UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. and FORTINET, INC.,
Petitioners,

v.

INFOEXPRESS INC.,
Patent Owner.

IPR2024-00676
U.S. Patent No. 8,677,450

DECLARATION OF DR. ERIC COLE IN SUPPORT OF THE PATENT OWNER'S PRELIMINARY RESPONSE TO THE PETITION



CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 1 of 42

TABLE OF CONTENTS

I. INTRODUCTION *1*

II. QUALIFICATIONS *2*

III. SCOPE OF WORK *9*

IV. BASIS FOR OPINIONS *9*

A. Validity and Infringement **9**

B. Level of Ordinary Skill in the Art **11**

C. Anticipation **12**

D. Obviousness **15**

V. OVERVIEW OF THE CHALLENGED PATENT *18*

VI. THE ASSERTED PRIOR ART REFERENCES *20*

A. U.S. Patent No. 2004/0111520 ("Krantz") **20**

B. U.S. Patent No. 2004/0107360 ("Herrmann") **24**

VII. SUMMARY OF OPINIONS *27*

VIII. CONCLUSION *39*

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 2 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 2 of 42

I, Eric Cole, of Ashburn, Virginia, declare that:

I. INTRODUCTION

1. I have been retained by InfoExpress, Inc. ("InfoExpress", "Owner", "Respondent") to offer opinions regarding claims 1–4, 7–10, 14, 16, 22, 23, 25 and 27 of U.S. Patent No. 8,677,450 (the '450 Patent"). I submit these opinions in support of Respondent's claim that the Challenged Claims of the '450 Patent are patentable under 35 U.S.C. §103, even in view of the references asserted by Petitioner. I am prepared to testify about the matters set forth herein. All the facts and my opinions herein are understood to be true and correct and are within my personal knowledge.

2. As stated, I have been requested by counsel for InfoExpress to provide opinions regarding patentability of the Challenged Claims of the '450 Patent in response to the claims made by Petitioners in the Petition.

3. This declaration and my opinions contained herein are based on information currently available to me. I may continue my investigation as new information is provided. Accordingly, I reserve the right to supplement and/or amend my opinions contained herein. I also reserve the right to provide opinions regarding any other patents at a later date.

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 3 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 3 of 42

II. QUALIFICATIONS

4. My academic credentials include a master's degree in computer science and a doctorate in information security, and I have worked in the cyber and technical information security industry for over twenty-five years. The details of my education and experience are summarized in my curriculum vitae ("CV"), which is provided as Exhibit A. My CV also includes a list of my publications over the past ten years.

5. I have worked in computer security for over twenty-five years. To briefly summarize my career, I have: 1) been responsible for the security of sensitive government projects; 2) managed security at major private sector companies; 3) consulted for major private sector companies; 4) been actively involved in designing, building, and deploying intrusion detection systems; 5) worked on protecting and securing critical information including trade secrets; 6) continually taught and written about cybersecurity.

6. I am the founder and president of Secure Anchor Consulting, LLC, located in Ashburn, Virginia. Secure Anchor Consulting provides cybersecurity consulting services and lead research and development initiatives to advance information systems security. Many of the clients I work with are responsible for

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 4 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 4 of 42

protecting sensitive client and/or consumer information and implementing effective security.

7. At Secure Anchor Consulting, I also actively work on incidents, and I have a detailed understanding of measures that organizations can take to both prevent and detect breaches. In addition, I have worked with organizations to design, build, and implement security measures that would be classified as both fixes and compensating controls, and I have detailed knowledge of the effort that is required to implement various remediation measures.

8. I worked for the U.S. government for eight years as an employee and have held various contracting jobs with government agencies, which involved working with classified information. I have worked for a wide range of government organizations, including the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Central Intelligence Agency (CIA), the Department of Energy, the Department of Defense (DOD), the Treasury Department, the Secret Service, and the Nuclear Regulatory Commission (NRC). I have held various top-secret security clearances with the DOD, the CIA, and the NRC. I was also involved in funded research from the Defense Advanced Research Projects Agency (DARPA), an agency of the DOD responsible for the development of new intrusion

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 5 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 5 of 42

detection technologies for use by the military. During this time, I have reviewed, edited, and created numerous security policies. On several occasions, I have also reviewed the reasonableness of measures intended to protect and secure Confidential Information through various types of documentation to include policies, procedures, standards, and baselines.

9. While serving as a Senior Officer for the CIA as Program Manager / Technical Director for the Internet Program Team with the Office of Technical Services, I implemented the Internet Program Team which designs, develops, tests, and deploys Internet security products in three- to six-month intervals. In this role, I received a letter of appreciation from the Director of Central Intelligence and six Exceptional Performance Awards.

10. As a member of the Information Security Assessment Team with the Office of Security, I evaluated and performed security assessments of network operating systems to identify potential vulnerabilities and solutions. I also designed a large-scale auditing system with an automated review capability and worked on several virus investigations for the Office of Security.

11. In my role as Chief Information Officer for the American Institutes for Research, I repaired and developed IT infrastructures for various organizations. I

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 6 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 6 of 42

was also responsible for building out the entire data classification program to ensure that critical and proprietary data was properly protected and secured. I was also one of the principal leads on research funding from DARPA. In this role, I was responsible for understanding the current state of the art in intrusion detection and designing and building a new cybersecurity system that could catch attacks that were targeting organizations.

12. As Chief Scientist and Senior Fellow for Lockheed Martin, I performed research and development in information systems security. I also specialized in evaluating and designing secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. At Lockheed Martin, I served as a technical advisor in high-profile security projects for government clients including the DOD, the FBI Sentinel case management systems, Department of Homeland Security Enterprise Acquisition Gateway for Leading Edge solutions, Jet Propulsion Labs, Hanford Labs, and FBI Information Assurance Technology Infusion programs.

13. As Chief Technical Officer for McAfee, I executed the strategy for technology platforms, partnerships, and external relationships to establish product vision and achieve McAfee's goals and business strategies. In this capacity, I

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 7 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 7 of 42

worked closely with groups tasked with the development of intellectual property. While at McAfee, I worked with many business customers responsible for protecting clients' information and helping them implement effective security solutions.

14. I was a fellow and instructor for twenty years with the SANS Institute, a research and education organization consisting of information security professionals. SANS is the largest source for information security training and security certifications in the world. I am an author of several security courses, such as SEC401-Security Essentials and SEC501-Enterprise Defender. SEC401-Security Essentials is a required course for agents of the FBI and the NSA. These courses have been taken by over 30,000 people, and I have taught more than 50% of these students via live and online training. The courses that I have written have multiple modules and lessons on security policies, employee agreements, and protection of intellectual property. As one of the top-rated instructors at SANS, I have delivered keynote addresses around the world.

15. I am a member of the European InfoSec Hall of Fame, a professional membership awarded by nomination and election by a panel of industry experts.

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 8 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 8 of 42

16. I hold a Certified Information System Security Professional (CISSP) certification and was the creator of the Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC).

17. I am a contributing author of "Securing Cyberspace for the 44th President" and served as a Commissioner on cybersecurity for President Obama. My Nine books on cybersecurity include "Online Danger," "Network Security Bible - 2nd Edition," "Advanced Persistent Threat," and "Insider Threat," which have become recognized as industry-standard sources. They are used in many classrooms and colleges around the world as authoritative texts on cybersecurity. I have also published several articles in the field.

18. The focus of my work over the last ten years has been on data protection for commercial organizations. I am very familiar with best practices in cybersecurity and have developed many of the standard practices.

