IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BRITISH TELECOMMUNICATIONS PLC and BT AMERICAS, INC.,	)	
Plaintiffs,	)	C. A. No. 18-_____
v.	)	**JURY TRIAL DEMANDED**
FORTINET, INC.,	)	
Defendant.	)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs British Telecommunications plc and BT Americas, Inc. (collectively, "BT") file this Complaint for Patent Infringement against Defendant Fortinet, Inc., ("Fortinet"), and allege as follows:

NATURE OF THIS ACTION

1. This is a patent infringement action brought by BT against Fortinet based on Fortinet's continued willful infringement of U.S. Patent No. 7,159,237 (entitled "*Method and system for dynamic network intrusion monitoring, detection and response*") ("the '237 Patent") and U.S. Patent No. 7,895,641 (entitled "*Method and system for dynamic network intrusion monitoring, detection and response*") ("the '641 Patent"), as well as Fortinet's infringement of U.S. Patent No. 7,370,358 (entitled "*Agent-based intrusion detection system*") ("the '358 Patent"), U.S. Patent No. 7,693,971 (entitled "*Distributed policy based system management with local management agents responsible for obtaining and storing policies thereat*") ("the '971 Patent"), and U.S. Patent No. 7,774,845 (entitled "*Computer security system*") ("the '845 Patent") (collectively, the "Patents-in-Suit").

2. A true and correct copy of the '237 Patent is attached as Ex. A.

3. A true and correct copy of the '641 Patent is attached as Ex. B.

4. A true and correct copy of the ’358 Patent is attached as Ex. C.

5. A true and correct copy of the ’971 Patent is attached as Ex. D.

6. A true and correct copy of the ’845 Patent is attached as Ex. E.

PARTIES

7. Plaintiff British Telecommunications plc is a corporation organized under the laws of England and Wales, and has a principal place of business at 81 Newgate Street, London EC1A 7AJ, United Kingdom.

8. Plaintiff BT Americas, Inc. is a Delaware corporation, and has a principal place of business at 8951 Cypress Waters Blvd, Suite 200, Dallas TX 75019.

9. Upon information and belief, Defendant Fortinet, Inc. is a Delaware corporation, and has a principal place of business at 899 Kifer Road, Sunnyvale, CA 94086. Fortinet can be served through its registered agent, Corporation Services Company, 251 Little Falls Drive, Wilmington, Delaware 19808

JURISDICTION AND VENUE

10. This is an action for patent infringement arising under the United States patent statutes, 35 U.S.C. § 100, *et seq.*

11. This Court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

12. This Court has personal jurisdiction over Defendant Fortinet because Fortinet is incorporated in Delaware and has continuous and systematic contacts with the State of Delaware, including, *inter alia*, continuous contacts with, and sales to, customers in Delaware. Further, Fortinet has committed acts within the District of Delaware giving rise to this action, directly and through subsidiaries or intermediaries, including distributing, offering for sale, selling, using,

importing and/or advertising products and services that infringe the claims of the Patents-In-Suit in the State of Delaware.

13. Fortinet is incorporated in Delaware and venue is proper in this District under 28 U.S.C. §§ 1391(b), 1391(c), and/or 1400(b).

FACTUAL BACKGROUND

British Telecommunications plc., BT Americas, Inc. and Counterpane

14. BT is the oldest telecommunications company in the world, tracing its origins back to the Electric Telegraph Company, which was incorporated in England in 1846. Today, BT provides communications services in 180 countries and employs more than 100,000 people worldwide.

15. From its earliest beginnings, BT has been on the forefront of research and innovation in the world of communications, starting with its adaption in the nineteenth century of leading-edge telegraphy technology, including the world's first commercial telegraph service.

16. In 1975, BT opened its renowned research facility at Adastral Park, near Ipswich in the county of Suffolk, England. Adastral Park has housed some of the leading technology researchers and engineers in the world, whose inventive efforts led to the issuance of more than 10,000 patents by the turn of the century.

17. BT, directly or through its subsidiaries, has continued to maintain its longstanding commitment to research and innovation, and spends over £500,000,000 (five hundred million pounds sterling) annually on research and development, with over 13,000 scientists and technologists worldwide. BT's inventive efforts have led to numerous patents, including the '358 Patent, the '971 Patent and the '845 Patent.

18. BT has also acquired various companies throughout the years as part of its strategy to develop global professional services capabilities and, with the proliferation and sophistication of cyberattacks, to enhance Internet and infrastructure security. Specifically, in 2006, BT acquired Counterpane Internet Security, Inc. ("Counterpane"), an Internet security company founded by Dr. Bruce Schneier. Counterpane's patent portfolio, including the '237 and '641 Patents, in which Dr. Schneier is a named inventor, were included in that acquisition and are now owned by BT Americas, Inc.

Fortinet

19. Upon information and belief, Fortinet is a cyber security company that offers a broad range of products and services which incorporate technologies invented by BT and Counterpane. These include, *inter alia*, Fortinet's security appliances (e.g., FortiGate, FortiWeb, and FortiMail), FortiSandbox, FortiManager, FortiAnalyzer, FortiGuard, FortiClient, and FortiClient EMS.

20. BT has notified Fortinet of Fortinet's infringement of the '237 and '641 Patents and requested that Fortinet enter into discussions with BT to address it, *e.g.*, through a licensing arrangement.

21. Fortinet has derived and will continue to derive substantial value from these products and services which incorporate the patented technologies. Nonetheless, Fortinet has failed to provide meaningful responses to BT's correspondence and chosen instead to continue to infringe the '237 and '641 Patents willfully and wantonly.

22. On December 11, 2014, the chief counsel for Intellectual Property Rights of BT ("BT's IP Counsel") sent a letter to Fortinet identifying the '237 and '641 Patents and providing clear notice that Fortinet infringed them. The December 11, 2014 letter identified representative

products that infringed each of them. It also stated that BT had prepared detailed charts that BT could present at an in person meeting.

23. Neither Fortinet nor Fortinet's counsel responded to BT's December 11, 2014 letter.

24. On April 9, 2015, BT sent a follow-up letter to Fortinet along with a copy of the December 11, 2014 letter. Neither Fortinet nor Fortinet's counsel responded to BT's follow-up or the December 11, 2014 letter.

25. On July 31, 2015, BT again sent another follow-up. Neither Fortinet nor Fortinet's counsel responded to that either.

26. On October 22, 2015, BT once again wrote to Fortinet. Neither Fortinet nor Fortinet's counsel responded to BT.

27. On January 5, 2016, BT's IP Counsel sent another letter to Fortinet in which BT told Fortinet that it had been more than a year since BT's initial letter, that BT had tried on several occasions to initiate a dialogue with Fortinet for patent licensing discussion but, unfortunately, BT's efforts had gone un-acknowledged and un-answered. BT explained Fortinet's infringement of a representative claim of each the '237 and '641 Patents on an element-by-element basis.

28. Finally, in February 1, 2016, Fortinet's outside counsel responded to BT's January 5, 2016 letter. However, Fortinet's response did not identify specific deficiencies in BT's analysis nor did it provide any meaningful explanation why Fortinet did not infringe the '237 and '641 Patents.

29. On March 21, 2016, BT responded to Fortinet's letter of February 1, 2016 noting that Fortinet had failed to identify why Fortinet's products did not infringe the '237 and '641 Patents.

30. Neither Fortinet nor Fortinet's outside counsel responded to BT's March 21, 2016 letter.

31. On September 13, 2016, BT sent a follow-up letter to Fortinet's outside counsel reminding Fortinet that BT had not received any response from Fortinet and, once again, inviting a response.

32. Neither Fortinet nor Fortinet's outside counsel responded to BT's September 13, 2016 letter either.

33. Despite BT's repeated attempts to reach an amicable resolution with Fortinet, and BT's numerous requests that Fortinet stop infringing the Patents-In-Suit, Fortinet has continued to infringe willfully and wantonly. BT brings this action to recover the just compensation it is owed for Fortinet's past infringement, and to prevent Fortinet from continuing to benefit from the patented inventions in the future without authorization or compensation to BT.

Fortinet Infringes the '237 and '641 Patents

34. The '237 Patent (U.S. Patent No. 7,159,237) was issued by the United States Patent and Trademark Office ("USPTO") on January 2, 2007. BT Americas, Inc. is the lawful owner by assignment of all rights, title and interest in the '237 Patent, including the right to sue for patent infringement and damages, including past damages.

35. The '641 Patent (U.S. Patent No. 7,895,641) was issued by the USPTO on February 22, 2011. The '641 patent is a continuation of the application that issued as the '237 patent. BT Americas, Inc. is the lawful owner by assignment of all rights, title and interest in the

'641 Patent, including the right to sue for patent infringement and damages, including past damages.

36. The '237 and '641 Patents represent important advances in the field of cybersecurity, and disclose an architecture for unearthing and addressing network intrusions. This architecture has now been widely adopted throughout the security industry, including by Fortinet.

37. One of the named inventors, Dr. Bruce Schneier, is an internationally renowned cryptographer and security expert who has been called a "security guru" by The Economist and is the author of several books on security topics, computer security and cryptography, including, but not limited to, Applied Cryptography, Cryptography Engineering, Secrets and Lies, and Schneier on Security.[1]

38. Another named inventor of the '237 and '641 Patents is Jon Callas. Also an internationally renowned security expert, Mr. Callas has served as the Chief Technology Officer of Entrust and worked on Apple's core security technology over the years, including Mac and iOS.[2]

39. The '237 and '641 Patents relate generally to a method and system for dynamic network intrusion monitoring that monitors network activity using a probe that collects status data from monitored components, and filters that data into what is good, what is bad and the remainder which is indeterminate. Prior art solutions consisted of anti-virus (and other anti-malware) software at the edge of the network that would be updated periodically with newly discovered viruses or malware. Decisions whether traffic was bad, good or indeterminate were

[1] *See, e.g.*, Bruce Schneier, Wikipedia (*available at* https://en.wikipedia.org/wiki/Bruce_Schneier) (last accessed 6/13/2018)
[2] *See, e.g.*, Jon Callas, Wikipedia (*available at* https://en.wikipedia.org/wiki/Jon_Callas) (last accessed 6/13/2018)

typically made immediately at the interface of the network based primarily on the presence or absence of patterns matching the viruses (or malware) that had been previously identified. However, prior art solutions had limited ability to address newer (or previously unknown) forms of viruses (and malware) and detect intrusions quickly enough to prevent them from doing a great deal of damage within a computer network.

40. The inventions of the ‘237 and ‘641 Patents are improvements in computer networks and technology that address these problems in the prior art, and take a far more flexible and dynamic approach to identify and remedy previously undetected malware and potential network attacks. To identify and address unknown attacks without generating false alerts that impair the performance of the network, probes comprised of network sensors extract status data which is run through a filtering subsystem to filter that status data into what is good or bad. However, the residue, which is indeterminate, is not discarded but rather transmitted to a secure operations center (SOC) where further analysis can be taken, e.g., by comparing status data collected from other probes situated at other locations. After further analysis of the indeterminate data, an update is sent back to the probe in order to arm the system relatively quickly.

