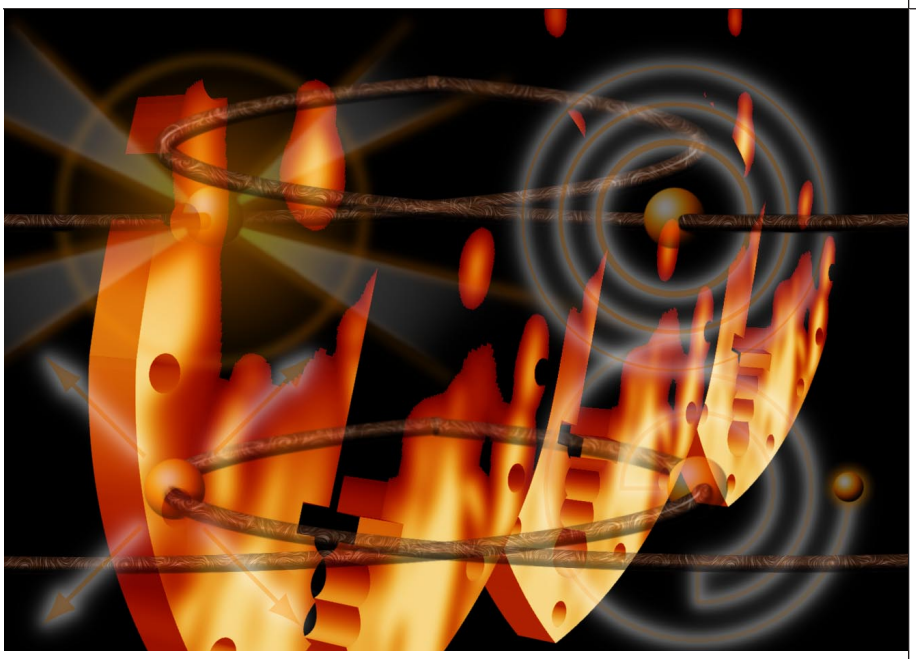
A Network Associates
Executive White Paper



The Active Firewall

The End of the Passive Firewall Era

A Dynamic New Model
for Integrated Active Response
Firewall Security

network ASSOCIATES

Table of Contents

Introduction

"Firewall"... the name itself conjures up vivid images of strength and safety. What executive wouldn't want to erect a flaming bastion of steel around the corporate network to protect it from unseemly elements lurking on the public Internet?

Unfortunately, this imagery no longer matches reality. In recent years, companies across all industry segments have been gradually tearing down the walls that once isolated their private networks from the outside world. Internet-based technologies have allowed significantly tighter links with customers, remote employees, suppliers, and business partners at a fraction of the cost. In many industries, it is no longer possible to remain competitive without extending the virtual corporation far beyond its previous boundaries.

With so many users rapidly approaching the enterprise from different points of entry, it is no longer possible for yesterday's security technology to adequately protect private networks from unauthorized access. The vast majority of firewalls in use today serve only as a *passive* enforcement point, simply standing guard at the main door. They are incapable of observing suspicious activity and modifying their protection as a result. They are powerless to prevent attacks from those already inside the network and unable to communicate information directly to other components of the corporate security system without manual intervention.

Recent statistics clearly indicate the danger of relying on passive security systems in today's increasingly interconnected world. According to the FBI, corporations reporting security incidents last year lost an average of $570,000 as a direct result, a 36 percent increase from the year before (1998 Computer Crime and Security Survey FBI/Computer Security Institute). And since the vast majority of security breaches are never reported, actual losses may be even higher.

In perhaps the most frightening statistic of all, it is estimated that as many as 95 percent of all computer security breaches today go completely undetected by the companies who are victimized. In a well-publicized security audit conducted recently at the Department of Defense, security consultants were asked to attack the DOD network and report back on their findings. Over a period of several months, auditors reported that fewer than 4 percent of all systems broken into were able to detect the attack. Even more disturbing, fewer than 1 percent responded in any way to the attack (Report on Information Security, GAO).

