. 39). "The FTP application gateway is a single process that mediates FTP connections between two networks." (TIS Firewall, p. 41.) "To control FTP access, the application gateway reads a configuration file, containing a list of FTP commands that should be logged, and a description of what systems are allowed to engage in FTP traffic." (TIS Firewall, pp. 41-42). Regarding proxies generally, TIS Firewall states that "[a] proxy for a network protocol is an application that runs on a firewall host and connects specific service requests across the firewall, acting as a gateway .... Proxies can give the illusion to the software on both sides of a direct point-to-point connection. Since many proxies interpret the protocol that they manage, additional access control and audit may be performed as desired. 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, p. 37.). Although the diagram of an application proxy on page 38 of TIS Firewall is specific to telnet rather than FTP, it shows that an application proxy is distinct from, and communicates with, an application daemon (telnetd server). TIS Firewall discloses the use of an FTP daemon ("common programs such as the FTP server, ftpd") in discussing the advantages of a proxy-based firewall design (TIS Firewall, p. 38; the WUArchive ftpd is referenced on p. 44 as an "FTP server daemon").

c) **As to claim 3,** the combination of Norman and TIS Firewall discloses 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 (Norman describes a proxy server that includes proxy services for SMTP (Norman, pp. 8, 11). TIS Firewall teaches a firewall design in which a sendmail proxy communicates with the SMTP daemon (sendmail server), in order to prevent direct network access to sendmail. "This sendmail-proxy, called smap,.., simply accepts all incoming messages and writes them to disk in a spool area .... A second process is responsible for scanning the spool area and delivering the mail messages to the real sendmail for delivery .... Smap preserves sendmail's functionality, while preventing an arbitrary user on the network from communicating directly with it." (TIS Firewall, p. 41.) TIS Firewall also discloses more generally that "[a] proxy forwarder for a network protocol is an application that runs on a firewall host and connects specific service requests across the firewall, acting as a gateway .... Proxies can give the illusion to the software on both sides of a direct point-to-point connection. Since many proxies interpret the protocol that they manage, additional access control and audit may be performed as desired." (TIS Firewall, p. 37.) Although the diagram of an application proxy on page 38 of TIS Firewall is specific to telnet rather than FTP, it shows that an application proxy is distinct from, and communicates with, an application daemon (telnetd server)).

Claims 4, 7-8 and 21 are rejected under 35 U.S.C. 103(a) as being obvious over **Norman Data Defense Systems, Inc., June 1995 (hereafter Norman)** (An Introduction to the Norman Firewall) in view of **David J. Stang, (hereafter Stang)** (ICSA's Computer Virus Handbook).

a) As to claim 4, Norman discloses a computer implemented method for detecting viruses in data transfers between a first computer and a second computer (Norman teaches a firewall, "based upon off-the shelf PC-compatible hardware" (Norman, p. 6), that "provides a single, highly secured route for data to travel between your network and the internet" (Norman, p. 4). The firewall "include[es] a fully configured secure computer system and virus detection capability" (Norman, p. 4), the method comprising the steps of: receiving at a server a data transfer request including a destination address With a proxy server between an internal network and external connections, "IP packets will not pass directly from the input to the output network interfaces", because "the proxy server runs two separate connections with the proxy as the carrier in between" (Norman, p. 1). The firewall of Norman "uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly." (Norman, p. 7.) Such a proxy server necessarily receives data transfer requests from internal network nodes. With respect to outgoing transfers, the firewall "log[s] into the workstation on the secure network to transfer the requested file" (Norman, p. 8). The firewall "can identify the packets' destination" (Norman, p. 5). Internet security products in general "'read' the address information in packets and direct each to its intended destination" (Norman, p. 5). Such devices employ packet routing and filtering, including on outgoing traffic: for example, screening router rules "rely on the origin and destination IP addresses to decide if a packet is 'good' or 'bad' "; "rules can be applied to the source and destination ports", and one can "specify separate sets of rules on incoming and outgoing connections" (Norman, p. 3); electronically receiving data at the server (Norman describes a firewall having a proxy server that receives incoming data. The proxy server stands "between the [internal] network and any external connections .... IP packets will not pass directly from the input to the output network interfaces in the proxy server environment." (Norman, p. 1.); determining whether the data contains a virus at the server (The firewall of Norman "uses a proxy server" (Norman, p. 1) which "automatically checks every incoming file for viruses before letting the file through" (Norman, p. 5); performing a preset action on the data using the server if the data contains a virus (The firewall of Norman "scans all incoming server if the data contains a virus; files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman, p. 5). "When a virus is located [by the firewall], the file transaction is blocked and logged." (Norman, p. 9.) The firewall "can be made to notify a network management station on the internal net through SNMP traps. If a virus.., is discovered, traps can be sent to one or several machines on the secure network." (Norman, p. 20.)); sending the data to the destination address if the data does not contain a virus ("Traffic that is due to be checked for viruses...[is] queued, and the [antivirus] module will then scan and give clearances for each file. When a file is cleared, it is then passed on by the proxy process." (Norman, p. 9.).

Norman does not disclose, however Stang discloses 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 (Stang explains that virus-infected files are likely to be MS-DOS executable files with particular file extensions. "Once in the machine, the virus does nothing until the program it is attached to is 'run'. At that moment, what it does depends entirely on the species in question. The simpler viruses set out to make copies of themselves in other 'executable' files they can find, increasing the size of those files slightly. Such executable files include any file ending with .EXE, .COM, .OVL, .SYS, or .BIN." (Stang, p.

54.) "Of the hundreds of files on your hard disk, viruses only infect those files that end with the extensions COM and EXE (and sometimes BIN, SYS, OVL, OVR, etc)." (Stang, p. 114.) Transmitting data from the server to the destination, without performing virus detection, simply represents the operation of prior art network gateways. Therefore, it would have been obvious at the time the invention was made to a person having ordinary skill in the art to have a proxy server follow prior art practices by transmitting data without performing virus detection if, using the technique suggested by Stang; the data was determined not to be likely to contain a virus).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ 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 in the system of Norman, as Stang teaches, so as to reduce the amount of data to be scanned for viruses and minimize delays in transmission of network traffic.

b) **As to claim 7**, the combination of Norman and Stang discloses 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 (Transmitting data unchanged, even if it contains a virus, simply represents the ordinary operation of prior art network gateways which performed no antivirus scanning); not transmitting the data (The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman, p. 5). "When a virus is located [by the firewall], the file transaction is blocked and logged." (Norman, p. 9.); 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 [firewall] system can even be configured to record the contents of packets and to store sus-pect packets for later review by a security officer." (Norman, p. 5.) At the time the invention was made a person having ordinary skill in the art would have readily appreciated that stored packet contents could be given a unique file name, and that the firewall system could notify the recipient of the file name to allow the recipient to request access to the file).

c) **As to claim 8,** the combination of Norman and Stang discloses 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 (Stang explains that virus-infected files are likely to be MS-DOS executable files with particular file extensions. "Once in the machine, the virus comparing an extension type of a file name for does nothing until the program it is attached to is 'run'. At that moment, what it does depends entirely on the species in question. The simpler viruses set out to make copies of themselves in other 'executable' files they can find, increasing the size of those files slightly. Such executable files include any file ending with .EXE, .COM, .OVL, .SYS, or .BIN." (Stang, p. 54.) "Of the hundreds of files on your hard disk, viruses only infect those files that end with the extensions COM and EXE (and sometimes BIN, SYS, OVL, OVR, etc)." (Stang, p. 114.)).

d) **As to claim 21,** Norman does not disclose, however Stang disclose a second means for determining whether the data is of a type that is likely to contain a virus (Stang explains that virus-infected files are likely to be MS-DOS executable files with particular file extensions. "Once in the machine, the virus does nothing until the program it is attached to is 'run'. At that moment, what it does depends entirely on the species in question. The simpler viruses set out to make copies of themselves in other 'executable' files they can find, increasing the size of those files slightly. Such executable files include any file ending with .EXE, .COM, .OVL, .SYS, or .BIN." (Stang, p. 54.) "Of the hundreds of files on your hard disk, viruses only infect those files that end with the extensions COM and EXE (and sometimes BIN, SYS, OVL, OVR, etc)." (Stang, p. 114) ; 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 (If using the technique suggested by Stang, the proxy server transmits data without performing virus detection if the data was determined not to be likely to contain a virus).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of 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 in the system of Norman, as Stang teaches, so as to reduce the amount of data to be scanned for viruses and minimize delays in transmission of network traffic.