41. As described in detail in Counts I and II below, Fortinet offers a series of products and services that infringe the ’237 and ’641 Patents. Fortinet’s “Advanced Threat Protection” (ATP) framework consists of several products and services, including Fortinet security appliances (*e.g.*, FortiGate, FortiWeb, and FortiMail) which are connected to the network to examine, analyze and filter the status data into what is good, bad or indeterminate. FortiSandbox receives indeterminate data to ascertain whether it might represent an unknown attack which, in turn, transmits it to Fortinet analysts, *e.g.*, FortiGuard.

Fortinet Infringes the ’358 Patent

42. The ’358 Patent (U.S. Patent No. 7,370,358) was issued by the USPTO on May 6, 2008. British Telecommunications plc is the lawful owner by assignment of all rights, title and interest in the ’358 Patent, including the right to sue for patent infringement and damages, including past damages.

43. The ’358 Patent relates generally to a system and method where security appliances are grouped, with each member of the group performing behavioral analysis on itself and associated data, and reporting detected issues to other devices that belong to the same group using a group-specific tag. Prior art solutions consisted of specific network or machine checkpoints to indicate the existence of an attack (or a threat) which required a separate specific sensing capability for every possible point of attack. However, with the proliferation of increasingly powerful macro viruses, some of which have port-scanning capabilities, these systems were insufficiently flexible, scalable or reactive to be able to deal effectively with new and potentially unknown security threats.

44. The inventions of the ’358 Patent are improvements in computer networks and technology that address these problems in the prior art. Specifically, heuristic analysis is performed at the endpoint to determine whether the system is operating within the boundaries of normal expectations or may be under attack. Groups of agents, comprised of intelligent software agents, communicate with other agents within the same group through communications bearing a group-specific tag. The communications pass along warnings following the detection of potential threats along with information as to what was anomalous about the pattern of behavior thereby providing a flexible, scalable, and reactive solution to potentially unknown security threats.

45. As described in detail in Count III below, Fortinet offers a number of products and services that infringe the ’358 Patent. For example, the Fortinet security appliances (*e.g.*, FortiGate, FortiWeb, and FortiMail) and corresponding software agents are associated with a FortiSandbox to form a group. Each security appliance (and associated agent) performs behavioral analysis on itself and associated data (e.g., with heuristic scanning) and communicates with members of its agent group through the FortiSandbox to report detected issues using group-specific (e.g., customer-specific) tags.

Fortinet Infringes the ’971 Patent

46. The ’971 Patent (U.S. Patent No. 7,693,971) was issued by the USPTO on April 6, 2010. British Telecommunications plc is the lawful owner by assignment of all rights, title and interest in the ’971 Patent, including the right to sue for patent infringement and damages, including past damages.

47. The ’971 Patent generally relates to a system and method for managing components within a computer network through a decentralized system in which policies governing the behavior of a computer network are distributed throughout the network and handled by agents. Prior art solutions consisted of a large number of heterogeneous components and systems with significant management burdens for system administrators (including IT administrators). Specifically, significant front-end manual intervention was required when new components were added to a computer system, both in terms of updating policies relevant to each new component and in re-writing existing policies to allow for a decentralized implementation of policies. Further, as the complexity of the computer system increased, management capability was additionally stretched.

48. The inventions of the ’971 Patent are improvements in computer network technology that address the problems in the prior art and take a far more flexible approach from prior art systems. Each agent is associated with a subnetwork and local components within the subnetwork are registered at the agents. The agent identifies and stores the roles to be performed by each registered component and obtains and stores policies (or rules) appropriate for the registered components. By adopting this flexible approach, the system components can delegate their policy handling responsibilities to a local instance of the agent, which will then monitor significant changes in this system environment, and evaluate and initiate the appropriate control actions. Policy handling is thus carried out, close to the managed components, and without the need for centralized coordination.

49. As described in detail in Count IV below, Fortinet offers a series of products and services that infringe the ’971 Patent. For example, Fortinet’s FortiGate manages different subsets of FortiClients (equipped at endpoint terminals), which apply policies. Each FortiGate is assigned to manage a different subnetwork of endpoint terminals equipped with FortiClient software. Fortinet also offers FortiClient EMS software and FortiManager, which works with the FortiGate and FortiClient, to manage the agents and update policies.

Fortinet Infringes the ’845 Patent

50. The ’845 Patent (U.S. Patent No. 7,774,845) was issued by the USPTO on August 10, 2010. British Telecommunications plc is the lawful owner by assignment of all rights, title and interest in the ’845 Patent, including the right to sue for patent infringement and damages, including past damages.

51. The ’845 Patent generally relates to a system and method of implementing a security system whereby one or more security devices detect and track security-related issues

identified by one or more security devices, and takes specified actions when a certain threshold of activities has been exceeded. Prior art solutions consisted of anti-virus (or other anti-malware) software that typically resided on individual machines and monitored the system to check for the presence of known viruses. The anti-virus software would run in the background and monitor operations performed on the computer (e.g. data received at and/or transmitted from the computer). If the byte-code signature of a known virus were detected by the program, the anti-virus program would inform the user and takes appropriate action against the data, such as deleting it or storing it in a protected drive. However, the prior art approach suffered from a big problem: delay. The process from the discovery of a new virus to the delivery of its signature to all protected machines took too long—i.e., it required an administrative authority (e.g., the anti-virus program manufacturer) to recognize the problem, take action to identify the virus's signature, update the anti-virus database, and distribute the updated database to each user. By the time such a sequence of actions was complete, the damage had already been done.

52. The inventions of the '845 Patent are improvements in computer network technology that address the problems in the prior art (e.g., delay), and take a far more rapid approach—one that can operate on the same time scales as the spread of the virus and thus provide much more rapid and cost-saving protection. The '845 Patent does so by empowering the endpoints to identify potential malware such that a count for each of the instances in which a particular piece of malware appears. Once the total count across endpoints exceeds a specified threshold of instances, action is taken. The count and threshold may be maintained at a central server from which a warning or other form of remedial action emanates once the threshold has been exceeded or may be maintained within each user computer with the exchange of warnings

occurring peer-to-peer. By decentralizing detection and allowing the decision to take place once the threshold has been passed, response time is accelerated.

53. As described in detail below in Count V, Fortinet offers a series of products and services that infringe the ’845 Patent, including FortiClient, FortiClient EMS, FortiGate and/or FortiAnalyzer. For example, Fortinet’s FortiClients detect and track various threats and communicate them to the FortiAnalyzer. The FortiClient EMS maintains a count of the various vulnerability-scan related information and the FortiAnalyzer triggers a certain action when the count exceeds a certain threshold.

COUNT I
(INFRINGEMENT OF U.S. PATENT NO. 7,159,237)

54. BT repeats and re-alleges the allegations contained in Paragraphs 1 through 53 above as if fully set forth herein.

55. Fortinet has directly infringed and continues to directly infringe, literally or under the doctrine of equivalents, one or more claims of the ’237 Patent in violation of 35 U.S.C. §271(a) by making, using, offering to sell, selling (directly or through intermediaries), and/or importing, in this District and elsewhere in the United States, various Fortinet products and services including, but not limited to, FortiGate, FortiWeb, FortiMail, FortiSandbox, FortiManager, FortiAnalyzer, and/or FortiGuard.

56. For example, Fortinet infringes claim 1 of the ’237 Patent, which provides as follows:

> A method of operating a probe as part of a security monitoring system for a computer network, comprising:
>
> a) collecting status data from at least one monitored component of said network;

b) analyzing status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;

c) transmitting information about said identified events to an analyst associated with said security monitoring system;

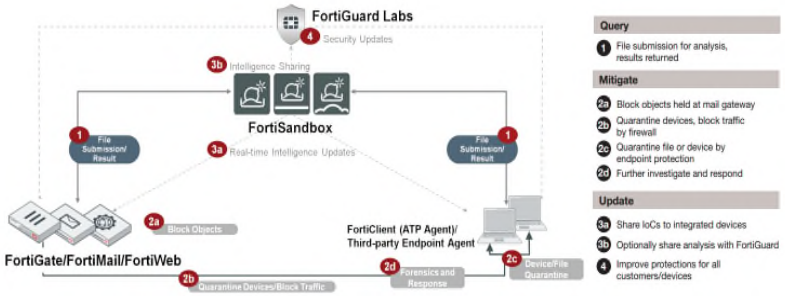
d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and

e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

57. Fortinet performs each and every step of claim 1, among other claims, and has been placed squarely on notice of its infringement of the ’237 Patent in various correspondence detailing its infringement (e.g., BT’s letters December 11, 2014 and January 5, 2016).

58. By way of example, Fortinet provides and operates a series of products that individually and collectively provide security services (“a security monitoring system”) for networks that belong to Fortinet’s customers. Fortinet refers to this system as the Fortinet “Advanced Threat Protection” (ATP) framework.

59. The following figure provides a detailed workflow of the ATP framework:



FortiSandbox Data Sheet[3]

[3] FortiSandbox Data Sheet (*available at* https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf) (last accessed 6/13/2018).

60. Fortinet collects status data from at least one monitored component of the network. Specifically, FortiGate/FortiMail/FortiWeb (collectively, the "Fortinet Security Appliances") are composed of multiple special purpose sensors. A sensor includes at least the portion of the Fortinet Security Appliances that receives network traffic destined for or originating from a monitored component of the network, and processes that traffic to collect information relevant to the state or condition of the network, network traffic, or the monitored component.[4]

61. The status data collected might reflect information derived from one or more processed network packets, either at a single point in time, or across relevant periods of time. Status data may also include both information extracted from the underlying network traffic (such as the IP addresses of the originating and/or destination computers) and information determined from the underlying network traffic (such as the frequency of messages, sensor IP, message count, and associated time stamps or the duration of an event). Other status data collected might provide context for other status data should it be subsequently desirable to correlate status data across multiple sensors to enhance the detection and response capabilities of the system.

[4] *See, e.g.*, Fortinet Advanced Threat Protection Solution guide (*available at* https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/atp-solution.pdf) ("In addition to its proactive research, global honeypot infrastructure, and 3,000,000+ network security appliances also acting as sensors, FortiGuard Labs has established more than 200 threat information-sharing agreements…") (last accessed 6/13/2018)

62. By way of example, Fortinet identifies "custom signature keywords" many of which are examples of collected and processed status information, including, but not limited to, the following:[5]

- "*ip_option*," "*ip_ttl*," "*protocol*," "*src_addr*," and "*dat_addr*," which are examples of status information extracted from the IP Header.
- "*ack*," "*dst_port*," "*src_port*," and "*tcp_flags*," which are examples of status information extracted from the TCP Header.
- "*dat_port*," and "*src_port*," which are examples of status information extracted from the UDP Header.