19. Today, my consulting efforts help organizations properly protect client information and relate to various alternative methods of security that can be implemented. This includes hardening of systems, securing servers, proper configuration, patching, and compensating controls. In cases where a fix cannot be made because it would negatively impact the business, I have extensive experience

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 9 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 9 of 42

in understanding various compensating controls as an alternative to minimize the risk to an acceptable level and how to implement those controls.

20. I routinely help clients develop and implement company-wide policies, training, and best practices to prevent potential cybersecurity incidents. My work addresses threats from both internal and external sources, including accidental and intentional incidents.

21. I have led, and been involved in working on, responses to many cybersecurity incidents. This includes performing root cause analysis, verifying the reasonableness of security measures, and validating the implementation of additional remediation measures.

22. In my consulting work and in the various positions that I have held, I have been responsible for protecting organizations to minimize and prevent data breaches, in addition to responding to breaches post detection. I have a very detailed understanding of what is and is not a reasonable level of security based on the hundreds of organizations with which I have worked and the various security task forces with which I have been involved.

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 10 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 10 of 42

III. SCOPE OF WORK

23. I have been asked to consider and provide my opinions on the Challenged Claims of the '450 Patent, including the technical subject matter and the application of various references relied upon by the Petitioners. In particular, I have been asked to consider what one of ordinary skill in the art would have understood from the claims and specification of the Challenged Patent, whether certain references disclose or suggest the features recited in the claims of the Challenged Patent.

24. I am compensated at a rate of $800/hour for my work. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of any proceeding.

IV. BASIS FOR OPINIONS

25. My opinions set forth below are based on my education, training, experience, and the content of the references considered. My opinions are further based on the Petition and materials submitted by Petitioners.

A. Validity and Infringement

26. I have been informed that InfoExpress' patents, including the '450 Patent, are presumed to be valid by virtue of having been issued by the United States

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 11 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 11 of 42

Patent and Trademark Office on March 18, 2014. Accordingly, I understand that Fortinet and Cisco, as IPR petitioners, bear the burden of proving by a preponderance of the evidence that the InfoExpress Patents, including the '450 Patent, are unpatentable. I am not presently aware of any contention by Fortinet or Cisco that any of the Challenged Claims are invalid, other than their general allegation the claims are unpatentable as obvious under 35 U.SC. § 103 in view of references Krantz and/or Herrmann (the "Asserted References"). If Fortinet or Cisco later offer any additional contentions that the '450 Patent is invalid, I reserve the right to address any such contentions and provide my responsive opinions.

27. I have been informed that the claims of a patent measure its scope and that each patent claim defines a separate invention. I have been further informed that a patent includes a written description of one or more preferred embodiments of the invention. With respect to the '450 Patent, I have considered the scope of the patent claims according to the plain and ordinary meaning of the claims when read in view of the specification and drawings.

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 12 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 12 of 42

B. Level of Ordinary Skill in the Art

28. My opinions are provided based on what a person of ordinary skill in the art in the technical field of the purported invention would have understood at the time of the purported invention of the Challenged Patent.

29. I have been informed and understand that the content of a patent and prior art should be interpreted the way a person of ordinary skill in the art would have interpreted those references at the time of the invention of the patent. I understand that the person of ordinary skill is a hypothetical concept referring to one who thinks along the lines of conventional wisdom at the time.

30. I was asked to provide an opinion as to the level of one of ordinary skill in the art pertinent to the subject matter set forth in the Challenged Patent at the time of the priority date. Around the time of filing of the '450 Patent, it is my opinion that a person of ordinary skill in the art in the field of the Challenged Patent would have been a person with a bachelor's degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cybersecurity, or a person with a master's degree in one of the foregoing and at least two years of experience in the aforementioned fields. Throughout this declaration, I use the term "POSITA" to refer to a person

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 13 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 13 of 42

with these or similar qualifications. To have similar qualifications, an individual with additional education or additional industrial experience could still be of ordinary skill in the art if that additional education or experience compensates for a deficit in one of the other aspects of the requirements stated above.

31. The basis for my familiarity with the level of ordinary skill is my interaction with large numbers of workers in the computer security industry who were at this level of skill. In reaching this opinion as to the hypothetical person of ordinary skill in the art, I have considered the types of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level and professional capabilities of workers in the field.

C. Anticipation

32. I understand and have been informed that in order for an inventor to be entitled to a patent, the invention must be "new," and the inventor must not have lost his or her right to a patent by delaying filing of a patent application directed to the invention. There are a number of ways that an invention can be "anticipated"—that is, not new.

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 14 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 14 of 42

33. One such way is when the invention was already patented or described in a printed publication anywhere in the world before the date of invention by the inventor or more than one year before the earliest effective filing date of the patent application. Additionally, a patented invention may not be new if it was on sale or publicly used more than one year before the filing of an application for patent. A patented invention is also not new if it was "known" or used by others in the United States before it was invented by the patent applicants. To invalidate a patent claim based on knowledge, I understand that the knowledge must be accessible to the public. If the subject matter covered by a patent claim is found within the "four corners" of a prior art reference, the claim is said to be anticipated by that reference.

34. A patent claim can be said to be anticipated if each and every limitation of the patent claim is found either expressly or inherently in a single item of prior art. While a prior art reference need not use the same words as a patent claim to anticipate the claim, the prior art reference must describe the requirements of the claim with sufficient clarity such that a POSITA would have been able to make and use the claimed invention based on the reference and his or her knowledge in the applicable technical field.

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 15 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 15 of 42

35. The disclosure of a feature of a claimed invention can be either "express," meaning that the text, figures, or other content of a reference actually teaches the aspects of the patent claim, or the disclosure can be "inherent." An express disclosure does not need to use the same words as the patent claim being considered and does not need to be depicted in exactly the same way, but the disclosure must actually convey the claimed invention to a POSITA using some combination of words, figures, data, or other portions of the patent. I have been informed and understand that in order to establish that an element of a claim is "inherent" in the disclosure in a prior art reference, it must be clear to a person skilled in the art that the missing element is an inevitable part of what is explicitly described in the reference, and that it would have been recognized as necessarily present by a person skilled in the art. Inherency cannot be established by probabilities or possibilities, and the mere fact that something may result from a given set of circumstances is not enough to establish inherency.

36. Finally, I further understand that to anticipate a claim, the elements of the claim must be found in the prior art reference "arranged as in the claim." I have been informed that this means that the elements of the prior art reference may not be recombined in a way that is not taught in the prior art to arrive at the invention;

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 16 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 16 of 42

instead, the prior art must teach the claimed subject matter in the arrangement required by the claims.

37. While I understand that Petitioners' grounds for unpatentability are not based on anticipation, but instead, are based on obviousness, I provide the above the understanding that any disclosure which anticipates a claim also renders that claim obvious.

D. Obviousness

38. I have been informed and understand that subject matter claimed in a patent is obvious under 35 U.S.C. § 103 if a person of ordinary skill in the art at the time the alleged invention was made would have had reason to combine or modify the disclosures of one or more prior art references to arrive at the claimed subject matter. A claim may be unpatentable even if each and every claim limitation is not present or disclosed in a single prior art item.

39. I have been informed and understand that, under the doctrine of obviousness, a claim is unpatentable if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 17 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 17 of 42

subject matter pertains. A person of ordinary skill in the art is presumed to have knowledge of the relevant prior art at the time of the claimed invention.

40. I have been informed and understand that obviousness is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and secondary indicia of obviousness and non-obviousness to the extent such indicia exist.