Claims 5-6 are rejected under 35 U.S.C. 103(a) as being obvious over **Norman Data Defense Systems, Inc. June 1995 (hereafter Norman)** (An Introduction to the Norman Firewall) in view of **David J. Stang, (hereafter Stang)** (ICSA's Computer Virus Handbook) and further in view of **Warner** (re: LZEXE and SCAN (PC), posting to VIRUS-L mailing list dated May 18, 1990, reprinted in VIRUS-L Digest , vol. 3, no. 99, May 21, 1990).

a) **As to claim 5,** the combination of Norman and Stang does not disclose, however Warner disclose 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 (Warner discloses a compressed file manager which scans compressed files for viruses: "it searches the compressed file for .EXE,.COM, .OBJ, and .SYS files, then uncompresses them into a temporary file and scans that temp file" (Warner, p. 2).

It would have been obvious to the ordinary skill in the art at the time of the invention to employ the use 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 in the system of Norman and Stang, as Warner teaches, so as to provide a specific technique to allow files being transmitted through the network (whether compressed or uncompressed) to be checked for viruses at the network gateway before such files could do damage on destination machines.

b) **As to claim 6**, the combination of Norman, Stang and Warner discloses the step of scanning is performed using a signature scanning process (Norman states that "[a]s new viruses are discovered and analyzed, their 'signatures' are included in the virus definition file (NVC.DEF)", a file that is updated regularly (Norman, p. 9).

Claim 9 is rejected under 35 U.S.C. 103(a) as being obvious over **Norman Data Defense Systems, Inc. June 1995 (hereafter Norman)** (An Introduction to the Norman Firewall) in view of **David J. Stang, (hereafter Stang)** (ICSA's Computer Virus Handbook) and further in view of TIS Firewall (TIS Firewall Toolkit Overview).

a) **As to claim 9,** the combination of Norman and Stang discloses determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network (Norman teaches a firewall that "can identify the packets' destination" (Norman, p. 5). Moreover, conventional network security products "'read' the address information in packets and direct each to its intended destination" (Norman, p. 5). For example, a screening router applies rules that "rely on the origin and destination IP-addresses to decide if a packet is 'good' or 'bad' " (Norman, p. 3); wherein the server is a FTP proxy server (The proxy server of Norman supports proxy services for FTP (Norman, pp. 8, 11)); 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 (Norman illustrates an FTP transaction on page 8. The two-way arrow labeled "ftp" between the proxy server inside the firewall and the external "Remote Host" shows the transfer of a file from the client node (Remote Host) to the FTP proxy server. In this case, the data is not being transferred into a first network (the external network containing the Remote Host).

The combination of Norman and Stang does not disclose, however TIS Firewall discloses wherein the step of electronically receiving data comprises 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 (TIS Firewall teaches a host-based application-level firewall design in which an FTP proxy controls the transfer of data files between an FTP daemon (which necessarily receives a file to be transferred from a file server) and a recipient node. A "bastion host provides application-level control" (TIS Firewall, p. 39). "The FTP application gateway is a single process that mediates FTP connections between two networks." (TIS Firewall, p. 41) "To control FTP access, the application gateway reads a configuration file, containing a list of FTP commands that should be logged, and a description of what systems are allowed to engage in FTP traffic." (TIS Firewall, pp. 41-42). Regarding proxies generally, TIS Firewall states that "[a] proxy for a network protocol is an application that runs on a firewall host and connects specific service requests across the firewall, acting as a gateway .... Proxies can give the illusion to the software on both sides of a direct point-to-point connection. Since many proxies interpret the protocol that they manage, additional access control and audit may be performed as desired. 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, p. 37) Although the diagram of an application proxy on page 38 of TIS Firewall is specific to telnet rather than FTP, it shows that an application proxy is distinct from, and communicates with, an application daemon (telnetd server). TIS Firewall discloses the use of an FTP daemon ("common programs such as the FTP server, ftpd") in discussing the advantages of a proxy- based firewall design (TIS Firewall, p. 38; the WUArchive ftpd is referenced on p. 44 as an "FTP server daemon").

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use 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 in the system of Norman and Stang, as TIS Firewall discloses, so as to allow secure file transfer as well as reuse of existing FTP facilities.

Claims 11-12, 14-17 and 37 are rejected under 35 U.S.C. 103(a) as being obvious over **Norman Data Defense Systems, Inc., June 1995 (hereafter Norman)** (An Introduction to the Norman Firewall) in view of **Warner** (re: LZEXE and SCAN (PC), posting to VIRUS-L mailing list dated May 18, 1990, reprinted in VIRUS-L Digest , vol. 3, no. 99, May 21, 1990).

a) **As to claim 11,** Norman discloses a computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer (Norman teaches a firewall which, unlike a mere packet filter or a router, "combines multiple secure computing and communications devices in a single package, including a fully configured secure computer system and virus detection capability" (Norman, p. 4). The firewall "automatically checks every incoming file for viruses before letting the file through" (Norman, p. 5). Incoming files include mail messages being transferred: the firewall "has proxy services for... SMTP (e-mail)" (Norman, p. 8), the firewall runs mail forwarding software (Norman, p. 6), and the antivirus module acts on contents of electronic mail (Norman, p. 9)), the method comprising the steps of: receiving a mail message request including a destination address (With a proxy server between an internal network and external connections, "IP packets will not pass directly from the input to the output network interfaces", because "the proxy server runs two separate connections with the proxy as the carrier in between" (Norman, p. 1). The firewall of Norman "uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly." (Norman, p. 7.) Such a proxy server necessarily receives data transfer requests from internal network nodes. With respect to outgoing transfers, the firewall "log[s] into the workstation on the secure network to transfer the requested file" (Norman, p. 8). The firewall "can identify the packets' destination" (Norman, p. 5). Intemet security products in general "'read' the address information in packets and direct each to its intended destination" (Norman, p. 5). Such devices employ packet routing and filtering, including on outgoing traffic: for example, screening router rules "rely on the origin and destination IP addresses to decide if a packet is 'good' or 'bad' "; "rules can be applied to the source and destination ports", and one can "specify separate sets of rules on incoming and outgoing connections" (Norman, p. 3)); electronically receiving the mail message at a server (Norman describes a firewall having a proxy server that receives incoming data. The proxy server stands "between the [internal] network and any external connections .... IP packets will not pass directly from the input to the output network interfaces in the proxy server environment." (Norman, p. 1.)); 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, decoding the encoded portions of the mail message to produced decoded portions of the mail message (Norman indicates that uuencoded files will be decoded portions for a virus, and testing whether decoded before being scanned for viruses: "Files the scanning step found any viruses; that are compressed using one of several known methods, will be uncompressed before scan. Methods currently supported include.. .UUencode." (Norman, p. 9.); performing a preset action on the mail message if the mail message contains a virus (The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman, p. 5). "When a virus is located [by the firewall], the file transaction is blocked and logged." (Norman, p. 9.) The firewall "can be made to notify a network management station on the internal net through SNMP traps. If a virus.., is discovered, traps can be sent to one or several machines on the secure network." (Norman, p. 20.)); and sending the mail message to the destination address if the mail message does not contains a virus ("A network administrator may also want to control the contents of electronic mail ....Traffic that is due to be checked for viruses and hotwords are queued, and the Anti-virus/Hotword module will then scan and give clearances for each file. When a file is cleared, it is then passed on by the proxy process." (Norman, p. 9.)

