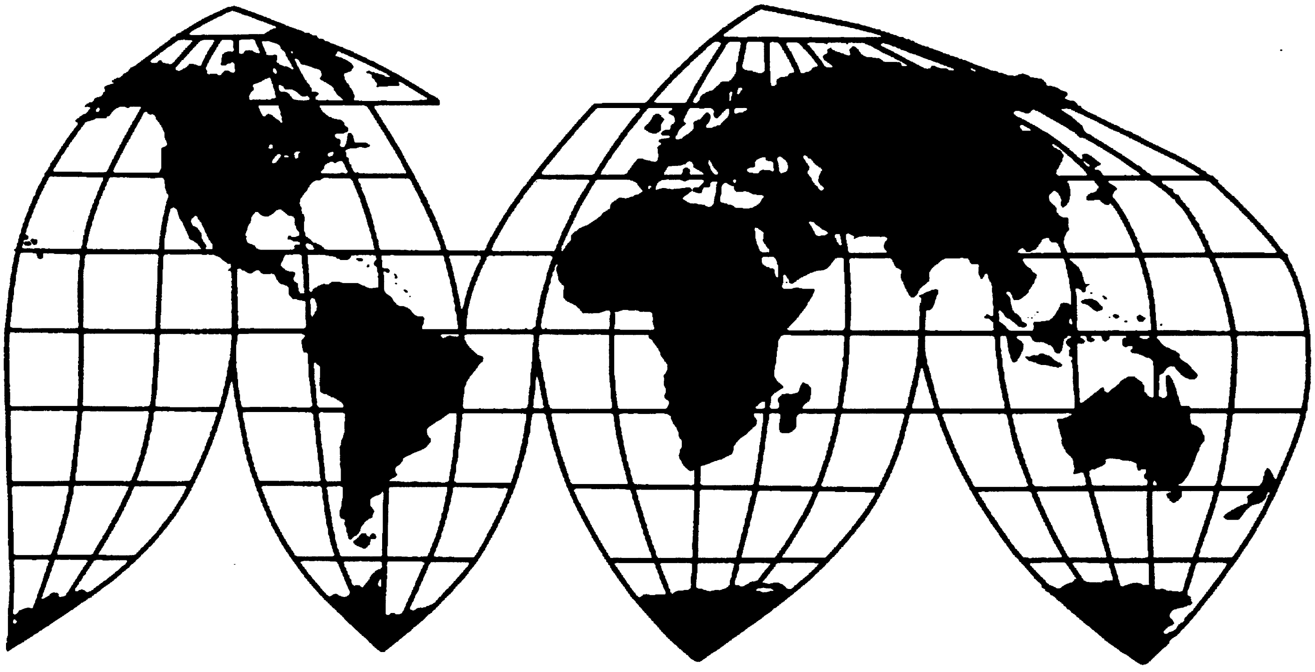
In the Matter of

Certain Systems for Detecting and Removing Viruses or Worms, Components Thereof, and Products Containing Same

Investigation No. 337-TA-510

Publication 3936 July 2007

U.S. International Trade Commission



Washington, DC 20436

U.S. International Trade Commission

COMMISSIONERS

Daniel R. Pearson, Chairman
Shara L. Aranoff, Vice Chairman
Deanna Tanner Okun
Charlotte R. Lane
Irving A. Williamson
Dean A. Pinkert

Address all communications to
Secretary to the Commission
United States International Trade Commission
Washington, DC 20436

U.S. International Trade Commission

Washington, DC 20436
www.usitc.gov

In the Matter of

Certain Systems for Detecting and Removing Viruses or Worms, Components Thereof, and Products Containing Same

Investigation No. 337-TA-510

UNITED STATES INTERNATIONAL TRADE COMMISSION

Publication 3936

July 2007

UNITED STATES INTERNATIONAL TRADE COMMISSION
Washington, D.C. 20436

In the Matter of

SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME

Inv. No. 337-TA-510
Consolidated Enforcement and Advisory Opinion Proceeding

COMMISSION DETERMINATION NOT TO REVIEW AN INITIAL DETERMINATION TERMINATING THE CONSOLIDATED ENFORCEMENT AND ADVISORY OPINION PROCEEDING; RESCISSION OF THE LIMITED EXCLUSION ORDER AND CEASE AND DESIST ORDER ISSUED IN THE UNDERLYING INVESTIGATION; VACATUR OF A SUMMARY INITIAL DETERMINATION ISSUED IN THE CONSOLIDATED ENFORCEMENT AND ADVISORY OPINION PROCEEDING

AGENCY: U.S. International Trade Commission.

ACTION: Notice.

SUMMARY: Notice is hereby given that the U.S. International Trade Commission has determined not to review an initial determination ("ID") issued by the presiding administrative law judge ("ALJ") terminating the above-captioned proceeding. The Commission has also determined to rescind the limited exclusion and cease and desist orders previously issued in the underlying investigation and to vacate a summary ID previously issued in the proceeding.

FOR FURTHER INFORMATION CONTACT: Timothy P. Monaghan, Esq., Office of the General Counsel, U.S. International Trade Commission, 500 E Street, S.W., Washington, D.C. 20436, telephone 202-205-3152. Copies of the public version of the ID and all nonconfidential documents filed in connection with this investigation are or will be available for inspection during official business hours (8:45 a.m. to 5:15 p.m.) in the Office of the Secretary, U.S. International Trade Commission, 500 E Street, S.W., Washington, D.C. 20436, telephone 202-205-2000. Hearing-impaired persons are advised that information on this matter can be obtained by contacting the Commission's TDD terminal on 202-205-1810. General information concerning the Commission may also be obtained by accessing its Internet server (*http://www.usitc.gov*). The public record for this investigation may be viewed on the Commission's electronic docket (EDIS) at *http://edis.usitc.gov*.

SUPPLEMENTARY INFORMATION: This investigation was instituted by the Commission on June 3, 2004, based on a complaint filed by Trend Micro Inc. ("Trend Micro") of Cupertino, California under section 337 of the Tariff Act of 1930, 19 U.S.C. § 1337. 69 *Fed. Reg.* 32044-45 (June 8, 2004). The complaint alleged violations of section 337 in the importation into the United States, the sale for importation into the United States, or the sale within the United States after importation of certain systems for detecting and removing computer viruses or worms, components thereof, and products containing same by reason of infringement of claims 1-22 of U.S. Patent No. 5,623,600 ("the '600 patent"). The notice of investigation named Fortinet, Inc., of Sunnyvale, California ("Fortinet") as the sole respondent.

On May 9, 2005, the ALJ issued his final ID in this investigation finding a violation of section 337 based on his findings that claims 4, 7, 8, and 11-15 of the '600 patent are not invalid or unenforceable, and are infringed by respondent's products. On July 8, 2005, the Commission issued notice that it had determined not to review the ALJ's final ID on violation, thereby finding a violation of section 337. 70 *Fed. Reg.* 40731 (July 14, 2005). The Commission also requested briefing on the issues of remedy, the public interest, and bonding. *Id.* Submissions on the issues of remedy, the public interest, and bonding were filed by all parties. On August 8, 2005, the Commission terminated the investigation, and issued a limited exclusion order and a cease and desist order covering respondent's systems for detecting and removing computer viruses or worms, components thereof, and products containing same that infringe claims 4, 7, 8, and 11-15 of the '600 patent.

On September 13, 2005, complainant Trend Micro filed a complaint for enforcement of the Commission's remedial orders. On October 7, 2005, the Commission determined to institute a formal enforcement proceeding to determine whether Fortinet was in violation of the Commission's cease and desist order issued in the investigation and what, if any, enforcement measures were appropriate. 70 *Fed. Reg.* 76076 (December 22, 2005).

On October 26, 2005, Fortinet filed a request for an advisory opinion under Commission rule 210.79, 19 C.F.R. § 210.79, that would declare that Fortinet's anti-virus "FortiGate" products incorporating Fortinet's newly redesigned anti-virus software does not infringe claims 4, 7, 8, and 11-15 of the '600 patent and, therefore, is not covered by the Commission's cease and desist and limited exclusion orders, issued on August 8, 2005. On December 16, 2005, the Commission determined to institute an advisory opinion proceeding to determine whether Fortinet's redesigned anti-virus software infringes the asserted claims of the '600 patent.

On January 11, 2006, the presiding ALJ consolidated the enforcement proceeding and advisory opinion proceeding.

On December 16, 2005, Trend Micro moved for summary determination that Fortinet had violated sections III(B), III(D), and III(E) of the cease and desist order. On January 12, 2006, the ALJ issued an ID (Order No. 26) granting Trend Micro's motion for summary determination that Fortinet violated section III(B) of the cease and desist order. On February 9, 2006, the Commission determined not to review Order No. 26.

On December 21, 2005, Fortinet filed a request for an additional advisory opinion concerning the so-called Clearswift license, which it later withdrew on February 15, 2006.

On January 27, 2006, Trend Micro and Fortinet entered into a settlement agreement that resolves their dispute before the Commission. On February 14, 2006, Trend Micro and Fortinet filed a joint motion to terminate the consolidated proceedings on the basis of the settlement agreement. The joint motion included a petition to rescind the limited exclusion and cease and desist orders issued in the investigation, and a petition to vacate Order No. 26. On February 27, 2006, the Commission investigative attorney filed a response in support of the joint motion to terminate and in support of the joint petitions to rescind the limited exclusion and cease and desist orders and to vacate Order No. 26.

On February 28, 2006, the ALJ issued an ID (Order No. 31) granting the joint motion to terminate the consolidated enforcement and advisory opinion proceedings based on the settlement agreement. The ALJ also recommended that the Commission rescind the limited exclusion order and cease and desist order issued in the investigation and vacate Order No. 26. No party petitioned for review of the ID.

The Commission has determined not to review the subject ID granting the parties' joint motion to terminate the consolidated enforcement and advisory opinion proceeding. Additionally, the Commission has determined that the parties' settlement agreement satisfies the requirement of section 337(k) and Commission rule 210.76(a)(1), 19 C.F.R.§ 210.76(a)(1), for changed conditions of fact or law and has therefore issued an order rescinding the limited exclusion order and cease and desist order previously issued by the Commission in the underlying investigation. Finally, in view of specific terms in the settlement agreement, the Commission has determined to vacate Order No. 26.

The authority for the Commission's determination is contained in section 337 of the Tariff Act of 1930, as amended (19 U.S.C. § 1337), and in sections 210.42 and 210.76 of the Commission's Rules of Practice and Procedure (19 C.F.R. §§ 210.42 and 210.76).

By order of the Commission.

Marilyn R. Abbott
Secretary to the Commission

Issued: March 29, 2006

UNITED STATES INTERNATIONAL TRADE COMMISSION
Washington, D.C. 20436

In the Matter of

SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME

Inv. No. 337-TA-510
Consolidated Enforcement and Advisory Opinion Proceeding

ORDER

This investigation was instituted by the Commission on June 3, 2004, based on a complaint filed by Trend Micro Inc. ("Trend Micro") of Cupertino, California under section 337 of the Tariff Act of 1930, 19 U.S.C. § 1337. 69 *Fed. Reg.* 32044-45 (June 8, 2004). The complaint alleged violations of section 337 in the importation into the United States, the sale for importation into the United States, or the sale within the United States after importation of certain systems for detecting and removing computer viruses or worms, components thereof, and products containing same by reason of infringement of claims 1-22 of U.S. Patent No. 5,623,600 ("the '600 patent"). The notice of investigation named Fortinet, Inc., of Sunnyvale, California ("Fortinet") as the sole respondent.

On May 9, 2005, the presiding administrative law judge ("ALJ") issued his final initial determination ("ID") in the investigation finding a violation of section 337 based on his findings that claims 4, 7, 8, and 11-15 of the '600 patent are not invalid or unenforceable and are infringed by respondent's products. On July 8, 2005, the Commission issued notice that it had determined not to review the ALJ's final ID on violation, thereby finding a violation of section 337. 70 *Fed. Reg*. 40731 (July 14, 2005). The Commission also requested briefing on the issues of remedy, the public interest, and bonding. *Id.* Submissions on the issues of remedy, the public interest, and bonding were filed by all parties. On August 8, 2005, the Commission terminated the investigation, and issued a limited exclusion order and a cease and desist order covering respondent's systems for detecting and removing computer viruses or worms, components thereof, and products containing same that infringe claims 4, 7, 8, and 11-15 of the '600 patent.

On September 13, 2005, complainant Trend Micro filed a complaint for enforcement of the Commission's remedial orders under Commission rule 210.75(b), 19 C.F.R. § 210.75(b). On October 7, 2005, the Commission determined to institute formal enforcement proceedings to determine whether Fortinet was in violation of the Commission's cease and desist order issued in the investigation and what, if any, enforcement measures were appropriate.

On October 26, 2005, Fortinet filed a request for an advisory opinion under Commission rule 210.79, 19 C.F.R. § 210.79, that would declare that Fortinet's anti-virus "FortiGate" products incorporating Fortinet's newly redesigned anti-virus software do not infringe claims 4, 7, 8, and 11-15 of the '600 patent and, therefore, are not covered by the Commission's remedial orders issued on August 8, 2005. On December 16, 2005, the Commission determined to institute an advisory opinion proceeding to determine whether Fortinet's redesigned anti-virus software infringes the asserted claims of the '600 patent. On January 11, 2006, the presiding ALJ consolidated the enforcement and advisory opinion proceedings.

On December 16, 2005, Trend Micro moved for summary determination that Fortinet violated sections III(B), III(D), and III(E) of the cease and desist order. On January 12, 2006, the

ALJ issued an ID (Order No. 26) granting Trend Micro's motion for summary determination that Trend Micro had established that Fortinet violated section III(B) of the cease and desist order. On February 9, 2006, the Commission determined not to review Order No. 26.

On January 27, 2006, Trend Micro and Fortinet entered into a settlement agreement that resolves their dispute before the Commission. On February 14, 2006, they filed a joint motion to terminate the combined proceedings on the basis of their settlement agreement. The joint motion included a petition under Commission rule 210.76, 19 C.F.R. § 210.76, to rescind the remedial orders issued in the investigation, and a petition to vacate Order No. 26. On February 27, 2006, the Commission investigative attorney filed a response in support of the joint motion to terminate the consolidated proceedings and the joint petitions to rescind the remedial orders and to vacate Order No. 26.

On February 28, 2006, the ALJ issued an ID (Order No. 31) granting the joint motion to terminate the consolidated enforcement and advisory opinion proceeding based on the settlement agreement. The ALJ also recommended that the Commission grant the joint petition to rescind the remedial orders issued in the investigation and the joint petition to vacate Order No. 26. No party petitioned for review of the ID.

Having examined the ID, the Commission has determined not to review it, thereby allowing it to become the Commission's final determination. In addition, the Commission has determined that the settlement agreement between Trend Micro and Fortinet represents a changed condition of fact or law sufficient under section 337(k) and Commission rule 210.76(a)(1) to support rescission of the limited exclusion order and cease and desist order previously issued by the Commission in the underlying investigation. The Commission has also determined that the specific terms of the settlement agreement between Trend Micro and Fortinet support vacatur of Order No. 26.

Accordingly, the Commission ORDERS THAT:

1. The joint petition for rescission of the limited exclusion order and cease and desist order issued in this investigation is *granted.*

2. Order No. 26 is *vacated.*

3. The Secretary will serve this Order on the parties to this investigation and the Secretary of the Treasury.

By Order of the Commission.

Marilyn R. Abbott
Secretary to the Commission

Issued: March 29, 2006

SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME

337-TA-510 (CONSOLIDATED ENFORCEMENT AND ADVISORY OPINION PROCEEDING

CERTIFICATE OF SERVICE

I, Marilyn R. Abbott, hereby certify that the attached **COMMISSION DETERMINATION NOT TO REVIEW AN INITIAL DETERMINATION TERMINATING THE CONSOLIDATED ENFORCEMENT AND ADVISORY OPINION PROCEEDING; RESCISSION OF THE LIMITED EXCLUSION ORDER AND CEASE AND DESIST ORDER ISSUED IN THE UNDERLYING INVESTIGATION; VACATUR OF A SUMMARY INITIAL DETERMINATION ISSUED IN THE CONDOLIDATED ENFORCEMENT AND ADVISORY OPINION PROCEEDING,** was served upon all parties via first class mail and air mail where necessary on March 30, 2006.

Marilyn R. Abbott, Secretary
U.S. International Trade Commission
500 E Street, SW Rm. 112
Washington, DC 20436

<u>ON BEHALF OF COMPLAINTANT TREND MICRO INCORPORATED:</u>

Mark G. Davis, Esq.
McDermott, Will & Emery
600 - 13th Street N.W.
Washington, DC 20005-3096

Keaton S. Parekh, Esq.
McDermott, Will & Emery
3150 Porter Drive
Palo Alto, CA 94304-1212

<u>ON BEHALF OF RESPONDENT FORTINET, INC:</u>

Sturgis M. Sobin, Esq.
Miller and Chevalier Chartered
655 Fifteenth Street, NW
Suite 900
Washington, DC 20005-5701

Kenneth B. Wilson, Esq.
Perkins Coie, LLP
180 Townsend Street, 3rd Floor
San Francisco, CA 94107

T.O. Kong, Esq.
Antonio R. Sistos, Esq.
Linda S. Smith
Wilson Sonsini Goodrich & Rosati
650 Page Mill Road
Palo Alto, CA 94304-1050

UNITED STATES INTERNATIONAL TRADE COMMISSION
Washington, D.C.

In the Matter of

CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME

Investigation No. 337-TA-510

NOTICE OF COMMISSION DECISION NOT TO REVIEW AN INITIAL DETERMINATION GRANTING IN PART COMPLAINANT'S MOTION FOR SUMMARY DETERMINATION OF VIOLATION OF THE CEASE AND DESIST ORDER

AGENCY: U.S. International Trade Commission.

ACTION: Notice.

SUMMARY: Notice is hereby given that the U.S. International Trade Commission has determined not to review an initial determination ("ID") issued by the presiding administrative law judge ("ALJ") granting in part complainant's motion for summary determination that respondent violated the cease and desist order.

FOR FURTHER INFORMATION CONTACT: Michelle Walters, Esq., Office of the General Counsel, U.S. International Trade Commission, 500 E Street, S.W., Washington, D.C. 20436, telephone (202) 708-5468. Copies of non-confidential documents filed in connection with this investigation are or will be available for inspection during official business hours (8:45 a.m. to 5:15 p.m.) in the Office of the Secretary, U.S. International Trade Commission, 500 E Street, S.W., Washington, D.C. 20436, telephone (202) 205-2000. General information concerning the Commission may also be obtained by accessing its Internet server at *http://www.usitc.gov*. The public record for this investigation may be viewed on the Commission's electronic docket (EDIS) at *http://edis.usitc.gov*. Hearing-impaired persons are advised that information on this matter can be obtained by contacting the Commission's TDD terminal on (202) 205-1810.

SUPPLEMENTARY INFORMATION: This enforcement proceeding was instituted on October 7, 2005, based on a complaint filed by Trend Micro, Inc. ("Trend Micro") of Cupertino, California. The complaint alleges that respondent Fortinet, Inc. ("Fortinet") and its distributors circumvented the cease and desist order issued by the Commission on August 8, 2005, by continuing to advertise, market, sell, and offer for sale in the United States the imported infringing products and antivirus features of Fortinet's infringing software.

On December 16, 2005, Trend Micro moved for summary determination that Fortinet violates sections III(B), III(D), and III(E) of the cease and desist order. On January 3, 2006, the Commission investigative attorney filed a response to Trend Micro's motion, and on January 5, 2006, respondent filed a partial opposition to the motion. On January 10, 2006, Trend Micro moved for leave to file a reply to Fortinet's opposition to address "false statements" in the opposition.

On January 12, 2006, the ALJ issued an ID granting Trend Micro's motion for summary determination in part. The ALJ concluded that Trend Micro established that Fortinet violated section III(B) of the cease and desist order. The ALJ based his conclusion on Fortinet's outright admission that it violated this section of the cease and desist order. Fortinet, however, objected to Trend Micro's assertion of violation with regard to sections III(D) and III(E), and the ALJ, resolving any doubt as to the existence of a genuine issue of material fact in favor of Fortinet, determined that Trend Micro had not established a violation of these two sections of the cease and desist order. No petitions for review of the ID were filed.

Having examined the record of this investigation, the Commission has determined not to review the ALJ's ID.

The authority for the Commission's determination is contained in section 337 of the Tariff Act of 1930, as amended (19 U.S.C. § 1337), and in section 210.42 of the Commission's Rules of Practice and Procedure (19 C.F.R. § 210.42).

By order of the Commission.

Marilyn R. Abbott
Secretary to the Commission

Issued: February 9, 2006

CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME

Investigation No. 337-TA-510
Consolidated Enforcement
Advisory Opinion Proceeding

CERTIFICATE OF SERVICE

I, Marilyn R. Abbott hereby certify that the attached **NOTICE OF COMMISSION DECISION NOT TO REVIEW AN INITIAL DETERMINATION GRANTING IN PART COMPLAINANT'S MOTION FOR SUMMARY DETERMINATION OF VIOLATION OF THE CEASE AND DESIST ORDER**, was served upon the Commission Investigative Attorney, Rett Snotherly, Esq., and upon the following parties via first class mail and air mail, where necessary on February 10, 2006.

Marilyn R. Abbott

Marilyn R. Abbott, Secretary
U.S. International Trade Commission
500 E Street, SW, Room 112
Washington, DC 20436

For Complainant Trend Micro Inc.:

Mark G. Davis
McDermott, Will & Emery
600 13th Street NW, 12th Floor
Washington, D.C. 20005-3096

Keaton S. Parekh, Esq.
McDermott, Will & Emery
3150 Porter Drive
Palo Alto, CA 94304-1212

Michael A. Landra, Esq.
James C. Otteson, Esq.
Wilson Sonsini Goodrich & Rosati
650 Page Mill Road
Palo Alto, CA 94306

For Respondent Fortinet, Inc.:

Kenneth B. Wilson, Esq.
Stefani E. Shanberg, Esq.
Perkins Coie, LLP
180 Townsend Street, 3rd Floor
San Francisco, CA 94107

Sturgis M. Sobin, Esq.
Leigh A. Bacon, Esq.
Miller and Chevalier Chartered
655 Fifteenth Street, NW
Washington, D.C. 20005

UNITED STATES INTERNATIONAL TRADE COMMISSION
Washington, D.C. 20436

In the Matter of

CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME

Inv. No. 337-TA-510

TERMINATION OF INVESTIGATION; ISSUANCE OF A LIMITED EXCLUSION ORDER AND A CEASE AND DESIST ORDER

AGENCY: U.S. International Trade Commission.

ACTION: Notice.

SUMMARY: Notice is hereby given that the U.S. International Trade Commission has terminated the above-captioned investigation in which it has found a violation of the Tariff Act of 1930 and has issued a limited exclusion order and a cease and desist order.

FOR FURTHER INFORMATION CONTACT: Jonathan J. Engler, Esq., Office of the General Counsel, U.S. International Trade Commission, 500 E Street, S.W., Washington, D.C. 20436, telephone 202-205-3112. Copies of the public version of the ID and all nonconfidential documents filed in connection with this investigation are or will be available for inspection during official business hours (8:45 a.m. to 5:15 p.m.) in the Office of the Secretary, U.S. International Trade Commission, 500 E Street, S.W., Washington, D.C. 20436, telephone 202-205-2000. Hearing-impaired persons are advised that information on this matter can be obtained by contacting the Commission's TDD terminal on 202-205-1810. General information concerning the Commission may also be obtained by accessing its Internet server (*http://www.usitc.gov*). The public record for this investigation may be viewed on the Commission's electronic docket (EDIS) at *http://edis.usitc.gov*.

SUPPLEMENTARY INFORMATION: This patent-based section 337 investigation was instituted by the Commission on June 3, 2004, based on a complaint filed by Trend Micro Inc. ("Trend Micro") of Cupertino, California. 69 *Fed. Reg.* 32044-45 (2004). The complaint alleged violations of section 337 in the importation into the United States, the sale for importation into the United States, or the sale within the United States after importation of certain systems for detecting and removing viruses or worms, components thereof, and products containing same by reason of infringement of claims 1-22 of U.S. Patent No. 5,623,600 ("the '600 patent"). The notice of investigation named Fortinet, Inc. ("Fortinet") of Sunnyvale, California as the sole respondent.

On October 12, 2004, the ALJ issued an initial determination (ID)(Order No. 6) terminating the investigation as to claims 2, 5-6, 9-10, and 16-22 of the '600 patent based upon Trend Micro's unopposed motion to withdraw these claims. The Commission did not review Order No. 6, hence the claims of the '600 patent in issue are claims 1, 3, 4, 7, 8, and 11-15.

On December 14, 2004, the ALJ issued an ID (Order No. 13) granting complainant Trend Micro's motion for a summary determination that it satisfies the economic prong of the domestic industry requirement. Order No. 13 was not reviewed by the Commission.

An evidentiary hearing was held from January 24, 2005 to January 28, 2005. On March 29, 2005, a second evidentiary hearing was conducted and additional exhibits received into evidence.

On May 9, 2005, the administrative law judge ("ALJ") issued his final ID finding a violation of section 337 based on his findings that claims 4, 7, 8, and 11-15 of the '600 patent are not invalid or unenforceable, and are infringed by respondent's products. The ALJ also found that claims 1 and 3 of the '600 patent are invalid as anticipated by prior art and that a domestic industry exists. He also issued his recommended determination on remedy and bonding.

On May 20, 2005, respondent Fortinet filed a petition for review of the final ID and complainant Trend Micro filed a contingent petition for review. The IA did not file a petition. On May 27, 2005, Fortinet filed a response to Trend Micro's contingent petition for review, and Trend Micro filed a response to Fortinet's petition for review. On June 2, 2005, the IA filed a response to Trend Micro and Fortinet's petition for review.

On July 8, 2005, the Commission issued a notice indicating that it had determined not to review the ALJ's final ID on violation, thereby finding a violation of section 337. 70 *Fed. Reg.* 40731 (July 14, 2005). The Commission also invited the parties to file written submission regarding the issues of remedy, the public interest, and bonding, and provided a schedule for filing such submissions.

Having reviewed the record in this investigation, including the parties' written submissions and responses thereto, the Commission determined that the appropriate form of relief in this investigation is a limited exclusion order prohibiting the unlicensed entry of systems for detecting and removing viruses or worms, components thereof and products containing same covered by claims 4, 7, 8, and 11-15 of the '600 patent. The order covers systems for detecting and removing viruses or worms, components thereof and products containing same that are manufactured abroad by or on behalf of, or imported by or on behalf of the respondent, or any of their affiliated companies, parents, subsidiaries, or other related business entities, or their successors or assigns.

The Commission also determined to issue a cease and desist order prohibiting the respondent from importing, selling, marketing, advertising, distributing, offering for sale, transferring (except for exportation), and soliciting U.S. agents or distributors for systems for detecting and removing viruses or worms, components thereof and products containing same.

The Commission further determined that the public interest factors enumerated in sections 337(d)(1) and (f)(1), 19 U.S.C. §§ 1337(d)(1) and (f)(1), do not preclude issuance of either the limited exclusion order or the cease and desist order. In addition, the Commission determined that the amount of bond to permit temporary importation during the Presidential review period shall be in the amount of 100 percent of the entered value of the imported articles. The Commission's orders and opinion in support thereof were delivered to the President on the day of their issuance.

This action is taken under the authority of section 337 of the Tariff Act of 1930, as amended (19 U.S.C. § 1337), and section 210.50 of the Commission's Interim Rules of Practice and Procedure (19 C.F.R. § 210.50).

By order of the Commission.

Marilyn R. Abbott
Secretary to the Commission

Issued: August 8, 2005

UNITED STATES INTERNATIONAL TRADE COMMISSION
Washington, D.C.

In the Matter of CERTAIN SYSTEMS FOR DETECTING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME	Inv. No. 337-TA-510

LIMITED EXCLUSION ORDER

The Commission has determined that there is a violation of section 337 of the Tariff Act of 1930 (19 U.S.C. § 1337), as amended, in the unlawful importation and sale by Respondent Fortinet, Inc. of certain systems for detecting and removing viruses or worms, components thereof, and products containing same, covered by one or more of claims 4, 7, 8, and 11-15 of U.S. Patent No. 5,623,600 owned by Complainant Trend Micro Inc.

Having reviewed the record in this investigation, including the written submissions of the parties, the Commission has made its determination on the issues of remedy, the public interest, and bonding. The Commission has determined that the appropriate form of relief is a limited exclusion order prohibiting the unlicensed entry of systems for detecting and removing viruses or worms, components thereof, and products containing same, that are manufactured by or on behalf of, or imported by or on behalf of, Fortinet, Inc. The Commission has further determined that the public interest factors enumerated in 19 U.S.C.

§ 1337(d) do not preclude issuance of the limited exclusion order, and that the bond during the Presidential review period shall be in the amount of 100 percent of the entered value of the articles in question.

Accordingly, the Commission hereby **ORDERS** that:

1. Systems for detecting and removing viruses or worms, components thereof, and products containing same, covered by one or more of claims 4, 7, 8, and 11-15 of U.S. Patent No. 5,623,600 that are embodied in a tangible medium and manufactured abroad by or on behalf of, or imported by or on behalf of, Fortinet, Inc., or any of its affiliated companies, parents, subsidiaries, or other related business entities, or their successors or assigns, are excluded from entry for consumption into the United States, entry for consumption from a foreign trade zone, or withdrawal from a warehouse for consumption, for the remaining term of that patent, except under license of the patent owner or as provided by law.

2. Systems for detecting and removing viruses or worms, components thereof, and products containing same and antiviral software modules that are excluded by paragraphs 1 and 2 of this Order are entitled to entry for consumption into the United States, entry for consumption from a foreign trade zone, or withdrawal from a warehouse for consumption, under bond in the amount of 100 percent of entered value pursuant to subsection (j) of section 337 of the Tariff Act of 1930, as amended, 19 U.S.C. § 1337(j), from the day after this Order is

received by the President until such time as the President notifies the Commission that he approves or disapproves this action but, in any event, not later than 60 days after the date of receipt of this action.

3. In accordance with 19 U.S.C. § 1337(l), the provisions of this Order shall not apply to systems for detecting and removing viruses or worms, components thereof, and products containing same that are imported by and for the use of the United States, or imported for, and to be used for, the United States with the authorization or consent of the Government.

4. The Commission may modify this Order in accordance with the procedures described in section 210.76 of the Commission's Rules of Practice and Procedure, 19 C.F.R. § 210.76.

5. The Secretary shall serve copies of this Order upon each party of record in this investigation and upon the Department of Health and Human Services, the Department of Justice, the Federal Trade Commission, and the U.S. Customs and Border Protection.

6. Notice of this Order shall be published in the *Federal Register*.

By Order of the Commission.

Marilyn R. Abbott
Secretary to the Commission

Issued: August 8, 2005

UNITED STATES INTERNATIONAL TRADE COMMISSION
Washington, D.C.

In the Matter of

CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME

Inv. No. 337-TA-510

ORDER TO CEASE AND DESIST

IT IS HEREBY ORDERED THAT Fortinet, Inc., 920 Stewart Drive, Sunnyvale, California 94085, cease and desist from conducting any of the following activities in the United States: importing, selling, marketing, advertising, distributing, offering for sale, transferring (except for exportation), and soliciting U.S. agents or distributors for, certain systems for detecting and removing viruses or worms, components thereof, and products containing same, covered by one or more of claims 4, 7, 8, and 11-15 of U.S. Patent No. 5,623,600, in violation of section 337 of the Tariff Act of 1930, as amended, 19 U.S.C. § 1337.

I.

Definitions

As used in this Order:

(A) "Commission" shall mean the United States International Trade Commission.

(B) "Trend Micro Incorporated," "Trend Micro" or "Complainant" shall mean Trend Micro Incorporated, 10101 De Anza Boulevard, Cupertino, California 95104.

(C) "Fortinet, Inc.," "Fortinet," or "Respondent" shall mean Fortinet Inc., 920 Stewart Drive, Sunnyvale, California 94085.

(D) "Person" shall mean an individual, or any non-governmental partnership, firm, association, corporation, or other legal or business entity other than Fortinet or its majority owned or controlled subsidiaries, successors, or assigns.

(E) "United States" shall mean the fifty States, the District of Columbia, and Puerto Rico.

(F) The terms "import" and "importation" refer to importation for entry for consumption under the Customs laws of the United States.

(G) The term "covered products" shall mean: systems for detecting and removing viruses or worms, components thereof (including software), and products containing same, that infringe one or more of claims 4, 7, 8, and 11-15 of U.S. Patent No. 5,623,600.

II.

Applicability

The provisions of this Cease and Desist Order shall apply to Respondent and to any of its principals, stockholders, officers, directors, employees, agents, licensees, distributors, controlled (whether by stock ownership or otherwise) and majority-owned business entities, successors, and assigns, and to each of them, insofar as they are engaging in conduct prohibited by Section III, *infra*, for, with, or otherwise on behalf of Respondent.

III.

Conduct Prohibited

The following conduct of Respondent in the United States is prohibited by the Order. For the remaining term of the respective patents, Respondent shall not:

(A) import or sell for importation into the United States covered products;

(B) market, distribute, offer for sale, sell, or otherwise transfer (including electronically), in the United States imported covered products (except for exportation);

(C) advertise imported covered products;

(D) solicit U.S. agents or distributors for imported covered products;

(E) aid or abet other entities in the importation, sale for importation, sale after importation, transfer, or distribution of covered products; or

(F) import (including electronically) into the United States, or use, duplicate, transfer or distribute by electronic means or otherwise, within the United States, anti-virus software that constitutes covered product.

IV.

Conduct Permitted

Notwithstanding any other provision of this Order, specific conduct otherwise prohibited by the terms of this Order shall be permitted if:

(A) in a written instrument, the owner of U.S. Patent No. 5,623,600 licenses or authorizes such specific conduct, or such specific conduct is related to the importation or sale of covered products by or for the United States; or

(B) the conduct is limited to the provision of maintenance releases and virus-signature releases of Fortinet's anti-virus software for customers that purchased their covered systems prior to the date of issuance of this Order; or

(C) the conduct is limited to the provision of service and replacement parts for customers that purchased their covered systems prior to the date of issuance of this Order.

V.

Reporting

For purposes of this reporting requirement, the reporting periods shall commence on July 1 of each year and shall end on the subsequent June 30. However, the first report required under this section shall cover the period from the date of issuance of this Order through June 30, 2006. This reporting requirement shall continue in force until such time as Respondent will have truthfully reported, in two consecutive timely filed reports, that it has no inventory of covered products in the United States.

Within thirty (30) days of the last day of the reporting period, Respondent shall report to the Commission the quantity in units and the value in dollars of covered products that Respondent has imported or sold in the United States after importation during the reporting period and the quantity in units and value in dollars of covered products that remain in inventory in the United States at the end of the reporting period.

Any failure to make the required report or the filing of any false or inaccurate report shall constitute a violation of this Order, and the submission of a false or inaccurate report may be referred to the U.S. Department of Justice as a possible criminal violation of 18 U.S.C. § 1001.

VI.

Record-keeping and Inspection

(A) For the purpose of securing compliance with this Order, Respondent shall retain any and all records relating to the sale, offer for sale, marketing, or distribution in the United States of covered products, made and received in the usual and ordinary course of business, whether in detail or in summary form, for a period of three (3) years from the close of the fiscal year to which they pertain.

(B) For the purpose of determining or securing compliance with this Order and for no other purpose, and subject to any privilege recognized by the federal courts of the United States, duly authorized representatives of the Commission, upon reasonable written notice by the Commission or its staff, shall be permitted access and the right to inspect and copy in Respondent's principal offices during office hours, and in the presence of counsel or other representatives if Respondent so chooses, all books, ledgers, accounts, correspondence, memoranda, and other records and documents, both in detail and in summary form as are required to be retained by subparagraph VI(A) of this Order.

VII.

Service of Cease and Desist Order

Respondent is ordered and directed to:

(A) Serve, within fifteen (15) days after the effective date of this Order, a copy of this Order upon each of its respective officers, directors, managing agents, agents, and employees who have any responsibility for the importation, marketing, distribution, or sale of imported covered products in the United States;

(B) Serve, within fifteen (15) days after the succession of any persons referred to in subparagraph VII (A) of this Order, a copy of the Order upon each successor; and

(C) Maintain such records as will show the name, title, and address of each person upon whom the Order has been served, as described in subparagraphs VII(A) and VII(B) of this Order, together with the date on which service was made.

The obligations set forth in subparagraphs VII(B) and VII(C) shall remain in effect until the date of expiration of U.S. Patent No. 5,623,600.

VIII.

Confidentiality

Any request for confidential treatment of information obtained by the Commission pursuant to Sections V and VI of this Order should be in accordance with Commission Rule 201.6, 19 C.F.R. § 201.6. For all reports for which confidential treatment is sought, Respondent must provide a public version of such report with confidential information redacted.

IX.

Enforcement

Violation of this Order may result in any of the actions specified in section 210.75 of the Commission's Rules of Practice and Procedure, 19 C.F.R. § 210.75, including an action for civil penalties in accordance with section 337(f) of the Tariff Act of 1930, 19 U.S.C. § 1337(f), and any other action as the Commission may deem appropriate. In determining whether Respondent is in violation of this Order, the Commission may infer facts adverse to Respondent if Respondent fails to provide adequate or timely information.

X.

Modification

The Commission may amend this Order on its own motion or in accordance with the procedure described in section 210.76 of the Commission's Rules of Practice and Procedure, 19 C.F.R. § 210.76.

XI.

Bonding

The conduct prohibited by Section III of this Order may be continued during the sixty (60) day period in which this Order is under review by the President pursuant to section 337(j) of the Tariff Act of 1930, 19 U.S.C. § 1337(j), subject to Respondent posting a bond of 100% of entered value of the covered products. This bond provision does not apply to conduct that is otherwise permitted by Section IV of this Order. Covered products imported on or after the date of issuance of this order are subject to the entry bond as set forth in the limited exclusion order issued by the Commission, and are not subject to this bond provision.

The bond is to be posted in accordance with the procedures established by the Commission for the posting of bonds by complainants in connection with the issuance of temporary exclusion orders. *See* Commission Rule 210.68, 19 C.F.R. § 210.68. The bond and any accompanying documentation is to be provided to and approved by the Commission prior to the commencement of conduct which is otherwise prohibited by Section III of this Order.

