SECURITY

Next-Gen Firewalls: What To Expect

Gary Audin

How will firewalls deal with new traffic types and higher processing demands? Leading suppliers weigh in.

Firewalls provide that warm secure feeling. But are they satisfying all your security requirements? Are they a commodity yet? NO. There are differences in today's products. There is still a future of changes, enhancements and new roles for these boxes.

No universal agreement has emerged for the predictions that vendors articulate about the next generation of firewalls. Some vendors point to a new architecture concept, others say the next generation is here, while some look ahead to firewalls targeted at specific applications, like voice over IP (VOIP—see *BCR*, October 2003, pp. 23–27). Who is right?

One Box, Two Boxes, Three Boxes Or More

Initially, the firewall was designed as a packet-filtering device that would block unauthorized intrusions from an untrusted network like the Internet. Forwarding rules and policies determined which packets could pass through the firewall; those that did not conform to the installed policies would be blocked.

The corporate firewall sits at the boundary between trusted and untrusted networks (Figure 1). Most firewall products are designed for data applications, not voice or video over IP.

Firewalls rarely deal with specific applications, although one vendor, Ingate, designs its firewalls for the Session Initiation Protocol (SIP), which supports converged voice-video-data applications. In addition to standalone devices, firewall technology is regularly installed as software in PCs, SOHO routers, servers and in a few IP voice gateways and IP phones.

A second type of box has entered the market, the intrusion detection system (IDS). The IDS is a passive observer that audits the policy enforcement of the firewall. Placed behind the firewall on the trusted network, the IDS's objective is to monitor traffic passing through the firewall and alert the network management when a possible intrusion has made it through the firewall. The IDS reports, but does not block, the intrusion. Many enterprises ignore IDS alerts because IDSs tend to produce many false positives—i.e., alerts when there is no security breach.

Some argue that the IDS should be part of the firewall, while others believe that two different vendors should be used—one for the firewall and another for the IDS—to ensure that the software and policies are designed by different groups. Think of it this way: Would you want your accountant to audit his own books, or would you prefer to have an independent opinion?

The third box to enter the protection environment is the intrusion prevention system (IPS). As an additional line of defense, the IPS is placed behind the firewall on the trusted network. The firewall behaves as a macro packet filter, while the IPS is a micro packet filter.

Security has become such a significant issue that the devices on the other side of the corporate firewall—i.e. remote sites—also require protection. Personal firewall software is available for the SOHO PC, teleworker and branch offices. Manufacturers of low-end routers have also included firewalls in their products for these markets.

