REMARKS

Upon entry of the amendment, claims 1-37 are pending for the Examiner's consideration with claims 1, 4, 11, 13, 18, 23, 24, 27, 28, 31, 34, 35 and 36 being the independent claims. New claims 23-37 are added. Support for new claims 23-37 can be found, for example, in at least Figures 4, 5A, 5B, 6A-6C, 7, 8A and 8B, and page 11, line 4 through page 25, line 2 of the application as originally filed on September 26, 1995. Patentee respectfully submits that, in accordance with 35 U.S.C. § 305, claims 23-37 do not enlarge the scope of the original claims of the patent under reexamination. As explained in Manual of Patent Examining Procedure (hereinafter "M.P.E.P.") § 2258. III.A., a claim presented in a reexamination proceeding enlarges the scope of the claims of the patent being reexamined where the claim is broader than ***each and every claim*** of the patent (emphasis added). A new claim is broader than an original patent claim if the new claim contains within its scope any conceivable product that would not have infringed the patent. M.P.E.P. §§ 2258.IV.G.; 1412.03. Patentee respectfully submits that new claims 23-37 are not broader than each and every claim of the patent, and, as such, are in compliance with 35 U.S.C. § 305.

Patent claims 1, 8, 11, 13 and 17 have been amended to correct what appears to be minor typographical errors. The scope of claims 1, 11, 13 and 17 as amended are not enlarged, and, as such, these claims are in compliance with 35 U.S.C. § 305.

As explained in detail below, Patentee respectfully submits that the rejections in the Office Action cannot properly be maintained for patent claims 1-22, nor for new claims 23-37 as presented herein. In accordance with M.P.E.P. § 2258 IV.G., submitted concurrently herewith is a Declaration of John C. Mitchell, Ph.D. Under 37 C.F.R. § 1.132 ("the Mitchell Declaration"), dated March 2, 2011, in support of the patentability of the claims.

I. Concurrent Litigation

In accordance with 37 C.F.R. § 1.565 and M.P.E.P. § 2282, the patent owner provides the following information regarding prior or concurrent proceedings involving the patent under reexamination:

CASE #	CASE NAME	COURT
04cv01785	Trend Micro Incorporated v. Fortinet, Inc.	N. D. Cal.
337-TA-510	Certain Systems for Detecting and Removing Viruses or Worms, Components Thereof, and Product Containing Same, Inv. 337-TA-510	U.S. International Trade Commission
07cv01806	Barracuda Networks Inc. v. Trend Micro Incorporated	N. D. Cal.
337-TA-624	Certain Systems for Detecting and Removing Viruses or Worms, Components Thereof, and Product Containing Same, Inv. 337-TA-624	U.S. International Trade Commission
08cv05371	Fortinet, Inc. v Trend Micro Incorporated	N.D. Cal.
2009-1485	Fortinet, Inc. v Trend Micro Incorporated	Court of Appeals for the Fed. Cir.
09-cv-149262	Trend Micro Incorporated v. Fortinet, Inc.	Superior Court of Cal., County of Santa Clara
10cv00048	Fortinet, Inc. v Trend Micro Incorporated	N.D. Cal.

In Investigation No. 337-TA-510, *Certain Systems for Detecting and Removing Viruses or Worms, Components Thereof, and Product Containing Same*, the Administrative Law Judge found in the Final Initial and Recommended Determinations that claims 1 and 3 of the '600 patent were anticipated under 35 U.S.C. § 102(a) by the Norman Firewall **product**, not any supporting documentation. Such a finding is not relevant in the present reexamination proceedings for at least two reasons. First, only a **final** holding of claim invalidity is controlling on the Office, and the Final

Initial and Recommended Determinations by the Administrative Law Judge in Investigation No. 337-TA-510 is not such a final holding. Second, even assuming *arguendo* that the Final Initial and Recommended Determinations were (or were considered to be) a **final** holding, the only prior art permissible in a reexamination proceeding is patents or printed publications, 35 U.S.C. §§ 301, 302. The Norman Firewall **product** ***was not and is not*** **currently presented as prior art** in the present reexamination proceeding, and ***could not*** **be properly presented or considered as prior art** before the U.S. Patent and Trademark Office.

I. The Rejections Under 35 U.S.C. § 103(a) are Unsupported and Should be Withdrawn

For rejections under 35 U.S.C. Section 103(a), the establishment of a *prima facie* case of obviousness requires that all the claim limitations must be taught or suggested by the prior art. M.P.E.P. § 2143. The establishment of a *prima facie* case of obviousness also requires that the claimed combination cannot render a reference unsatisfactory or inoperable for its intended purpose, or change the principle of operation of a reference. M.P.E.P. § 2143.01 V., VI.

In *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727 (2007), the Supreme Court set the standard for evaluating obviousness, and enunciated the following principles:

> "When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, § 103 likely bars it patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. A court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions." *Id.* at 1731.

Simply using the benefit of hindsight in combining references is improper. *In re Lee*, 277 F.3d 1338, 1342-45 (Fed. Cir. 2002). The Supreme Court, while recognizing the need to "guard against slipping into the use of hindsight," acknowledged the following principles:

> "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *Id.* at 1741, citing *In re Kahn*, 441 F.3d 977, 988 (C.A.Fed.2006).
>
> "...it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does." *Id.*

The Supreme Court in *KSR* further stated that:

> " ...a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was independently, known in the prior art." *Id.* at 1731.

An examiner may often find every element of a claimed invention in the prior art. "Virtually all inventions are combinations and virtually all are combinations of old elements." *Environmental Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 698 (Fed. Cir. 1983), cert. denied, 464 U.S. 1043 (1984); see also *Richel, Inc. v. Sunspool Corp.*, 714 F.2d 1573, 1579-80 (Fed. Cir. 1983). If identification of each claimed element in the prior art were sufficient to negate patentability, very few patents would ever issue.

Furthermore, rejecting patents solely by finding prior art corollaries for the claimed elements would permit an examiner to use the claimed invention itself as a blueprint for piecing together elements in the prior art to defeat the patentability of the claimed invention. Such an approach would be "an illogical and inappropriate process by which to determine patentability." *Sensonics, Inc. v. Aerosonic Corp.*, 81 F.3d 1566, 1570 (Fed. Cir. 1996). In other words, the examiner must show reasons that the skilled artisan, confronted with the <u>same</u> problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. The Supreme Court in *KSR* has also stated that:

> "...when the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be nonobvious." *KSR* at 1740, citing *United States v. Adams*, 383 U.S. 39, 51-52, 86 S.Ct. 708 (1966).

The claims at issue in the present proceeding define substantial improvements over the applied art in the form of combinations of functionalities, and elements that perform those functionalities. When properly viewed against the applicable standard and as shown in detail below, none of the asserted references, when considered either individually or collectively, teaches or suggests the claimed combinations of functionalities and elements. The claimed subject matter of the presently pending claims would have been unobvious to a person of ordinary skill at the time of the effective filing date of the '600 patent.

II. The 35 U.S.C. § 102(a) Rejection of Claims 18-20 and 22 over the Norman Reference

A. No Evidence that the Norman Reference Qualifies as a Printed Publication Under 35 U.S.C. § 102(a)

Beginning on page 5 of the Office Action, the Examiner has rejected claims 18-20 and 22 under 35 U.S.C. § 102(a) as being anticipated by "Norman Data Defense Systems, An Introduction to the Norman Firewall," June 1995 (hereinafter "the Norman reference" or "Norman").

To qualify as prior art under § 102(a), the Norman reference must qualify as a "printed publication," as it is not a patent. There is no evidence in the record, and there has been no showing whatsoever that the document "has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *Bruckelmyer v. Ground Heaters, Inc.,* 445 F.3d 1374, 1378 (Fed. Cir. 2006); *In re Wyer*, 655 F.2d 221, 226 (C.C.P.A. 1981); M.P.E.P. § 2128. The Norman reference itself provides no evidence that it was accessible to any member of the public before either the filing date or the priority date, and, without more, cannot form the basis of a rejection under 35 U.S.C. § 102(a).

Carella v. Starlight Archery, 804 F.2d 135, 139 (Fed. Cir. 1986); M.P.E.P. § 2128. There is no evidence that the Norman reference was accessible to the public through, for example, a library or patent office, or that it was included in a journal or trade press available to the public. Even if the Norman reference was technically accessible prior to either the filing date or the priority date of the patent under reexamination, there is no evidence in the record that the Norman reference was disseminated to provide knowledge to the public. *In re Tenney*, 254 F.2d 619, 629 (C.C.P.A. 1958) ("Knowledge is not in the possession *of the public* where there has been no dissemination, as distinguished from technical accessibility, and surely the former is the concept underlying the expression 'printed publication.'") (emphasis in original; Rich, J. concurring); M.P.E.P. § 2128.01. I. Because the Examiner has failed to provide any showing that the Norman reference was not only accessible to the public but also disseminated to provide knowledge to the public before either the filing date or the priority date of the patent under reexamination, the Examiner has not established that the Norman reference qualifies as a "printed publication" under 35 U.S.C. § 102(a). Accordingly, in addition to the current rejection of claims 18-20 and 22 under 35 U.S.C. § 102(a) over the Norman reference, each and every rejection of record, as set forth in 1. - 5. below, that also relies upon the Norman reference cannot properly be maintained because the Examiner has not established that this document is a printed publication.

> 1. Starting on page 24 of the Office Action, the Examiner rejected claims 1-3 and 13 under 35 U.S.C. § 103(a) as being obvious over Norman in view of *A Toolkit and Methods for Internet Firewalls* by Marcus J. Ranum et al. (hereinafter "Ranum").[2]
>
> 2. Starting on page 32 of the Office Action, the Examiner rejected claims 4, 7-8 and 21 under 35 U.S.C. § 103(a) as being obvious over Norman in view of the *ICSA's Computer Virus Handbook* by David J. Stang (hereinafter "Stang").
>
> 3. Starting on page 36 of the Office Action, the Examiner also rejected claims 5 and 6 under 35 U.S.C. § 103(a) as being obvious over Norman in view of Stang and further in view of the VIRUS-L

[2] Although the Examiner refers to the TIS Firewall reference as the basis for the rejection in the January 6, 2011 Office Action (*see* pg. 24), the actual quotes from the prior art cited by the Examiner in the Office Action in connection with this rejection are from the Ranum article (and not the TIS Firewall reference). Accordingly, this section of the present Response will refer to the Ranum article, even though the Office Action incorrectly refers to the TIS Firewall reference.

Digest, dated May 21, 1990, Volume 3 : Issue 69 (hereinafter "Warner").

4. Starting on page 37 of the Office Action, the Examiner rejected claims 9 and 10 under 35 U.S.C. § 103(a) as being obvious over Norman in view of Stang, and further in view of Ranum.[3]

5. Starting on page 41 of the Office Action, the Examiner rejected claims 11-12 and 14-17 under 35 U.S.C. § 103(a) as being obvious over Norman in view of Warner.

Accordingly, because the Examiner has not established that Norman qualifies as a printed publication, the rejection of the claims as set forth in 1. - 5. above also cannot properly be maintained.

B. Norman does not disclose "means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name"

Claim 20 recites the element of "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." The Office Action does not allege that Norman discloses this element, and provides no citation to Norman in support of this element. As such, the Examiner has not established that the Norman reference anticipates claim 20, and, for this reason as well, the rejection cannot properly be maintained.

III. The 35 U.S.C. § 103(a) Rejections of Claims 1-3 Over Cheswick, Cheswick-Bellovin, and Further in View of TIS Firewall

Beginning on page 8 of the Office Action, the Examiner rejected claims 1-3 under 35 U.S.C. § 103(a) over *The Design of a Secure Internet Gateway* article ("Cheswick") in view of the *Firewalls and Internet Security* article (hereinafter "Cheswick-Bellovin") and further in view of the *TIS Firewall Toolkit Overview* reference (hereinafter "TIS Firewall").

[3] Although the Examiner refers to the TIS Firewall reference as the basis for the rejection in the January 6, 2011 Office Action (*see* pg. 37), the actual quotes from the prior art cited by the Examiner in the Office Action in connection with this rejection are from the Ranum article (and not the TIS Firewall reference). Accordingly, this section of the present Response will refer to the Ranum article, even though the Office Action incorrectly refers to the TIS Firewall reference.

A. Cheswick does not disclose "the memory including a server for scanning data for a virus"

Claim 1 recites the element of "the memory including a server for scanning data for a virus." The Office Action alleges that Cheswick teaches this element. Patentee respectfully disagrees.

Page 8 of the Office Action cites the following passages and language from Cheswick in support of Cheswick's alleged disclosure of "the memory including a server for scanning data for a virus" element:

> 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.

These passages of Cheswick cited by the Examiner do not pertain to "the memory including a server for scanning data for a virus." In fact, the term "virus" does not appear in the portions of Cheswick cited by the Examiner. Cheswick states that "Inet checks the destination" of inbound mail. As would be readily apparent to one skilled in the art, this is not the same as, and does not even suggest, "the memory including a server for scanning data for a virus" as recited in claim 1. Moreover, Cheswick specifies no "data handling actions dependent on the existence of a virus," as recited in claim 1. Mitchell Declaration, ¶¶ 4-5.

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Cheswick, and cannot find language to support the conclusions which the Examiner derives from the words in Cheswick. In sum, Cheswick does not disclose "the memory including a server for scanning data for a virus," or specify "data handling actions dependent on the existence of a virus," both as recited in claim 1.