The solution to this growing problem will never be found by simply upgrading an existing passive firewall or buying the latest hot security product and hoping for the best. What's needed is an entirely new model of integrated network security which recognizes the strengths of the firewall as an enforcement point, then empowers it to *actively* communicate with other security tools responding in concert to new attacks and modifying security measures accordingly. What is required is a distributed firewall system that integrates alarms, scanners, and central monitoring to implement a company's security policy and effectively prevent security breaches from both inside and outside the network. *What's needed is an Active Firewall.*

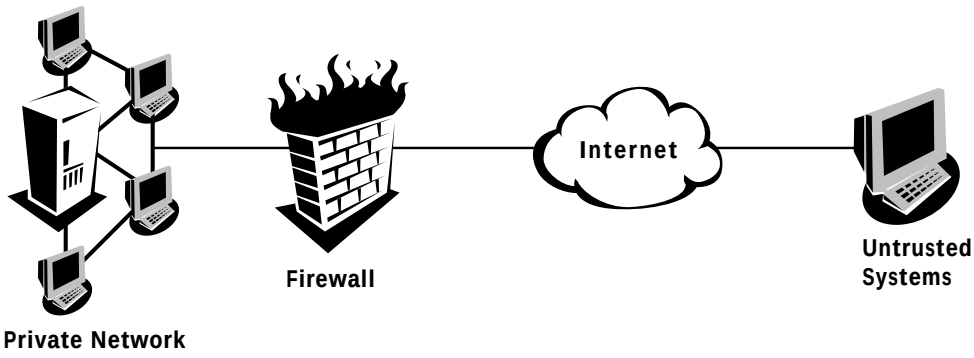
What is a Firewall?

It is nearly impossible to compete in today's fast-paced business environment without connecting your private network to the public Internet and other untrusted networks. Your employees need to rapidly access and share information with customers, suppliers and the world at large if you are to stay ahead of the competition. Unfortunately, such connectivity provides an easy path for untrusted parties on the outside to penetrate a company's private network and access or tamper with internal information and resources.

A firewall is a security enforcement point that separates a trusted network from an untrusted one, such as the Internet (see Figure A). Firewalls screen all connections between two networks, determining which traffic should be allowed and which should be disallowed based on some form of security policy determined in advanced by the security administrator.

FIGURE A

A firewall is a security enforcement point that separates a trusted network from an untrusted one, such as the Internet.



Firewalls are most commonly used to protect an internal corporate network from the public Internet, but are increasingly being deployed internally as well as to separate individual departments and remote offices from the rest of the network or from external users who may gain access without going through the primary firewall (see Figure B). Using firewalls throughout an internal network gives security administrators the ability to apply different access control rules across a variety of working groups and network subnets as appropriate. Internal firewalls also enhance security by providing a layer of protection against internal breaches. Setting up a separate firewall in front of the human resources department, for example, would make it far more difficult for contractors or employees in other departments to access sensitive HR data.