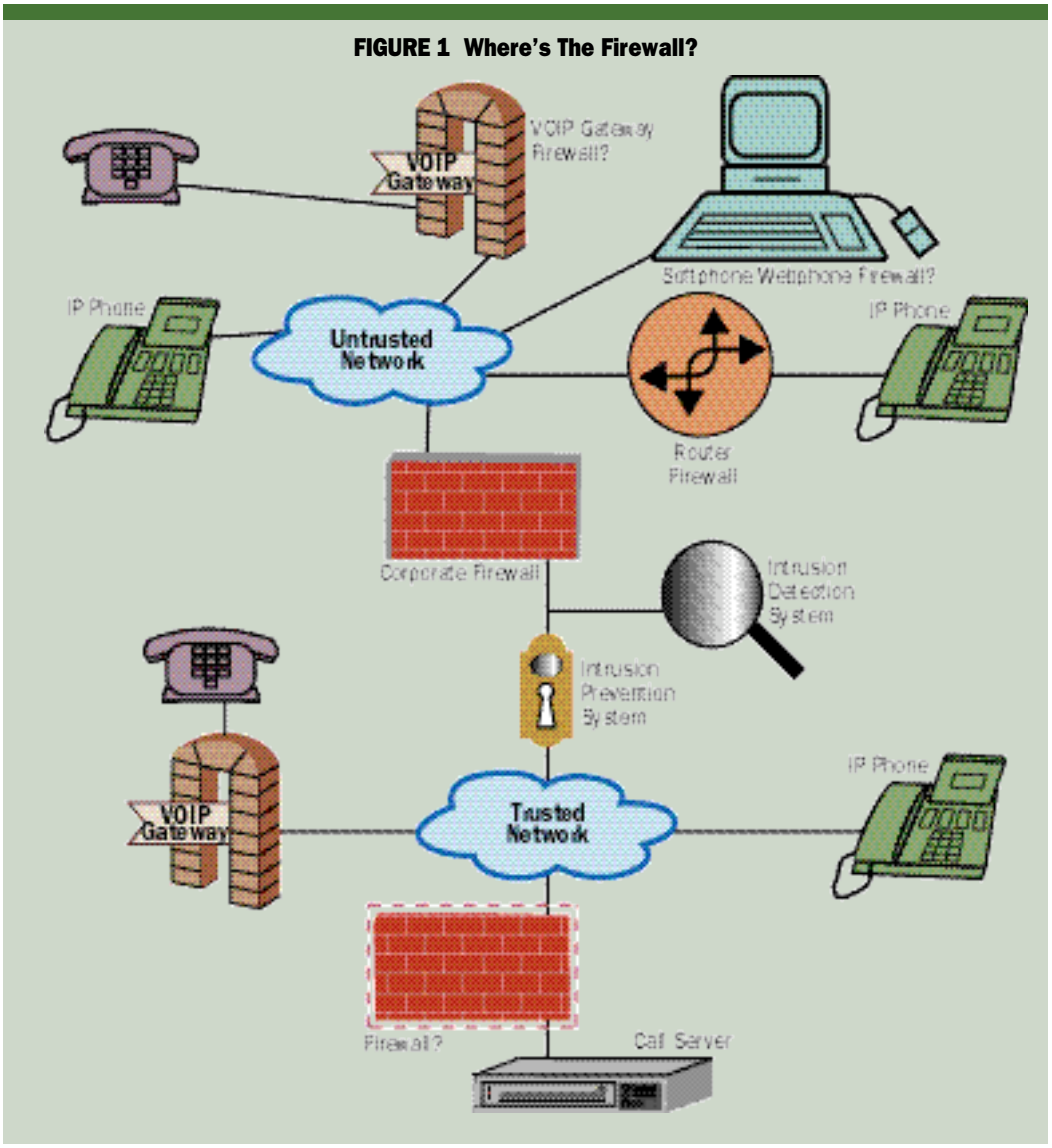
Nostradamus For Firewalls

For this article, seven vendors were asked to discuss the future of firewalls: Avaya, Checkpoint, Cisco, Ingate, NetScreen, Nortel and SecureLogix (see "Article Interview Resources," p. 58). These are not the only sources of firewall technology but, based on their markets and involvement with voice over IP (VoIP), they represent a variety of viewpoints.

Each of the vendors received a list of 12 questions before the interviews began. Telephone interviews were then conducted, with limited discussion of present products; the future was the subject. Each vendor was interviewed for 60 to 90

Gary Audin is president of Delphi, Inc., an independent consulting and training firm. He has extensive experience in the planning, design, implementation and operation of all kinds of networks, and he is the instructor for a number of BCR seminars. He can be reached at delphi-inc @worldnet.att.net.

FIGURE 1 Where's The Firewall?



Throughput, latency and concurrent-session support are the big concerns

minutes. The remainder of this article focuses on the responses to the questions that generated the most interest.

For purposes of this article, the 12 questions have been consolidated into eight sets of opinions.

■ **What limitations do you see in the present firewall devices?**

There is a common opinion that today's firewalls have done a good job securing the network by mostly securing Layer 3. Because the firewall looks at Layer 3, Layers 1 and 2 are not a consideration for traffic passing through the firewall.

Most firewalls also analyze and process traffic at Layer 4 (Transport) using TCP and UDP port numbers as part of the packet-filtering process. All respondents agree that the next generation of firewalls should move up to and include Layer 7 (Application).

