The Cisco ASA 5500 as a Superior Firewall Solution

The Cisco ASA 5500 Series Adaptive Security Appliance provides leading-edge firewall capabilities and expands to support other security services.

Firewalls provide the first line of defense in any organization's network security infrastructure. They do so by matching corporate policies about users' network access rights to the connection information surrounding each access attempt. If the variables don't match, the firewall blocks the access connection. If the variables do match, the firewall allows the acceptable traffic to flow through the network.

In this way, the firewall forms the basic building block of an organization's network security architecture. It pays to use one with superior performance to maximize network uptime for business-critical operations. The reason is that the rapid addition of voice, video, and collaborative traffic to corporate networks is driving the need for firewall engines that operate at very high speeds and that also support application-level inspection. While standard Layer 2 and Layer 3 firewalls prevent unauthorized access to internal and external networks, firewalls enhanced with application-level inspection examine, identify, and verify application types at Layer 7 to make sure unwanted or misbehaving application traffic doesn't join the network. With these capabilities, the firewall can enforce endpoint user registration and authentication and provide administrative control over the use of multimedia applications.

The Need for Speed

As networks evolve to increase business productivity, collaboration, and communication, the firewall is evolving in parallel. The Cisco® ASA 5500 Series Adaptive Security Appliance, for example, was purpose-built to support both standard policy enforcement and application-level firewall inspection for hundreds of application protocols. Independent third-party tests show that it currently outperforms the other firewalls in its class. In addition, it ranked in the highest position in worldwide market research company Gartner's firewall "Magic Quadrant" in June 2006 for leadership and vision.

The Cisco ASA 5500 Series' high-performance application-inspection capabilities automate the network to treat traffic according to detailed policies based not only on port, state, and addressing information, but also on application information buried deep within the packet header. By comparing this deep-packet inspection information with corporate policies, the firewall will allow or block certain traffic. For example, it will automatically drop application traffic attempting to gain entry to the network through an open port—even if it appears to be legitimate at the user and connection levels—if a business's corporate policy prohibits that application type from being on the network.

Such unwanted traffic might consist of non-business-related, peer-to-peer traffic that consumes large volumes of bandwidth. It might constitute instant messaging traffic other than traffic that conforms to the corporate instant messaging standard. Or it might be any other non-critical application traffic that the corporation chooses to filter off the network.

The Cisco ASA 5500 Series Adaptive Security Appliance detects and filters protocols with industry-leading performance. In September 2005, Miercom, an independent testing laboratory in Cranbury, New Jersey, demonstrated that the midrange Cisco ASA 5520 performed more than six times better in delivering HTTP (Web) traffic throughput over TCP/IP connections than its three closest competitors. At the same time, the Cisco ASA 5520 scored 100 percent overall on threat detection success; the competing devices, by contrast, performed with just 30 to 40 percent accuracy rates.

With these levels of performance and security accuracy, businesses can use the Cisco ASA 5500 Series to expand their network deployments and applications securely and at speeds that accommodate the response-time demands of corporate users.

Enterprise Network Security Components

The key components of an enterprise network security architecture include:

- Firewalls deployed at the traditional corporate WAN-edge perimeter, at branch-office WAN edges, and strategically throughout the internal enterprise to ensure legitimate user access
- IPSs to filter malware off the network
- VPNs for encryption (both IPsec for site-to-site connections and SSL for mobile connections) to protect against data theft
- Endpoint, or anti-X, security to keep remote and mobile user connections free of viruses and compliant with required software and security versions

Adding Intrusion Prevention

Gartner's definition of a next-generation firewall is one that combines firewall filtering and intrusion prevention systems (IPSs). Like firewalls, IPSs filter packets in real time. But instead of filtering based on user profiles and application policies, they scan for known malicious patterns in incoming code, called signatures. These signatures indicate the presence of malware, such as worms, Trojan horses, and spyware.

Malware can overwhelm server and network resources and cause denial of service (DoS) to internal employees, external Web users, or both. By filtering for known malicious signatures, IPSs add an extra layer of security to firewall capabilities; once the malware is detected by the IPS, the system will block it from the network.

Next-generation firewalls, according to Gartner, integrate firewalls and IPSs such that traffic is inspected just once for both functions. By contrast, having to inspect traffic once for connection-layer access information and then again for malware would significantly slow down system throughput.

The Cisco ASA 5500 Series provides businesses with the flexibility to add IPS services to combat the additional malware. The Cisco ASA 5500 Series Firewall Edition operates as a standalone firewall appliance and inherently includes an VPN concentrator for handling encrypted sessions. To add intrusion prevention, organizations can install the Adaptive Inspection and Prevention Security Services Module (AIP-SSM) alongside the firewall in the system's chassis for single-pass firewall/IPS packet inspection.

A Cisco ASA 5500 Series Adaptive Security Appliance can be expanded to support not only IPS, but also other key security protection mechanisms needed throughout the enterprise: Secure Sockets Layer (SSL) VPNs and endpoint security (also called "anti-X" security). With this built-in expandability, businesses have the flexibility to adapt the appliance to meet their security needs,

depending on their specific requirements in each segment of the network. At the same time, standardizing on a single platform can reduce the overall operational cost of security.