B. 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"

Claim 1 recites the element of "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." The Office Action alleges that TIS Firewall teaches this element. Patentee respectfully disagrees.

Page 10 of the Office Action cites the following passage and language from TIS Firewall in support of TIS Firewall's alleged disclosure of "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" element:

> TIS Firewall, pg. 4 - The toolkit software provides proxy services for common applications like FTP and TELNET, and security for SMTP mail.[4]
>
> TIS Firewall, pg. 4 - The toolkit is designed to support users who want to implement firewalls based on the "that which is not expressly permitted is denied" approach.[5]

These passages of TIS Firewall cited by the Examiner do not pertain to "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." The term "virus" does not appear in the portions of TIS Firewall cited by the Examiner. In fact, the term "virus" does not appear in TIS Firewall at all.

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in TIS Firewall, and cannot find language to support the conclusions which the Examiner derives from the words in TIS Firewall. In sum, TIS Firewall does not disclose "the proxy server

[4] The language cited in the Office Action is slightly different. The language cited above is the actual citation from TIS Firewall.

[5] The language cited in the Office Action is slightly different. The language cited above is the actual citation from TIS Firewall.

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" as recited in claim 1.

The passages of TIS Firewall cited by the Examiner in rejecting claims 2 and 3 on pages 11 and 12 of the Office Action are inapposite because the FTP proxy server and SMPT proxy server disclosed in TIS Firewall do not "scan[] 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," as required by claim 1

C. The Cheswick, Cheswick-Bellovin and TIS Firewall References Cannot Properly be Combined

Patentee respectfully submits that the Cheswick, Cheswick-Bellovin, and TIS Firewall references cannot properly be combined. A person of ordinary skill in the art, who is familiar with the Cheswick, Cheswick-Bellovin, TIS Firewall references, would not reasonably combine their teachings as alleged on page 11 of the Office Action.

First, a mere statement that a person of ordinary skill in the art would combine references without some objective reason to combine the teachings of the references is not sufficient by itself to establish a *prima facie* case of obviousness. *Ex parte Levengood*, 28 U.S.P.Q.2d (BNA) 1300 (Bd. Pat. App. & Inter. 1993), M.P.E.P. § 2143.01 IV. Page 11 of the Office Action does not set forth an objective reason for combining these references, and alleges only the following conclusory assertion:

> It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of...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...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.

Office Action, pg. 11 (emphasis added).

In fact, this is not a reason to combine the references, because, as discussed above in Section III.B, 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." Accordingly, the reasoning set forth by the Examiner on page 11 of the Office Action as to why Cheswick, Cheswick-Bellovin, TIS Firewall would be combined is improper as no objective reason has been given that correctly reflects what is actually disclosed by the references at issue.

For at least all of the above reasons, the rejection of independent claim 1, and the more narrow claims 2-3 depending therefrom, cannot properly be maintained.

IV. The 35 U.S.C. § 103(a) Rejections of Claims 4 and 7 Over Cheswick-Bellovin in View of Sidewinder

Beginning on page 12 of the Office Action, the Examiner rejected claims 4 and 7 under 35 U.S.C. § 103(a) over Cheswick-Bellovin in view of *Special Report: Secure Computing Corporation and Network Security* (hereinafter "Sidewinder").

A. Cheswick-Bellovin does not disclose "performing a preset action on the data using the server if the data contains a virus"

Claim 4 recites the element of "performing a preset action on the data using the server if the data contains a virus." The Office Action alleges that Cheswick-Bellovin teaches this element. Patentee respectfully disagrees.

Pages 12 and 13 of the Office Action cite the following passage and language from Cheswick-Bellovin in support of Cheswick-Bellovin's alleged disclosure of "performing a preset action on the data using the server if the data contains a virus" element:

> 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.
>
> Office Action, pages 11-12.

This passage of Cheswick-Bellovin cited by the Examiner does not pertain to "performing a preset action on the data using the server if the data contains a virus." The passage merely pontificates that "[a] location with many users ***might wish*** to scan incoming files for viruses." (emphasis added.) However, the passage says nothing about what might be done with a virus once it is detected, even assuming *arguendo* that one "***might wish*** to scan incoming files for viruses." There is no indication in the passage above that shows how Cheswick-Bellovin would "perform[] a preset action on the data using the server if the data contains a virus," as recited in claim 4.

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited passage of Cheswick-Bellovin, and cannot find language to support the conclusions which the Examiner derives from the words in Cheswick-Bellovin. In sum, Cheswick-Bellovin does not disclose "performing a preset action on the data using the server if the data contains a virus," as recited in claim 4.

B. Sidewinder does not disclose "sending the data to the destination address if the data does not contain a virus"

Claim 4 recites the element of "sending the data to the destination address if the data does not contain a virus." The Office Action alleges that Sidewinder teaches this element. Patentee respectfully disagrees.

Page 13 of the Office Action cites the following passage and language from Sidewinder in support of Sidewinder's alleged disclosure of "sending the data to the destination address if the data does not contain a virus" element:

> 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.
>
> Office Action, pg. 13 (emphasis added).

This passage of Sidewinder cited by the Examiner does not pertain to "sending the data to the destination address if the data does not contain a virus." Sidewinder merely blocks news that does not fit the statistical properties of English-language plaintext. Sidewinder, pg. SR-454.9. Sidewinder makes no affirmative determination as to whether "the data does not contain a virus," as recited in claim 4. Moreover, the passage of Sidewinder cited by the Examiner indicates that Sidewinder only searches for "news." This is a further indication that Sidewinder does not make an affirmative determination that "the data does not contain a virus," as recited in claim 4, because viruses are typically and often contained in sources (e.g., files) other than "news." It is not apparent that Sidewinder would be able to determine with sufficient certainty that the "data does not contain a virus" as recited in claim 4 by merely "block[ing] all mail which does not fit the statistical properties of English-language plaintext." Sidewinder, pg. SR-454.9. Mitchell Declaration, ¶¶ 6-7.

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Sidewinder, and cannot find language to support the conclusions which the Examiner derives from the words in Sidewinder. In sum, Sidewinder does not disclose "sending the data to the destination address if the data does not contain a virus" as recited in claim 4.

C. 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 the element of "storing the data with a new name and notifying a recipient of the data transfer request of the new file name." The Office Action alleges that Sidewinder teaches this element. Patentee respectfully disagrees.

Page 14 of the Office Action cites the following passage and language from Sidewinder in support of Sidewinder's alleged disclosure of "storing the data with a new name and notifying a recipient of the data transfer request of the new file name" element:

> 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).
>
> Office Action, pg. 14.

This passage of Sidewinder cited by the Examiner does not pertain to "storing the data with a new name and notifying a recipient of the data transfer request of the new file name." Sidewinder merely blocks mail that does not fit the statistical properties of English-language plaintext. Sidewinder, pg. SR-454.9. Claim 7 depends from independent claim 4, which recites "performing a preset action on the data using the server if the data contains a virus." As discussed above, Sidewinder does not detect a virus and, accordingly, does not perform "storing the data with a new name and notifying a recipient of the data transfer request of the new file name" as recited in claim 7. Applicants find no teaching in Sidewinder pertaining to "storing the data with a new name and notifying a recipient of the data transfer request of the new file name," as recited in claim 7.

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Sidewinder, and cannot find language to support the conclusions which the Examiner derives from the words in Sidewinder. In sum, 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" as recited in claim 7.

V. The 35 U.S.C. § 103(a) Rejections of Claims 5, 8, 11-14 and 16-17 Over Cheswick-Bellovin in View of Sidewinder and further in View of MIME*sweeper*

Beginning on page 14 of the Office Action, the Examiner rejected claims 5, 8, 11-14 and 16-17 under 35 U.S.C. § 103(a) over Cheswick-Bellovin in view of Sidewinder and further in View of the MIME*sweeper* Administrator Guide (hereinafter "MIME*sweeper*").

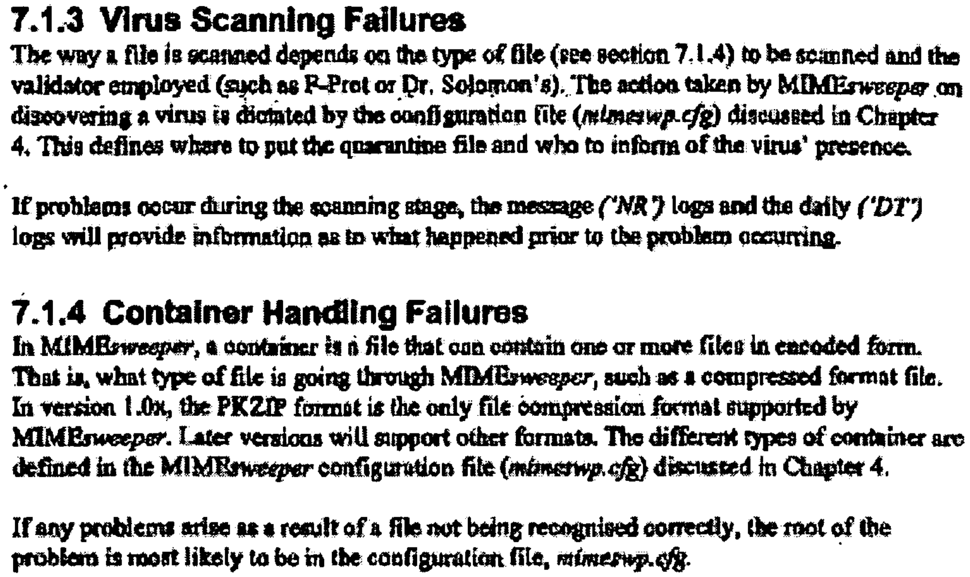
A. MIME*sweeper* does not disclose "determining whether the data is of a type that is likely to contain a virus is performed by comparing an extension type of a file name for the data to a group of known extension types"

Claim 8 recites the element 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 of known extension types." The Office Action alleges that MIME*sweeper* teaches this element. Patentee respectfully disagrees.

Page 15 of the Office Action cites the following passage and language from MIME*sweeper* in support of MIME*sweeper*'s alleged disclosure 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 of known extension types" element:

> MIME*sweeper*, page 49 - "The way a file is scanned depends on the type of file ... to be scanned and the validator employed".
>
> Office Action, pg. 15.

The Examiner has cited an incomplete passage from MIME*sweeper*. For context, a fuller portion of MIME*sweeper* is provided below for the Examiner's reference.



7.1.3 Virus Scanning Failures

The way a file is scanned depends on the type of file (see section 7.1.4) to be scanned and the validator employed (such as F-Prot or Dr. Solomon's). The action taken by MIME*sweeper* on discovering a virus is dictated by the configuration file (*mimeswp.cfg*) discussed in Chapter 4. This defines where to put the quarantine file and who to inform of the virus' presence.

If problems occur during the scanning stage, the message (*'NR'*) logs and the daily (*'DT'*) logs will provide information as to what happened prior to the problem occurring.

7.1.4 Container Handling Failures

In MIME*sweeper*, a container is a file that can contain one or more files in encoded form. That is, what type of file is going through MIME*sweeper*, such as a compressed format file. In version 1.0x, the PKZIP format is the only file compression format supported by MIME*sweeper*. Later versions will support other formats. The different types of container are defined in the MIME*sweeper* configuration file (*mimeswp.cfg*) discussed in Chapter 4.

If any problems arise as a result of a file not being recognised correctly, the root of the problem is most likely to be in the configuration file, *mimeswp.cfg*.

When the document is viewed as a whole, as the Examiner must, it is readily apparent that MIME*sweeper* does not disclose or suggest "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." MIME*sweeper* makes no reference to an extension type of a file name, such as a .EXE, .COM, .OBJ, and/or a .SYS file, let alone suggest that these extensions are compared to "a group of known extension types," as recited in claim 8. *See*, e.g., '600 patent, column. Mitchell Declaration, ¶ 8.

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in MIME*sweeper* cited by the Examiner, has reviewed additional portions of MIME*sweeper*, and has provided the excerpt above from MIME*sweeper* for the Examiner's benefit. The Patentee cannot find language to support the conclusions which the Examiner derives from the words in MIME*sweeper*. In sum, MIME*sweeper* 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," as recited in claim 8.

B. Cheswick-Bellovin does not disclose "performing a preset action on the data using the server if the data contains a virus"

Claim 11 recites the element of "performing a preset action on the data using the server if the data contains a virus." The Office Action alleges that Cheswick-Bellovin teaches this element. Patentee respectfully disagrees.

Pages 15 and 16 of the Office Action cite the following passage and language from Cheswick-Bellovin in support of Cheswick-Bellovin's alleged disclosure of "performing a preset action on the data using the server if the data contains a virus" element:

> 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.
>
> Office Action, pages 15-16.

This passage of Cheswick-Bellovin cited by the Examiner does not pertain to "performing a preset action on the data using the server if the data contains a virus." The passage merely pontificates that "[a] location with many users ***might wish*** to scan incoming files for viruses." (emphasis added.) However, the passage says nothing about what might be done with a detected virus, even assuming arguendo that one "***might wish*** to scan incoming files for viruses." There is no indication in the passage above that shows how Cheswick-Bellovin would "perform[] a preset action on the data using the server if the data contains a virus," as recited in claim 11.