Norman does not disclose, however Warner discloses storing each encoded portion of the mail message in a separate temporary file and scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses (Warner discloses a compressed file manager which scans compressed files for viruses: "it searches the compressed file for .EXE, .COM, .OBJ, and .SYS files, then uncompresses them into a temporary file and scans that temp file" (Warner, p. 2)).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of storing each encoded portion of the mail message in a separate temporary file and scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses in the system of Norman, as Warner teaches, so as to allow compressed files being transmitted through the network to be checked for viruses at the network gateway before such files could do damage on destination machines.

b) As to claim 12, the combination of Norman and Warner discloses the step of determining whether the mail message includes any encoded portions searches for uuencoded portions ("Files that are compressed using of several known methods, will be uncompressed before scan. Methods currently supported include...UUencode." (Norman, p. 9.)).

c) As to claim 14, the combination of Norman and Warner discloses 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 (Warner discloses a compressed file manager which scans compressed files for viruses: "it searches the compressed file for .EXE, .COM, .OBJ, and .SYS files, then uncompresses them into a temporary file and scans that temp file" (Warner, p. 2)).

d) As to claim 15, the combination of Norman and Warner discloses wherein step of scanning is performed using a signature scanning process (Norman states that "[a]s new viruses are discovered and analyzed, their 'signatures' are included in the virus definition file (NVC.DEF)", a file that is updated regularly (Norman, p. 9)).

e) As to claim 16, the combination of Norman and Warner discloses 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 (Transmitting data unchanged, even if it contains a virus, simply represents the ordinary operation of prior art network gateways which performed no antivirus scanning); not transferring the mail message (The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman, p. 5). "When a virus is located [by the firewall], the file transaction is blocked and logged." (Norman, p. 9.); 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 ("The [firewall] system can even be configured to record the contents of packets and to store suspect packets for later review by a security officer." (Norman, p. 5.) At the time the invention was made a person having ordinary skill in the art would have readily appreciated that stored packet contents could be given a unique file name, and that the firewall system could notify the recipient of the file name to allow the recipient to request access to the file); **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.

f) **As to claim 17**, the combination of Norman and Warner discloses 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 (Transmitting data unchanged, even if it contains a virus, simply represents the ordinary operation of prior art network gateways which performed no antivirus scanning); transferring the mail message with the encoded portions having a virus deleted (According to the recitation in claim 11, encoded portion is stored in a separate temporary file, decoded, and scanned for viruses. At the time the invention was made a person having ordinary skill in the art would have found it rudimentary to configure the firewall system of Norman to delete a particular infected portion from the original mail message (since its precise location within the original mail message file would be known) and to transmit the modified mail message using ordinary electronic mail techniques); 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 (At the time the invention was made a person having ordinary skill in the art would have readily appreciated that the temporary file recited in claim 11 must have a known path name indicating its location in some directory in the file system. It would have been rudimentary to copy such a file to a specified file system directory using basic operating system facilities, the copy having a new path name.

Moreover, it would have been obvious at the time the invention was made to a person having ordinary skill in the art to configure the firewall system to notify the recipient of the path name of the file, using known electronic mail techniques, because it would enable the recipient to request access to the file); 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 (Modification by the mail forwarding system of the data in a mail message to include the output of a particular process simply uses file modification and electronic mall techniques well known in the art at the time the invention was made. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the firewall system of Norman by having the system edit a mail message that has had infected encoded portions removed to contain the result of the scanning process in the message, and then having the system send the message to the destination, because it would allow the recipient to know that a particular sender had sent infected data).

g) **As to claim 37**, the combination of Norman and Warner discloses wherein performing a preset action on the mail message comprises 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 (The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman: p. 5). "If the packet is found to be O.K, it is passed on" (Norman: p. 4).

Claims 23-25, 27-29 are rejected under 35 U.S.C. 103(a) as being obvious over **Norman Data Defense Systems, Inc., June 1995 (hereafter Norman)** (An Introduction to the Norman Firewall) in view of **Warner** (re: LZEXE and SCAN (PC), posting to VIRUS-L mailing list dated May 18, 1990, reprinted in VIRUS-L Digest , vol. 3, no. 99, May 21, 1990).

a) **As to claim 23**, Norman discloses a computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer (Norman teaches a firewall which, unlike a mere packet filter or a router, "combines multiple secure computing and communications devices in a single package, including a fully configured secure computer system and virus detection capability" (Norman: p. 4). The firewall "automatically checks every incoming file for viruses before letting the file through" (Norman: p. 5). Incoming files include mail messages being transferred: the firewall "has proxy services for... SMTP (e-mail)" (Norman: p. 8), the firewall runs mail forwarding software (Norman: p. 6), and the antivirus module acts on contents of electronic mail (Norman: .p. 9)), comprising: receiving a mail message request including a destination address (With a proxy server between an internal network and external connections, "IP packets will not pass directly from the input to the output network interfaces", because "the proxy server runs two separate connections with the proxy as the carrier in between" (Norman: p. 1). The firewall of Norman "uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly." (Norman: p. 7). Such a proxy server necessarily receives data transfer requests from internal network nodes. With respect to outgoing transfers, the firewall "log[s] into the workstation on the secure network to transfer the requested file" (Norman: p. 8). The firewall "can identify the packets' destination" (Norman: p. 5). Intenet security products in general "'read' the address information in packets and direct each to its intended destination" (Norman: p. 5). Such devices employ packet routing and filtering, including on outgoing traffic: for example, screening router rules "rely on the origin and destination IP addresses to decide if a packet is 'good' or 'bad' "; "rules can be applied to the source and destination ports", and one can "specify separate sets of rules on incoming and outgoing connections" (Norman: p. 3)); electronically receiving the mail message at a server (Norman describes a firewall having a proxy server that receives incoming data. The proxy server stands "between the [internal] network and any external connections .... IP packets will not pass directly from the input to the output network interfaces in the proxy server environment." (Norman: p. 1.)); determining whether the mail message contains a virus, the determination of whether the mail message contains a virus comprising (i) determining whether the mail message includes any encoded portions, (iii) decoding the encoded portions of the mail message to produced decoded portions of the mail message; (v) scanning each unencoded portion of the mail message for a virus, (vii) determining if the unencoded portions of the mail message contain a virus (The '600 Patent refers to uuencode as an example of an encoding scheme. Norman indicates that uuencoded files will be decoded before being scanned for viruses: "Files that are compressed using one of several known methods, will be uncompressed before scan. Methods currently supported include.. .UUencode." (Norman: p. 9); performing a preset action on the mail message if any of the decoded portion of the mail message contain a virus or if the unencoded portions of the mail message contain a virus; and sending the mail message to the destination address if the mail message does not contain a virus (The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman: p. 5). "If the packet is found to be O.K, it is passed on" (Norman: p. 4).