41. I have been informed and understand the determination of whether the asserted claims would have been obvious to a person of ordinary skill in the art and, therefore, invalid is not governed by any rigid test or formula. A determination that a claim is obvious is, instead, based on a common-sense determination that the claimed invention is merely a combination of known limitations to achieve predictable results. Any of the following rationales are acceptable justifications to conclude that a claim would have been obvious: (1) the claimed invention is simply a combination of known prior art methods to yield predictable results; (2) the claimed invention is a simple substitution of one known element for another to obtain predictable results; (3) the claimed invention uses known techniques to improve similar devices (methods or products) in the same way; (4) the claimed invention applies a known technique to a known device (method or product) ready

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 18 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 18 of 42

for improvement to yield predictable results; (5) the claimed invention was "obvious to try"—choosing from a finite number of identified, predictable solutions with a reasonable expectation of success; (6) there is known work in one field of endeavor that may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; or (7) there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference to combine prior art teachings to arrive at the claimed inventions.

42. I have been informed and understand that a claim may be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found in the reference can be supplied by the common sense or knowledge of one of ordinary skill in the art or taught in different areas of the single reference.

43. I have been informed and understand that an analysis of whether a claimed invention is obvious must not rely on a hindsight combination of prior art. The analysis must proceed in the context of the time of the invention or claimed priority date and consider whether the invention as a whole would have been obvious

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 19 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 19 of 42

to a person of ordinary skill in the art, taking into consideration any interrelated teachings of the prior art, the effects of demands known to the design community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine any known elements in the fashion claimed by the patent at issue.

V. OVERVIEW OF THE CHALLENGED PATENT

44. The Abstract to the '450 Patent describes the disclosed technology as follows:

> A new approach to network security includes manipulating an access point such that an initial communication from an external device is passed to a restricted subset of a computing network including a gatekeeper. The gatekeeper is configured to enforce a security policy against the external device before granting access to a less-restricted subset of the computing network. If requirements of the security policy are satisfied, then the gatekeeper reconfigures the access point such that further communication from the external device may be received by elements of the less-restricted subset. Enforcement of the security policy optionally includes performing a security audit of the external device.

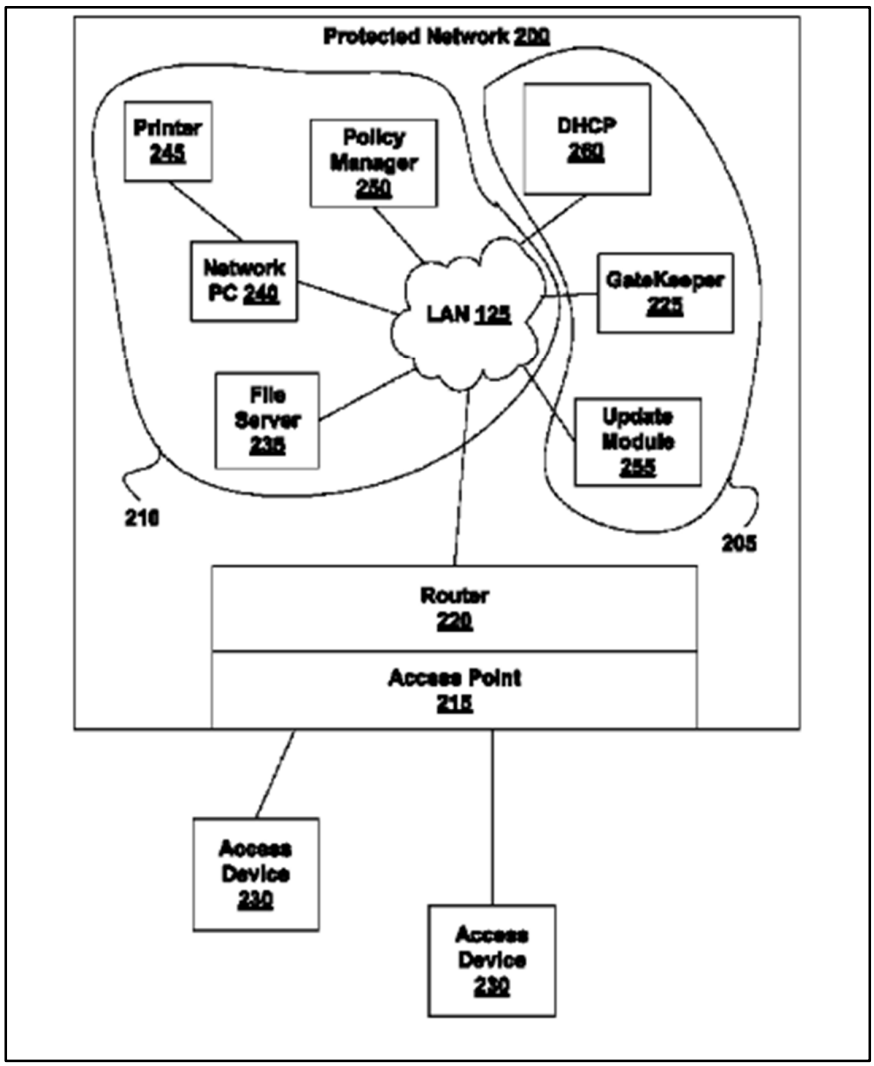
45. Generally, the '450 Patent discloses a novel method of evaluating security policies related to a device attempting to access a protected network, and manipulating an access point to allow limited access to a network while enforcing

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 20 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 20 of 42

security policies, before allowing an external device located on the restricted part of the network to access the less-restricted parts of the network. In other words, when a device attempts to connect to a network, rather than completely denying access or allowing complete access, the novel method places the device on a restricted part of the network where it cannot access more sensitive data but can still function. Then the gatekeeper determines whether the device meets certain security requirements set forth in the configured security policies. If the device passes, then the access point from which the device connected to the network is reconfigured to allow broader access to the network. This invention also allows the performance of security audits on such devices to be performed.

46. Figure 2 depicts embodiments of the invention described in the '450 Patent:

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 21 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 21 of 42



See Fig. 2.

VI. THE ASSERTED PRIOR ART REFERENCES

A. U.S. Patent No. 2004/0111520 ("Krantz")

47. Petitioners allege that the '450 Patent is rendered obvious by U.S. Patent No. 2004/0111520 ("Krantz") in view of U.S. Patent App. No. 2004/0107360

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 22 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 22 of 42

("Herrmann"). Krantz was filed on December 6th, 2002, and published on June 10, 2004. I have assumed for purposes of this declaration that Krantz qualifies as prior art, but at present have no opinions regarding this assumption. As stated, and explained with detail elsewhere, it is my opinion that the '450 Patent is not rendered obvious by Krantz.

48. The alleged prior art, Krantz, is described as follows:

> A computer system attempts to authenticate with a server to gain authorization to access a first network. It is determined by the server that the computer system is not authorized to access the first network. The computer system is given authorization to access a second network for at least the purpose of downloading files (e.g., signup and configuration files) needed to access the first network. A user-interface for receiving user-entered signup information is automatically presented at the computer system. A first schema-based document including user-entered information is transferred to the server. If the server determines that the user-entered information is appropriate, a second-schema document, which includes an indication of authorization to access the first network (e.g., a user-identifier and password), is received. A third schema-based document is executed at the computer system to compatible configure the computer system for accessing the first network.