63. Fortinet also collects status data that is derived from a received packet, such as "Host/UserName."[6]

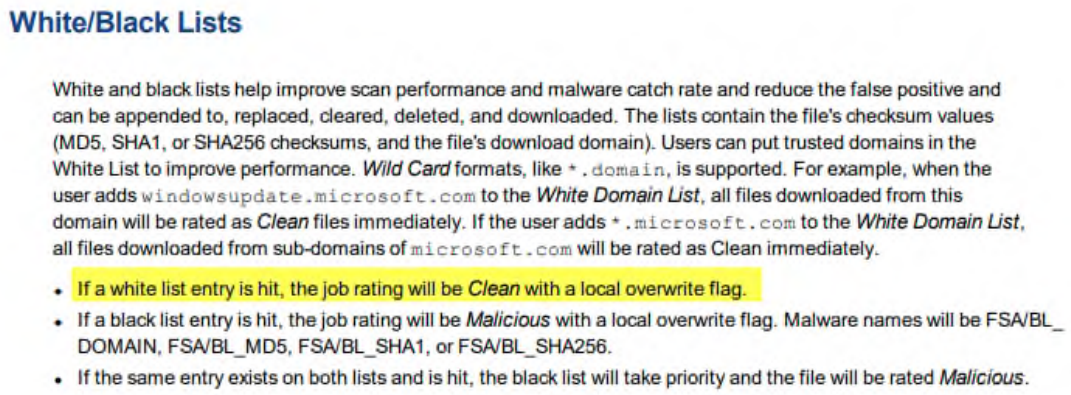
64. Fortinet performs filtering and analysis of the status data to identify security related events that represent suspicious and/or malicious activity ("to identify potentially security-related events represented in the status data").

65. Once the network traffic data has been processed and status data relating to it is under consideration, the Fortinet Security Appliances can then make one of three choices. The first two choices involve the application of the filter to determine what is good or bad (which includes what is suspicious). Here, based upon analysis of related status data, the traffic that is good can be allowed and the traffic that is known to be bad (or suspicious) can be blocked. For example, the Fortinet Security Appliances may use "white listing" and "black listing" techniques

[5] *See, e.g.*, Fortinet Custom Signatures Keywords (*available at* http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20signature%20keywords.htm?Highlight=rules.) (last accessed 6/13/2018)
[6] FortiSandbox Administration Guide, v 2.4.1 (*available at* https://docs.fortinet.com/uploaded/files/3801/fortisandbox-v2.4.1-administration-guide.pdf) (last accessed 6/13/2018).

or similar but more advanced processes to allow or block traffic based on a generated alert or the absence of a generated alert.

66. In white listing, the Fortinet Security Appliances determine from the status data that there is no need for an alert as the status data does not appear to represent a security event (i.e., the Fortinet Security Appliances determine that the status data represents normal expected traffic). White listing could be applied, for example, by filtering based on an IP address extracted by the sensor during the collection of status information.[7] In addition, white listing can also be applied to domain names. For example, trusted domain names that are a hit to the white list will be flagged as "Clean."



White/Black Lists

White and black lists help improve scan performance and malware catch rate and reduce the false positive and can be appended to, replaced, cleared, deleted, and downloaded. The lists contain the file's checksum values (MD5, SHA1, or SHA256 checksums, and the file's download domain). Users can put trusted domains in the White List to improve performance. *Wild Card* formats, like `*.domain`, is supported. For example, when the user adds `windowsupdate.microsoft.com` to the *White Domain List*, all files downloaded from this domain will be rated as *Clean* files immediately. If the user adds `*.microsoft.com` to the *White Domain List*, all files downloaded from sub-domains of `microsoft.com` will be rated as Clean immediately.

- If a white list entry is hit, the job rating will be *Clean* with a local overwrite flag.
- If a black list entry is hit, the job rating will be *Malicious* with a local overwrite flag. Malware names will be FSA/BL_DOMAIN, FSA/BL_MD5, FSA/BL_SHA1, or FSA/BL_SHA256.
- If the same entry exists on both lists and is hit, the black list will take priority and the file will be rated *Malicious*.

FortiSandbox – Administration Guide[8]

67. In black listing, the Fortinet Security Appliances determine from the status data that there is a sufficiently high likelihood that it represents a security related event (e.g., bad or

[7] *See, e.g.*, Blacklisting & Whitelisting Clients (*available at* http://help.fortinet.com/fweb/550/Content/FortiWeb/fortiweb-admin/blacklisting.htm) ("**Trusted IPs** — Almost always allowed to access to your protected web servers. Trusted IPs are exempt from many (but not all) of the restrictions that would otherwise be applied by a server policy.") (last accessed 6/13/2018).

[8] *See, e.g.*, FortiSandbox – Administration Guide (*available at* https://docs.fortinet.com/uploaded/files/3244/fortisandbox-v2.3.0-administration-guide.pdf) (last accessed 6/13/2018)

suspicious), allowing for the generation of an appropriate alert. The Fortinet Security Appliances can use the alert to automatically block the underlying network traffic to which the derived status data/alert relates. For example, the Fortinet Security Appliances identify status data as representing a malicious event using techniques such as looking for known attack signatures. Black listing could be applied, for example, by filtering based on an IP address extracted by the sensor during the collection of status information. More specifically, requests can be blocked based upon their source IP address, their current reputation known to Fortinet Security Appliances, or a country or region with which the IP address is associated:

Blacklisting & Whitelisting Clients[9]

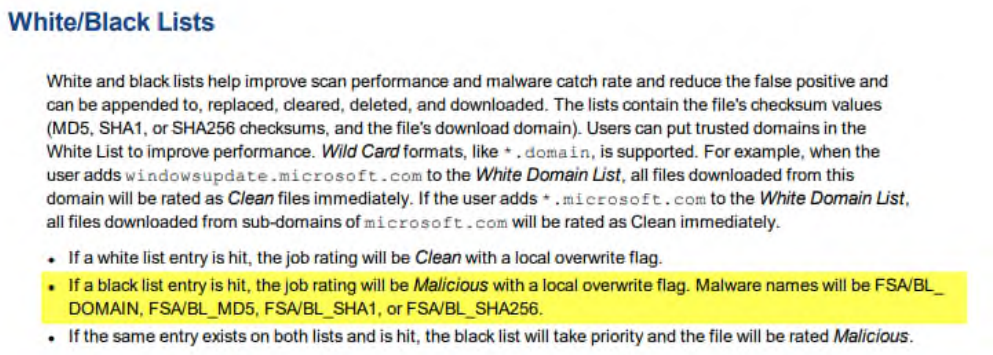
68. Requests from blacklisted IP addresses could receive a warning message as shown below:

Blacklisting & Whitelisting Clients[10]

[9] *Id.*

[10] Blacklisting & whitelisting clients (*available at* http://help.fortinet.com/fweb/550/Content/FortiWeb/fortiweb-admin/blacklisting.htm) (last accessed 6/13/2018).

69. In addition, blacklisting can also be applied to domain names. For example, untrusted domain names that are a hit to the black list will be flagged as "Malicious."



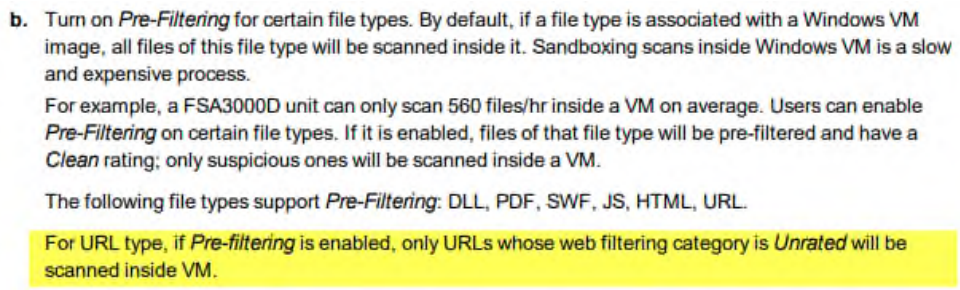
White/Black Lists

White and black lists help improve scan performance and malware catch rate and reduce the false positive and can be appended to, replaced, cleared, deleted, and downloaded. The lists contain the file's checksum values (MD5, SHA1, or SHA256 checksums, and the file's download domain). Users can put trusted domains in the White List to improve performance. *Wild Card* formats, like `*.domain`, is supported. For example, when the user adds `windowsupdate.microsoft.com` to the *White Domain List*, all files downloaded from this domain will be rated as *Clean* files immediately. If the user adds `*.microsoft.com` to the *White Domain List*, all files downloaded from sub-domains of `microsoft.com` will be rated as Clean immediately.

- If a white list entry is hit, the job rating will be *Clean* with a local overwrite flag.
- If a black list entry is hit, the job rating will be *Malicious* with a local overwrite flag. Malware names will be FSA/BL_DOMAIN, FSA/BL_MD5, FSA/BL_SHA1, or FSA/BL_SHA256.
- If the same entry exists on both lists and is hit, the black list will take priority and the file will be rated *Malicious*.

FortiSandbox – Administration Guide[11]

70. Data neither discarded nor selected by filtering represents status data that is indeterminate and has not been selected or discarded by the initial analysis. This indeterminate data can include, by way of example, domain names that are in the "unrated" category (as shown below) or executables.



b. Turn on *Pre-Filtering* for certain file types. By default, if a file type is associated with a Windows VM image, all files of this file type will be scanned inside it. Sandboxing scans inside Windows VM is a slow and expensive process.

For example, a FSA3000D unit can only scan 560 files/hr inside a VM on average. Users can enable *Pre-Filtering* on certain file types. If it is enabled, files of that file type will be pre-filtered and have a *Clean* rating; only suspicious ones will be scanned inside a VM.

The following file types support *Pre-Filtering*: DLL, PDF, SWF, JS, HTML, URL.

For URL type, if *Pre-filtering* is enabled, only URLs whose web filtering category is *Unrated* will be scanned inside VM.