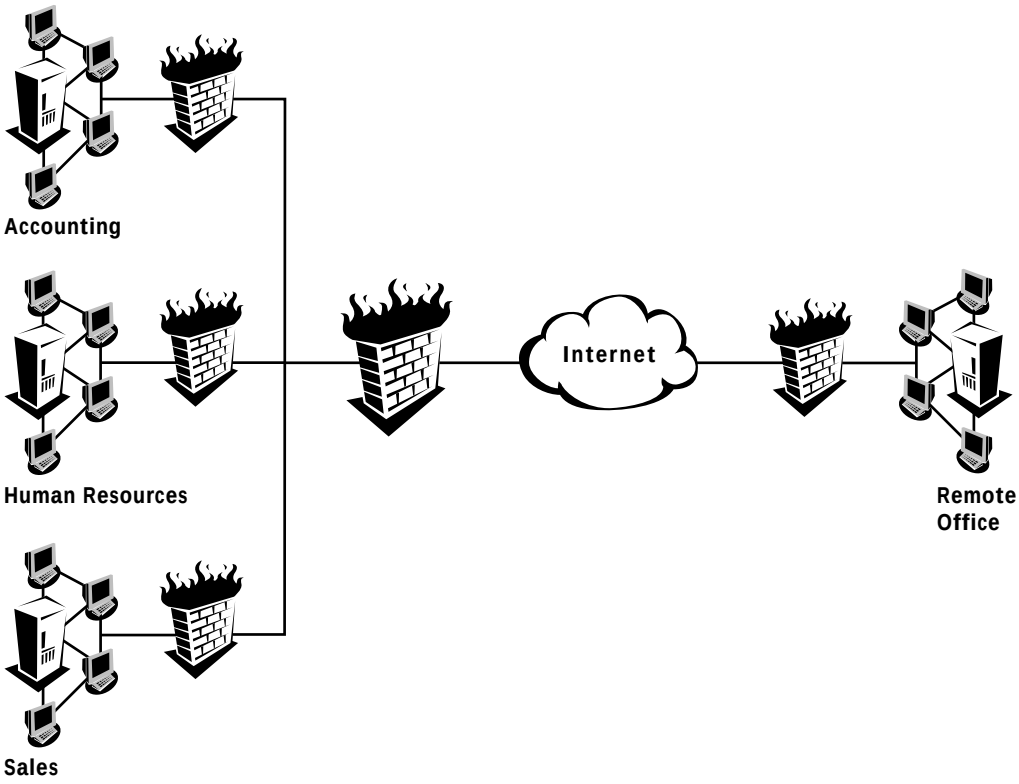


FIGURE B

Firewalls are increasingly being deployed internally as well as to separate individual departments or workgroups from the rest of the network.

The Virtual Corporation

While firewalls remain the best way to examine attempted connections to a private network, it is no longer adequate to protect an entire corporate network by simply stationing a passive guard at the front door.

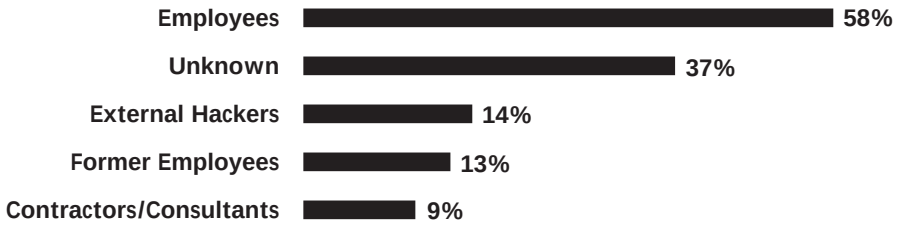
The rapid adoption of Internet-based technology has allowed companies to develop increasingly tighter ties with customers, suppliers, partners, and remote employees. Most companies now realize that they can achieve substantial cost savings and frequent competitive advantages by extending broad connectivity far beyond the walls of their physical network. The more “virtual” a company becomes, in fact, the greater its ability to adapt to changing market demands ahead of its competition. Corporations who fail to embrace this trend may find themselves unable to compete successfully in the new world order.

Unfortunately, the virtual corporation can also be a dangerously insecure place to conduct business. Electronic business applications often provide unprecedented external access deep inside a company's network infrastructure. Once users are behind the firewall, security holes in operating systems, application services, databases, and communications software may expose the entire enterprise to compromise.

In addition, firewalls can only affect traffic that is routed through them. If an internal employee or contractor attempts to gain unauthorized access to a local server, for example, the corporate firewall has absolutely no way to see or respond because both parties are already behind the firewall. Despite the publicity given to Internet "hackers", most research surveys indicate that more than half of all security breaches originate with employees, contractors, consultants, and other internal users (see Figure C).