Norman and Warner disclose scanning each of the decoded portions for a virus, Norman does not disclose, however Warner discloses (ii) storing each encoded portion of the mail message in a separate temporary file and (iv) scanning each of the decoded portions for a virus, and (vi) determining if any of the decoded portions of the mail message contain a virus (Warner discloses a compressed file manager which scans compressed files for viruses: "it searches the compressed file for .EXE, .COM, .OBJ, and .SYS files, then uncompresses them into a temporary file and scans that temp file" (Warner: p. 2)).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of storing each encoded portion of the mail message in a separate temporary file; scanning each of the decoded portions for a virus, and determining if any of the decoded portions of the mail message contain a virus in the system of Norman, as Warner teaches, so as to allow compressed files being transmitted through the network to be checked for viruses at the network gateway before such files could do damage on destination machines.

b) **As to claim 24**, Norman discloses a computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer (Norman teaches a firewall which, unlike a mere packet filter or a router, "combines multiple secure computing and communications devices in a single package, including a fully configured secure computer system and virus detection capability" (Norman: p. 4). The firewall "automatically checks every incoming file for viruses before letting the file through" (Norman: p. 5). Incoming files include mail messages being transferred: the firewall "has proxy services for... SMTP (e-mail)" (Norman: p. 8), the firewall runs mail forwarding software (Norman: p. 6), and the antivirus module acts on contents of electronic mail (Norman: p. 9)), comprising: receiving a mail message request including a destination address (With a proxy server between an internal network and external connections, "IP packets will not pass directly from the input to the output network interfaces", because "the proxy server runs two separate connections with the proxy as the carrier in between" (Norman: p. 1). The firewall of Norman "uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly." (Norman: p. 7). Such a proxy server necessarily receives data transfer requests from internal network nodes. With respect to outgoing transfers, the firewall "log[s] into the workstation on the secure network to transfer the requested file" (Norman: p. 8). The firewall "can identify the packets' destination" (Norman: p. 5). Intenet security products in general "'read' the address information in packets and direct each to its intended destination" (Norman: p. 5). Such devices employ packet routing and filtering, including on outgoing traffic: for example, screening router rules "rely on the origin and destination IP addresses to decide if a packet is 'good' or 'bad' "; "rules can be applied to the source and destination ports", and one can "specify separate sets of rules on incoming and outgoing connections" (Norman: p. 3)); electronically receiving the mail message at a server (Norman describes a firewall having a proxy server that receives incoming data. The proxy server stands "between the [internal] network and any external connections .... IP packets will not pass directly from the input to the output network interfaces in the proxy server environment." (Norman: p. 1.)); determining whether the mail message includes any encoded portions, decoding the encoded portions of the mail message to produced decoded portions of the mail message; (The '600 Patent referes to uuencode as an example of an encoding scheme. Norman indicates that uuencoded files will be decoded before being scanned for viruses: "Files that are compressed using one of several known methods, will be uncompressed before scan. Methods currently supported include.. .UUencode." (Norman: p. 9); performing one of i) a preset action on the mail message if the mail message contains a virus (Because of the way the claim is structured, it can be understood that only one of the step can be performed. At least Norman discloses step i). The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman: p. 5). "When a virus is located [by the firewall], the file transaction is blocked and logged." (Norman: p. 9). The firewall "can be made to notify a network management station on the internal net through SNMP traps. If a virus.., is discovered, traps can be sent to one or several machines on the secure network." (Norman: p. 20)); ii) sending the mail message to the destination address without first scanning the mail message for viruses if the mail message does not contain any encoded portions; and iii) sending the mail message to the destination address if the encoded portions of the mail message do not contains a virus.

Norman and Warner disclose scanning each of the decoded portions for a virus, Norman does not disclose, however Warner discloses storing each encoded portion of the mail message in a separate temporary file and scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses (Warner discloses a compressed file manager which scans compressed files for viruses: "it searches the compressed file for .EXE, .COM, .OBJ, and .SYS files, then uncompresses them into a temporary file and scans that temp file" (Warner: p. 2)).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of storing each encoded portion of the mail message in a separate temporary file; scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses in the system of Norman, as Warner teaches, so as to allow compressed files being transmitted through the network to be checked for viruses at the network gateway before such files could do damage on destination machines.

c) **As to claims 25 and 29**, the combination of Norman and Warner discloses wherein performing a preset action on the mail message comprises creating a modified mail message without any viruses and transferring the mail message to the destination address (The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman: p. 5). "If the packet is found to be O.K, it is passed on" (Norman: p. 4).

d) **As to claim 27**, Norman discloses a computer implemented method for detecting viruses in all mail message transferred between a first computer and a second computer (Norman teaches a firewall which, unlike a mere packet filter or a router, "combines multiple secure computing and communications devices in a single package, including a fully configured secure computer system and virus detection capability" (Norman: p. 4). The firewall "automatically checks every incoming file for viruses before letting the file through" (Norman: p. 5). Incoming files include mail messages being transferred: the firewall "has proxy services for... SMTP (e-mail)" (Norman: p. 8), the firewall runs mail forwarding software (Norman: p. 6), and the antivirus module acts on contents of electronic mail (Norman: p. 9)), comprising: receiving a mail message request including a destination address (With a proxy server between an internal network and external connections, "IP packets will not pass directly from the input to the output network interfaces", because "the proxy server runs two separate connections with the proxy as the carrier in between" (Norman: p. 1). The firewall of Norman "uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly." (Norman: p. 7). Such a proxy server necessarily receives data transfer requests from internal network nodes. With respect to outgoing transfers, the firewall "log[s] into the workstation on the secure network to transfer the requested file" (Norman: p. 8). The firewall "can identify the packets' destination" (Norman: p. 5). Intenet security products in general "'read' the address information in packets and direct each to its intended destination" (Norman: p. 5). Such devices employ packet routing and filtering, including on outgoing traffic: for example, screening router rules "rely on the origin and destination IP addresses to decide if a packet is 'good' or 'bad' "; "rules can be applied to the source and destination ports", and one can "specify separate sets of rules on incoming and outgoing connections" (Norman: p. 3)); electronically receiving the mail message at a server (Norman describes a firewall having a proxy server that receives incoming data. The proxy server stands "between the [internal] network and any external connections .... IP packets will not pass directly from the input to the output network interfaces in the proxy server environment." (Norman: p. 1.)); determining for all messages received at the server whether the mail message contains a virus, the determination of whether the mail message contains a virus comprising (i) determining whether the mail message includes any encoded portions, (iii) decoding the encoded portions of the mail message to produced decoded portions of the mail message; (v) scanning each unencoded portion of the mail message for a virus, (vii) determining if the unencoded portions of the mail message contain a virus (The '600 Patent refers to uuencode as an example of an encoding scheme. Norman indicates that uuencoded files will be decoded before being scanned for viruses: "Files that are compressed using one of several known methods, will be uncompressed before scan. Methods currently supported include.. .UUencode." (Norman: p. 9); performing a preset action on the mail message if any of the decoded portion of the mail message contain a virus or if the unencoded portions of the mail message contain a virus; and sending the mail message to the destination address if the mail message does not contain a virus (The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman: p. 5). "If the packet is found to be O.K, it is passed on" (Norman: p. 4).

