Securing Business Applications with Cisco ASA 5500 Series

A new level of application security provided by Cisco ASA 5500 adaptive security appliances.

Network security threats increasingly target the application layer. Network and security administrators are often forced to make difficult compromises between deploying new services to increase business productivity and protecting those services from attack. The new Cisco ASA 5500 Series of adaptive security appliances breaks the cycle of compromise by allowing rapid, robust, and secure deployment of new applications.

Overview

Networked applications form a critical element of the business infrastructure. Traditional security solutions lack the breadth of application coverage, the depth of inspection services, the integral network services, and the level of performance required to defend these applications against attack. The Cisco® ASA 5500 Series enables a new class of uncompromising application security, meeting the challenge of protecting networked applications from both today's and tomorrow's threats.

Challenge

The explosive growth of the Internet has caused a rapid migration of business processes onto the network. Networked applications form the backbone of these business processes. Applications such as Web browsing, e-mail communications, and IP telephony are core elements of the business infrastructure. Messaging and presence applications (instant messaging, for example) are increasingly seen as valuable business tools for communication among employees, as well as with partners and customers. Coupled with the deployment of high-performance networks, networked applications have enabled great gains in business productivity.

APPLICATION SECURITY INSPECTION ENGINES IN THE CISCO ASA 5500 SERIES

- Web browsing (HTTP)
- Electronic mail (SMTP/eSMTP)
- Enterprise IP telephony (SIP, H.323, SCCP)
- Provider voice services (MGCP, GTP)
- File transfers (FTP)
- Tunneled applications (peer-to-peer or instant messaging)
- Domain Name System (DNS)
- And many more!

As organizations increase their reliance on the network, the availability and integrity of these applications becomes critical to doing business. Enforcing the security policies designed to ensure this availability, however, is becoming more difficult, with tools for the misuse or abuse of applications enabling users to circumvent traditional security technologies. Indeed, applications such as peer-to-peer file sharing networks are increasingly integrating such tools directly into the applications themselves. Application behavior such as "port-hopping" and tunneling allows applications to intelligently scan for and find open ports in the firewall, such as for Web browsing (port 80), and to tunnel themselves through those openings-making it virtually impossible for a traditional security device to enforce network segmentation and acceptable-use policies. This

lack of control over application usage can drain employee productivity and network resources, and can expose an organization to regulatory and legal concerns.

In addition, an increasing number of attacks target the application layer. These attacks threaten to disrupt the productivity enhancements enabled by networked applications by targeting the availability and integrity of those applications. From IP telephony to Web-enabled applications, the need for protection against application-layer attacks has never been greater. However, traditional security devices provide little protection for the application layer, and the few protections provided do not address the threats of today and tomorrow.

Finally, traditional solutions have lacked the critical network services and performance profile required for deployment in a modern network. Business-critical traffic, such as IP telephony, must be highly available, and delivered across the network with toll-quality service. It is unacceptable for security services to impact service delivery across the network.

These challenges place security and network administrators in the difficult position of compromising on either application delivery or application security. A new class of solution is needed to break this cycle of compromise and provide security for today's critical business applications.

Solution: Application Security In The Cisco ASA 5500 Series

Today's security threats require a new approach to security. Comprehensive application security requires application awareness across a network's applications, instead of an individual approach to every application on the network. Each application requires a set of common services, as well as application-specific inspection services. These application inspection services must meet the demanding performance and services requirements of today's networks. All of these requirements must be tied together in a clear and comprehensive architecture that allows flexible deployment and enforcement of application security policies. Cisco ASA 5500 Series adaptive security appliances have been designed to enable this new approach to application security, and help protect the availability and integrity of critical business applications.

The Cisco ASA 5500 Series brings a new level of security and policy control to networks via the Modular Policy Framework architecture. With application security inspection engines spanning all major network protocols, the Cisco ASA 5500 Series enables deployment of a comprehensive application security policy. Each inspection engine monitors the application flow, and can flag and block protocol violations as appropriate to the specific protocol. For example, the Web inspection engine allows an administrator to enforce traffic compliance with HTTP RFCs and other standards, helping to ensure that traffic flowing over port 80 is valid Web traffic. This provides two major benefits. First, the inspection engine detects and blocks non-HTTP applications attempting to circumvent security policy by tunneling over port 80 (peer-to-peer programs, such as Kazaa, fall into this category). Second, it protects against both known and unknown attacks targeting the application layer by evaluating protocol semantics and best practices. Malware that targets vulnerabilities in application processing can be thwarted by standards conformance.

In addition to protocol compliance, inspection engines extend the access control toolset of security administrators through a robust set of controls that govern the use of individual features or capabilities within an application. The FTP inspection engine allows the administrator to protect file servers by controlling the specific commands a user is allowed to perform on that file server-allowing users to retrieve files but not delete them or upload potentially malicious content, for example.

For these inspection engines to be deployable in a production network environment, they must meet the demanding performance and network service requirements of today's networks. The Cisco ASA 5500 Series was built to meet the high performance needs of today's networks, providing up to 450 Mbps of concurrent protective services. In addition, the stringent service-level agreements (SLAs) of latency-sensitive voice traffic can be handled with ease through integrated quality of service (QoS) mechanisms, including a dedicated low-latency queue for voice traffic. Finally, the availability of the security infrastructure is protected by advanced high-availability capabilities, including Active/Active failover services, in which network administrators can capitalize on their redundancy investments by allowing both devices in a failover pair to inspect application traffic under normal network operation.

The Modular Policy Framework architecture ties together the multitude of application security inspection engines and network services available in the Cisco ASA 5500 series. Using a modular services processing architecture enables the use of specific security or network services on a per-traffic flow basis, delivering highly granular policy controls and with streamlined traffic processing. The efficiencies of this architecture, as well as software extensibility and hardware extensibility via user-installable security services modules (SSMs), enables the evolution of existing services as well as deployment of new services without requiring a platform replacement or performance compromise. As the architectural foundation of the Cisco ASA 5500 Series, the Modular Policy Framework architecture enables highly customizable security policies and unprecedented services extensibility to help protect against the rapidly evolving threat environment.

Conclusions

Networked applications have enabled great gains in business productivity, and promise further gains still. In order for these gains to be realized, the availability and integrity of applications must be secured. The Cisco ASA 5500 Series introduces a new class of protection, providing comprehensive application security without the compromises of traditional solutions. The Cisco ASA 5500 Series provides comprehensive protocol support, depth of application controls, and tight integration with network services, tied together in the flexible and high-performance Modular Policy Framework architecture. This flexibility helps ensure that the Cisco ASA 5500 Series has the performance to protect today's networks, and the flexibility to protect tomorrow's.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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 C11-453493-00 02/08