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited passage of Cheswick-Bellovin, and cannot find language to support the conclusions which the Examiner derives from the words in Cheswick-Bellovin. In sum, Cheswick-Bellovin does not disclose "performing a preset action on the data using the server if the data contains a virus," as recited in claim 11.

C. Sidewinder does not disclose "sending the mail message to the destination address if the mail message does not contain a virus"

Claim 11 recites the element of "sending the mail message to the destination address if the mail message does not contain a virus." The Office Action alleges that Sidewinder teaches this element. Patentee respectfully disagrees.

Page 16 of the Office Action cites the following passage and language from Sidewinder in support of Sidewinder's alleged disclosure of "sending the mail message to the destination address if the mail message does not contain a virus" element:

> 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.
>
> Office Action, pg. 16 (emphasis added).

This passage of Sidewinder cited by the Examiner does not pertain to "sending the mail message to the destination address if the mail message does not contain a virus." Sidewinder merely blocks mail that does not fit the statistical properties of English-language plaintext. Sidewinder, pg. SR-454.9. Sidewinder makes no affirmative determination as to whether "the mail message does not contain a virus," as recited in claim 11. Moreover, the passage of Sidewinder cited by the Examiner indicates that Sidewinder only searches for "news." This is a further indication that Sidewinder does not make an affirmative determination that "the mail message does not contain a virus," as recited in claim 11, because viruses are typically and often contained in sources (e.g., files) other than "news." It is not apparent that Sidewinder would be able to determine with sufficient certainty that the "mail message does not contain a virus" as recited in claim 11 by merely "block[ing] all mail which does not fit the statistical properties of English-language plaintext." Sidewinder, pg. SR-454.9. Mitchell Declaration, ¶¶ 6-7.

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Sidewinder, and cannot find language to support the conclusions which the Examiner derives from the words in Sidewinder. In sum, Sidewinder does not disclose "sending the mail message to the destination address if the mail message does not contain a virus" as recited in claim 11.

D. Sidewinder does not disclose "sending the mail message to the destination address if the mail message does not contain a virus"

Claim 13 recites the element of "sending the mail message to the destination address if the mail message does not contain a virus." The Office Action alleges that Sidewinder teaches this element. Patentee respectfully disagrees.

Page 18 of the Office Action cites the following passage and language from Sidewinder in support of Sidewinder's alleged disclosure of "sending the mail message to the destination address if the mail message does not contain a virus" element:

> 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.
>
> Office Action, pg. 18 (emphasis added).

This passage of Sidewinder cited by the Examiner does not pertain to "sending the mail message to the destination address if the mail message does not contain a virus." Sidewinder merely blocks mail that does not fit the statistical properties of English-language plaintext.

Sidewinder, pg. SR-454.9. Sidewinder makes no affirmative determination as to whether "the mail message does not contain a virus," as recited in claim 13. Moreover, the passage of Sidewinder cited by the Examiner indicates that Sidewinder only searches for "news." This is a further indication that Sidewinder does not make an affirmative determination that "the mail message does not contain a virus," as recited in claim 13, because viruses are typically and often contained in sources (e.g., files) other than "news." It is not apparent that Sidewinder would be able to determine with sufficient certainty that the "mail message does not contain a virus" as recited in claim 13 by merely "block[ing] all mail which does not fit the statistical properties of English-language plaintext." Sidewinder, pg. SR-454.9. Mitchell Declaration, ¶¶ 6-7.

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Sidewinder, and cannot find language to support the conclusions which the Examiner derives from the words in Sidewinder. In sum, Sidewinder does not disclose "sending the mail message to the destination address if the mail message does not contain a virus," as recited in claim 13.

E. 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 the element of "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 Office Action alleges that Sidewinder teaches this element. Patentee respectfully disagrees.

Page 21 of the Office Action cites the following passage and language from Sidewinder in support of Sidewinder's alleged disclosure of "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" element:

> 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).
>
> Office Action, pg. 21.

This passage of Sidewinder cited by the Examiner does not pertain to "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 states that messages can be passed to or forwarded to a System Administrator, kept in a "trash" folder, or discarded. Sidewinder does not teach or suggest "creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address" as recited in claim 16. Claim 16 depends from independent claim 11, which recites "performing a preset action on the mail message if the mail message contains a virus." As discussed above, Sidewinder does not detect a virus and, accordingly, does not perform "performing a preset action on the mail message if the mail message contains a virus" as recited in claim 16.

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Sidewinder, and cannot find language to support the conclusions which the Examiner derives from the words in Sidewinder. In sum, 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" as recited in claim 16.

F. 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 the element of "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." The Office Action alleges that Sidewinder teaches this element. Patentee respectfully disagrees.

Page 21 of the Office Action cites the following passage and language from Sidewinder in support of Sidewinder's alleged disclosure of "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" element:

> 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).
>
> Office Action, pg. 21.

This passage of Sidewinder cited by the Examiner does not pertain to "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." Sidewinder states that messages can be passed to or forwarded to a System Administrator, kept in a "trash" folder, or discarded. Sidewinder does not teach or suggest "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" as recited in claim 17. Since claim 16 recites "renaming the encoded portions of the mail message containing a virus" and, as discussed above, Sidewinder does not detect a virus, Sidewinder does not "renam[e] the encoded portions of the mail message containing a virus."

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Sidewinder, and cannot find language to support the conclusions which the Examiner derives from the words in Sidewinder. In sum, 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" as recited in claim 17.

G. Sidewinder does not 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 the element of "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." The Office Action alleges that Sidewinder teaches this element. Patentee respectfully disagrees.

Page 21 of the Office Action cites the following passage and language from Sidewinder in support of Sidewinder's alleged disclosure of "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" element:

> 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).
>
> Office Action, pg. 18.

This passage of Sidewinder cited by the Examiner does not pertain to "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 states that messages can be passed to or forwarded to a System Administrator, kept in a "trash" folder, or discarded. Sidewinder does not teach or suggest "writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message" as recited in claim 17. Since claim 17 recites "writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus" and, as discussed above, Sidewinder does not detect a virus, Sidewinder does not "writ[e] the output of the determining step into the mail message in place of respective encoded portions that contain a virus."

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Sidewinder, and cannot find language to support the conclusions which the Examiner derives from the words in Sidewinder. In sum, Sidewinder does not 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" as recited in claim 17.

VI. The 35 U.S.C. § 103(a) Rejections of Claims 6 and 15 Over Cheswick-Bellovin in View of Sidewinder, in View of MIME*sweeper*, and Further in View of TIS Firewall

Beginning on page 21 of the Office Action, the Examiner rejected claims 6 and 15 under 35 U.S.C. § 103(a) over Cheswick-Bellovin in view of Sidewinder, in view of MIME*sweeper* and further in view of TIS Firewall. Claim 6 depends from claim 5 which, in turn, depends from claim 4. Patentee submits that the rejection of claim 6 cannot properly be maintained for at least the reasons set forth above in Section IV. Claim 15 depends from claim 11. Patentee submits that the rejection of claim 15 cannot properly be maintained for at least the reasons set forth above in Section V.

VII. The 35 U.S.C. § 103(a) Rejections of Claims 9 and 10 Over Cheswick-Bellovin in View of Sidewinder, and Further in View of Ranum[6]

Beginning on page 22 of the Office Action, the Examiner rejected claims 9 and 10 under 35 U.S.C. § 103(a) over Cheswick-Bellovin in view of Sidewinder, and further in view of Ranum. Claims 9 and 10 depend from claim 4. Patentee submits that the rejection of claims 9 and 10 cannot properly be maintained for at least the reasons set forth above in Section IV.

[6] Although the Examiner refers to the TIS Firewall reference as the basis for the rejection in the January 6, 2011 Office Action (*see* pg. 22), the actual quotes from the prior art cited by the Examiner in the Office Action in connection with this rejection are from the Ranum article (and not the TIS Firewall reference). Accordingly, this section of the present Response will refer to the Ranum article, even though the Office Action incorrectly refers to the TIS Firewall reference.

A. Ranum does not disclose "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"

Claim 9 recites the element of "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." The Office Action alleges that Ranum teaches this element. Patentee respectfully disagrees.

Page 23 of the Office Action cites the following passage and language from Ranum in support of Ranum's alleged disclosure of "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" element:

> [Ranum] pg. 41 - The FTP application gateway is a single process that mediates FTP connections between two networks. Routers can control traffic at an IP level, by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level, forcing traffic to move out of the protocol layer for more detailed examination. As an example, the FTP proxy can block FTP export of files while permitting import of files, representing a granularity of control that router-based firewalls cannot presently achieve.
>
> Office Action, pg. 23.

This passage of Ranum cited by the Examiner does not disclose "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." The passage makes no mention of a "server task," or "an FTP daemon," let alone the particular limitation recited: "transferring the data from a server task to an FTP daemon, and then from the FTP daemon to the FTP proxy server."

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Ranum, and cannot find language to support the conclusions which the Examiner derives from the words in Ranum. In sum, Ranum does not disclose "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" as recited in claim 9.

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

Claim 10 recites the element of "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."

Pages 22-23 of the Office Action cite the following passage and language from Ranum in support of Ranum's alleged disclosure of "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" element:

> [Ranum] pg. 41 - The FTP application gateway is a single process that mediates FTP connections between two networks. Routers can control traffic at an IP level, by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level, forcing traffic to move out of the protocol layer for more detailed examination.
>
> Office Action, pp. 22-23.

This passage of Ranum cited by the Examiner does not disclose "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 passage makes no mention of a "proxy server," or "an FTP daemon," let alone the particular limitation recited: "transferring the data from the FTP proxy server to a FTP daemon."

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Ranum, and cannot find language to support the conclusions which the Examiner derives from the words in Ranum. In sum, Ranum does not disclose "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" as recited in claim 10.

VIII. The 35 U.S.C. § 103(a) Rejections of Claims 1-3 and 13 Over Norman in View of Ranum[7]

Beginning on page 24 of the Office Action, the Examiner rejected claims 1-3 and 13 under 35 U.S.C. § 103(a) over Norman in view of Ranum.

As discussed above in Section II, the Examiner has not established that the Norman reference is a printed publication and qualifies as prior art. Accordingly, and for at least this reason, the rejection of claims 1-3 and 13 should be withdrawn.

A. 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"

Claim 1 recites the element of "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

[7] Although the Examiner refers to the TIS Firewall reference as the basis for the rejection in the January 6, 2011 Office Action (*see* pg. 24), the actual quotes from the prior art cited by the Examiner in the Office Action in connection with this rejection are from the Ranum article (and not the TIS Firewall reference). Accordingly, this section of the present Response will refer to the Ranum article, even though the Office Action incorrectly refers to the TIS Firewall reference.

proxy server for receiving the data to be transferred." The Office Action alleges that Ranum teaches this element. Patentee respectfully disagrees.

Pages 26-27 of the Office Action cite the following passage and language from Ranum in support of Ranum's alleged disclosure of "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" element:

> [Ranum] teaches a firewall design in which a sendmail proxy communicates with the SMTP daemon (sendmail server), in order to prevent direct networkcaccess 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 send mail for delivery .... Smap preserves sendmail's functionality, while preventing an arbitrary user on the network from communicating directly with it." ([Ranum], p. 41). [Ranum] 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." ([Ranum], page 37). The diagram of a telnet application proxy on page 38 of [Ranum] shows that an application proxy is distinct from, and communicates with, an application daemon (telnetd server).
>
> Office Action, pp. 26-27.

This passage of Ranum cited by the Examiner is incompatible with, and does not result in the claimed invention. The claimed invention recites the following:

proxy server for ***receiving data to be transferred***, the proxy server scanning the data to be transferred....

a daemon...the data input of the daemon coupled to the data output of the proxy server for ***receiving the data to be transferred***

Accordingly, the present invention recites a proxy server for receiving data to be transferred, a data input of a daemon that receives (the same) data to be transferred, and a data input of the daemon that is coupled to a data output of the proxy server. Ranum does not disclose these features or architecture, as alleged by the Examiner.