FIGURE C

Most security incidents today, whenever malicious or unintentional, originate from employees, contractors, and consultants already behind the primary Internet firewall.



MULTIPLE RESPONSES ALLOWED
Source: Information Week/PricewaterhouseCoopers, 1998

In Search of a Solution

The inability of standalone firewalls to protect networks from increasingly sophisticated security threats has given rise to many new technologies over the past few years. Products such as security vulnerability scanners, intrusion detection monitors, virtual private networking solutions (VPNs) and firewall-based virus scanners, for example, were each designed to supplement the protection of a traditional firewall. In the same way that the security in your house increases when you add an alarm system to its existing locks, the risk of network security breach is diminished with each new security product deployed. To be truly effective, however, these security components must become seamlessly integrated with the firewall itself.

As these new supplemental security technologies become mature, the role of the firewall itself is evolving from that of a standalone system enforcing access rules into that of a distributed firewall system involving several tightly integrated components positioned strategically throughout the network (see Figure D). As the threats of network penetration extend beyond a frontal attack at the Internet gateway, our concept of what a firewall is must expand as well.

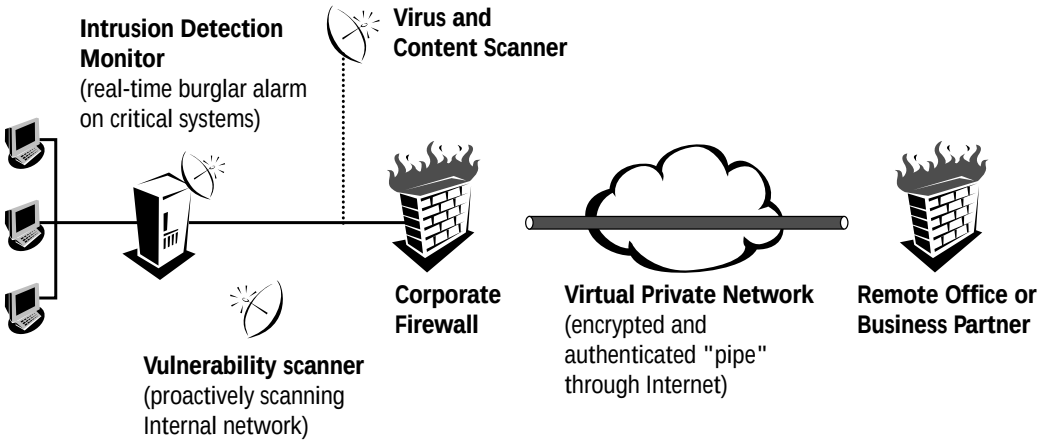


FIGURE D

Products such as vulnerability scanners, intrusion detection monitors, VPNs and firewall-based virus scanners were each designed to extend the protection of the standalone firewall. To be truly effective, they must become seamlessly integrated with the firewall.

A Complete Firewall Security System

Consider for a moment the physical security components that protect a public building such as a museum. Each of these components is an integral part of a complete security system designed to keep out intruders. No single element is sufficient in and of itself.

Guards at the Door

In a secured facility such as a museum, security guards are stationed at each of the perimeter doors. All other doors and windows are securely locked to ensure that entry can be gained only by passing through a guarded door. The primary job of each guard, of course, is to ensure that no unauthorized personnel gain entry through that door. In a large museum, you will also likely find guards posted at internal doors between adjoining wings of the museum.

In a computer network, firewalls play the role of the security guard, scanning all network traffic to determine which connections should be allowed and which should be rejected. Guards protecting internal wings of a large facility are analogous to Intranet firewalls placed in front of individual departments or internal facilities.

Testing the Locks

Another critical aspect of securing a physical building is the process of routinely testing the various doors, windows, and alarm systems to ensure that everything is working properly and that no new security holes have opened up. Because a museum is filled with people each day, both employees and visitors, it is critical to test the various security systems at the end of each day to ensure that no alternative entry points were left open inadvertently.