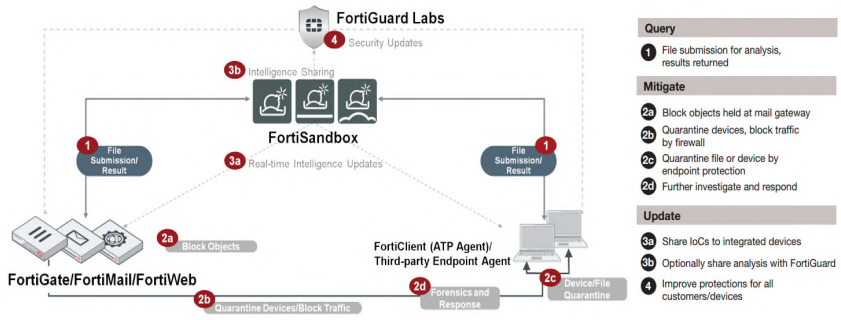
FortiSandbox – Administration Guide[12]

[11] *See, e.g.*, FortiSandbox – Administration Guide (*available at* https://docs.fortinet.com/uploaded/files/3244/fortisandbox-v2.3.0-administration-guide.pdf) (last accessed 3/2/2018)

[12] *See, e.g.*, FortiSandbox – Administration Guide (*available at* https://docs.fortinet.com/uploaded/files/3244/fortisandbox-v2.3.0-administration-guide.pdf) (last accessed 3/2/2018)

71. The Fortinet Security Appliances will then deliver to the FortiSandbox the indeterminate status data to determine whether it might represent an unknown attack. The analysis of the status data by FortiSandbox is transmitted to at least one "analyst" that is associated with the Fortinet security monitoring system. Specifically, FortiSandbox will transmit information to Fortinet's threat research & response labs, FortiGuard, for "in-depth analysis so that appropriate fixes that take into account all of the security layers can be done and delivered to the different security enforcement points, such as the Firewall. This may include updated AV and IPS signature, updated IP reputation database, etc."[13]

72. Fortinet receives feedback at FortiGate based on empirically-derived information. This is illustrated below in 3(a) which is labeled "Real-time Intelligence Update":



FortiSandbox Data Sheet[14]

73. Moreover, Fortinet notes that "FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform" including the following:

[13] *See* https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/MSSP-ATP.pdf
[14] FortiSandbox Data Sheet (*available at* https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf) (last accessed 6/13/2018)

FortiSandbox	Intelligence from IPS, AntiVirus, IP Reputation, Web Filtering, and FortiCare services.
FortiClient	Intelligence from Application Control, AntiVirus, Web Filtering, Vulnerability Scan, and FortiCare services.
FortiCache	Intelligence from AntiVirus, Web Filtering, Content Analysis, and FortiCare services.
FortiMail	Intelligence from AntiVirus, AntiSpam, FortiSandbox Cloud, and FortiCare services.
FortiWeb	Intelligence from Web Application Security, AntiVirus, IP Reputation, Vulnerability Scan, and FortiCare services.
FortiADC	Intelligence from IP Reputation Web Application Security, and FortiCare services.
FortiDDoS	Intelligence from IP Reputation and FortiCare services.
FortiDB	Intelligence from Database Security and FortiCare services.

FortiGuard Security Services[15]

74. Fortinet dynamically modifies the analysis capability of the Fortinet Security Appliances during operation such that the methods of analysis are improved based on then-current intelligence.[16] Specifically, Fortinet is able to push up-to-date security intelligence to Fortinet Security Appliances, delivering timely protection against new and emerging threats.[17]

75. Despite BT's written notice to Fortinet of Fortinet's infringement of the '237 Patent, Fortinet has not stopped its infringement. Rather, Fortinet continues to make, use, and offer its products and services in a manner which infringes the '237 Patent.

76. Fortinet's infringement of the '237 Patent has been and is willful because Fortinet has known of the '237 Patent, known that its products and services infringe the '237 Patent, and still continues to offer them in an infringing manner in disregard of BT's patent rights.

77. More particularly, following BT's notice, Fortinet has continued to infringe by supplying infringing equipment and using the claimed method to service its clients. In this regard, Fortinet has knowingly encouraged and intended—and continues to encourage and

[15] FortiGuard Security Services (*available at* https://isecurenet.net/wp-content/uploads/2016/06/Brochure-FortiGuard-Security-Services.pdf) (last accessed 6/8/2018)
[16] *See, e.g.*, Fortinet Advanced Threat Protection (*available at https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/atp-solution.pdf*) (last accessed 6/13/2018)
[17] Id. ("As a new threat emerges, certain detection and prevention products communicate directly for immediate, automated response. Additionally, FortiGuard Labs 24x7x365 global operations pushes up-to-date security intelligence in real time to Fortinet solutions, delivering instant protection against new and emerging threats.");

intend—for its customers to use Fortinet products/services in infringing manners. For example, Fortinet's websites and videos advertise FortiSandbox" as "the only solution using a pre-filter" "keeping threats out without having to activate and analyze."[18] In addition, Fortinet notes that it is able to "correlate information across security products and identify areas for security improvement" and that its "[t]hreat [i]ntelligence…[will] constantly assess threats, trends and emerging attack vectors and techniques."[19]

78. Furthermore, Fortinet markets the value of pre-filtering to counter the "processor and time intensive" nature of sandboxing noting that the process would otherwise be "slow" and "slow is a problem."[20]

79. Fortinet also specifically encourages sandboxing pre-filtering: "It is recommended to turn on sandboxing pre-filtering for web files."[21]

80. Fortinet does not have a license or permission to use the claimed subject matter.

81. BT has been damaged and continues to be damaged by Fortinet's infringement.

82. BT is entitled to recover from Fortinet the damages sustained by BT as a result of Fortinet's wrongful acts in an amount subject to proof at trial and up to three times its actual damages due to Fortinet's willful infringement.

83. BT is suffering and will continue to suffer irreparable harm for which there is no adequate remedy at law as a result of Fortinet's infringement of the '237 Patent. By way of

[18] FortiSandbox webpage (*available at* https://www.fortinet.com/products/sandbox/fortisandbox.html) (last accessed 6/13/2018)
[19] https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/MSSP-ATP.pdf) (last accessed 1/8/2018)
[20] *Id.*
[21] FortiSandbox Administration Guide, v 2.4.1 (*available at* https://docs.fortinet.com/uploaded/files/3801/fortisandbox-v2.4.1-administration-guide.pdf) (last accessed 6/13/2018).

example, Fortinet's infringing products and/or services compete with those of BT Americas. Unless enjoined, Fortinet will continue its infringing conduct.

COUNT II
(INFRINGEMENT OF U.S. PATENT NO. 7,895,641)

84. BT repeats and re-alleges the allegations contained in Paragraphs 1 through 53 above as if fully set forth herein.

85. Fortinet has directly infringed and continues to directly infringe, literally or under the doctrine of equivalents, one or more claims of the '641 Patent in violation of 35 U.S.C. §271(a) by making, using, offering to sell, selling (directly or through intermediaries), and/or importing, in this District and elsewhere in the United States, various Fortinet products and services including, but not limited to, FortiGate, FortiWeb, FortiMail, FortiSandbox, FortiManager, FortiAnalyzer, and/or FortiGuard.

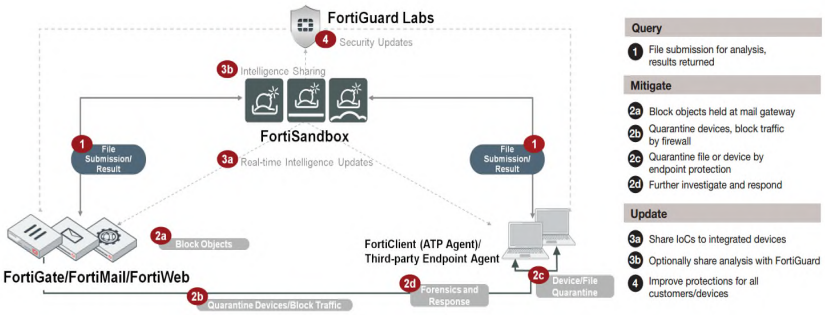
86. For example, Fortinet infringes claim 1 of the '641 Patent, which provides as follows:

> A system for operating a probe as part of a security monitoring system for a computer network, the system comprising:
>
> a) a sensor coupled to collect status data from at least one monitored component of the network;
>
> b) a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
>
> c) a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;
>
> d) a receiver for receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system; and

e) a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.

87. Fortinet offers and operates a series of products that individually and/or collectively infringe claim 1, among other claims, and has been placed squarely on notice of its infringement of the '641 Patent in various correspondence detailing its infringement (*e.g.*, BT's letters December 11, 2014 and January 5, 2016).

88. By way of example, Fortinet offers a series of products that individually and collectively provide security services ("a security monitoring system") for networks that belong to Fortinet's customers. Fortinet refers to this system as the Fortinet "Advanced Threat Protection" (ATP) framework. The following figure provides a detailed workflow of the ATP framework:



FortiSandbox Data Sheet[22]

89. The FortiGate/FortiMail/FortiWeb (collectively, the "Fortinet Security Appliances") are composed of multiple special purpose sensors. A sensor includes at least the portion of the Fortinet Security Appliances that receives network traffic destined for or originating from a monitored component of the network, and processes that traffic to collect

[22] FortiSandbox Data Sheet (*available at* https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf) (last accessed 6/13/2018)

information relevant to the state or condition of the network, network traffic, or the monitored component.[23]

90. The status data collected might reflect information derived from one or more processed network packets, either at a single point in time, or across relevant periods of time. Status data may also include both information extracted from the underlying network traffic (such as the IP addresses of the originating and/or destination computers) and information determined from the underlying network traffic (such as the frequency of messages, sensor IP, message count, and associated time stamps or the duration of an event). Other status data collected might provide context for other status data should it be subsequently desirable to correlate status data across multiple sensors to enhance the detection and response capabilities of the system.

91. By way of example, Fortinet identifies "custom signature keywords" many of which are examples of collected and processed status information, including, but not limited to, the following:[24]

- "*ip_option*," "*ip_ttl*," "*protocol*," "*src_addr*," and "*dat_addr*," which are examples of status information extracted from the IP Header.
- "*ack*," "*dst_port*," "*src_port*," and "*tcp_flags*," which are examples of status information extracted from the TCP Header.
- "*dat_port*," and "*src_port*," which are examples of status information extracted from the UDP Header.

[23] *See, e.g.*, Fortinet Advanced Threat Protection Solution guide (*available at* https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/atp-solution.pdf) ("In addition to its proactive research, global honeypot infrastructure, and 3,000,000+ network security appliances also acting as sensors, FortiGuard Labs has established more than 200 threat information-sharing agreements…") (last accessed 6/13/2018)

[24] Fortinet Custom Signatures Keywords (*available at* http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20signature%20keywords.htm?Highlight=rules.) (last accessed 6/13/2018)

92. Fortinet also collects status data that is derived from a received packet, such as "Host/UserName."[25]

93. The Fortinet Security Appliances and FortiSandbox are composed of various sub-systems that perform filtering and analysis. These sub-systems span the first two primary phases in Fortinet's ATP framework – i.e., "Prevention – blocking, as much as possible, typically known threats, often based on global intelligence" and "Detection – continuing inspection, usually for unknown threats based on local analysis and intelligence."[26] The filtering sub-system is coupled to analyze status data in that the sub-system is operatively connected to the sensor such that the collected status information can be received and processed.