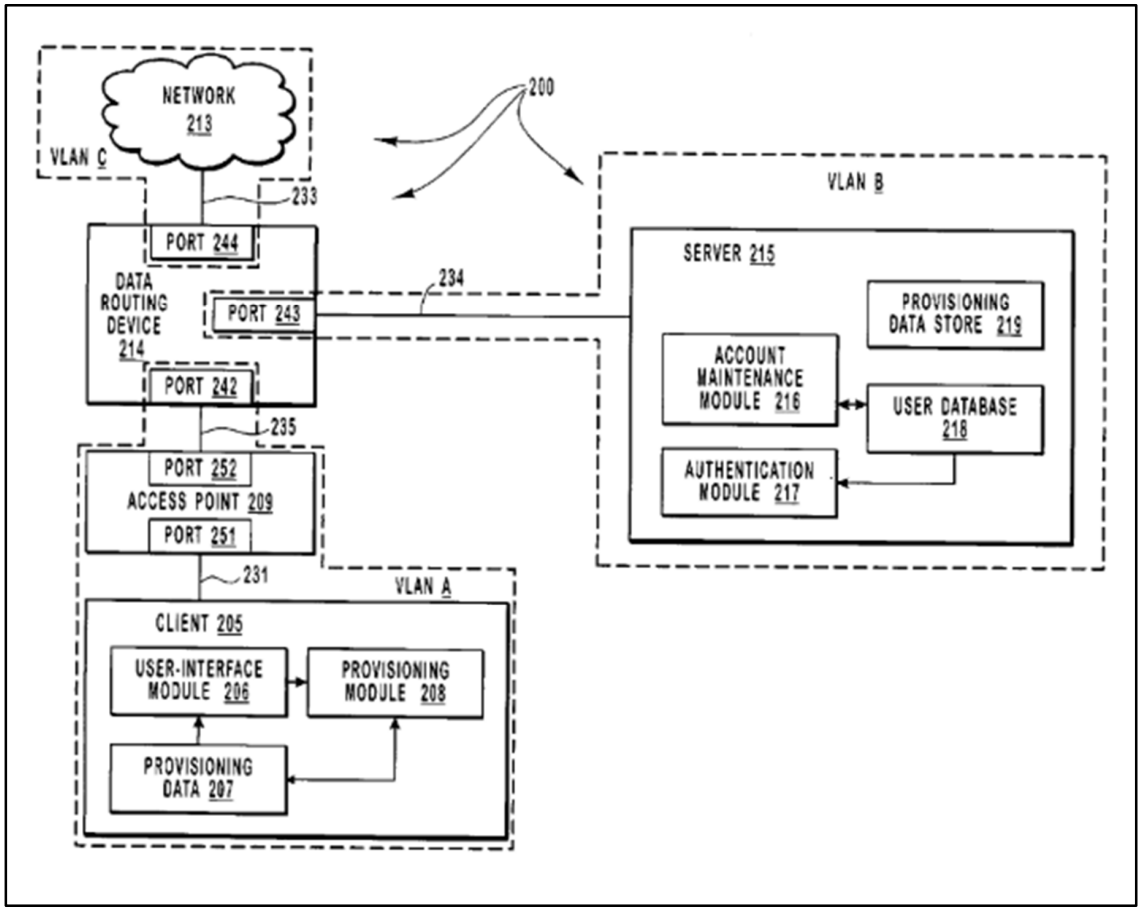
See Krantz, Abstract.

49. In short, Krantz may be summarized as a concept where upon the failure of a computer system to authenticate to one network, the computer system is permitted to access a second network for the limited purpose of downloading files

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 23 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 23 of 42

by a server. In addition, Krantz's evaluation of access requests is limited to user authentication. While several different methods of user identification are discussed, Krantz is limited to user authentication. Notably, Krantz does not include evaluating a device's configuration for compliance with a networks security policy. On its face, the description provided by Krantz of this concept starkly differs from the description of the '450 Patent, which actually performs audits on devices to ensure compliance with security policies, rather than simply denying access to the network for devices that fail to properly authenticate by entering the correct login credentials. The '450 Patent also protects the main network while allowing the user to do more than simply download files on the restricted end of the network. Additionally, as one can see from the figure provided below, the parts and set up of these concepts are entirely different.

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 24 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 24 of 42



See Krantz, Fig. 1 (provided above), cf. '450 Patent (Fig. 3B) (provided below). Notably, the "data routing device 214" serves the function of controlling the data traffic. See, e.g., Krantz, ¶ [0060]. Moreover, nothing in Krantz suggests any modification being made to access point 209 as a result of a security policy compliance check, including configuring an access point based on the auditing of a device.

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 25 of 42

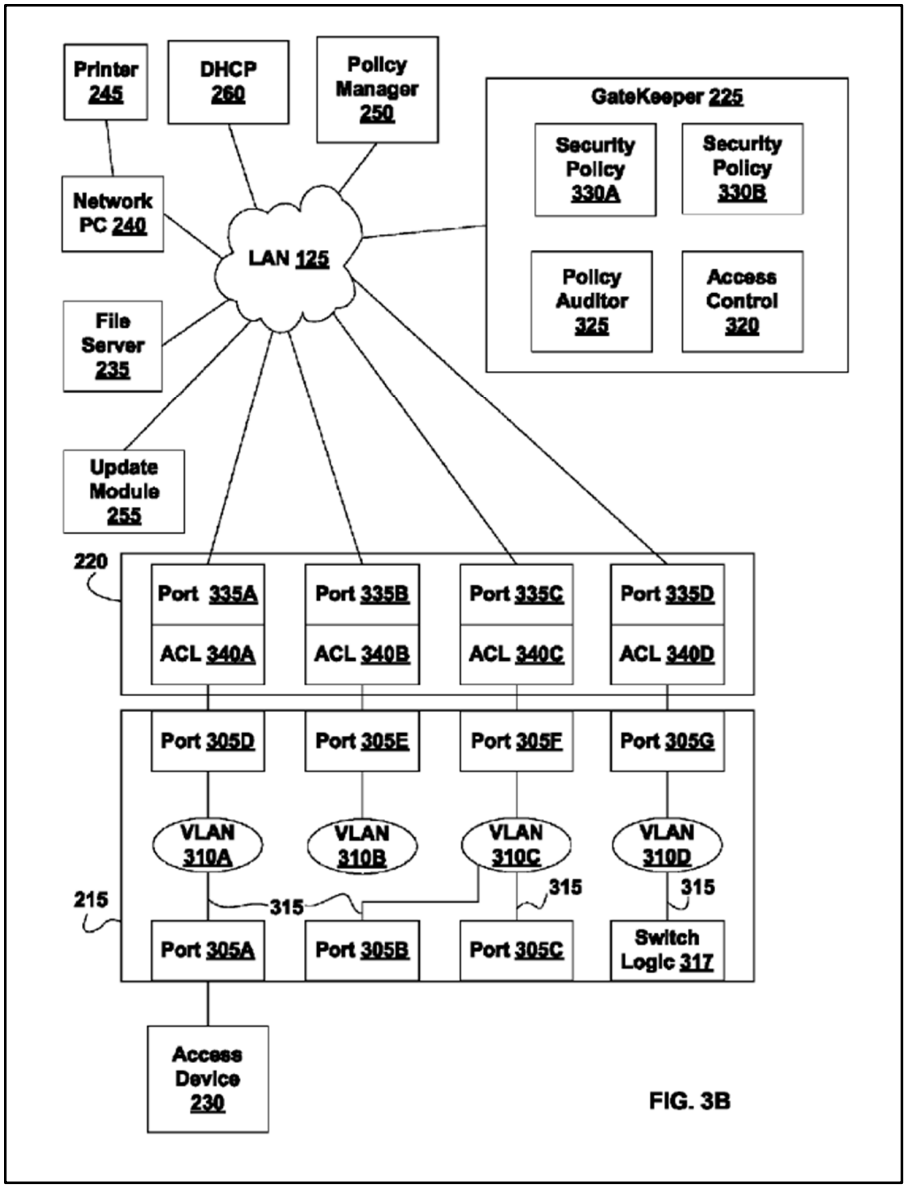


FIG. 3B

B. U.S. Patent No. 2004/0107360 ("Herrmann")

50. As noted above, Petitioners allege that the '450 Patent is rendered obvious by Krantz in view of U.S. Patent App. No. 2004/0107360 ("Herrmann"),

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 26 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 26 of 42

which was filed on March 3, 2003, and published on June 3, 2004. As stated, and explained with detail elsewhere, it is my opinion that the '450 Patent is not rendered obvious by Krantz in combination with Herrmann.