The bond is to be forfeited in the event that the President approves, or does not disapprove within the Presidential review period, this Order, unless the U.S. Court of Appeals for the Federal Circuit, in a final judgment, reverses any Commission final determination and order as to Respondent on appeal, or unless Respondent exports the products subject to this bond or destroys them and provides certification to that effect satisfactory to the Commission.

The bond is to be released in the event the President disapproves this Order and no subsequent order is issued by the Commission and approved, or not disapproved, by the President, upon service on Respondent of an order issued by the Commission based upon application therefore made by Respondent to the Commission.

By Order of the Commission.

Marilyn R. Abbott
Secretary to the Commission

Issued: August 8, 2005

CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME **337-TA-510**

CERTIFICATE OF SERVICE

I, Marilyn R. Abbott, hereby certify that the attached **NOTICE OF TERMINATION OF INVESTIGATIN; ISSUANCE OF A LIMITED EXCLUSION ORDER AND A CEASE AND DESIST ORDER** were served upon the Commission Investigative Attorney, Rett Snotherly, Esq., and all parties via first class mail and certified mail where necessary on August 8, 2005.

Marilyn R. Abbott, Secretary
U.S. International Trade Commission
500 E Street, SW Rm 112
Washington, DC 20436

<u>ON BEHALF OF COMPLAINTANT TREND MICRO INCORPORATED:</u>

Mark G. Davis, Esq.
McDermott, Will & Emery
600 - 13th Street N.W.
Washington, D.C. 20005-3096

<u>ON BEHALF OF RESPONDENT FORTINET, INC.</u>

Sturgis M. Sobin, Esq.
Miller & Chevalier
655 15th Street, N.W.,
Suite 900
Washington, D.C. 20005-5701

Kenneth B. Wilson, Esq.
Perkins Coie, LLP
180 Towsend Street
3rd Floor
San Francisco, CA 94107

James C. Otteson, Esq.
WILSON SONSINI GOODRICH & ROSATI
650 Page Mill Road
Palo Alto CA 94304-1050

PUBLIC VERSION

UNITED STATES INTERNATIONAL TRADE COMMISSION
Washington, D.C.

In the Matter of: CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME	Inv. No. 337-TA-510

COMMISSION OPINION ON REMEDY, THE PUBLIC INTEREST, AND BONDING

BACKGROUND

This patent-based Section 337 investigation was instituted by the Commission on June 3, 2004, based on a complaint filed by Trend Micro, Inc. ("Trend Micro") of Cupertino, California. 69 *Fed. Reg.* 32044-45 (2004). The complaint alleged violations of Section 337 of the Tariff Act of 1930, 19 U.S.C. § 1337, in the importation into the United States, the sale for importation into the United States, or the sale within the United States after importation of certain systems for detecting and removing computer viruses or worms, components thereof, and products containing same by reason of infringement of claims 1-22 of U.S. Patent No. 5,623,600 ("the '600 patent"). The notice of investigation named Fortinet, Inc. ("Fortinet") of Sunnyvale, California as the sole respondent. Claims 1, 3, 4, 7, 8, and 11-15 of the '600 patent remained at issue at the time that the administrative law judge ("ALJ") issued his final initial determination ("ID").

On May 9, 2005, the ALJ issued his final ID finding a violation of section 337 based on his findings that claims 4, 7, 8, and 11-15 of the '600 patent are not invalid or unenforceable, and are infringed by respondent's products. These claims cover the software module in the infringing systems. The ALJ also found that claims 1 and 3 of the '600 patent are invalid as anticipated by prior art and that a domestic industry exists. He also issued his recommended determination ("RD") on remedy and bonding. Petitions for review were filed by both private parties on May 20, 2005. The Commission investigative attorney ("IA") did not file a petition. On May 27, 2005, both private parties filed responses. The IA filed a single response to both of the parties' petitions on June 2, 2005.

On July 8, 2005, the Commission issued a notice that it had determined not to review the ALJ's final ID on violation, thereby finding a violation of Section 337. 70 *Fed. Reg.* 40731 (July 14, 2005). The Commission also requested briefing on the issues of remedy, the public interest, and bonding. *Id.* Submissions on the issues of remedy, the public interest, and bonding were filed on July 18, 2005, by all parties. All parties filed response submissions on July 25, 2005.

DISCUSSION

I. REMEDY

Having found a violation of Section 337, we must consider the issues of remedy, the public interest, and bonding. 19 U.S.C. §§ 1337(d) and (f). With respect to remedy, the Commission may issue a remedial order excluding the goods of the person(s) found in violation (a limited exclusion order) or, if certain criteria are met, against all infringing goods regardless of the source (a general exclusion order). The Commission also has authority to issue cease and desist orders prohibiting conduct in violation of Section 337. *See* 19 U.S.C. § 1337(f). The

Commission has broad discretion in selecting the form, scope and extent of the remedy in a Section 337 proceeding, and judicial review of its choice of remedy is governed by the abuse of discretion standard. *Fuji Photo Film Co. v. United States Int'l Trade Comm'n*, 386 F.3d 1095, 1106-1107 (Fed. Cir. 2004).

In this investigation, all the parties agree that the appropriate remedy is a limited exclusion order excluding the importation of any Fortinet FortiGate products covered by the asserted claims of the '600 patent. The parties disagree, however, as to whether the exclusion order should be limited to the importation of all FortiGate products, including hardware, components and software, or only to FortiGate hardware when combined with the infringing software module. The parties also disagree as to whether the exclusion order should prohibit the distribution of software maintenance releases and updates, and the importation of hardware and related articles that would allow Fortinet to service systems purchased before the Commission enters its order. The parties also do not agree as to whether a certification provision should be included in the order, the appropriate amount of any bond during the Presidential review period, and the appropriate scope of a cease and desist order.

Complainant Trend Micro argues that the exclusion order should cover all FortiGate products, including hardware, software and components that do not have substantial non-infringing uses, including components and software necessary for the repair and service of Fortigate products that entered the United States prior to entry of the Commission's order. Moreover, Trend Micro argues for a cease and desist order that would prohibit any activity in the United States relating to the infringed patent, including technical support and service.

Respondent Fortinet argues that the limited exclusion should cover only the software module that infringes the asserted claims of the '600 patent and not other Fortinet hardware and software which have no nexus to the infringement. Fortinet also contends that the exclusion order should allow Fortinet to continue to import articles necessary to service, repair, and properly use FortiGate units imported prior to the effective date of the Commission's orders. With respect to the cease and desist order, Fortinet submits that the order should be limited to the infringing antivirus software module and not other non-infringing Fortinet products, and permit Fortinet to provide service and repair of FortiGate products imported and sold by Fortinet before the effective date of the order.

The scope of the remedy is dependent on the scope of the investigation, which is determined by the notice of investigation. *See Certain Insect Traps*, Inv. No. 337-TA-498, Order No. 7 (April 2004). In this case, the notice of investigation identified the infringing products as *systems* for detecting and removing viruses or worms, components thereof, and products containing same. Therefore, the scope of the investigation extends to hardware that is part of an infringing system. Accordingly, our remedial orders cover FortiGate hardware components only in instances where an infringing anti-virus software module is installed on the FortiGate hardware. We determine to issue both a limited exclusion order which prohibits the importation of any infringing FortiGate products, including software that would result in infringement of the '600 patent whether alone or when combined with other Fortinet components, and a cease and desist order directed to Fortinet prohibiting certain infringing conduct.

Our exclusion order bars the importation of infringing antiviral software in a tangible medium but, consistent with Commission practice and out of deference to the U.S. Bureau of Customs and Border Protection (Customs), does not prohibit the electronic transmission of the infringing software. *See Certain Hardware Logic Emulation Systems and Components Thereof,* Inv. No. 337-TA-383, Comm'n Opinion at 27 (March 1998) ("*Hardware Logic*")(holding that while the Commission has the legal authority to exclude electronic transmissions, such transmissions would not be covered by the exclusion order out of deference to Customs, which has determined not to regulate electronic transmissions).[1]

We decline to include a certification provision in our limited exclusion order because Customs is capable of determining whether imported FortiGate hardware contains the infringing software, and there is no evidence that Fortinet imported non-infringing products prior to the issuance of the exclusion order. Consequently, we determine that a certification provision is neither necessary or appropriate in this case.

Our cease and desist order bars the electronic transmission of the infringing antivirus software module by Fortinet. As the Commission noted in *Hardware Logic,* for a cease and desist order not to cover electronic transmissions would allow for an obvious method of circumvention such that the cease and desist order would be rendered "meaningless." *Hardware Logic*, Comm'n Op. at 39. We also find, consistent with Commission precedent, that a cease and desist order is appropriate here because the record indicates that Fortinet has a commercially

[1] Software maintenance releases and database updates are provided to Fortinet's customers through electronic transmissions. *See*, Xie, Hearing Tr. at 1370. Thus, because the limited exclusion order does not cover electronic submissions, it is not necessary to include a specific provision in the exclusion order to address this exception.

significant inventory of infringing product in the U.S. *See Certain Crystalline Cefadroxil Monohydrate*, Inv. No. 337-TA-293, Comm'n Opinion at 6 (January 19, 1990). Moreover, in view of *Hardware Logic*, which exempted the importation of spare parts to service products already in the hands of respondent's customers, our cease and desist order also includes an exception to allow Fortinet to provide its current customers with software maintenance releases and virus updates to Fortinet's virus signature database via electronic transmission. The cease and desist order also allows for the provision of service or replacement parts for customers that purchased their covered systems prior to the date of issuance of our Order. We make these exceptions because if Fortinet's customers are denied receiving software maintenance releases, updates, services or replacement parts, the antivirus capabilities of the FortiGate products already held by customers may be quickly become ineffective. *See Certain Sortation Systems, Parts Thereof, and Products Containing Same*, Inv. No. 337-TA-460, Comm'n Op. at 20.

II. The Public Interest

Section 337(d) directs the Commission to consider public interest factors before issuing a remedial order, including the effect of any such remedial order on the "public health and welfare, competitive conditions in the United States economy, the production of like or directly competitive articles in the United States, and United States consumers." 19 U.S.C. § 1337(d) and (f).

We find that there are no public interest concerns that would preclude issuance of remedial orders in this investigation. While the protection of computer systems from viruses and worms could be considered a matter of public welfare, no reason exists to believe that the U.S.

demand for such products cannot be met by entities other than Fortinet. The fact that the proposed orders allow for current customers of Fortinet to receive maintenance and repair services, and to obtain maintenance releases and updates to the virus signature database further allays any concerns of this nature. Finally, the public interest favors the protection of U.S. intellectual property rights by excluding infringing imports.

III. Fortinet's Bond

Section 337(j) provides for the entry of infringing articles during the sixty (60) day Presidential review period upon posting of a bond, and states that the bond is to be set at a level sufficient to "protect complainant from any injury" during the Presidential review period. 19 U.S.C. § 1337(j); *see also* Commission Rule 210.50(a)(3), 19 C.F.R. § 210.50(a)(3).

The ALJ found that "both Fortinet and Trend Micro have numerous relevant models and product lines," and that "the price comparison is made more difficult by the fact that Fortinet's products are a combination of hardware and software while those of Trend Micro are software only." ID at 164. As a result, he recommends that a bond of 100 percent of entered value of the infringing imported products be set to permit temporary importation during the Presidential review period. For the reasons stated by the ALJ, we determine that the amount of the temporary importation bond provided for under section 337(j)(3) shall be 100 percent of the entered value of the articles covered by the limited exclusion order. Where there is inadequate pricing information, the Commission has traditionally set the bond at 100 percent of entered value of the infringing imported product. *See Certain Oscillating Sprinklers, Sprinkler Components, and Nozzles*, Inv. No. 337-TA-448, Limited Exclusion Order at 4 (March 2002). Fortinet has neither substantiated its assertion that a lower bond rate is appropriate given the value of the infringing software, nor its contention that a 100% bond rate would effectively prevent the importation of the infringing products during the Presidential review period.

By order of the Commission.

Marilyn R. Abbott
Secretary to the Commission

Issued: August 23, 2005

UNITED STATES INTERNATIONAL TRADE COMMISSION
Washington, D.C. 20436

In the Matter of **CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME**	**Inv. No. 337-TA-510**

NOTICE OF COMMISSION DECISION NOT TO REVIEW A FINAL INITIAL DETERMINATION FINDING A VIOLATION OF SECTION 337; REQUEST FOR WRITTEN SUBMISSIONS ON THE ISSUES OF REMEDY, THE PUBLIC INTEREST, AND BONDING

AGENCY: U.S. International Trade Commission.

ACTION: Notice.

SUMMARY: Notice is hereby given that the U.S. International Trade Commission has determined not to review a final initial determination ("ID") issued by the presiding administrative law judge ("ALJ") in the above-captioned investigation on May 9, 2005, finding a violation of section 337 of the Tariff Act of 1930, 19 U.S.C. § 1337. Notice is also hereby given that the Commission is requesting briefing on the issues of remedy, the public interest, and bonding.

FOR FURTHER INFORMATION CONTACT: Jean H. Jackson, Esq., Office of the General Counsel, U.S. International Trade Commission, 500 E Street, S.W., Washington, D.C. 20436, telephone 202-205-3104. Copies of the public version of the ID and all nonconfidential documents filed in connection with this investigation are or will be available for inspection during official business hours (8:45 a.m. to 5:15 p.m.) in the Office of the Secretary, U.S. International Trade Commission, 500 E Street, S.W., Washington, D.C. 20436, telephone 202-205-2000. Hearing-impaired persons are advised that information on this matter can be obtained by contacting the Commission's TDD terminal on 202-205-1810. General information concerning the Commission may also be obtained by accessing its Internet server (*http://www.usitc.gov*). The public record for this investigation may be viewed on the Commission's electronic docket (EDIS) at *http://edis.usitc.gov*.

SUPPLEMENTARY INFORMATION: The Commission instituted this investigation on June 3, 2004, based on a complaint filed by Trend Micro Inc. of Cupertino, California ("Trend Micro"). 69 *Fed. Reg.* 32044-45 (2004). The complaint alleged violations of section 337 in the importation into the United States, the sale for importation into the United States, or the sale within the United States after importation of certain systems for detecting and removing viruses or worms, components thereof, and products containing same by reason of infringement of claims 1-22 of U.S. Patent No. 5,623,600 ("the '600 patent"). The notice of investigation named Fortinet, Inc. ("Fortinet") as the sole respondent.

On October 12, 2004, the ALJ issued Order No. 6 terminating the investigation as to claims 2, 5-6, 9-10, and 16-22 of the '600 patent based upon Trend Micro's unopposed motion to withdraw these claims. The Commission did not review Order No. 6, hence the claims of the '600 patent in issue are claims 1, 3, 4, 7, 8, and 11-15.

On December 14, 2004, the ALJ issued Order No. 13 granting complainant Trend Micro's motion for a summary determination that it satisfies the economic prong of the domestic industry requirement. Order No. 13 was not reviewed by the Commission.

An evidentiary hearing was held from January 24, 2005 to January 28, 2005. On March 29, 2005, a second evidentiary hearing was conducted and additional exhibits received into evidence.

On May 9, 2005, the ALJ issued his final ID and recommended determinations on remedy and bonding. He found a violation of section 337 based on his determinations that claims 4, 7, 8, 11, 12, 13, 14 and 15 of the '600 patent are not invalid or unenforceable, and that they are infringed by respondent's products. The ALJ also found that an industry exists that is related to the '600 patent, and that the respondent has imported infringing product. The ALJ further found that claims 1 and 3 of the '600 patent are anticipated by prior art.

On May 20, 2005, respondent Fortinet filed a petition for review of the final ID and complainant Trend Micro filed a contingent petition for review. The IA did not file a petition. On May 27, 2005, Fortinet filed a response to Trend Micro's contingent petition for review, and Trend Micro filed a response to Fortinet's petition for review. On June 2, 2005, the IA filed a response to Trend Micro's and Fortinet's petitions for review.

Having examined the record in this investigation, including the ALJ's final ID, the petitions for review, and the responses thereto, the Commission has determined not to review the ID, thereby finding a violation of section 337.

In connection with the final disposition of this investigation, the Commission may issue (1) an order that could result in the exclusion of the subject articles from entry into the United states, and/or (2) a cease and desist order that could result in the respondent being required to cease and desist from engaging in unfair action in the importation and sale of such articles.

Accordingly, the Commission is interested in receiving written submissions that address the form of remedy, if any, that should be ordered. If a party seeks exclusion of an article from entry into the United States for purposes other than entry for consumption, the party should so indicate and provide information establishing that activities involving other types of entry are either adversely affecting it or likely to do so. For background, *see In the Matter of Certain Devices for Connecting Computers via Telephone Lines*, Inv. No. 337-TA-360, USITC Pub. No. 2843 (December 1994) (Commission Opinion).

When the Commission contemplates some form of remedy, it must consider the effects of that remedy upon the public interest. The factors the Commission will consider include the effect that an exclusion order and/or cease and desist orders would have on (1) the public health and welfare, (2) competitive conditions in the U.S. economy, (3) U.S. production of articles that are like or directly competitive with those that are subject to investigation, and (4) U.S. consumers. The Commission is therefore interested in receiving written submissions that address the aforementioned public interest factors in the context of this investigation.

If the Commission orders some form of remedy, the President has 60 days to approve or disapprove the Commission's action. During this period, the subject articles would be entitled to enter the United States under a bond, in an amount determined by the Commission and prescribed by the Secretary of the Treasury. The Commission is therefore interested in receiving submissions concerning the amount of the bond that should be imposed.

WRITTEN SUBMISSIONS: The parties to the investigation, interested government agencies, and any other interested persons are encouraged to file written submissions on the issues of remedy, the public interest, and bonding. Such submissions should address the ALJ's recommended determination on remedy and bonding. Complainant and the Commission investigative attorney are also requested to submit proposed remedial orders for the Commission's consideration. Complainant is further requested to state the expiration date of the '600 patent and the HTSUS numbers under which the infringing products are imported. The main written submissions and proposed remedial orders must be filed no later than July 18, 2005. Response submissions must be filed no later than July 25, 2005. No further submissions will be permitted unless otherwise ordered by the Commission.

Persons filing written submissions must file the original document and 12 true copies thereof with the Office of the Secretary on or before the deadlines stated above. Any person desiring to submit a document (or portions thereof) to the Commission in confidence must request confidential treatment unless the information has already been granted such treatment during the proceedings. All such requests should be directed to the Secretary of the Commission and must include a full statement of the reasons why the Commission should grant such treatment. *See* 19 C.F.R. § 210.5. Documents for which confidential treatment is granted by the Commission will be treated accordingly. All non-confidential written submissions will be available for public inspection at the Office of the Secretary.

This action is taken under the authority of section 337 of the Tariff Act of 1930, as amended (19 U.S.C. § 1337), and sections 210.42, 210.43, and 210.50 of the Commission's Interim Rules of Practice and Procedure (19 C.F.R. §§ 210.42, 210.43, and 210.50).

By order of the Commission.

Marilyn R. Abbott
Secretary to the Commission

Issued: July 8, 2005

CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME **337-TA-510**

CERTIFICATE OF SERVICE

I, Marilyn R. Abbott, hereby certify that the attached **NOTICE OF COMMISSION DECISION NOT TO REVIEW A FINAL INITIAL DETERMINATION FINDING A VIOLATION OF SECTION 337; REQUEST FOR WRITTEN SUBMISSIONS ON THE ISSUES OF REMEDY, THE PUBLIC INTEREST, AND BONDING** was served upon the Commission Investigative Attorney, Rett Snotherly, Esq., and upon all parties via first class mail and air mail where necessary on **July 11, 2005.**

Marilyn R. Abbott

Marilyn R. Abbott, Secretary
U.S. International Trade Commission
500 E Street, SW, Rm 112
Washington, DC 20436

<u>ON BEHALF OF COMPLAINTANT TREND MICRO INCORPORATED:</u>

Mark G. Davis, Esq.
McDermott, Will & Emery
600 - 13th Street N.W.
Washington, D.C. 20005-3096

Kenneth S. Korea, Esq.
McDermott, Will & Emery
3150 Porter Drive
Palo Alto, CA 94304-1212

<u>ON BEHALF OF FORTINET:</u>

Kenneth B. Wilson, Esq.
Perkins Coie, LLP
180 Townsend Street, 3rd Floor
San Francisco, CA 94107

Sturgis M. Sobin, Esq.
Miller and Chevalier Chartered
655 Fifteenth Street, NW
Suite 900
Washington, DC 20000

PUBLIC VERSION

UNITED STATES INTERNATIONAL TRADE COMMISSION
Washington, D.C.

In the Matter of	)	
	)	
CERTAIN SYSTEMS FOR DETECTING	)	Investigation No. 337-TA-510
AND REMOVING VIRUSES OR	)	
WORMS, COMPONENTS THEREOF,	)	
AND PRODUCTS CONTAINING SAME	)	
	)	

Final Initial and Recommended Determinations

This is the administrative law judge's Final Initial Determination, under Commission rule 210.42. The administrative law judge, after a review of the record developed, finds that claims 4, 7, 8, 11, 12, 13, 14 and 15 of U.S. Patent No. 5,623,600 are not invalid; that said patent is enforceable; and that said claims are infringed. Thus, he finds that a violation of section 337 of the Tariff Act of 1930, as amended (19 U.S.C. § 1337), has occurred.

This is also the administrative law judge's Recommended Determination on remedy and bonding, pursuant to Commission rules 210.36(a) and 210.42(a)(1)(ii). The administrative law judge recommends that the Commission issue a limited exclusion order and a cease and desist order. He further recommends that any bond, during the Presidential review period, be in the amount of 100 percent of the entered value for any importation involving infringing products.

APPEARANCES

For Complainant Trend Micro Incorporated:

Raphael V. Lupo
Mark G. Davis
McDermott, Will & Emery
600 13th Street, NW, 12th Floor
Washington, DC 20005-3096

Kenneth S. Korea
Keaton S. Parekh
McDermott, Will & Emery
3150 Porter Drive
Palo Alto, CA 94304-1212

For Respondent Fortinet, Inc.:

Kenneth B. Wilson
Gina M. Steele
Sarah E. Piepmeier
Perkins Coie, LLP
180 Townsend Street
3rd Floor
San Francisco, CA 94107

Sturgis M. Sobin
Leigh A. Bacon
Miller & Chevalier, Chartered
655 Fifteenth Street, NW
Washington, DC 20005

Staff: Rett Snotherly, Esq.

TABLE OF CONTENTS

OPINION

PAGE

ABBREVIATIONS

CBr	Complainant's Post-hearing Brief
CORPFF	Complainant's Objection To Respondents' Proposed Finding
COSPFF	Complainant's Objection To Staff's Proposed Finding
CPFF	Complainant's Proposed Finding
CPHS	Complainant's Pre-hearing Statement
CRBr	Complainant's Post-hearing Reply Brief
CRRPFF	Complainant's Rebuttal Finding to Respondent's Proposed Finding
CRSBr	Complainant's Supplemental Post-hearing Statement
CRRSBr	Complainant's Supplemental Post-hearing Reply statement
CRSPFF	Complainant's Rebuttal Finding To Staff's Proposed Finding
CX	Complainant's Exhibit
RBr	Respondent's Post-hearing Brief
RPHS	Respondent's Pre-hearing Statement
RRBr	Respondent's Post-hearing Reply Brief
RRX	Respondent's Rebuttal Exhibit
ROCPFF	Respondent's Objection To Complainant's Proposed Finding
ROSPFF	Respondent's Objection To Staff's Proposed Finding
RPFF	Respondent's Proposed Finding
RRCPFF	Respondent's Rebuttal Finding To Complainant's Proposed Finding
RRSPFF	Respondent's Rebuttal Finding To Staff's Proposed Finding
RRSBr	Respondent's Supplemental Post-hearing Statement

RRRSBr	Respondent’s Supplemental Post-hearing Reply Statement
RX	Respondent’s Exhibit
SPBr	Staff’s Pre-hearing Brief
SBr	Staff's Post-hearing Brief
SPFF	Staff's Proposed Finding
SRBr	Staff’s Post-hearing Reply Brief
SRRPFF	Staff's Rebuttal Finding To Respondent’s Proposed Finding
SRSBr	Staff's Supplemental Post-hearing Statement
SRRSBr	Staff’s Supplemental Post-hearing Reply Statement
SRCPFF	Staff's Rebuttal Finding To Complainant’s Proposed Finding
Tr.	Transcript Of Pre-hearing Conference And Hearings

I. Procedural History

By notice, which issued on June 3, 2004, the Commission instituted this investigation, pursuant to subsection (b) of section 337 of the Tariff Act of 1930, as amended, 19 U.S.C. § 1337, to determine whether there is a violation of subsection (a)(1)(B) of section 337 in the importation into the United States, the sale for importation into the United States, or the sale within the United States after importation of certain systems for detecting and removing viruses or worms, components thereof, and products containing same by reason of infringement of claims 1-22 of U.S. Patent No. 5,623,600 (the '600 patent) and whether an industry in the United States exists as required by subsection (a)(2) of section 337.

The complaint was filed with the Commission on May 5, 2004 under section 337 of the Tariff Act of 1930, as amended, 19 U.S.C. § 1337, on behalf of Trend Micro Incorporated of Cupertino, California (Trend Micro). Letters supplementing the complaint were filed on May 24 and June 1.[1] The complainant requested that the Commission institute an investigation and, after the investigation, issue a permanent exclusion order and a permanent cease and desist order. In the notice the Commission named as the only respondent Fortinet, Inc., 920 Stewart Drive, Sunnyvale, California 94085 (Fortinet).

Order No. 3, which issued on July 1, 2004, set a target date of August 8, 2005 meaning that any final initial determination on violation should be filed no later than Monday, May 9.

[1] On May 13, 1997, Trend Micro filed a complaint against Network Associates, Inc. in the U.S. District Court for the Northern District of California, wherein it alleged that Network Associates infringed the '600 patent. (Complainant at X.B.1. (Civil Action No. C97-20438 RMW (PVT) ENE (NAI litigation)).) The suit was dismissed pursuant to a settlement agreement that included a license to Network Associates for the use of the '600 patent. (Complaint at X.B.1.; see 35 U.S.C. Section 103 analysis, infra, for other licenses.) On May 5, 2004, Trend Micro, also filed a complaint against Fortinet in the U.S. District Court for the Northern District of California alleging infringement of the '600 patent. (Complaint at X.A.1.) The case is stayed pending the resolution of this investigation.

Order No. 6, which issued on October 12, 2004, terminated the investigation as to claims 2, 5-6, 9-10 and 16-22 of the '600 patent. The Commission, in a notice dated October 27, determined that it would not review Order No. 6. Hence the claims of the '600 patent in issue are claims 1, 3, 4, 7, 8 and 11-15.

On November 17, 2004, the administrative law judge received a "Stipulation Regarding Importation" entered into by complainant and respondent. The administrative law judge also has received a "Stipulation Regarding Customer Support And Use Of Fortinet Products" entered into by complainant and respondent and which was served on December 7.

Order No. 9, which issued on November 30, 2004, ordered the parties to state their positions with supporting documentation on issues in the investigation.

Order No. 13, which issued on December 14, 2004, granted complainant's Motion No. 510-4 for partial summary determination that complainant has satisfied the economic prong of the domestic industry. The Commission determined not to review Order No. 13 in a notice that issued on January 6, 2005.

An evidentiary hearing was conducted on January 24, 25, 26, 27, 28 and 29, 2005 with complainant, respondent and the staff participating. On January 29 the evidentiary record in the investigation was closed and dates for post-hearing submissions set.

On January 28, 2005, respondent moved in Motion No. 510-16 for leave to: 1) take further discovery with respect to a Normal Firewall source code; 2) to proffer the Norman Firewall source code as documentary (and, if electronic versions of such code are obtained, a physical exhibit containing such code) evidence; 3) to identify Kristian Bognaes as a sponsoring witness; and 4) to take the deposition of Bognaes. In Motion No. 510-16, respondent also sought leave to have Bognaes' deposition (or such portions thereof as the parties designate via a joint exhibit), and any associated documentary or physical exhibits, admitted into evidence in lieu of live testimony under Commission rule 210.28(h); and in the alternative, if the record is closed prior to the completion of the above discovery and proffer, to reopen the record to have admitted into the record the source code and related discovery and testimony, as permitted by Commission rule 210.42(g). Order No. 18, which issued on February 4, 2005, granted in part Motion No. 510-16.

On March 3, 2005, complainant filed an unopposed motion to extend the period for filing post-hearing reply briefs and rebuttal findings of fact and conclusions of law. (Motion Docket No. 510-17.) Motion No. 510-17 was granted on March 3. On March 8, 2005, complainant moved to seek leave to file its rebuttals to respondent's post-hearing findings of fact and conclusion of law one-day late. (Motion Docket No. 510-18.) Motion No. 510-18 is granted. Post-hearing submissions, pursuant to the post-hearing submission schedule set on January 29, have been filed.

On March 9, 2005, respondent moved in Motion No. 519-19 for, inter alia, leave to reopen the record and admit into the record certain material. Order No. 19, which issued on March 15, granted Motion No. 510-19 in part which involved, inter alia, setting a second evidentiary hearing date of March 29. On March 29 the evidentiary hearing was conducted pursuant to Order No. 19 and additional exhibits received into evidence. Supplemental post-hearing submissions have been filed. On April 11, complainant filed an unopposed motion to file an errata to its rebuttal findings of fact and conclusions of law. (Motion Docket No. 510-20.) Motion No. 510-20 is granted. Additional post-hearing submissions have been filed. The investigation is now ready for a final initial determination on violation and recommendations on remedy and bond.

These final initial and recommended determinations are based on the record compiled at the hearings and the exhibits admitted into evidence in connection with the January and March 2005 evidentiary hearings. The administrative law judge has also taken into account his observation of the witnesses who appeared before him during the hearings. Proposed findings of fact submitted by the parties not herein adopted, in the form submitted or in substance, are rejected as either not supported by the evidence or as involving immaterial matters and/or as irrelevant. Certain findings of fact included herein have references to supporting evidence in the record. Such references are intended to serve as guides to the testimony and exhibits supporting said findings. They do not necessarily represent complete summaries of the evidence supporting said findings.

II. Parties

See FF 1-53.

III. Jurisdiction

The Commission has personal jurisdiction over respondent Fortinet. (CX-25 at 2.)

As for subject matter jurisdiction, Trend Micro and Fortinet have stipulated to Fortinet's importation of certain hardware components of the accused products. (See CX-300 (Stipulation).) Thus, the parties stipulated, with respect to certain Fortinet products (designated "Fortinet Products" in the Stipulation), that the hardware is manufactured and assembled outside the United States (Stipulation ¶ 3); that the Fortinet Products are sold in the United States (Stipulation ¶ 5); that for other Fortinet products (designated "Fortinet U.S. Products" in the

Stipulation), the FortiASIC content processing chip used in these products is imported into the United States (Stipulation ¶ 8); and that the Fortinet U.S. Products are sold in the United States. (Stipulation ¶ 11.)

With respect to the software component of the Fortinet Products, the parties stipulated that the software is either transmitted electronically to Fortinet's facility in the United States (where it is installed on the hardware) or the software is installed on these products prior to their importation into the United States (Stipulation ¶ 4); and that, as for the Fortinet U.S. Products, the software in those products is transmitted electronically to Fortinet's facility in the United States where it is installed on the hardware. (Stipulation ¶ 10.)

Fortinet argued that the evidence shows that Fortinet's products do not infringe the '600 patent and that, even if infringement were found, there are substantial non-infringing uses for the articles imported. Hence, it argued that subject matter jurisdiction is lacking. (RBr at 20.) The administrative law judge rejects Fortinet's argument. In Bell v. Hood, 327 U.S. 678 (1946) plaintiffs brought suit against the Federal Bureau of Investigation, seeking money damages based on alleged violations of their rights under the Fourth and Fifth Amendments to the Constitution. The District Court dismissed for lack of jurisdiction on the ground that the action did not "arise under the Constitution or laws of the United States." The Supreme Court reversed, holding that since the complaint on its face clearly sought relief based on the Constitution, the District Court must assume jurisdiction to decide whether the allegations state a claim upon which relief can be granted. The Court concluded:

> Jurisdiction, therefore, is not defeated as respondents seem to contend, by the possibility that the averments might fail to state a cause of action on which petitioners could actually recover. For it is well settled that the failure to state a

> proper cause of action calls for a judgement on the merits and not for a dismissal for want of jurisdiction. Whether the complaint states a cause of action on which relief could be granted is a question of law and just as issues of fact it must be decided after and not before the court has assumed jurisdiction over the controversy. If the court does later exercise its jurisdiction to determine that the allegations in the complaint do not state a ground for relief, then dismissal of the case would be on the merits, not for want of jurisdiction.

Bell v. Hood, 317 U.S. at 682 (citations omitted) (emphasis added). In Amgen, Inc. v. United States Int'l Trade Comm'n, 902 F.2d 1532, 1536 (Fed. Cir. 1990), the Federal Circuit specifically found that Amgen's complaint alleged that respondent Chugai was importing rEPO and that rEPO was made by a process covered by a patent in issue and thus, on its face the complaint came within the jurisdiction of the Commission; and that the fact that Amgen was later unable to sustain those allegations was not material to the issue of jurisdiction. It then held that the Commission should have assumed jurisdiction, and, if the facts indicated that Amgen could not obtain relief under section 1337(a)(1)(B)(ii), the Commission should have dismissed the merits. Based on the Stipulation, Bell and Amgen, the administrative law judge finds that there is subject matter jurisdiction existing in this investigation.

IV. Products In Issue

Fortinet's products at issue are Fortinet's FortiGate products, which have gateway-based antivirus capabilities and are currently commercially available in the United States. (RPFF 483, 487 (undisputed).) The FortiGate products are a combination of both hardware and software (Xie, Tr. at 1352).[2] Fortinet's software, FortiOS, is the operating system that runs on the

[2] Michael Xie is the chief technology officer and vice president of engineering for respondent. He has been working at respondent for four years. (Tr. at 1346; see also FF 29-34, 36, 37.)

FortiGate units. (RPFF 490-91 (undisputed).) Specifically, the Fortinet products in issue include the FortiGate-50, FortiGate-50A, FortiGate-60, FortiWiFi-60, FortiGate-100, FortiGate-100A, FortiGate-200, FortiGate-200A, FortiGate-300, FortiGate-300A, FortiGate-400, FortiGate-400A, FortiGate-500, FortiGate-500A, FortiGate-800, FortiGate-800F, FortiGate-1000, FortiGate-4000S (chassis only, must be used in conjunction with FortiBlade-4010 to provide antivirus capabilities), FortiGate-4000P (chassis only, must be used in conjunction with FortiBlade-4010 to provide antivirus capabilities), FortiBlade-4010, and FortiBlade-5001 (must be used in conjunction with a chassis to provide antivirus capabilities, such as the FortiGate-5020, FortiGate-5050, or FortiGate-5140) sold in the United States. (CX-300C at 1.)

The "Fortinet U.S. Products" include the FortiGate-3000, FortiGate-3600, FortiGate-3600LX2, FortiGate-3600LX4, FortiGate-5020 (chassis only, must be used in conjunction with FortiBlade-5001 to provide antivirus capabilities), FortiGate-5050 (chassis only, must be used in conjunction with FortiBlade-5001 to provide antivirus capabilities) and FortiGate-5140 (chassis only, must be used in conjunction with FortiBlade-5001 to provide antivirus capabilities). Each of the Fortinet U.S. Products contains the FortiASIC content processing chip (once chassis and blade(s) are fully assembled, where applicable). Fortinet imports the FortiASIC content processing chip into the United States prior to hardware assembly of the Fortinet U.S. Products. The hardware for each of the Fortinet U.S. Products is assembled in the United States. Fortinet's software is developed outside of the United States and is transmitted electronically to Fortinet's United States facility, where it is installed on the hardware of the Fortinet U.S. Products. (CX-300C.)

Trend Micro's engineers in the United States developed Trend Micro's internet gateway products. (JX-010C at 12.) Trend Micro's internet gateway product was originally named InterScan Virus Wall (ISVW), and was later re-named InterScan Mail (Message) Security Suite (IMSS) and InterScan Web Security Suite (IWSS). (JX-010C at 12.) InterScan VirusWall is still on the market and is offered in different versions. (JX-010C at 13.) Trend Micro also sells other products including, for consumers, PC-Cillin or Virus Buster, and for corporate customers, OfficeScan. In the corporate file server, Trend Micro offers Server Protect, Incorporate Mail Server and Scan Mail. For the domino server, Scan Mail for Domino is also offered. (JX-010C at 14.) Trend Micro also offers hardware products called GateLock and Network Virus Wall. (JX-0010C at 15.)

The products in issue of both Trend Micro and Fortinet include antivirus software that involves a gateway and a computer network. Trend Micro's first product that implemented the concept of the '600 patent was called ISVW. (Chen, Tr. at 35-36.) Since that time, Trend Micro has developed and marketed several products in the United States that embody the '600 patent. (CPFF26 (undisputed).) Currently, Trend Micro's products in the United States, include its ISVW products for Windows NT and UNIX platforms, IMSS and IWSS. (Id.) Trend Micro's products are sold as software that the purchaser then combines with its own hardware. (Mitchell, Tr. at 584.[3]) Fortinet's products, on the other hand, are sold as an encased combination of hardware and software. (See, e.g., CX-399; Lacy, Tr. at 1590.) As part of the hardware, the accused products contain a FortiASIC chip, i.e., an "application specific integrated circuit." (Xie,

[3] John Clifford Mitchell was qualified as complainant's expert witness in the area of computer security and computer networks. (Tr. at 450.) Mattew A. Bishop was qualified as respondent's expert in the area of computer networking and computer security. (Tr. at 1839.) Leroy Paul Lacy was qualified as respondent's expert in network security programming. (Tr. at 1589.)