This problem is magnified exponentially in a network environment where thousands of potential entry points are in a constant state of flux. Security vulnerability scanners are tools that allow network security administrators to routinely test their own network for potential weaknesses or security holes. In much the same way that virus scanners routinely scan for malicious code, vulnerability scanners routinely check for security policy violations and weaknesses. These tools also generate reports that identify any potential vulnerabilities, rank their importance, and offer suggestions for how they can be secured. Because networks are constantly changing, new vulnerabilities open up every day. Proactively scanning for vulnerabilities on a regular basis is an essential part of any network security solution.

Motion Sensors, Security Cameras, and Alarms

In addition to posting guards at each entrance point and routinely checking for problems, museums also typically install motion sensors on valuable exhibits. If anyone in the building, including a trusted employee, attempts to tamper with a protected painting or artifact, an alarm sounds. Similar alarms may be installed on interior doors that lead to private offices, exhibit storage, or other confidential areas. Security cameras will also likely be installed near important exhibits to record suspicious activity and create a record for analysis if break-in or tampering is suspected.

In a network environment, this role is played by real-time intrusion detection monitors. Intrusion detection monitors watch internal network traffic and specific servers in real time for signs of attack. If a penetration is detected, these systems can trigger alerts to an administrator warning of a potential attack in progress. Intrusion detection monitors also provide security administrators with log files that serve as an internal security audit trail. Intrusion protection sensors are often the only way to detect security breaches that originate inside the protected network, behind the firewall. Intrusion detection monitors against outside hackers who gain access through an improperly configured firewall.

Metal Detectors

While a patron entering our museum may look harmless, we may also want him or her to pass through a metal detector at the main entrance to ensure that no dangerous objects enter the museum. If an object such as a pocket knife is rejected by the museum, but has been carried in without malicious intent, it may be possible to simply confiscate the banned item and allow entrance to the patron who brought it.

In the same way, network security administrators should add virus and content scanners at each Internet gateway to scan for the presence of malicious code such as viruses, trojans, or hostile Java and ActiveX applets. Viruses that have infected an otherwise secure email transmission may be removed at the gateway, allowing the original message to continue as a clean document.

Central Control Room

Perhaps the most important component of a good physical security environment is the central control room. From this room, security personnel monitor security cameras throughout the entire facility, maintain two-way radio contact with all guards, and listen for alarms. The security personnel who monitor such rooms operate against a prescribed security policy. If they see a particular event occur under a certain set of circumstances, they initiate a pre-established response. Security issues that fall within the prescribed policy are responded to automatically, without involving any outside personnel. Only events that require supervisory decisions are escalated to senior security officers.

In a physical security environment, the central control room also serves as a way to correlate events that might otherwise appear insignificant. Suppose, for example, that one of the security guards at our museum reported the presence of an unmarked van in the parking lot after hours. Thirty minutes later, another guard reported seeing a brief flash of light in the bushes near the west wing, while an internal security monitor noted a malfunctioning motion sensor inside the same wing. Independently, these events would merit only caution and a note in a log book. Together, however, they may indicate a pattern that warrants a response.

The same principles hold true in the information security arena. The only way to provide meaningful integration between distributed security components is to coordinate all communications through a central event manager. In this model, all monitors, sensors, and scanners on the network report events into the event manager. If a response is required, the event manager initiates the resultant action based on the security policy set in advance by the security administrator.

Using a central event manager gives security administrators far more control over the security of their networks without unnecessarily disrupting normal business processes. No administrator can reasonably keep pace with the sheer volume of information generated daily by a company's firewall, vulnerability scanners, intrusion detection monitors, traffic analyzers, and other sensors around the network. By routing selected information through a central event manager and applying a set of policy filters, however, it becomes possible to automate the search for potentially related events that might otherwise slip under the radar.