The second agreed-upon point is that, as applications increase and traffic grows, the performance of firewalls will have to improve. Respondents saw performance as three separate issues:

1. Throughput, i.e. the number of packets processed per second, must increase.

2. Latency, the delay for packets passing through the firewall, must be short for real-time applications like voice and video. The goal would be less than 1 millisecond (ms).

3. Vendors must continue to increase the number of concurrent sessions that can be supported. In the case of VOIP, this represents the number of phone calls that can pass through the firewall at the same time.

■ **Define what you mean by a next-generation firewall and its market.**

Ingate, Nortel and SecureLogix say that deep-packet inspection for all traffic will become common. Ingate and Avaya believe that encrypted transmission of signaling and content will be supported. But when encryption is used, it will limit or eliminate the participation of the firewall in the signaling process (H.323, SIP, MGCP)—the firewall will not be able to perform deep packet inspection of encrypted packets. The choice will

The most important device to secure in a VOIP network is the call server

be encryption or deep packet inspection, not both at the same time.

All the respondents agree that whatever processing occurs, performance cannot be degraded. The next-generation firewalls must process traffic at wire speed.

Avaya does not believe that multiple security devices are the future solution; rather, it contends that firewalls will be embedded in wired LAN and wireless LAN (WLAN) switches, and that virtual private networks (VPNs) will become common on WLANs.

In contrast, Nortel has already started to pursue a solution to enhance performance by using multiple firewalls behind a single load-balancing device. As more performance is required, additional firewalls can be placed in parallel, behind the load balancer, to increase performance in a modular fashion, instead of purchasing a bigger firewall. This approach is more cost effective and would help in future-proofing the configuration for performance, the company contends.

All respondents foresee that, as firewalls move up to Layer 7 support, a few key data applications will be supported. According to Cisco, Web-based protocols comprise about 90 percent of the traffic that passes through a firewall. NetScreen (an independent company when we spoke with them, now a part of Juniper Networks) sees "application intelligence"—a term they have coined for application-aware firewalls—as the next wave for the firewall.

NetScreen/Juniper doesn't include VOIP on the list of applications it expects will be important at this point, since the volume of VOIP traffic currently traversing enterprise firewalls is still relatively modest.

Cisco observed that managing multiple firewalls would require centralized policy directors. They believe the management issues will be one of the drivers for the development of the next generation of firewalls.

SecureLogix acknowledges that some vendors do not plan to introduce application-specific firewalls. Rather, the vendor, which places a strong emphasis on voice traffic, anticipates a conflict between stateful and deep packet inspection for VOIP. An HTTP transmission can be stopped in midstream for a security problem, but such a stoppage would degrade voice quality on a VOIP connection. SecureLogix predicts that a number of vendors will focus on firewalls for VOIP and other real-time traffic.

NetScreen/Juniper does not expect firewall products to be divided into separate vertical markets. They also do not believe many new vendors will appear in the future.

The products that vendors already have in the market will influence next-generation firewalls. Any new vendors will position themselves based on what they perceive as the weaknesses of the existing data firewall vendors. No vendor predicted that a new revolutionary technology would be emerging for the next generation of firewalls.

Article Interview Resources

The following company officials were interviewed for this article:

- Mark Collier, CTO and VP of engineering at SecureLogix
- Kevin Johnson, product manager/security at Avaya
- Steven Johnson, president of Ingate Systems
- Mark Krynak, product marketing at Checkpoint Software Technologies
- Chris Roeckl, director of corporate marketing and Mike Ehlers, product manager at NetScreen (now Juniper)
- Tom Russel, director of marketing, VPN/security business and Joel McFarland, manager, security appliances at Cisco
- Richard Schmidli, marketing and Rad Setheuramam, product manager at Nortel□

■ How will firewalls support real time applications like voice and video, and differentiate between supporting voice/video signaling and content?

The most important device to secure in the VOIP network is the call server. A firewall in front of the call server would only need to process the signaling packets (H.323, SIP, MGCP), not the voice or video payload packets.

There is also speculation that the future IDS will only monitor the signaling packets, with a later IDS generation processing the voice and video packets.