Tr. at 1373-74.) In addition, the accused products use an operating system Fortinet refers to as FortiOS, and all of the accused products have one of the following three FortiOS versions: FortiOS 2.5, FortiOS 2.8 MR6, and FortiOS 2.8 MR7. The primary difference between FortiOS 2.8 MR6 and FortiOS 2.8 MR7 is that in version FortiOS 2.8 MR7 a "splice-disabled" mode has been eliminated for certain FTP and SMTP transfers. (Gray, Tr. at 1534.[4]) When the accused products operate in "splice-mode," portions of the data are intermittently sent to the destination node in order to avoid what is called "timing out" during virus detection. (CX-205; Gray, Tr. at 295; Mitchell, Tr. at 796-97.) Timing out occurs as a result of a destination node being configured to terminate a communication if it does not receive additional information within a certain amount of time. (Gray, Tr. at 300-01.)

V. The '600 Patent

The '600 patent, titled VIRUS DETECTION AND REMOVAL APPARATUS FOR COMPUTER NETWORKS, has a filing date of September 26, 1995 and was issued on April 22, 1997 to Shuang Ji and Eva Chen with twenty-two claims. The '600 patent was originally assigned by the inventors to Trend Micro Devices, Inc., a Chinese corporation. The U.S. Patent and Trademark Office (PTO) issued a Notice of Assignment for this transfer of April 30, 1996. (CX-229 at TMI00006897.) The '600 patent was subsequently assigned to complainant. (See id. at TMI00006723 (Notice of Recordation issued by the PTO on June 25, 1997).)

Claims 1 and 3 in issue are each directed to a system and read:

> 1. A system for detecting and selectively removing viruses
> in data transfers, the system comprising:

[4] Gray is employed by respondent, as are Jeff Crawford and Ellery D'Souza referenced infra. (FF 45, 47.)

a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus;

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

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

a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmissions of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred; and

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

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

Claims 4, 7-8 and 11-15 in issue are each directed to a method and read:

4. A computer implemented method for detecting viruses in data transfers between a first computer and a second

computer, the method comprising the steps of:

receiving at a server a data transfer request including a destination address;
electronically receiving data at the server;
determining whether the data contains a virus at the server;
performing a preset action on the data using the server if the data contains a virus;
sending the data to the destination address if the data does not contain a virus;
transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus.

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

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

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

receiving a mail message request including a destination address;

electronically receiving the mail message at a server;

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

performing a present action on the mail message if the mail message contains a virus; and

sending the mail message to the destination address if the mail message does not contains a virus.

12. The method of claim 11, wherein the step of determining whether the mail message includes any encoded portions searches for unencoded portions.

13. A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:

receiving a mail message request including a destination address; electronically receiving the mail message at a server; scanning the mail message for encoded portions; determining whether the mail message contains a virus;

performing a present action on the mail message if the mail message contains a virus;

sending the mail message to the destination address if the mail message does not contains a virus; and

wherein the step of sending the mail message to the destination address is performed if the mail message does not contain any encoded portions; the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to node having an address matching the destination address.

> 14. The method of claim 11, wherein the step of determining whether the mail message contains a virus, further comprises the steps of:
>
> storing the message in a temporary file;
> scanning the temporary file for viruses; and
> testing whether the scanning step found a virus.
>
> 15. The method of claim 11, wherein step of scanning is performed using a signature scanning process.

(JX-1.)

The '600 patent, under the heading "BACKGROUND OF THE INVENTION" and subheading "1. Field of the Invention," discloses that the present invention "more particularly" relates to a system and method for detecting and removing computer viruses from file and message transfers between computer networks. (JX-1, col. 1, lns. 10-14.)

The '600 patent, under the subheading "2. Description of the Related Art" discloses:

> During the recent past, the use of computers has become widespread. Moreover, the interconnection of computers into networks has also become prevalent.

(JX-1, col. 1, lns. 15-17.) The inventors then referred to FIG. 1 which was disclosed as "a block diagram of a portion of a prior art information system 20." (JX-1, col. 1, lns. 18-20.) FIG. 1 is as follows:

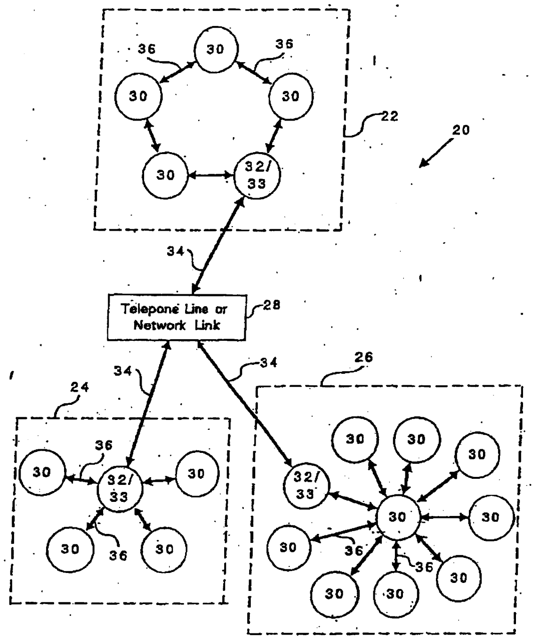


Fig. 1 (Prior Art)

With reference to FIG. 1, the '600 patent discloses:

> The portion of the information system 20 shown comprises a first network 22, a second network 24 and third network 26. This information system 20 is provided only by way of example, and those skilled in the art will realize that the information system 20 may include any number of networks, each of the networks being its own protected domain and having any number of nodes. As shown in FIG. 1, each of the networks 22, 24, 26 is formed from a plurality of nodes 30, 32. Each of the nodes 30, 32 is preferably a microcomputer. The nodes 30, 32 are coupled together to form a network by a plurality of network connections 36. For example, the nodes 30, 32 may be connected together using a token ring format, ethernet format or any of the various other formats known in the art. Each of the networks 22, 24, 26 includes a node 32 that acts as a gateway to link the respective network 22, 24, 26 to other networks 22, 24, 26. Each of the gateway nodes 32 is preferably

> coupled by a standard telephone line connection 34 such as POTS (Plain Old Telephone Service) or a T-1 link to the other gateway nodes 32 through a telephone switching network 28. All communication between the networks 22, 24, 26 is preferably performed through one of the gateway nodes 32.

(JX-1, col. 1, lns. 19-42.)

As seen from the foregoing and FIG. 1, at the time the application for the ‘600 patent was filed on September 26, 1995, the interconnection of computers into networks, e.g., networks 22, 24, 26, had become prevalent with each network having any number of nodes, e.g., nodes 30, 32, which were preferably microcomputers, with the nodes connected by a variety of network connections. As seen also from the foregoing, the inventors termed the node 32 as a "gateway node" which linked the respective networks 22, 24, 26 to other networks 22, 24, 26.

FIG. 1 is also described by the inventors as "a block diagram of a prior art information system with a plurality of networks and a plurality of nodes upon which the present invention operates." (JX-1, col. 3, lns. 19-22.) However, the inventors further refer to FIG. 1 under the DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT, stating:

> The virus detection system and method of the present invention preferably operates on an information system 20 as has been described above with reference to FIG.1. The present inventions, like the prior art, preferably includes a plurality of node systems 30 and at least one gateway node 33 [which is referenced in FIG. 1] for each network 22, 24, 26. However, the present invention is different from the prior art because it provides novel gateway node 33 that also performs virus detection for all files being transmitted into or out of a network. Furthermore, the novel gateway node 33 also performs virus detection on all messages being transmitted into or out of an associated network.

(JX-1, col. 3, lns. 52-63.) Thus the inventors utilize FIG. 1 to describe their invention.

VI. Person Of Ordinary Skill In Pertinent Art

Complainant argued that one of ordinary skill in the art of the ‘600 patent is a person with a Bachelor of Science in Computer Science or Computer Engineering with two or three years of experience in the field of networking or virus detection. (CBr at 7-8.)

Respondent argued that a person of ordinary skill in the art of the ‘600 patent would have had a Bachelor’s degree in computer science (or equivalent), experience with the UNIX operating system, networking and anti-virus, and two to three years of work experience. (RBr at 11.)

The staff argued that person of ordinary skill in the art of the ‘600 patent in 1995 would have had an undergraduate degree in computer science (or equivalent knowledge) and two or three years of additional work experience in networking and operating systems and, to a much lesser extent, some knowledge of anti-virus software. (SBr at 55.)

It is essential, as disclosed by the ‘600 patent, that the claimed invention use conventional operating systems known to those skilled in the art. (See JX-1, col. 5, lns. 11-16, FIG. 3.) Also, those skilled in the art should be familiar with different networking configurations and have knowledge of various virus detection methods. (See JX-1, col. 4, lns. 25-32, col. 7, lns. 58-65, FIG. 6B.) Hence, the administrative law judge finds that a person of ordinary skill in the art of the ‘600 patent in the 1995 time frame period, when the application for the ‘600 patent was filed, should have had an undergraduate degree in computer science (or equivalent) and further have had some experience with conventional operating systems and have had knowledge of various virus detection methods.

VII. Claim Interpretation

Claim interpretation, as to each of the asserted claims, is a question of law. Markman v. Westview Instruments, Inc., 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc), aff'd, 517 U.S. 370 (1996); Cybor Corp. v. FAS Techs., Inc.,138 F.3d 1448, 1455 (Fed. Cir. 1998). In construing claims, the court should first look to intrinsic evidence consisting of the language of the claims, the specification and the prosecution history as it "is the most significant source of the legally operative meaning of disputed claim language." Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996); see Bell Atl. Network Servs., Inc. v. Covad Communications Group, Inc., 262 F.3d 1258, 1267 (Fed. Cir. 2001). Claim construction analysis begins with words of the claim. Tex. Digital Sys., Inc. v. Telegenix, Inc., 308 F.3d 1193, 1201 (Fed. Cir. 2002). The ordinary and customary meaning of a claim term may be determined by reviewing a variety of sources, which may include the claims themselves, dictionaries and treatises, and the written description, the drawings and the prosecution history. Ferguson Beauregard/Logic Controls v. Mega Sys., LLC, 350 F.3d 1327, 1338 (Fed. Cir. 2003).

In addition to the intrinsic evidence, the administrative law judge may, but need not, consider extrinsic evidence when interpreting the claims. Extrinsic evidence consists of all evidence external to the patent and the prosecution history, including inventor testimony, expert testimony, and learned treatises.[5] This extrinsic evidence may be helpful in explaining scientific principles, the meaning of technical terms, and terms of art. See Vitronics Corp., 90 F.3d at 1583; Markman, 52 F.3d at 980. However, "[e]xtrinsic evidence is to be used for the court's

[5] Although dictionaries are technically extrinsic evidence, it is proper to consult a dictionary to determine the ordinary and accustomed meaning of a claim term. See, e.g., Kopykake Enters., Inc. v. Lucks Co., 264 F.3d 1377, 1382 (Fed. Cir. 2001).

understanding of the patent, not for the purpose of varying or contradicting the terms of the claims." Markman, 52 F.3d at 981. Indeed, in all cases, "a construing court does not accord the specification, prosecution history, and other relevant evidence the same weight as the claims themselves, but consults these sources to give the necessary context to the claim language." Eastman Kodak Co. v. Goodyear Tire & Rubber Co., 114 F.3d 1547, 1552 (Fed. Cir. 1997).

Patent claims should be construed so as to maintain their validity. If more than one reasonable interpretation is possible, the construction that preserves the claim's validity should be chosen. See Modine Mfg. Co. v. United States Int'l Trade Comm'n, 75 F.3d 1545 (Fed. Cir. 1996), cert. denied, 518 U.S. 1005 (1996). However, if the only reasonable interpretation renders the claim invalid, then the claim should be found invalid. See, e.g., Rhine v. Casio, Inc., 183 F.3d 1342, 1345 (Fed. Cir. 1999).

According to the staff, the following are the disputed claim terms: (i) communications unit, (ii) daemon, (iii) encoded portions, (iv) processing unit, (v) proxy server, (vi) scanning, (vii) server (viii) temporary file and (ix) virus. (SBr 16-38.)

Complainant argued that there appears to be only six claim terms in dispute, viz. (i), (ii), (v), (vi), (viii) and (ix), supra. It noted that it accepts the staff's construction of "encoded portions" and thus complainant does not believe a dispute exists as to that term.[6] (CBr at 11.)

Respondent argued that (i), (ii), (v), (viii) and (ix) supra are in dispute. (RBr at 22-45.) In a footnote in its post-hearing brief, respondent stated that the parties appear to either agree

[6] The staff has interpreted "encoded portions" as data that has been changed from its native form by use of a code. (SBr at 14.) Respondent interpreted the phrase as "portion(s) of data that has been converted by use of a code." (Appendix B to RBr.) The administrative law judge finds the interpretations of respondent and the staff substantially identical.

upon a definition, or to agree that "ordinary meaning" should govern, for the following terms and phrases except to the extent the phrases and terms include language which is disputed: (1) data, (2) receiving at a server a data transfer request including a destination address, (3) performing a preset action on the data using the server if the data contains a virus, (4) sending the data to the destination address if the data does not contain a virus, (5) destination address, (6) transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus, (7) electronically receiving data at the server, (8) determining whether the data contains a virus at the server, (9) SMTP daemon, (10) SMTP proxy server, (11) processing unit, (12) determining whether the data is of a type likely to contain a virus, and (13) server. (RBr at 21, n.7.) It further stated that the agreed upon definitions, or a statement that the parties agree upon ordinary meaning, can be found as Appendix B to its RBr.[7] (Id.)

[7] Respondent, in Appendix B, as to the claimed term "determining whether data is of a type that is likely to contain a virus," stated:

> Ordinary meaning. Trend Micro proposes that ordinary meaning is "determining whether the data, because of its characteristic (sic) is deemed more likely to contain a virus than other data." Fortinet believes that Trend Micro's reference to "its characteristic" renders the phrase more confusing, rather than less, but substantively, Fortinet does not have a problem with Trend Micro's definition.

As to the claimed term "electronically receiving data at the server," in Appendix B, respondent stated:

> Ordinary meaning. Trend Micro proposes that ordinary meaning is "receiving data at the server through the use of electronic devices." Fortinet believes that Trend Micro's proposed definition is confusing insofar as it vaguely references "electronic devices," but Fortinet does not have a substantive problem with the proposal.

(continued...)

Respondent represented that the parties' respective definitions for the terms "encoded portions" and "scanning" are set forth in Appendix A to RBr. With regard to "encoded portions," it believed that Trend Micro's proposed definition would render the claims of the '600 patent more confusing, rather than clarify the claim language and, therefore, favored its own construction or that of the staff. Respondent and the staff did not believe that there is much of a substantive difference between respondent's and Trend Micro's proposed definitions for "encoded portions." Also, the staff and respondent did not believe that the inclusion of the example of a file attached to an electronic mail message as Trend Micro proposed in its proposed definition of "encoded portions" aided in the understanding of the term. The staff argued that the phrase "into a different form" is inappropriately broad, and respondent agreed. Regarding the term "scanning," respondent did not believe this term is in dispute among the private parties and further did not think there is much of a substantive difference between its definition and that of the staff. (RBr at 20-21.)

[7](...continued)
As to the claimed term "server", respondent, in its Appendix B, stated:

> Fortinet believes the correct construction of server is "a computer or program that performs services for other computers or programs." Trend Micro believes the correct construction of server is "a computer system that performs specified functions for other computers (which are called "clients") or software running on a computer system that performs such server functions." The Staff agrees with Trend Micro's proposed definition. Trend Micro has stated that the parties appear to be largely, if not completely, in agreement. Fortinet agrees, but believes the Court should adopt its proposed definition over that proposed by Trend Micro because its proposal is more clearly written, and Trend Micro concedes that subsantively the two proposals are essentially the same.

A. The Claimed Term "Communications Unit"

The term "communications unit" appears in claim 1 in issue, and throughout the specification of the '600 patent. The following are the proposed constructions of the parties for the claimed term "communications unit:"

Fortinet's And Staff's Proposed Construction of "Communications Unit"	Trend Micro's Proposed Construction of "Communications Unit"
A device for facilitating communications between computers or computer networks.	A device used to communicate between a gateway node and other networks.

(CBr at 14; RBr at 28; SBr at 10.)

The plain language of asserted claim 1 indicates that the claimed communications unit is a unit which at least receives and sends data in response to control signals with said unit having an input and an output. The parties also agree that the claimed communications unit is a unit that is used to communicate or facilitate communication between at least two points. (CBr at 15; RBr at 29; SBr at 10.) The parties, however, differ as to the two points between which any communication occurs. Thus in issue is whether a "communications unit" must either be on a gateway node or must only communicate between gateway nodes[8] and other networks as Trend Micro appears to argue or whether the term "communications unit" is broad enough to include

[8] While the term "gateway node" is frequently found in the specification of the '600 patent, it does not appear in the asserted claims of said patent.

also communications between computer nodes within a given network, i.e. intra-network traffic as Fortinet and the staff argued. (See RBr at 32; SBr at 10-11.)

Claim 1 of the '600 patent discloses "a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output." See supra. Claim 1 does not on its face suggest where the claimed system (and therefore the communications unit) must reside. (Id.) Thus, the plain language of the claim is broad enough to cover communications between computer nodes within a given network.

The specification of the '600 patent under the heading SUMMARY OF THE INVENTION discloses:

> The central processing unit of the gateway node also executes the FTP proxy server for transmitting and receiving files over the communications unit, and executes the SMTP proxy server for transmitting and receiving messages over the communications unit.

(JX-1, col. 2, lns. 54-58.) Thereafter, under the heading DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT, referring to the following FIG. 2,:

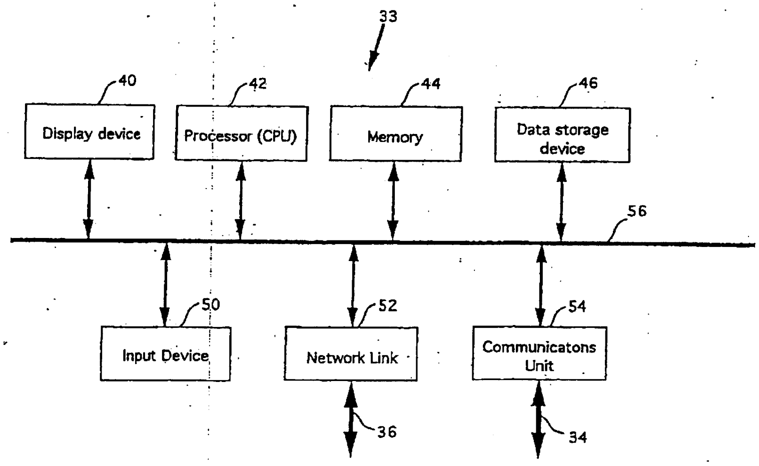


Fig. 2

the specification discloses:

> The bus 56 is also coupled to the communications unit 54 to facilitate communication between the gateway node 33 and the other networks. Specifically, the communications unit 54 is coupled to the CPU 42 for sending data and message to other networks. For example, the communications unit 54 may be a modem, a bridge or a router coupled to the other networks in a conventional manner. In the preferred embodiment of the present invention, the communications unit 54 is preferably a router. The communications unit 54 is in turn coupled to other networks via a media 34 such as a dedicated T-1 phone line, fiber optics, or any one of a number of conventional connecting methods.
>
> The CPU 42, under the guidance and control of instructions received from the memory 44 and from the user through the input device 50, provides signals for sending and receiving data using the communications unit 54. The transfer of data between networks is broken down into the sending and receiving files and messages which in turn are broken down into packets. The methods of the present invention employ a virus detection scheme that is applied to all transfers of messages and files into or out of a network via its gateway node 33.

(JX-1, col. 4, lns. 33-55 (emphasis added).) In addition, the specification, referring to FIG. 3[9] of the '600 patent, discloses:

> While the apparatus of the present invention, in particular the FTP proxy server 60 and SMTP proxy server 62, has been described above as being located and preferably is located on the gateway node 33, those skilled in the art will realize that the apparatus of the present invention could also be included on a FTP server or a world wide web server for scanning files and messages as they are downloaded from the web. Furthermore, in an alternate embodiment, the apparatus of the present invention may be included in each node of a network for performing virus detection on all messages received or transmitted from that node.

(JX-1, col. 5, lns. 28-38 (emphasis added).) Hence, the administrative judge finds that the specification of the '600 patent would disclose to a person of ordinary skill in the art that the claimed term "communications unit" is not limited to communications between gateway nodes and other networks but also may cover communications within a network.

[9] FIG. 3, which has an "operating system" 64, is described as a "block diagram of a preferred embodiment for a memory of the gateway node including the apparatus of the present invention." (JX-1, col. 3, lns. 26-29.) It is further disclosed as "the preferred embodiment of the memory 44 for the gateway node 33." (JX-1, col. 4, lns. 56-63.) With reference to an operating system, the '600 patent discloses:

> The present invention preferably uses a conventional operating system 28 such as Berkeley Software Distribution UNIX. Those skilled in the art will realize how the present invention may be readily adapted for use with other operating systems such as MACINTOSH System Software version 7.1, DOS, WINDOWS or WINDOWS NT. The memory 44 may also include a variety of different application programs 68 including but not limited to computer drawing programs, word processing programs, and spreadsheet programs.

(JX-1, col. 5, lns. 9-19.)

The administrative law judge further finds that Trend Micro's proposed construction is contrary to the prosecution history of the '600 patent. Referring to the prosecution history, the application for the '600 patent was filed with twenty-five original claims. Original claim 1 read:

> 1. A system for detecting and selectively removing viruses in data transfers, the system comprising:
>
> a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus;
>
> a communications unit for receiving and sending data in responses to control signals, the communications unit have an input and an output[10]; and
>
> a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted.

(JX-2 at FHC000600.)

A "Petition To Make Special" was received by the PTO on July 2, 1996. Applicants in that petition reported that a search resulted in the identification of certain U.S. patent documents, which included U.S. Patent No. 5,511,163 which had issued to Lerche et al. A "detailed discussion" of the identified references was provided. (JX-2 at FHC 000693-705.) A PTO paper mailed September 5, 1996 granted said petition. (JX-2 at FHC 000706.)

[10] A comparison of original claim 1 and asserted claim 1 in issue shows that original claim 1 contains the exact same language for the "communications unit" that appears in claim 1 as issued.

After the filing on July 2, 1996 of the "Petition To Make Special," the Examiner, in an Office Action dated August 27, 1996, stated, inter alia:

> 8. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lerche et al. United States Letters Patent No. 5,511,163 in view of Hile et al. United States Letters Patent No. 5,319,776.
>
> As per claim 1:
>
> Lerche et al. substantially teach the claimed system for detecting viruses in data transfers, the system comprising:
>
> a) a memory for storing data and routines, see the teachings by Lerche et al. regarding the personal computer, fig. 1. In the memory is stored a virus scan program to scan the transferred data favoring for virus infection;
>
> b) a communications unit for receiving and sending data, figure 2- - the Token-Ring adaptor has an input and an output;
>
> c) a network adaptor to receive information on the network. "The network adaptor is connected to a computer [processing unit] which together with the adaptor can perform an assembling and scanning of substantially all files on the network and carry out a recognition of virus signatures." Emphasis added. If a virus signature is detected in a file, information is simultaneously provided on the transmitting stations and the receiving stations and an alarm is activated, whereby a further spreading of the virus can be prevented.
>
> Although, Lerche et al. teach scanning for viruses in transferred data, Lerche et al. do not explicitly disclose selectively transferring data depending on the existence of viruses in the data being transmitted.
>
> However, Hile et al. in an analogous art teach that when virus is detected, the virus detection function inform the user that a virus has been detected and gives the user the option to cancel the transfer–suggesting selectively transferring a file or not.
>
> Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the virus detection system as disclosed by Lerche et al. by including means and step to selectively transfer data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Hile et al., to

> give the user the option to cancel the transfer of a file or data that is found to be infected with a virus.

(JX-2 at FHC 000636-637.)

While the Examiner in the Office Action of August 27, 1996 relied on the Lerche patent as the basic reference in rejecting original claim 1 under 35 U.S.C §103(a), complainant's expert Mitchell agreed that the Lerche patent does not disclose a gateway node. (Tr. at 931-32.) He further stated that the Examiner in the August 27, 1996 Office Action found that the Lerche patent discloses a communications unit despite the fact that said unit in the Lerche patent does not facilitate communication between a gateway node and other networks. (Tr. at 934-35.) Moreover, Mitchell testified that routers are used in communications between computers within the same networks. (Tr. at 473-74; see JX-1, col. 4, lns. 38-40 (disclosing that communications unit may be a router).) Complainant argued that applicants in the prosecution stated that:

> Applicant's claimed invention prevents the spread of viruses in data transfers which are routed through the server such as those between a first computer outside the server's network and a second computer inside the network. By contrast, Lerche et al. observes local network traffic and reacts only to viruses which have already entered the network by issuing alarms or vaccines to the affected parties.

(CBr at 17, quoting JX-2 at FHC000703.) Complainant, however, failed to point out that those statements were made by applicants in the "Petition To Make Special" filed July 2, 1996 which was before issuance of the Office Action of August 27, 1996. Moreover, earlier in the "Petition To Make Special," it was argued that:

> [a]pplicant's claimed invention provides for the detection and selective removal of viruses in data transfers by communicating or transmitting the transferred data to a server, determining whether the data contains a virus at the server, performing data handling actions on the transferred data where a virus is detected , and selectively allowing the transfer of the data to a destination based upon the presence of a virus

> in the data. Since Applicant's [sic] claimed invention can selectively stop completion of a transfer based upon the detection of a virus, it can prevent the virus from ever penetrating a network (or permeating, where an intranetwork transfer is routed through the server, or leaving, where the destination is outside the network). Moreover, since the server participates in the transfer of data, a variety of virus detection techniques may be implemented in addition to signature scanning such as emulation. Additionally, again because the server participates in the transfer of data, remedies such as removal of the virus from the affected file may be undertaken so that clean data may be exchanged to or from a computer on the network.

(JX-2 at FHC000697 (emphasis added).)

The construction proposed by Fortinet and the staff is found further to be consistent with contemporaneous dictionary definitions which generally define the term "communications" in the computer science context as a "transfer of data among functional units by means of data transmission according to a protocol." (RX-202 at 167, IBM Dictionary of Computing (10th Edition, 1993 (IBM Dictionary).) Unit is defined as "a device having a special function" by the IBM Dictionary. (Id. at 718). Combining "communications" and "unit," the IBM Dictionary defines the term as "a device having the function of transferring data among functional units by means of data transmission, according to a protocol." (Id. at 167, 718.) Combining the definitions of "communications" and "unit" that appear in Webster's New World Dictionary of Computer Terms (5th Edition, 1994), defines the term as "a device having the function of transferring information from one point to another." (RX-195 at 102, 598.) None of these definitions suggest that a communications unit should be limited to a gateway.

Based on the foregoing, the administrative law judge finds that the proper construction of the claimed term "communications unit" is a unit which receives and sends data in response to control signals with said unit having an input and an output and with said unit facilitating communications between computers or computer networks.

B. The Claimed Term "Server"

The claimed term "server" is found in claims in issue and in certain instances, said term is modified by the word "proxy," and/or "SMTP proxy." However, the term is also found in claims in issue where there is no such modification, including claims 4, 7, 8, 11, 12, 14 and 15. Independent claim 13 in issue states that "the server includes a SMTP proxy server" which would indicate to a person of ordinary skill that the claimed term "server" is broader in meaning than the term "proxy server."

Respondent, in its Appendix B of its RBr, set forth what it considered the positions of the parties as for the proposed construction of the claimed term "server." (See fn. 7 supra (relating to respondent's Appendix B).) Respondent also at the pre-hearing conference specifically stated that it doesn't mind complainant's proposed construction of server to the extent that it is defined as "a computer system that performs specified functions for other computers or software running on a computer system that performs such server functions." (Tr. at 111-12.) The staff noted that a server may be software performing a service for a client program running on the same computer; that it appears that Fortinet's construction ("a computer or program that performs services for other computers or programs") may be the more accurate, citing Newton's Telecom Dictionary (17th ed. 2001) ("A server is a program which provides some service to other (client) programs."), which the staff argued is due to the fact that it is not altogether clear that Trend Micro's construction would cover the situation where a client and server program reside on the same computer system; and that the presence of a "server" necessitates, by definition, interaction with "a client" (either hardware or software) that it serves and "[i]n general, a server is a process that waits for a client to contact it, requesting some type of service," citing RX-7 at FHC0003542 (excerpt from "Advanced Programming in the UNIX Environment"). (SBr at 32-33.)

The administrative law judge finds that the proper construction of the claimed term "server" is "a computer and/or software that performs services for other computers or programs," which construction he finds consistent with the use of the term server throughout the '600 patent. (See, e.g., JX-1 col. 2, lns. 54-61; col. 5, lns. 28-35; col. 6, lns. 45-48; col. 7, lns. 51-67; col. 9, lns. 43-48; claims 1-5, 7, 9-11, 13 and 17.) Said construction is also found consistent with how a person of ordinary skill in the art would have understood the term server as of the filing date of the '600 patent. (See SX-4 at 153 (defining server as "(a) software that allows a computer to offer a service to another computer. [] (b) The computer on which the server software runs."); accord SX-7 at 513.) Based on the foregoing, the administrative law judge finds that a person of ordinary skill in the art, as of the filing date of the '600 patent, would have understood that a "server" would not necessarily be limited to either hardware or software, but could include both hardware and software.

C. The Claimed Term "Daemon"

The claimed term "daemon" is in independent claim 1 in issue. Dependent claims 3 and 13 in issue refer to "SMTP daemon." The following are the proposed constructions of the parties for the claimed term "daemon":

Trend Micro's Construction of "Daemon."	Staff's Construction of "Daemon."	Fortinet's Construction of "Daemon."
A server program that runs without supervision and that provides services to other programs.	A program that runs without user (i.e., human) intervention.	A program that works unobtrusively in the background.

(SBr at 12.)

Claim 1 in issue, in reciting "daemon," characterizes "daemon" as:

> 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.

(JX-1, col. 12, lns. 25-32.) Dependent claim 3 and independent claim 13 in issue recite an "SMTP daemon."[11] (See JX-1.) The claims however do not indicate whether the claimed "daemon" should be limited to a program that provides services to other programs.

The administrative law judge finds that the plain language of claim 1 indicates that a daemon at least transfers data from a proxy server, in response to control signals from the proxy server, with the daemon having a control input, a data input and a data output and with said control input coupled to the control output of the proxy server for receiving control signals and with said data input coupled to the data output of the proxy server for receiving the data to be transferred. All the parties also appear to agree that the claimed "daemon" is a program that runs

[11] The '600 patent defines SMTP as a "Simple Mail Transfer Protocol." (JX-1, col. 2, lns. 49-51.)

"without supervision" or "without user (i.e., human) intervention." (CBr at 17; RBr at 41; SBr at 12.) The parties, however, disagree as to whether a program must be a server in order to be a daemon, i.e., whether a daemon is a "server program," and whether it provides services to other programs, i.e., whether the definition of "daemon" should be limited to a program that provides services to other programs.

It is a fact that claims 1, 3 and 13 in issue separately refer to server and daemon. Hence, to avoid redundancy the administrative law judge finds that a daemon is not merely "a computer and/or a program that performs services for other computers or programs," which the administrative law judge has found how a person of ordinary skill in the art would define "server."

Referring to the specification of the '600 patent, while the specification indicates that a daemon may be a program executed by the gateway node which includes a server (JX-1, col. 9, ln. 53 - col. 10; ln. 25, col. 14, lns. 24-25), the specification also specifically states that "[t]he daemon 70 is a program that is part of the operating system 64, and it runs in the background." (JX-1, col. 7, lns. 5-6.) The specification further explains that "[t]he FTP daemon 78 is a program executed by the gateway node 33 that communicates the transfer commands to the server task 82...." (JX-1, col. 7, lns. 45-48.)

Complainant argued that "daemon" is defined in Webster's New World Dictionary of Computer Terms at 129 (6th ed. 1997) (RX-195) as "[a] program, usually on a computer running UNIX, that serves obscure function (such as routing e-mail to its recipients) and usually has a very limited user interface." (CBr at 18 (emphasis by complainant).) Complainant, however, acknowledges that the IBM Dictionary of Computing at 163 (10th ed. 1993) (RX-202) defines a "daemon" as "[i]n the AIX operating system, a program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically." (CBr at 18 (emphasis added by the administrative law judge).)

Based on the foregoing, the administrative law judge finds that a person of ordinary skill in the art would interpret the claimed daemon as transferring data from a proxy server, in response to control signals from the proxy server, with the daemon having a control input, a data input and a data output and with said control input coupled to the control output of the proxy server for receiving control signals and with said data input coupled to the data output of the proxy server for receiving the data to be transferred. He further finds nothing in the intrinsic evidence the would limit the claimed term "daemon" to a program that provides services to other programs. Rather, he finds that a person of ordinary skill in the art, in the critical time period, would understand the claimed term daemon from the intrinsic evidence to be a program that runs without user (i.e. human) intervention and is further not limited to providing services to other programs, but rather is a program that is part of the operating systems and runs in the background. Also, he finds a person of ordinary skill would interpret SMTP daemon as a daemon that uses the simple mail transfer protocol in the underlying mail message transfer.

D. The Claimed Term "Virus"

The term "virus" or "viruses" is found in each of the asserted claims either directly or through dependency. In issue is how one of ordinary skill in the art would interpret the claimed term virus when the '600 patent application was filed on September 26, 1995. The following are the proposed constructions of the parties for the claimed term "virus":

Fortinet's Proposed Construction of "Virus"	Trend Micro's Proposed Construction of "Virus"	Staff's Proposed Construction of "Virus"
Malicious code.	A section of malicious code that is buried or hidden in another program. When executed, the malicious code may attach itself to other programs, open a backdoor for a hacker or other malicious code, destroy data, perform a prank, or other actions harmful to the server or recipient client computer.	The staff agrees with Fortinet's construction, and in particular agrees that the term as used in the '600 patent covers a form of malicious code referred to as a worm.

(CBr at 11; RBr at 23; SBr at 35.) All of the parties rely on, inter alia, contemporaneous dictionary definitions and documents to support their proposed constructions. Thus, complainant argued:

> Those of ordinary skill in the art at the time of the invention distinguished between viruses and worms. CFF215. One such example is found in CX-395, the 1995 FAQ, of which Fortinet's expert Dr. Bishop was a contributing author. CFF216. This 1995 FAQ sheet is dated the same year that the patent was filed. This 1995 FAQ sheet provides different definitions for "virus" and "worms" that clearly distinguishes them. CFF216-18. In particular, the 1995 [FAQ sheet] defines a "computer WORM" as "a self-contained program (or set of programs), that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections))." CFF218. On the other hand, the 1995 FAQ separately defines "viruses" as "a self-replicating program containing code that explicitly copies itself and that can 'infect' other programs by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the virus." CFF217. Most notably, the FAQ specifically distinguishes between "worms" and "viruses" by stating that "unlike viruses, worms do not need to attached [sic] themselves to a host program." CFF219.

(CBr at 13 (emphasis in original).) Respondent argued:

> Contemporaneous dictionary definitions and documents also support Fortinet's and the Staffs pre-hearing position that virus should be defined as malicious

> content, and specifically that the term virus includes worms. (RPFF 654, RX-195, Webster's New World Dictionary of Computer Terms (5th Edition, 1994) defines "virus" as "a computer program that can wreak havoc on a system either by destroying data or simply gumming up the works"; RPFF 655, RX-202, IBM Dictionary of Computing (10th Edition, 1993) defines "virus" as a "self-propagating program that infects and may damage another program; malicious logic that consumes storage and attempts to violate data security (attack); a program which places copies of itself into connected systems and that may do damage or waste resources; a copy protection program that destroys stored data when it detects an illegally copied program.").
>
> Although, Dr. Mitchell testified that he was aware of a FAQ document that drew a distinction between viruses, worms and Trojan horses, that document actually supports Fortinet's claim construction position. (RPFF 698). CX-395 is the FAQ document on which Dr. Mitchell based his conclusion that in the 1995 time frame, a distinction was drawn between viruses, worms and Trojan horses. (RPFF 699). Dr. Mitchell agrees that CX-395 is one indication of how the term "virus" was understood in 1995. (RPFF 700). Yet CX-395 strongly supports Fortinet's construction of virus, as it states that "many people use the term virus loosely to cover any sort of program that tries to hide its potentially malicious function and/or tries to spread onto as many computers as possible, though some of these programs may more correctly be called worms or Trojan horses." (RPFF 701). Dr. Mitchell admits, as he must, that in the 1995 time frame, many people did indeed use the term virus loosely to cover any sort of program that tries to hide its potentially malicious function and/or tries to spread onto as many computers as possible, though some of these programs may more correctly be called worms or Trojan horses. (RPFF 702). Similarly, manufacturers and sellers of virus scanning software used the term "anti-virus" software to refer to software that detected and removed worms. (RPFF 460, 705-06).

(RBr at 24-25.) The staff argued:

> [ ] Fortinet's expert witness, Dr. Bishop, persuasively testified that the term "virus" was often used as a term for malicious code in general, a term that included "worm." Bishop Tr. 1879-80; RDX-10; *Newton's Telecom Dictionary* (11th ed. 1996) ("virus" and "worm" both defined as a program capable of replicating itself).

(SBr at 36.)

The administrative law judge finds that the citations by the parties to contemporaneous documents are not definitive in determining how a person of ordinary skill in the art, in the critical time frame, would interpret the claimed term "virus" as it is used in the '600 patent in view of the fact that contemporaneous documents vary as to the usage of "virus." Rather, he finds that the person would look to how the word "virus" is used in the '600 patent.

Complainant argued that the "inventors of the '600 patent opted to act as their own lexicographers and provided a specific meaning for the term virus." (CBr at 12.) The inventors under the subheading "Description of the Related Art" stated:

> One particular problem that has plagued computers, in particular microcomputers, has been computer viruses and worms. A computer virus is a section of code that is buried or hidden in another program. Once the program is executed, the code is activated and attaches itself to other programs in the system. Infected programs in turn copy the code to other programs. The effect of such viruses can be simple pranks that cause a message to be displayed on the screen or more serious effects such as destruction of programs and data. Another problem in the prior art is worms. Worms are destructive programs that replicate themselves throughout disk and memory using up all available resources eventually causing the computer system to crash. Obviously, because of the destructive nature of worms and viruses, there is a need for eliminating them from computers and networks.
>
> The prior art has attempted to reduce the effects of viruses and prevent their proliferation by using various virus detection programs. . . .