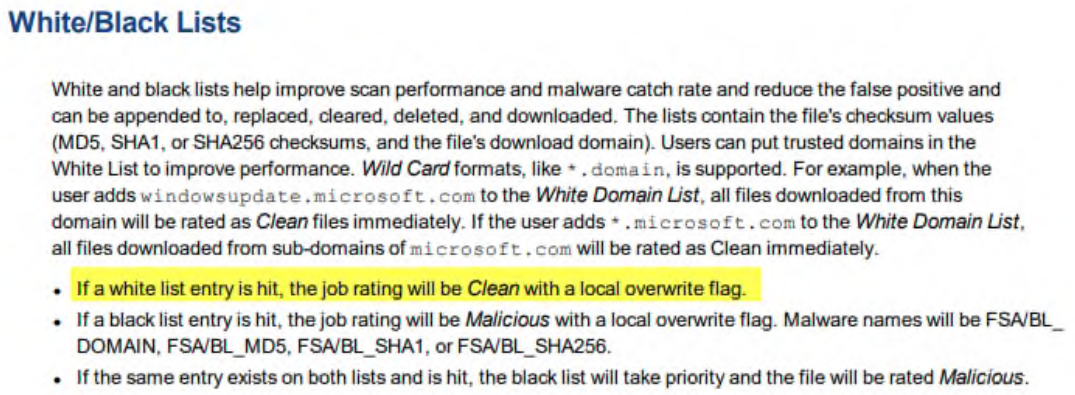
94. By analyzing status data present in network traffic, Fortinet's products have the ability to identify security related events that represent suspicious and/or malicious activity ("to identify potentially security-related events represented in the status data").

95. The Fortinet Security Appliances will subject that information to further processing (*i.e.*, "filtering") in order to determine whether the status data is actually indicative of an event that requires one or more network packets to be blocked.[27] The Fortinet Security Appliances can then make one of three choices. The first two choices involve the application of the filter to determine what it good or bad (which includes what is suspicious). Here, based upon analysis of related status data, the traffic that is known to be good can be allowed and the traffic that is known to be bad (or suspicious) can be blocked. For example, the Fortinet Security

[25] FortiSandbox Administration Guide, v 2.4.1 (*available at* https://docs.fortinet.com/uploaded/files/3801/fortisandbox-v2.4.1-administration-guide.pdf) (last accessed 6/13/2018).
[26] Fortinet Advanced Protection (*available at* https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/atp-solution.pdf) (last accessed 6/13/2018).
[27] *See Id.*

Appliances may use "white listing" and "black listing" techniques or similar, but more advanced processes to allow or block traffic based on a generated alert or the absence of a generated alert.

96. In white listing, the Fortinet Security Appliances determine from the status data that there is no need for an alert as the status data does not appear to represent a security event (*i.e.*, the Fortinet Security Appliances determine that the status data represents normal expected traffic). White listing could be applied, for example, by filtering based on an IP address extracted by the sensor during the collection of status information.[28] In addition, white listing can also be applied to domain names. For example, trusted domain names that are a hit to the white list will be flagged as "Clean."



White/Black Lists

White and black lists help improve scan performance and malware catch rate and reduce the false positive and can be appended to, replaced, cleared, deleted, and downloaded. The lists contain the file's checksum values (MD5, SHA1, or SHA256 checksums, and the file's download domain). Users can put trusted domains in the White List to improve performance. *Wild Card* formats, like `*.domain`, is supported. For example, when the user adds `windowsupdate.microsoft.com` to the *White Domain List*, all files downloaded from this domain will be rated as *Clean* files immediately. If the user adds `*.microsoft.com` to the *White Domain List*, all files downloaded from sub-domains of `microsoft.com` will be rated as Clean immediately.

- If a white list entry is hit, the job rating will be *Clean* with a local overwrite flag.
- If a black list entry is hit, the job rating will be *Malicious* with a local overwrite flag. Malware names will be FSA/BL_DOMAIN, FSA/BL_MD5, FSA/BL_SHA1, or FSA/BL_SHA256.
- If the same entry exists on both lists and is hit, the black list will take priority and the file will be rated *Malicious*.

FortiSandbox – Administration Guide[29]

97. In black listing, the Fortinet Security Appliances determine from the status data that there is a sufficiently high likelihood that it represents a security related event (e.g., bad or

[28] *See, e.g.*, Blacklisting & Whitelisting Clients (*available at* http://help.fortinet.com/fweb/550/Content/FortiWeb/fortiweb-admin/blacklisting.htm) ("**Trusted IPs** — Almost always allowed to access to your protected web servers. Trusted IPs are exempt from many (but not all) of the restrictions that would otherwise be applied by a server policy.") (last accessed 6/13/2018).

[29] *See, e.g.*, FortiSandbox – Administration Guide (*available at* https://docs.fortinet.com/uploaded/files/3244/fortisandbox-v2.3.0-administration-guide.pdf) (last accessed 6/13/2018)

suspicious), allowing for the generation of an appropriate alert. The Fortinet Security Appliances can use the alert to automatically block the underlying network traffic to which the derived status data/alert relates. For example, the Fortinet Security Appliances identify status data as representing a malicious event using techniques such as looking for known attack signatures. Black listing could be applied, for example, by filtering based on an IP address extracted by the sensor during the collection of status information. More specifically, requests can be blocked based upon their source IP address, their current reputation known to the Fortinet Security Appliances, or a country or region with which the IP address is associated:

Blacklisting & Whitelisting Clients[30]

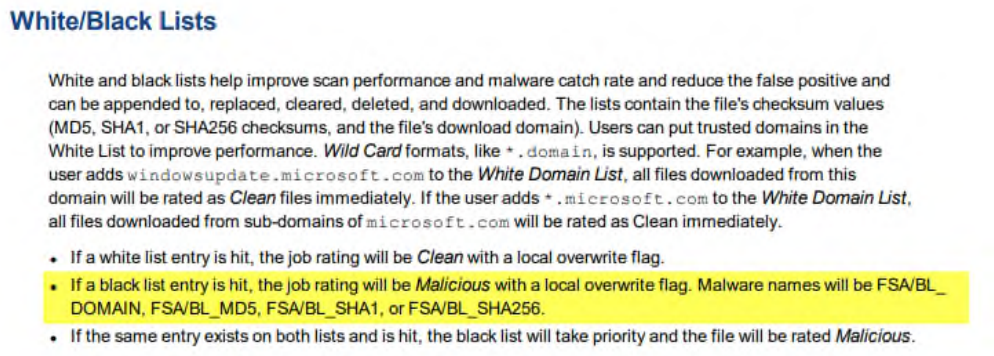
98. Requests from blacklisted IP addresses would receive a warning message as shown below:

Blacklisting & Whitelisting Clients[31]

[30] Id.

[31] Blacklisting & whitelisting clients (*available at* http://help.fortinet.com/fweb/550/Content/FortiWeb/fortiweb-admin/blacklisting.htm) (last accessed 6/13/2018).

99. In addition, blacklisting can also be applied to domain names. For example, untrusted domain names that are a hit to the black list will be flagged as "Malicious."



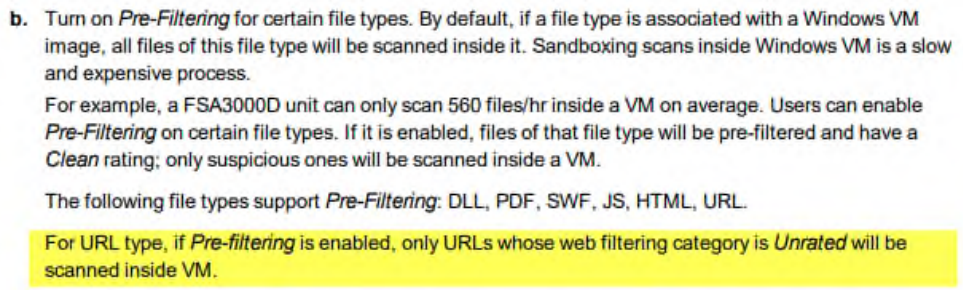
White/Black Lists

White and black lists help improve scan performance and malware catch rate and reduce the false positive and can be appended to, replaced, cleared, deleted, and downloaded. The lists contain the file's checksum values (MD5, SHA1, or SHA256 checksums, and the file's download domain). Users can put trusted domains in the White List to improve performance. *Wild Card* formats, like `*.domain`, is supported. For example, when the user adds `windowsupdate.microsoft.com` to the *White Domain List*, all files downloaded from this domain will be rated as *Clean* files immediately. If the user adds `*.microsoft.com` to the *White Domain List*, all files downloaded from sub-domains of `microsoft.com` will be rated as Clean immediately.

- If a white list entry is hit, the job rating will be *Clean* with a local overwrite flag.
- If a black list entry is hit, the job rating will be *Malicious* with a local overwrite flag. Malware names will be FSA/BL_DOMAIN, FSA/BL_MD5, FSA/BL_SHA1, or FSA/BL_SHA256.
- If the same entry exists on both lists and is hit, the black list will take priority and the file will be rated *Malicious*.

FortiSandbox – Administration Guide[32]

100. Data neither discarded nor selected by filtering represents status data that is indeterminate in that it has not been selected or discarded by the initial analysis. The indeterminate data can include, by way of example, domain names that are in the "unrated" category (as shown below) or executables.



b. Turn on *Pre-Filtering* for certain file types. By default, if a file type is associated with a Windows VM image, all files of this file type will be scanned inside it. Sandboxing scans inside Windows VM is a slow and expensive process.

For example, a FSA3000D unit can only scan 560 files/hr inside a VM on average. Users can enable *Pre-Filtering* on certain file types. If it is enabled, files of that file type will be pre-filtered and have a *Clean* rating; only suspicious ones will be scanned inside a VM.

The following file types support *Pre-Filtering*: DLL, PDF, SWF, JS, HTML, URL.

For URL type, if *Pre-filtering* is enabled, only URLs whose web filtering category is *Unrated* will be scanned inside VM.

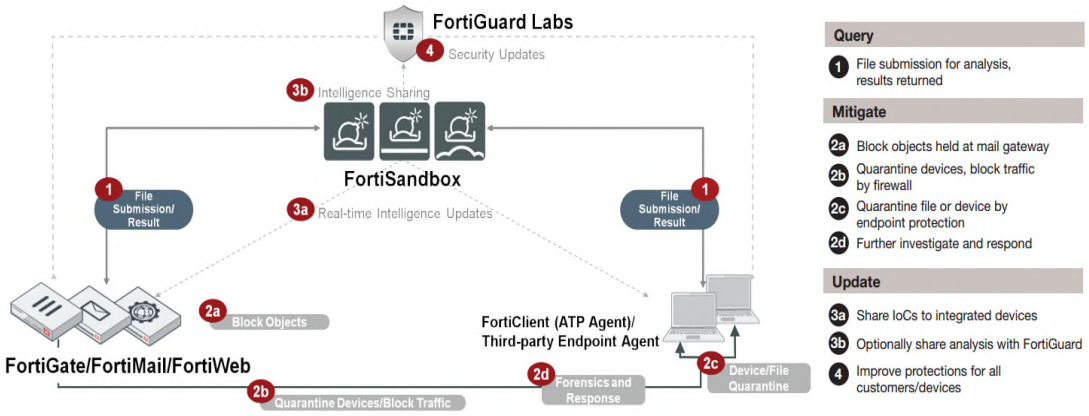
101. The Fortinet Security Appliances will deliver to the FortiSandbox the indeterminate status data to determine whether it might represent an unknown attack. The analysis of the status data by FortiSandbox is transmitted to at least two different "analyst systems" that are associated with the Fortinet security monitoring system.