Norman and Warner disclose scanning each of the decoded portions for a virus, Norman does not disclose, however Warner discloses (ii) storing each encoded portion of the mail message in a separate temporary file and (iv) scanning each of the decoded portions for a virus, and (vi) determining if any of the decoded portions of the mail message contain a virus (Warner discloses a compressed file manager which scans compressed files for viruses: "it searches the compressed file for .EXE, .COM, .OBJ, and .SYS files, then uncompresses them into a temporary file and scans that temp file" (Warner: p. 2)).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of storing each encoded portion of the mail message in a separate temporary file; scanning each of the decoded portions for a virus, and determining if any of the decoded portions of the mail message contain a virus in the system of Norman, as Warner teaches, so as to allow compressed files being transmitted through the network to be checked for viruses at the network gateway before such files could do damage on destination machines.

e) **As to claim 28**, Norman discloses a computer implemented method for detecting viruses in all mail messages transferred between a first computer and a second computer (Norman teaches a firewall which, unlike a mere packet filter or a router, "combines multiple secure computing and communications devices in a single package, including a fully configured secure computer system and virus detection capability" (Norman: p. 4). The firewall "automatically checks every incoming file for viruses before letting the file through" (Norman: p. 5). Incoming files include mail messages being transferred: the firewall "has proxy services for... SMTP (e-mail)" (Norman: p. 8), the firewall runs mail forwarding software (Norman: p. 6), and the antivirus module acts on contents of electronic mail (Norman: p. 9)), comprising: receiving a mail message request including a destination address (With a proxy server between an internal network and external connections, "IP packets will not pass directly from the input to the output network interfaces", because "the proxy server runs two separate connections with the proxy as the carrier in between" (Norman: p. 1). The firewall of Norman "uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly." (Norman: p. 7). Such a proxy server necessarily receives data transfer requests from internal network nodes. With respect to outgoing transfers, the firewall "log[s] into the workstation on the secure network to transfer the requested file" (Norman: p. 8). The firewall "can identify the packets' destination" (Norman: p. 5). Intenet security products in general "'read' the address information in packets and direct each to its intended destination" (Norman: p. 5). Such devices employ packet routing and filtering, including on outgoing traffic: for example, screening router rules "rely on the origin and destination IP addresses to decide if a packet is 'good' or 'bad' "; "rules can be applied to the source and destination ports", and one can "specify separate sets of rules on incoming and outgoing connections" (Norman: p. 3)); electronically receiving the mail message at a server (Norman describes a firewall having a proxy server that receives incoming data. The proxy server stands "between the [internal] network and any external connections .... IP packets will not pass directly from the input to the output network interfaces in the proxy server environment." (Norman: p. 1.)); determining for all mail messages received at the server whether the mail message includes any encoded portions, decoding the encoded portions of the mail message to produced decoded portions of the mail message; (The '600 Patent referes to uuencode as an example of an encoding scheme. Norman indicates that uuencoded files will be decoded before being scanned for viruses: "Files that are compressed using one of several known methods, will be uncompressed before scan. Methods currently supported include.. .UUencode." (Norman: p. 9); performing at least one of i) a preset action on the mail message if the mail message contains a virus (Because of the way the claim is structured, it can be understood that only one of the step can be performed. At least Norman discloses step i). The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman: p. 5). "When a virus is located [by the firewall], the file transaction is blocked and logged." (Norman: p. 9). The firewall "can be made to notify a network management station on the internal net through SNMP traps. If a virus.., is discovered, traps can be sent to one or several machines on the secure network." (Norman: p. 20)); ii) sending the mail message to the destination address without first scanning the mail message for viruses if the mail message does not contain any encoded portions; and iii) sending the mail message to the destination address if the encoded portions of the mail message do not contains a virus.

Norman and Warner disclose scanning each of the decoded portions for a virus, Norman does not disclose, however Warner discloses storing each encoded portion of the mail message in a separate temporary file and scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses (Warner discloses a compressed file manager which scans compressed files for viruses: "it searches the compressed file for .EXE, .COM, .OBJ, and .SYS files, then uncompresses them into a temporary file and scans that temp file" (Warner: p. 2)).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of storing each encoded portion of the mail message in a separate temporary file; scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses in the system of Norman, as Warner teaches, so as to allow compressed files being transmitted through the network to be checked for viruses at the network gateway before such files could do damage on destination machines.

Claims 26 and 30 are rejected under 35 U.S.C. 103(a) as being obvious over **Norman Data Defense Systems, Inc., June 1995 (hereafter Norman)** (An Introduction to the Norman Firewall) in view of **Warner** (re: LZEXE and SCAN (PC), posting to VIRUS-L mailing list dated May 18, 1990, reprinted in VIRUS-L Digest, vol. 3, no. 99, May 21, 1990) and further in view of **LANProtect**.

The combination of Norman and Warner does not explicitly disclose, however LANProtect discloses performing a preset action on the mail message comprises 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 (LANProtect: p. 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: p. 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.") (LANProtect: p. 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.").

Claims 35-36 are rejected under 35 U.S.C. 103(a) as being obvious over **Norman Data Defense Systems, Inc., June 1995 (hereafter Norman)** (An Introduction to the Norman Firewall) in view of **NetShield.**

a) As to claim 35, Norman discloses a computer implemented method for detecting viruses in data transfers between a first computer, a server comprising a proxy server, and a second computer, the computer implemented method comprising: (Norman teaches a firewall which, unlike a mere packet filter or a router, "combines multiple secure computing and communications devices in a single package, including a fully configured secure computer system and virus detection capability" (Norman: p. 4). The firewall "automatically checks every incoming file for viruses before letting the file through" (Norman: p. 5). Incoming files include mail messages being transferred: the firewall "has proxy services for... SMTP (e-mail)" (Norman: p. 8), the firewall runs mail forwarding software (Norman: p. 6), and the antivirus module acts on contents of electronic mail (Norman: p. 9)), transmitting, by the first computer, a data transfer request including a destination address of the second computer, receiving at the server the data transfer request and the destination address (With a proxy server between an internal network and external connections, "IP packets will not pass directly from the input to the output network interfaces", because "the proxy server runs two separate connections with the proxy as the carrier in between" (Norman: p. 1). The firewall of Norman "uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly." (Norman: p. 7). Such a proxy server necessarily receives data transfer requests from internal network nodes. With respect to outgoing transfers, the firewall "log[s] into the workstation on the secure network to transfer the requested file" (Norman: p. 8). The firewall "can identify the packets' destination" (Norman: p. 5). Intenet security products in general "'read' the address information in packets and direct each to its intended destination" (Norman: p. 5). Such devices employ packet routing and filtering, including on outgoing traffic: for example, screening router rules "rely on the origin and destination IP addresses to decide if a packet is 'good' or 'bad' "; "rules can be applied to the source and destination ports", and one can "specify separate sets of rules on incoming and outgoing connections" (Norman: p. 3)); electronically receiving data at the server in response to the data transfer request (Norman describes a firewall having a proxy server that receives incoming data. The proxy server stands "between the [internal] network and any external connections .... IP packets will not pass directly from the input to the output network interfaces in the proxy server environment." (Norman: p. 1.)); determining, by the proxy server, whether the data contains a virus, wherein the server utilizes a protocol layer hierarchy that includes an application layer, and wherein the proxy server resides below the application layer and detection of a virus by the proxy server occurs below the application layer (With a proxy server between an internal network and external connections, "IP packets will not pass directly from the input to the output network interfaces", because "the proxy server runs two separate connections with the proxy as the carrier in between" (Norman: p. 1). The firewall of Norman "uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly." (Norman: p. 7). Such devices employ packet routing and filtering, including on outgoing traffic: for example, screening router rules "rely on the origin and destination IP addresses to decide if a packet is 'good' or 'bad' "; "rules can be applied to the source and destination ports", and one can "specify separate sets of rules on incoming and outgoing connections" (Norman: p. 3)). A more secure approach than packet filtering and routing is the use of so-called proxy processes to convey the traffic between the inside and the outside net. All traffic will then be divided into two separate sessions. One session is established between the internal user and the firewall, and one session is established between the firewall and the external host (Norman: p. 4 and Fig. under the section 3.3. Using proxy processes); performing, by the server, a preset action on the data if the data contains a virus; sending the data to the destination address of the second computer if the data does not contain a virus (The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman: p. 5). "If the packet is found to be O.K, it is passed on" (Norman: p. 4).