(JX-1, col. 1, lns. 45-60 (emphasis added).) Thus, the inventors refer to only one particular problem that plagued computers, viz. "computer viruses and worms," which problem equated viruses and worms.[12] Thereafter, after providing separate definitions for "computer virus" and "worms" and indicating "a need" for eliminating "them" (worms and viruses), the inventors disclose how the prior art has attempted to reduce the effects of "viruses." Then the inventors in

[12] The caption for this investigation, CERTAIN SYSTEMS FOR DETECTION AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME, does not differentiate between a system for detecting and removing viruses and a system for detecting and removing worms.

the specification, after referencing prior art, disclose how the prior art approaches have shortcomings with respect to "viruses" and indicate a need for a system and method for effectively detecting "viruses." (JX-1, col. 2, lns. 12-33.) Under the heading SUMMARY OF THE INVENTION, the inventors disclose how the present invention overcomes the limitations and shortcomings of the prior art with an apparatus and method for detecting and eliminating "viruses" on a computer network. (JX-1, col. 2, lns. 39-43.)

The administrative law judge finds it significant that the inventors, in '600 patent, other than initially providing separate definitions for "computer virus" and "worms" after the recitation of "[o]ne particular problem" (JX-1, col. 1, lns. 45-55), make no distinction between scanning for viruses and scanning for worms. In view of the inventors' statement that "because of the destructive nature of worms and viruses, there is a need for eliminating them from computers and networks," the earlier recitation by the inventors of only "[o]ne particular problem" (JX-1, col. 1, lns. 43-44, 55-56) and the fact that there is no distinction in the '600 patent between scanning for viruses and scanning for worms, the administrative law judge finds that a person of ordinary skill in the art would interpret the term "virus(es)" as found in the '600 patent at col. 1, ln. 58 and thereafter, as well as in the title, abstract and col. 1, lns. 10-12 of the '600 patent to mean malicious code and to be a shorthand for both worms, as defined at JX-1, col. 1, lns. 52-55, and "computer virus," as defined at JX-1, col. 1, lns. 45-51.

E. The Claimed Term "Temporary File"

Independent claim 11 recites "storing each encoded portion of the mail message in a separate temporary file." Claim 14, dependent on claim 11, requires "storing the [mail] message in a temporary file" and "scanning the temporary file for viruses." Trend Micro's proposed construction of "temporary file" is "a non-permanent collection of related records treated as a unit." (CBr at 23.) The staff argued that complainant's proposed construction is "essentially correct." (SBr at 33.) Respondent argued that Trend Micro's definition "might be useable if added to the end of the definition were the phrase 'with an assigned name so that the operating system can refer to it through a system call.'" (RBr at 45.)

Webster's dictionary defines "temporary" as "lasting or effective for a limited time only, not permanent." (CDX-178, citing Webster's College Dictionary (1991) at 1374.) The IEEE Dictionary defines a "file" as a collection of related records treated as a unit." (CDX-178, citing IEEE Standard Dictionary of Electrical and Electric Terms (3d Ed. 1984).) Another dictionary defines a "temporary file" as "[a] file created either in memory or on disk, by the operating system or some other program, to be used during a session and then discarded." (CDX-178, citing Microsoft Press Computer Dictionary (CX-564); see also CX-568 (21st Century Dictionary of Computer Terms).) A "temporary file" is also defined as "[a] file that can be erased or overwritten when it is no longer needed. Contrast with permanent file." (CDX-178, citing IBM Dictionary of Computing at 685.) Hence, the administrative law judge finds that dictionary definitions support Trend Micro's proposed construction. In addition, in the prosecution of '600 patent, the Examiner in his initial rejection of claim 6 stated that the limitation of "storing the data in a temporary file at the server" was taught by the Hile patent by virtue of the fact that the incoming data was placed in the input buffer. (JX-2 at FHC 000639, citing Hile, col. 4, ln. 7.) The administrative law judge finds that the Hile patent makes clear that the input buffer "comprises a portion of RAM," i.e., volatile memory. (RX-158, col. 2, ln. 67.) Thus, he finds that the Examiner's conclusion indicates that a data record residing in RAM can constitute a temporary file.

Based on the foregoing, the administrative law judge finds that a person of ordinary skill in the art would interpret temporary file as a non-permanent collection of related records treated as a unit and would conclude that a data record residing in RAM can constitute a temporary file.

F. The Claimed Term "Scanning"

Independent claim 1 in issue states in part "a server for scanning data for a virus" and "proxy server scanning the data to be transferred for virus." Independent claim 11 in issue states in part "scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses." Independent claim 13 in issue states in part "scanning the mail message for encoded portions" while claim 14, dependent on claim 11, states in part "scanning the temporary file for viruses; and testing whether the scanning step found a virus." Claim 15, also dependent on claim 11, states "wherein step of scanning is performed using a signature scanning process."

Respondent argued that scanning means "examining." (See Appendix A of RBr.) The staff argued that scanning means "examining in a sequential fashion." (SBr at 29.) Complainant argued that the '600 patent does not specifically mention the term "sequential" and that the claimed term "scanning" should be provided its "ordinary meaning." (CBr at 24.)

Webster's Seventh New Collegiate Dictionary at 768 (1961) defines each of scan, scanned and scanning as "to examine intensively." Hence, the administrative law judge finds that a person of ordinary skill in the art would understand the claimed term "scanning" to mean to examine intensively.

G. The Claimed Term "Proxy Server"

Independent system claim 1 in issue contains the limitation "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred." (JX-1, col. 12, lns. 18-24 (emphasis added).) In addition, claim 2 (not in issue) and claim 3 in issue of the '600 patent, which depend from claim 1, further limit the proxy server of the system claimed in claim 1 "wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files..." and "wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages...," respectively. (JX-1, col. 12, lns. 33-34, 38-39 (emphasis added).) Independent method claims 4 and 11 in issue do not recite "proxy server." However, independent method claim 13 in issue does recite "SMTP proxy server." The parties have proposed the following constructions for the claimed term "proxy server":

Trend Micro's Construction of "Proxy Server"	Staff's Construction of "Proxy Server"	Fortinet's Construction of "Proxy Server"
An intermediary server that processes and forwards data requests and replies using Internet protocols between clients in an internal network and external servers whether originating from the clients or the external servers.	A network gateway, or an application (*i.e.*, a software program) running on a network gateway, that relays packets of data at the application layer between a trusted client and an untrusted host.	An intermediary software process that acts as both a server and a client: the proxy server is a server to the client connecting to it, and a client to the server that it connects to.

(CBr at 18; RBr at 32; SBr at 22.)

It is a fact that neither the claims of the '600 patent nor its specification define the disputed term "proxy server." Also, the '600 patent file wrapper does not define "proxy server." (See JX-2.) The '600 patent specification contains only two instances of the term "proxy server," by itself, under the heading SUMMARY OF THE INVENTION.

> The present invention also comprises a method for processing a file before transmission from the network. The preferred method for processing a file comprises the steps of: receiving the data transfer command and file name; transferring the file to the proxy server; performing virus detection on the file; determining whether the file contains any viruses; transferring the file from the proxy server to a recipient node if the file does not contain a virus; and performing a preset action with the file if it does contain a virus.

(JX-1, col. 3, lns. 4-16 (emphasis added).) However, the terms "FTP proxy server"[13] and "SMTP proxy server"[14] appear throughout the '600 patent specification. (See, e.g., JX-1, col. 4, ln. 65; col. 5, lns. 22-23; col. 5, ln. 29; see also JX-1, Abstract (reciting "FTP proxy server" and "SMTP proxy server").)

Considering the plain language of claim 1 in which "proxy" modifies "server", the claimed proxy server is at least a server and the administrative law judge, supra, has found that a person of ordinary skill in the art would understand "server" as "a computer and/or software that performs services for other computers or programs." In addition to the claimed proxy server being a server, the administrative law judge finds that the plain language of claim 1 indicates to a person of ordinary skill in the art that the proxy server is also a server which (a) receives data to be transferred, (b) scans the data to be transferred for viruses (c) controls transmission of said

[13] FTP proxy server refers to a File Transfer Protocol proxy server. (JX-1, col. 2, lns. 49-50.)

[14] SMTP proxy server refers to a Simple Mail Transfer Protocol proxy server. (JX-1, col. 2, lns. 50-51.)

data according to present handing instructions and the presence of viruses and (d) has a data input, a data output and a control input with the data input coupled to receive the data to be transferred.

Complainant argued that "[n]othing requires that the [proxy] server be limited to software," while respondent argued that the claimed proxy server should be limited to a software process(es), excluding "a separate intermediary computer as Trend Micro contends." (CBr at 19; RBr at 36; see RPFF 835.) The staff argued that the term proxy server is properly construed to include hardware and software components. (SBr at 22; SRBr at 19.)

Respondent relied on, inter alia, passages within the '600 patent specification to support its argument that the claimed proxy server should be limited to software alone. (See RBr at 36.) The first passage, under the heading SUMMARY OF THE INVENTION, states:

> The memory further comprises an operating system including a kernel, a File Transfer Protocol (FTP) proxy server, and a Simple Mail Transfer Protocol (SMTP) proxy server.

(JX-1, col. 2, lns. 48-51.) The administrative law judge finds no indication in the aforementioned portion of the '600 patent specification that would limit the claimed proxy server to software only. As for the other portions of the '600 patent specification respondent relied on to support its position, the administrative law judge finds that said portions refer to descriptions of the preferred embodiments of the memory 44 and SMTP proxy server 62. (See JX-1, col. 4, ln. 56 to col. 5, ln. 8; col. 9, lns. 32-36.) Moreover, the '600 patent specification discloses an embodiment where the FTP proxy server determines if a file contains viruses by invoking a separate virus-checking program. (See JX-1, col. 7, lns. 57-61.) Absent any indication in the claims, the specification or the file history of the '600 patent to limit the claimed proxy server to a preferred embodiment, viz. software, the administrative law judge rejects respondent's argument that the claimed proxy server consists solely of software. Moreover, in a preceding section of this Initial Determination, the administrative law judge found that a person or ordinary skill in the art would have understood that a server could include both hardware and software and would not necessarily be limited to hardware or software alone. See Section VII.B., supra. A "proxy server," as the plain language indicates, is a server.

The parties agree that the definition of proxy server refers to an intermediary component. (CBr at 19, RBr at 32, 39, SBr at 21-22.) However, they disagree as to the specific location of the claimed proxy server. Referring to FIG. 7 of the '600 patent, complainant argued that the proxy server "resides between clients in an internal network." (CBr at 19.) Respondent acknowledged that the proxy server could be located between an internal network and external servers or that "there could be a proxy server within a given network." (RBr at 39 (emphasis in original).) The staff argued that the proxy server must "sit on the gateway to the first network" because of the claimed proxy server's "ability to communicate between a first network and a second network for all computers on the first network." (SBr at 22.)

With respect to the location of the FTP and SMTP proxy servers, the '600 patent specification discloses that:

> While the apparatus of the present invention, in particular the FTP proxy server 60 and SMTP proxy server 62, has been described above as being located and preferably is located on the gateway node 33, those skilled in the art will realize that the apparatus of the present invention could also be included on a FTP server or a world wide web server for scanning files and messages as they are downloaded from the web. Furthermore, in an alternate embodiment, the apparatus of the present invention may be included in each node of a network for performing virus detection on all messages received or transmitted from that node.

(JX-1, col. 5, lns. 28-38 (emphasis added).) In describing a preferred method of operation and an embodiment for the FTP proxy server 60, the '600 patent specification teaches that said "method can best be understood with reference to FIGS. 5A and 5B, that graphically show the functions performed by ... the FTP proxy server 60 ... which resides on the gateway node 33." (JX-1, col. 6, lns. 32-36; see FIGS. 5A and B.) As for the SMTP proxy server 62, the '600 patent discloses that "[t]he SMTP proxy server 62 is preferably a program that resides on the gateway node 33...." (JX-1, col. 9, lns. 32-34.) (emphasis added). Based on the foregoing, the administrative law judge finds that the claimed proxy server does reside at a location intermediate the trusted client and untrusted host, but is not limited exclusively to the location of the preferred embodiment, viz. at the novel gateway node 33.

With respect to the claimed phrase "the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred," respondent argued that the claimed proxy server covers transfers between computer networks, (i.e., inter-network transfers) and transfers within computer networks (i.e., intra-network transfers), relying on, inter alia, the following passage from the '600 patent specification:

> [I]n an alternate embodiment, the apparatus of the present invention may be included in each node of a network for performing virus detection on all messages received or transmitted from that node.

(JX-1, col. 5, lns. 35-38; see RBr at 39.) Complainant argued that the claimed proxy server acts only on inter-network traffic, exclusive of intra-network transfers; and that respondent's attempt to cover the "alternate embodiment" improperly broadens the scope of claim 1 to read on all embodiments disclosed in the specification. (CBr at 20-21.) The staff argued that the proxy server limitation of claim 1 implicitly covers inter-network transfers only; that every embodiment in the specification need not read on every claim in the patent as respondent has attempted with its proposed construction of proxy server; and that the portion of the '600 patent specification respondent cited "could very well refer to an embodiment covering the original claim 1 (which would have covered intranet transfers and perhaps even transfers without intermediary hardware, but which was later abandoned)." (SBr at 22-23.)

Claim 1 in issue says nothing about the claimed proxy server covering internetwork and/or intranetwork transfers. Also "proxy server" within the context of claims 3 and 13 has no express requirements relating to internetwork and/or intranetwork transfers. Referring to the specification of the '600 patent, the patentees in the SUMMARY OF THE INVENTION section of the patent disclose that:

> [T]he gateway node of the present invention is particularly advantageous because the impact of using the FTP proxy server and SMTP proxy server for the detection of viruses is minimized because only the files leaving or entering the network are evaluated for the presence of viruses and all other 'intra' network traffic is unaffected.

(JX-1, col. 2, ln. 64 to col. 3, ln. 3.) However, the lead-in sentences of the SUMMARY OF THE INVENTION section read:

> [T]he present invention overcomes the limitations and shortcoming of the prior art with an apparatus and method for detecting and eliminating viruses <u>on a computer network</u>. A system including the present invention is a network formed of a plurality of nodes and a gateway node for connection to other networks.

(JX-1, col. 2, lns. 42-44.) In addition, the '600 patent expressly discloses an embodiment in which "the apparatus of the present invention may be included in each node of a network for performing virus detection on all messages received or transmitted from the node." (RPFF 765 (undisputed).)

Referring to the prosecution history of the '600 patent and original claim 1 that was filed on September 26, 1995 and is reproduced in Section VII.A., supra, as seen in the language of original claim 1, said claim did not include a proxy server or a daemon, although those elements were included in original claim 2 which was dependent on original claim 1. (JX-2 at FHC 000600-601.) Significantly, while original claim 1 was rejected by the Examiner in his office action of August 27, 1996 on prior art, as set forth in said Section VII. A, original dependent claim 2 was indicated in said office action to involve "allowable subject matter." Moreover, while it was stated that dependent claim 2 was objected to as being dependent upon a rejected base claim (original claim 1), the Examiner stated that claim 2 "would be allowable if rewritten in independent form including all of the limitations of the base claim [original rejected claim 1]." (JX-2 at FHC 000634.) The recited "proxy server" in original dependent claim 2 said nothing about the claimed proxy server covering only internetwork transfers and excluding intranetwork transfers. (JX-2 at FHC 000600-601.) Significantly, applicants in the amendment dated September 24, 1996 did amend original claim 1 by including in original claim 1 the language of original claim 2. (JX-2 at FHC 000709-710.) Thus, claim 1, as amended, included all the language of original claim 1 in addition to the proxy server and daemon limitations of dependent claim 2. Thereafter, amended claim 1, was allowed and became claim 1 in issue without said claim saying anything about whether the claimed proxy server should cover internetwork and/or intranetwork transfers. (JX-2 at FHC 000719.) Consistent with the "proxy server" limitation covering both internetwork and intranetwork transfers, applicants in the "Petition To Make Special" filed July 2, 1996 stated that applicants' invention "can prevent the virus from ever penetrating a network (or permeating, <u>where an intranetwork transfer its routed through the</u>

server, or leaving, where the destination is outside the network." (JX-2 at FHC000697 (emphasis added).)

Based on the language of claim 1, the specification of the '600 patent and the prosecution history of said patent, consistent with the administrative law judge's interpretation of the claimed term "communications unit," the administrative law judge finds that a person a ordinary skill in the art would not limit the proxy server recitation to internetwork transfers, but rather would interpret the claimed proxy server to cover both internetwork and intranetwork transfers.

Complainant argued that the proper construction of proxy server necessarily includes the use of Internet protocols; that said construction is not redundant in light of the other claims of the '600 patent that include limitations directed to specific Internet protocols, for example, "claim 3 only limits the internet protocol to the specific SMTP protocol"; that the use of Internet protocols is a requirement for the proxy server limitation because the Internet protocols used by the proxy server "may be HTTP, FTP, SMTP, or others"; and that the construction of proxy server should not be limited exclusively to the FTP and SMTP Internet protocols. (CBr at 21-22; see CDX-172.) Respondent argued that there is no requirement that the proxy server use Internet protocols; and that "Fortinet does not dispute that the claim term is broad enough to cover Internet protocols; it just does not believe a requirement of 'using Internet protocols' can be properly read into the definition of 'proxy server.'" (RBr at 38.) As to whether the proxy server limitation includes a requirement that said proxy server use Internet protocols, the staff argued that several inter-networking protocols, aside from Internet protocols, existed at the time of the invention claimed in the '600 patent; and that the claimed proxy server in issue should not be limited to Internet protocols exclusively. (SBr at 26.)

Claim 1 of the '600 patent, which contains the proxy server limitation in issue, does not contain the express limitation "use of Internet protocols," nor does such limitation appear in any other claim of the '600 patent. The prosecution history does not provide any indication that the applicants intended to limit the claimed proxy server to the "use of Internet protocols." Complainant relies on, inter alia, portions of the '600 patent specification in support of its position that the proxy server limitation of claim 1 includes the use of Internet protocols. (See CPFF 277.) However, said disclosures relate specifically to the SMTP and FTP proxy servers without indicating whether the proxy server limitation of claim 1 is limited to the use of Internet protocols. (See JX-1, col. 2, lns. 48-64; col. 4, ln. 60 to col. 5, ln. 9; col. 5, lns. 28-35.) While complainant also cites a portion of the '600 patent specification describing FIG. 4 (i.e., JX-1, col. 5, lns. 52-60), said FIG. 4 "is a block diagram of a preferred embodiment for a protocol layer hierarchy constructed according to the present invention compared to the OSI layer model of the prior art." (JX-1, col. 3, lns. 29-32 (emphasis added).) Moreover, a person of ordinary skill in the art at the time the '600 patent application was filed would have understood not only that other inter-networking protocols existed aside from Internet protocols, but also that the claimed proxy server would not necessarily need to understand all commands of a given protocol. (See SPFF 74, 75 (undisputed); http://www.cs.colostate.edu/helpdocs/ftp.html (last visited on March 15, 2005)). Based on the foregoing, the administrative law judge finds that the proxy server limitation in issue is not limited to the use of Internet protocols.

The staff argued that the claimed proxy server "relays packets of data at the application layer." (SBr at 28 (emphasis added).) Both complainant and respondent disagreed that the "at the application layer" requirement is a limitation of the claimed proxy server. (CBr at 28; RBr at 33.)

With respect to the SMTP and FTP proxy servers' relationship to the application layer, the '600 patent discloses that:

> While the FTP proxy server layer 421 and the SMTP proxy server layer 422 have been shown in FIG. 4 as being their own layer to demonstrate the coupling effects they provide between the file transfer layer 423 and the file transfer protocol 417, and the electronic mail layer 424 and the SMTP protocol layer 418, <u>those skilled in the art will realize that the FTP proxy server layer 421 and the SMTP proxy server layer 422 can also be correctly viewed as being part of the file transfer protocol layer 417 and the SMTP protocol layer 418, respectively, because they are invisible or transparent to the application layer 406</u>.

(JX-1, col. 6, lns. 17-27 (emphasis added).) Accordingly, the administrative law judge finds that the claimed proxy server is not limited to relaying data requests and replies between a trusted client and an untrusted host at the application layer.

Based on the foregoing, the administrative law judge finds that a person of ordinary skill in the art at the time the application for the '600 patent was filed would conclude that the claimed "proxy server" means a computer and/or software program that performs services for other computers or programs which proxy server (a) receives data to be transferred, (b) scans the data to be transferred for viruses which would include worms, (c) controls transmission of said data according to preset handing instructions and the presence of said viruses, (d) has a data input, a data output and a control input with the data input coupled to receive the data to be transferred and with the location of the proxy server residing intermediate the trusted client and untrusted host. The person would also conclude that the claimed "proxy" server may be, but is not limited to, a novel gateway node location or to relaying data requests and replies at the application layer. Said person would also interpret SMTP proxy server as a proxy server that uses the simple mail transfer protocol in the underlying mail message transfer.

As seen from the foregoing, the administrative law judge has found that the proper interpretation of the claimed term"proxy server" requires, inter alia, that the proxy server relay data requests and replies between a trusted client and an untrusted host and that the proxy server resides intermediate the trusted client and untrusted host. On questions from the administrative law judge on March 29, as to independent method claim 4 in issue, which does not recite "proxy server," but recites "server," complainant argued that one of ordinary skill in the art does not need to read the "server" of claim 4 as a proxy server and that the "only thing that would be required by the claim is that it's a server in addition to the - - these two other that's standing between the two computers that are transmitting data"; and that under claim 4 one certainly needs to have at least "three different things." (Tr. at 2610-11, 2613.) Respondent argued that claim 4 does not require "any type of an intermediate computer or piece of hardware." (Tr. at 2611.) The staff's position is that a person of ordinary skill in the art would interpret each of independent method claims 4 and 11 to cover both internetwork and intranetwork transfers. (Tr. at 2621.) Complainant's position is that claim 11, in addition to claim 4, should be restricted to internetwork transfers. (Tr. at 2612.) Respondent's position is that claim 11, as well as claim 4, should not be limited to internetwork transfers only, but rather, the claims embrace intranetwork transfers too. (Tr. at 2622)

Complainant, in support of its position that independent method claims 4 and 11 should contain an internetwork limitation and relying on Omega Engineering, Inc. v. Raytek Corp., 334 F.3d 1314 (Fed. Cir. 2003), argued that prosecution history disclaimer "limits the literal scope of the claims to avoid that which is disclaimed, which was the intranetwork." (Tr. at 2625-26.) However, as the Court said in Omega, while prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on definitive statements made during prosecution, the Court has "declined to apply the doctrine of prosecution disclaimer where the alleged disavowal of claim scope is ambiguous." Omega, 334 F.3d at 1324.

Referring to the prosecution history of the '600 patent, the five steps constituting original claim 5 of the '600 patent application are the same as the first five steps of issued claim 4 of the '600 patent. Also, as indicated supra, applicants in the Petition To Make Special filed on July 2, 1996 represented that applicants' invention can prevent the virus from ever "permeating, where an intranetwork transfer is routed through the server...." (JX-2 at FHC000697.) Thereafter, the Patent Office, in an office action dated August 27, 1996, rejected original claim 5 based on a Hile patent in light of a Lerche patent (JX-2 at FHC000638-39).[15] However, said claim 5 was later amended to issued claim 4, in an amendment dated September 24, 1996, by adding the limitation of "determining whether the data is of a type that is likely to contain a virus; and transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus." (JX-2 at FHC 000602, FHC 000710.) Significantly, the amendment was thus made not to clarify anything about the server, but rather to add the last two elements of issued claim 4. Hence, the administrative law judge finds that a person of ordinary skill in the art would interpret claims 4 and 11 as covering both internetwork and intranetwork transfers, in addition to

[15] Hile U. S. Patent No. 5,319,776 involved two computers connected by a communication link, and scanning on the receiving computer after the data is received over the modem link in a buffer on the receiving computer. (RX-158; Mitchell, Tr. at 1020). Said patent does not disclose an intermediary computer between a first computer and a second computer for scanning data for viruses and also does not disclose a gateway. Instead it discloses a simple transfer between two computers as a modem link between the two computers. (Mitchell, Tr. at 1021.)

contemplating that the claimed methods of claim 4 and 11 use three distinct computers or hardware devices, viz. a first computer, a server and a second computer, wherein the data is transferred from a first computer to a second computer via a server.

VIII. Domestic Industry

Complainant argued that it satisfies the domestic industry requirement. (CBr at 61-68.) Respondent argued that complainant failed to show that the technical prong is satisfied because it has not established that any Trend Micro product practiced a claim of the '600 patent in May 2004, when its complaint in this investigation was filed. (RBr at 138.)

The staff argued that the evidence shows that the three Trend Micro products relied upon to establish the domestic industry requirement, viz. the IWSS, the ISVW[16], and the IMSS, practice certain claims of the '600 patent when used in conjunction with the required hardware; that specifically, IMSS and ISVW practice claims 1, 3, 4, 7, 8 and 11-15 and IWSS practices claims 1, 4, 7 and 8; that those three software products require the appropriate hardware to practice the claims (IWSS, ISVW and IMSS systems in combination) and are intended to be used in conjunction with hardware; and that Trend Micro has implemented such combinations and practices those claims by performing product testing at its facilities in the United States. (SBr at 49-50.)

Complainant bears the burden of demonstrating the existence of an industry in the United States that practices the '600 patent in issue and meets the requirements of section 337(a)(3). Certain Microsphere Adhesives, Process for Making Same, and Products Containing Same,

[16] There are separate Windows NT and UNIX versions of ISVW. (Mitchell, Tr. at 582.)

Including Self-Stick Repositionable Notes, Inv. No. 337-TA-366, USITC Pub 2949, Comm'n Op. at 8 (January 1996) (Microsphere Adhesives).

In proving the existence of a domestic industry under subparts (A) and (B) of 19 U.S.C. § 1337(a)(3), a complainant must establish that its activities in the United States meet the threshold set forth in the statute (economic prong) and that those activities are devoted to a product or process which is covered by the patent(s) in issue (technical prong). In re Certain Removable Elec. Cards and Elec. Card Reader Devices and Prods. Containing Same, Inv. No. 337-TA-396, 1998 WL 479084 at *9 (Comm'n Op. Aug. 1998) (U.S.I.T.C. Pub. No. 3123). In this investigation, the Commission has found that the economic prong of the domestic industry requirement has been satisfied. (See Section I., Procedural History, supra, and its reference to Order No 13.)

Referring to the technical prong, although there must be a domestic industry with respect to the asserted patent, there is no requirement that all the claims asserted against a respondent be practiced by the domestic industry. See Microsphere Adhesives. Thus, a complainant need only show that its products meet one claim of a patent at issue. Certain Lens Fitted Film Packages, Inv. No. 337-TA-406, Final Initial Determination at 203 (Feb. 24, 1999), reviewed-in-part on other grounds (April 9, 1999); Certain Toothbrushes and Packages Thereof, Inv. No. 337-TA-391, Order 8 (July 7, 1997) (Unreviewed Initial Determination).

The administrative law judge finds that the evidence shows that the three Trend Micro products, viz. IWSS, ISVW and IMSS, practice at least claim 4 of the '600 patent when used in conjunction with hardware.[17] Thus, Trend Micro's IMSS systems[18] are a computer

[17] Trend Micro's products in issue are sold as software. A purchaser of the products then (continued...)

implementation of a method for detecting viruses in data transfers between computers as required by claim 4 of the '600 patent. (See, e.g., CX-318 at TMI00099321-22.) The IMSS systems perform the "receiving" step of claim 4 of the '600 patent. In IMSS systems, data from incoming emails are processed first by postfix and then sent via SMTP to IMSS and IMSS scans the incoming emails for viruses, which include requests containing destination addresses. (Yang, Tr. at 89, 97, 98, 99; Mitchell, Tr. at 597-603, 667-68.) In the IMSS systems, the server electronically receives data and, therefore, practices the "electronically receiving" step of claim 4 of the '600 patent. IMSS contains a virus filter to determine if the data contains a virus. (Yang, Tr. at 99-100.) The virus filter is located at the IMSS server. (CX-318 at TIM0009322; Mitchell, Tr. 668-69.) The IMSS product further satisfies the "performing" step of claim 4 of the '600 patent because the server of IMSS performs a preset action on data if it contains a virus. (Yang, Tr. at 109.) The IMSS systems contain predefined handling instructions that are used to determine actions to be taken as a result of scanning for viruses. (Yang, Tr. at 110; Mitchell, Tr. at 669-70.) In IMSS, predefined handling instructions are used to determine actions to be taken as a result of scanning for viruses. (Yang, Tr. at 101.) This includes sending the data to the destination address if it does not contain a virus. (Id.; Mitchell, Tr. at 671.) Trend Micro's IMSS determines whether the data is of a type likely to contain a virus as required by the "determining"

[17](...continued)
combines the software with its own hardware to perform the functions set forth in claim 4 of the '600 patent. See Section IV., supra.

[18] While reference here is made to Trend Micro's IMSS systems, all three of the products (IMSS, ISVW and IWSS) from an architectural standpoint are essentially the same. (Yang, Tr. at 67-68.) Thus, with regard to the functionality that is pertinent to claim 4, the system architectures are all very similar. (Mitchell, Tr. at 583.) Hence, the reference to IMSS systems in the section is found applicable to the ISVW and IWSS systems.

step of claim 4 of the '600 patent. (Yang, Tr. at 102, 103, 106, 107, 109; CX-318 at TMI000099414; see Mitchell, Tr. at 671-72.) IMSS selectively scans those files that are likely to contain a virus using IntelliScan or filename extensions. (Yang, Tr. at 107-08.) Trend Micro's IMSS satisfies the "transmitting" step because it transmits data from the server to the destination without performing the "determining" and "performing a preset action" steps if the data is not likely to contain a virus. (Mitchell, Tr. at 672.) By using IntelliScan or filename extensions, files that are not likely to contain a virus are not scanned for viruses. (See Yang, Tr. at 101-02, 107-08.)

IX. Infringement

Complainant has argued that the accused FortiGate products directly infringe the asserted claims of the '600 patent and, alternatively, infringe said claims under the doctrine of equivalents. Complainant further argued that Fortinet actively induces infringement of the '600 patent and contributes to the infringement of said patent. (CBr at 26-60.)

Respondent argued that complainant has not met its burden in establishing infringement; and that there can be no question that the accused products do not utilize the architecture claimed by the '600 patent. (RBr at 46.)

The staff argued that there has been direct infringement of the asserted claims and induced infringement, but argued that complainant has not met its burden in establishing contributory infringement. (SBr at 41-48.)

Under the provisions of 35 U.S.C. § 271, liability for infringement arises if "whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor." 35 U.S.C. § 271(a). This infringement of a patented invention is the usual meaning of the expression "direct (literal) infringement." See Joy Techs., Inc. v. Flakt, Inc., 6 F.3d 770, 773 (Fed. Cir. 1993). However, even though an alleged infringer is not making, using, selling or importing a patented invention, a party's acts in connection with selling a product may, however, constitute active inducement of infringement or contributory infringement of a patented invention under either 35 U.S.C. § 271(b) and/or 35 U.S.C. § 271(c). Liability for either active inducement of infringement (under 35 U.S.C. § 271(b)) or for contributory infringement (under 35 U.S.C. § 271(c)) is dependent upon the existence of direct infringement. See Joy Techs., Inc., 6 F.3d at 773.

A determination of infringement requires a two-step analysis. First, the patent claim must be properly construed to determine its scope and meaning. Second, the claim as properly construed must be compared to the accused device or process. Zelinski v. Brunswick Corp., 185 F.3d 1311, 1315 (Fed. Cir. 1999), citing Markman v. Westview Instruments, Inc., 52 F.3d 967, 976 (Fed. Cir. 1995). Whereas claim construction is a matter of law and, therefore, the exclusive province of the court, "whether a claim encompasses an accused device, either literally or under the doctrine of equivalents, is a question of fact." Zelinski, 185 F.3d at 1315, citing N. Am. Vaccine, Inc. v. Am. Cyanamid Co., 7 F.3d 1571, 1574 (Fed. Cir. 1993).

To prove literal infringement, the patentee must show that the accused device contains every limitation in the asserted claims. WMS Gaming Inc. v. Int'l Game Tech., 184 F.3d 1339, 1350 (Fed. Cir. 1999), citing Mas-Hamilton Group v. LaGard, Inc., 156 F.3d 1206, 1211 (Fed. Cir. 1998). An accused device that does not literally infringe a claim may nonetheless infringe under the doctrine of equivalents if differences between the accused device and the claimed invention are "insubstantial." Desper Prods. Inc. v. QSound Labs, Inc., 157 F.3d 1325, 1338 (Fed. Cir. 1998). Equivalency of a claimed element to an element of an accused device is determined on an element-by-element basis at the time of infringement. Warner-Jenkinson Co. v. Hilton Davis Chem. Co., 520 U.S. 17, 40 (1997).

A. The Accused Products

The accused products are set forth in Section IV., supra. As Section IV. discloses, respondent has different versions of the accused products which involve multiple hardware versions with multiple versions of source code.[19] (Xie, Tr. at 1352-53.) However, the hardware functions in terms of antivirus functionality are identical. The accused products are sold as an encased combination of hardware and software and as part of the hardware, the accused products contain a chip. See Section IV., supra. Hence, one looks at the encased combination of hardware and software to determine whether there is infringement of the asserted claims.

B. Direct Infringement Of Independent Claim 1 And Dependent Claim 3

Complainant argued that the accused products directly infringe independent claim 1 and claim 3 which is dependent on claim 1. While respondent denies infringement, the staff argued that complainant has established direct infringement of claims 1 and 3.

1. Preamble, Memory, Communications Unit And Processing Unit Claimed Elements

The preamble of claim 1 calls for a system for detecting and selectively removing viruses in data transfers. The accused FortiGate products scan for viruses at the gateway. (CX-186C

[19] The current version of FortiOS is version 2.8 and there are multiple releases of version 2.8. The version of respondent's source code just prior to version 2.8 was version 2.5 which is still commercially available in parallel to version 2.8. (Xie, Tr. at 1352-53.)

(Fortinet White Paper entitled "Why less is more in Antivirus Protection by Joe Wells) at 8; CX-287 (Virus Scanning Firewall Technology, Fortinet Approach) at 3; CX-443 (Fortinet Real Time Content Security) at FHC 004651; CX-544C (Fortinet Content Processing Network Protection Technology) at 5; CX-547C (White Paper: University Network Security Challenges; How Fortinet Closes the Security Gap and Delivers Lower Total Cost of Ownership) at 10-11; CX-550C at 10, 13; CX-569C (FortiGate 1000-Real Time Content Security for Large Enterprises) at 1; CX-573C (FortiGate 2000 - the Next Generation Gigabit Content Processing Architecture) at 4.) Hence, the administrative law judge finds that complainant has met its burden in establishing the preamble element of claim 1 in the accused products.[20]

Claim 1 recites a memory. The administrative law judge finds that complainant has established that the accused FortiGate products satisfy the claimed memory recitation of claim 1. (See Lacy, Tr. at 1807.) In the FortiGate product, the memory is indirectly connected to the CPU via a bus. (Crawford, Tr. at 187.) When the client computer has some sort of data it wishes to send, it will begin writing that data down to its kernel and that kernel will break that data into packets. Each of these packets contains headers. There will be an Ethernet header, there will be an IP header, a TCP header, and if it is a high level protocol, there will be the high level protocol header. Each of those packets is sent to the next device, in this case, the FortiGate device. (Crawford, Tr. at 185-186.) {

[20] Respondent, in its post-hearing brief and reply brief, did not argue that the accused products do not meet the preamble element or the "communications unit," "memory" and "processing unit" elements of claim 1. It did argue that the accused products do not contain a proxy server or daemon of the type claimed and that the accused products do not selectively transfer data depending on the existence of a virus. (See RBr at 47-56; RRBr at 42-55.)

}

(Crawford, Tr. at 187.){

} (JX-007C at 207.) A memory needs to have inputs and outputs in order for it to work. (Mitchell, Tr. at 963.)

Claim 1 recites a communications unit. The administrative law judge has found that a person of ordinary skill in the art would interpret the claimed recitation of "communications unit" to include respondent's proposed construction for the term. See Section VII.A., supra. Respondent has admitted that the accused products contain a "communications unit" as construed by respondent. (See RRCPFF 414-17.) Thus, the administrative law judge finds that complainant has established that the accused FortiGate products satisfy the claimed communications unit recitation of claim 1.

Claim 1 recites a processing unit.[21] The administrative law judge finds that complainant has established that there is a processing unit, according to claim 1, in each accused FortiGate product which receives signals from the memory and the communications unit. Thus the processing unit, which has inputs and outputs, memory and the communications unit are

[21] A processor, in ordinary computer architecture, carries out the computing steps. Those computing steps generally involve instructions to be executed and data to operate on. In the standard architecture, the processing unit draws instructions and data out of memory. If the FortiGate product utilizing the standard computer architecture is going to communicate through a communications unit to an external network, then there has been some form of connection between the processing unit and the communications unit as well. (Mitchell, Tr. at 966.) Moreover, a processing unit needs to have some form of input and output in order to work. (Mitchell, Tr. at 965.)

connected up on a bus and they interact so that software can execute on the processing unit to access memory and communicate over the network. Instructions can be loaded onto this unit. The processing unit can read and write data, which means it is connected to memory so that it can read and write from memory through a bus and standard architectural support. (Mitchell, Tr. at 729-730; CDX-4.) In addition the figure from a Fortinet Whitepaper referenced in CDX-5 shows that certain components of the accused FortiGate products are connected by a system bus within the operating system including general purpose computer central processing unit(s). (See CX-213.) At the bottom of said figure, which Mitchell referred to as "standard computer architecture," there are physical network interfaces and the two-headed arrows at the bottom of said figure indicate the network connections with "the things above the bus being portions of the system at an architectural high-level processing unit, an operating system, memory, and so on." (Mitchell, Tr. at 730-731; CDX-5; see CX-213.) The system bus connects the CPU and the memory. (JX-007C at 113.)

