

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.

IPR2024-00679
U.S. Patent No. 7,523,484

DECLARATION OF HUGH SMITH, Ph.D.

I, Hugh Smith, Ph.D., hereby declare as follows:

I. INTRODUCTION

1. I am a computer scientist and Professor in the Department of Computer Engineering at California Polytechnic State University.
2. I have been engaged by Patent Owner InfoExpress Inc. as an expert in connection with the present *Inter Partes* Review filed by Petitioners Cisco Systems, Inc. and Fortinet, Inc.
3. This Declaration sets forth the opinions I have formed and the bases for them concerning claims 28, 38, 39, 41–43, 53, 56–59, 61–63, and 65–68 of U.S. Patent No. 7,523,484.
4. I have relied on my knowledge, experience, and expertise in the technologies involved, which I have acquired over my career, in providing the analysis and opinions contained in this report. All of my conclusions and opinions are provided within a reasonable degree of professional certainty.

II. SUMMARY OF OPINIONS

5. It is my opinion that claims 28, 38, 39, 41–43, 53, 56–59, 61–63, and 65–68 find written description support in EX2011 and EX2013.

6. It is my opinion that claims 28, 38, 39, 41–43, 53, 56–59, 61–63, and 65–68 find written description support in U.S. Provisional Patent Application Serial No. 60/513,080 (EX2006).

III. QUALIFICATIONS AND EXPERIENCE

A. Education and Experience

7. A detailed record of my professional qualifications, and a list of cases in which I have testified by trial or deposition in the last ten years, is attached as EX2008.

8. I am a tenured full professor in the Department of Computer Engineering at the California Polytechnic State University. I also served as Director of the Cal Poly Computer Engineering Program, both in 2009-2013 and again in 2016-2017. I received my B.S. degree in Computer Science from Xavier University in 1985. I received my M.S. degree in Computer Science from Michigan State University in 1994 with a research focus on parallel and distributed computing. I received my Ph.D. in Computer Science in 1999 from Michigan State University.

9. Upon receiving my Ph.D., I joined the faculty of the Cal Poly Department of Computer Science in 2000 and moved to Cal Poly's newly created Department of Computer Engineering in 2021. At Cal Poly, I have been teaching and doing research on computer networks, distributed systems, embedded systems,

programming, and robotics for the last 24 years. I have developed and taught the senior level Computer Networks I and Networks II courses and the Graduate Level Computer Networks course. These courses involve the study and analysis of the theory and implementation of computer networks. Course activities included the theoretical aspects of computer networks, including wired and wireless networks, network security and the implementation of protocol layers from the physical to the application layer. As part of my teaching and work, I cover topics including network security, firewalls, virtual private networks (VPNs), virtual LANs (VLAN), user privacy and authentication from both a theoretical perspective as well as using these technologies in the real-world.

10. I have written a number of articles in the area of computer networks during my academic career. I wrote three articles that were published in the Network Computer Magazine which covered security products, including an article analyzing the implementation of different commercial network security products including how these security devices supported VPNs and virus detection. I have also published network related papers on the development of a network coprocessor and the controlling of the transmission rate of video over the Internet.

11. I have over 40 years of experience in computer engineering and computer science. In addition to my educational and teaching/research experience, I have

professional experience in computer system design and implementation. From 2011 to 2013, I developed, implemented, and sold an Android App called Lockmenu. I was a Group Manager, Senior Systems Analyst/Project Manager, and Systems Analyst for the Procter and Gamble Company from 1985-1992. I managed all aspects of a large, distributed Purchasing and Inventory Control system, which included over 2,000 users, processed over \$250 million in yearly purchases, and tracked over \$60 million in inventory. I led a support team, developed software upgrades, managed capacity planning, and on-going maintenance. Before that, I was a Programmer Analyst at the Merrell Dow Research Institute from 1983-1985.