Norman does not disclose, however Netshield discloses determining, by the proxy server, whether the data is of a type that is likely to contain a virus (NetShield explicitly teaches the desirability of scanning only a subset of files (e.g., excluding data files) (Netshield: p. 16) (noting scanning "all files for viruses, including data files, ... may impact server performance ... scanning all files is generally not recommended."). The default files scanned on access by NetShield are indicated to be ".COM, .EXE, .OV?, and .SYS." (NetShield: p. 16); and transmitting the data, in response to the data transfer request, from the server to the destination of the second computer without determining whether the data contains a virus and without performing a preset action if the data is not of a type that is likely to contain a virus (transmitting data from the server to the destination, without performing virus detection, simply represents the operation of prior art network gateways. Therefore, it would have been obvious at the time the invention was made to a person having ordinary skill in the art to have a proxy server follow prior art practices by transmitting data without performing virus detection if, using the technique suggested by NetShield, the data was determined not to be likely to contain a virus).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of determining whether a file was likely to be infected with a virus by examining its file extension in the system of Norman, as NetShield discloses so as to reduce the amount of data to be scanned for viruses and minimize delays in transmission of network traffic.

b) As to claim 36, Norman discloses a computer implemented method for detecting viruses, comprising: receiving, at a server comprising a proxy server, a data transfer request, data , and a destination address (With a proxy server between an internal network and external connections, "IP packets will not pass directly from the input to the output network interfaces", because "the proxy server runs two separate connections with the proxy as the carrier in between" (Norman: p. 1). The firewall of Norman "uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly." (Norman: p. 7). Such a proxy server necessarily receives data transfer requests from internal network nodes. With respect to outgoing transfers, the firewall "log[s] into the workstation on the secure network to transfer the requested file" (Norman: p. 8). The firewall "can identify the packets' destination" (Norman: p. 5). Intenet security products in general "'read' the address information in packets and direct each to its intended destination" (Norman: p. 5). Such devices employ packet routing and filtering, including on outgoing traffic: for example, screening router rules "rely on the origin and destination IP addresses to decide if a packet is 'good' or 'bad' "; "rules can be applied to the source and destination ports", and one can "specify separate sets of rules on incoming and outgoing connections" (Norman: p. 3)). Norman describes a firewall having a proxy server that receives incoming data. The proxy server stands "between the [internal] network and any external connections .... IP packets will not pass directly from the input to the output network interfaces in the proxy server environment." (Norman: p. 1.)); determining, by the proxy server, whether the data contains a virus, wherein the server utilizes a protocol layer hierarchy that includes an application layer, and wherein the proxy server resides below the application layer and detection of a virus by the proxy server occurs below the application layer (With a proxy server between an internal network and external connections, "IP packets will not pass directly from the input to the output network interfaces", because "the proxy server runs two separate connections with the proxy as the carrier in between" (Norman: p. 1). The firewall of Norman "uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly." (Norman: p. 7). Such devices employ packet routing and filtering, including on outgoing traffic: for example, screening router rules "rely on the origin and destination IP addresses to decide if a packet is 'good' or 'bad' "; "rules can be applied to the source and destination ports", and one can "specify separate sets of rules on incoming and outgoing connections" (Norman: p. 3)). A more secure approach than packet filtering and routing is the use of so-called proxy processes to convey the traffic between the inside and the outside net. All traffic will then be divided into two separate sessions. One session is established between the internal user and the firewall, and one session is established between the firewall and the external host (Norman: p. 4 and Fig. under the section 3.3. Using proxy processes); performing, by the server, a preset action on the data if the data contains a virus; sending the data to the destination address of the second computer if the data does not contain a virus (The firewall of Norman "scans all incoming files for any of 7100+ viruses, and sets them aside for later examination rather than forwarding them, if they are infected" (Norman: p. 5). "If the packet is found to be O.K, it is passed on" (Norman: p. 4).

Norman does not disclose, however Netshield discloses determining, by the proxy server, whether the data is of a type that is likely to contain a virus (NetShield explicitly teaches the desirability of scanning only a subset of files (e.g., excluding data files) (Netshield: p. 16) (noting scanning "all files for viruses, including data files, ... may impact server performance ... scanning all files is generally not recommended."). The default files scanned on access by NetShield are indicated to be ".COM, .EXE, .OV?, and .SYS." (NetShield: p. 16); and transmitting the data, in response to the data transfer request, from the server to the destination of the second computer without determining whether the data contains a virus and without performing a preset action if the data is not of a type that is likely to contain a virus (transmitting data from the server to the destination, without performing virus detection, simply represents the operation of prior art network gateways. Therefore, it would have been obvious at the time the invention was made to a person having ordinary skill in the art to have a proxy server follow prior art practices by transmitting data without performing virus detection if, using the technique suggested by NetShield, the data was determined not to be likely to contain a virus).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of determining whether a file was likely to be infected with a virus by examining its file extension in the system of Norman, as NetShield discloses so as to reduce the amount of data to be scanned for viruses and minimize delays in transmission of network traffic.

III. Response to Arguments

a) On page 22 of the Remarks, Patent Owner argues that there is no evidence that the Norman reference qualifies as a printed publication.

The Norman reference was marketed by Norman Data Defense Systems, Inc. with information about the company address for further communication. The document is clearly written for an outside audience (as opposed to dissemination of information to a closed set of individuals in a company). Given the nature of the document (i.e. a document containing product information) and the fact that contact information implies that they wish interested parties to contact them for further information, it is more likely than not that this reference was publicly disseminated. As such, it is considered a printed publication.

b) As to claim 1, on page 25 of the Remarks, Patent Owner argues that Cheswick does not disclose "the memory including a server for scanning data for a virus".

The Cheswick reference discloses a secure Internet gateway (Cheswick: the title of the document; "it would be nice to have a gateway that is demonstrably secure to protect the internal machines", last paragraph on col. 2 of page 233). The new Inet gateway machine 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 (Cheswick: col. 1, page 234). The claimed "server" can be interpreted by a person of ordinary skill in the art as a computer and/or software that performs services for other computers or programs. It is inherently understood that the Inet is a computing system with memory including a server. Cheswick further discloses ways to protect Inet (Cheswick: col. 2, page 235, "we have taken some steps to avoid denial-of-service attacks", "...all the important executable files are periodically checksummed and checked for changes". Computer viruses can be viewed as denial-of-service attack. Checksum and check for changes are understood as ways to scan for virus). On col. 1, page 236, Cheswick concludes "our best defense is continued scanning of internal machines for security holes in case such a program gets loose". As such, Cheswick teaches a secure Inet gateway having a memory including a server for scanning data for a virus.

c) As to claim 1, on page 26 of the Remarks, Patent Owner argues that TIS Firewall does not disclose "the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handling instructions and the presence of viruses".

TIS Firewall reference discloses the TIS Firewall toolkit is a software or a set of programs and configuration practices designed to facilitate the building of network firewalls (TIS Firewall: first paragraph, page 1). TIS Firewall discloses the bastion host running firewall software to support dual-homed gateways, screened host gateways, and screened subnet gateways. The toolkit software provides proxy services for common applications like FTP, Telnet, and security for SMTP mail (TIS Firewall: paragraph 4, page 4). TIS Firewall discloses in detail SMTP service, FTP and Telnet (TIS Firewall: "...smapd is responsible for scanning the smap spool directory periodically and submitting the queued messages to sendmail for final delivery", page 9. "ftpd: anonymous FTP service...this is to obviate any bugs that may be in the implementation of ftpd and is consistent with the overall configuration practice of preventing any system on an untrusted network from being able to directly connect to a privileged application running in an unrestricted file system", "syslogd: permitting real-time scanning of system logs and real-time alerts, page 13). It is understood that TIS Firewall does teach the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handling instructions and the presence of viruses.

d) As to claim 1, on page 44 of the Remarks, Patent Owner argues that Ranum does not disclose "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".