The administrative law judge finds that each accused FortiGate product{

} (Mitchell, Tr. at 737.) In the FortiGate accused products, the CPU writes to and reads from particular areas of memory. (Crawford, Tr. at 187; Lacy, Tr. at 1807). The CPU contained within the accused FortiGate products is able to communicate with memory contained in said product. (Lacy, Tr. at 1808; see JX-007C at 114.) Said CPU reads and writes from RAM contained within said products. (Lacy, Tr. at 1813.) The CPU is indirectly connected to the Ethernet interface. (JX-007C at 113.) The CPU and Ethernet interface can communicate with one another. (JX-007C at 113.) {

} (Crawford, Tr. at 183; JX-007C at 110.) FortiOS, an umbrella term, can be considered all of the software that runs on the accused FortiGate products. (Gray, Tr. at 266, 267.)

2. The Proxy Server Claimed Element

Claim 1 recites "a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to present handing instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred." (JX-1.) The administrative law judge has found that the proper interpretation of the claimed term "proxy server" means a computer and/or software program that performs services for other computers or programs which proxy server (a) receives data to be transferred, (b) scans the data to be transferred for viruses which would include worms, (c) controls transmission of said data according to preset handing instructions and the presence of said viruses, (d) has a data input, a data output and a control input with the data input coupled to receive the data to be transferred and with the location of the proxy server residing intermediate the trusted client and untrusted host. He further has found that the claimed "proxy" server may be, but is not limited to a novel gateway node location or to relaying data requests and replies at the application layer. The administrative law judge finds that the accused products literally satisfy the "proxy server" element as he has construed the term.

Thus, the proxy server of the accused products resides intermediate the trusted client and untrusted host. In addition, the proxy server in the accused products is between the client and server and observes all client to server connections. {

}(CX-205C (FortiGate Proxy Splice Feature Technical Feature Notes) at 2.) Physically the FortiGate product is between client and the server. The data that the client is sending to the server is physically going through the cable which enters the FortiGate product and then goes out another cable coming out of the FortiGate product and observes the data between those two proxies. (Gray, Tr. at 286.) The proxy server in the accused products involves FortiOS which is a collection of software modules. (JX-007C at 89.) Thus, it is an intermediary software process and everything that the client sends to the server including connection requests goes through the FortiGate accused products. (Gray, Tr. at 285; CX-205.)

The administrative law judge finds that the FortiGate accused encased combinations of hardware and software are devices that are used at a network gateway. (Crawford, Tr. at 156-57.)

{

} (Crawford, Tr. at 210.)

Fortient argued that the accused combinations of hardware and software do not have a proxy server that scans for viruses because{

}(RBr at 51–53.) However, the administrative law judge has found that the proper interpretation of "proxy server" may include hardware and software components and hence he finds that the claimed term "proxy server" is broad enough to cover several components within the casing of the accused combinations of hardware and software. The administrative law judge finds no requirement in the '600 patent that the claimed proxy server be implemented as a single process. Moreover, the "intelligent bridge"[22] and virus scanning engine in the accused combinations of hardware and software are{

}

Respondent argued that unlike a proxy server, Fortinet's accused products{

} (RRBr at 45-46.) However, the administrative law judge's construction of proxy server does not require that a claimed proxy server be capable of

{ }

[22] Respondent has admitted that its expert Lacy in connection with this investigation was first to apply the term "intelligent bridge" to the accused products. (RBr at 49, n.20.) The first date when Fortient used the term "intelligent bridge" was on or around October 4, 2004. (CPFF 569 (undisputed).) The first time Fortinet's Andrew Gray used the term "intelligent bridge" was around September or October of 2004. (CPFF 571 (undisputed).) Andrew Gray first heard the term "intelligent bridge" from Fortinet's counsel, Sara Piepmeier. (CPFF 572 (undisputed).)

Respondent also argued that, unlike a proxy server, the accused products cannot be an end point in a communication session. (RRBr at 46.) The administrative law judge finds such argument irrelevant since a proper construction of the claimed proxy server does not require it to be an end point in the communication in and of itself.

3. The Daemon Claimed Element

Claim 1 requires "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." (JX-1, col. 12, lns. 25-32.) Claim 3 requires a "daemon" with specific functionality involving the transfer of data to its destination and configured in a particular manner.

The administrative law judge has found that the claimed term daemon means transferring data from a proxy server in response to control signals from the proxy server with the daemon having a control input, a data input and a data output and with said control input coupled to the control output of the proxy server for receiving control signals and with said data input coupled to the data output of the proxy server for receiving the data to be transferred and that the daemon involves a program that runs without user (i.e., human) intervention, which program is part of the operating system and runs in the background. The administrative law judge finds that the accused products literally satisfy the claimed "daemon" element as the administrative law judge has construed the term.

Respondent argued that the accused products do not contain a daemon that satisfies claim 1 because the accused products do not have a daemon for transferring data from the proxy server since the Fortinet Products do not have a proxy server. (RRBr at 51-52.) However, the administrative law judge has found that the accused products do have the claimed proxy server. Moreover, complainant's expert Mitchell found{

} (Mitchell, Tr. at 772-74.[23])

Dependent claim 3 recites "[t]he system of claim 1, wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node." The administrative law judge finds that the accused products have an SMTP proxy server and SMTP daemon. (Mitchell, Tr. at 789-90.)

[23] The administrative law judge finds that the fact that the source code files of respondent that{

} (Mitchell, Tr. at 772-73.)

Based on the foregoing, the administrative law judge finds that complainant has met its burden in establishing that claims 1 and 3 of the '600 patent are directly (literally) infringed, assuming said claims are not invalid.

C. Direct Infringement Of Independent Claim 4 And Dependent Claims 7 And 8

Complainant argued that the accused products literally satisfy each element of claim 4. (CBr at 38-45.) It is further argued that the accused products literally infringe claims 7 and 8, each of which is dependent on claim 4. (CBr at 43-45.)

Respondent argued that complainant has provided no evidence that Fortinet's version 2.8 products infringe claim 4 of the '600 patent[24]; that said products{

} Further, because claims 7 and 8 depend from claim 4, respondent argued that Fortinet's version 2.8 products do not infringe claims 7 and 8 of the '600 patent. (RBr at 57.)

The staff argued that the accused products directly infringe claims 4, 7 and 8 of the '600 patent. (SBr at 42-44, 46.)

The administrative law judge finds that complainant has established that the accused products directly infringe the method described in independent claim 4 which pertains to

[24] Respondent has admitted that the last two steps of claim 4, which it characterized as the "likelihood analysis," are performed by the accused FortiOS 2.5 products. (RBr at 58-59.)

scanning only those files of a type likely to contain a virus. Thus, those systems: (1) electronically receive data at a server, including the intended destination address for the data (Mitchell, Tr. at 790-92; CDX-42-43); (2) determine whether the data contains a virus (Mitchell, Tr. 793-94; CDX-44); (3) perform certain preset actions if the data contains a virus (Mitchell, Tr. at 794-95; CDX-45); (4) otherwise send the data to its destination (Mitchell, Tr. at 795-96; CDX-46); (5){ }(Mitchell, Tr. at 804-06, 808-09; CDX-47); and (6) perform those steps at a server between two computers. (Mitchell, Tr. at 790; CDX-42.)

As for claims 7 and 8 he finds that complainant has established that the accused products practice the additional limitation of dependent claim 7, which requires that the "preset action" of claim 4 consist of transmitting the data unchanged, not transmitting the data, or storing the data in a file with a new name and notifying the recipient of the new name (i.e., quarantining). (Mitchell, Tr. at 810-12; CDX-52-56.) He also finds that{

} (Gray, Tr. at 1559-60; Mitchell, Tr. at 814; CDX-57.)

While Fortinet argued that filetyping in FortiOS 2.8 applies to all data equally rather than selectively, Fortinet's Jeff Crawford testified that in a FortiGate product,{

} Thus, he testified:

Q.{

}

(Crawford, Tr. at 225-26 (emphasis added).) Fortient's expert Lacy testified that{

} Thus, Lacy testified:

{

}

(Lacy, Tr. at 1818-19 (emphasis added).)

In addition, while Fortinet claims that its FortiOS 2.8 products{

}(RBr at 60-62.){

}(Gray, Tr. at 1529-31.) {

} (Gray, Tr. at 320.) {

} (Gray, Tr. at 333.) {

}

(D'Souza, Tr. at 373.){ }(D'Souza, Tr. at 373.)

{ }

(D'Souza, Tr. at 374.) {

} (Crawford, Tr. at 226-227.) {

} (Crawford, Tr. at 228-229.) Hence, the administrative law judge rejects respondent's argument that, with respect to the FortiOS 2.8 accused product, the same process is performed for all files regardless of the file type.

D. Direct Infringement Of Independent Claim 11 And Dependent Claims 12, 14 And 15

Complainant argued that the accused products directly infringe each of independent claim 11 and claims 12, 14 and 15, each of which is dependent on claim 11. (CBr at 45-50, 52-53.) Respondent argued that the accused products do not infringe claims 11, 12, 14 and 15 of the '600 patent because the accused products do not store each encoded portion of a mail message in a separate temporary file. (RBr at 67-68.) The staff argued that the accused products practice each of claims 11, 12, 14 and 15 and hence directly infringe said claims. (SBr at 44-46.)

Respondent, in support of its non-infringement argument, argued that the accused products{

} (RBr at 68 (emphasis added).) Respondent further argued that{

} (Id.)[25]

[25] The '600 patent has a September 26, 1995 filing date. The state of the art with respect to email transfers in 1995 as opposed to today has changed. Thus, the evidence shows that MIME standard was not a prevalent standard in 1995, and thus processing MIME encoded mail messages was not a strong selling point to potential customers of network security. (JX-16 (Crider Depo.) at TMI00176092.) The primary encoding method, when the application for the '600 patent was filed, was uuencoding. (Id. at TMI00176092.) With uuencoding, "portions of messages usually start with a line like 'begin 64 filename' and end with a line like 'end.'" (JX-1, col. 10, lns. 32-34.)

As the language of independent claim 11 indicates, the limitations of claim 11 involve scanning for encoded portions and storing such portions in separate temporary files. The administrative law judge has found that the proper interpretation of "temporary file" is a non-permanent collection of related records treated as a unit and would include a data record sending in RAM. <u>See</u> Section VII.E., <u>supra</u>. The accused products{

}(Mitchell, Tr. at 817.){

}(<u>Id.</u>){

}(<u>Id.</u>; D'Souza, Tr. at 382; CX-209.){

}(<u>Id.</u>){

} Hence, the accused products are found to meet the limitation that each encoded portion be stored in a separate temporary file.

As seen from the foregoing, as for independent claim 11, the administrative law judge finds the accused products, in addition to meeting the limitations that are very similar to those of claim 4 (preset action, destination address, server, <u>etc.</u>), also implement a method that (a)
{

} and (b){

} (Mitchell, Tr. at 814-22; CDX-58-65.)

Referring to claims 12, 14, and 15 which depend from claim 11, the administrative law judge finds that the accused products practice claim 12 inasmuch as the evidence shows that they
{ } practice claim 14 by (a){

} and (b){

} (Mitchell, Tr. at 842, 850-51, 856-58; CDX-66; CDX-77-80.)

Based on the foregoing, the administrative law judge finds that complainant has established that the accused products directly infringe independent claim 11 and dependent claims 12, 14 and 15.

E. Direct Infringement Of Independent Claim 13

Complainant argued that the accused products directly infringe each element of claim 13. (CBr at 50-52.) Respondent argued that the accused products do not infringe claim 13. (RBr at 79.) The staff argued that the accused products infringe claim 13. (SBr at 45, 46.)

Respondent's arguments are essentially the same as that set out for independent claims 1 and 4 except that the arguments are directed only to the SMTP proxy server and SMTP daemon as claim 13 recites an SMTP proxy server and SMTP daemon. Independent method claim 13 does have the requirement that the mail message is sent to the destination address, if the message contains no encoded portions, without first scanning for viruses.

Reference is made to the findings, supra, of the administrative law judge with respect to infringement of independent claims 1 and 4 and also with respect to infringement of dependent claim 3. Said findings are incorporated by reference here. Moreover, the administrative law judge finds that complainant has established the requirement of independent method claim 13 that{

} (Mitchell, Tr. at 846-47; CDX-75.) Hence, he finds that complainant has established that the accused products directly infringe independent claim 13.

F. Active Inducement Of Infringement

Complainant argued that Fortinet actively induced the infringement of the '600 patent. (CBr at 57.) Respondent argued that it does not induce infringement of the '600 patent. (RRBr at 85.) The staff argued that there is active inducement of infringement by respondent. (SBr at 46-47.)

To succeed in establishing active inducement of infringement, complainant must establish "(1) an act of direct infringement of the patent; (2) the accused infringer actively induced a third party to infringe the patent; and (3) the accused infringer knew or should have known that his actions would induce infringement." Certain Flash Memory Circuits and Products Containing Same, Inv. No. 337-TA-382, U.S.I.T.C. Pub. 3046, Comm'n Op. on Remedy, the Public Interest, and Bonding at 16 (July 1997) (Flash Memory). The administrative law judge has found that the use of the accused products directly infringes each of the asserted claims of the '600 patent.

{

} (CX-300C; CX-303C; CX-304C.) Carpenter, the director of channels at Fortinet, testified during deposition that a Fortinet user manual would provide an end user instructions on how to set up Fortinet's products, how to configure the product, and how to perform some troubleshooting. (JX-008C at 88-89; see FF 51.) Fortinet also provides training and support to certain resellers and end users. (CX-357C at ¶¶ 10, 11, 22, 23.)

Fortinet has identified three levels of support. (JX-008C at 52-54.) {

}[26] (JX-008C at 52.) Fortinet also provides support services to end users which services include certifications with respect to a basic understanding of how Fortinet's products operate, associated with the "Fortinet Certified Service Engineer" certification, as well as certification in VPN specialization and FortiManager specialization. (JX-008C at 58.)

Based on the foregoing, the administrative law judge finds that complainant has established that Fortinet induces users of Fortinet's accused products to use the antivirus functionality of its products and Fortinet knew or should have known that the accused products would be used in that manner. Hence, the administrative law judge finds that complainant has established active inducement of infringement.

G. Contributory Infringement

Complainant argued that Fortinet contributes to the infringement of the '600 patent. (CBr at 58.) Respondent denies any contributory infringement. (RRBr at 83.) The staff argued that complainant has not met its burden of proving contributory infringement. (SBr at 48.)

To prove contributory infringement, a complainant must establish that "(1) there has been an act of direct infringement by a third party; (2) the accused contributory infringer knows that the combination for which its component was made was both patented and infringing; and (3) there are no substantial non-infringing uses for the component part i.e., the component is not a 'staple article' of commerce." Flash Memory, Comm'n Op. at 9-10 (emphasis added). The record in this investigation establishes that the "FortiOS" is the name that Fortinet gave to the

[26] { } (JX-008C at 55.)

collection of software modules that run on the hardware of the accused products (Crawford, Tr. at 182; Gray, Tr. at 271; Xie, Tr. at 1374-75);{ } (Xie, Tr. at 1375; Gray, Tr. at 1548);{ }(Crawford, Tr. at 210; Xie, Tr. at 1375);{ } (Xie, Tr. at 1375; Gray, Tr. at 1548);{ }antivirus functionality provide all of the other functionalities of the FortiGate products, including firewall, virtual private networking (VPN), content filtering, URL blocking, intrusion detection, and traffic shaping. (Xie, Tr. at 1375.)

The administrative law judge further finds that the record in this investigation establishes that the accused products are multi-function devices that include many other functions in addition to virus scanning on a single stand-alone piece of hardware (JX-009c (Richard Kagan Depo.) at 104); Xie, Tr. at 1348, 1378; Crawford, Tr. at 157; RX-187 (FortiGate 50A/100: Real Time Network Protection for SOHO/Branch Office)); that Fortinet's co-founder and Chief Technical Officer testified that the FortiGate series of products have the basic functionality of network firewall, VPN, and also have the functionality of traffic shaping and intrusion protection, as well as the application level security modules, including anti-virus, web content filtering, and e-mail filtering, all in one box (Xie, Tr. at 1348, 1371); that the accused products are not "primarily" designed to provide anti-virus functionality (Xie, Tr. at 1371);{

}(Xie, Tr. at 1376);{

} (Xie, Tr. at 1374); and that Fortinet's business model focuses on integrating many security functionalities into a single product. (Xie, Tr. at 1347.)

Based on the record, supra, the administrative law judge finds that the accused products have substantial non-infringing uses. Thus he finds that complainant, who has the burden, has not established that there are no substantial non-infringing uses for the accused products. Hence, he finds that complainant has not established contributory infringement.

X. Validity

A. 35 U.S.C. Section 102

35 U.S.C. § 102 provides that a person is entitled to a patent unless, inter alia:

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent, or
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in the public use or on sale in this country, more than one year prior to the date of the application for patent in the United States, or
>
> * * *
>
> (g)(2) before such person's invention thereof, the invention was made in this country by another inventor who had not abandoned, suppressed, or concealed it. In determining priority of invention under this subsection, there shall be considered not only the respective dates of conception and reduction to practice of the invention, but also the reasonable diligence of one who was first to conceive and last to reduce to practice, from a time prior to conception by the other.

Patent claims are entitled to a strong presumption of validity and each claim of a patent is presumed valid independently from the validity of other claims. 35 U.S.C. § 282; see Robotic

Vision Sys., Inc. v. View Eng'g, Inc., 189 F.3d 1370, 1377 (Fed. Cir. 1999); Continental Can Co. v. Monsanto Co., 948 F.2d 1264,1266-67 (Fed. Cir. 1991).

As issued patents are afforded a strong presumption of validity, a respondent seeking to invalidate a patent with anticipatory prior art per section 102(a) or 102 (g) must do so by clear and convincing evidence. See, e.g., Innovative Scuba Concepts, Inc. v. Feder Indus., Inc., 26 F.3d 1112, 1115 (Fed. Cir. 1994). Moreover,

> [w]hile a patentee may have the burden of going forward with rebuttal evidence once a challenger has presented a prima facie case of invalidity, the presumption of validity remains intact and the ultimate burden of proving invalidity remains with the challenger throughout the litigation. The role of the trial court is to determine whether the challenger has carried its burden, and it requires full consideration of all relevant evidence, including that presented in rebuttal.

Id. (citations omitted); see Hybritech Inc. v. Monoclonal Antibodies, Inc., 802 F.2d 1367, 1375 (Fed. Cir. 1986). For example, if a respondent established that a section 102(a) prior art reference was known before the filing date and that the reference disclosed each and every limitation of the claimed invention, the patentee would have the opportunity to present rebuttal evidence that the inventor invented the subject matter of the invention before the reference pursuant to the priority of invention rules in section 102(g)(2). See Markurkar v. C.R. Bard, Inc., 79 F3d 1572, 1576-77 (Fed. Cir. 1996).

To prove anticipation under section 102(a), a respondent must establish that the prior art involved each and every limitation of the claim in issue. Glaxo Inc. v. Novopharm Ltd., 52 F.3d 1043, 1047 (Fed. Cir. 1995). With respect to inherent disclosures of a prior art reference, the Federal Circuit has commented:

> [t]o serve as an anticipation when the reference is silent about the asserted inherent characteristic, such gap in the reference may be filled with recourse to extrinsic evidence. Such evidence must make clear that the missing descriptive

> matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.
>
> * * *
>
> This modest flexibility in the rule that 'anticipation' requires that every element of the claims appear in a single prior art reference accommodates situations where the common knowledge of technologists is not recorded in the reference; that is where technological facts are known to those in the field of the invention, albeit not known to judges.

Continental Can, 948 F.2d at 1268-69 (citations omitted).

Section 102(g)(2) of the patent statute defines the "prior invention" category of prior art. A prior art device can anticipate a claimed invention "if it was conceived and reduced to practice prior to the filing date of the patent." Sandt Tech., Ltd. v. Resco Metal and Plastics Corp., 264 F.3d 1344, 1350 (Fed. Cir. 2001). As with section 102(a) prior art references, the prior invention must include "all elements of a claimed invention arranged as in that [asserted] claim." Id.

With respect to witness testimony of a prior use under 35 U.S.C. § 102(a), or a prior invention under 35 U.S.C. § 102(g), courts require that such testimony is corroborated by other evidence, such as physical or documentary exhibits. See, e.g., Juicy Whip v. Orange Bang, Inc., 292 F.3d 728, 743 (Fed. Cir. 2002) (concluding testimony of six "inter-connected" witnesses corroborated by single document did not constitute clear and convincing evidence to invalidate for prior public knowledge); Finnigan Corp. v. Int'l Trade Comm'n, 180 F.3d 1354, 1367 (Fed. Cir. 1999) (reversing invalidity determination and finding oral testimony of uninterested witness, by itself, insufficient to establish prior public use under § 102(b)); Woodland Trust v. Flowertree Nursery, 148 F.3d 1368, 1373 (Fed. Cir. 1998) (determining uncorroborated testimony of four witnesses insufficient to invalidate patent for prior public knowledge and use per 102(a)). Documentary or physical evidence that is made contemporaneously with the inventive process "provide the most reliable proof that the inventor's testimony has been corroborated." Sandt

Tech., Ltd., 264 F.3d at 1350-51, citing Woodland Trust, 148 F.3d at 1373. Aside from the corroboration requirement, the Federal Circuit has endorsed a list of factors to consider when assessing the credibility of oral testimony regarding potentially invalidating prior art. Juicy Whip, 292 F.3d at 741, citing In re Reuter, 670 F.2d 1015, 1021 n.9 (C.C.P.A. 1981). Said factors include:

> (1) delay between event and trial, (2) interest of witness, (3) contradiction or impeachment, (4) corroboration, (5) witnesses' familiarity with details of alleged prior structure, (6) improbability of prior use considering state of the art, (7) impact of the invention on the industry, and (8) relationship between witness and alleged prior user.

Juicy Whip, 292 F.3d at 741.

1. Norman Firewall

Respondent argued that the Norman Data Defense Systems' Norman Firewall product anticipates and/or renders obvious each and every asserted claim of the '600 patent. (RRBr at 94-104.) Complainant argued that the Norman Firewall product does not invalidate any of the claims in issue. The staff argued that while the Norman Firewall product invalidates claims 1 and 3 in issue, said product does not invalidate the remaining claims in issue.

Respondent, in support of its invalidity argument, argued that the Norman Firewall product is prior art to the '600 patent under "at least" 35 U.S.C. §§ 102(a) and (g).[27] (RBr at 86, at 101, 107, 115, 116, 120, 121.) Respondent argued that the Norman Firewall was first publicly

[27] Fortinet is relying on the Norman Firewall as prior art "that was known or conceived of before the invention date of the '600 patent under Sections 102(a) and 102(g)." (RRBr at 99.) "[A]s Fortinet has repeatedly pointed out, the prior art reference here is the Norman Firewall product itself, not the documents describing the reference." (RRBr at 95 (emphasis added).) Fortinet does not assert that the Norman Firewall is a 35 U.S.C. § 102(b) reference. (RRSBr at 8.)

demonstrated and offered for sale at a Federal Office Systems Expo (FOSE) trade show that began on March 21, 1995 (RBr at 84); that in connection with the FOSE show, Norman issued a press release entitled "Norman Data Defense Systems Unveils the Norman Firewall," which notes the product's virus checking capabilities, use of proxy servers and use of SMTP and FTP protocols (Id.; see RX-95); that the antivirus and FTP capabilites of the Norman Firewall were physically demonstrated at the FOSE show; that observers were informed that the product included SMTP capabilities, which were not exhibited for "logistical reasons"[28] (RBr at 84); that "the Norman Firewall used proxy servers and daemons to perform content checking of various kinds, including antivirus checking, as FTP files and SMTP mail messages crossed the firewall (RBr at 85); that if the file received was of a type unlikely to contain a virus, said file was sent directly to its destination without being scanned (Id.); that if the file was of the type that was likely to contain a virus the file would be scanned and transferred to its final destination if no virus was found (Id.); and that if the Norman Firewall detected a virus on the transferred file, "then the message could be blocked or quarantined." (Id.)

Respondent further argued that "the documentation of record makes clear that by April 1995, the Norman Firewall had an SMTP proxy server that received mail messages and scanned them for viruses" (RRBr at 100; see RPFF 1649-70); that while the Norman Firewall documentation of record discusses the product's ability to scan all files for viruses contrary to the

[28] As to the Norman Firewall's SMTP capabilities at the FOSE show, respondent argued that the SMTP proxy was working as of March 1995, which feature was confirmed through the testimony of Crider and Nispel, as well as supporting documentation entitled "An Introduction to the Norman Firewall" (RX-9) and "The Norman Firewall User and Administration/Maintenance Guide" (RX-122). (RBr at 85.) Respondent further argued that the "Introduction to the Norman Firewall" document, which is dated June 1995, accurately described the Norman Firewall "as it existed prior to May 1995." (RBr at 86; see RX-9.)

limitation of the '600 patent's claim 4, Stang and Nispel's hearing testimony confirms that such statements were "just marketing hype" (RRBr at 102); and that Stang's testimony that the Norman Firewall was able to scan only file types likely to contain a virus was consistent with testimony of Nispel and Crider. (Id.) Respondent also argued that "there is substantial evidence ... [that] the Norman Firewall could scan mail messages for encoded portions, place each encoded portion in a separate temporary files (under Fortinet's definition), decode the encoded portions, and scan the decoded portions and test for viruses by August 1995" (RRBr at 103); that if the administrative law judge construes the "temporary file" limitation of claim 11 consistent with complainant's proposed construction and determines that Fortinet practices said limitation, "the Norman Firewall also practiced this element from the time it was first capable of scanning and decoding emails with attachments, which was by May 1995"[29] (RRBr at 104; see RPFF 1731-32); and that claim 13 should similarly be found invalid for the same reasons relating to the alleged invalidity of claims 1, 3 and 11. (RRBr at 104.)

In response to complainant's arguments about the sufficiency of the testimony relating to the functionality of the Norman Firewall, as well as the supporting Norman Firewall documentation to corroborate such testimony, respondent argued that the Norman Firewall product itself, not the supporting documentation, is the prior art reference under Sections 102(a) and (g) of the Patent Act (RRBr at 95); that the dates of publication for each of the documents "An Introduction to the Norman Firewall" (RX-9), "The Norman Firewall User and Administration/Maintenance Guide" (RX-122) and "The Norman Firewall Whitepaper" (RX-

[29] Respondent argued that if the administrative law judge construes "temporary file" consistent with its proffered construction and finds that claim 11 was conceived on or before August 1995, then claim 11 would have been obvious to a person of ordinary skill in the art. (RRBr at 104.)

123) are irrelevant because such documentation "accurately describes the Norman Firewall in all material aspects in April 1995" (RRBr at 95); that the undisputed evidence reflects that RX-122 was drafted by April 1995 as indicated by the date on the document, RX-9 was drafted by June 1995 and RX-123 "appears to have been drafted by early 1996" (RRBr at 96; see RPFF 1591); and that while respondent concedes that said documents are not identical because they were created at different times, the documents are sufficiently contemporaneous to establish the structure and operation of the Norman Firewall in April 1995. (RRBr at 96.)

Complainant argued that the Norman Firewall references, viz. "The Introduction to Norman Firewall" (RX-9), "The Norman Firewall User's Guide" (RX-122) and "The Norman Firewall White Paper" (RX-123), should not be considered prior art to the '600 patent because respondent has not established that said references depict the state of the Norman Firewall product prior to the September 26, 1995 filing date of the '600 patent (CBr at 83); and that while RX-9 and RX-122 are dated prior to the '600 patent filing date, "Nispel and Crider's testimony indicates that all three references [RX-9, RX-122, RX-123] were not available to the public until well after the filing date, and more importantly includes features that were not implemented until well after the filing date." (CRBr at 81.) Complainant further argued that the three aforementioned references are insufficient to corroborate testimony regarding the allegedly invalidating firewall due to inaccuracies and inconsistencies; that RX-9, dated June 1995, describes a two-processor implementation, while RX-122, dated April 1995, describes a three-processor implementation; that the undated RX-123 describes the Norman Firewall as including an HTTP proxy while RX-122, dated April 1995, indicates that the Norman Firewall does not contain an HTTP proxy; and that RX-123 describes a different version of the Norman Firewall than the one demonstrated at the FOSE trade show "because RX-123 describes a complied version of the Norman Firewall, whereas the Norman Firewall at the FOSE trade show was in{ }(CRBr at 82.) As to the "Norman Data Defense Systems Unveils the Norman Firewall" press release, complainant argued that said release is an ambiguous document and unreliable as corroborating evidence, citing Finnigan Corp. v. ITC, 180 F.3d at 1366 (CBr at 85); and that the hearing testimony of Stang and Nispel, as well as Crider's deposition testimony from the NAI litigation, is merely uncorroborated testimony regarding the allegedly invalidating Norman Firewall product.[30] (CBr at 86-89 citing Finnigan Corp., 180 F.3d at 1366 and Juicy Whip, 292 F.3d at 741 ; see CRBr at 80 (arguing evidence insufficient to establish Norman Firewall as prior art under 102(g)), 81 (arguing evidence insufficient to establish Norman Firewall as prior art under 102(a)).)

Complainant also argued that respondent failed to prove that the Norman Firewall product contained the claimed memory, processing unit and communications unit limitations (CBr at 90; CRBr at 85; see CRRPFF 1626-48); that the Norman Firewall references do not disclose the claimed proxy server because "the FTP mechanism apparently used by the Norman Firewall is not a proxy server because it has two clients - the first client downloading a file from an external server and the second client uploading the file to the internal client" (CBr at 91); that respondent's expert admitted that the Norman Firewall does not practice the claimed proxy server limitation (CRBr at 85-86); that contrary to the staff's position, both Mitchell and Bishop

[30] Complainant argued, as one example of a lack of corroboration, that the only support for respondent's assertion that the Norman Firewall was completed and tested by the end of 1994 is Crider's deposition testimony from the NAI litigation, which is uncorroborated by any other evidence of specifically what was completed and tested by the end of 1994. (CRBr at 80; see CRRPFF 1538-57.)

agree that the Norman Firewall does not meet the proxy server limitation when processing FTP transfers (CRBr at 94, citing CRSPFF 138-77); that there is insufficient evidence to support a finding that the Norman Firewall teaches or suggests an SMTP proxy server (CBr at 91-92; CRBr at 86-87); and that an SMTP proxy server for scanning viruses was never implemented in the Norman Firewall and therefore, does not teach or suggest the SMTP proxy server and daemon limitations of claim 3. (CBr at 92; CRBr at 87-88.)

Complainant in addition argued that Norman Firewall references fail to anticipate at least the following claim limitations: "performing a preset action on the data using the server if the data contains a virus," "sending the data to the destination address if the data does not contain a virus," and "determining whether the data is of a type that is likely to contain a virus" (CBr at 92); and that the documents offered to corroborate the functionality of the Norman Firewall teach away from the "determining whether the data is of a type that is likely to contain a virus" limitation because they indicate that the Norman Firewall scans all files for viruses. (CRBr at 88-89.) Complainant further argued that the Norman Firewall references do not contain any disclosure on scanning emails for encoded portions "or the kind of detail that's relevant to claims 11, 12, 13, 14 or 15 regarding handling of email messages that have attachments and encoded portions" (CBr at 93); that respondent relies solely on Nispel's testimony to prove that the Norman Firewall practices the claim limitation of storing encoded portions in a separate temporary file without any other corroborating evidence (CRBr at 90); and that the Norman Firewall does not disclose the SMTP proxy server and daemon as claimed in asserted claim 13. (CBr at 94; see CRBr at 92-93.)

The staff disagreed with complainant's position that the Norman Firewall documents (RX-9, RX-122, RX-123) do not corroborate the public use of the Norman Firewall in March 1995 and argued that the alleged inconsistencies among the documents merely reflect modifications to the Norman Firewall after March 1995, which "modifications and updates are, of course, the standard practice with software" (SRBr at 6); that Crider's deposition testimony from the NAI litigation referencing the source code relating to the firewall aspect of the Norman Firewall, as opposed to its antivirus functionality, should be considered sufficient corroborating evidence regarding the functionality of the Norman Firewall (SBr at 61, n.34, <u>citing</u> JX-16); that there is no inconsistency between RX-123 and Crider's deposition testimony because the evidence shows that the source code for the Norman Firewall at the time of the FOSE trade show { } at the beginning of 1996 (SRBr at 6); that the fact that RX-123 indicates that the Norman Firewall contains an HTTP proxy server while earlier corroborating documents do not, merely indicates that the HTTP functionality was added "some time after January 1996"; that RX-9 indicates that the Norman Firewall comes with two CPUs yet can support a four-CPU configuration, thereby eliminating any inconsistency among Norman Firewall documents describing two and three-CPU implementations (SRBr at 7); and that the Norman Firewall was publicly demonstrated at the FOSE trade show in Washington, D.C. that began on March 21, 1995 and ran for several days, which public use is corroborated by a press release announcing the "unveiling" of the Norman Firewall at the FOSE show. (SBr at 62, <u>citing</u> RX-95.) As to corroboration of the Norman Firewall demonstration at the FOSE show, the staff argued that the firewall portion of the Norman Firewall product source code written by Crider was produced in the NAI litigation, which Crider referred to in his deposition testimony, included the SMTP proxy code indicating that it was last modified on March 23, 1995; and that "the dates on the front of RX-9 and RX-122 and the testimony of witnesses with knowledge of their creation demonstrate that these documents were created close enough to the time of the FOSE trade show that they can be considered contemporaneous." (SRBr at 8, n.2.)

As to claim 1 of the '600 patent, the staff argued that the Norman Firewall practiced the preamble and memory, communications unit and processing unit limitations of claim 1 (SBr at 63-64); that the Norman Firewall, as demonstrated at the FOSE show in March 1995, meets the proxy server limitation of claim 1 even under complainant's construction of the proxy server limitation because "in an FTP transfer, the Norman Firewall forwards data requests and replies using Internet protocols between clients in an internal network (the LAN workstation) and external servers (remote hosts) whether originating from the clients or the external servers" (SBr at 64-65, citing RX-9); that despite complainant's contention that the Norman Firewall does not contain a proxy server because the workstation uses the TELNET protocol to log into the firewall, "a Norman Firewall user still issues FTP commands from the workstation and the remote host issues FTP replies, and the proxy servers understand these commands and forwards or responds to these commands accordingly" (SBr at 67); that regardless of whether the Norman Firewall uses FTP client software to transfer the file to the workstation, "[l]ooking at the overall transaction between an internal workstation and a remote host, it is clear that the Norman Firewall is acting as a server to the internal workstation insofar as the workstation initiates the communication with the firewall" (SBr at 70; see JX-16); and that the evidence shows that no human interaction was required to send a scanned file from the Norman Firewall on to the destination address and therefore satisfies the daemon limitation of claim 1. (SBr at 71.)

As to asserted claim 3 of the '600 patent, the staff argued that the Norman Firewall was capable of practicing the SMTP proxy server and SMTP daemon limitations of claim 3 when demonstrated at the FOSE show in March 1995; and that "clear and convincing proof exists in the fact that the SMTP proxy software module indicates that it was last modified on{

} (SBr at 71.)

The staff further argued that the Norman Firewall, alone or in combination with other references, has not been shown to invalidate claims 4, 7, 8 and 11-15 (SBr at 71); that respondent has failed to prove by clear and convincing evidence that the Norman firewall practiced the claim limitation of "determining whether the data is a type that is likely to contain a virus" and transmitting the data "without determining whether the data contains a virus . . . if the data is not of a type that is likely to contain a virus" due to conflicting testimony in the record (SBr at 72; compare JX-16 (Stang) at TMI 00176004-07 with Nispel, Tr. at 1197-98); and that respondent has also failed to prove by clear and convincing evidence that the Norman Firewall possessed the limitation in independent claims 11 and 13 relating to scanning encoded portions or storing in separate temporary files and decoding. (SBr at 73.)

a. Independent System Claim 1 And Dependent Claim 3

In issue is whether the Norman Firewall anticipates independent system claim 1 and dependent system claim 3 under 35 U.S.C. §§ 102(a) and (g). Section 102(a) requires that the prior knowledge or use of the invention be public "in some minimum sense" to be invalidating. 1 Donald S. Chisum, Chisum On Patents § 3.05 (2004); see Woodland Trust, 148 F.3d at 1370. An invention will be deemed to have been used publicly if the device shown to the public practices the claim. There is no requirement where, as here, computer programming code is at issue, the actual source code providing the patented functionality be publicly disclosed. Netscape Comm. Corp. v. Konrad, 295 F.3d 1315, 1323 (Fed. Cir. 2002); see also Eolas, Technologies Inc. et al. v. Microsoft, 399 F.3d 1325, 1334-35 (Fed. Cir. 2005).

{

}[31]{ } (Nispel, Tr. at 1170.) {

} (Nispel, Tr. at 1168, 1170.) {

} (Id.) {

}[32] (Nispel, Tr. at 1172.){

}(Niespel, Tr. at 1173-75.){

}(JX-16 (Crider Depo., NAI Litigation, June 22, 1999) at TMI00176181-82 (referring to firewall as "classified machine").){

}(Nispel, Tr. at 1175; JX-16 at TMI00176078.){

[31] {
}

[32] A technical dictionary published within the relevant time period in issue defines firewall as:

> A combination of hardware and software which limits the exposure of a computer or group of computers to an attack from the outside. A firewall is a system or combination of systems that enforce a boundary between two or more networks.

(SX-6 at 253.)

}(JX-16 at TMI00175976; Nispel, Tr. at 1176.) The programmers tried many antivirus products to remedy the virus problem, and of the many tried, only a software product from Norman Data Defense Systems, Inc. (NDD) successfully removed the virus. (JX-16 at TMI00175976, 6078-79.)

Crider testified that in February or March of 1994, while Crider was still working at DSA, at least Crider and David Stang, President of NDD, met on two occasions to discuss the concept of incorporating Norman's antivirus engine into a firewall architecture. (JX-16 at TMI00175977-78.) However, it was not until after Nispel and Crider left DSA and formed Communications, Arts and Sciences (CAS) in September 1994 that Nispel and Crider, on behalf of CAS, entered into an agreement with NDD to commercialize their firewall product. (JX-16 at 175972.) In November 1994 CAS and Norman signed an agreement to jointly develop and market a firewall. (Nispel, Tr. at 1179; see JX-16 at TMI00175979-80.) By at least December 1994, the parties to the agreement understood that the firewall product would include some antivirus functionality. (Compare Nispel, Tr. at 1180 with JX-16 at 175982.)