Ranum discloses the following:

Figure 1: An Application Proxy

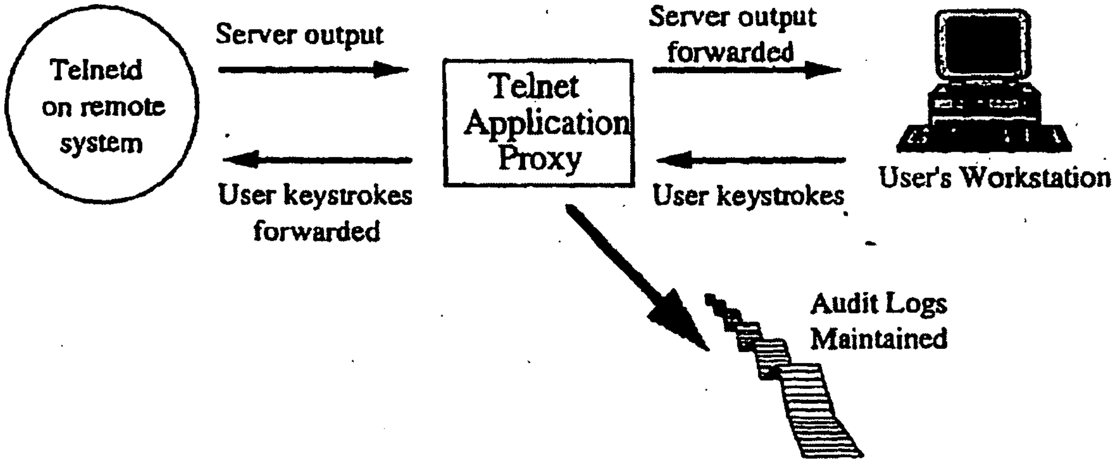


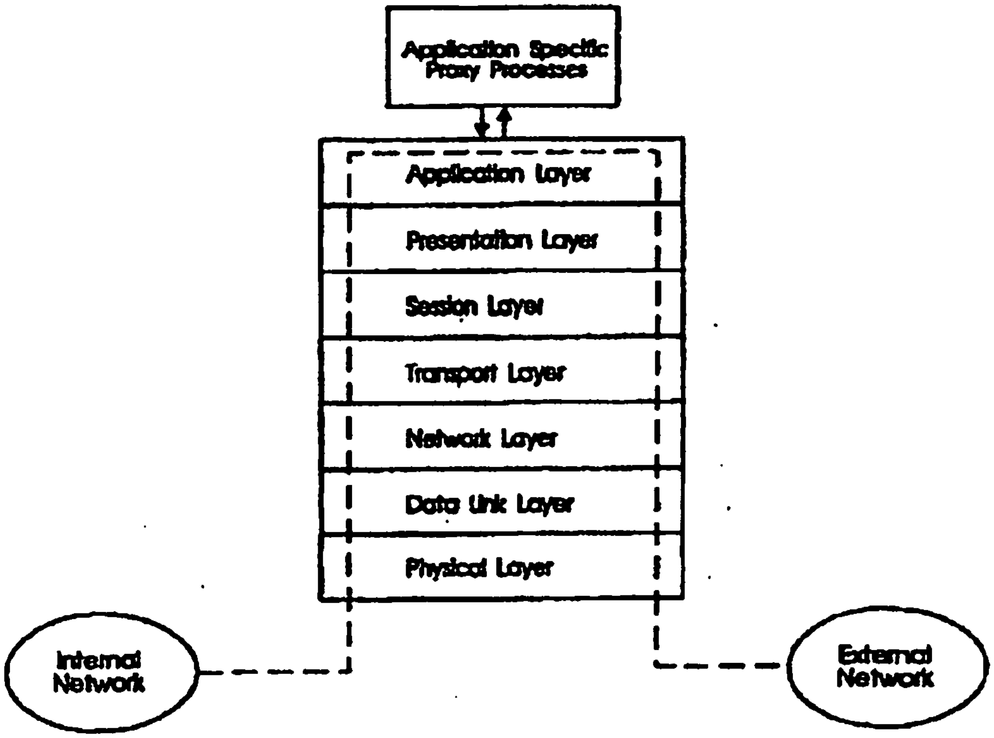
Figure 1, Ranum, pg. 38.

As indicated in the passage above, the Examiner asserts that the Telnetd server (in Figure 1 of Ranum, above) is the daemon. However, such an interpretation and application of Ranum does not result in the claimed invention. There is simply no reason for the Telnetd daemon (shown in Figure 1 of Ranum) to receive data to be transferred from the Telnet Application Proxy (also shown in Figure 1 of Ranum), and then have the Telnet Application Proxy receive that same data, as required by claim 1. Such a configuration would result in a needless transmission of data from the Norman Firewall (or Telnet Application Proxy) to the Telnetd daemon, and does not result in the claimed invention, particularly insofar as Ranum makes clear that the Telnetd daemon does not have a daemon for transferring data ***from*** the Norman Firewall (or from the Telnet Application Proxy) but has a daemon for receiving data on a remote system, as shown above in Figure 1 of Ranum. Mitchell Declaration, ¶¶ 9, 10, 14.

In addition, Patentee respectfully submits that Norman and Ranum cannot properly be combined, and, for this reason as well submits that the Examiner has not established a *prima facie* case of unpatentability. A proposed modification or combination that changes the basic principle under which the primary reference construction was designed to operate is not sufficient to render the claims *prima facie* obvious. M.P.E.P. § 2143.01 VI. (citing *In re Ratti*, 270 F.2d 810, 813 (C.C.P.A. 1959)).

More particularly, Norman provides a technique of connecting from a client to a remote host via a firewall. The firewall of Norman does not, however, provide the illusion of a point-to-point connection. For example, page 8 of Norman discloses that "[o]ne session is established between the internal user and the firewall, and one session is established between the firewall and external host." Norman, pg. 8. Accordingly, the internal user of Norman would not have the illusion of a point-to-point contact with the external network shown in the figure from Norman below. This is apparent because the proxy processes shown in the figure below are above the application layer, which indicates that the internal user of Norman does not have the illusion of a point-to-point connection. Mitchell Declaration, ¶¶ 11, 12.

3.3 Using Proxy processes



In contrast to the technique of Norman, which does not provide the illusion of a point-to-point connection, Ranum discloses a proxy technique that does provide the illusion of a point-to-point connection. For example, Ranum states that "[p]roxies can give the illusion to the software on both sides of a direct point-to-point connection." Ranum, pg. 37. In fact, the Examiner cites this very passage of Ranum on page 27 of the Office Action. Therefore, the basic principle of operation of Norman—where the internal user does not have the illusion of a point-to-point connection—is completely opposite to the operating principle of the system disclosed in Ranum, where the internal user does have the illusion of a point-to-point connection. Mitchell Declaration, ¶ 13.

In contrast to the Examiner's assertion regarding Ranum as applied to claim 1, the claim language at issue above can be illustrated, for example, by the embodiment of Figure 5A (shown below) of the '600 patent.

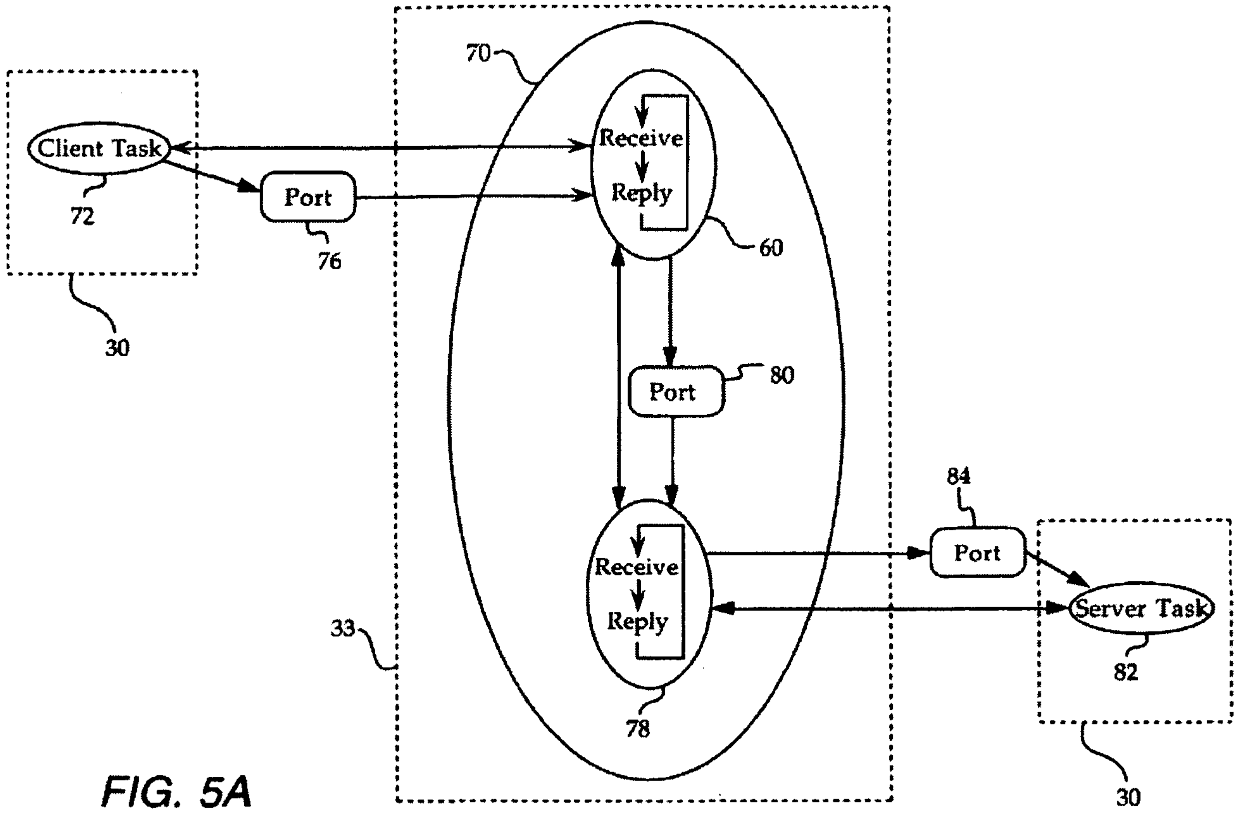


FIG. 5A

Figure 5A shows client task **72** sending files, Internet daemon **70**, FTP proxy server **60**, and FTP daemon **78**. Accordingly, proxy server **60** receives data that is to be transferred to server task **82**, and also scans the data to be transferred. In addition, the data input of FTP daemon **78** is coupled to the data output of the proxy server **60** so that the FTP daemon **78** can receive data to be transferred. *See, e.g.,* '600 patent, Col. 7, Lines 29-45.

In sum, the Examiners proposed combination of Norman and Ranum would, as discussed above, result in a needless transmission of data from the Norman Firewall (or Telnet Application Proxy) to the Telnetd daemon, and does not result in the claimed invention. In contrast, Figure 5A of the '600 patent shows that proxy server **60** receives data that is to be transferred to server task **82**. The '600 patent also shows that the data input of FTP daemon **78** is coupled to the data output of the proxy server **60** so that the FTP daemon **78** can receive data to be transferred.

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Ranum, and cannot find language to support the conclusions which the Examiner derives from the words in Ranum. In sum, 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," as recited in claim 1.

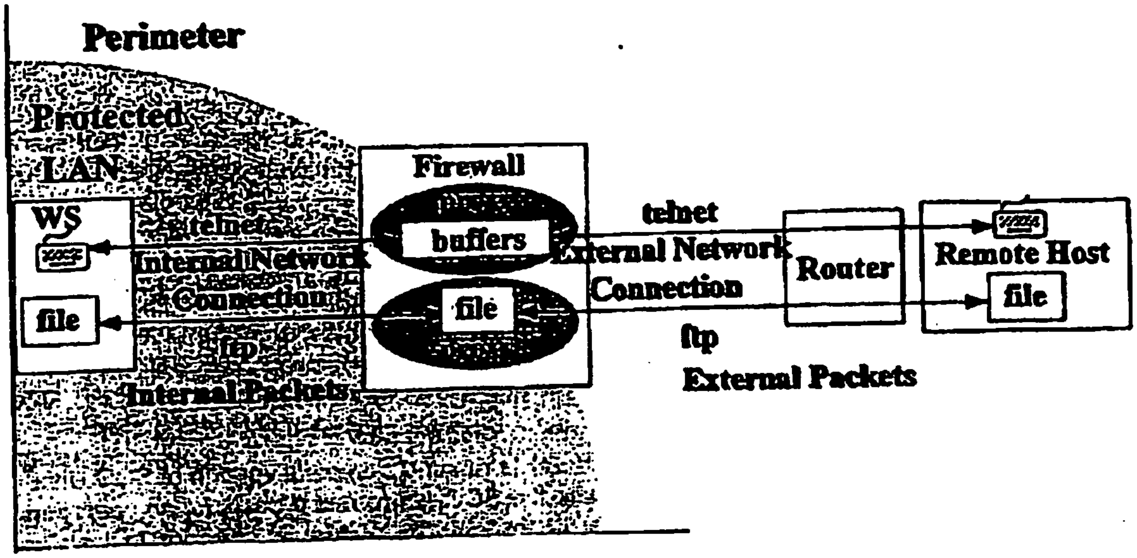
B. Ranum does not disclose "the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address"

Claim 13 recites the element of "the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address." The Office Action alleges that Ranum teaches this element. Patentee respectfully disagrees.

Claim 13 also recites "electronically receiving the mail message at a server." With regard to this limitation, pages 29-30 of the Office Action refer to the following passage of Norman:

> 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).
>
> Office Action, pp. 29-30.

The Figure below is from page 8 of Norman, which illustrates this architecture.



The figure above illustrates how an ftp transaction works through the NORMAN Firewall. A unique feature of the NORMAN Firewall is that it will log into the workstation on the secure network to transfer the requested file.

Thus, according to the Office Action, the Firewall of Norman (shown in the Figure above) corresponds to the "server" recited in claim 13.

Page 31 of the Office Action cites the following passage and language from Ranum in support of Ranum's alleged disclosure of "the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address" element:

> [Ranum] teaches a firewall design in which a sendmail proxy communicates with the SMTP daemon (sendmail server), in order to prevent direct network access to send mail. "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 send mail for delivery [to the destination address]. Smap preserves

> send mail's functionality, while preventing an arbitrary user on the network from communicating directly with it." ([Ranum], page 41). [Ranum] 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." ([Ranum], 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).
>
> Office Action, pg. 31.