[32] *See, e.g.*, FortiSandbox – Administration Guide (*available at* https://docs.fortinet.com/uploaded/files/3244/fortisandbox-v2.3.0-administration-guide.pdf) (last accessed 6/13/2018)

102. In the first scenario, FortiSandbox transmits information to FortiManager and FortiAnalyzer, which analyze data to "continually assess network activity and security posture," "constantly assess threats, trends and emerging attack vectors and techniques" and "correlate information across security products and identify areas for security improvement."[33]

103. In a second scenario, FortiSandbox transmits information to Fortinet's threat research & response labs, FortiGuard, for "in-depth analysis so that appropriate fixes that take into account all of the security layers can be done and delivered to the different security enforcement points, such as the Firewall. This may include updated AV and IPS signature, updated IP reputation database, etc."[34]

104. FortiGate contains a network card and associated systems that receives information from the analyst systems based on empirically-derived information. This is illustrated below in 3(a) which is labeled "Real-time Intelligence Update":



FortiSandbox Data Sheet[35]

105. Moreover, Fortinet notes that "FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform" including the following:

[33] *Id.* https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
[34] *Id.*
[35] FortiSandbox Data Sheet (*available at* https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf) (last accessed 6/13/2018)

FortiSandbox	Intelligence from IPS, AntiVirus, IP Reputation, Web Filtering, and FortiCare services.
FortiClient	Intelligence from Application Control, AntiVirus, Web Filtering, Vulnerability Scan, and FortiCare services.
FortiCache	Intelligence from AntiVirus, Web Filtering, Content Analysis, and FortiCare services.
FortiMail	Intelligence from AntiVirus, AntiSpam, FortiSandbox Cloud, and FortiCare services.
FortiWeb	Intelligence from Web Application Security, AntiVirus, IP Reputation, Vulnerability Scan, and FortiCare services.
FortiADC	Intelligence from IP Reputation Web Application Security, and FortiCare services.
FortiDDoS	Intelligence from IP Reputation and FortiCare services.
FortiDB	Intelligence from Database Security and FortiCare services.

FortiGuard Security Services[36]

106. The Fortinet Security Appliances dynamically modify its analysis capability during operation such that the methods of analysis are improved based on then-current intelligence.[37] Specifically, Fortinet is able to push up-to-date security intelligence to Fortinet appliances, delivering timely protection against new and emerging threats.[38]

107. Despite BT's written notice to Fortinet of Fortinet's infringement of the '641 Patent, Fortinet has not stopped its infringement. Rather, Fortinet continues to make, use, and offer its products and services in a manner which infringes the '641 Patent.

108. Fortinet's infringement of the '641 Patent has been and is willful because Fortinet has known of the '641 Patent, known that its products and services infringe the '641 Patent, and still continues to offer them in an infringing manner in disregard of BT's patent rights.

109. More particularly, following BT's notice, Fortinet has continued to infringe by supplying infringing equipment and using the claimed method to service its clients. In this

[36] FortiGuard Security Services (FortiGuard Security Services (*available at* https://isecurenet.net/wp-content/uploads/2016/06/Brochure-FortiGuard-Security-Services.pdf) (last accessed 6/8/2018)

[37] *See, e.g.*, Fortinet Advanced Threat Protection (*available at https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/atp-solution.pdf*) (last accessed 6/13/2018).

[38] *See, e.g., Id.* ("As a new threat emerges, certain detection and prevention products communicate directly for immediate, automated response. Additionally, FortiGuard Labs 24x7x365 global operations pushes up-to-date security intelligence in real time to Fortinet solutions, delivering instant protection against new and emerging threats.").

regard, Fortinet has knowingly encouraged and intended—and continues to encourage and intend—for its customers to use Fortinet products/services in infringing manners. For example, Fortinet's websites and videos advertise that "FortiSandbox is the only solution using a pre-filter" "keeping threats out without having to activate and analyze."[39] In addition, Fortinet notes that it is able to "correlate information across security products and identify areas for security improvement" and that its "[t]hreat [i]ntelligence…[will] constantly assess threats, trends and emerging attack vectors and techniques."[40]

110. Furthermore, Fortinet markets the value of pre-filtering to counter the "processor and time intensive" nature of sandboxing noting that the process would otherwise be "slow" and "slow is a problem."[41]

111. Fortinet also specifically encourages sandboxing pre-filtering: "It is recommended to turn on sandboxing pre-filtering for web files."[42]

112. Fortinet does not have a license or permission to use the claimed subject matter.

113. BT has been damaged and continues to be damaged by Fortinet's infringement.

114. BT is entitled to recover from Fortinet the damages sustained by BT as a result of Fortinet's wrongful acts in an amount subject to proof at trial and up to three times its actual damages due to Fortinet's willful infringement.

---

[39] FortiSandbox webpage (*available at* https://www.fortinet.com/products/sandbox/fortisandbox.html) (last accessed 6/13/2018).
[40] MSSP Advanced Threat Protection Service (*available at* https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/MSSP-ATP.pdf) (last accessed 6/13/2018).
[41] FortiSandbox webpage (*available at* https://www.fortinet.com/products/sandbox/fortisandbox.html) (last accessed 6/13/2018).
[42] FortiSandbox Administration Guide, v 2.4.1 (*available at* https://docs.fortinet.com/uploaded/files/3801/fortisandbox-v2.4.1-administration-guide.pdf) (last accessed 6/13/2018).

115. BT is suffering and will continue to suffer irreparable harm for which there is no adequate remedy at law as a result of Fortinet's infringement of the '641 Patent. By way of example, Fortinet's infringing products and/or services compete with those of BT Americas. Unless enjoined, Fortinet will continue its infringing conduct.

COUNT III
(INFRINGEMENT OF U.S. PATENT NO. 7,370,358)

116. BT repeats and re-alleges the allegations contained in Paragraphs 1 through 53 above as if fully set forth herein.

117. Fortinet has directly infringed and continues to directly infringe, literally or under the doctrine of equivalents, one or more claims of the '358 Patent in violation of 35 U.S.C. §271(a) by making, using, offering to sell, selling (directly or through intermediaries), and/or importing, in this District and elsewhere in the United States, various Fortinet products and services including, but not limited to, FortiGate, FortiWeb, FortiMail, FortiSandbox, FortiManager, FortiClient, and/or FortiGuard.

118. For example, Fortinet infringes claim 50 of the '358 Patent, which provides as follows:

> A method comprising computer security for a plurality of inter-communicating software agents together forming a plurality of agent groups, each agent corresponding with other agents in its respective group but not with agents in other groups via a message-exchange system including the exchange of group specific tags, the agents cooperating to perform said method comprising:
>
> comparing at each agent actual behavior patterns of an agent's own group with stored expected behavior patterns; and
>
> each agent communicating by a message-exchange system in which, when one agent determines that a security threat does or may exist, that agent sends a warning message, including an anomaly pattern indicative of the threat, to other agents in its group.

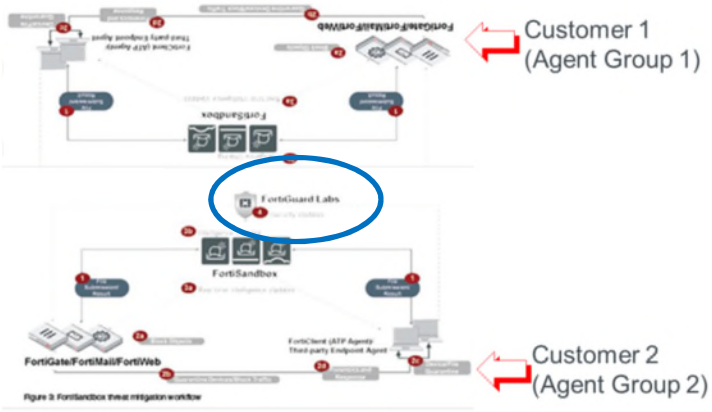
119. Fortinet offers a series of products that are employed to secure a customer network. These products contain software that operates in a distributed manner to monitor, detect and share attack signatures (e.g., "software agents").

120. Software agents are pre-loaded on a hardware appliance, such as the FortiGate. Other software agents are loaded on a customer's endpoint device, such as the FortiClient. The software agents (circled in red in the below diagram) are located at a particular Fortinet customer site and are associated with the same FortiSandbox to form an "agent group" (circled in green below).

FortiSandbox Data Sheet[43]

121. Fortinet connects the various customer-specific agent groups through the use of FortiGuard (circled in blue below). For example, two groups of agents are shown in the below diagram reflecting two Fortinet customer installations (with the top network image being represented as a structural mirror to the bottom network image). The two agent groups are connected through FortiGuard:

[43] FortiSandbox Data Sheet (*available at* https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf) (last accessed 6/13/2018)



122. FortiSandbox operates as a message exchange system that facilitates communications within various agent groups. For example, an agent located at a particular Fortinet customer network talks to members of that group (through the FortiSandbox) and does not communicate with agents located on other customer networks ("each agent corresponding with other agents in its respective group but not with agents in other groups"). Further, each agent group has a unique identifier of its associated Sandbox, known as a "devid," that uniquely identifies the agent group. This "devid" is an example of a "group specific tag" in that is unique to a group of agents.[44]

123. FortiGate uses heuristic scanning to identify files that behave in a manner expected of viruses.[45] Similarly, FortiClient has a "Heuristic" anti-virus scan mode that looks at the behavior of code to determine whether it is suspicious or legitimate.[46] In each case, the agent is comparing a stored expected behavior pattern (*i.e.*, how a non-malicious file of a given type would be expected to behave when it executed on a given client) with the actual behavior of the

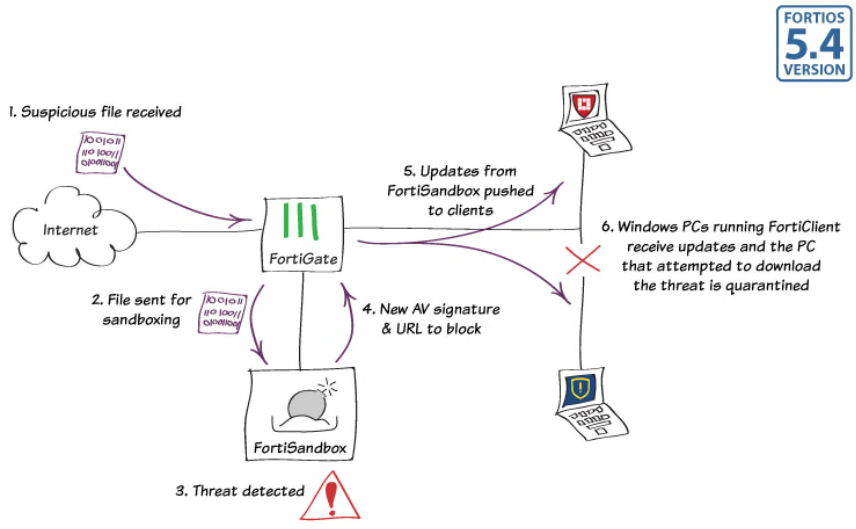
[44] *See e.g.*, http://docs.fortinet.com/uploaded/files/2952/fortisandbox-v2.2.0-log-reference.pdf at p. 6 (last accessed 6/13/2018)
[45] *See* http://kb.fortinet.com/kb/viewContent.do?externalId=11008. (last accessed 6/13/2018)
[46] *See* http://kb.fortinet.com/kb/documentLink.do?externalID=FD31397. (last accessed 6/13/2018)

file to identify divergences ("comparing at each agent actual behavior patterns of an agent's own group with stored expected behavior patterns").