Putting it all Together

Creating a network environment that is secure from both internal and external compromise clearly involves more than just installing a firewall at the Internet gateway. What's required is a more comprehensive distributed firewall system incorporating complementary solutions such as vulnerability scanning, virus and malicious code scanning, intrusion detection, virtual private networking and internally deployed firewalls. Companies who rely on a passive standalone firewall at the Internet gateway are locking the door, but potentially leaving all the windows open. Regardless of how good the lock is, everything inside is at risk.

The Active Firewall Concept

In a physical security environment, we also take for granted that the various security components interact with each other, working in concert to share information and adapt to new threats as they occur. When a guard hears an alarm go off on an exhibit, he adapts his actions accordingly. He might, for example, temporarily block all passage through his door until the incident is resolved. Or he might simply increase the level of security checks conducted on those leaving the museum for a period of time. If a side access door is found to have a broken lock during a routine check, security is increased at that exit until the problem can be resolved. If a guard spots suspicious activity or an attempted break-in, he immediately radios an incident report to the central monitoring room so that other guards and those watching the security cameras can be on the lookout.

What if our museum guard ignored alarms, turned off his radio, and responded to an attempted break-in by simply jotting down a written note, but making no effort to notify others? He would probably be fired for incompetence, even if his door was never penetrated. Yet we are often forced to accept this kind of passive performance from our corporate security systems today. Our firewalls may be guarding their respective doors effectively, but they are not empowered to communicate or respond to changing threats and conditions.

The type of active communications we have long taken for granted in the arena of physical security are virtually nonexistent in the realm of network security. Traditional firewalls do not communicate with vulnerability scanners. And they are largely deaf to the alarms of intrusion protection monitors. When suspicious activity is observed elsewhere on the network, traditional firewalls do not increase the detail in their log files to create a better audit trail. They cannot correlate observations from around the network, nor can they close a known security hole without manual human intervention.

To truly address the rapidly growing security threat, firewalls must evolve from passive guards simply watching the gate into active guards working in concert with other security components on the network to actively respond to changing threats.

Making Active Firewalls a Reality

Several of the leading security vendors are working to solve such issues. Some have formed partnerships or licensing agreements to cross-bundle complementary security products. Others have announced their intent to develop proprietary APIs (application programming interfaces) that would enable other vendors to integrate around their product line. While such efforts are to be commended, they do not yet offer a practical solution to the problem of passive firewalls in a world of constantly changing threats.

Network Associates believes the answer to building and deploying practical active firewall solutions lies in integrating security products around an open event management system, in much the same way that a physical facility directs all communications through a central monitoring room. This method offers several important advantages.

1) More flexible security policy administration.

With a central event management system receiving all alerts and coordinating all resultant actions, administrators can apply a single security policy that takes into account the behavior and activity of multiple scanners, sensors, and monitors at the same time. Hard coded integration between individual security products simply does not allow for this flexibility. Even if an intrusion detection vendor were to offer working integration with a firewall vendor, for example, the two products would have no visibility into events recorded by other security products.

2) Single point of integration.

Hard-coded integration between individual point products is also problematic when new versions are released. In most cases, maintaining working integration requires multiple vendors to coordinate release schedules and have intimate knowledge of each other's product road maps. Coordinating all integration through an open event manager eliminates this problem. As long as each component product speaks to the event manager, integration is maintained, regardless of whether or not other connected products are current.

3) Far fewer complexities.

Most industry observers are hard pressed to find examples of multi-vendor coalitions in any industry segment that have actually produced meaningful integration between disparate products. In most cases, multi-vendor coalitions fail because members are simply unwilling to make integration a priority by coordinating releases and disclosing product road map details. In other instances, integration efforts break down because the founding member fails to deliver reliable APIs and integration guidelines. Even integration efforts that do succeed initially frequently stumble when it comes to ongoing support of the multi-vendor solution.