Ranum discloses the following:

Figure I: An Application Proxy

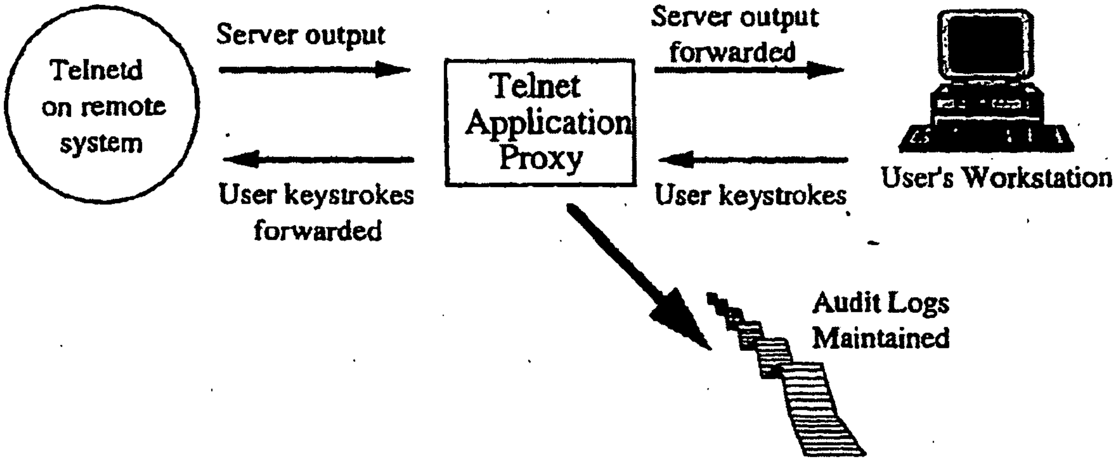


Figure 1, Ranum, pg. 38.

At the outset, Applicants note that Figure 1 of the NORMAN reference illustrates how an FTP transaction works through the NORMAN Firewall. Page 8 of the NORMAN reference also states that the NORMAN Firewall has proxy services for telnet, ftp, and SMTP.

Patentee also notes that Section 4.5 of Norman discusses proxy services as follows:

> The NORMAN Firewall uses nothing but proxy services to pass traffic from one network to the other. No packets will be allowed to pass directly. ***A user on the inside must authenticate himself/herself to the firewall machine by actually logging on to the system.*** NORMAN's security is at work already because the task of authenticating a user is not left to the workstation on the internal net but rather to the B1 firewall system.
>
> After logging on (using telnet), the user is presented with a menu of available services. For the users of this System, there is no way to bypass this menu.
>
> Norman, pg. 7 (emphasis added).

That is, the NORMAN reference teaches that "[a] user on the inside must authenticate himself/herself to the firewall machine by actually logging on to the system." *See,* NORMAN, pg. 7. NORMAN's only illustration of how one logs into the system is provided in the Figure 1 of the NORMAN reference, as set forth above.

As indicated in the passage cited from Ranum above, the Examiner asserts that the Telnetd server is the daemon. However, such an interpretation and application of Ranum does not result in the claimed invention. As shown above in Figure 1 of Ranum, the Telnetd daemon is on a "remote system" and thus cannot reside on the Firewall of Norman (or the Telnet Application Proxy of Ranum).

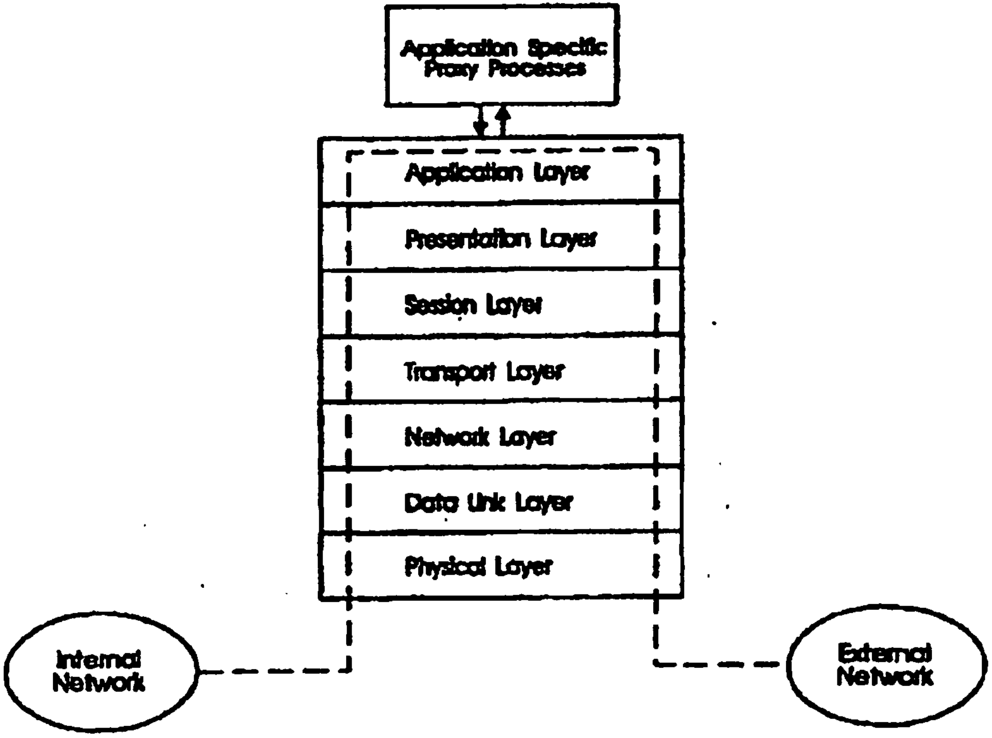
Simply put, the Examiner's assertion that the "remote system" as disclosed in Ranum is the same as the alleged server (i.e., the Norman Firewall) that "electronically receiv[es] the mail message" and that includes an SMPT daemon is incorrect. The Examiner has alleged and indicated that the Norman Firewall server corresponds to the "server" recited in claim 13. From an architectural and operational perspective, it is then, if anything, the Telnet Application Proxy (as shown in Figure 1 of Ranum) that would need to include the SMPT daemon, since it is the Telnet Application Proxy that more closely corresponds to the Norman Firewall that the Examiner has alleged satisfies the "server" recited in claim 13.

The Examiner's position that the Norman Firewall (which the Examiner has stated corresponds to the "server" in claim 13) and the Remote System of Ranum having the Telnetd daemon (which claim 13 also requires the "server" to include—"a SMTP daemon") is a misapplication of the prior art to the claimed invention and does not result in the claimed invention. There is simply no indication of, or any reason why, the Norman Firewall (or Telnet Application Proxy as shown in Figure 1 of Ranum) would transmit a mail message to the Telnetd daemon of Ranum, and then have the Telnetd daemon of Ranum transmit the mail message back to the Telnet Application Proxy of Ranum and then, presumably, to the User's Workstation shown in Figure 1 of Ranum. Such a configuration would result in a needless transmission of data from the Norman Firewall (or Telnet Application Proxy of Ranum) to the Telnetd daemon (of Ranum), particularly insofar as Ranum makes clear that the Telnetd daemon receives data (e.g., on a remote system) on a remote system, but there is no indication that the Telnet daemon transfers that same data "to a node having a destination address matching the destination address," as recited in claim 13. Mitchell Declaration, ¶¶ 9, 10, 14.

In addition, Patentee respectfully submits that Norman and Ranum cannot properly be combined, and, for this reason as well submits that the Examiner has not established a *prima facie* case of unpatentability. A proposed modification or combination that changes the basic principle under which the primary reference construction was designed to operate is not sufficient to render the claims *prima facie* obvious. M.P.E.P. § 2143.01 VI. (citing *In re Ratti*, 270 F.2d 810, 813 (C.C.P.A. 1959)). Mitchell Declaration, ¶ 13.

More particularly, Norman provides a technique of connecting from a client to a remote host via a firewall. The firewall of Norman does not, however, provide the illusion of a point-to-point connection. For example, page 8 of Norman discloses that "[o]ne session is established between the internal user and the firewall, and one session is established between the firewall and external host." Norman, pg. 8. Accordingly, the internal user of Norman would not have the illusion of a point-to-point contact with the external network shown in the figure from Norman below. This is apparent because the proxy processes shown in the figure below are above the application layer, which indicates that the internal user of Norman does not have the illusion of a point-to-point connection. Mitchell, Declaration, ¶ 12.

3.3 Using Proxy processes



In contrast to the technique of Norman, which does not provide the illusion of a point-to-point connection, Ranum discloses a proxy technique that does provide the illusion of a point-to-point connection. For example, Ranum states that "[p]roxies can give the illusion to the software on both sides of a direct point-to-point connection." Ranum, pg. 37. In fact, the Examiner cites this very passage of Ranum on page 27 of the Office Action. Therefore, the basic principle of operation of Norman—where the internal user does not have the illusion of a point-to-point connection—is completely opposite to the operating principle of the system disclosed in Ranum, where the internal user does have the illusion of a point-to-point connection. Mitchell Declaration, ¶ 13.

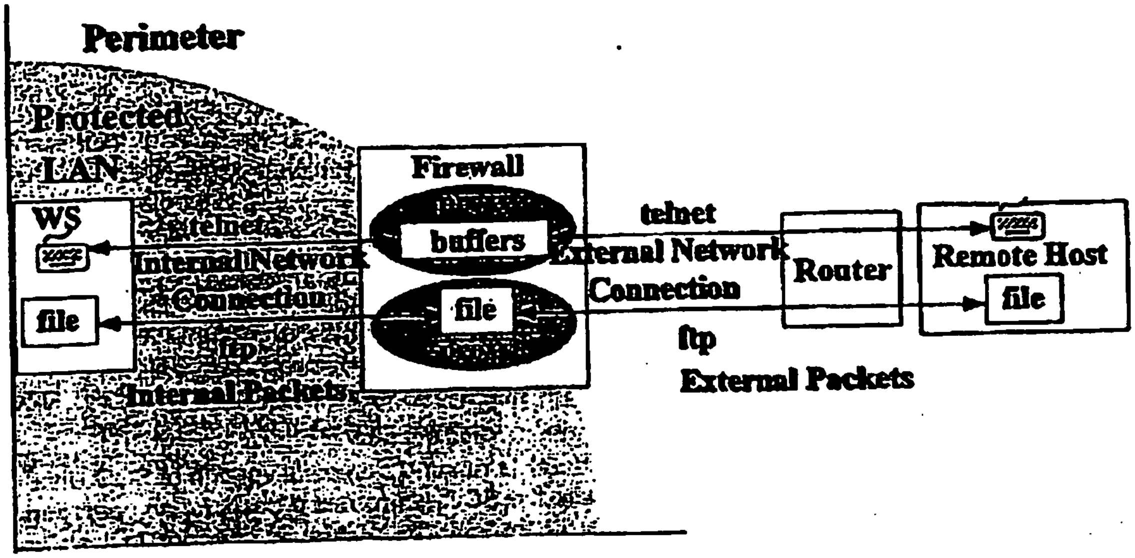
The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Ranum, and cannot find language to support the conclusions which the Examiner derives from the words in Ranum. In sum, Ranum does not disclose "the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address," as recited in claim 13.

IX. The 35 U.S.C. § 103(a) Rejection of Claims 4, 7, 8 and 21 Using Norman In View of Stang

As discussed above in Section II, the Examiner has not established that the Norman reference is a printed publication and qualifies as prior art. Accordingly, and for at least this reason, the rejection of claims 4, 7, 8 and 21 should be withdrawn.

Beginning on page 32 of the Office Action, the Examiner rejected claims 4, 7, 8 and 21 under 35 U.S.C. § 103(a) over Norman in view of *ICSA's Computer Virus Handbook* (hereinafter "Stang"). Even assuming *arguendo* that Norman is prior art (which the Patentee does not accept and has refuted above in Section II), the burden of establishing a *prima facie* case of obviousness based on the above references has not been met, and no rationale exists to support a *prima facie* case of obviousness. Accordingly, the § 103(a) rejection based on Norman in view of Stang is respectfully requested to be withdrawn.

Norman utilizes a proxy server between an internal network and an external network connection. *See*, Norman, pg. 1. The Figure below is from page 8 of Norman, which illustrates this architecture.



The figure above illustrates how an ftp transaction works through the NORMAN Firewall. A unique feature of the NORMAN Firewall is that it will log into the workstation on the secure network to transfer the requested file.

Operationally, Norman checks all incoming files for viruses. For example, Norman states that "...the NORMAN Firewall ***automatically checks every incoming file*** for viruses for letting the file through." Norman, pg. 5 (emphasis added). Norman also states that "[t]he NORMAN Firewall ***scans all incoming files for any of the 7100+ viruses***, and sets them aside for later examination rather than forwarding them, if they are infected. The entire process of store-examination-forward is extremely rapid, and in a typical configuration can process about 86,400 files per day." Norman, pp. 5-6 (emphasis added). Mitchell Declaration, ¶ 15.

In contrast to Norman, Stang is concerned with detecting viruses on a "machine," and not at a firewall as is disclosed in Norman. For example, Stang discloses that "[o]nce in a machine, the virus does nothing until the program is attached to is 'run'."[8]

Moreover, as noted above, the Norman Firewall checks <u>all</u> files. In contrast, Stang states that "...the only files that should never change are the files a virus might infect, and must change during the process." Stang, pg. 114. Stang further discloses that "[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.)." Stang, pg. 5.

On page 34 of the Office Action, the Examiner states:

> 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.
>
> Office Action, pg. 34.