Trend Micro argued that it "appears that the [November 1994] contact only required CA&S [CAS] to make a firewall and there was no work done in November 1994 to modify the firewall to allow for processing of anti-virus requests." (CRSBr at 16.) Contrary to Trend Micro's argument, the evidence indicates that the relevant technological know-how that Norman had for the November 1994 joint development contract between CAS and Norman was Norman's antivirus capabilities. The actual joint development agreement was produced in the case Trend Micro filed against Network Associates, i.e. the NAI ligitation, and Crider, among others, testified about{

}

(JX-16 at TMI00175982 (emphasis added).)

Pursuant to the November 1994 agreement between NDD and CAS, Crider and Nispel began working on the firewall aspect of the Norman Firewall product in November 1994 while Kristian Bognaes was working on the antivirus component of the project in Norway.[34] (JX-16 at 175980-984, 175988, 176064; see Nispel, Tr. at 1181-82.) Bognaes was the individual at Norman responsible for the antivirus programming while Crider wrote most, if not all, of the software relating to firewall capabilities. (Nispel, Tr. at 1181.) Crider testified that he started working on the "first proxy"; that said first proxy that he and Nispel worked on was the FTP proxy; that CAS delivered a "beta version" of the Norman Firewall to NDD by January 7, 1995; and that said beta version included an FTP proxy that could "intercept the transmission of a file being transferred in the FTP protocol, detour[] it into the antivirus engine, and then based on the results, pass[] it on to the user if it was allowed."[35] (JX-16 at TMI175984-85.) At the hearing, Nispel recalled that CAS delivered two prototype versions of the Norman Firewall to NDD, one

[33] See JX-16 (Crider Depo.) at TMI00175979-82 (agreement marked as Exhibit 608 in deposition). As with other documents that existed in the NAI litigation, the agreement itself could not be located during discovery in this investigation and thus is not of record.

[34] Bognaes's deposition was taken on February 14, 2005 in Europe and the deposition testimony was admitted into evidence at the March 29 hearing.

[35] Crider testified that by January 7, 1995, working beta versions of the Norman Firewall were installed at NDD in Fairfax, Virginia and at a location in Norway. (JX-16 at 175987.)

in February 1995 and the other in the first half of April 1995. (Nispel, Tr. at 1183.) Nispel indicated that the first delivery version utilized the Norman antivirus scanner and that the second delivery encompassed a firewall, two Intel platforms and the Norman antivirus engine. (Id. at 1184.) With respect to CAS's February and April 1995 deliveries to NDD, Nispel testified that both versions of the Norman Firewall included "some form of antivirus function although he was not positive "how well that function worked on the February delivery." (Id. at 1188.)

Stang, Crider and Nispel all testified that NDD exhibited and publicly demonstrated the then-current version of the Norman Firewall at the Federal Office Systems Expo (FOSE) held in March 1995 in Washington, D.C.[36] (Stang, Tr. at 1091-94; JX-16 at 176008-13; Nispel, Tr. at 1189.) As to the specifics of the Norman Firewall demonstration, Crider testified:

> Q. [] [W]hy were you there [at FOSE], you personally?
>
> A. Excuse me. I was there to demonstrate the firewall to the general public, anyone that appeared interested in the booth setup. We had a combination slide show demonstration and a physical setup, three-computer-system setup involving an internal workstation, the Norman firewall and an external system. Basically, it was a set of three components networked together to show the user interface, the virus scanning capabilities, the hotwords scanning capabilities, the networking auditing capabilities and the denial of access capabilities of the system.

[36] Both Crider and Stang testified that the Norman Firewall public demonstration at the FOSE show happened in March 1995. (JX-16 at 176008-09; Stang, Tr. at 1091.) The administrative law judge finds that Crider and Stang's testimony regarding the March 1995 date of the FOSE show is corroborated by RX-95, a press release with a headline "Norman Data Defense Systems Unveils The Norman Firwall" and dateline "FOSE '95, Washington, March 21." (See RX-95.) The press release expressly notes the firewall's virus checking capabilities, use of proxy servers, and use of FTP and SMTP protocols. At said FOSE show, the Norman booth included a slide show as well as actual demos of FTP file transfers (one clean, one infected) from a laptop on one side of the firewall to a laptop connected on the other side. (Nispel, Tr. 1189-91, 1214.) The FOSE show was open to the general public and individuals who watched the demonstration were not required to sign non-disclosure agreements. (Nispel, Tr. 1190; JX-16 at TMI00176008, 6010.)

Q. Did you actually have a working system at your booth at - at the FOSE trade show?

A. Yes.

Q. And as part of your demonstration, did you attempt to transfer data through the firewall at the booth?

A. Yes.

Q. Okay. What types of data transfers did you attempt while the system was set up in the booth at the FOSE show?

A. The only protocol that we were demonstrating at the FOSE show was the FTP protocol. Specifically, we were transferring two separate files, one that contained a virus, and the second one that did not, and I had testified prior that I didn't remember the virus that was being transferred back and forth between the two systems. It was the Jerusalem virus that was being transferred back and forth between the two systems. That was the specific virus that was being caught for demonstration purposes.

* * *

Q. And can you tell me approximately how many times you demonstrated the operation of the Norman firewall at that show each day?

A. Each day, I'm not sure that I can give you an accurate count of that, but I can tell you that we collected around 400 or so names of interested parties that had stayed to see either the slide show or the demonstration and had had their exposition card swiped by the - the tracking software in the booth.

* * *

Q. Did you require anyone to - who saw the system demonstrated to sign any kind of non-disclosure agreement?

A. Oh, as far as demonstration purposes are concerned no.[37]

* * *

Q. Did you discuss the system with any of the people who stopped to see a demonstration at the booth?

[37] Both Stang and Nispel testified that NDD did not require that exhibit attendees sign non-dislosure agreements relating to the Norman Firewall demonstration at the NDD booth at the FOSE show. (Stang, Tr. at 1099; Nispel, Tr. at 1190.)

A. Absolutely. That was the whole purpose of the show was to publicize the fact that the Norman firewall existed, and to convey to the general public that it was a high-assurance product that protected against intrusion and protected against virus attacks.

Q. And did you describe any of the details about how the system worked to any of the people who asked you about it?

A. To anybody who stopped and asked.

Q. Did you disclose to people that it included an FTP proxy server?

A. Yes.

Q. Do you recall discussing with - with folks that stopped at the booth that it included - that it had an SMTP proxy server?

A. The statements that we made were that the proxies available at the time were the FTP, TELNET and SMTP and that other modified proxies would be available as they were developed....

(JX-16 at176009-10, 176012 (objections omitted) (emphasis added).) Nispel testified that the antivirus functionality of the Norman Firewall was "consistently effective" to demonstrate at the time of the FOSE show. (Nispel, Tr. at 1188-89.) Nispel further testified that the Norman Firewall, as of the time of the FOSE show in March 1995, did not require human intervention at the firewall to transfer files between computer networks. (Nispel, Tr. at 1191.) With respect to the FOSE demonstration, Nispel testified that the Norman firewall implemented an FTP proxy server and an FTP daemon. (Id. at 1192.) The evidence further shows that the Norman Firewall had SMTP capabilities in March 1995, when it was publicly displayed at the FOSE show, with some form of SMTP file scanning enabled within weeks, one way or another, of the FTP implementation. (Nispel, Tr. at 1192-93; RX-9 at TMI00057538.) {

} Thus in Crider's deposition, the source code for the firewall portion of the Norman Firewall was produced, and

Crider testified extensively about it. {

}(JX-16 at TMI00176004-07.)

As respondent's expert Bishop testified, the Norman Firewall satisfies each and every element of claim 1 of the '600 patent. Bishop explained how the Norman Firewall, as it existed prior to May 1995, practiced the first three elements of claim 1 (the memory element, the processing unit element, and the communications unit element). (Bishop, Tr. at 2002-08.) As Bishop further testified, the Norman Firewall also satisfied the proxy server and daemon elements of claim 1. (Bishop, Tr. at 2009-11.) Specifically, the documentation of record makes clear that prior to May 1995, the Norman Firewall had an SMTP proxy server that received mail messages and scanned them for viruses, and an SMTP daemon that transferred the mail messages from the proxy server to the destination without human intervention. (JX-16 at TMI 0176005, TMI 0176007, TMI 0176024, TMI 0176026-27; Nispel, Tr. at 1215-17, 1224, 1228; RX-9 at TMI 00057538, TMI 00057541, TMI 00087228; RX-122 at FHC 003341.) Also, the FTP proxy server was demonstrated at the FOSE show in March 1995, with the Norman Firewall having SMTP capabilities in March 1995 and with the SMTP proxy server and daemon being fully operational to scan for viruses by April 1995. (JX-16 at TMI 0176010; Nispel, Tr. at 1215-17, 1224, 1228.[38])

[38] Trend Micro argued that uunencoding is needed to handle emails for viruses and until that functionality was added, the Norman Firewall would not send emails for viruses. (CRSBr at 9.) Uuencoding, however, is only necessary to send non-text (binary) files as attachments to email. (Bishop, Tr. at 2498-99.) Uuencoding is not needed for mail messages without attachments or for mail messages with text attachments. (Mitchell, Tr. at 2569.) Thus, whether the Norman Firewall had the ability to handle uuencoded portions has no relevancy to claims 1 and 3.

Various technical documentation describing the functionality and features of the Norman Firewall was admitted into the record at the hearing. (See RX-9; RX-122; RX-123.) RX-122 is a 27-page document entitled "Norman Firewall User and Administration/Maintenance Guides" and bears the date "April 1995" on the first page. (RX-122 at FHC 03335-61.) Crider testified that he was involved in drafting almost all of the technical documentation for the Norman Firewall, including said Norman Firewall User and Administration/Maintenance Guides. (JX-16 at 176019.) While RX-122 bears the date "April 1995," Crider testified that work began on the document prior to it being published in April 1995. (JX-16 at 176021.) Nispel testified that RX-122 accurately describes the structure and functionality of the Norman Firewall as of April 1995. (Nispel, Tr. at 1224.) The Product Overview section of RX-122 describes the Norman Firewall as "the most secure internetworking firewall device available" and "the only firewall on the market to incorporate impenetrable firewall protection with an antivirus engine." (RX-122 at FHC 003337.)

The administrative law judge finds that the FOSE press release (RX-95) and Norman Firewall User Administration/Maintenance Guides (RX-122) corroborate the testimony of Crider and Nispel pertaining to their development of the Norman Firewall, viz. a system for detecting and selectively removing viruses in data transfers. For example, the press release corroborates Crider, Nispel and Stang's testimony relating to the demonstration of the Norman Firewall at the FOSE show in March 1995. (RX-95 at TMI0087225 ("Norman Data Defense Unveils The Norman Firewall").) Moreover, the document also discloses that the "Norman Firewall combines an integrated front-end server, proxy server and virus detector to defend systems and information"; that "[t]he existence and operation of the proxy server allows integration of robust security mechanisms to prevent an outside sender from violating the system"; and that "[t]he Norman Firewall essentially opens incoming and outgoing data packets, and inspects, virus-checks (against more than 6,500 known viruses), and repackages the data packets, before delivery to their destination[] [such that] [n]o packets ever need to directly enter or leave internal networks." (Id. at TMI0087225-26.) In addition, the press release includes a product specifications section relating to the Norman Firewall's satisfaction of the communications unit limitation of claim 1, which states that the product "attached LANs to the Internet via dial-up or dedicated 66KB or T1 facilities" and is Ethernet compatible. (Id. at TMI00087227.)

With respect to the proxy server and daemon limitations of asserted claim 1, the Norman Firewall User Administration/Maintenance Guides disclose that "all of its user services are [provided] through proxy," that such proxy services "are executed on your behalf by the firewall" and that [t]his difference is nearly invisible to you."[39] (RX-122 at FHC 003341.) The document also indicates that the Norman Firewall supports "SMTP (Internet E-Mail)," which specifically relates to the additional limitation that dependent claim 3 adds to claim 1. (Id.) With respect to the processing unit limitation of claim 1, RX-122 references the Norman Firewall's "multiple independent processors" that include a "SecureWare SMP+ Operating System," a "Front End System (DOS, Windows, Windows NT, UNIX, etc.)" and an "Antivirus System." (RX-122 at FHC 003344; see id. at FHC 003357 ("The hardware platform of the Norman Firewall is an Intel 80486 multi processor system.").)

Further corroboration of the testimony of Crider and Nespel pertaining to the development of the Norman Firewall is found in new evidence admitted into the record at the

[39] The Norman Firewall conducted file transfers at the application layer. (RPFF 1614 (undisputed).)

March 29, 2005 hearing. The administrative law judge finds that the new evidence established that{

}(JX-18 (Bognaes Depo.) at 13-18.) In evidence are the{ }(RX-215) and{ }(RX-212).

{ }(JX-18 at 57.) The directory of files indicates that{ }(RX-212; JX-18 at 56-57, 95.){ }(RX-212; JX-18 at 61).) The evidence shows that{

}(JX-18 at 93.) The fact that{ } is also corroborated by other testimony. (Nispel, Tr. at 1245 (testifying that{ }

Significantly,{ } corroborates the development time line provided by other witnesses. (JX-18 at 15; Bishop, Tr. at 2400.) The administrative law judge further finds that said new evidence shows that the antivirus engine being used was from 1994, thus indicating that the Norman Firewall possessed the

[40] { } (RX-215 at F-NN00002.)

scanning functionality required by claims 1 and 3, and specifically that the Norman Firewall included "a proxy server scanning the data to be transferred for viruses." Also the evidence admitted into the record on March 29 shows that the{

}(See, e.g., JX-18 at 13, 25-26; Bishop, Tr. at 2406, 2417.) The administrative law judge finds that such evidence corroborates the testimony of Crider and others that{

}.[41] In addition, evidence admitted on March 29, 2005 shows that the{

}(See JX-18 at 69; Mitchell, Tr. at 2567-68.)

Trend Micro argued that "Bognaes confirmed that the Norman Firewall{

} (CRSBr at 29.)

Bognaes, however, did not testify that{

[41] See JX-16 at TMI00176001{

}TMI00176060{

}),

TMI00176083-84{

} TMI00176089-91, TMI00176094, TMI00176105-08.)

} (JX-18 at 77.) Thus, Bognaes testified that{

} (JX-18 at 13, 25-26; see Bishop, Tr. at 2406, 2417.) The administrative law judge finds that Bognaes' testimony is corroborated by that of Crider (as well as the proxy source code about which he testified) that the{

}(See fn. 41 supra.) Hence, he finds that there was no need for{

} Rather, the only required capability of the platform was{

} (JX-16 at TMI00176080-96.)

Trend Micro argued that there is insufficient corroboration as to the{ }portion of the Norman Firewall source code because Bognaes lacked personal knowledge of the code. (CRSBr at 9.) However, the administrative law judge finds that the mere fact that Bognaes did not write the code does not detract from the fact that he had access to it and was familiar enough with it during the relevant time frame so that he could write the source code,{ }that tied the proxy source code to the antivirus platform. (JX-18 at 13-15.)

Trend Micro argued that the evidence indicates that the Norman Firewall was not conceived and reduced to practice in the United States of America, as required by 35 U.S.C. § 102(g) because Bognaes testified that the "AV platform source code" was conceived and reduced to practice in Norway. (CRSBr at 14.) However, the evidence indicates that the Norman Firewall fulfilled the "made in this country" requirement of 35 U.S.C. 102(g) when it was "embodied in tangible form," and thus was reduced to practice, in the United States. Scott v. Koyama, 281 F.3d 1243, 1247 (Fed. Cir. 2002). Thus, the administrative law judge finds that the evidence shows that Bognaes traveled to the United States three to four times in the beginning of 1995 and, with Nispel and Crider, tested the Norman Firewall with the conjoined proxy code (written by Crider) and the av platform code (written by Bognaes and Kenneth Walls of Norman). (JX-18 at 20-21.) The administrative law judge further finds that the evidence shows that Bognaes attended trade shows in the United States. (JX-18 at 21-22.) The evidence further indicates that the developers had a working commercial product by the contractually-required delivery date of February 7, 1995.[42] Hence having been reduced to practice in the United States, the Norman Firewall was "made in this country" pursuant to section 102(g).

Trend Micro argued that even if the Norman Firewall was reduced to practice in March 1995, it was thereafter "suppressed" and therefore it cannot be anticipatory under 35 U.S.C. §102(g). (CRSBr at 18.) In support it argued that the evidence of record is clear that{

[42] {

} (JX-16 at TMI00175986.) After that,{

} (Id. at TMI00175986-87.)

}(CRSBr at 18.) However, as to the source code, there is no need to make it publicly available to avoid a finding of "suppression" if, as here, the claim limitations speak in broader terms (i.e., the patent does not claim actual source code methodology). Lockwood v. American Airlines, Inc., 107 F.3d 1565, 1570 (Fed. Cir. 1997). A public use occurs if the device shown to the public practices the claim and there is no requirement that where, as here, computer programming code is running, the actual source code providing the patented functionality be publicly disclosed. See Konrad, 295 F.3d at 1323.

Based on the foregoing, the administrative law judge finds that the Norman Firewall anticipates asserted claims 1 and 3 of the '600 patent pursuant to 35 U.S.C. § 102(a) at least by April 1995, prior to the September 26, 1995 filing date of the '600 patent. (See JX-1.) Complainant, however, can establish that the inventors of the '600 patent, viz. Shuang Ji and Eva Chen, conceived their invention prior to April 1995 to avoid a definitive ruling that claims 1 and 3 are invalid for anticipation under 35 U.S.C. § 102(a). See Markurkar v. C.R. Bard, Inc., 79 F3d 1572, 1576-77 (Fed. Cir. 1996).

Complainant argued that, as of late 1994, co-inventor Eva Chen had already conceived of detecting viruses in email attachments and had already attempted to do so by May 1995 (CPFF 1425, 1427); that when Chen arrived in the United States on May 12, 1995, she had already conceived of the inventions claimed in the '600 patent (CPFF 1422-28); that Chen contacted co-inventor Shuang Ji in May 1995 "to discuss her concept and seek aid in developing the inventions" (CPFF 1429-33); that as of June 20, 1995 the{ } (CPFF 1445-51); and that after the inventors had working prototypes,{ } (CBr at 68-69; see CPFF 1438-40, 1472.)

The staff argued that the conception date of claim 1 was the second week of June 1995 (SBr at 56, citing JX-14 at 111-17, 121); that inventor Ji's testimony is corroborated by "(1) a 'spec' attached to a consulting agreement that Mr. Ji executed with Trend Micro; CX-412; and (2) a July 7, 1995 paper written by Mr. Ji for circulation within Trend Micro; CX-413" (SBr at 56-57[43]); that inventor Chen's brief phone conversation with inventor Ji does not establish the necessary elements of conception (SBr at 56, n.31, citing JX-14 at 109); that "the evidence shows that by the end of June or early July of 1995, Mr. Ji had mapped out the means to implement an SMTP transfer with virus scanning at a gateway as well as the elements of 'preset actions,' 'likely to contain a virus,' and other features of claims 3, 4, 7, 8, and 13" (SBr at 57, citing JX-14 at 153-56, CX-413); and that the evidence shows that the conception date for claims 11, 12, 14 and 15 was the end of June or beginning of July 1995. (SBr at 57-58; see CX-413; JX-14 at 175-76.)

Respondent argued that complainant did not offer any evidence of a conception date for any claim of the '600 patent earlier than the filing date of September 26, 1995 (RBr at 100; RRBr at 89-90); that inventor Chen's testimony complainant relies on to establish an earlier conception

[43] With respect to CX-412, the staff noted that "[a]lthough the document indicates that it became effective on July 6, 1995, the spec indicates that it was drafted on June 26, 1995, approximately a week after the meeting between the co-inventors." (SBr at 57, n.32, citing CX-412, JX-14 at 101, 107-08.)

date does not indicate that she had "'a definite and permanent idea of an operative invention, including every feature of the subject matter sought to be patented'"; that Chen's testimony relating to conception in late 1994 or by May 1995 is uncorroborated; that as to the "mid-June 1995 [] prototype of 'the invention,'" neither inventor testified that the prototype would satisfy the proxy server or daemon elements of claim 1; and there is no documentary evidence corroborating the existence or operation of said prototype. (RRBr at 91.) As to the July 6, 1995 consulting agreement between inventor Ji and Trend Micro, as well as the one-page specification attached thereto, respondent argued that there is no testimony that said agreement or specification discloses all of the elements of any claim of the '600 patent (RRBr at 91); that as to CX-413, there is no testimony "to tie this document to the specific elements of the asserted claims of the '600 patent" (RRBr at 92); and that in any event, CX-413 "does not disclose putting data into a temporary file until after it is decoded, and makes no disclosure of putting each encoded data portion into its own separate temporary file." (Id.)

With respect to the standard applied to establish conception of an invention, the Federal Circuit has commented:

> It is well settled that in establishing conception a party must show possession of every feature recited in the count, and that every limitation of the count must have been known to the inventor at the time of the alleged conception. Conception must be proved by corroborating evidence which shows that the inventor disclosed to others his 'completed thought expressed in such clear terms as to enable those skilled in the art' to make the invention.

Coleman v. Dines, 754 F.2d 353, 359 (Fed. Cir. 1985) (citations omitted); but see Burroughs Wellcome Co. v. Barr Labs, Inc., 40 F.3d 1223, 1231 (Fed. Cir. 1994) ("Obviously, enablement and conception are distinct issues, and one need not necessarily meet the enablement standard of 35 U.S.C. § 112 to prove conception."). Conception has been considered a two-part test where the first part or directing conception element represents the idea "that a certain desired result may be obtained by following a particular plan" and "the second part of conception is 'the selection of the means for effectively carrying out the directing conception.'" Oka v. Youssefyeh, 849 F.2d 581, 583 (Fed. Cir. 1988), quoting Townsend v. Smith, 36 F.2d 292, 295 (CCPA 1929). "[W]here testimony merely places the acts [of conception] within a stated time period, the inventor has not established a date for his activities earlier than the last day of the period." Oka, 849 F.2d at 584, quoting Haultain v. DeWindt, 254 F.2d 141 (CCPA 1958).

Conception represents the inventor's mental act and thus "courts require corroborating evidence of a contemporaneous disclosure that would enable one skilled in the art to make the invention." Burroughs Wellcome Co., 40 F.3d at 1228, citing Coleman, 754 F.2d at 359. However, an inventor does not need to know that his or her invention will work for conception to be complete. Rather, the inventor must establish only that he or she had the idea. Burroughs Wellcome Co., 40 F.3d at 1228. "[T]he discovery that an invention actually works is part of its reduction to practice." Id.; see Sewall v. Walters, 21 F.3d 411, 415 (Fed. Cir. 1994) ("Conception is complete when one of ordinary skill in the art could construct the apparatus without unduly extensive research or experimentation.").

Shuang Ji and Eva Chen are listed as the inventors of the '600 patent. (JX-1.) Chen, currently the Chief Executive Officer at Trend Micro (FF 6), first spoke with Ji in a telephone conversation in late May or early June 1995. (JX-14 (Ji Depo.) at 108 (Trend Micro, Inc. v. McAfee Assocs., No. C-97-20438-RMW (N.D. Ca. March 26, 1998)); JX-15 (Chen Depo.) at 72 (Trend Micro, Inc. v. McAfee Assocs., No. C-97-20438-RMW (N.D. Ca. March 10, 1998)).) During this initial conversation, Chen conveyed her idea of scanning data transfers (FTP) between computers for viruses at a gateway location and the inventors discussed the use of a daemon and proxy server. (JX-14 at 111-12; JX-15 at 73, 76.) At the hearing, Chen described her approach to devising a solution for Internet-borne computer viruses:

> Q. What were those problems that you were attempting to solve?
>
> A. I remember it was when I was in Taiwan there was an engineer, he showed me that -- how he can exchange file with FTP protocol with remote server and just directly sending the file exchange and also how he can attach a file to an SMTP e-mail and exchange it to his friend over in, I forgot which country, very remote country, and by the time I saw it, I see that, I say, wow, if there is a virus in there, then our current solution cannot adequately block it because it never get to store to a destination hard drive. It is just sending on to -- sending out.
>
> And so at that time that's my first time I think, wow, there is a need for a new solution to fix this type of problem.
>
> Q. And, I'm sorry, explain a little bit more why you thought that your desktop and your file server antivirus products wouldn't address the issue?
>
> A Okay. First of all, because this is computer spreading around the world, there is no way you will know that the destination have antivirus loaded on their computer. Plus, if you send out an e-mail attachment, you can send it out to a thousand people at the same time. And those 1,000 people will get the virus infection at the same time. And how are you going to ensure those 1,000 people have the antivirus loaded and have the most up-to-date virus pattern file, virus signature file at that time?
>
> And the file server is -- you have to store the file onto the file server for the file server antivirus to detect it. But in this type of FTP or SMTP transfer,

there is no file server involved in there. So there is no way you can centrally detect those viruses and block them.

* * *

Q. What were your thoughts on how to solve these problems?

A. I start to think, well, this, on the Internet, when you do all this file transfer or especially the SMTP transfer, you have to go through lots of relay servers, and I think if we can insert a proxy server, a server in between that will perform the virus detection before it reach the final destination, that will be the best way.

It is just like when you get into a country, you need to get through the customs and they search and block, say, the immunization check or check your luggage at the gateway. That is the right way to detect and block viruses.

Q. Were there challenges to putting the virus detection on the border, if you will?

A. Yes. A lot.

Q. What were the challenges?

A. First, there was, in early 1995, for instance, if I want to detect viruses attached to e-mail, there is different encoding method. So we need to see what kind of an encoding method we can use to decode the file that would need to scan for viruses. Also there is other challenges such as timeout, because when you are doing the file transfer, two computers connect to each other. If one computer sent a request, the other computer hasn't received it for a period of time, the connection will break out, break up, so that's timeout issues.
So there is various challenges, technical challenge we have to overcome to try to insert the intermediate server to scan for viruses.

Q. How did you address the timeout problem?

A. Are you referring to how the product actually did?

* * *

Q. For your concept in your invention that's reflected in JX 1, what was your concept of having -- of how to solve the timeout problem that you perceived?

A. The timeout problem was solved by various methods. One of them is we used a proxy server concept where we can receive and forward the request, so that the destination will receive the request, so that's one way.

Also we decided that some of the protocols that is capable of containing viruses, we only scan those protocol that is capable of containing, transferring virus file. And we think those files, we also decide if certain file is capable of containing viruses, certain file type, for instance, JPEG file is impossible to containing viruses and we don't need to scan those JPEG files.

Q. How did you address the challenge of the multiple protocols?

A. The multiple protocols, we examine it and we see that the most common use and most possible to transfer viruses is through SMTP protocol and FTP protocol, so we use those two protocols. We scan those two protocols.

Q. When did you come up with the solution to these problems?

A. It was May 1995.

Q. How do you remember that it was May of '95?

A. It was the first day I arrive at the United States. I remember I was sitting in between my luggage and I receive a call from my cousin who is doing his Ph.D. study in Brown University, Boston, and I was

> telling him what I was trying to do to develop something that can scan for viruses at the Internet gateway or Internet server, but at that time most of the Internet gateway servers are running on UNIX platform, so I was asking him does he know anyone that is good at UNIX, developer, UNIX programmers, and he referred me to Shuang Ji, his classmate.

(Chen, Tr. at 20, 22, 24 (emphasis added).)

At some point between the end of May 1995, but before the end of the second week in June 1995, Ji met Chen at Trend Micro's offices "for a couple of hours" to further discuss the inventors' approach to scanning for viruses in data transfers between computers. (JX-14 at 115-16; see JX-15 at 112.) Chen and Ji discussed the use of a proxy server in FTP transfers, the gateway location of the FTP proxy program, the use of a daemon and detecting viruses in email attachments by looking for uuencoded attachments.[44] (JX-14 at 115-18, 121-23; JX-15 at 112-13, 115-16, 141-42.) Ji testified that he and Chen agreed that Ji would have an FTP-specific prototype in "a week or so" after the date of their meeting at Trend Micro's office and that he began working on said prototype a few days later. (JX-14 at 125, 128.) Ji began writing code for the prototype and described its functionality as follows:

{

}

[44] Ji testified that he did not recall if he and Chen discussed SMTP implementation during this meeting. (JX-14 at 126.)

(JX-14 at 137.) Ji testified that{ }(Id. at 139-40.) Chen testified that{ } while Ji indicated that{ }[45] (JX-15 at 122; JX-14 at 143-44.)

At some point after the{ }, Chen, on behalf of Trend Micro, and Ji began negotiating what was later memorialized as the Trend Micro Devices, Inc. Consulting Agreement between Trend Micro and Ji (Consulting Agreement). (JX-14 at 102, 145, 173; see CX-412 (Consulting Agreement).) The Consulting Agreement states that it{ }(CX-412 at TMI00002497.) Exhibit A to the Consulting Agreement is a Project Description that states that it is{ } (Id. at TMI00002502; see JX-15 at 145.) Inventor Ji signed the Project Description under the title "CONSULTANT." (Id.) Exhibit A to the Consulting Agreement describes the project as follows:

> { }

(Id. at TMI00002503.) Inventor Ji prepared the aforementioned specification, dated

[45] Chen testified that the inventors were able to scan FTP transfers for viruses by June 20, 1995 or "actually way before." (JX-15 at 177.)

June 26, 1995, attached to the Project Description, which states:

{

}

(CX-412 at TMI00002504; see JX-14 at 107-08.)

The record also contains a document entitled{ } dated{ } and authored by inventor Ji, which provides a more detailed description of Ji and Chen's invention as compared to the June 26th specification. (CX-413.) Ji testified that he was working actively on CX-413 between{ } while Chen recalled seeing multiple drafts of CX-413 and at least one in June 1995.[46] (JX-14 at 150; JX-15 at 71, 125.) In addition, Ji testified that all the{ } at Trend Micro reflected in CX-413 would have been completed by{ } but that he been had working on testing{ } prior to the{ } date.[47] (JX-14 at 153-56, 175-76.) Ji also testified that prior to the { }date, Chen had contributed the concepts of scanning SMTP transfers, scanning only files with certain extensions for viruses and taking certain actions if a virus is detected. (JX-14 at 174.)

Based on the foregoing, the administrative law judge finds that inventors Chen and Ji had conceived all of the elements of asserted independent claim 1 no later than June 26, 1995. The administrative law judge further finds that Chen and Ji's testimony regarding their first face-to-face meeting at Trend Micro, their account of Ji's demonstration of the FTP prototype and the overall development of their invention between May 12 and June 26, 1995 are sufficiently corroborated by the contemporaneous disclosure of the Project Description and the June 26th Specification attached to the Consulting Agreement. For example, both documents disclose

[46] Inventor Ji testified that CX-413 was not related to the first prototype that he demonstrated at Trend Micro's offices. (JX-14 at 152.)

[47] See also JX-14 at 163-64 (indicating that Internet daemon was running in the background and would "hand" connection to proxy program); 168-69 (discussing FTP proxy server scanning data for viruses and continuing transfer if no viruses found); 216 (describing FTP proxy program passing command between client and FTP server); JX-15 at 129-31 (indicating that SMTP scanning had been completed before the end of June 1995).)

scanning FTP data transfers for viruses. (CX-412 at TMI00002503-04.) The Project Description describes a program running on a "{

}" relating to at least the memory, communications unit, processing unit and proxy server recitations of claim 1. (Id. at TMI00002503; see also CX-413 at TMI00002512{

} In addition, the use of an FTP proxy server in connection with scanning data transfers for viruses is disclosed under the { } of the June 26th Specification. (Id. at TMI00002504.) Moreover, the fact that inventor Ji had already began drafting the more detailed{ } paper before June 26, 1995 further confirms that both he and inventor Chen had a definite and permanent idea of the system of asserted claim 1 as of June 26, 1995. (See CX-413.)

The administrative law judge has found that the inventions claimed in asserted claims 1 and 3, at least by April 1995, were anticipated under 35 U.S.C. § 102(a). He also has found that inventors Chen and Ji had not conceived all the elements of asserted independent claim 1 until June 1995. Hence, he finds that complainant has not established that the inventors Chen and Ji invented the subject matter of independent claim 1, including claim 3 dependent on claim 1, pursuant to the priority of invention rules in 35 U.S.C. § 102(g), before said April 1995 date. Thus, he finds that respondent has established by clear and convincing evidence that independent claim 1 and dependent claim 3 are anticipated by the Norman Firewall under 35 U.S.C. § 102(a).

b. Independent Claim 4 And Dependent Claims 7 And 8

Independent claim 4 has the following language:

> determining whether the data contains virus at the server;
>
> * * *
>
> transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a present action if the data is not of a type that is likely to contain a virus.

(JX-1.)

In order for respondent to establish that independent claim 4 and its dependent claims 7 and 8 are invalid in view of the Norman Firewall, respondent must establish, by clear and convincing evidence, that the Norman Firewall practiced the above limitations which involve scanning only those files of a type likely to contain a virus. Referring to the evidence admitted prior to the March 29, 2005 hearing, the administrative law judge finds conflicting testimony on this point. Thus, while David Stang believed that the firewall did examine file types and would allow certain file types to pass through the firewall without scanning them for viruses, Nispel stated in his 1999 deposition that he was under the impression that the{

}.[48] (Compare Stang, Tr. at 1100-01 with Nispel, Tr. at 1197-98.) Nispel's testimony is corroborated by the Normal Firewall documents that state that the firewall scans every incoming file for viruses. (See, e.g., RX-9 at TMI00057535.) The evidence does show that if file typing was performed, it was performed on the antivirus side of the Norman Firewall.

[48] The evidence shows that Stang was removed from the day-to-day development of the Norman Firewall and had little, if any, involvement in writing the source code. (Stang, Tr. at 1107-08, 1112-13, and 1120.)

(Nispel, Tr. at 1198; JX-16 at TMI00176153{

}

{

}

(Bishop, Tr. at 2420-21.) However, the evidence shows that{

} (Bishop, Tr. at 2421; RX-216 at F-NN00113-14.){

} (JX-18 (Bognaes Depo.) at 85-91; Bishop, Tr. at 2422, 2489; RX-216 at F-NN00113-114.) {

} (JX-18 at 129.) Bishop at the March 29 hearing, some ten years later, hypothesized that{

} (Bishop, Tr. at 2422-24.)

For respondent to show that Norman Firewall anticipates claims 4, 7 and 8, respondent must prove, by clear and convincing evidence, that{ }only scanned those files that were of a type likely to contain a virus. On this point the administrative law judge finds that the January 21, 1997 version of{

} (Bishop, Tr. at 2412-13.) In addition, the{

} (JX-18 at 85-91; Mitchell, Tr. at 2518-19; Bishop, Tr. at 2421-22.) Bognaes did testify regarding the February 28, 1994 version of av.c:

> {
>
> }

(JX-18 at 92 (emphasis added).) However, Bognaes, as for the functionality of the{ } code, testified:

> {

}

Q. Is there any doubt in your mind?

A. No, I am sure about that.

(JX-18 at 126-27 (emphasis added).) As for evidence in the record corroborating this testimony of Bognaes, reference is made to the factors when accessing the credibility of oral testimony regarding potentially invalidating prior art. See Juicy Whip supra. It is a fact that Bognaes has a relationship with the alleged prior user. Thus, he was a Norman employee at the time of the Norman Firewall's development as well as today. Significantly, he wrote the relevant source code some ten years ago and also wrote subsequent versions of the codes at later stages of time. (JX-18 at 8.) The administrative law judge finds those facts raise doubts about Bognaes' ability to remember whether certain functionality was implemented in the critical time frame of early 1995. The administrative law judge finds that it is also significant that the only version of

{

} (Nispel, Tr. at 1197-98.) Nispel's testimony is also supported by certain Normal Firewall documents stating that the firewall scanned every incoming file for viruses. (See, e.g., RX-9 at TMI00057535.) This evidence is consistent with the fact that the Norman Firewall placed a premium on security over performance[49] and that during the 1997 time

[49] See JX-16 at TM100176117-18. Specifically, Crider testified as follows:

{

(continued...)

period other firewall products provided administrators with an option of scanning every file for viruses. For example, early versions of Trend Micro products, such as the 1997 version of InterScan VirusWall, provided administrators with a viable option of scanning every file for viruses for the most secure configuration. (See CX-322.[50]) Also, there is nothing in the record that indicates that the Norman Firewall was a successful product. However, there is evidence that Trend Micro's implementation was a success. (Chen, Tr. at 37-46; see also 35 U.S.C. Section 103 analysis, infra.)

[49](...continued)

}

> Q So if there had to be a trade-off made, you favored security over speed?
>
> A Absolutely.

[50] The Administrator's Guide for InterScan VirusWall 2.0 provided as follows:

> InterScan can check all or specified types of an email attachments for viruses, including the individual files contained in a compressed file.
>
> 7. To scan all file types, regardless of extension, click the **Scan all E-mail attached files** radio button. This is the most secure configuration.
>
> * * *
>
> **Note**: Although decreasing the aggregate number of files InterScan checks for viruses can increase performance, it should be noted that doing so comes at the potential cost of some security.

(CX-322 at TMI00101135-36 (bold in original).)

Fortinet argued that in the Normal Firewall further{ }(RX-216); and that Bognaes stated, and as Bishop confirmed, the Norman Firewall was{ } (RRSBr at 22.) However, in addition to evidence in the record that Norman Firewall placed a premium on security over performance which would involve scanning every file for viruses, there is evidence in the record that{ } Thus, Mitchell testified:

{

}

Q Sir, when you referred to Norman documents in your testimony, what did you mean by that?

A I'm referring to the white paper introduction to Norman Firewall, the documents that were available earlier in this case and that we discussed in January.

Q Does that also include Norman user guide?

A Yes.

(Mitchell, Tr. at 2517-19 (emphasis added).)

Fortinet argued that because Trend Micro argued that Fortinet's accused products practice the last two steps of claim 4 in that{ } the Norman Firewall practiced said steps of claim 4 as there would have been no virus signatures for text files, and there would have been no virus signatures for files that did not match any of the extension types identified "in av.c." (RRSBr at 26, n.15.) Fortinet, however, has not established, by clear and convincing evidence, that the Norman Firewall{ } worked the same as Fortinet's own antivirus engine. Moreover, there is evidence that unlike the Fortinet code where a virus signature may only be applied to certain file types,

{

} (See Bishop, Tr. at 2490.)