51. The alleged prior art, Herrmann, is described as follows:

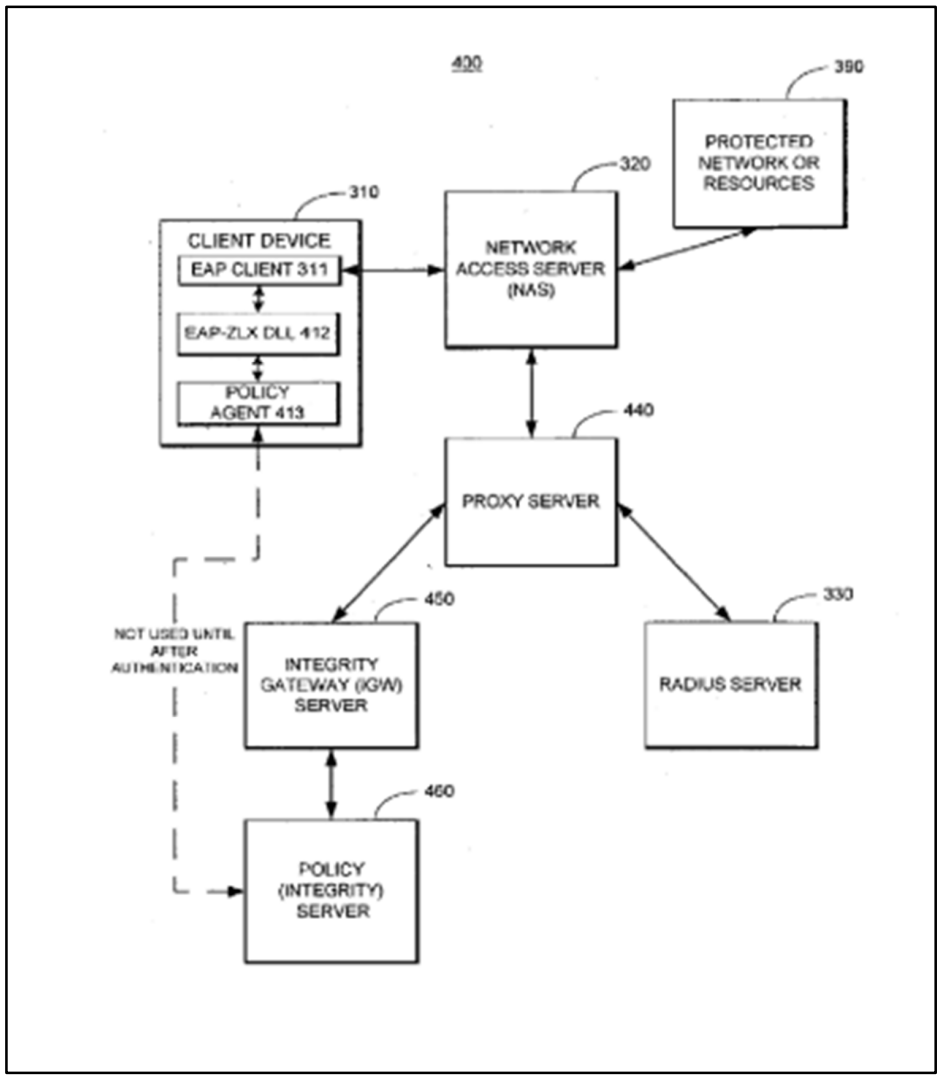
> A system and methodology for policy enforcement during authentication of a client device for access to a network is described. A first authentication module establishes a session with a client device requesting network access for collecting information from the client device and determining whether to authenticate the client device for access to the network based, at least in part, upon the collected information. A second authentication module participates in the session with the client device for supplemental authentication of the client device for access to the network. The supplemental authentication of the client device is based, at least in part, upon the collected information and a policy required as a condition for network access.

See Herrmann, Abstract.

52. In short, Herrmann merely describes a system and methodology for policy enforcement during authentication of a client device for access to a network, which generally requires the device attempting to connect to pass a generic security protocol. Herrmann does not provide active security policy enforcement, does not perform continual audits on devices connected to the network, and is unlike the '450 Patent.

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 27 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 27 of 42

53. The stark contrast between the technology described in the '450 Patent and the generic authentication method described in Herrmann is further illustrated by the Figure provided in Herrmann.



See Herrmann, Fig. 4, cf. '450 Patent, Fig. 2. Similar to Krantz, Herrmann discloses the use of a Network Access Server (NAS) placed between a client device and a

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 28 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 28 of 42

restricted network. Also similar to Krantz, Herrmann includes no disclosure of any modification or changes to the NAS to allow data from a client to pass to the restricted network based on approving the audit data of a device.

VII. SUMMARY OF OPINIONS

54. It is my opinion that the Challenged Claims of the '450 Patent are not rendered obvious by Krantz in combination with Herrmann.

55. Claim 1 of the '450 Patent recites the following:

> **1**. A method for applying a security policy to network devices, the method comprising:
>
> performing an authentication of a device connected to an access point;
>
> scanning the device to collect information regarding the device;
>
> applying a security policy, the security policy including one or more requirements pertaining to the authentication and the information, the application of the security policy taking place in response to a gatekeeper, and
>
> configuring the access point in response to a result of applying the security policy.

'450 Patent, 16:10-22.

56. Claim 1 is not rendered obvious by Krantz in view of Herrmann because this ground (as set forth in the Petition) does not disclose three claim

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 29 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 29 of 42

elements: (1) "scanning the device to collect information regarding the device[,]" (2) "applying a security policy, the security policy including one or more requirements pertaining to the authentication and the information, . . ." and (3) "configuring the access point . . ." Krantz merely discloses a system for receiving user or device credentials (identifying information) in order to authenticate a user or a user's device. Krantz's authentication merely consist of simple security measures, like requiring login credentials such as usernames and passwords. Krantz has nothing to do with "information regarding the device," which relates to its posture compliance, for example its antivirus software and its operating system:

> **In order to communicate electronically on a computer network a computer system may need to be authorized to access the computer network**. For example, before a computer system can communicate electronically on the Internet, **a user of the computer system is often required to register with an Internet Service Provider** (hereinafter referred to as an "ISP") that can authorize access to the Internet. Registering with an ISP typically includes some form of communication other than electronic communication on a network. For example, a user may be required to initiate telephonic communication with a representative of an ISP in order to establish an account with the ISP.
>
> During this telephonic communication, a user can provide the ISP representative with general information (e.g., name, address, etc.) and a form of payment (e.g., a credit card number). **In return, the ISP can provide the user with a username and password that can be used to authenticate the user and authorize access to the Internet**. In many cases, the ISP also sends, via a postal or other delivery service, access software (e.g., a dialer, Web browser, etc.) and/or hardware (e.g., a DSL

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 30 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 30 of 42

modem or cable modem) that must be installed at a computer system. For the user to connect the ISP and thereby access the Internet, any access software and hardware must be correctly installed at the computer system. As such, a user desiring to access the Internet is frequently required to wait until such software and hardware is received. Then, after access software and/or hardware is received, the user must correctly install the access software and/or hardware at the computer system to enable Internet access.