B. Compensation

12. I am being compensated for my time at the rate of \$700 per hour. The compensation is not contingent upon my performance, the outcome of this or any other proceeding, or any issues involved in or related to this matter.

C. Documents and Other Materials Considered

13. In addition to my education, training, and knowledge, my opinions are based on review of the documents and other materials identified in this Declaration, including:

EX1501	U.S. Patent No. 7,523,484
--------	---------------------------

EX2001	Declaration of Dr. Eric Cole
EX2006	U.S. 60/513,080
EX2011	“LAN Based Policy Enforcement Engineering Specification”
EX2013	“InfoExpress’s CyberGatekeeper Policy Manager”

D. Prior Testimony and Publications

14. My prior testimony and publications are listed on my curriculum vitae (EX2008).

IV. STATEMENT OF LEGAL PRINCIPLES

15. I have been advised of certain legal principles applicable to this inter partes review. I have incorporated and applied these legal principles within the opinions set forth below in this Declaration.

16. I am informed that a patent owner may antedate or “swear behind” certain references by showing conception prior to a critical date for the reference(s) and reasonably continuous diligence throughout the critical period from just before the effective date of the prior art until reduction to practice.

17. I am informed that a party can show conception by demonstrating it had possession of every feature recited in the claimed invention.

18. I am informed that a patent application can constitute a “constructive reduction to practice” if the patent application provides “written description” for the claimed invention.

19. I am informed that pre-A.I.A. 35 U.S.C. § 112, first paragraph includes a “written description” requirement. I am informed that one test for compliance with the written description requirement is “whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date.”

20. I am informed that “it is the specification itself that must demonstrate possession.” I am informed that the “level of detail required to satisfy the written description requirement varies depending on the nature and scope of the claims and on the complexity and predictability of the relevant technology.” I am further informed that, to meet the written description requirement, the specification can include “words, structures, figures, diagrams, formulas, etc.” that “fully set forth the claimed invention.”

21. I am informed that the exact words of the claim need not appear in the specification, but that “the specification must contain an equivalent description of the claimed subject matter.”

V. SCOPE OF OPINIONS

22. I have been asked only to provide my independent opinions and analysis of the issues I specifically discuss in this declaration. I note that the Petition (and the evidence it cites) appears to raise many other issues, but I have not been asked to provide my opinions as to any of those other issues.

VI. OVERVIEW OF THE PATENT

23. The '484 Patent is directed to a novel and seminal approach to a security solution for controlling access to a protected network. Before Patent Owner's inventions, network security required a "gatekeeper" placed directly between each client, i.e., user, and the network. EX1501, Fig. 1, 2:31-42; EX2001, ¶¶ 44-46. But as the '484 Patent further explains, access control further required evaluation of each accessing device's hardware and software, e.g., virus protection and operating systems, before the gatekeeper granted such access—thus consuming substantial network resources and creating bottlenecks. EX1501, 2:14-25, 34-39.