Based on the foregoing the administrative law judge finds that respondent has not established, by clear and convincing evidence, that the Norman Firewall anticipates claims 4, 7 and 8 of the '600 patent.

c. Independent Claim 11, Dependent Claims 12, 14 And 15 And Independent Claim 13

Independent Claim 11 has the language:

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

(JX-1.) Independent claim 13 has the language:

> wherein the step of sending the mail message to the destination address is performed if the mail message does not contain any encoded portions; the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to node having an address matching the destination address.

(JX-1.)

As seen from the language of independent claim 11, its limitations involve scanning for encoded portions and storing such portions in separate temporary files. Independent claim 13 involves the additional limitation of sending mail messages without encoded portions (i.e. text files) on to the destination address.

In order for respondent to establish that independent claim 11 and its dependent claims 12, 14 and 15 and independent claim 13 are invalid in view of Norman Firwall, respondent must establish, by clear and convincing evidence, that the Norman Firewall practiced the above limitations of independent claims 11 and 13. The administrative law judge finds that respondent has not met its burden. The record has no documentary evidence which involved the Norman Firewall and showed testing or source code for scanning mail messages and encoded portions even prior to the September 26, 1995 filing date of the '600 patent. Moreover, while January 21, 1997 version of firewall.c indicates that the code may possess some functionality allowing for the decoding, scanning and processing of an encoded email attachment, the fact remains that the submitted verison of firewall.c code is dated more than a year after the filing date of the application that matured into the '600 patent.

Respondent argued that the source code for the antivirus platform of the Norman Firewall and Bognaes' testimony further corroborates, as Bishop confirmed, that the antivirus platform of the Norman Firewall did, in fact, determine whether each object included any encoded portions, store each encoded portion in a separate temporary file, decode the encoded portions of the mail message to produce decoded portions of the mail message, scan each of the decoded portions for a virus, and test whether the scanning step found any viruses by comparing the results of the scan with known virus signatures and providing a report from the antivirus platform to the firewall.

(RRSBr at 27-28.) However, respondent relied only on{ }(See RX-212; RX-215.) { }

In view of certain inconsistencies in defining constants, the administrative law judge finds that respondent has not established, by clear and convincing evidence, that they were used with one another. Thus, while{ } (Mitchell, Tr. at 2528-29.) The failure of{ } would indicate that the version of the Norman Firewall that operated with{ } (See CX-582.) Also given that the "last modified" date on{ } the administrative law judge finds that the state of the code in early 1995 is better reflected in{ }

In addition, Fortinet acknowledged that{ } (RRSBr at 32; Mitchell, Tr. at 2527-28; Bishop, Tr. at 2448-49.) Hence, the administrative law judge finds that{ } would not satisfy the limitation of claim 11 that requires that each encoded portion of a mail message be stored in a separate temporary file. Fortinet argued that adding such capability would be fairly straightforward. (RRSBr at 32.) However, it is a fact that Norman did not implement the functionality, notwithstanding the fact that{

}

Fortinet argued that the manner in which compressed files are stored and scanned meets the requirement of claim 11 (under Trend Micro's construction) that each encoded portion be stored in a separate temporary file prior to scanning. (RRSBr at 30-31.) However, the evidence shows that compressed files are not encoded files, as Fortinet's own expert Bishop, testified. (Bishop, Tr. at 2441-42; accord Mitchell, Tr. at 2530.) Accordingly, the administrative law judge finds that the information on the method by which the Norman Firewall stored and scanned compressed files does not lead to the conclusion that the Norman Firewall met this limitation of claim 11. Hence he finds that firewall.c does not provide the functionality needed to invalidate claim 11 or dependent claims 12, and 14-15.

The administrative law judge further finds that Fortinet has failed to meet its burden of proof with respect to claim 13 for the same reason it has failed with respect to claims 4, 7, and 8. Claim 13 requires that a mail message be passed on without being scanned in the event that it does not have an attachment. However, the administrative law judge finds that the evidence shows that{

} thereby failing to practice the claim limitation. (Bishop, Tr. at 2452.)

2. Intel LANProtect/LANDesk

Respondent argued that the Intel LANProtect product[51] constitutes prior art to the '600 patent under "at least" 35 U.S.C. §§ 102(a) and (g) and anticipates asserted claims 4, 7 and 8 of the '600 patent (RBr at 88; see RBr at 109, 115, 116); and that the "operation of the LANProtect as it existed prior to May 1995 is described in the 1992 Intel LANProtect 30-Day Test Drive Version, (RX-76), and the 1992 Intel LANProtect Software User's Guide, RX-77." (RBr at 88; see RPFF 1794-96; RRBr at 104-05.) Respondent further argued that the LANProtect was a file server-based antivirus program that was capable of connecting to other networks and functioning as an internal gateway between two networks (RBr at 86); that the Intel LANProtect operated as an intermediary server scanning data and mail messages in transfer between a source and destination (Id.; RRBr at 105-06); and that the LANProtect determined whether the data transferred was of a type likely to contain a virus as it performed "real-time scanning by default on only files of selected file extensions that represented executable files, and were therefore likely to contain a virus." (RBr at 87, 116.)

As to the Intel LANProtect/LANDesk references, complainant argued that respondent has failed to establish which features and functions the Intel references possessed prior to September 1995, especially considering that respondent has not produced any actual Intel LANDesk product

[51] Respondent, in its post-hearing submissions, referred to the Intel LANDesk Virus Protect and the Intel LANProtect products "jointly as 'Intel LANProtect' or 'LANProtect.'" (RBr at 86, n.37.) The administrative law judge is following the same naming convention with respect to the Intel prior art references asserted by respondent and thus any reference herein to Intel LANProtect encompasses both the Intel LANDesk Virus Protect and the Intel LANProtect products. Moreover, the parties agree that the Intel LANDesk Virus Protect was a later version of the Intel LANProtect product. (See CRRPFF 1776; SRRPFF 1776.) Respondent asserted and the staff agreed that "there was substantial functional overlap between the two versions," while complainant argued that neither Intel product was capable of scanning for viruses at a gateway. (RBr at 86, n.37; SRRPFF 1777; see CRRPFF 1777.)

in this investigation (CBr at 95); that of the sources of information relating to the LANDesk references respondent relies on for its invalidity defense, RX-131 bears a publication date of 1997, after the filing date of the '600 patent; that RX-75 is dated 1995, but that respondent has failed to establish when in 1995 the document was published (CBr at 95-96); and that as to RX-76 and RX-77, both of which are dated 1992, respondent "has failed to produce any evidence that the references, in fact, describe the actual features or functions of the Intel systems, or that the documents are accurate." (CBr at 96.) Complainant further argued that the Intel systems are not designed to detect viruses in the transfer of data between networks; that the server of the Intel systems "refers to a file server in a client server group - not the 'server' claimed in the '600 patent" (CRBr at 96); that given that the files that the Intel systems scan for viruses reside at a file server, there is no virus detection being performed on data transfers between a first computer and a second computer nor a server electronically receiving data in said data transfer, as required by asserted claim 4 (CRBr at 98, 100); that there is no first computer, server and second computer as required by claim 4 unless, within the context of the Intel systems, the file server and second computer are considered one and the same (CBr at 99); and that "there is insufficient evidence that Intel LANProtect was capable of operating to transfer data between networks as the file server is only operating on a local area network interconnecting workstations on that LAN."[52] (CRBr at 101.)

The staff argued that Fortinet has failed to meet its burden of proving that the Intel LANProtect references anticipate any of the asserted claims of the '600 patent by clear and convincing evidence (SBr at 74); that "[i]n order for a prior art reference to read upon any of the

[52] LAN is an acronym for Local Area Network.

asserted claims of the '600 patent, the virus-scanner must reside at an intermediary hardware device stationed between the sending and receiving hardware devices" (Id.); that the evidence of record does not support Fortinet's argument that by mid-1995, that a file server with LANDesk installed performed antivirus scanning in data transfers between "two other computers" (SRBr at 14); and that the LANDesk file server does not constitute intermediary hardware between two other computers in a data transfer, but rather, is "at best, one of the endpoints." (SRBr at 15; see SBr at 74, citing RX-75 at TMI00015518 ("The passage does not readily suggest that the network could be infected with viruses transferred from outside of the network.").)

Claim 4 of the '600 patent claims "[a] computer implemented method for detecting viruses in data transfers between a first computer and a second computer..." where said method includes the steps of, inter alia, "receiving at a server a data transfer request including a destination address," "electronically receiving data at the server" and "transmitting the data from the server to the destination...." (JX-1, col. 12, lns. 43-57 (emphasis added).) As the plain meaning of the claim language indicates, the method comprises data transfers from a first computer to a second computer through a server. See C.R. Bard, Inc. v. M3 Sys., Inc., 157 F.3d 1340, 1350 (Fed. Cir. 1998). Accordingly, the method contemplates the use of three distinct computers or hardware devices, viz. a first computer, a server and a second computer, wherein the data is transferred from a first computer to a second computer via a server. (See Section VII.B., supra (finding claim term "server" encompasses both hardware and software).)

The Intel LANProtect documentation discloses that the LANProtect is a "100% server-based virus protection software product" that "continuously shields file servers from inbound and outbound virus activity."[53] (RX-76 at FHC00366.) Thus, LANProtect performs virus scanning operations on either: (1) files sent to the file server from a workstation or (2) files that are residing on the file server that are being transferred from said file server to a workstation. (See RX-76 at FHC00370 (distinguishing between network traffic originating outside the file server and network traffic originating at the file server); Chen, Tr. at 18[54]; JX-10 at 164;JX-15 at 325.) To this end, the LANProtect product documentation discloses that it "scan[s] all incoming and outgoing files from the server." (RX-76 at FHC003375 (emphasis added); see id. ("Rather than scanning the file server, the Real Time File Scan looks at files going into and/or out of the file server."); accord RX-77 at FHC003404.) While the LANProtect product scans file transfers originating from or ending at a file server, the method claimed in claim 4 of the '600 patent is a method for detecting viruses in data transfers between a first computer and a second computer via a server. At best, the LANProtect is capable of scanning transfers between a server and a first computer or vice versa. Accordingly, the administrative law judge finds that respondent has not established, by clear and convincing evidence, that the Intel LANProtect products anticipate asserted claim 4 because the LANProtect products do not employ a method for detecting viruses in data transfers between a first computer and second computer via a server. As asserted claims 7 and 8 of the '600 patent depend from independent claim 4, the administrative law judge further finds that respondent has failed to establish that the Intel LANProtect products anticipate said asserted claims 7 and 8.

[54] Chen testified that Trend Micro developed the LANProtect product on its own before it began cooperating with Intel to add additional features to the product. (JX-15 at 59-60.)

3. CyberSoft MpScan

Respondent argued that the MpScan is prior art under "at least" 35 U.S.C. § 102(b) because it was in public use and on sale in 1993, well over a year before the '600 patent application was filed; that the testimony of CyberSoft's founder Peter Radatti, as well as contemporaneous corroborating documentation, establish that Radatti demonstrated MpScan's antivirus functionality in 1993 at the "UNIX Expo" and that MpScan was "on sale" for the purposes of § 102(b) at the time of said 1993 UNIX Expo[55] (RRBr at 123, 127); and that the MpScan product anticipates claims 1, 3, 11-13 and 15 of the '600 patent (RBr at 90; see RBr at 103 (claim 1), 107 (claim 3), 118 (claim 11), 120 (claim 12), 121 (claim 15), 122 (claim 13).) Respondent further argued that the testimony of Radatti and Bishop, as well as the corroborating documents of record, establish that the MpScan product satisfies all the limitations of asserted claim 1 of the '600 patent (RBr at 103; RPFF 2457-81); that Bishop similarly testified that the MpScan product employed an SMTP proxy server and SMTP daemon in the virus scanning process (RBr at 107); and that the unrebutted testimony of Radatti and Bishop establish that the MpScan satisfies the limitations of claims 11 and 13. (RBr at 118-19, 122; see RRBr at 124-25 (arguing that MpScan also satisifies limitations of asserted claims 12 and 15).)

[55] In response to complainant's argument that the MpScan product does not constitute prior art under § 102(b), respondent argued that:

> Thus, whether actually sold or not, and whether actually ever used by a customer or not, MpScan was in public use and on sale before the 'critical date' for the '600 patent. Moreover and more fundamentally, Fortinet has asserted that MpScan constitutes prior art under 35 U.S.C. § 102(a) and 102(g). Neither of these statutes require an actual public use or sale.

(RRBr at 127 (emphasis added).)

Complainant argued that the CyberSoft MpScan does not anticipate asserted claims 1, 3, 11-13 and 15 of the '600 patent because the MpScan does not have any virus detection capabilities and instead was designed to block outgoing and incoming email messages based on whether the emails contained classified or confidential information (CBr at 118); that "none of the documents of record in this investigation describes MpScan as having the capability to scan for viruses" (CBr at 120; see CRBr at 119-20); and that respondent has offered insufficient evidence to corroborate Radatti's testimony that the MpScan had virus detection capability or that he publicly displayed the MpScan at a UNIX Expo in 1993 or 1994 (CBr at 119, 121; see CBr at 122-23) (arguing that evidence is insufficient to establish that MpScan practiced the limitations of claims 1 and 3); 124-27 (arguing no anticipation as to claims 11-13 and 15 based on, inter alia, inability of MpScan to detect viruses).) As to respondent's argument that the Cybersoft Virus Description Language (CVDL) supports MpScan's alleged virus-scanning capabilities, complainant argued that the evidence indicates that CVDL does not scan for viruses aside from its incorporation into another Cybersoft product, VFind, which product is separate from the asserted MpScan (CRBr at 117-18); that respondent has not established that Cybersoft's MpScan and VFind were ever linked, interfaced or "integrated into a single solution"(CRBr at 123; see id. at 118-19); and that Bishop's reliance on RX-26D, a marketing brochure for VFind, "pulls his analysis out of anticipation and into obviousness at best."

The staff argued that the CyberSoft MpScan was "an email security system that was intended to electronically detect and block outgoing classified or confidential material contained in emails" (SBr at 80); that "there is no evidence that MpScan was ever sold to anyone and, as a result, there is no evidence that any purchaser ever used MpScan for virus detection and removal" (SBr at 81); and that aside from the testimony of CyberSoft's principal Peter Radatti and respondent's expert Bishop, respondent has failed to provide any corroborating evidence that the MpScan practiced the virus scanning limitations of the asserted claims and therefore has failed to meet its burden of proving, by clear and convincing evidence, that the MpScan anticipates the asserted claims by clear and convincing evidence. (SRBr at 17.)

Peter Radatti is the owner and CEO of CyberSoft, Inc., a company that he founded in 1988. At the hearing, Radatti testified that CyberSoft's first software product was a product called VFind, which he described as an antivirus program that ran on UNIX systems. (Radatti, Tr. at 1269.) VFind, which Radatti personally developed, was designed to scan for viruses on UNIX systems. (RPFF 2410 (undisputed).) Radatti further testified that prior to September 12, 1993, CyberSoft developed the CyberSoft Virus Description Language (CVDL), which Radatti described as "a way of describing patterns." (Radatti, Tr. at 1290-91.) CyberSoft's product documentation for VFind indicates that "VFind includes the CVDL generic pattern matching language...." (RX-26D at F-CSI 00146.) While Radatti testified that VFind was capable of detecting viruses, it is undisputed that CVDL scans for patterns other than viruses and does not scan for viruses aside from its incorporation into VFind.[56] (CPFF 1854-55 (undisputed); see

[56] The CVDL Technical White Paper makes the following description about the relationship between CVDL and VFind:

> It was determined that since CVDL would be a language of general utility it could be used to scan for patterns other than viruses. CVDL can search for any pattern while VFind is performing a virus check. In this way, VFind with CVDL is capable of hitting two birds with one stone.

(RX-120 at F-CSI 00109.) RX-120 lays out the specifications for CVDL. (RPFF 2420 (undisputed).)

Radatti, Tr. at 1292-93.) As of 1993, CyberSoft also had a product known as MpScan, which Radatti described as a "[m]ail protocol scanner" and "a software program to scan e-mail [that could scan] for anything you wanted to look for, including viruses." (Tr. at 1295-96.) The MpScan product documentation indicates that MpScan "uses the very powerful, user tested, CVDL scanning language used in CyberSoft's VFind product." (RX-28K at F-CSI 00046.)

Radatti testified that in 1993, CyberSoft introduced Version 4 of VFind and MpScan at the UNIX Expo International (UNIX Expo) held from September 21-23, 1993. (Tr. at 1295.) The parties do not dispute that the UNIX Expo was an international computer conference, and was probably the largest trade show of its type on the East Coast, and perhaps in the United States as of 1993. (RPFF 2414 (undisputed).) Radatti testified that CyberSoft had a booth at the '93 UNIX Expo where CyberSoft exhibited MpScan and its antivirus functionality by demonstrating it on a computer. (Tr. at 1296-97.) Radatti further testified that CyberSoft was offering MpScan for sale at the '93 UNIX Expo and that CyberSoft again exhibited MpScan and its antivirus functionality at the '94 UNIX Expo. (Tr. at 1297.)

As to the MpScan's ability to scan incoming and outgoing email for viruses, Radatti testified that MpScan was used as a "gateway" in the CyberSoft laboratory in Conshohocken, PA prior to it's first showing at the '93 UNIX Expo. (Tr. at 1299.) Radatti further testified that the MpScan would scan incoming and outgoing email messages using a proxy program "which would have VFind scan the e-mail message" (Tr. at 1301); that at that time, MpScan was running on a computer that had a memory, a communications device such as a network connection and a microprocessor (Tr. at 1301-02); that for an incoming email being processed through MpScan, a daemon would accept email, which was then handed to a proxy program which would invoke the

VFind program to scan the message; that said message would either be quarantined or sent for delivery depending on whether a virus was detected (Tr. at 1303); that as of 1993 MpScan supported SMTP and had the ability to scan email text and attachments (Id. at 1304); and that MpScan had the ability to detect uuencoded email attachments, decode said attachments and store them in separate temporary files. (Id. at 1306-07.)

With respect to Radatti's testimony that CyberSoft exhibited at the '93 UNIX Expo, the record contains pages from the "Official Show Directory," which indicate that CyberSoft was an exhibitor at said '93 UNIX Expo. (RX-28E at F-CSI 00043-44.) The directory indicates that CyberSoft, at said '93 UNIX Expo, was "announcing or showing for the first time five new products" including "VFind Version 4 - More and better features" and "MpScan - E-mail document sensitivity scanner." (Id. at F-CSI 00044.) Pages from the "Official Show Directory" from the '94 UNIX Expo contain identical disclosures regarding CyberSoft and MpScan as compared to the '93 directory. (See RX-28B at F-CSI 00038.) However, aside from Radatti's scant testimonial recount as to what CyberSoft exhibited at the UNIX Expos, the record contains no evidence that corroborates Radatti's testimony regarding any demonstration of MpScan's capabilities or its antivirus functionality at either the '93 or '94 UNIX Expo. In fact, CyberSoft's "New Product Announcement" associated with the '93 UNIX Expo states that "MpScan helps the System Administrator or Information Security Officer electronically scan and block outgoing company classified email," but makes no reference to MpScan's alleged virus scanning or detection features. (RX-28F at F-CSI 00140.) Based on the foregoing, the administrative law judge finds that respondent has not established, by clear and convincing evidence, that the

CyberSoft exhibitions of MpScan at the '93 and '94 UNIX Expos constitute a public use under 35 U.S.C. § 102(b).

While the record also contains information relating to license fees of the MpScan on both a per mail server and an unlimited site license basis, the administrative law judge finds further that respondent has not established that CyberSoft or Radatti ever communicated said license terms to a third party for the purposes of establishing an offer for sale within the meaning of 35 U.S.C. § 102(b). (See RX-28F at F-CSI 00181; see also RX-28K at F-CSI 00046.) Even assuming that the MpScan product had been offered for sale in 1993, the administrative law judge finds that respondent has not established that the MpScan product practiced any limitation of asserted claims 1, 3, 11-13 and 15 of the '600 patent. No MpScan product or source code relating to the MpScan product has been offered into evidence. In addition, the vast majority of the MpScan documentation of record does not corroborate Radatti's testimony as to the functionality of the MpScan product or even indicate that the MpScan had virus scanning or detection capabilities. (See, e.g., RX-26B; RX-26I; RX-28F at F-CSI 00141.) While the MpScan documentation indicates that MpScan employed CVDL, it is undisputed that CVDL scans for patterns other than viruses and does not scan for viruses aside from its incorporation into VFind. (CPFF 1854-55 (undisputed).) Moreover, the CyberSoft documentation describes MpScan and VFind as separate products and makes no reference to their incorporation. (See RX-26B; see also RX-26A at F-CSI 00105-06.) Accordingly, the administrative law judge finds that respondent has not established, by clear and convincing evidence, that the MpScan anticipates asserted claims 1, 3, 11-13 and 15 of the '600 patent.

4. Cheswick

Respondent argued that the book Firewalls and Internet Security written by William Cheswick and Steven Bellovin and published in 1994 (Cheswick) is prior art under "at least" 35 U.S.C. §§ 102(a) and (b); and that said Cheswick reference anticipates asserted claims 1 and 3. (RBr at 91; see RBr at 102 (claim 1), 107 (claim 3); RRBr at 115-18.)

Complainant argued that respondent has failed to establish, by clear and convincing evidence, that Cheswick provides an enabling disclosure as to each limitation of asserted claims 1 and 3 of the '600 patent and therefore, has failed to establish that Cheswick anticipates claims 1 and 3 (CBr at 110); that Bishop, while testifying that Cheswick disclosed the limitations of the preamble of claim 1, also testified that "the firewalls taught by Cheswick do not teach using the firewall in conjunction with virus scanning" (CBr at 111); and that respondent concedes that Cheswick does not disclose in detail how the virus-scanning would be implemented. (CRBr at 108.)

As to the Cheswick reference, the staff argued that the book contains nothing more than a "passing suggestion" to antivirus functionality in the context of an application-level gateway "in stark contrast to the eight columns of the '600 patent specification devoted to enabling the preferred embodiment" (SBr at 77); and that accordingly, respondent has failed to establish that Cheswick, alone or in combination with other references, invalidates the asserted claims of the '600 patent. (Id.)

Cheswick's sole disclosure relating to antivirus functionality, which appears within its discussion of Application-Level Gateways and their use to "prevent theft of valuable company programs and data," states the following:

> 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.

(RX-34 at FHC004774.) Thereafter, Cheswick "note[s] that the mechanisms just described are intended to guard against attack from the outside." (Id.) In response to the staff and complainant's argument that Cheswick does not provide a sufficiently enabling description of the virus detection and removal limitations of asserted claims 1 and 3, respondent relied on the following testimony of its expert Bishop:

> Q. Did the Cheswick book describe, in detail, how virus scanning might be implemented?
>
> A. No, it did not.
>
> Q. Do you have any opinion what that is?
>
> A. Because at the time it was very, very well-known. The book was about firewalls, and there was no particular reason to go into scanning for viruses when people knew how to do it.

(Bishop, Tr. at 1960 (emphasis added).) Bishop, however, provided no corroborating documentation. Aside from Cheswick's failure to disclose methods for implementing virus scanning techniques, which respondent admits, Cheswick also fails to disclose a system for detecting and selectively removing viruses in data transfers that includes each and every limitation relating to virus detection and removal as required in asserted claim 1 and its dependent claim 3. (See, e.g., JX-1 at col. 11, ln. 66 to col. 12, ln. 2 ("memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus"); col. 12, lns. 18-22 (the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses").) Based on the foregoing, the administrative law judge finds that respondent has not established, by clear and convincing evidence, that Cheswick anticipates asserted claims 1 and 3 of the '600 patent under 35 U.S.C. § 102(a) or § 102(b).

5. SMG

Respondent argued that the Secure Network Server Mail Guard (SMG) developed by Secure Computing Corporation constitutes prior art under "at least" 35 U.S.C. §§ 102(a) and (g) because the SMG product was known and reduced to practice no later than 1994; and that the SMG reference anticipates claim 1, 3, 4, 7 and 13. (RBr at 92; see RBr at 104, 107, 112, 115, 123; RRBr at 111-14.)

Complainant argued that respondent has failed to satisfy its burden that the SMG reference anticipates any asserted claims of the '600 patent by relying solely on a "single ten-page high-level marketing document (RX-23) as allegedly representing the SMG product," without any other technical documentation, user manuals, source code or actual product to establish the SMG's features or functionality (CBr at 103); that respondent has failed to establish that the SMG product practiced any of the limitations specific to asserted claims 1, 3, 4, 7 and 13 (CBr at 103-08; CRBr at 104-07); and that "there is no evidence of record that the SMG product ever incorporated virus scanning of email." (CBr at 103; see CRBr at 103.)

The staff argued that the SMG reference was "an intra-company email filtering system that allowed workstations with a certain security classification to send email to users at a workstation with a different security classification" (SBr at 79); that the SMG documents describing its functionality "are clearly focused on describing how SMG secures email traffic among multi-level classifications through the use of filters" (SBr at 79; SRBr at 15); that as for the two mentions of viruses in the SMG documentation of record, it is unclear whether the disclosure relates to an "across-the-board" blocking of binary files or a "more selective processing of binary files based upon an actual virus scan (that is not further described)" (SRBr at 16); and that without any source code, additional documentation or testimony from someone responsible for the development of the SMG product, respondent has failed to establish, by clear and convincing evidence, that the SMG system, alone or in combination, invalidates any asserted claims of the '600 patent. (SBr at 80; SRBr at 17.)

Respondent's expert Bishop testified that he relied on RX-23 in forming his opinion that the SMG reference anticipates asserted claims 1, 3, 4, 7 and 13 of the '600 patent. (See Bishop, Tr. at 2040; see also Tr. at 2041-49.) RX-23 is a document entitled "Constructing a High Assurance Mail Guard" dated 1994 and contains the following disclosure relating to the SMG reference:

> The SNS Mail Guard (SMG) provides a highly trustworthy device for transferring electronic mail between networks of differing security levels in accordance with site specific policies.
>
> * * *
>
> The first phase of SNS has produced the SNS Mail Guard (SMG), a device capable of controlled reclassification of electronic mail (e-mail). The SMG connects to local networks that use the Internet protocol suite and the Simple Mail Transfer Protocol (SMTP). Users on such networks operating at different security levels can use the SMG to exchange e-mail in a controlled fashion (Figure 1.)
>
> * * *
>
> If a classified user composes an unclassified message, there must be a special facility to reliably release the unclassified information to the unclassified network. This facility must be highly trustworthy to prevent the wrong information from flowing between the networks. This is the purpose of the high assurance SMG.

(RX-23 at FHC 003295.) With respect to the alleged virus detection and removal features of the SMG reference, RX-23 discloses the following:

> Attachment file types. The filter searches the message for attached files in a variety of application specific formats. Each attached file must be of a type that is

> permitted to traverse the SMG. A site can use this facility to block the accidental importation of executable binary files that may contain virus software.
>
> * * *
>
> The message transfer agents are not allowed to read messages across the boundary between security levels in either direction. This forces all reclassification to go through filters, where virus checks on incoming executable files and other such activities may occur.

(RX-23 at FHC 003296, 003298 (emphasis added).) While the aforementioned disclosures reference "virus checks," the administrative law judge finds that such disclosure does not sufficiently corroborate Bishop's testimony that the SMG reference satisfies each and every limitation of asserted claims 1, 3, 4, 7 and 13. Rather he finds that said disclosures merely indicate that SMG may have been able to block or detect viruses, although said disclosures are not supported or further explained by any other evidence of record, including testimony from one of ordinary skill in the art who participated in the development of SMG. Moreover, Bishop did not review any SMG source code, user manuals or other technical documentation discussing the alleged virus detection capabilities of the SMG reference and did not have an actual SMG product to inspect for his validity analysis. Accordingly, the administrative law judge finds that respondent has failed to establish, by clear and convincing evidence that the SMG reference anticipates asserted claims 1, 3, 4, 7 and 13 of the '600 patent under either 35 U.S.C. §§ 102(a) or 102(g).

B. 35 U.S.C. Section 103

Respondent argued that the Norman Firewall renders claim 14 of the '600 patent obvious. (RBr at 86, 121; see RBr at 118.) Respondent also argued that the CyberSoft MpScan prior art reference renders claim 14 obvious. (RBr at 90, 121.) Respondent further argued that the Cheswick reference, "in combination with commercially available antivirus software such as

Trend Micro's PC Rx product," renders obvious asserted claims 4, 7, 8 and 11-15 of the '600 patent. (RBr at 91; see RBr at 112, 119, 120, 121.) In addition respondent argued that the SMG product renders obvious claims 8, 11-12 and 14-15. (RBr at 92; see RBr at 120, 121); that a Sidewinder product coupled with "the teachings of Mr. Boebert's 'Sidewinder and Virus Scans' postings" render each of the asserted claims of the '600 patent obvious (RBr at 93-94; see RBr at 105, 113, 120, 121, 124); that a person of ordinary skill in the art "naturally would have combined the collective teachings of SMG, Sidewinder and Boebert's 'Sidewinder and Viruses Scans' postings," thereby rendering claim 1 obvious (RBr at 106); that a Trusted Information Systems Firewall Toolkit (TIS) anticipates or renders obvious claims 1 and 3 of the '600 patent; that in combination with commercially available antivirus software, such as Trend Micro's Rx software, TIS renders obvious the remaining asserted claims of the '600 patent (RBr at 95-96; see RBr at 106, 114, 125); and that while a Gelb Firewall does not itself render the claims of the '600 patent invalid "it helps demonstrate the obviousness of all the asserted claims by showing the ease with which anti-virus software could be added to a network firewall in the 1992-94 time frame." (RBr at 97.)

Each of complainant and the staff has argued that the asserted claims are not invalid under 35 U.S.C. § 103.

Obviousness under 35 U.S.C. § 103 is evaluated under the so-called Graham factors: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims at issue; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness. Graham v. John Deere Co., 383 U.S. 1, 17 (1966). When combining references in an attempt to show obviousness, the accused infringer must make "a showing of a suggestion, teaching, or motivation to combine the prior art references." Brown & Williamson Tobacco Corp. v. Philip Morris Inc., 229 F.3d 1120, 1124-25 (Fed. Cir. 2000).

To prove obviousness, Fortinet must establish that "there is a reason, suggestion, or motivation in the prior art that would lead one of ordinary skill in the art to combine the references, and that would also suggest a reasonable likelihood of success." Smiths Indus. Medical Sys., Inc. v. Vital Signs, Inc., 183 F.3d 1347, 1356 (Fed. Cir. 1999) (emphasis added); see also United States Surgical Corp. v. Ethicon, Inc., 103 F.3d 1554, 1564 (Fed. Cir. 1997). The references in combination "must suggest the invention as a whole." In the Matter of Certain ERPROM, EEPROM, Flash Memory, and Flash Microcontroller Semiconductor Devices and Products Containing Same, Inv. No. 337-TA-395, ID at 87 (Mar. 19, 1998) (U.S.I.T.C. Pub. No. 3392). In the absence of a suggestion to combine references, "one can do no more than piece the invention together using the patented invention as a template; such hindsight reasoning is impermissible." Id. at 140-41 (citations omitted). Furthermore, the Federal Circuit has held that not only must a motivation to combine the references exist but the motivation must be directed toward combining prior art references in the particular manner claimed. See In re Kotzab, 217 F.3d 1365, 1371 (Fed. Cir. 2000); In re Rouffet, 149 F.3d 1350, 1357 (Fed. Cir. 1998). The patent challenger "must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the invention, would select elements from the cited prior art references for combination in the manner claimed." Rouffet, 149 F.3d at 1357 (emphasis added).

The administrative law judge finds that Fortient has failed to provided any motivation for combining any of the prior art references, in the manner claimed, which it cited in its obviousness analysis. Moreover, the administrative law judge finds that the added art does not cure the deficiencies set forth supra with respect to the Norman Firewall, CyberSoft, MpScan, Cheswick and SMG references.

As for the Sidewinder reference, Fortinet concedes that the reference, which was an application-layer gateway, did not possess antivirus functionality. (Bishop, Tr. at 2054.) Fortinet, however, relies upon a series of email exchanges discussing firewalls to support its argument that to add antivirus functionality to Sidewinder would have been obvious. (RX-112, at 112A, 112B.) The emails in question are between one of the chief architects of Sidewinder, Earl Boebert, and Marcus Ranum, a pioneer in the field of firewalls and proxy servers. (Bishop, Tr. at 2054, 2119; see Avolio, Tr. at 1731 (crediting Ranum with inventing firewall proxy servers).) In the emails, the two debate the feasability of adding antivirus functionality to an application gateway such as Sidewinder. (RX-112, 112A-B.) While Boebert argues that such an integration would be straightforward, Ranum disputes Boebert's claim. (Id.) Fortinet's expert witness Bishop, asserts that Boebert provides sufficient detail in the emails as to how to integrate antivirus scanning into Sidewinder. (Bishop, Tr. at 2059.) However, it is clear that Boebert was unable to convince, Ranum, an expert in the field at the time, that it could be done. (See Bishop Tr. at 2119[57]; RX-112 at 112A, 112B.)

The cited TIS Firewall (and its commercial embodiment called Gauntlet) was a firewall that existed prior to 1995. The TIS Firewall looked for a pipe symbol ("|") in an email header that itself was a vulnerability exploited by the Morris Internet Worm. (Avolio, Tr. at 1745-48,

[57] Bishop stated that he thought Ranum's skepticism was actually based on a mistaken belief by Ranum that Boebert was claiming that all viruses could be detected. (Bishop, Tr. at 2128.) However, the administrative law judge finds nothing in Boebert's comments to suggest that he was proposing a method of virus-filtering that would catch all viruses.

1779; RX-117 at 148606.) However, it was not until 1996 that Gauntlet contained anti-virus functionality. (Avolio, Tr. at 1782-83.) The administrative law judge finds that the evidence further shows that implementing the few lines of software code needed to spot the pipe symbol (and reject an email on that basis) is a different undertaking than integrating a true antivirus scanner into an intermediary device as claimed in the '600 patent. Thus, such a minor search did not involve the complexities of an actual virus scanner, such as the timing out of connections and throughput concerns. (See Mitchell, Tr. at 2202-03 (viruses involve scanning executable code rather than text and in doing so must identify much more complicated patterns than identifying a single text character or text string requires).)

Referring to the Gelb Firewall, Gelb indicated that the antivirus software he used had nothing to do with the gateway:

{

}

(JX-17C at 126 (emphasis added).) Gelb also verified that his firewall did not send any data to be scanned for viruses, testifying that:

{

}

(JX-17C at 127.) Moreover, Gelb also indicated that the anti-virus software used in his system was loaded only on the file server and was initiated only via some type of user intervention. Thus, Gelb explained:

{

}

(JX-17C at 183-84 (emphasis added).){

} (JX-17C at 217.) None of the parties have asserted that the claims of the '600 patent have any thing remotely to do with antivirus software that is only initiated by user intervention.

In addition to the deficiencies in the art relied on for invalidity under 35 U.S.C. § 103, there is evidence of objective indicia of nonboviousness. For example in 1996, Trend Micro's InterScan product scanned for viruses at the gateway. (CX-1B.) InterScan checked e-mail, FTP transfers, web transfers, and compressed or encoded formats such as ZIP, UUENCODE, or MIME. (CX-1B). PC Week Magazine's August 1996 article, "This 'wall' has ears" reviewed InterScan E-mail VirusWall 1.5 for Windows NT as a product that eased corporate worries of the vulnerability of their networks' susceptibility to viruses. (CX-4.) In October, 1996, Windows NT Magazine announced the winners of its UNIX/Windows NT Technology awards which were presented at UNIX Expo in New York City. (CX-4A.) The awards were given to companies and products that were making a difference in the UNIX/Windows NT market. (CX-4A.) InterScan VirusWall received a Technical Excellence Award at that time. (CX-4A.) In December 1996, InterScan VirusWall 1.5 was considered to be one of "the most inexpensive way to guard your NT server against email attachment viruses." (CX-4B.) In December 1996, Windows NT Magazine reran the UNIX Expo award, indicating that Trend Micro's InterScan VirusWall 1.5 won for "overall technical excellence." (CX-1D.) It states that the "great challenge to virus detection is finding viruses before the can do damage"and that Trend Micro's product addressed this problem by scanning data streams as they are delivered over the network. (CX-1D.) Also, syndicated columnist Dr. Keith Orlando Hilton selected InterScan VirusWall as one of the top 25 computer products in 1996. (CX-1.) In addition, Internet and Java Advisor's "Net Watch" for January 1997 included InterScan VirusWall 2.0 on its list of recognized security tools. (CX-14 at TMI00001969.) InterScan VirusWall was featured in InfoWorld Canada magazine in March, 1997 as a product for protecting NT servers. (CX-4J.) In March 1997, InterScan VirusWall beat out McAfee's product to win the Editor's Choice Award. (CX-297; see CX-3.) The April 1997 PC Magazine Editor's Choice award article cited InterScan VirusWall's ease of installation and management, among other features. (CX-3 at TMI00002236; CX-297 at TMI00005888.) The magazine found that InterScan VirusWall was the only product among McAfee's, Integralis' and Trend Micro's that automatically updated virus signature patterns, and that allowed users to conveniently clean viruses from infected data. (CX-3 at TMI00002236; CX-297 at TMI00005888.) InterScan VirusWall received the SMAU Industrial Design Award, too. (CX-297 at TMI00005888.) In 1997, InterScan VirusWall was further featured in PC Magazine On-Line in connection with its Editor's Choice award. (CX-4D.) It was featured in PC Magazine's annual Utility Guide. (CX-4D; CX-4E; CX-4F; CX-4G.)

National Software Testing Laboratories (NSTL) is the leading independent hardware and software testing organization in the microcomputer industry. (CX-310C at 3.) NSTL declared Trend Micro the leader in virus protection for Internet traffic after final testing of competing products from Symantec, Integralis and McAfee. (CX-310C at 4.) NSTL found "Trend Micro's InterScan VirusWall outscored the other three products in all tested areas, providing significantly better performance, far better usability, and more features." (CX-310C at 3.) NSTL also found that InterScan VirusWall was the most powerful of the products tested: "Trend does not sacrifice usability for this power. The product combines the most intuitive interface with excellent documentation and a number of usability enhancements that clearly define InterScan as the leader of the four products tested for Internet virus protection." (CX-310C at 4.) InterScan VirusWall 3.1 earned Network Computing's Editor's Choice Award, "for its cutting-edge protection and for detecting more viruses than any other product." (CX-423C at TMI00014700.) In December

1996, Trend Micro supported InterScan VirusWall for HP-UX, the first virus protection available for Hewlett Packard's enterprise-class Unix operating system. (CX-361 at 1.)