Both Avaya and NetScreen commented that performance would be a major issue when supporting voice conversations. Signaling processing will not be seriously affected by the performance of the firewall. An extra 100 ms delay for signal packet processing will probably not be noticed, but the same delay will be unacceptable for the voice packet processing.

These vendors believe IP-VPN tunnels will be used as the primary security tool for both the signaling and voice payload packets. Avaya mentioned a draft standard from the IETF, called MIDCOM (Figure 2). In this scenario, the firewall consults with the VOIP call server to get permission to allow a voice call to pass through the firewall (see "MIDCOM Standard.")

SecureLogix speculates that if the MIDCOM standard is not completed soon, vendors will produce their own proprietary solutions. Indeed, a newer company called Ridgeway Systems has a solution that is similar to MIDCOM, using a proxy server interacting with the call server and supporting H.323. The proxy server operates

behind the firewall on the trusted network, but only for voice traffic. The data traffic bypasses the proxy server.

SecureLogix also believes alliances may be formed among vendors supporting the proprietary solutions, making it more difficult for customers to mix "best-of-breed" security products. SecureLogix believes that performance issues are more important for voice than for video—customers will tolerate shaky video before they will tolerate shaky voice.

Inspecting signaling packets will require less processing than "bearer" packets, because there are fewer signaling packets. SecureLogic predicts that, in most traditional data firewalls, signaling inspection will be supported before deep packet inspection of voice packets.

Cisco predicts that special-purpose application-specific firewalls will enter the market, but that data firewalls, enhanced to support VOIP, will dominate. Because customers do not want more boxes to manage, Cisco foresees most enterprises buying an adaptable platform with quality of service (QOS). They expect that more security software (i.e., firewall functions) will be available to reside in the call server. Voice packet inspection will not be supported in the call server, since the call itself does not pass through the call server—only the signaling does.

Nortel also predicts that signaling security support will arrive first. Voice packet inspection will be offered later, once the performance issues have been addressed. They also doubt that support for proprietary signaling methods will be common, believing standard signaling (H.323, SIP, MGCP) will be the norm.

Signaling security will precede voice packet inspection

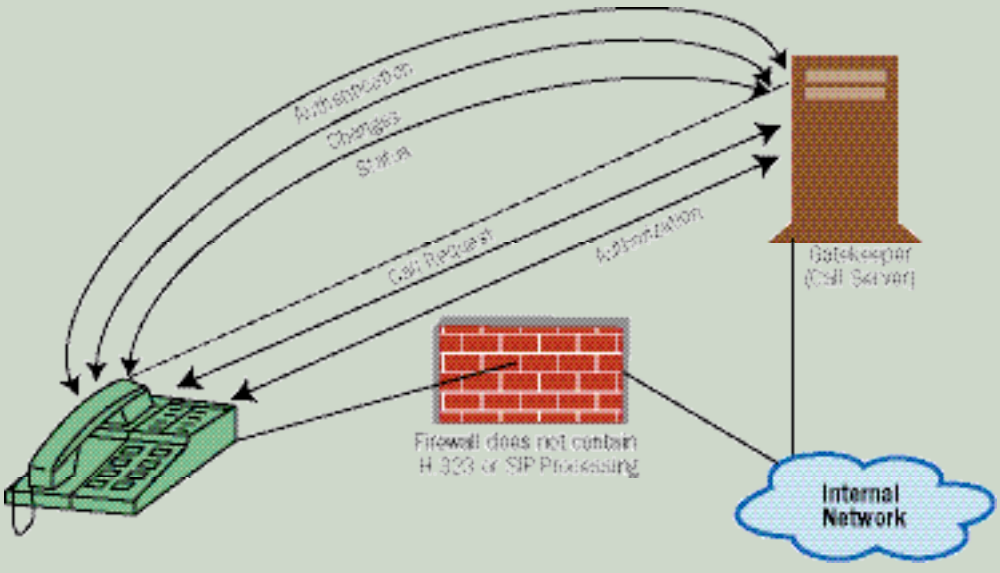
MIDCOM Standard

Middlebox Communication (MIDCOM) is an IETF draft standard, RFC 3304, that recognizes the need for applications to be able to communicate with security systems in the network, such as a firewall, IDS, IPS and Network Address Translation (NAT) device. The standard assumes one or more middle boxes in the data path, an external requesting entity (hardware or software) and, when the requesting entity is untrusted, another entity for consultation purposes.