The Patentee respectfully submits that the Examiner's position that "[t]ransmitting data from the server to the destination, without performing virus detection ..." would render the Norman Firewall unsatisfactory or inoperable for its intended purpose, and change the principle of operation of the Norman Firewall which, as discussed above, is to scan all files for viruses at the server (the Norman Firewall). Accordingly, the combination of Norman and Stang as proposed by the Examiner would change the principle of operation of Norman or render the reference inoperable for its intended purpose. M.P.E.P. § 2143.03. Therefore, the basic principle of operation of Norman—which is to scan all files for viruses at the server—is completely opposite to the operating principle

[8] The Examiner also cites this portion of Stang on page 34 of the Office Action.

of the system disclosed in Stang— which scans only certain files for viruses at a personal computer. *See,* M.P.E.P. § 2143.03 V., VI. Mitchell Declaration, ¶¶ 16, 17.

Moreover, since Stang detects viruses on a personal computer, and not on a server as disclosed in Norman, one skilled in the art would understand that files reside on the PCs of Stang for some time in order to allow the method of Stang to monitor files and detect changes in file size. This is in sharp contrast to 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." Norman, pp, 5-6. Therefore, another operating principle of Norman—to scan all files for viruses in an extremely rapid manner—is completely opposite to the operating principle of the system disclosed in Stang, which is to take a period of time to monitor, compare and detect changes in file size over time. For this reason as well, incorporating the technique of Stang into the system disclosed in Norman as suggested by the Examiner would require a change in the basic principle under which the system of Norman was designed to operate. *See,* M.P.E.P. § 2143.03 V., VI. Mitchell Declaration, ¶ 18.

Accordingly, the teaching away in Stang from searching all files for viruses as disclosed in Norman, and the teaching away in Stang from providing a virus detection technique that would occur in an "extremely rapid" manner as disclosed in Norman, would cause one of ordinary skill to look away from Stang, rather than to combine Stang with Norman. Because it is improper to combine references where the references teach away from their combination, the rejection of claims 4, 7-8 and 21 as set forth on pages 32-36 of the Office Action should be withdrawn for at least these reasons. *See* M.P.E.P. § 2145 X. D.

X. The 35 U.S.C. § 103(a) Rejection of Claims 5 and 6 Using Norman In View of Stang and Further in View of Warner

Beginning on page 36 of the Office Action, the Examiner rejected claims 5 and 6 under 35 U.S.C. § 103(a) over Norman in view of Stang and further in view of *VIRUS-L mailing list dated May 18, 1990,* VIRUS-L Digest, vol. 3, no. 99, May 21, 1990 (hereinafter "Warner"). The rejection of claims 5 and 6 should be withdrawn for at least the reasons set forth above in Section II, since there in no evidence that Norman is a printed publication.

In addition, the combination of Norman, Stang and Warner cannot stand because, as Patentee has discussed above in Section IX, combining Stang with Norman would change at least two basic principles of operation of Norman: i) scanning all files for viruses at the server; and ii) accomplishing the scanning in an extremely rapid manner.

In addition, on page 37 of the Office Action, the Examiner states that Warner "searches the compressed file for .EXE, .COM, .OBJ, and .SYS files, then uncompresses them into a temporary file and scans that temp file." However, the Examiner's citation of Warner omits a critical sentence that indicates that Warner's operability is in question and that Warner therefore does not provide an enabling disclosure. What Warner actually discloses is the following:

> If I understand its functioning correctly what actually occurs is that it searches the compressed file for .EXE, .COM, .OBJ, and .SYS files, then uncompresses them into a temporary file and scans that temp file. ***I am not sure on that.***"
>
> Warner, pg. 2.

According to the M.P.E.P.:

> A reference contains an "enabling disclosure" if the public was in possession of the claimed invention before the date of invention. "Such possession is effected if one of ordinary skill in the art could have combined the publication's description of the invention with his [or her] own knowledge to make the claimed invention." *In re Donohue*, 766 F.2d 531, 226 USPQ 619 (Fed. Cir. 1985).
>
> M.P.E.P. § 2121.01.

Here, the Examiner has provided no evidence that one skilled in that art "could have combined the publication's description of the invention with his [or her] own knowledge to make the claimed invention," as required by the M.P.E.P, particularly since the author of Warner is "not sure" how the referenced software operates. Patentee respectfully that if the author of Warner is "not sure" how the software operates, then the Examiner and the Patentee cannot be sure either. Accordingly, the Examiner has not set forth a *prima facie* case of obviousness.

Moreover, it appears that Warner, like Stang, operates on a PC, and not on a server. This is in contradistinction to the language of claim 5, which recites "storing the data in a temporary file ***at the server***..." Claim 5 of the '600 patent, emphasis added. The Examiner's assertion that Warner discloses "storing the data in a temporary file at the server" is therefore incorrect and inapposite. Because Warner, like Stang, operates on a PC and not on a server, the Warner reference suffers from the same infirmities as Stang, and there would be no motivation to combine Warner with Norman for the same or substantially same reasons as set forth above in Section IX. Mitchell Declaration, ¶ 19.

Even assuming *arguendo* that Norman is prior art (which the Patentee does not accept and has refuted above), the burden of establishing a *prima facie* case of obviousness based on the above references has not been met, and no rationale exists to support a *prima facie* case of obviousness. Accordingly, the § 103(a) rejection based on Norman in view of Stang and further in view of Warner is respectfully requested to be withdrawn.

For at least these reasons, the features recited in claim 5 have not been met. Accordingly, the Examiner is requested to withdraw the rejection of claim 5, and claim 6 which depends therefrom.

XI. The 35 U.S.C. § 103(a) Rejection of Claims 9 and 10 Using Norman In View of Stang and Further in View of Ranum[9]

On pages 37-41 of the Office Action, the Examiner rejected claims 9 and 10 under 35 U.S.C. § 103(a) over Norman in view of Stang and further in view of Ranum. The rejection of claims 9 and 10 should be withdrawn for at least the reasons set forth above in Section II, since there is no evidence that Norman is a printed publication.

[9] Although the Examiner refers to the TIS Firewall reference as the basis for the rejection in the January 6, 2011 Office Action (*see* pg. 37), the actual quotes from the prior art cited by the Examiner in the Office Action in connection with this rejection are from the Ranum article (and not the TIS Firewall reference). Accordingly, this section of the present Response will refer to the Ranum article, even though the Office Action incorrectly refers to the TIS Firewall reference.

In addition, the combination of Norman, Stang and Warner cannot stand because, as Patentee has discussed above in Section IX, combining Stang with Norman would change at least two basic principles of operation of Norman: i) scanning all files for viruses at the server; and ii) accomplishing the scanning in an extremely rapid manner.

A. Ranum does not disclose "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"

Claim 9 recites the element 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." The Office Action alleges that Ranum teaches this element. Patentee respectfully disagrees.

Pages 38-39 of the Office Action cites the following passage and language from Ranum in support of Ranum's alleged disclosure 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" element:

> A "bastion host provides application-level control" ([Ranum], p. 39). "The FTP application gateway is a single process that mediates FTP connections between two networks." ([Ranum], 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." ([Ranum], pp. 41-42). Regarding proxies generally, [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], 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] 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], p. 38; the WUArchive ftpd is referenced on p. 44 as an "FTP server daemon".
>
> Office Action, pp. 38-39.

This passage of Ranum cited by the Examiner does not disclose "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." This passage of Ranum cited by the Examiner is incompatible with, and does not result in the claimed invention. The claimed invention recites the following:

> electronically receiving data at ***the server*** [claim 4];
> wherein the ***server is a FTP proxy server***; [claim 9]
> wherein the step of electronically receiving data comprises the steps of ***transferring the data <u>from</u> a server task <u>to</u> an FTP daemon***, and then ***<u>from</u> the FTP daemon <u>to</u> the FTP proxy server*** if the data is being transferred into the first network [claim 9]

Accordingly, the present invention requires electronically receiving data at a FTP proxy server, wherein the step of electronically receiving data (at the FTP proxy server) comprises i) transferring data from a server task to an FTP daemon, and then ii) from the FTP daemon to the FTP proxy server. That is, the claim language requires that that the FTP proxy server (e.g., the Norman Firewall) include the FTP daemon. Accordingly, the FTP daemon cannot reside on a remote server as shown in Figure 1 of Ranum, and as alleged by the Examiner.

Ranum does not disclose these features or architecture, and the combination of Norman, Stang and Ranum does not result in the claimed invention, as alleged by the Examiner.

Instead, Ranum discloses the following:

Figure 1: An Application Proxy

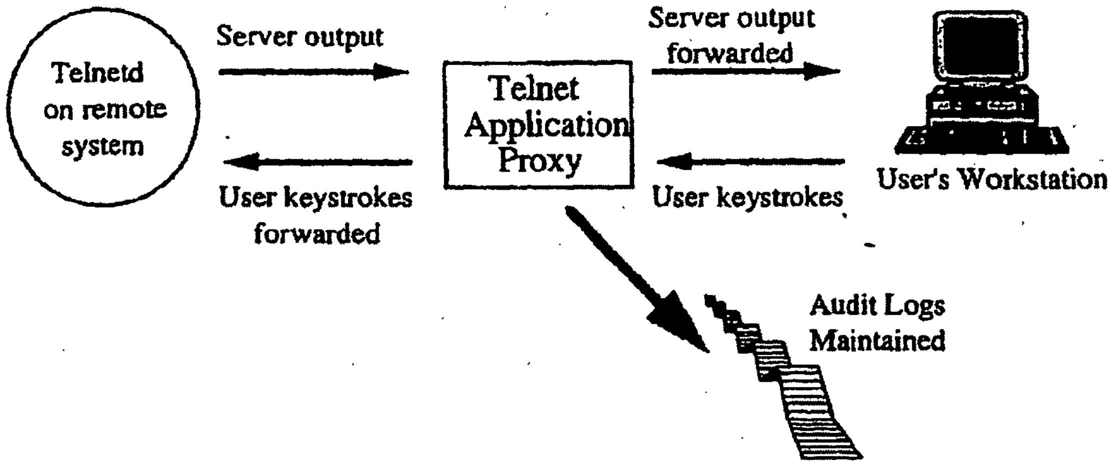
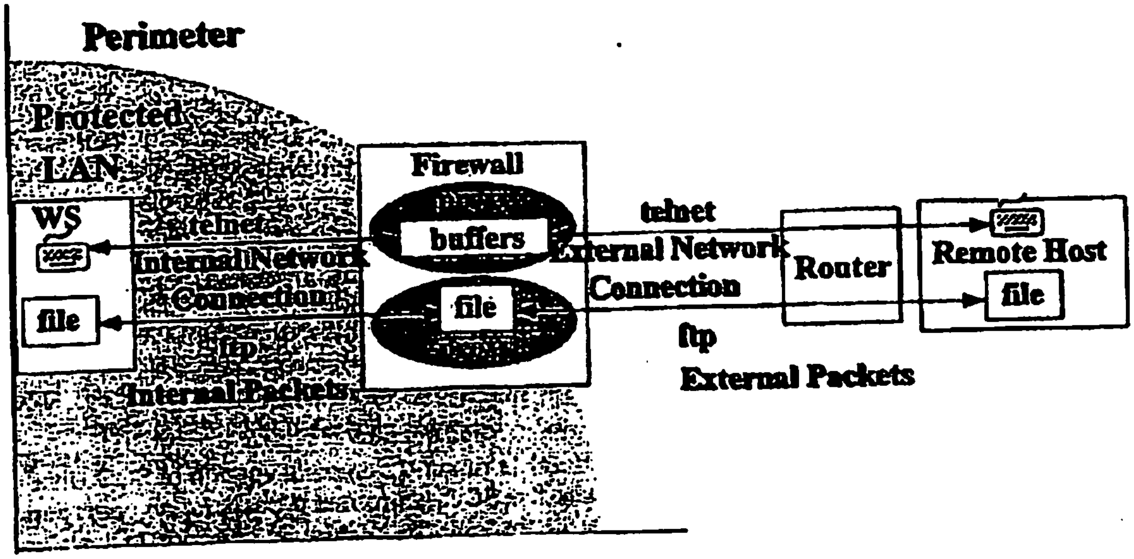


Figure 1, Ranum, pg. 38.

As indicated in the passage above, the Examiner asserts that the Firewall / proxy server disclosed in Figure 1 of Norman (below) is the recited "FTP proxy server." *See*, Office Action. pg. 38. Accordingly, it is the Firewall / proxy server shown in Figure 1 of Norman that electronically receives data comprising "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," as recited in claim 9.



The figure above illustrates how an ftp transaction works through the NORMAN Firewall. A unique feature of the NORMAN Firewall is that it will log into the workstation on the secure network to transfer the requested file.

The Examiner also asserts that the Telnetd server (in Figure 1 of Ranum, above) is the FTP daemon. *See*, Office Action, pg. 39. However, in contrast to the Examiner's allegation, the claim language requires that the FTP proxy server (e.g., the Norman Firewall) include the FTP daemon. Accordingly, the FTP daemon cannot reside on a remote server as shown in Figure 1 of Ranum, and as alleged by the Examiner.