As for licensing, a litigation between Trend Micro and Integralis was resolved through a settlement that resulted in a license to the '600 patent. (JX-012C at 21.) A litigation between Trend Micro and Sybari also was resolved through a settlement by which Sybari made payments to Trend Micro and Sybari took a license to the '600 patent. (JX-012C at 21.) Trend and Intel had an ongoing licensing and co-development effort that dates back to 1991. (JX-012C at 51.) A March 31, 1998 Intel-Trend Micro Development and License agreement specifically covers, among other things, the '600 patent. (JX-012C at 49, 52; CX-312 at 3, ¶ 8.) It was during the course of drafting said March 1998 license that Intel sought a license to the '600 patent and that request came "out of the blue." (JX-012C at 52-54.) Moreover, the provision is a very specific, stand-alone paragraph in the 1998 agreement. (JX-012C at 54, CX-312 at 3, ¶ 8.) Intel indicated that it was interested in obtaining a license for the '600 patent solely because they thought that one day Intel might want to go into the business of selling Internet Gateway scanning technology. (JX-012C at 54.) The patent license fee for the '600 patent was a{ } (CX-312 at 3, ¶ 7.3.)

An IBM-Trend Micro license agreement is a broad cross-license through which Trend Micro received a license to "all of IBM's" patents. (JX-012C at 56; CX-534 at 2.) In exchange, IBM received a license to all of Trend Micro's patents, which at the time was probably one or two, with respect to anti-virus technology. (JX-012C at 56-57; CX-534 at 2.) IBM had approached Trend Micro for the license. (JX-012C at 56.) The IBM-Trend Micro license is dated December, 1, 1997. (CX-534 at 1.) The December 1997 Agreement between IBM and Trend

Micro included at least ten issued or pending Trend Micro patents including the '600 patent which was at the time the subject of lawsuits between Trend Micro and Network Associates, and Symantec Corporation. (CX-534C at 13). Included in the License Agreement is IBM's worldwide portfolio as it relates to computer anti-virus products. (CX-534C at 13.) Trend Micro licensed the '600 patent to Check Point, particularly in connection with the sale of Check Point's firewall. (JX-012C at 59; CX-435 at 1.) However, the agreement between Check Point and Trend Micro did not require{ }for a worldwide license to the '600 patent. (CX-435C (Cooperative Development and Marketing Agreement and Patent License Agreement between Check Point and Trend Micro).) Integralis is also a licensee under the '600 patent. (JX-012C at 67; CX-433 at 1.) That license resulted from the litigation with Trend Micro. (JX-012C at 67.) The license agreement was a cross-license under which Trend Micro received the license to some of Integralis' technology. (JX-012C at 68; CX-433 at 2.) Trend Micro entered into the Integralis license on January 1, 1998. (JX-012C at 68; CX-433 at 1.)

Sybari has a license to the '600 patent. (JX-012C at 70; CX-307 at 1-3.) The license with Sybari resulted from litigation. (JX-012C at 70; CX-307 at 1, 4.) Under said license agreement, Sybari received the right to practice the '600 patent. (JX-012C at 70; CX-307 at 3.) One benefit that Trend Micro received from entering into that license was that it resolved the litigation which Sybari had initiated against Trend Micro. (JX-012C at 70; CX-307 at 1, 4.) Under the terms of the Sybari license, Sybari also paid Trend Micro{ } (JX-012C at 71; CX-307 at 4.)

Symantec is also a licensee under the '600 patent. (JX-012C at 72, CX-434 at 1, 2 and 9.) Symantec was a defendant in the NAI litigation. (JX-012C at 72, CX-434 at 1 and 6.) The license agreement between Trend Micro and Symantec, a result of that litigation, is a cross-license of both companies' complete portfolios of patents,{

}(JX-012C at 72-73; CX-434 at 1, 2, 6 and 9.) Essentially, it was an agreement to let each party continue to go out and compete and not run afoul of each other's patents relating to antivirus technology. (JX-012C at 73.) Symantec and Trend Micro also agreed to do was share virus samples which had been done informally in the past. (JX-012C at 73; CX-434 at 13.) { } (JX-012C at 74; CX-434 at 10.) The Symantec and Trend Micro agreement also included a provision that{

} The Symantec agreement was dated April 6, 1998. (JX-012C at 75; CX-434 at 1, 6.) Network Associates is a licensee under the '600 patent. (JX-012C at 76.)

The license agreement between Trend Micro and Network Associates resolved the NAI litigation between the parties. (JX-012C at 76.) The license agreement between Trend Micro and Network Associates was a portfolio cross-license between the two companies, and{

} including the '600 patent and{

} (JX-012C at 76.) In addition to the cross-license, Network Associates{ }(JX-012C at 77.) The Network Associates-Trend Micro license agreement was entered into in 2000. (JX-012C at 77.) {

}(JX-012C at 77.)

Worldtalk is a licensee of the '600 patent. (JX-012C at 78; CX-432 at 2.) {

} (JX-012C at 78.) Worldtalk's product was complimentary to what

Trend Micro was doing and what they created was a convenient place to scan for viruses and messages and attachments that flowed between companies. (JX-012C at 78.) There was a{ } between the parties whereby{ } (JX-012C at 79; CX-432 at 3.) Worldtalk and Trend Micro entered in this agreement on April 24, 1997. (CX-432 at 1.) Internet Dynamics had an agreement with Trend Micro that was similar to that between Trend Micro and Worldtalk. (JX-012C at 81.) Under the terms of the Internet Dynamics-Trend Micro agreement, Internet Dynamics was able to sell Trend Micro's products along with Internet Dynamic's products, and{ } (JX-012C at 81, CX-309 at 1-2.) { } Internet Dynamics made{ } (JX-012C at 81; CX-309 at 11.) An agreement between Trend Micro and Infonet was somewhat like the agreements with Worldtalk and Internet Dynamics,{ } (JX-012C at 83; CX-425 at 1, 3.)

With respect to revenue for Trend Micro for fiscal year 2001, third-party product revenue for Trend Micro products totaled{ } (CX-566C at TMI00177177.) For fiscal year 2002, the third-party revenue totaled{ } (Id.) For fiscal year 2003, the total product revenue from third-parties amounted to{ } (Id.) For fiscal year 2004 up to March 31, 2004, the total third-party product revenue amounted to{ }(Id.)

Based on the foregoing the administrative law judge finds that respondent has not established by clear and convincing evidence that asserted claims 4, 7, 8 and 11 to 15 are obvious under 35 U.S.C. §103.

C. Enablement

Respondent argued that the '600 patent contains "significant" errors and omissions in the written description. In support it argued that the '600 patent does not explain how to configure the FTP proxy server, that modifications to the FTP server necessary to practice the invention of the '600 patent are not disclosed in the '600 patent; that while the '600 patent describes redefining the bind function in a shared library that is part of the operating system, the '600 patent has no description as to how to do so; that the specific commands necessary for the functioning of the daemons and servers in the '600 patent are not disclosed; and that the Figure 6B of the '600 patent fails to disclose the connections necessary to perform an outbound file transfer using FTP. (RBr at 127-128.)

Complainant argued that the '600 patent enables one of ordinary skill in the art to make and use the claimed invention. (CBr at 69-75.) The staff argued that Fortinet has not satisfied its heavy burden in establishing that the '600 patent is invalid for lack of enablement. (SBr at 84.)

With respect to the enablement requirement, 35 U.S.C. §112 states:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it contains, or with which it is most nearly connected, to make and use the same....

35 U.S.C. § 112, ¶ 1. Enablement is a legal determination of "whether a patent enables one skilled in the art to make and use the claimed invention, ... is not precluded even if some experimentation is necessary, although the amount of experimentation needed must not be unduly extensive, ... and is determined as of the filing date of the patent application...." Hybritech Incorp. v. Monoclonal Antibodies, Inc., 802 F.2d 1367, 1384 (Fed. Cir. 1986) (citations omitted); see Bristol-Myers Squibb Co. v. Rhone-Poulenc Rorer, Inc., 326 F.3d 1226, 1234 (Fed. Cir.

2003) ("enablement involves an assessment of whether a patent disclosure would have enabled one of ordinary skill in the art at the time the application was filed to make and use the claimed invention"). To prove invalidity due to lack of an enabling disclosure, a party must demonstrate, by clear and convincing evidence, that a person of ordinary skill in the art would be unable to practice the claimed invention without undue experimentation. Koito Mfg. Co. v. Turn-Key-Tech, LLC, 381 F.3d 1142, 1155 (Fed. Cir. 2004); Nat'l Recovery Techs. v. Magnetic Separation Sys., Inc., 166 F.3d 1190, 1195 (Fed. Cir. 1999).

The administrative law judge has found that the claimed invention uses conventional operating systems and that a person of ordinary skill in the art should have knowledge of various virus detection methods. Hence, he found in Section VI., supra, that such a person should have certain qualifications. The administrative law judge finds that the record establishes that at the time the application for the '600 patent was filed there existed substantial prior art explaining the general subject matter that Fortinet alleges is lacking in the '600 patent specification. For example, the Internet daemon for UNIX, inetd, was well known in the prior art and was the subject of many articles. (See, e.g., RX-34 at FHC004781-82.) Furthermore, configuring an application-gateway to process FTP transfers was described in the landmark book Firewalls and Internet Security by Cheswick and Bellovin (1994), which was well-known at the time of the '600 patent invention. (Bishop, Tr. at 1956-57; RX-34; see also SX-9.) Thus the administrative law judge finds that respondent has not established, by clear and convincing evidence, that the '600 patent lacks enablement in view of the necessary qualifications of a person of ordinary skill in the pertinent art and the published literature at the time the application for the '600 patent was filed.

D. Best Mode

Respondent argued that the inventors on the '600 patent did not meet their obligations to disclose the best mode of the '600 patent. (RBr at 129-131.) Complainant argued that the '600 patent complies with the best mode requirement. (CBr at 75-77.) The staff argued that the evidence fails to satisfy Fortinet's burden of showing a violation of the best mode requirement. (SBr at 81-83.)

A patentee must disclose in the specification his or her best mode contemplated for practicing the invention. See 35 U.S.C. §112, ¶1. The best mode requirement "creates a statutory bargained-for exchange by which a patentee obtains the right to exclude others from practicing the claimed invention for a certain time period, and the public receives knowledge of the preferred embodiments for practicing the claimed invention." Teleflex v. Ficosa N.A. Corp., 299 F.3d 1313, 1330 (Fed. Cir. 2002), citing Eli Lilly & Co. v. Barr Labs., Inc., 251 F.3d 955, 963 (Fed. Cir. 2001). To prove that a patent is invalid for failure to disclose the best mode, a respondent must establish, by clear and convincing evidence, that at the time the patent application was filed an inventor knew of yet concealed a better mode for carrying out the claimed invention than what is disclosed in the specification. Teleflex, 299 F.3d at 1330.

Determining whether a patentee satisfied the best mode requirement is a two-pronged inquiry. Teleflex, 299 F.3d at 1330; see Bayer AG v. Schein Pharmaceuticals, 301 F.3d 1306, 1320 (Fed. Cir. 2002). The first prong is subjective, focusing on the inventor's state of mind at the time the application was filed and considers whether the inventor then possessed a best mode for practicing the invention. Teleflex, 299 F.3d at 1330; Bayer, 301 F.3d at 1320, quoting Eli Lilly & Co., 251 F.3d at 963. The second prong is objective and considers whether the inventor adequately disclosed his best mode, which is dependent on the scope of the invention and the level of skill in the art. Bayer, 301 F.3d at 1320, quoting N. Telecom Ltd v. Samsung Elec. Co., 215 F.3d 1281, 1286 (Fed. Cir. 2000). The Federal Circuit has cautioned that an "analysis of compliance with the best mode requirement must begin and remain focused on the language of the claim." Teleflex, 299 F.3d at 1329-30 (emphasis added); see Bayer, 301 F.3d at 1319 (concluding that Federal Circuit precedent finding best mode violation centers on a failure to disclose a preference for carrying out the claimed invention).

Respondent, to meet its burden, argued that the inventors of the '600 patent did not meet their obligations to disclose the best mode of the '600 patent because they began discussing{

} (RBr at 129-31.) It is argued that the named inventors of the '600 patent{

} (RRBr at 136-37.)

The administrative law judge finds that the record does not establish, prior to the September 26, 1995 filing date of the '600 patent, that the inventors knew that to improve performance, processes should be altered such that the processes would be waiting before a connection was initiated. Thus, inventor Chen testified:

Q. Would it be fair to say that in the view of you{

}

A. {

}

Q. { }

A. {

}

(JX-15 at TM100092139 (emphasis added).) Hence, the record indicates that{

} Significantly,{

} which was after the filing date of the patent in issue. Thus, Chen testified:

Q. Do you know at what stage of the InterScan product planning this document [Exhibit 507] represents?

A. {

}

Q. {

}

A. {

}

Q. { }

A. Yes.

Q. { }

A. Yes.

Q. { }

A. Yes.

(JX-15 at TMI00091316-17 (emphasis added).)

Based on the foregoing, the administrative law judge finds that respondent has not established, by clear and convincing evidence, that the inventors on the patent application for the '600 patent, which was filed on September 26, 1995, at that time knew of and yet concealed a better mode for carrying out the claimed invention.

E. Indefiniteness

Respondent argued that the '600 patent fails for indefiniteness due to an "irreconcilable conflict in its varying usages of the term server throughout the specification and the claims of the patent." (RBr at 131-32.)

Complainant argued that Fortinet's argument is nonsensical at its core; that software runs on hardware and, similarly, hardware serves no function without software; that as properly construed, the claimed "server" is "a computer system that performs specified functions for other computers (which are called "clients"), or separately [refers] to the software running on a computer system that performs such server functions," and thus, the term "server" specifically encompasses both software and hardware solutions. (CBr at 78.)

The staff argued:

> While there is a general rule that a term means the same thing within a single patent claim, it is only a general rule, and a term can have a different meaning if it appears reasonable in the context of the specification. More importantly, the term is not construed inconsistently; the specification instructs one skilled in the art that "server" may be implemented in either hardware or software or a combination thereof. Indeed, as Trend Micro points out, Fortinet's expert witness, Dr. Bishop, was clearly able to interpret the claims for purposes of his invalidity analysis.

(SRBr at 36.)

The administrative law judge has found that the proper construction of the claimed term "server" is either a computer and/or software that performs service for other computers or programs. Thus, the claimed word server can be identified with either software and/or hardware and such would be understood by a person of ordinary skill in the art. See Section VI., supra. Hence, he finds that respondent has not established, by clear and convincing evidence, that the '600 patent is invalid because of any indefiniteness in the use of the word "server."

XI. Enforceability

Respondent argued that the '600 patent is unenforceable due to inequiteable conduct by the inventors. In support, it is argued that the inventors were aware of and failed to disclose the Intel LANProtect product to the Patent Office. (RBr at 133-37.)

Complainant argued that Fortinet's inequitable conduct allegations fails as a matter of law because the alleged failure to disclose the Intel products was not material and there is not a scintilla of evidence to suggest an intent to deceive the Patent Office. (CBr at 138-42.)

The staff argued that Fortinet did not meet its burden of establishing, by clear and convincing evidence, that the inventors withheld any reference in order to deceive or mislead the Examiner. (SBr at 76.)

To establish unenforceability due to inequitable conduct, a respondent must prove, by clear and convincing evidence, that a patentee failed to disclose material information during prosecution of the patent with an intent to mislead the PTO. Bristol-Myers Squibb Co. v. Rhone-Poulenc Rorer, Inc., 326 F.3d 1226, 1233 (Fed. Cir. 2003). Within the context of an inequitable conduct analysis, "[i]nformation is deemed material if there is a substantial likelihood that a reasonable examiner would consider it important in deciding whether to allow the application to issue as a part." Brasseler, U.S.A. I,L.P. v. Stryker Sales Corp., 267 F.3d 1370, 1380 (Fed. Cir. 2001); accord Baxter Int'l Inc. v. McGaw, Inc. 149 F.3d 1321, 1327, (Fed. Cir. 1998). A withheld reference may be "highly material" and "[g]enerally, when withheld information is highly material, a lower showing of deceptive intent will be sufficient to establish inequitable conduct." Certain Ammonium Octamolybdate Isomers, Inv. No. 337-TA-4377, U.S.I.T.C. Pub. No. 3668, Comm'n Op. at 48 (January 2004) (emphasis added) (Ammonium), citing GFI, Inc. v. Franklin Corp., 265 F.3d 1268, 1273 (Fed. Cir. 2001); Critikon, Inc. v. Becton Dickinson Vascular Access, Inc., 120 F.3d 1253, 1256 (Fed. Cir. 1997) "In a case involving an omission of a material reference to the PTO, there must be clear and convincing evidence that the applicant made a deliberate decision to withhold a known material reference." Baxter Int'l, Inc., 149 F.3d at 1329, citing Molins PLC v Textron, Inc., 48 F.3d 1172, 1181 (Fed. Cir. 1995).

This administrative law judge recently found that inventors of a '928 patent committed inequitable conduct in withholding highly material prior art from the Patent Office with an intent to deceive. See Certain Audio Digital-To-Analog Converters And Products Containing Same Inv. No. 337-TA-499, ID at 47-48 (November 15, 2004). The Commission, in its notice filed December 30, 2004, did not review said finding. The administrative law judge finds the underlying facts in Inv. No. 337-TA-499 in stark contrast to the underlying facts in this investigation. Thus, while he found the withheld art highly material in Inv. No. 337-TA-499, he has found, supra, that, at best, the Intel LANProtect was capable of scanning transfers between a server and a first computer or vice versa; and that the LANProtect products do not anticipate asserted claim 4 because the LANProtect products do not employ a method for detecting viruses in data transfers between a first computer and second computer via a server. Moreover, in Inv. No. 337-TA-499, the inventor considered the withheld art "competitive" with what was being claimed. See ID at 35. In this investigation, inventor Chen testified:

{

}

(JX-10C at 97 (emphasis added).) Also, Intel has a license on the '600 patent. See Section X.B., supra.

Based on the foregoing, the administrative law judge finds that respondent has not established, by clear and convincing evidence, that the Intel LANProtect product was material to what is claimed in the '600 patent. Moreover, he finds that respondent has not established that the inventors of the '600 patent made a deliberate decision to withhold the Intel LANProtect product from the Patent Office. Hence he finds that respondent has not established, by clear and convincing evidence, that the '600 patent is unenforceable.

XII. Remedy

The Commission has broad discretion in selecting the form, scope and extent of the remedy in section 337 proceedings. Integrated Circuit Telecommunication Chips, Inv. No. 337-TA-337, Comm'n Op. (August 3, 1993), citing Viscofan, S.A. v. U.S. Int'l Trade Comm'n, 787 F.2d 544, 548 (Fed. Cir. 1986). An exclusion order can exclude from importation goods and products that directly or contributorily infringe the patented technology. In the Matter of Certain Hardware Logic Emulation Systems & Compnents Thereof, Inv. No. 337-TA-383, USITC Pub. 3089, Comm'n Op. at 27 (March 1998) (Hardware Logic). Direct infringement does not have to precede importation for an exclusion order to reach components that contribute to the infringement of a patent-in-issue. Hardware Logic, Comm'n Op. at 19-20. In Certain Personal Computers & Components Thereof, Inv. No. 337-TA-140, USITC Pub. No. 1504 (March 1984), the Commission excluded from entry into the United States personal computers and components thereof "which are less than complete when imported but [which] are designed and intended to be employed by their owner, importer, consignee or agent of either to make a personal computer which directly infringes any of the [patents-in-suit]."

The Commission also has the authority to issue cease and desist orders where a respondent has a sufficient inventory of infringing goods in the United States. See Certain Plastic Encapsulated Integrated Circuits, Inv. No. 337-TA-315, USITC Pub. 2574, Comm'n Op. at 37 (November 1992). A "sufficient inventory" may consist of one infringing product. See, e.g., Hardware Logic, Comm'n Op. at 26.

A cease and desist order can issue in lieu of or in addition to an exclusion order to prevent the sale, distribution or other use of infringing imported products in the United States. The scope of section 337 is broad enough to prevent every type and form of unfair practice, including the transmission of infringing software by electronic means, electronic transmission of software and/or data that induces an infringing use of an imported product and the servicing of imported products that induce infringement. Hardware Logic, Comm'n Op. at 25-29; Certain Digital Satellite Systems Receivers, Inv. No. 337-TA-392, USITC Pub. 3418, Initial Determination at 239-44 (Oct. 1997); id., Order No. 53 at 7-11 (June 9, 1997).

A. Exclusion Order

Complainant argued that it is entitled to a limited exclusion order which bars the importation of any of the accused products because they infringe asserted claims; that any exclusion order should bar Fortinet from importing source code electronically from Canada; and that the limited exclusion should also bar the importation of "other non-staple components that do not have substantial non-infringing uses, such as FortiASIC content processor." (CBr at 145-46.)

Respondent argued that if a violation is found, the scope of any limited exclusion order should be limited to those products and components found to have a "nexus" to infringement and should not prohibit electronic transmissions. With respect to electronic transmissions, respondent argued that in the past, the Commission has expressly declined to issue an exclusion order covering electronic transmissions to accommodate the views of Customs, citing Hardware Logic; that electronic transmissions are not contained in the Harmonized Tariff Schedule and do not enter the United States through ports of entry used by "articles"; and that as such, administration by Customs of an exclusion order covering electronic transmissions would be impossible. (RBr at 142.)

The staff did not agree that any exclusion order should cover the electronic transmission of software into the United States. It argued that in Hardware Logic (Comm'n Op. at 28) the Commission held that while the Commission has the legal authority to exclude electronic transmissions, such transmissions in the exclusion order would not be covered out of deference to U.S. Customs, which has determined not to regulate electronic transmissions, and because a cease and desist order could be issued that would cover these transmissions. Hence, the staff argued that the limited exclusion order should not cover electronic transmissions. (SBr at 87.)

The administrative law judge, in view of Hardware Logic, recommends that any limited exclusion order should bar the importation of any infringing FortiGate products including duplication of software that would result in infringement of the '600 patent when combined with other Fortinet components, but that any limited exclusion order should not bar the electronic transmissions of software into the United States. He also recommends that the limited exclusion order should not cover the distribution to current customers of software maintenance releases and updates to respondent's virus signature database in view of Hardware Logic which exempted the importation of spare parts to service the emulators already in the hands of respondents' customers. This recommendation is made on the ground that if respondent's customers are denied receiving software maintenance releases and updates, the antivirus capabilities of the accused FortiGate products that the customers already have may quickly become ineffective. (Xie, Tr. at 1368-69.) See Certain Sortation Systems, Parts Thereof, and Products Containing Same, Inv. No. 337-TA-460, Comm'n Op. at 20.

B. Cease and Desist Order

Complainant argued that it is entitled to a cease and desist order prohibiting respondent Fortinet and its affiliates, subsidiaries, divisions, licensees, agents, contractors, and other related entities, and each of their successors and assigns, from engaging in any activity in the United States relating to infringing systems for detecting and removing viruses or worms and components thereof. 19 U.S.C. § 1337(f)(1).{

} citing respondent Fortinet's Responses to Trend Micro Incorporated's Seventh Set of Interrogatories (CX-030C (Interrogatory Nos. 228-273) at Exh. A; {

} (Id.). (See CBr at 146.)

Respondents argued that should a violation of section 337 be found, the scope of any cease and desist order should be limited to products or components found to have the "requisite nexus" and should not bar support services or exports. (RBr at 142.)

The staff argued that if a violation is found, a cease and desist order against Fortinet is appropriate; and that any cease and desist order should prohibit the electronic submission of software into the United States. In support the staff cited Hardware Logic. (SBr at 88.)

Where a respondent maintains a commercially significant inventory of infringing products in the United States under Commission precedent, a cease and desist order against the respondent is appropriate. See Certain Crystalline Cefadroxil Monohydrate, Inv. No. 337-TA-293, Comm'n Op. at 6 (January 19, 1990). The evidence in this investigation shows that Fortinet keeps significant inventory of accused products in the United States. (CX-409.) Hence, the administrative law judge recommends that if a violation is found, a cease and desist order against Fortinet is appropriate. Moreover, he further recommends that the cease and desist order should prohibit the electronic submission of software into the United States because, as the Commission noted in Hardware Logic, for a cease and desist order not to cover electronic transmissions would allow for an obvious method of circumvention such that the cease and desist order would be rendered "meaningless." Hardware Logic, Comm'n Op. at 39.

XIII. Bond

Pursuant to Commission rules 210.36(a) and 210.42(a)(1)(ii), the administrative law judge is to issue a recommended determination on bonding since the accused products are entitled to entry under bond during the 60-day Presidential review period. See 19 U.S.C. § 1337(j)(3). To the extent possible, the bond should be an amount that would be sufficient to protect a complainant from an injury. See Commission rule 210.50(a)(3). In setting a bond amount, "the Commission typically has considered the differential in sales price between the patented product made by the domestic industry and the lower price of the infringing imported product." See, e.g., Microsphere Adhesives, Comm'n. Op. at 24. However, where it is difficult or impossible to calculate a bond based upon price differentials, the Commission has traditionally set the bond at 100 percent of entered value of the infringing imported product. See Certain Oscillating Sprinklers, Sprinkler Components, and Nozzles, Inv. No. 337-TA-448, Limited Exclusion Order at 4 (March 2002).

Complainant argued that a bond amount of 100 percent of the entered value for any importation of infringing products during the 60-day Presidential review period should be required; and that a bond amount of 100 percent is appropriate as there is little evidence of pricing with respect to the comparable products of Fortinet and Trend Micro. (CBr at 149.) Respondent argued that if a violation of section 337 is found, any bond that issues should be based on a reasonable royalty rate of 5 percent. (RBr at 147.) The staff argued that a bond of 100 percent of entered value is appropriate. (SBr at 89.)

The administrative law judge finds that the evidence establishes that both Fortinet and Trend Micro have numerous relevant models and product lines. (CX-15 (Response to Interrogatory No. 18) (showing 16 different Fortinet models); RX-183 (Response to Interrogatory No. 4) (Trend Micro's line of InterScan Web Security Suite, InterScan VirusWall, and InterScan Messaging Security Suite product lines).) Moreover the price comparison is made more difficult by the fact that Fortinet's products are a combination of hardware and software while those of Trend Micro are software only. See Section IV., supra. Hence, he recommends a bond, during the period of Presidential review, of 100 percent of entered value of the infringing imported products.

XIV. Additional Findings

A. Parties

1. The office of complainant Trend Micro in the United States is located at 10101 De Anza Boulevard, Cupertino, CA. (JX-010C at 17.)

2. Trend Micro also has offices in Lake Forest and Dallas/Fort Worth. (JX-010C at 18.)

3. At the Cupertino location,{ }are provided. At the Dallas/Fort Worth location, { } service is provided; at the Lake Forest location,{ } is provided. (JX-010C at 18.)

4. There are about{ }employees in the Cupertino office. (JX-010C at 18.)

5. At least some source code for Trend Micro Internet Gateway Products are developed at the Cupertino office. (JX-010C at 19.)

6. On January 1, 2005, inventor Eva Chen became Chief Executive Officer of Trend Micro. (Chen, Tr. at 9.)

7. Eva Chen resides at 965 Emcompo Drive, Pasadena, CA. (CX-390 at 2.)

8. Eva Chen works at 10101 De Anza Boulevard, Cupertino, CA. (CX-390 at 2.)

9. Samuel Chen has been the Global Director of Product Development of Trend Micro's Global Resource and Development Organization. (CX-353 at 1.)

10. Matt Yang is Trend Micro's research and development manager. (CX-392 at 7.)

11. Inventor Shuang Ji has been the Architect Lead of Trend Micro, Inc. U.S. (CX-

353 at TM100150695.)

12. Trend Micro has about{ }engineers involved in research and development in its U.S. facilities. (JX-010C at 11.)

13. The{ } Trend Micro engineers involved in research and development in its U.S. facilities have{ } responsibility for research and development in the United States. (JX-010C at 11.)

14. Trend Micro's Engineers develop internet gateway products which includes Internet Mail Security Suite and Internet Web Security Suite. (JX-010C at 12.)

15. The server that is loaded with Trend Micro's software products, which is distributed through the Web for people to purchase it electronically, is located in the United States. (JX-010C at 16-17.)

16. Trend Micro's software products sold in the United States contain CDs prepared and labeled in the United States. (JX-010C at 17.)

17. Trend Micro's Internet Gateway Products include either variations of InterScan VirusWall, Internet Mail Security Suite, and Internet Web Security Suite. One version of InterScan VirusWall is for small and medium size businesses. (JX-010C at 20.)

18. Trend Micro also sells one version of the InterScan VirusWall loaded onto a Linux-based PC. (JX-010C at 21.)

19. Trend Micro was formed in 1989 and inventor Chen was a co-founder of Trend Micro. (Chen, Tr. at 11.)

20. Trend Micro started offering its first product called "KeyLog" which is a software piracy protection device in 1989. (Chen, Tr. at 11.)

21. Around 1989, Trend Micro started to offer antivirus products along with other anti-piracy products. (Chen, Tr. at 15.)

22. Trend Micro offered an antivirus product called "Virus Buster" which was a desktop antivirus protection program. (Chen, Tr. at 15.)

23. Around the 1989 to 1991 timeframe, there were a lot of boot sector viruses which inserted its code onto the disk and got spread around by people swapping diskettes and booting up from the diskette. (Chen, Tr. at 16.)

24. Around the 1991 -1992 timeframe, other types of viruses became more common such as file virus which inserts its code into a file like an executable file, and when the file was executed then the virus will insert itself onto another executable program. Those file viruses would typically spread by people exchanging files. (Chen, Tr. at 16.)

25. Trend Micro developed a product called "Server Protect" which was involved in a license with Intel. (Chen, Tr. at 18.)

26. Trend Micro licensed to Intel the product the "Intel Lap Protect" around 1992. (Chen, Tr. at 18.)

27. With the growth of the internet, new viruses such as "macro viruses emerged" that are usually embedded in the document file such as an Excel spreadsheet or Microsoft Word document. As soon as the user opens up the document the code gets executed and then other files or documents are infected. This kind of file usually gets attached to the email. (Chen, Tr. at 18-19.)

28. Respondent Fortinet is a Delaware Corporation having its corporate headquarters and principal place of business at 920 Stewart Drive, Sunnyvale, California 94085. (CX-36 at 3.)

29. Michael Xie is the Chief Technology Officer and Vice President of Engineering for Fortinet. (Xie, Tr. at 1346.)

30. Xie received a second Masters degree in the area of electrical and computer engineering with a concentration in power transmission and simulation by computer from the University of Manitoba in 1997. (JX-007 at 14.)

31. Xie worked at Milky Way Networks for about a year and a half, which was involved in the firewall business. (JX-007 at 17.)

32. Xie started a firewall business called Infotron after leaving Milky Way Networks, which company was "wound up" in late 2002 or early 2003. (JX-007 at 18-19.)

33. Xie worked for ServGate, which manufactures and sells computer network gateway products including the ServGate-200 and ServGate-300. (JX-007 at 20-21.)

34. Xie began working for Fortinet in the latter half of 2000. (JX-007 at 25.)

35. Fortinet designs, manufactures, and sells network security gateway products. (JX-007 at 27.)

36. Xie joined Fortinet as the Chief Technology Officer where he was responsible in helping to design product strategies and organize product development. (JX-007 at 29.)

37. Xie and his brother Ken Xie founded the company in October 2000. (Xie, Tr. at 1346-1347.)

38. Fortinet develops, markets and sells the ForiGate series of antivirus firewalls. (Xie, Tr. at 1347.)

39. Fortinet initially made appliances for firewall and VPN functionalities. At a later date, Fortinet began to add security functionalities to their products. (Xie, Tr. at 1347.)

40. Fortinet has over 500 employees. (Xie, Tr. at 1348.)

41. Fortinet's target customers are corporate customers, business networks, small offices, home offices and large internet service providers. (Xie, Tr. at 1350.)

42. Traffic shaping allows the network administrator to define policies for the flow rate of different types of traffic. (Xie, Tr. at 1350.)

43. Jeff Crawford is Fortinet's Director of Antivirus Research and Development. (Crawford, Tr. at 158.)

44. Crawford has been employed by Fortinet for the last four years. (Crawford, Tr. at 154.)

45. { } (JX-007 at 51.)

46. { } (Crawford, Tr. at 159.)

47. { } (Crawford, Tr. at 159.)

48. { } (Crawford, Tr. at 160.)

49. A FortiGate product is a device that is used at a network gateway. (Crawford, Tr. at 156-157.)

50. Craig Carpenter began working at Fortinet as the director of channel marketing in August 2002. (CX-436 at 25, 26.)

51. Carpenter was responsible for building Fortinet's global channel program, enlisting resellers, distributors and integrators, training the sales force and marketing communication activities. (CX-436 at 25.)

52. Richard Kagan became a marketing consultant for Fortinet in March of 2002. (CX-437 at 14-15.)

53. Richard Kagan was Vice President of Marketing for Fortinet from July 1, 2002 until September 1, 2004. (CX-437 at 15-16.)

CONCLUSIONS OF LAW

1. The Commission has in rem jurisdiction and in personam jurisdiction.

2. There has been an importation of certain accused systems for detecting and removing viruses or worms, components thereof and products containing same which are the subject of the alleged unfair trade allegations.

3. An industry exists in the United States, as required by subsection (a)(2) of section 337, that exploits the products that are covered by the '600 patent.

4. The asserted claims 1 and 3 of the '600 patent are not valid.

5. Asserted claims 4, 7, 8, 11, 12, 13, 14 and 15 of the '600 patent are not invalid.

6. The '600 patent is enforceable.

7. Respondent's accused products infringe asserted claims 4, 7, 8, 11, 12, 13, 14 and 15 of the '600 patent.

8. There is a violation of section 337.

9. The record supports issuance of a limited exclusion order, cease and desist order, and a bond during the period of Presidential review in the amount of 100 percent of the entered value for any importation involving infringing products.

ORDER

Based on the foregoing, and the record as a whole, it is the administrative law judge's Final Initial Determination that there is a violation of section 337 in the importation into the United States, sale for importation, and the sale within the United States after importation of certain systems for detecting and removing viruses or worms, components thereof, and products containing same. It is also the administrative law judge's recommendation that a limited exclusion order and a cease and desist order should issue. The administrative law judge further recommends that a bond be imposed during the Presidential review period in the amount of 100 percent of the entered value for any importation involving infringing products.

The administrative law judge hereby CERTIFIES to the Commission his Final Initial and Recommended Determinations together with the record consisting of the exhibits admitted into evidence. The pleadings of the parties filed with the Secretary and the transcript of the pre-hearing conference, and the hearings are not certified, since they are already in the Commission's possession in accordance with Commission rules.

Further it is ORDERED that:

1. In accordance with Commission rule 210.39, all material heretofore marked in camera because of business, financial and marketing data found by the administrative law judge to be cognizable as confidential business information under Commission rule 201.6(a) is to be given in camera treatment continuing after the date this investigation is terminated.

2. Counsel for the parties shall have in the hands of the administrative law judge those portions of the final initial and recommended determinations which contain bracketed confidential business information to be deleted from any public version of said determinations,

no later than May 27, 2005. Any such bracketed version shall not be served by telecopy on the administrative law judge. If no such bracketed version is received from a party it will mean that the party has no objection to removing the confidential status, in its entirety, from these initial and recommended determinations.

3. The initial determination portion of the Final Initial and Recommended Determinations, issued pursuant to Commission rule 210.42(h)(2), shall become the determination of the Commission forty-five (45) days after the service thereof, unless the Commission, within that period shall have ordered its review or certain issues therein or by order has changed the effective date of the initial determination portion. The recommended determination portion, issued pursuant to Commission rule 210.42(a)(1)(ii), will be considered by the Commission in reaching a determination on remedy and bonding pursuant to Commission rule 210.50(a).

Paul J. Luckern

Paul J. Luckern
Administrative Law Judge

Issued: May 9, 2005

CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME

Investigation No. 337-TA-510

CERTIFICATE OF SERVICE

I, Marilyn R. Abbott, hereby certify that the attached **Public Version Final Initial and Recommended Determinations** was served by hand upon Commission Investigative Attorney Rett Snotherly, Esq. and upon the following parties via first class mail, and air mail where necessary, on August 22, 2005.

Marilyn R. Abbott

Marilyn R. Abbott, Secretary
U.S. International Trade Commission
500 E Street, SW - Room 112
Washington, DC 20436

For Complainant Trend Micro Incorporated:

Raphael V. Lupo
Mark G. Davis
McDermott, Will & Emery
600 13th Street, NW, 12th Floor
Washington, DC 20005-3096

Keaton S. Parekh
McDermott, Will & Emery
3150 Porter Drive
Palo Alto, CA 94304-1212

CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME

Investigation No. 337-TA-510

CERTIFICATE OF SERVICE page 2

For Respondent Fortinet, Inc.:

Kenneth B. Wilson,
Stefani E. Shanberg
Gina M. Steele
Sarah E. Piepmeier
Perkins Coie, LLP
180 Townsend Street
3rd Floor
San Francisco, CA 94107

Sturgis M. Sobin
Leigh A. Bacon
Miller and Chevalier Chartered
655 Fifteenth Street, NW
Washington, DC 20005

CERTAIN SYSTEMS FOR DETECTING AND REMOVING VIRUSES OR WORMS, COMPONENTS THEREOF, AND PRODUCTS CONTAINING SAME

Investigation No. 337-TA-510

PUBLIC MAILING LIST

Sherry Robinson
LEXIS-NEXIS
8891 Gander Creek Drive
Miamisburg, OH 45342

Ronnita Green
West Group
Suite 230
901 Fifteenth Street, NW
Washington, DC 20005

(PARTIES NEED NOT SERVE COPIES ON LEXIS OR WEST PUBLISHING)