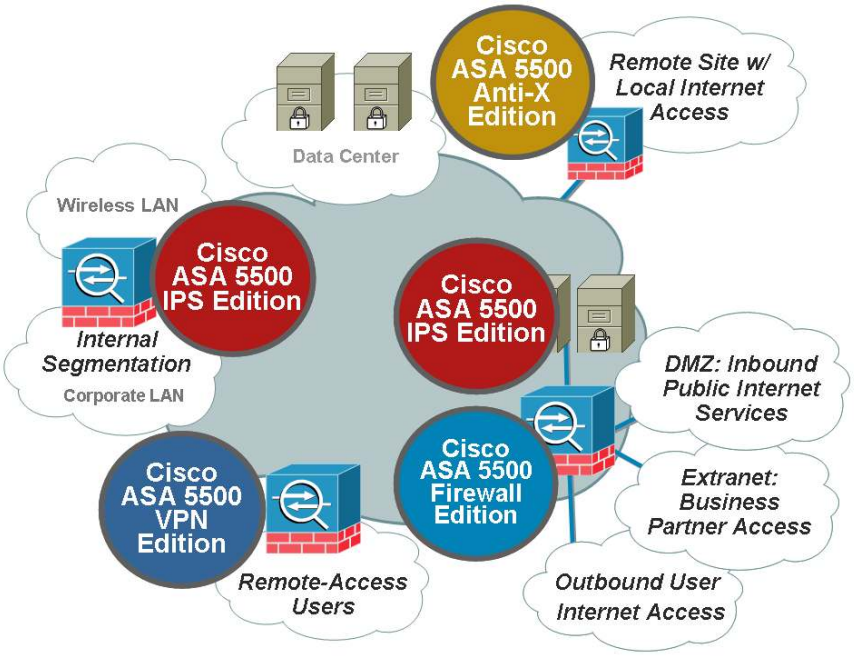
To further reduce costs, organizations that have consolidated servers and data centers can segment the Cisco ASA 5500 Series Adaptive Security Appliance into multiple “virtual” firewalls for scalability. In other words, a single physical Cisco ASA 5500 Series appliance can operate as several logical firewalls, allowing it to do the job of multiple devices and helping to reduce capital expenditures (CapEx). Cisco ASA 5500 Series appliances are “plug-and-play”: network administrators do not have to make any switch or router configuration changes in order to add them to the existing network infrastructure.

The Right Services for the Right Location

The Cisco ASA 5500 Series offers enterprises a comprehensive portfolio of services that are customized through product editions tailored for firewall, IPS, anti-X, and VPN support. These editions enable superior protection by allowing network administrators to deploy the right security services for the right location. Each edition combines a focused set of Cisco security services to meet the needs of specific environments within the enterprise network.

For medium-sized and large enterprises, a Cisco ASA 5500 Series appliance can function in a standalone fashion as a firewall/IPsec VPN concentrator, an IPS, an anti-X security system, or an SSL VPN concentrator. The Cisco ASA 5500 Series Anti-X Edition protects the corporate network from viruses in remote and mobile clients and checks to make sure remote devices are compliant with required versions of operating system, application, and security software. The VPN Edition adds support starting with licenses for 10 concurrent SSL VPN users, with additional SSL licenses available (Figure 1).

Figure 1. Cisco ASA 5500 Series Solutions—Business Solutions and the Corporate Network



Cisco ASA 5500 Series Adaptive Security Appliances can be deployed strategically throughout an organization for a defense-in-depth, best-practices approach to security, operating as any one of these devices in the specific segments of the network where each service is required. The

appliance can perform one of these roles in a certain part of the network and then be redeployed in another network segment supporting a different security function, should requirements change.

Alternatively, the appliance can support the multiple security functions in a single chassis, which is often a desirable and economical configuration for branch offices. To combine functions, the Cisco ASA 5500 Series appliance chassis supports modular blades for IPS and anti-X protection. SSL VPN usage simply requires additional software and licensing. As other modules and/or software capabilities are added to the Cisco ASA 5500 Series Firewall Edition, the firewall capabilities can remain enabled or be disabled, depending on requirements.

Larger enterprises are more likely to have the budgets and staff expertise to select, install, and manage separate best-in-class products, possibly from different vendors. However, next-generation converged devices are a solid alternative: they closely integrate security functions not only for convenience and CapEx savings; they also offer stronger security, because the separate functions can share security-event information. They also afford higher performance, in that a single-pass packet inspection can scan for multiple threats. As such, converged-function security devices are likely to capture the interest of larger enterprises.

The Cisco ASA 5500 Series is highly accurate and, as noted, outperforms its competition. The Miercom independent lab tests mentioned previously compared firewall performance, unified firewall and IPS performance, IPsec VPN throughput, and connections-per-second performance. The Cisco ASA 5520 delivered more than three times the Triple Digital Encryption Standard (3DES) IPsec VPN throughput than other devices in its class, and its connection-establishment rate was four times higher than its competitors' rates. In the Miercom tests, a total of 126 threats, or test cases, were presented to all four systems tested. Each test case was executed separately for each system, and all the signatures were enabled for each system. For more particulars about the tests, visit: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_white_paper0900aecd80350d4e.pdf.

Conclusion

Firewalls are the basic building block of an organization's network security architecture and, as such, should be deployed at every possible intrusion point throughout the enterprise network. According to industry-leading market researchers, next-generation firewalls will consolidate firewall and IPS filtering and possibly other security functions, in part for capital savings and operational simplicity. In addition, integration can also actually enhance security by correlating security-data events, and can provide the superior performance of single-pass packet inspection.

The Cisco ASA 5500 Series Adaptive Security Appliance can operate as a firewall only, yet is also expandable using chassis modules and integrated software capabilities to perform the entire range of security functions. The appliances scale from the smallest home office to the largest enterprise at price points appropriate to the throughput and number of simultaneous connections required in each network segment.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-381449-00 12/06