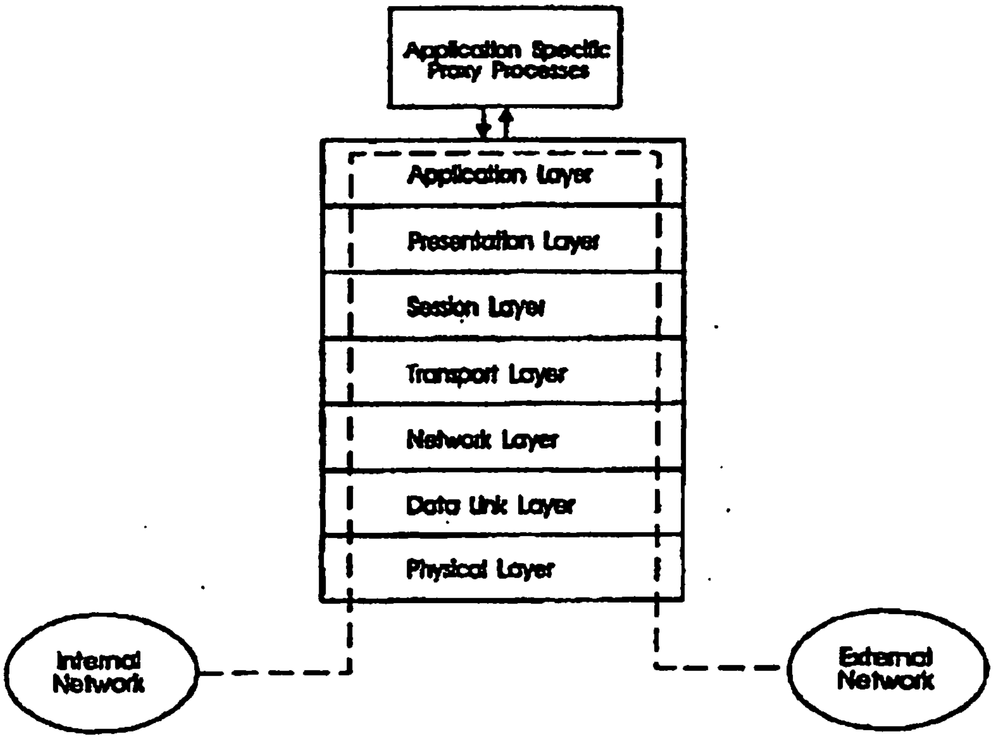
More particularly, claim 9 requires electronically receiving data at the server, and that the receiving step comprises ***"transferring the data from a server task to an FTP daemon***, and then ***from the FTP daemon to the FTP proxy server*** if the data is being transferred into the first network." Accordingly, the claim language requires that the FTP server i) transfer the data from a server task to an FTP daemon, and then ii) from the FTP daemon to the FTP proxy server if the data is being transferred into the first network.

As noted above, the Examiner alleges that the Telnetd server (in Figure 1 of Ranum, above) is the FTP daemon. *See*, Office Action, pg. 39. However, as shown in Figure 1 of Ranum above, the FTP daemon (or Telnetd daemon) is on a remote server. Accordingly, the FTP daemon (or Telnetd daemon) does not reside on the Firewall of Norman as alleged by the Examiner, since claim 9 requires that the electronically receiving data at the FTP proxy server include transferring data to an FTP daemon that resides on the FTP server. Mitchell Declaration, ¶ 10.

In addition, Patentee respectfully submits that Norman and Ranum cannot properly be combined, and, for this reason as well submits that the Examiner has not established a *prima facie* case of unpatentability. A proposed modification or combination that changes the basic principle under which the primary reference construction was designed to operate is not sufficient to render the claims *prima facie* obvious. M.P.E.P. § 2143.01 VI. (citing *In re Ratti*, 270 F.2d 810, 813 (C.C.P.A. 1959)).

More particularly, Norman provides a technique of connecting from a client to a remote host via a firewall. The firewall of Norman does not, however, provide the illusion of a point-to-point connection. For example, page 8 of Norman discloses that "[o]ne session is established between the internal user and the firewall, and one session is established between the firewall and external host." Norman, pg. 8. Accordingly, the internal user of Norman would not have the illusion of a point-to-point contact with the external network shown in the figure from Norman below. This is apparent because the proxy processes shown in the figure below are above the application layer, which indicates that the internal user of Norman does not have the illusion of a point-to-point connection. Mitchell, Declaration, ¶ 12.

3.3 Using Proxy processes



In contrast to the technique of Norman, which does not provide the illusion of a point-to-point connection, Ranum discloses a proxy technique that does provide the illusion of a point-to-point connection. For example, Ranum states that "[p]roxies can give the illusion to the software on both sides of a direct point-to-point connection." Ranum, pg. 37. In fact, the Examiner cites this very passage of Ranum on page 27 of the Office Action. Therefore, the basic principle of operation of Norman—where the internal user does not have the illusion of a point-to-point connection—is completely opposite to the operating principle of the system disclosed in Ranum, where the internal user does have the illusion of a point-to-point connection. Mitchell Declaration, ¶ 13.

In contrast to the Examiner's assertion regarding Ranum as applied to claim 9, the claim language at issue above can be illustrated, for example, by the embodiment of Figure 5B (shown below) of the '600 patent.

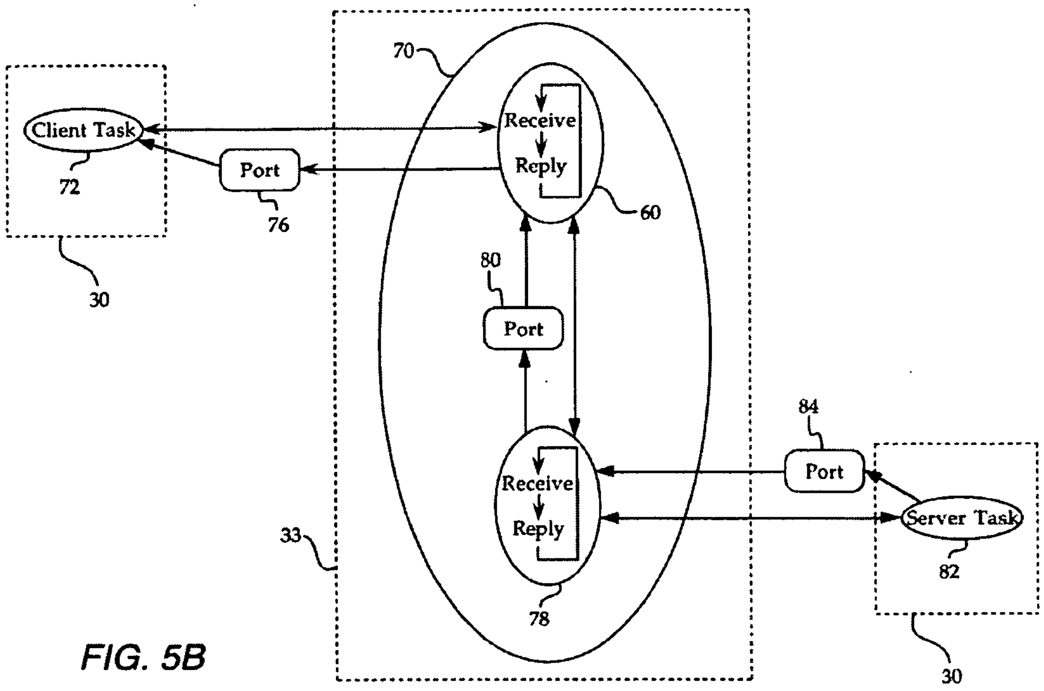


FIG. 5B

Figure 5B shows client task **72** receiving files, Internet daemon **70**, FTP proxy server **60**, and FTP daemon **78**. Accordingly, server task **82** transmits data to FTP daemon **78**, and FTP daemon **78** transmits data to FTP proxy server **60** if the data is being transferred into the first network (e.g., to client task 72). *See*, *e.g.*, '600 patent, column 8, lines 40 - Column 9, line 27.

In sum, the FTP daemon (or Telnetd daemon) does not reside on the Firewall of Norman as alleged by the Examiner, and as required by claim 9. In contrast, Figure 5B of the '600 patent shows client task **72** receiving files, Internet daemon **70**, FTP proxy server **60**, and FTP daemon **78**. Server task **82** transmits data to FTP daemon **78** (of gateway node **33**), and FTP daemon **78** (of gateway node **33**) transmits data to FTP proxy server **60** (of gateway node **33**) if the data is being transferred into the first network (e.g., to client task 72).

The Patentee has thoroughly reviewed the Examiner's comments, has read the cited pages in Ranum, and cannot find language to support the conclusions which the Examiner derives from the words in Ranum. In sum, Ranum does not disclose "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" as recited in claim 9. Ranum does not disclose "wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network."

Claim 10 recites the element of "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."

Pages 40-41 of the Office Action cite the following passage and language from Ranum in support of Ranum's alleged disclosure of "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" element:

> [Ranum] 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; the FTP daemon necessarily transmits imported files to an internal node or file server. A "bastion host provides application-level control" ([Ranum], p. 39). "The FTP application gateway is a single process that mediates FTP connections between two networks." ([Ranum], 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." ([Ranum], pp. 41-42). Regarding proxies generally, [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], 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] 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], p. 38; the WUArchive ftpd is referenced on p. 44 as an "FTP server daemon")
>
> Office Action, pp. 40-41.

This passage of Ranum cited by the Examiner does not disclose "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." This passage of Ranum cited by the Examiner is incompatible with, and does not result in the claimed invention. The claimed invention recites the following:

> electronically receiving data at ***the server*** [claim 4];
> ***sending the data*** to the destination address if the data does not contain a virus; [claim 4];
> wherein the ***server is a FTP proxy server***; [claim 10]
> wherein the step of ***sending the data*** to the destination address comprises ***transferring the data <u>from</u> the FTP proxy server <u>to</u> a FTP daemon***, and then ***<u>from</u> an FTP daemon <u>to</u> a node having the destination address***, if the data is not being transferred into the first network [claim 10]

Accordingly, the present invention requires electronically receiving data at a FTP proxy server, wherein the step of electronically sending the data (from the FTP proxy server) comprises i) transferring the data from the FTP proxy server to a FTP daemon, and then ii) from an FTP daemon to a node having the destination address. That is, the claim language requires that that the FTP proxy server (e.g., the Norman Firewall) include the FTP daemon. Accordingly, the FTP daemon cannot reside on a remote server as shown in Figure 1 of Ranum, and as alleged by the Examiner.

Ranum does not disclose these features or architecture, and the combination of Norman, Stang and Ranum does not result in the claimed invention, as alleged by the Examiner.

Ranum discloses the following:

Figure 1: An Application Proxy

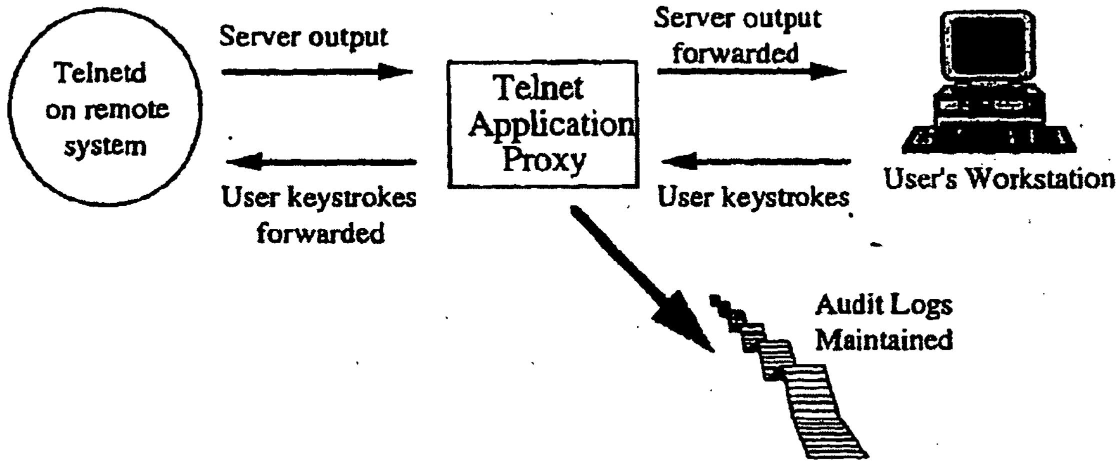
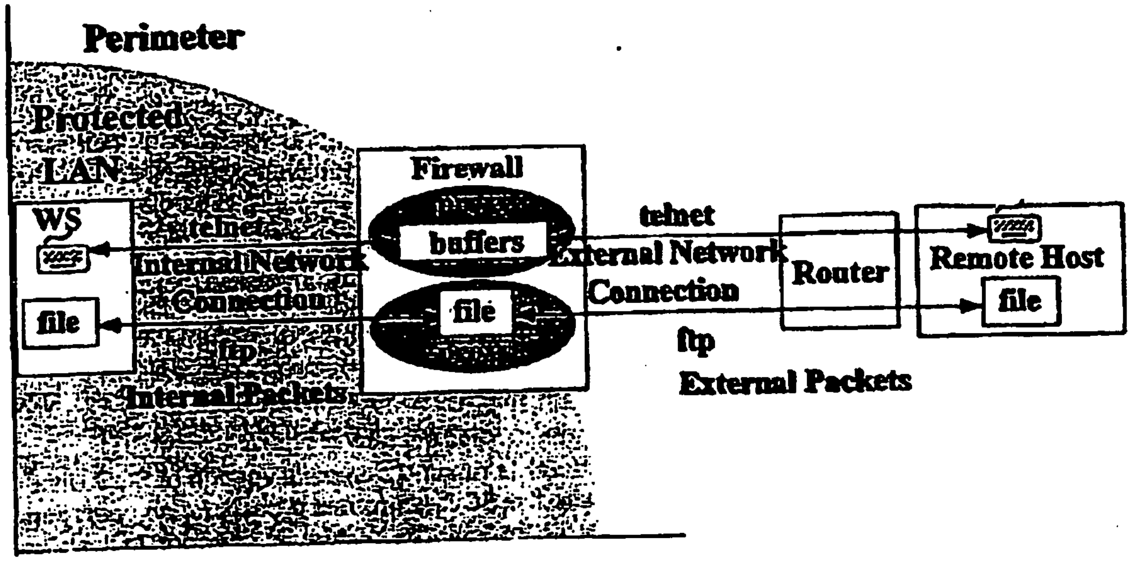


Figure 1, Ranum, pg. 38.