If correctly installed, a **user may be to connect to the ISP and enter the username and password provided by the ISP**. The **ISP can authenticate the user based on the username and password** and if appropriate (e.g., when the user's payments are up to date) **the ISP can authorize the user's computer system to access the Internet**. Unfortunately, if a user is not currently registered with an ISP, there is in most cases no way to use electronic communication on the Internet to initiate a registration process. This is because most ISPs are accessed from the Internet and when a user has no way to access the Internet they in turn have no way to access an ISP for registration.

Krantz, ¶¶ [0005]-[0007] (emphasis added).

A determination of whether data from the client is to be transferred to the first network or the second network can be implemented using any number of techniques, such as, for example, Virtual Local Area Networks ("VLANs"), Internet Protocol ("IP") filtering, Virtual Private Networks ("VPNs"), or use of IP Security ("IPSec") protocols. In some embodiments, similar techniques can also be used within a single network. In these embodiments, the server (based at least in part on received credentials) may authorize the client for at least partial access to the single network, such as, for example, by authorizing client access to selected computer systems or modules on the single network.

Sending credentials can include sending an **Extensible Authentication Protocol ("EAP") Response/Identity message** from the client to the server. If the client is attempting to connect to a network via an access

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 31 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 31 of 42

point, the EAP Response/Identity message may be encapsulated within some other type of message that can be transferred through the access point. In VLAN embodiments, the access point can insert a Tag Header into the encapsulating message to indicate to a data routing device that the encapsulating message is to be transferred to the first network. The access point may also be configured to block communications from the client that use protocols other than EAP and 802.1X.

If credentials do not authorize full access to the second network (e.g., credentials cannot be authenticated, credentials are guest credentials, or an authenticated user is not authorized), the server can respond by sending a notification, such as, for example, an EAP-Notification or a Type-Length-Value ("TLV") object within Protected EAP ("PEAP"), to the client. The notification can be encrypted and integrity checked in accordance with PEAP. The notification can include a Uniform Resource Identifier ("URI") to a master document that contains information for provisioning the client. The **notification can also include conditions (e.g., signup, renewal, etc.) a user must satisfy to become authorized for (full access to resources located on the second network.**

Krantz, ¶¶ [0017]-[0019] (emphasis added).

A first schema-based document that includes the user-entered information is submitted to the server (e.g., by executing an HTTP or HTTPS post). This can include submitting an XML document that is defined in accordance with an XML sign-up schema. After submitting the first schema-based document, the client can receive an indication that the server authorized the client to access resources located on the second network. **This can include receiving a second schema-based document that includes a user-identifier and password or that includes an indication that a credit card payment has been approved**. In VLAN embodiments, when a client is authorized to access resources located on the second network, the access point may insert Tag Headers into client data to indicate to the data routing device that client data is to be transferred to the second network. The access point may also

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 32 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 32 of 42

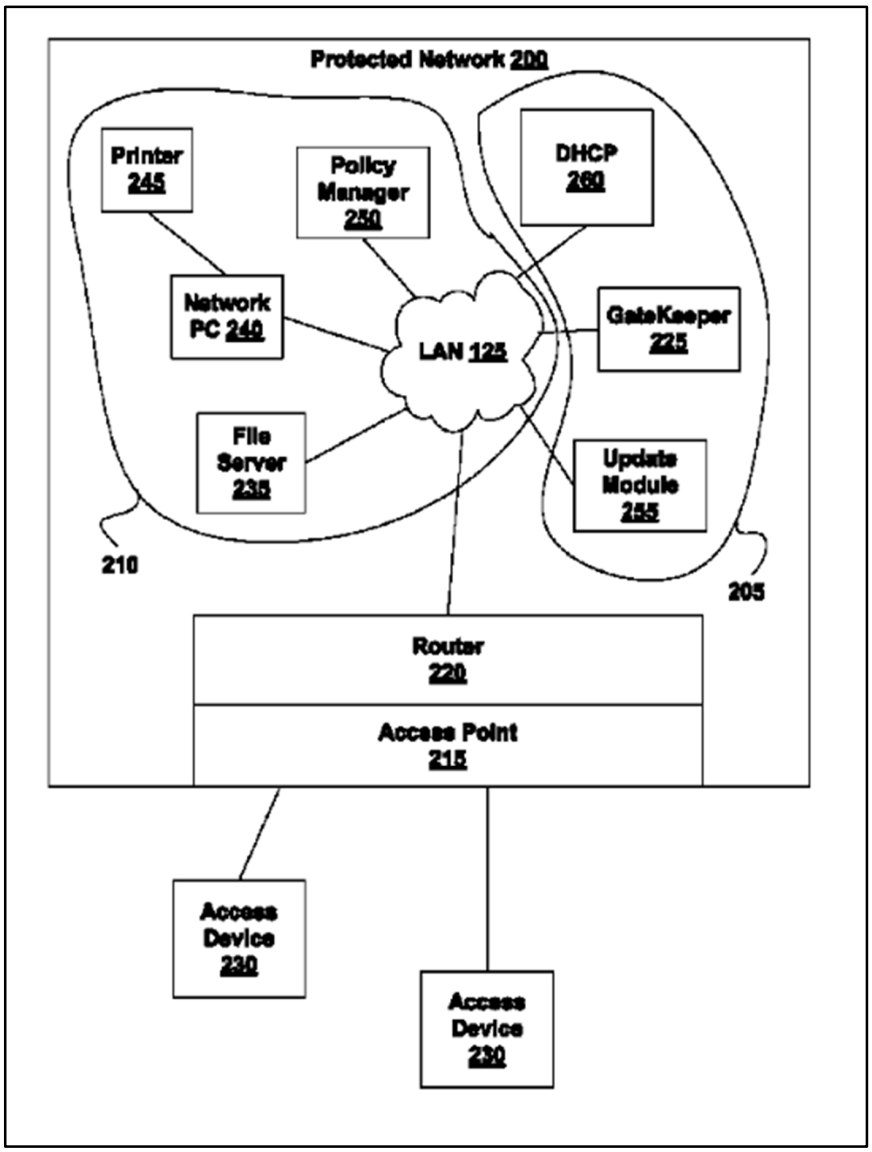
> enable communication using other currently blocked protocols, such as, for example, Simple Mail Transfer Protocol ("SMTP") and Dynamic Host Control Protocol ("DHCP").

See Krantz, ¶ [0023] (emphasis added) (describing authentication as merely consisting of an EAP Response/Identity message, i.e., basic login credentials such as a username and password).