24. An example of the prior art architecture is shown in annotated FIG. 1 of the '484 Patent.

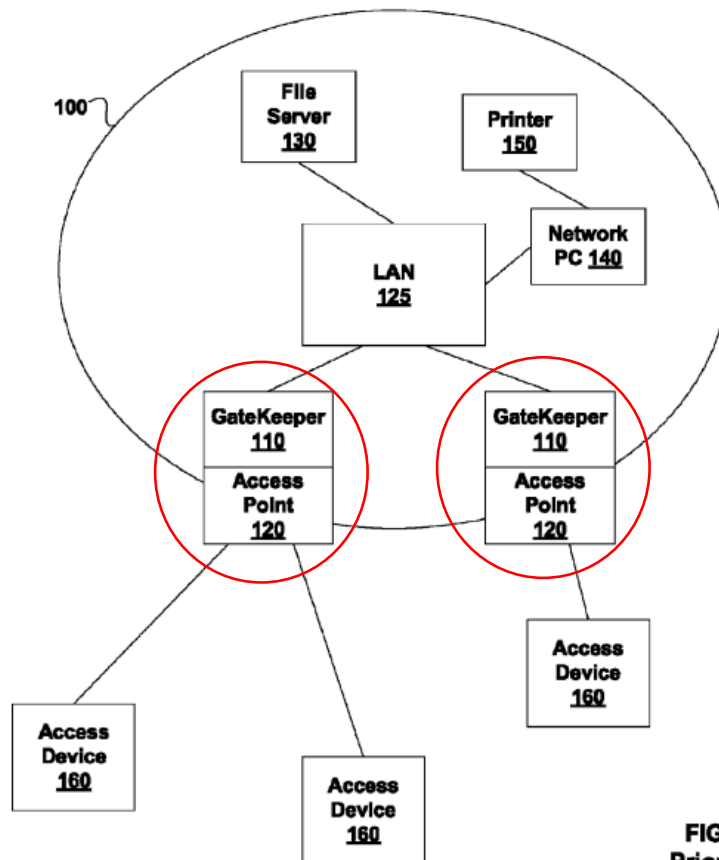


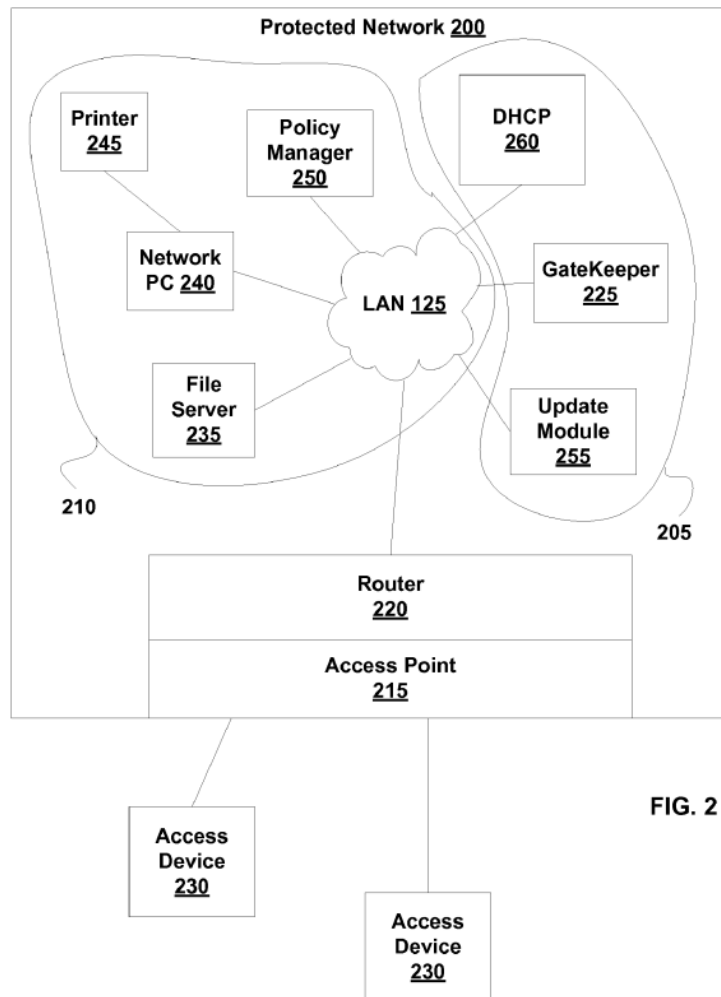
FIG. 1
Prior Art

The protected network 100 includes two Gatekeepers 110, each associated with a different instance of an Access Point 120. All devices attempting to access the protected network are required to be evaluated by the gatekeeper. With large corporate networks including many access points, the "use of one instance of GateKeeper 110 to support numerous instances of Access Device 160 is limited by bandwidth and required sophistication (e.g., cost) of GateKeeper 110." EX1501,

2:31-34. The gatekeeper then becomes a limiting bottleneck on the bandwidth of the system. EX1501, 2:34-39.