An example would be a firewall corresponding with a VOIP gatekeeper (call server) in order to verify that an incoming call from a VOIP device should be allowed to pass through the firewall from the untrusted network. The standard specifically deals with the Real Time Protocol (RTP) and Real Time Control Protocol (RTCP) used in VOIP. One of the goals is to remove stateful inspection of VOIP protocols (H.323 and SIP) from the firewall to improve scalability and performance, thus reducing the cost of firewalls.

The standard is also intended to deal with the problems that NAT causes for voice over IP calls (see *BCR*, April 2003, pp. 55–58). It is unlikely that the standard will become widely used. Proprietary approaches mimicking the behavior of MIDCOM are already appearing, further diluting the possibility the MIDCOM standard will survive□

FIGURE A Midcom Operation



Avaya already has firewall software in some of its VOIP products. These also support transmission encryption using the Advanced Encryption Standard (AES). Avaya intends to protect signaling to and from the call server first, then focus on the voice conversations among gateways and IP telephones.

■ **Will the next generation firewall perform voice and video pattern analysis?**

For years, pattern analysis of legacy voice calls has been performed to reduce abuse and misuse. The Call Detail Record (CDR) of a PBX can be used to look for unusual calling times, origination and destination locations, call length, call frequency and access to unauthorized phone numbers.

Pattern analysis for VOIP will have to go deeper into the call itself and ensure that the packets are for VOIP and are not another device masquerading as a VOIP device in order to enter the trusted network.

None of the currently available firewalls offers speech packet pattern analysis

Voice over IP signaling packets:

- Should normally occur at the beginning and end of the call, unless features like call waiting are used.
- Will be transmitted over one or two static TCP or one UDP port number(s).
- Will be limited to a small number of predefined formats.
- Verify that IP phone registration will only interact with a few predetermined IP addresses.
- Should be authenticated as being transmitted by an authorized device, not a proxy impersonator.
- Should not be modified when the control packets are passed between proxies across the network.
- Should not be broadcast or multicast like a broadcast of disconnect packets.

VoIP voice packets:

- Are usually constant in length during a call.
- Are small, usually 20 to 120 bytes.
- Arrive at a constant rate.
- Arrive at the destination with a near-constant time between packets.
- Are half duplex in transmission, except during arguments.
- Have a digitized content that follows voice patterns; i.e. the content does not change significantly on a byte-by-byte basis.
- Are effectively filled with null bytes when silence occurs during the call, unless silence suppression is used.

None of the currently available firewalls can perform this type of pattern analysis. All the respondents felt signaling pattern analysis would probably be performed in the next generation, though Avaya and Nortel say that this level of inspection will produce performance problems for firewalls. Nortel believes that the VOIP pattern analysis is not a service provider issue but may be an issue for enterprises. Their service provider customers have not requested pattern analysis in the firewalls. NetScreen/Juniper believes that when speech packet pattern analysis is available, this function will be supported in IDS, rather than a firewall.

■ **What will happen with the current IDS and IPS products?**

The Gartner Research Note, "Four Paths to True Network Security," by Richard Stiennon, discusses the future of firewalls, IDS and IPS products. Although media analysts and consultants agree with some of the report's conclusions, many object to the prediction that IDS and IPS products will disappear in the future.

All our respondents predict that, for the low-end market, the firewall, IDS and IPS will be one product. This will be especially true for the SOHO market, where performance issues will be non-existent, since there will be only one, or a very few, users behind the firewall. These customers cannot afford multiple boxes, nor can they manage them.

Vendor opinions differed as to whether enterprise-class firewalls will continue to exist as separate units or be integrated. Cisco, Ingate and Nortel predict that there will be a market for the standalone IDS. In fact, they expect the market to increase as IDS-derived network forensic information becomes more important. They also say the IDS may even measure performance.