124. When a FortiClient or a FortiGate determines that a threat exists (or may exist), it triggers the generation of a "warning message" by sending the suspicious file to the FortiSandbox.

FortiSandbox Data Sheet[47]

125. As a result of the submissions made by the agents, the FortiSandbox generates signature updates which are sent back to the agents in the group:



Sandboxing with FortiSandbox and FortiClient[48]

[47] FortiSandbox Data Sheet (*available at* https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf) (last accessed 6/13/2018)

126. The message sent by the Sandbox to all of the members of the agent group are "warning messages" that includes "Indicators of Compromise" (IOC) which are "anomaly patterns indicative of the threat."

127. Fortinet does not have a license or permission to use the claimed subject matter.

128. BT has been damaged and continues to be damaged by Fortinet's infringement.

129. BT is entitled to recover from Fortinet the damages sustained by BT as a result of Fortinet's wrongful acts in an amount subject to proof at trial.

COUNT IV
(INFRINGEMENT OF U.S. PATENT NO. 7,693,971)

130. BT repeats and re-alleges the allegations contained in Paragraphs 1 through 53 above as if fully set forth herein.

131. Fortinet has directly infringed and continues to directly infringe, literally or under the doctrine of equivalents, one or more claims of the '971 Patent in violation of 35 U.S.C. §271(a) by making, using, offering to sell, selling (directly or through intermediaries), and/or importing, in this District and elsewhere in the United States, various Fortinet products and services including, but not limited to, FortiGate, FortiClient, and/or FortiManager.

132. For example, Fortinet infringes claim 12 of the '971 Patent, which provides as follows:

> A method of managing a computer network having a plurality of network components comprising distributing policy-based management across the network using a distributed policy-based manager comprising a plurality of distributed management agents arranged in a hierarchy and being associated with sub-networks of said network, said method comprising:

[48] Sandboxing with FortiSandbox and FortiClient (*available at* http://cookbook.fortinet.com/sandboxing-fortisandbox-forticlient-54/) (last accessed 6/13/2018)

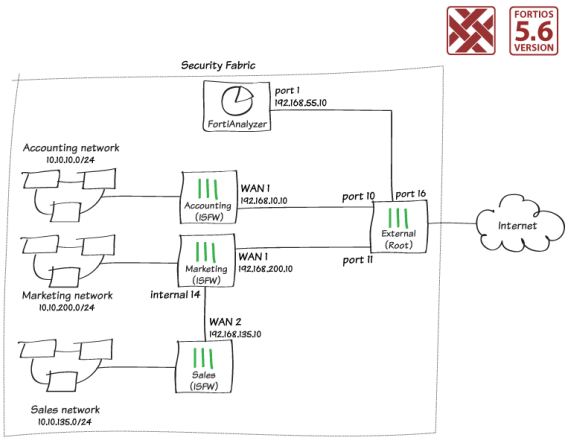
registering local network components at each of said agents,

identifying and storing at each of said agents one or more roles associated with each component, and

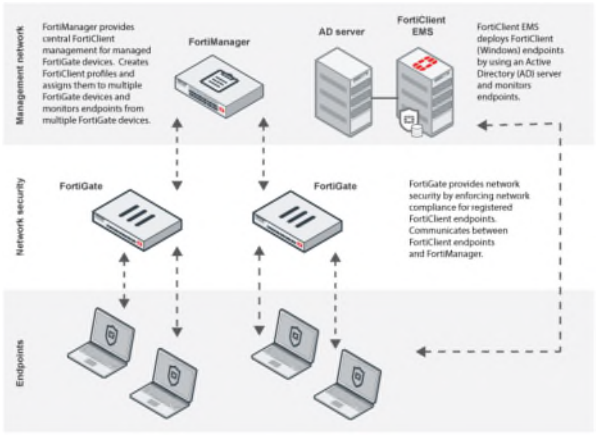
obtaining at each of said agents policies relevant to the stored roles of the registered components,

wherein each of the policies are locally stored and specify a subject role identifying the components in the system which are expected to respond to a policy and an action element specifying an action to be carried out.

133. Fortinet offers a series of products that manages endpoint terminals executing a FortiClient. In a first infringing configuration, a FortiGate serves as the manager for one or more other FortiGates (see left schematic below). In a second infringing configuration, a FortiManager serves as the manager of one or more FortiGates (see right schematic below).



First Configuration [49]



Second Configuration[50]

134. The networks in both configurations include plural endpoint terminals ("network components") which run the FortiClient software application.

[49] Security Fabric installation and audit (*available at* http://cookbook.fortinet.com/security-fabric-installation-56/) (last accessed on 6/13/2018)

[50] FortiManager – Administration Guide Version 5.4.3 (8/17/2017) (available at http://docs.fortinet.com/uploaded/files/3738/FortiManager-5.4.3-Administration-Guide.pdf) (last accessed on 6/13/2018)

135. The FortiGate firewalls use "FortiClient profiles" as policies to manage ("policy based management") the FortiClient equipped endpoint terminals. Each FortiClient profile sets out rules that govern choices in the behavior of the respective FortiClient Endpoint terminal in response to events set out in the FortiClient profile.[51]

136. The policy-based management is divided amongst multiple FortiGates ("distributed"), with each FortiGate managing a different sub-network of FortiClient equipped endpoint terminals. As such, the FortiClient equipped endpoint terminals are managed by multiple FortiGate firewalls, each of which manages a different subset of the endpoint terminals, which govern their own behavior based on policies.

137. In both configurations, FortiGate firewalls are arranged in a hierarchy and are associated with sub-networks of said network. With regard to the first configuration, the FortiGate firewalls are arranged with one dominant FortiGate acting as the network edge firewall and two subordinate internal segmentation FortiGate firewalls.[52] Each of the subordinate internal segmentation firewalls manages its respective subnetwork of FortiClient equipped endpoint terminals. With regard to the second configuration, the FortiGate firewalls are managed by a FortiManager, which enable provisioning, configuration and update management of a network of FortiGate firewalls.[53]

[51] http://docs.fortinet.com/uploaded/files/2827/fortios-handbook-54.pdf (FortiOs™ Handbook FortiOS 5.4.5) (last accessed 6/13/2018)
[52] See Security Fabric installation and audit (*available at* http://cookbook.fortinet.com/security-fabric-installation-56/) (last accessed on 6/13/2018)
[53] FortiManager – Administration Guide Version 5.4.3 (8/17/2017) (available at http://docs.fortinet.com/uploaded/files/3738/FortiManager-5.4.3-Administration-Guide.pdf) (last accessed on 6/13/2018)

138. Each FortiGate firewall monitors the network and gathers and stores ("registers") information about the endpoint terminals, including the endpoint terminals it manages ("local network components").

139. FortiGate monitors the network and gathers information about the endpoint terminals operating on the network including the "role" of each endpoint terminal. More specifically, FortiGate detects and stores the "operating system," (also called "device type") and "user name." Further, device type groups (based on operating system) and/or user groups can be created for purposes of assigning endpoint profiles.

140. FortiClient profiles ("policies") are "obtained" at each of the FortiGate firewalls in one of the following three ways. First, profiles created manually or an existing policy are assigned to a user group or device group. Second, FortiManager deploys profiles to FortiGates, which then push the profiles to the respective FortiClient. Third, profiles are predefined and by default are assigned to a default group.

141. Each of the FortiClient profiles is locally stored at the respective FortiGate at the time it is created or received from another FortiGate or FortiManager.[54] The FortiGate profile is then transferred to the FortiClient to which it pertains. Further, the FortiClient profile stored within the FortiGate firewall unit is correlated with the specific device type group (e.g., "Windows and Mac OS") and/or user group to which the FortiClient profile must be deployed ("specify a subject role identifying the components in the system which are expected to respond to a policy"). The recipient Endpoint terminal, as identified by the device group, and/or user group of the FortiClient profile takes a specific action as specified in the profile.

142. Fortinet does not have a license or permission to use the claimed subject matter.

[54] See FortiOs™ Handbook FortiOS 5.4.5 (*available at* http://docs.fortinet.com/uploaded/files/2827/fortios-handbook-54.pdf) (last accessed 6/13/2018)

143. BT has been damaged and continues to be damaged by Fortinet's infringement.

144. BT is entitled to recover from Fortinet the damages sustained by BT as a result of Fortinet's wrongful acts in an amount subject to proof at trial.

COUNT V
(INFRINGEMENT OF U.S. PATENT NO. 7,774,845)

145. BT repeats and re-alleges the allegations contained in Paragraphs 1 through 53 above as if fully set forth herein.

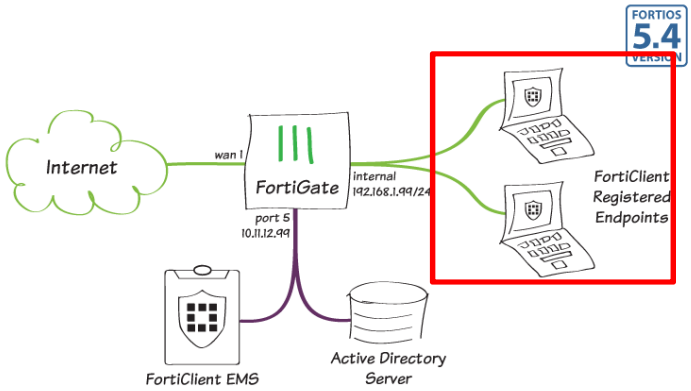
146. Fortinet has directly infringed and continues to directly infringe, literally or under the doctrine of equivalents, one or more claims of the '845 Patent in violation of 35 U.S.C. §271(a) by making, using, offering to sell, selling (directly or through intermediaries), and/or importing, in this District and elsewhere in the United States, various Fortinet products and services including, but not limited to, FortiGate, FortiClient, FortiClient EMS, and/or FortiAnalyzer.

147. For example, Fortinet infringes claim 1 of the '845 Patent, which provides as follows:

> A computer security system for use in a network environment comprising at least a group of user computers arranged to communicate over a network, the system comprising:
>
> a warning message exchange system operable to allow communications from the group of user computers of warning messages relating to a piece or set of suspect data identified by one or more of the group of user computers as a possible security threat;
>
> an identity generator operable to generate an identifier of the piece or set of suspect data;
>
> a message counting system operable to maintain a count for every particular piece or set of suspect data based on a number of warning messages communicated over the network relating to each of the piece or set of suspect data; and

> a network security system operable to act in respect of any particular piece or set of suspect data when the count maintained therefor is substantially equal to or greater than at least one threshold value, wherein the threshold value is greater than one.