57. Unlike Krantz, claim 1 of the '450 Patent addresses a different layer of security because the claimed invention "scan[s] the device to collect information regarding the device" and then "appl[ies] a security policy, the security policy including one or more requirements pertaining to . . . the information[.]" configures an access point for the network based upon the results of the audit. This method is not what is taught in Krantz, which merely consists of requiring user login credentials. Rather, the technology described in the '450 Patent, including the performance of a security audit on the device using security policies and reconfiguration of the access point, is substantially different from Krantz for many reasons. For one, the '450 Patent actually determines whether a device should be granted access and provides permissions accordingly. As such, it would be intellectually dishonest to suggest references such as Krantz, which merely require a username and password, render obvious the '450 Patent because the '450 Patent

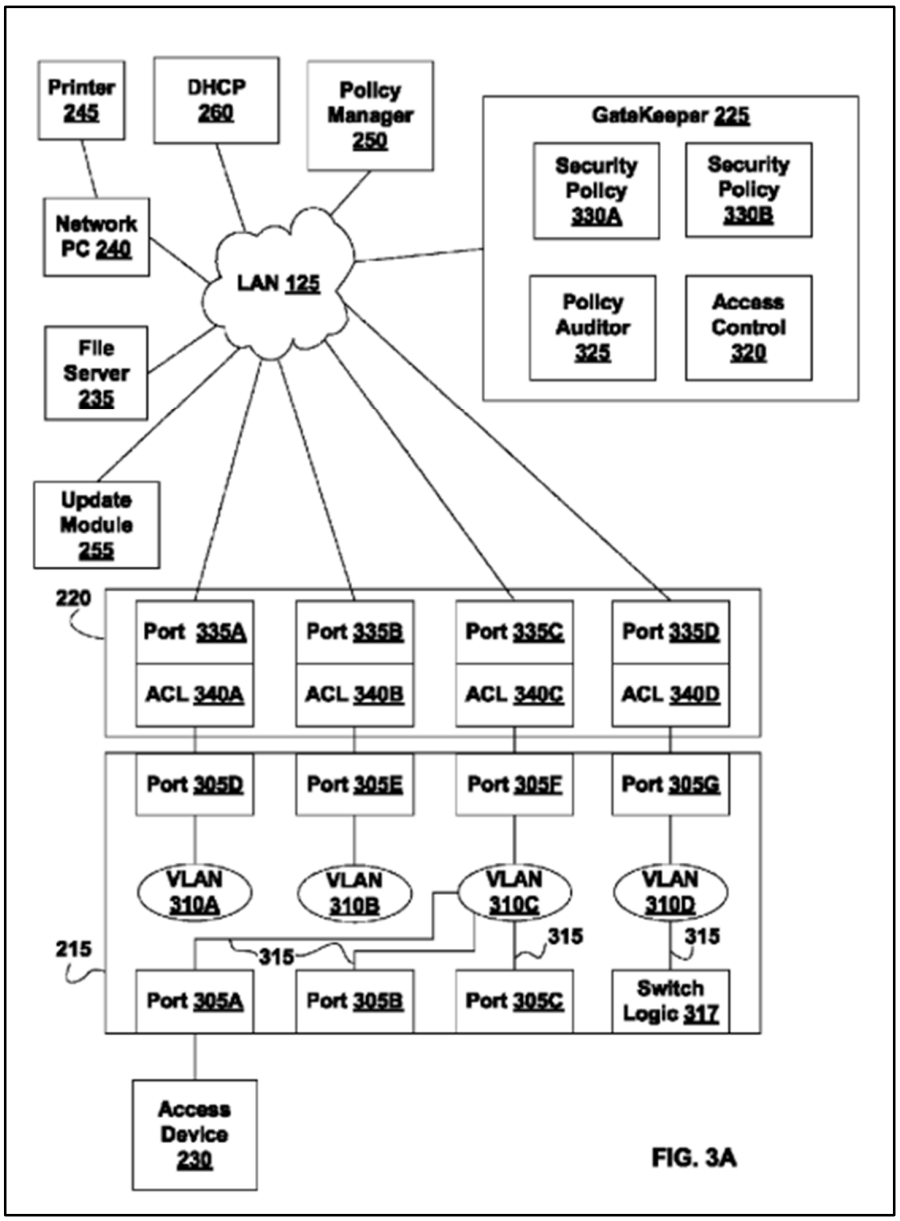
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 33 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 33 of 42

simply provides a completely different kind of security precaution and continually monitors devices connected to the network, rather than simply trusting that they are compliant after simply entering in the correct login credentials.



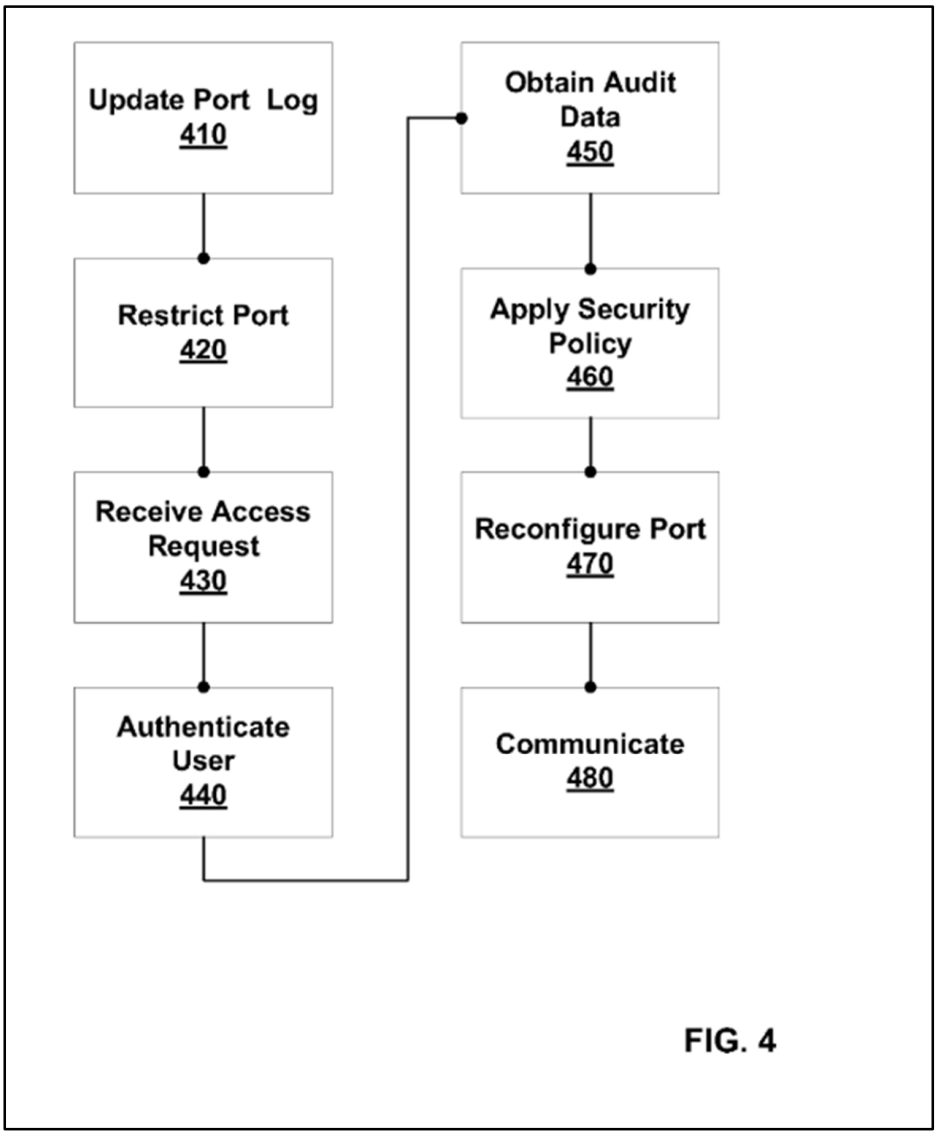
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 34 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 34 of 42

See generally '450 Patent, Fig. 2 (a block diagram showing further details of the access point, policy auditor, router and gatekeeper).



CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 35 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 35 of 42

See generally '450 Patent, Fig. 3A (a block diagram showing further details of the access point, policy auditor, router and gatekeeper).



See '450 Patent, Fig. 4 (a flowchart illustrating a method of granting access to a protected network, according to various embodiments of the invention).