Ranum teaches TIS Internet Firewall Toolkit in which a sendmail proxy communicates with the SMTP daemon (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) to prevent direct network access to sendmail. "This sendmail proxy, called smap, ...simply accepts all incoming messages and writes them to disk in a spool area...A second process is responsible for scanning the spool area and delivering the mail messages to the real sendmail for delivery...Smap preserves sendmail's functionality, while preventing an arbitrary user on the network from communicating directly with it" (Ranum: col. 1, page 5).

Ranum also teaches "To implement a firewall that relies on routing and screening, one must permit at least a degree of direct IP-level traffic between the Internet and the protected network. Application level firewalls ...require development of specialized application forwarders known as "proxies"...A proxy for a network protocol is an application that runs on a firewall host and connects specific service requests across the firewall, acting as a gateway...Proxies can give the illusion to the software on both sides of a direct point-to-point connection (Ranum: col. 2, page 1). Figure 1 on page 2 of Ranum shows that an application proxy is distinct from, and communicates with, an application daemon (i.e. telnetd server). As addressed above, Ranum discloses an SMTP proxy with two processes (one to receive and copy to a spool area, and a second for scanning the spool area and delivering the mail) (Ranum: col. 1, page 5). Ranum also indicates that firewalls are vulnerable to data-driven attacks and suggests scanning mail as they are present in the firewall (Ranum: col. 2, page 5). The proxy daemons in

Ranum should not be mixed up with the client telnet daemon (i.e. Telnetd on remote system). In Fig. 1 on page 2, the Telnet daemon refers to the remote site external to the firewall, where the user is communicating with a daemon on the remote system. That is the communications session (i.e. network login service to the firewall) that is being proxied. The "Telnet application proxy" component of Fig. 1 resides on the firewall, and as addressed above, that application proxy contains two processes for handling two separate sessions resident on the firewall.

e) As to claim 4, on page 28 of the Remarks, Patent Owner argues that Cheswick-Bellovin (CB) does not disclose "performing a preset action on the data using the server if the data contains a virus".

CB reference discloses extensively the use and construction of a firewall or other system that can detect viruses in data transfers. Chapter 3, "Firewall Gateways", presents packet filtering, filtering rules, filter placement, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. CB also discloses implementing various security operations at the gateway, including selective scanning and potential operations that could be performed in the event a threat is found (CB: p. 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."). Clearly, CB discloses "performing a preset action (i.e. scan incoming files) on the data using the server if the data contains a virus".

f) As to claim 4, on page 29 of the Remarks, Patent Owner argues that Sidewinder does not disclose "sending the data to the destination address if the data does not contain a virus".

Sidewinder discloses the system administrator uses filtering to block (i.e. sending or receiving) mails that are dangerous, offensive, or illegal material such as virus-containing object code, personal encrypted messages, or pornographic pictures (Sidewinder: last paragraph on page SR-454.09 and SR-454.10). It is inherently understood that those mails that are not "virus-containing object code, personal encrypted messages, or pornographic pictures" will not be blocked (i.e. will be transmitting).

g) As to claim 7, on page 31 of the Remarks, Patent Owner argues that Sidewinder does not disclose "storing the data with a new name and notifying a recipient of the data transfer request of the new file name".

Claim 7 recites "...performing one step from the group of: transmitting ..., not transmitting..., and storing...". The way claim 7 is structured, it is interpreted that only one step needs to be performed. In this case, at least Sidewinder discloses the step "not transmitting the data" (Sidewinder: pages SR-454.8 – SR-454-12).

h) As to claim 8, on page 32 of the Remarks, Patent Owner argues that MIMESweeper does not disclose "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 of known extension types".

MIMESweeper discloses "the way a file is canned depends on the type of file to be scanned and the validator employed" (MIMESweeper: p. 49). The MIMEsweeper configuration file defines the different types of files are to be detected for viruses (MIMESweeper: p. 33, lists container types recognized and handled, Configuration data for the executable container type, configuration data for the ZIP archive container type). It is inherently understood that once the executable files (group of known extension types) are defined in the mimesep.cfg, they can be used as a reference to help detecting viruses.

i) As to claim 11, on page 34, Patent Owner argues that Cheswick-Bellovin (CB) does not disclose "performing a preset action on the data using the server if the data contains a virus".

CB reference discloses extensively the use and construction of a firewall or other system that can detect viruses in data transfers. Chapter 3, "Firewall Gateways", presents packet filtering, filtering rules, filter placement, protocol specific filtering, including a discussion of "safe" and "unsafe" types of content. CB also discloses implementing various security operations at the gateway, including selective scanning and potential operations that could be performed in the event a threat is found (CB: p. 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."). Clearly, CB discloses "performing a preset action (i.e. scan incoming files) on the data using the server if the data contains a virus".

j) As to claim 11, on page 35 of the Remarks, Patent Owner argues that Sidewinder does not disclose "sending the data to the destination address if the data does not contain a virus".

Sidewinder discloses the system administrator uses filtering to block (i.e. sending or receiving) mails that are dangerous, offensive, or illegal material such as virus-containing object code, personal encrypted messages, or pornographic pictures (Sidewinder: last paragraph on page SR-454.09 and SR-454.10). It is inherently understood that those mails that are not "virus-containing object code, personal encrypted messages, or pornographic pictures" will not be blocked (i.e. will be transmitting).

k) As to claim 13, on page 36 of the Remarks, Patent Owner argues that Sidewinder does not disclose "sending the data to the destination address if the data does not contain a virus".

Sidewinder discloses the system administrator uses filtering to block (i.e. sending or receiving) mails that are dangerous, offensive, or illegal material such as virus-containing object code, personal encrypted messages, or pornographic pictures (Sidewinder: last paragraph on page SR-454.09 and SR-454.10). It is inherently understood that those mails that are not "virus-containing object code, personal encrypted messages, or pornographic pictures" will not be blocked (i.e. will be transmitting).

l) As to claim 16, on page 37 of the Remarks, Patent Owner argues that Sidewinder does not disclose "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 recites "...performing one step from the group of: transferring ..., not transferring...,storing..., and creating". The way claim 16 is structured, it is interpreted that only one step needs to be performed. In this case, at least Sidewinder discloses the step "not transferring the mail message" (Sidewinder: pages SR-454.8 – SR-454-12).

m) As to claim 17, on pages 38, 40 of the Remarks, Patent Owner argues that Sidewinder does not disclose "renaming the encoded 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".

Claim 17 recites "...performing one step from the group of: transferring ..., transferring..., renaming ...and writing...". The way claim 17 is structured, it is interpreted that only one step needs to be performed. In this case, at least Sidewinder discloses the step "transmitting the mail message unchanged" (i.e. messages can be forwarded to a system administrator, Sidewinder: pages SR-454.8 – SR-454-12).

n) As to claim 4, on pages 56-59 of the Remarks, Patent Owner argues that the combination of Norman and Stang would change the principle of operation of Norman or render the reference inoperable for its intended purpose because the Norman firewall automatically checks every incoming file for viruses while Stang states that "...the only files that should never change are the files a virus might infect, and must change during the process", and "..[o]f the hundreds of files on your hard disk, viruses only infect those files that end with the extensions COM and EXE (and sometimes BIN, SYS, OVL, OVR, etc.); Norman teaches detecting viruses at a firewall, while Stang detects viruses on a "machine"; and the technique disclosed in Norman, where "[t]he entire process of store-examination-forward is extremely rapid, and in a typical configuration can process about 86,400 files per day, while Stang takes a period of time to monitor, compare and detect changes in file size over time.