"Of the different alternatives available for automating security policies, the use of a central event manager is the most practical. Using an event manager, it is possible to tighten up and automate the security of a company's IT infrastructure... Hard-coded integration between point products has limited appeal to many organizations because it is typically inflexible, can cause problems when new versions are rolled out, and usually requires the cooperation of multiple vendors to intimately coordinate product road maps."

- Hurwitz Group, 1998

The Network Associates' Solution

With Gauntlet* Active Firewall, Network Associates is leading the charge out of the Passive Firewall Era into the new Active Firewall Era. Gauntlet Active Firewall integrates multiple security products into a single system that is truly more than the sum of its parts (see Figure E). This groundbreaking solution combines proactive vulnerability scanning, real-time intrusion detection monitoring, anti-virus scanning, and virtual private networking into a single active firewall system:

Gauntlet Firewall	Widely regarded to be the world's most secure firewall
CyberCop Scanner	Proactive scanning of internal network for security vulnerabilities
CyberCop Monitor	Real-time monitoring of critical systems for signs of attack
WebShield Anti-virus	Scanning for viruses and hostile code at the firewall
Gauntlet VPN	Virtual private networking built into the firewall

Gauntlet Active Firewall also includes two important middleware components that make its integration a practical reality.

Event Orchestrator	This standards-based event manager coordinates all integration
Net Tools PKI Server	A universal PKI (public key infrastructure) server ships with every Gauntlet Active Firewall to ensure that inter-application communications cannot be altered or forged. For customers who already have an existing PKI, Gauntlet Active Firewall supports certificates from PKI leaders such as VeriSign and Entrust.

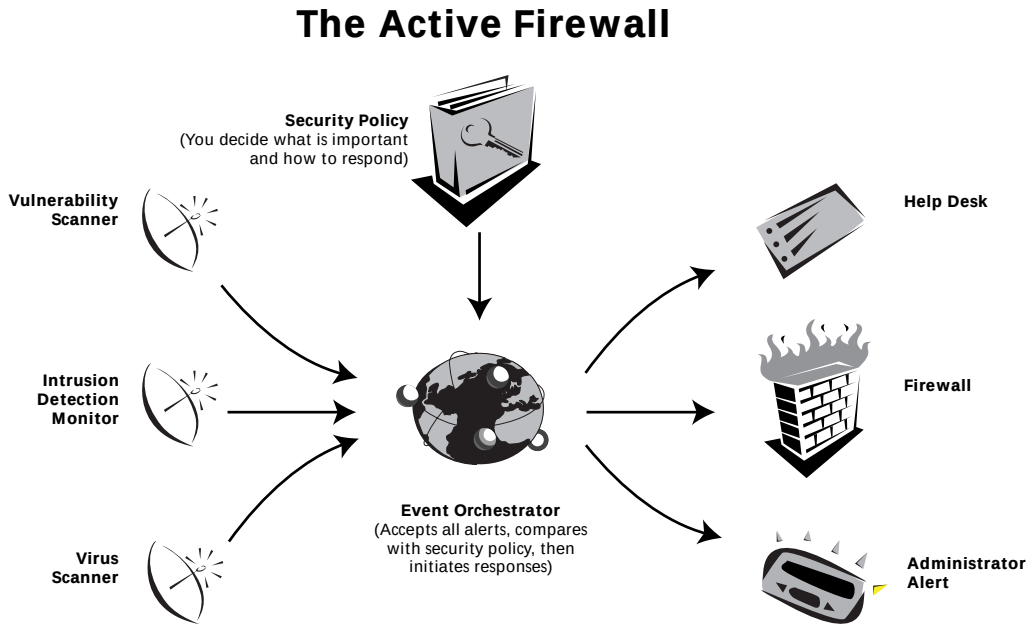


FIGURE E

Sensors and scanners on the network (left side of diagram) forward security information to Event Orchestrator where it is applied against the corporate security policy. If actions are required, Event Orchestrator initiates them (right side).