25. The '484 Patent addressed this particular problem with a new, novel, and non-obvious approach that relieves computer resources by configuring an access point in response to approval of a device by the gatekeeper. By configuring the access point to allow devices that have been approved by the gatekeeper to meet both user authentication requirements and device compliance with security policies to access the protected network, subsequent evaluation of the user/device by the gatekeepers when the previously evaluated device is attempting to access the protected network again is obviated.

26. By way of example, the '484 Patent discloses a protected network that includes a restricted subset with a gatekeeper and one or more less-restricted subsets.



EX1501, Fig. 2. In this embodiment, before an access device is granted access to a less-restricted subset 210, its request is first passed to the restricted subset (in this embodiment indicated as 205). EX1501, 2:50-52, 5:31-33. A gatekeeper in the restricted subset checks whether the access device satisfies security policies (e.g.,

updated virus protection software). EX1501, 11:39-50, 12:10-16. An evaluation regarding whether the user or device is authorized (e.g., username, password, MAC address) to access the protected network may also be performed. EX1501, 11:31-38. In this embodiment, if the access device is qualified, it is granted access to a less-restricted subset of the protected network. EX1501, 2:52-56.

27. A key feature of the '484 Patent is that rather than require all device access requests to pass through the gatekeeper, the access point itself is configured in response to approval of the device by the gatekeeper. The Detailed Description gives the following example of configuring the access point in response to approval of the device by the gatekeeper.

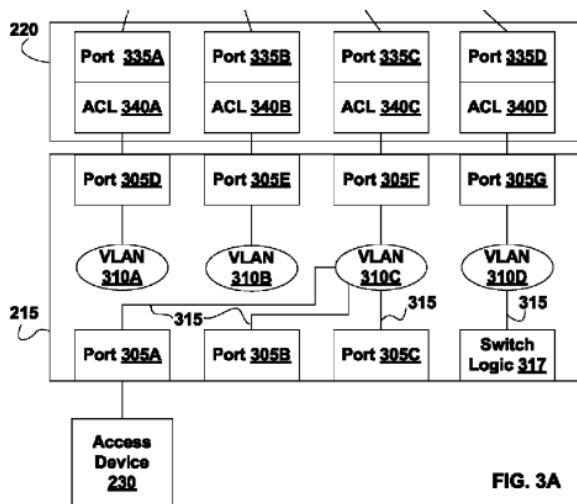


FIG. 3A

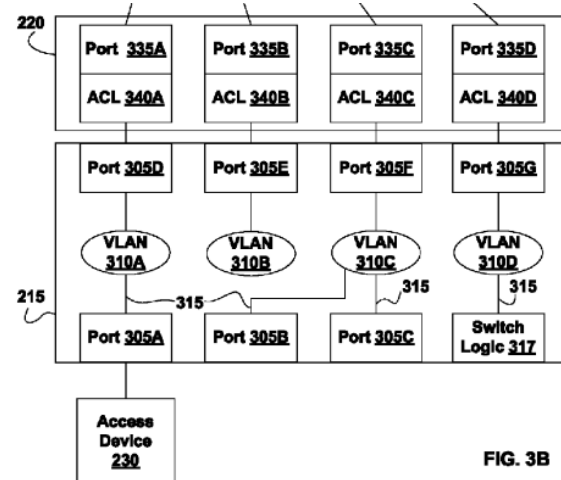


FIG. 3B

Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at

Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F.

EX1501, 8:16-23.

By configuring the access point in response to approval of the device by the gatekeeper, network traffic for previously approved devices can pass to the less-restricted subset of the network without needing to pass through and be evaluated by the gatekeeper. Thus, after access has been granted, most network traffic does not need to pass through the gatekeeper, thereby alleviating the burden on the gatekeeper.