Avaya, SecureLogix and NetScreen/Juniper believe the IDS and IPS will be combined, except where the budget justifies separate units. Having separate units is a good idea for customers with strong security auditing requirements, but it's not very affordable. Only a very few vertical markets (such as defense and financial) would desire separate units so that one vendor can audit another's product. Checkpoint believes that this is a major reason for retaining a separate IDS.

■ **Can Firewalls Be Futured-Proofed?**

With the galloping pace of technology advances, it is a wonder that anyone believes we can "future-proof" firewalls. Yet the customer must have some assurance that the security investment made today will not be obsolete tomorrow.

The consensus among our respondents is that security devices will continue to evolve and that software more than hardware will provide some measure of future-proofing. Ingate's Steve Johnson believes the customer expects the security

device to be future-proofed during the write-off (capitalization) period. He therefore sees future-proofing as a financial issue. Other participants see future-proofing as a technical, rather than a financial issue.

All participants feel that three to four years is the limit for future-proofing security devices. Ultimately, the customer must decide when to purchase a device. If the procurement decision is delayed, the lifecycle of the device that's eventually purchased may be half over before the box is installed, thereby shortening its useful life.

■ Will next-generation firewall functions affect personal firewalls? If so, how?

The real question is: "Can the corporate firewall trust a remote security device?" Most of the vendors interviewed for this article do not have a personal firewall product line, and if they go in that direction in the future, it would most likely take the form of an acquisition.

Application security, security management and standards are the next wave of firewall issues

The possibility that personal firewalls will interact with the corporate firewall is not on the near horizon. The interaction may have the corporate firewall verifying the security performed by the personal firewall and trusting it to perform security functions, to reduce the load on the corporate firewall. All respondents agree that teleworking and VOIP will become synonymous as these two applications grow. SecureLogix recommends that, in order for corporate and personal firewalls to interact, the same vendor should produce both. Avaya feels that the MIDCOM standard might become useful for the interaction, but the standards committee has not formally addressed this issue.

So for the foreseeable future, the personal firewall will protect its local resources, not work in conjunction with the corporate firewall. The personal firewall will also be generic and not perform security for specific applications. For VOIP, the personal firewall will look like most data firewalls. VOIP security will be implemented through VPN tunnels.

■ Are the products migrating to an all-hardware or software solution?

Three opinions emerged concerning the balance of hardware and software solutions for the firewall: Use an ASIC, implement with network processors or use a standard processor platform.

NetScreen/Juniper focuses on the ASIC for its performance advantages, however, they also believe there will always be some software components to ensure that the device can be updated as new security considerations arise.

Ingate prefers the standard processor-based platform. This design does not have the high performance of the ASIC, but is stable and easy to support. Their opinion is that, for most customers, the ability to use the same software on ever-improving processor hardware platforms allows them to future-proof their system. As traffic increases, hardware can be changed while retaining the investment in software.

CheckPoint also points out that this approach is useful when the firewall function is embedded in other devices such as IP gateways, IP phones, Web phones and call servers.

For Avaya, Cisco and SecureLogix, the network processor provides most of the performance benefits of the ASIC while retaining the flexibility of the software approach. Compared to the ASIC-based design, this reduces the time to market for major new functions.

Nortel believes that, with their multiple-box load-balancing approach, the ASIC will be used for repetitive-function performance-based design, while the network processor will be used for the more specialized functions. Software on a network processor delivers flexibility while the ASIC delivers performance.

Conclusion

This is not the last article on what the firewall of the future will look like. Security is a fast-growing industry. For every new protection tool, there will be someone trying break through to the trusted network. The next most likely set of articles will focus on application security, security management and standards. Get ready for the next wave of predictions□

Companies Mentioned In This Article

Avaya (www.avaya.com)

Checkpoint Software Technologies (www.checkpoint.com)

Cisco (www.cisco.com)

Ingate Systems (www.ingate.com)

NetScreen (now Juniper, www.juniper.net)

Nortel (www.nortelnetworks.com)

Ridgeway Systems (www.ridgewaysystems.com)

SecureLogix (www.securelogix.com)