Norman discloses checking every incoming file for viruses, Stang presents how the viruses work on page 54, specifically states "the simpler virures set out to make copies of themselves in other "executable" files they can find, increasing the size of those files slightly. Such executable files include any file ending with .EXE, .COM, .OVL, .SYS, or .BIN". Stang further discusses detecting viruses and program change as a detection method, where "of the hundreds of files on your hard disk, viruses only infect those files that end with the extensions COM and EXE (and sometimes BIN, SYS, OVL, OVR, etc.) Most viruses will change the files they infect in some way, adding code at the top or bottom (or rarely, the middle, too)" (Stang: p. 114). Stang does not disclose not to check every file for viruses.

Norman teaches detecting viruses at a firewall, and Stang in his International Computer Security Assocation (ICSA) Computer Virus Handbook, at least at the table of contents, discloses facts about viruses, how they work, viruses names, how to prevent, to detect, to identify, and to recover from viruses. These viruses are not limited at a firewall, they are on the Internet, in anti-virus software, in trusted systems, in packaged software, in operating system (Stang: table of content).

Norman's technique is described as "[t]he entire process of store-examination-forward is extremely rapid, and in a typical configuration can process about 86,400 files per day, while Stang also indicates monitoring, comparing and detecting changes in the next hour or so (Stang: p. 114).

As addressed above, it is proper to combine the teaching of Norman and Stang to address virus issues and the Norman-Stang combination would not change the principle of operation of Norman or render the reference inoperable for its intended purpose.

o) As to claim 5, on pages 59-61 of the Remarks, Patent Owner argues that while Warner explains how he understands the software should work, he also states that "I'm not sure on that". If the author (Warner) is not sure, then the Examiner and Patentee can not be sure either. Therefore a prima facie case of obviousness can not be set forth. Patent Owner also argues that Warner operates on a PC, and not on a server.

MPEP 2121.01(II) that states:

A prior art reference provides an enabling disclosure and thus anticipates a claimed invention if the reference describes the claimed invention in sufficient detail to enable a person of ordinary skill in the art to carry out the claimed invention; "proof of efficacy is not required for a prior art reference to be enabling for purposes of anticipation." Impax Labs. Inc. v. Aventis Pharm . Inc., 468 F.3d 1366, 1383, 81 USPQ2d 1001, 1013 (Fed. Cir. 2006). See also MPEP § 2122.

Regardless of the writer not being "sure", the disclosure provides sufficient detail to allow one of ordinary skill in the art to carry out or practice the claimed invention. Further Warner's disclosure shows that such a feature was known in the prior art, since he understood the concept enough to suggest it as a possibility.

The claimed term “server” can be reasonably interpreted to be “a computer and/or software that performs services for other computers or programs”. As such, a PC in Warner is qualified as the claimed server.

p) As to claim 9, on page 62 of the Remarks, Patent Owner argues that Ranum does not disclose “electronically receiving data comprises the step 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 if being transferred into the first network”.

Norman illustrates how an ftp transaction works through the Norman Firewall. The two-way arrow labeled "ftp" between the workstation in the protected LAN and the proxy server in the firewall shows the transfer of a file through internal packets from the server task (workstation) to the firewall, for final delivery to the first network (Remote Host) (Norman: figure on p. 8).

Ranum teaches an application-level firewall design in which an FTP proxy controls the transfer of data files between an FTP daemon (receive a files to be transferred from a file server) and a recipient node (Ranum: col. 2, p. 39, "...the bastion host provides application-level control"). The FTP application gateway is a single process that mediates FTP connections between two networks (Ranum: col. 2, p. 41) and "to control FTP access, the application gateway reads a configuration file, containing a list of FTP commands that should be logged, and a description of what systems are allowed to engage in FTP traffic" (Ranum: col. 2, p. 41). Ranum states that "[a] proxy for a network protocol is an application that runs on a firewall host and connects specific service requests across the firewall, acting as a gateway .... Proxies can give the illusion to the software on both sides of a direct point-to-point connection. Since many proxies interpret the protocol that they manage, additional access control and audit may be performed as desired. 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." (Ranum: col. 2, p. 37). Although the diagram of an application proxy on page 38 of Ranum is specific to telnet rather than FTP, it shows that an application proxy is distinct from, and communicates with, an application daemon (telnetd server). Ranum also discloses the use of an FTP daemon ("common programs such as the FTP server, ftpd") in discussing the advantages of a proxy- based firewall design, Ranum: col. 1, p. 38) (the WUArchive ftpd is referenced on p. 44 as an "FTP server daemon").

As such, the combination of Norman, to implement a firewall providing FTP services, and Ranum, the design in which a file server transfers a file to an FTP server daemon, which transfers the file to an FTP proxy, does disclose the claimed invention, to allow secure file transfer as well as reuse of existing FTP facilities.

q) As to claim 16, on pages 75-76 of the Remarks, Patent Owner argues that neither Norman nor Warner disclose "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".

Claim 16 recites "...performing one step from the group of: transferring ..., not transferring...,storing ...and creating...". The way claim 16 is structured, it is interpreted that only one step needs to be performed. In this case, at least Norman discloses the step "not transferring the mail message" (i.e. when a virus is located [by the firewall], the file transaction is blocked and logged, Norman: p. 9).

r) As to claim 17, on pages 76-77 of the Remarks, Patent Owner argues that neither Norman nor Warner disclose "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 recites "...performing one step from the group of: transferring ..., transferring...,renaming ...and writing...". The way claim 17 is structured, it is interpreted that only one step needs to be performed. In this case, at least the step "transferring the mail message unchanged" is disclosed (i.e. transmitting data unchanged, even if it contains a virus, simply represents the ordinary operation of prior art network gateways which performed no antivirus scanning).

IV. STATEMENT OF REASONS FOR PATENTABILITY AND/OR CONFIRMATION

Claims 10 and 13 are patentable.

The following is an examiner's statement of reasons for patentability and/or confirmation of the claims found patentable in this reexamination proceeding:

Claim 10 provides the limitation requiring "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". The prior art cited by the Requesters fail to teach or suggest this feature.

Claim 13 provides the limitation requiring "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". The prior art cited by the Requesters fails to anticipate or render obvious claim 13.

Any comments considered necessary by PATENT OWNER regarding the above statement must be submitted promptly to avoid processing delays. Such submission by the patent owner should be labeled: "Comments on Statement of Reasons for Patentability and/or Confirmation" and will be placed in the reexamination file.

CORRESPONDENCE

All correspondence relating to this ex parte reexamination proceeding should be directed:

By EFS: Registered users may submit via the electronic filing system EFS-Web, at https://sportal.uspto.gov/authenticate/authenticateuserlocalepf.html.

By Mail to:
Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to:
(571) 273-9900
Central Reexamination Unit

By hand:
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

For EFS-Web transmissions, 37 CFR 1.8(a)(1)(i) (C) and (ii) states that correspondence (except for a request for reexamination and a corrected or replacement request for reexamination) will be considered timely filed if (a) it is transmitted via the Office's electronic filing system in accordance with 37 CFR 1.6(a)(4), and (b) includes a certificate of transmission for each piece of correspondence stating the date of transmission, which is prior to the expiration of the set period of time in the Office action.

Any inquiry concerning this communication or earlier communications from the Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/Minh Dieu Nguyen/

Minh Dieu Nguyen
Primary Examiner
USPTO, Art Unit 3992
(571) 272-3873

Conferee: ____________

Conferee: AW