VII. CLAIMS 28, 38, 39, 41–43, 53, 56–59, 61–63, AND 65–68 FIND WRITTEN DESCRIPTION SUPPORT IN EX2011 AND EX2013.

28. In my opinion, EX2011 and other InfoExpress documents discussed herein show conception of at least claims 28, 38, 39, 41–43, 53, 56–59, 61–63, and 65–68 of the '484 Patent at least as early as November 14, 2002. My analysis is detailed in EX2009 and below.

29. EX2011 is entitled “LAN Based Policy Enforcement Engineering Specification”. EX2011 at 1. In my experience, such specifications are used to define key features of software for implementation (*e.g.*, software programming or “coding”) by programmers. Thus, the features defined in a specification are

typically produced through lines of instructions in one or more computer programming languages that can be executed by one or more computers.

30. I understand EX2013 to be a product manual for InfoExpress's CyberGatekeeper Policy Manager. I further understand that the InfoExpress CyberGatekeeper Policy Manager referred to herein was a component that was associated with a former InfoExpress product known as CyberGatekeeper Remote—i.e., the Remote Product.

31. I understand EX2013 and the CyberGatekeeper Policy Manager product to have been created prior to EX2011 and, thus, reflect background knowledge of InfoExpress and further demonstrates conception of the claimed invention.

32. EX2009 is a claim chart I prepared demonstrating my analysis of where the '484 Patent claim elements are supported and found in EX2011 and EX2013.

33. EX2011 details a method and system involving a network having:

- a. a “less-restricted” subset (a “trusted network” in EX2011 as discussed at §§ 2, 3.4.3, & 5.2.1.2); and
- b. a “restricted” subset (an “untrusted network” in EX2011 as discussed at §§ 3, 3.2.3, 3.4.3, 3.5.2, 3.5.3, 3.6.2, 3.6.3, 5.2.2, 5.2.3.3, 5.2.3.7, & 5.2.3.8).
- c. requests for “access” as discussed, *e.g.*, at § 2.

34. EX2011 further details the following:
- a. Figures 1 and 2 describe an “Access Point” and “Switch.” EX2011 at 6-7. As discussed at Section 2, “Switches have ports that connect all the nodes on a network, and allow communication between them.” EX2011 at 5.
 - b. CyberGatekeeper Server (CGS) acts as a gatekeeper that operates on the server side (relative to the CGAgent operating on the client side). *See, e.g.*, EX2011 at 7 (Figure 2 depicting CGS on opposite side of Access Point (Switch) from CGAgents).
 - c. CGS can be located outside of the “restricted” subset of the network. *E.g.*, EX2011 at 7 (“everyone connects to the switch can only access to the untrusted network”).
 - d. Given that the access point can restrict access to the “less-restricted”/”trusted” network until the audit is completed, an access device would not be able to communicate with the CGS (e.g., for an initial audit, for a further audit if the initial audit fails) if the CGS was located within the “less-restricted”/”trusted”. Therefore, it must be in the “restricted”/”untrusted” network. *Id.*

e. Section 3 states that [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

35. EX2011 also provides significant explanation and details for auditing including auditing performed based on policies. See, *e.g.*, EX2011 at 8 (§ 4.6).

This is further detailed below by way of the following examples:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

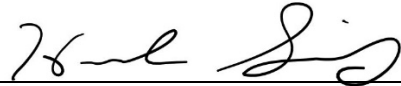
[REDACTED]

**VIII. CLAIMS 28, 38, 39, 41–43, 53, 56–59, 61–63, AND 65–68 FIND
WRITTEN DESCRIPTION SUPPORT IN U.S. PROVISIONAL PATENT
APPLICATION SERIAL NO. 60/513,080.**

36. EX2010 is a claim chart I prepared demonstrating my analysis of where the '484 Patent claim elements are supported and found in the '080 Provisional (EX2006).

37. I, Hugh Smith, declare upon penalty of perjury that the forgoing is true and correct to the best of my understanding and belief.

Dated: 7/25/24



Hugh Smith, Ph.D.