Typical Scenario

Suppose CyberCop Scanner is scheduled to run through a series of routine vulnerability scans on the corporate network at 2:00am every morning. During one of these scans, CyberCop Scanner discovers that an employee has set her PC up as an insecure ftp server, inadvertently exposing data on the private network to attack. CyberCop Scanner forwards this information to Event Orchestrator. Event Orchestrator receives the information and compares it against the customer's security policy to determine the appropriate course of action. After consulting the security policy, Event Orchestrator forwards an encrypted and authenticated command to the Gauntlet Firewall instructing it to shut down all communications with that specific ftp server until the IT staff arrives the following morning.

A second Event Orchestrator command may then be sent to the help desk, generating a trouble ticket that describes the problem in detail. When the user arrives in the morning and calls the help desk to find out why her ftp service is not working, the IT staff is already aware of the issue and can advise her of the security risks she exposed through her actions.

Because Gauntlet Active Firewall uses an extensible modular architecture and is based on an open event management system, its actions can be customized to meet the unique security requirements of each customer. In all circumstances, the customer determines which security scenarios require supervisory intervention and which responses should be automated.

Features in Search of a Product

As a result of these emerging trends, products like vulnerability scanners, intrusion detection monitors, firewall-based virus scanners, and VPNs are rapidly evolving from standalone point products into integrated features of a firewall.

This trend is a natural part of a product life cycle that has played itself out time and time again. Ten years ago, for example, spell checkers and font packages were sold independently by multiple vendors at a premium. Today, they are integrated seamlessly into every word processor we purchase as standard features. Over time, the firewall market is almost certain to follow suit as vendors like Network Associates lead the way towards meaningful and compelling integration between previously disparate products.

Summary

Today's technology advancements offer greater opportunities than at any time in the history of computing. With those opportunities, however, come equally significant security risks. A few short years ago, security administrators could reasonably protect most networks from intrusion by installing a single passive firewall at their Internet connection. Today, the lines between corporate networks have become increasingly blurred as companies develop closer electronic ties with customers, suppliers, partners, and remote employees. As these "virtual" networks extend their boundaries into the outside world, corporate firewalls must be reinvented to keep pace.

Many industry observers see the role of the firewall expanding to include complementary "features" such as vulnerability scanning, virus scanning, intrusion detection monitoring, and virtual private networking. When combined with the firewall, these additional features help to form a more complete distributed firewall system that has visibility into multiple aspects of the corporate security environment.

Tomorrow's distributed firewall systems will only be successful if the various components are also empowered to interoperate in a meaningful way. Without the ability to rapidly communicate with other security components, a firewall is like a museum guard who watches a thief enter a nearby window, but says nothing because it is "not his job" to watch the window. To truly address the rapidly growing security threat, firewalls must evolve from *passive* guards simply watching the gate into *active* guards working in concert with other security components strategically placed throughout the network to actively respond to changing threats.

Gauntlet Active Firewall from Network Associates addresses the passive firewall problem by integrating multiple security products into a single system that is truly more than the sum of its parts. This groundbreaking new solution combines vulnerability scanning, intrusion detection monitoring, anti-virus scanning, and virtual private networking into a single active firewall system in which components work together in concert to actively respond to changing security threats. With Gauntlet Active Firewall, Network Associates is truly leading the charge out of the Passive Firewall Era into the new Active Firewall Era.

network ASSOCIATES

Who's watching your network

For more information on products, services, and support, contact your authorized Network Associates sales representative

CORPORATE HEADQUARTERS

3965 Freedom Circle
Santa Clara, CA 95054
TEL: (408) 988-3832*
FAX: (408) 970-9727

**Call for additional World Wide Sales Offices*

Visit our Website

http://www.nai.com

P/N 6-VZG-ACT-001 1/99