148. In general, Fortinet offers a series of products that collectively and individually function as a "computer security system." The Fortinet computer security system operates on customer networks that have multiple endpoints ("at least a group of user computers arranged to communicate over a network"). An exemplary graphical representation of a portion of the Fortinet "computer security system" is shown below:



Sandboxing with FortiSandbox and FortiClient[55]

149. As shown in this image above (see red box), a number of FortiClient Registered Endpoints (running on "a group of user computers") communicate over a network with both a FortiGate and a server running FortiClient EMS software, both of which facilitate the management of the various endpoints.

150. The FortiAnalyzer operates as a warning message exchange system such that FortiClients, upon detection of an actual or possible security threat, will send "warning messages" to the FortiAnalyzer that detail what the FortiClient has detected.

---

[55] Sandboxing with FortiSandbox and FortiClient (*available at* http://cookbook.fortinet.com/sandboxing-fortisandbox-forticlient-54/) (last accessed 6/13/2018)

Upload Logs to FortiAnalyzer/FortiManager		Turn on to upload FortiClient logs to the FortiAnalyzer or FortiManager device at the specified address or hostname.
	Upload Traffic Logs	Enable to upload traffic logs.
	Upload Vulnerability Logs	Enable to upload vulnerability logs.
	Upload Event Logs	Enable to upload event logs.
	IP Address/Hostname	Enter the IP address. When connecting to FortiAnalyzer 5.6+, use the format *https://FAZ-IP:port/logging*. Otherwise, use the format *https://FAZ-IP/jsonrpc/fazapi/logs*.
	SSL Enabled	Enable SSL.
	Upload Schedule (minutes)	Configure the upload schedule in minutes.
	Log Generation Timeout (seconds)	Configure the log generation timeout in seconds.
	Log Retention (days)	Configure the duration of time to retain logs in days.

FortiClient EMS at P. 82.

151. The log messages include "warning messages relating to a piece or set of suspect data identified by one or more of the group of user computers as a possible security threat." For example, the logs can include "alerts" generated as a result of an anti-virus scan.

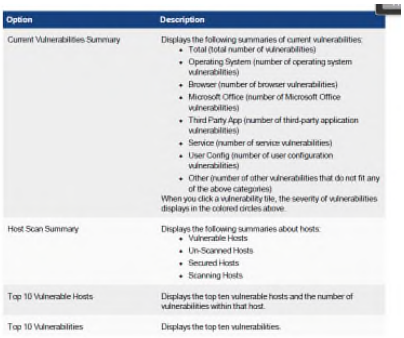
Logging Level	Description
Emergency	The system becomes unstable.
Alert	Immediate action is required.

FortiClient, Logging[56]

152. The FortiClient contains an "identity generator" such that an Indicator of Compromise (IOC) of a piece of "suspect data" is generated and included in various log messages.[57] Further, the FortiSandbox (an analytics product designed to operatively connect to the FortiClient and FortiGate) also generates an IOC, which includes a hash or checksum of malware detected.[58]

[56] See FortiClient, Logging (*available at* http://help.fortinet.com/fclient/olh/5-4-1/Content/FortiClient-5.4-Admin/1300_Settings/1015_Logging+.htm) (last accessed 6/13/2018)
[57] *See* Logging and Reporting, FortiOS Handbook v3 at p. 40 (*available at* http://docs.fortinet.com/uploaded/files/1048/fortigate-loggingreporting-40-mr3.pdf) (last accessed 6/13/2018)
[58] *See* FortiSandbox-v2.4.1-administration-guide.pdf, pp. 95 (*available at* http://docs.fortinet.com/uploaded/files/3801/fortisandbox-v2.4.1-administration-guide.pdf) (last accessed 6/13/2018)

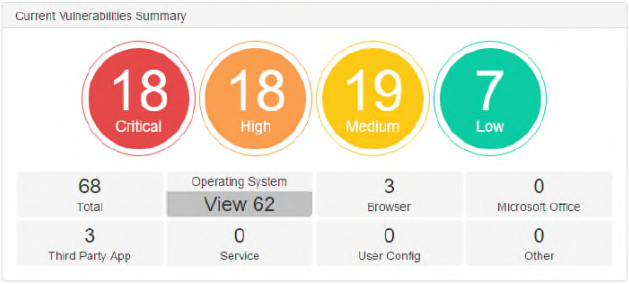
153. Upon information and belief, as shown below, the FortiClient EMS maintains counts of various vulnerability-scan related information. This count is calculated based on the number of received warning messages.



Option	Description
Current Vulnerabilities Summary	Displays the following summaries of current vulnerabilities: • Total (total number of vulnerabilities) • Operating System (number of operating system vulnerabilities) • Browser (number of browser vulnerabilities) • Microsoft Office (number of Microsoft Office vulnerabilities) • Third Party App (number of third-party application vulnerabilities) • Service (number of service vulnerabilities) • User Config (number of user configuration vulnerabilities) • Other (number of other vulnerabilities that do not fit any of the above categories) When you click a vulnerability tile, the severity of vulnerabilities displays in the colored circles above.
Host Scan Summary	Displays the following summaries about hosts: • Vulnerable Hosts • Un-Scanned Hosts • Secured Hosts • Scanning Hosts
Top 10 Vulnerable Hosts	Displays the top ten vulnerable hosts and the number of vulnerabilities within that host.
Top 10 Vulnerabilities	Displays the top ten vulnerabilities.

FortiClient EMS v 1.2.1 Administration Guide [59]

154. In addition, the below screenshot shows counts of all of the various detected vulnerabilities grouped by severity level.

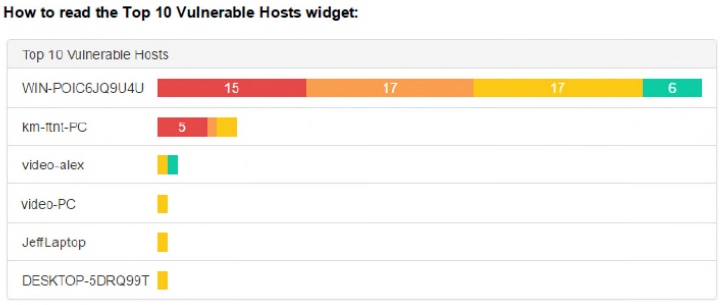


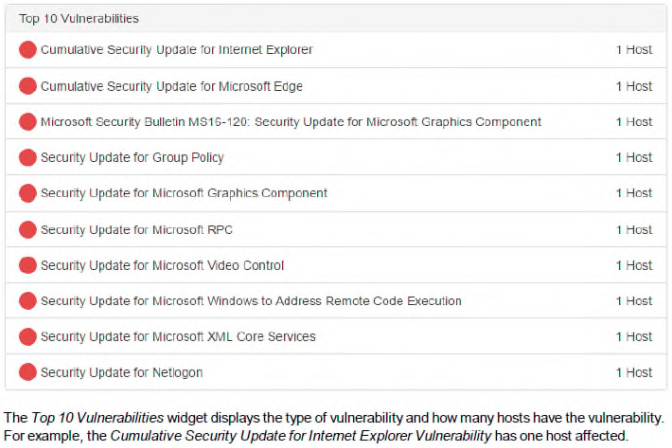
FortiClient EMS v 1.2.1 Administration Guide[60]

155. Further still, an additional count identifies the number of vulnerabilities on each host and by vulnerability. For example, as shown in the diagram on the left, at the first host, WIN-POIC6JQ9U4U, there are: 15 critical vulnerabilities; 17 high risk vulnerabilities; 17

[59] See FortiClient EMS v 1.2.1 Administration Guide (*available at*: http://docs.fortinet.com/uploaded/files/3824/forticlient-ems-v1.2.1-admin-guide.pdf) (last accessed 6/13/2018)
[60] FortiClient EMS v 1.2.1 Administration Guide at p. 41 (*available at*: http://docs.fortinet.com/uploaded/files/3824/forticlient-ems-v1.2.1-admin-guide.pdf) (last accessed 6/13/2018)

medium risk vulnerabilities; and 6 low risk vulnerabilities. As shown in the right, a count is maintained by vulnerability.





Count by Host[61] **Count by Vulnerability**[62]

156. The FortiAnalyzer is designed to operate "event handlers" which trigger action at some numbers of alerts which are greater than one.

Field	Description
Generate alert when at least	Enter threshold values to generate alerts. Enter the number, in the first text box, of each type of event that can occur in the number of minutes entered in the second text box.

FortiAnalyzer – Administration Guide, v. 5.4.0[63]

157. Fortinet does not have a license or permission to use the claimed subject matter.

158. BT has been damaged and continues to be damaged by Fortinet's infringement.

159. BT is entitled to recover from Fortinet the damages sustained by BT as a result of Fortinet's wrongful acts in an amount subject to proof at trial.

---

[61] *Id.*
[62] *Id.*
[63] FortiAnalyzer – Administration Guide, v. 5.4.0 (*available at* http://docs.fortinet.com/uploaded/files/2885/FortiAnalyzer-5.4.0-Administration-Guide.pdf) (last accessed 6/13/2018)

PRAYER FOR RELIEF

WHEREFORE, BT respectfully requests that this Court enter judgment against Fortinet, granting BT the following relief:

A. A judgment holding Fortinet liable for direct infringement of the Patents-In-Suit;

B. All damages available under 35 U.S.C. § 284 resulting from Fortinet's infringement of the Patents-in-Suit in an amount to be proven at trial, but no less than a reasonable royalty, together with pre-judgment interest and post-judgment interest;

C. An order and judgment permanently enjoining Fortinet from further acts of infringement of the '237 and '641 Patents;

D. A judgment holding Fortinet's infringement of the '237 and '641 Patents to be willful and deliberate, and a trebling of damages pursuant to 35 U.S.C. § 284;

E. A judgment holding this to be an exceptional case, and an award to BT for its attorneys' fees, costs and expenses incurred prosecuting this action pursuant to 35 U.S.C. § 285; and

F. Such other and further relief as the Court deems just and equitable.

DEMAND FOR JURY TRIAL

BT demands a trial by jury of all issues so triable.

POTTER ANDERSON & CORROON LLP

OF COUNSEL:

James H. Shalek
Baldassare Vinti
Nolan M. Goldberg
Fabio E. Tarud
PROSKAUER ROSE LLP
Eleven Times Square
New York, New York 10036
(212) 969-3000

By: */s/ Philip A. Rovner*
Philip A. Rovner (#3215)
Jonathan A. Choa (#5319)
Hercules Plaza
P.O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com
jchoa@potteranderson.com

Attorneys for Plaintiff British Telecommunications plc and BT Americas, Inc.

Dated: July 10, 2018
5862871