The Examiner asserts that the Firewall / proxy server disclosed in Figure 1 of Norman (below) is the recited "FTP proxy server." *See*, Office Action. pg. 39. Accordingly, it is the Firewall / proxy server shown in Figure 1 of Norman that transfers "***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," as recited in claim 10.



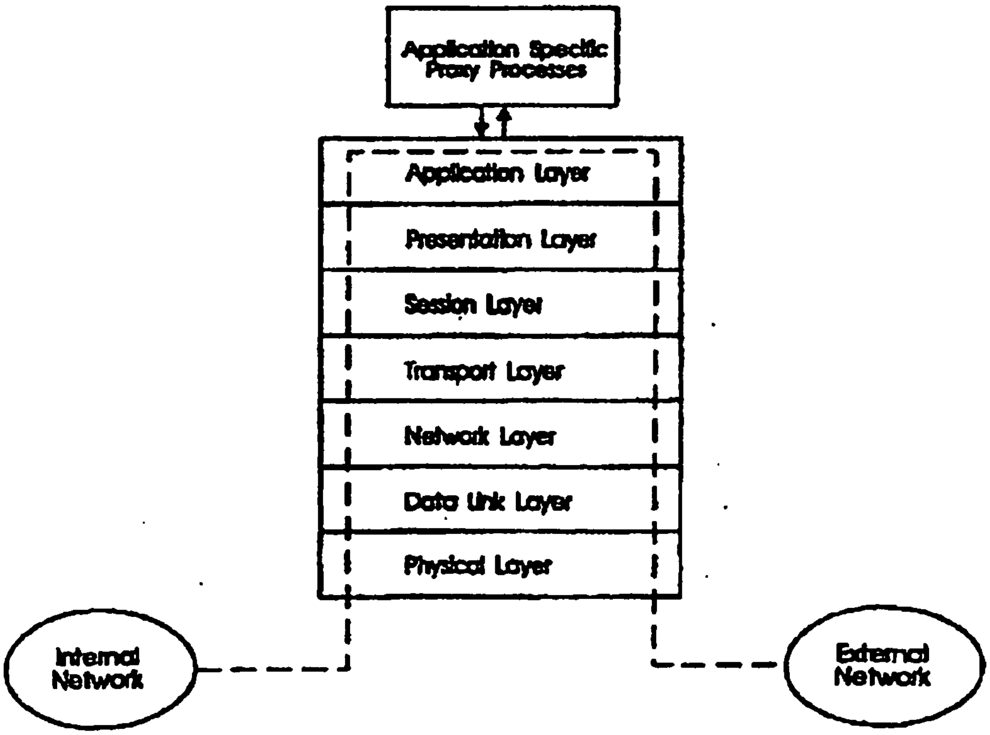
The figure above illustrates how an ftp transaction works through the NORMAN Firewall. A unique feature of the NORMAN Firewall is that it will log into the workstation on the secure network to transfer the requested file.

The Examiner also asserts that the Telnetd server (in Figure 1 of Ranum, above) is the FTP daemon. *See*, Office Action, pp. 40-41. However, in contrast to the Examiner's allegation, the claim language requires that the FTP proxy server (e.g., the Norman Firewall) include the FTP daemon. Accordingly, the FTP daemon cannot reside on a remote server as shown in Figure 1 of Ranum, and as alleged by the Examiner, since claim 10 requires that the electronically receiving data at the proxy server include transferring data to an FTP daemon that resides on the FTP server. Mitchell Declaration, ¶ 10.

In addition, Patentee respectfully submits that Norman and Ranum cannot properly be combined, and, for this reason as well submits that the Examiner has not established a *prima facie* case of unpatentability. A proposed modification or combination that changes the basic principle under which the primary reference construction was designed to operate is not sufficient to render the claims *prima facie* obvious. M.P.E.P. § 2143.01 VI. (citing *In re Ratti*, 270 F.2d 810, 813 (C.C.P.A. 1959)).

More particularly, Norman provides a technique of connecting from a client to a remote host via a firewall. The firewall of Norman does not, however, provide the illusion of a point-to-point connection. For example, page 8 of Norman discloses that "[o]ne session is established between the internal user and the firewall, and one session is established between the firewall and external host." Norman, pg. 8. Accordingly, the internal user of Norman would not have the illusion of a point-to-point contact with the external network shown in the figure from Norman below. This is apparent because the proxy processes shown in the figure below are above the application layer, which indicates that the internal user of Norman does not have the illusion of a point-to-point connection. Mitchell, Declaration, ¶ 10.

3.3 Using Proxy processes



In contrast to the technique of Norman, which does not provide the illusion of a point-to-point connection, Ranum discloses a proxy technique that does provide the illusion of a point-to-point connection. For example, Ranum states that "[p]roxies can give the illusion to the software on both sides of a direct point-to-point connection." Ranum, pg. 37. In fact, the Examiner cites this very passage of Ranum on page 27 of the Office Action. Therefore, the basic principle of operation of Norman—where the internal user does not have the illusion of a point-to-point connection—is completely opposite to the operating principle of the system disclosed in Ranum, where the internal user does have the illusion of a point-to-point connection. Mitchell Declaration, ¶¶ 12, 13.

In contrast to the Examiner's assertion regarding Ranum as applied to claim 10 the claim language at issue above can be illustrated, for example, by the embodiment of Figure 5A (shown below) of the '600 patent.

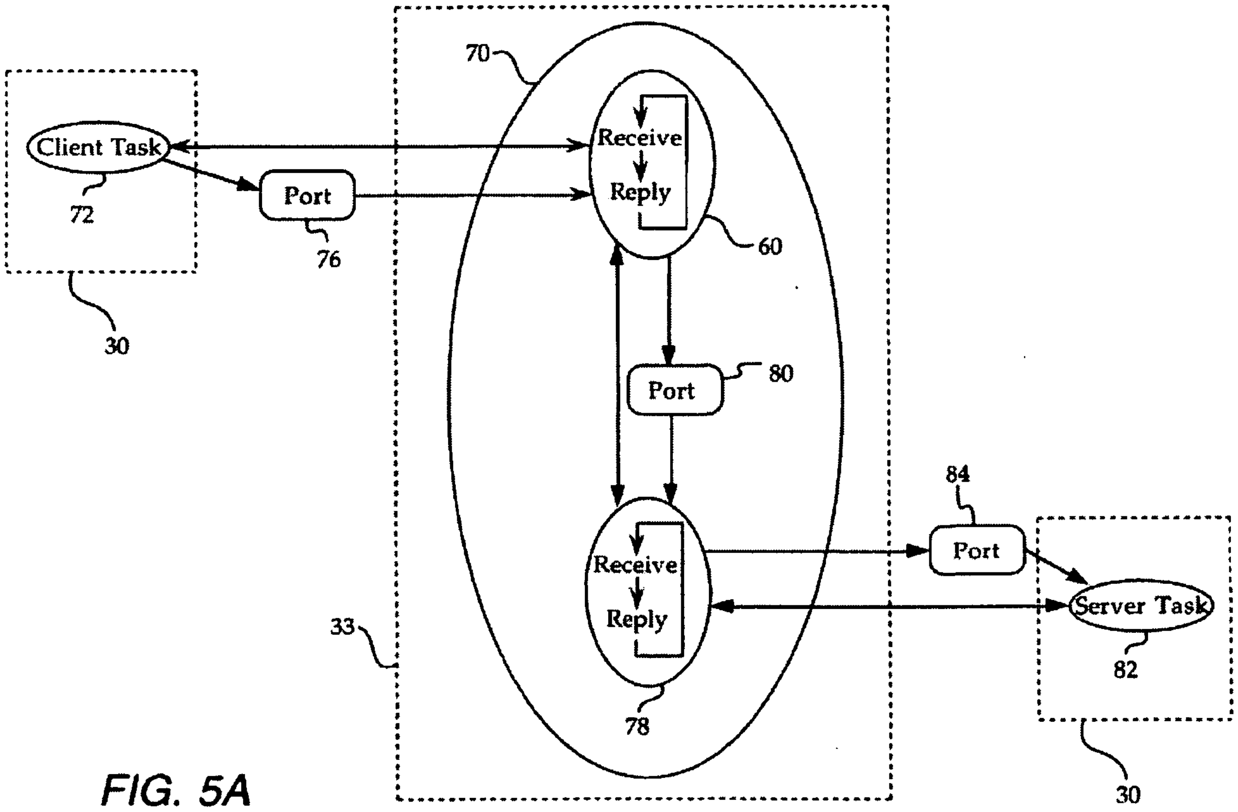


FIG. 5A

Figure 5A shows client task **72** sending data, to FTP proxy server **60**, and then to FTP daemon **78**. In turn, FTP daemon **78** sends the data to server task **82** if the data is being transferred out of the network. *See*, *e.g.*, '600 patent, column 7, lines 29-51.

For at least these reasons, the features recited in claims 9 and 10 have not been met. Accordingly, the Examiner has not established a *prima facie* case of obviousness, and the rejection cannot properly be maintained.

XII. The 35 U.S.C. § 103(a) Rejection of Claims 11, 12 and 14-17 Using Norman In View of Warner

Beginning on page 41 of the Office Action, the Examiner rejected claims 11, 12 and 14-17 under 35 U.S.C. § 103(a) over Norman in view of Warner. The rejection of claims 11, 12 and 14-17 should be withdrawn for at least the reasons set forth above in Section II, since there is no evidence that Norman is a printed publication.

A. Warner does not 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"

On page 43 of the Office Action, the Examiner states that Warner "searches the compressed file for .EXE, .COM, .OBJ, and .SYS files, then uncompresses them into a temporary file and scans that temp file." However, the Examiner's citation of Warner omits a critical sentence that indicates that Warner's operability is in question and that Warner therefore does not provide an enabling disclosure. What Warner actually discloses is the following:

> If I understand its functioning correctly what actually occurs is that it searches the compressed file for .EXE, .COM, .OBJ, and .SYS files, then uncompresses them into a temporary file and scans that temp file. ***I am not sure on that.***"
>
> Warner, pg. 2.

According to the M.P.E.P.:

> A reference contains an "enabling disclosure" if the public was in possession of the claimed invention before the date of invention. "Such possession is effected if one of ordinary skill in the art could have combined the publication's description of the invention with his [or her] own knowledge to make the claimed invention." *In re Donohue*, 766 F.2d 531, 226 USPQ 619 (Fed. Cir. 1985).

M.P.E.P. § 2121.01.

Here, the Examiner has provided no evidence that one skilled in that art "could have combined the publication's description of the invention with his [or her] own knowledge to make the claimed invention," as required by the M.P.E.P, particularly since the author of Warner is "not sure" how the referenced software operates. Patentee respectfully that if the author of Warner is "not sure" how the software operates, then the Examiner and the Patentee cannot be sure either. Accordingly, the Examiner has not set forth a *prima facie* case of obviousness.

B. Neither Norman nor Warner discloses "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 the element of "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." Pages 44-46 of the Office Action do not allege that Norman or Warner disclose this element, and provide no citation to Norman or Warner in support of this element. As such, the Examiner has not established a *prima facie* case of unpatentability, and the rejection cannot properly be maintained.

C. Norman does not 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 "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." Page 46 of the Office Action alleges the following basis as to why it would have allegedly been obvious to modify Norman to arrive at the claimed "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" element recited in claim 17.

> 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 mail 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.
>
> Office Action, pg. 46.

The Examiner acknowledges that Norman doses not 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." Accordingly, the Examiner's unsubstantiated conclusion as articulated on page 46 of the Office Action appears to be within the personal knowledge of the Examiner. Patentee requests that the Examiner either provide a reference that discloses "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," or provide an affidavit indicating same. In the absence of either, Applicants request that the Examiner withdraw the rejection of claim 17. *See,* M.P.E.P. § 2144.03 C.; 37 C.F.R. § 1.104(d)(2).

III. Conclusion

Patentee believes that a full and complete response has been made to the Office Action. In view of the foregoing amendments and remarks, Patentee requests withdrawal of all outstanding rejections and confirmation of the patentability of claims 1-37. Favorable consideration of this Response is respectfully requested.

Dated: March 4, 2011

Respectfully submitted,

By Andrea G Reist

Andrea G. Reister
    Registration No.: 36,253
Gregory S. Discher
    Registration No.: 42,488
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401
(202) 662-6000
Attorneys for Patentee