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 36 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 36 of 42

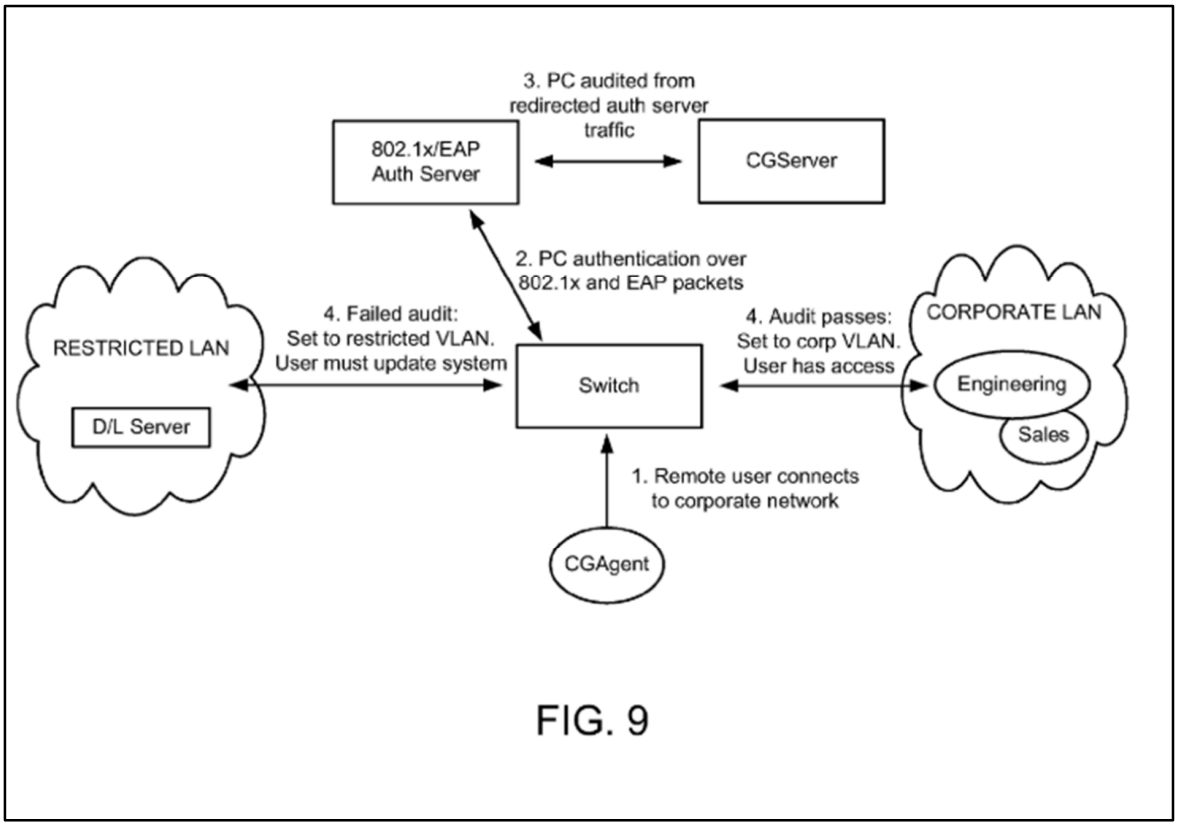


FIG. 9

See '450 Patent, Fig. 9.

58. In contrast, a POSITA would understand the authentication described in Krantz to be referring to usernames, passwords, or MAC addresses because Krantz uses the phrase "Operating System Credential" (Krantz, ¶ [0099])– a term used in the industry to refer to username and password credentials that are used to gain authorization to act on a system. This type of credentials would not be understood by a POSITA to refer to "information regarding the device," like the '450 Patent recites. Instead, such "information regarding the device" would be understood

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 37 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 37 of 42

by a POSITA to relate to checking a device for certain software and/or hardware and compliance with network requirements.

59. As such, Krantz in view of Herrmann does not render the '450 Patent obvious, as Krantz's authentication methods are limited to user authentication, whereas the '450 Patent, claim 1 describes an invention which provides an additional layer of security much more sophisticated than merely requesting a username and password for the user to authenticate. In addition, claim 1 requires "applying a security policy, the security policy including one or more requirements pertaining to the authentication and ***the information***." And since Krantz does not disclose any "information regarding the device," this element too is not disclosed.

60. Turning now to claim 16 of the '450 Patent, it is my opinion that Krantz in view of Herrmann fails to render this claim obvious, for similar reasons I stated with respect to claim 1.

61. Claim 16 of the '450 Patent recites:

> **16**. A method of providing access over a communication network, the method comprising:
>
> receiving at an access point a request for access to a less-restricted network, the request coming from an access device;

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 38 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 38 of 42

> ***applying a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device***;
>
> ***providing information to the access device to improve compliance of the access device to the security policy***, in response to the audit;
>
> granting access to the less-restricted network based on satisfaction of the security policy by the updated access device; and
>
> authenticating a user of the access device, wherein granting access is further based on the authentication.

'450 Patent, 16:54-67, 17:1-2 (emphasis added).

62. As I explained above, Krantz discloses limited methods of user authentication; Krantz discloses neither "scanning the device to ***collect information regarding the device***;" nor "applying a security policy, the security policy including one or more requirements pertaining to the authentication ***and the information***." By that same token, with respect to claim 16, Krantz does not disclose "applying a security policy . . . including performing an audit of the access device"; nor does it disclose "providing information to the access device to improve compliance of the access device to the security policy[.]" This is because (as explained in further detail above), Krantz discloses user identification and authentication information. Analyzing that information is ***not*** "performing an audit" of the user device;

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 39 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 39 of 42

providing information such as provisioning files (*see* Pet. at 87) is not "providing information to the access device to improve compliance of the access device to the security policy[.]"

63. Furthermore, claims 1 and 22 of the '450 Patent require "configuring the access point" such that a qualified user can accesses a restricted part of the protected network. In my opinion, this requires that the access point has to actually be changed. Krantz does not disclose anything along these lines. Instead, Krantz very clearly discloses an access point 209, which in every instance sends data through the data routing device 214. Moreover, the data routing device 214 either reads "tag headers" that are inserted into client data (Krantz at, *e.g.*, [0061]) or uses "IP filtering" (Krantz, [0053]-[0056]) to direct traffic.

64. Herrmann, likewise, does not teach the use of a network akin to the type described in the '450 Patent. Importantly, to the extent that Petitioners rely on Herrmann for its disclosure of "configuring the access point," Herrmann teaches no such claim element.

65. I note that Petitioners rely on the disclosure in Krantz of assigning a header tag to the user credentials for the claimed "configuring." This alleged

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 40 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 40 of 42

reconfiguration is merely a reconfiguration of the user ID, rather than the reconfiguration of the access point.

66. As such, the '450 Patent claims 1 and 22 are not rendered obvious by Krantz, in combination with Herrmann for that reason.

67. To the extent that the remaining claims of the '450 Patent depend upon claims 1, 16 or 22, it is my opinion that they are not obvious in view of Krantz, whether alone or in combination with Herrmann. I note that with respect to the '450 Patent, that Petitioners rely on Herrmann for the disclosure of an agent on the client device. Whether Herrmann includes such a disclosure is immaterial in that the combination of Krantz and Herrmann still fail to disclose at least any reconfiguring of the access point.

VIII. CONCLUSION

For the foregoing reasons, it is my opinion that the '450 Patent is valid and enforceable, as not obvious in view of Krantz, alone or in combination with Herrmann.

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 41 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 41 of 42

Date: July 25, 2024



Dr. Eric Cole

CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 42 of 42
CISCO/FORTINET v. INFOEXPRESS
IPR2024-00676
Page 42 of 42