Global Information Assurance Certification Paper

Cisco Perimeter Security and the Cisco Intrusion Detection System

Cisco Systems offers a wide array of network products: routers, switches, and dedicated appliances, most of which come with some form of security software. Currently, Cisco products comprise much of the Internet's backbone. The Cisco Security Solution comprises key components that enable a consistent approach to be administered preventing unauthorized entry and protection of valuable data and network resources from corruption and/or intrusion. The goal of this paper is to provide an overview of Cisco Perimeter Security and the Cisco Intrusion Detection system with an emphasis on the Cisco Secure product line.

Cisco Secure PIX Firewall

Perimeter security provides secure access for critical network applications, data and services that only authenticated and authorized users and information can pass through the network. This level of security is applied at the perimeter of the network, the point of entry where untrustworthy connections often occur. This could be the point between the corporate network and the ISP and/or the telephone company. It can also be a point between two departments within the corporation, such as Finance and Engineering.

Security control is provided at the perimeter by access-limiting devices, commonly classified as firewalls. These devices can be Cisco routers with traffic-limiting access lists and basic firewall features or dedicated firewall solutions such as a PIX Firewall. The strength of the security features within the PIX hinges on the fact that it was designed solely as a firewall. The PIX Firewall will do a limited amount of routing however its true purpose is to deny unrequested outside traffic from your LAN . Since the PIX utilizes the Internet Engineering Task Force IPSec standard for secure private communications over the Internet, it is also a logical choice to terminate IPSec VPN traffic from IPSec-compliant network equipment and to form secure Virtual Private Networks between remote location

Although a router can also provide some of the functions of a PIX by implementing access control lists, it also has to deal with routing packets from one network to another. Depending on what model router is being used, access lists tend to burden the CPU, especially if there are numerous access lists that must be referenced for every packet that travels through the router. This can impact the performance of the router causing other problems such as network convergence time. Useful information on improving security on Cisco routers can be found at http://www.cisco.com/warp/public/707/21.html

A router by nature has a much larger operating system and as such must be carefully configured to stop intrusion, secure the network and prevent denial of service attacks. The PIX however only requires six commands before it can be effective since it was originally designed as a Network Address Translation (NAT) device and not a general-purpose operating system, unlike both Windows 2000 and UNIX. Thus, the PIX has a small operating system that presents fewer opportunities for a security breach. The PIX is also free from many security holes that plague both UNIX and Windows NT since the

operating system is proprietary and its source code is not accessible by the public whatsoever.

Currently, there are four versions of the PIX Firewall with throughput rates ranging from 10 Mbps (PIX 506) for high-end small offices to 1.0Gbps with the ability to handle 500,000 concurrent connections (PIX 535) for enterprise and service provider use. There is also a dedicated PIX Firewall VPN Accelerator Card that can perform hardware acceleration of VPN traffic encryption/decryption providing 100Mbps IPSec throughput using 168-Bit 3DES. Further information on the Cisco Secure PIX Firewall series is available at www.cisco.com/go/pix.

The PIX Firewall, regardless of model number, provides full protection to the corporate network by completely concealing the internal network to the outside world. Since the PIX is designed as a security appliance, it provides a wealth of features to secure a network including

- Packet Filtering Services
- Cut-through proxy
- Stateful Filtering using Adaptive Security Algorithm (ASA)
- Network Address Translation (NAT)
- Port Address Translation (PAT)
- IP Sequence random numbering
- FTP and URL Logging
- DHCP client and server support
- Automatic Telnet Denial
- Secure shell (SSH) support
- Active X Blocking / Java Filtering
- AAA Authorization and Accounting

The Flood Defender feature limits the total number of connections and number of half-open connections UDP response packets that either have not been requested or arrive after a timeout period are also dropped.

IP Frag Guard limits the number of IP full-fragment packets to an internal host that in turn prevents denial of service attacks like LAND and teardrop. The Flood Guard feature is designed to prevent DoS attacks that continuously request the authentication of a user attacks that are designed to use memory resources on a network device. When an excessive amount of authentication requests are received, the PIX starts dropping these requests and reclaiming memory. A wealth of information on Denial of Service attacks can be found at www.cert.org/tech_tips/denial_of_service.html.

There exists several advantages to using the PIX over a router or a Linux, UNIX or Windows NT based firewall. The benefits of using the PIX include

- Throughput speeds up to 100Mbps
- Up to 500,000 connections simultaneously

- PIX's Adaptive Security Algorithm (ASA), combined with cut-through proxy, allows the PIX to virtually eliminate all SYN-based DoS attacks
- IPSec VPN support
- NAT and PAT fully supported
- Low cost of ownership due to no operating system maintenance
- Integrated Intrusion Detection system

The Cisco PIX Firewall is built around a non-UNIX embedded operating system that leads to excellent performance without compromising security. When a proxy server receives an Ethernet packet, it strips off the header, extracts the IP packet, moves that packet up through the OSI model until it reaches the application layer where the proxy server software changes the address. The new IP is then rebuilt and sent down to layer 1 where it is transmitted. This uses a large number of CPU cycles and increases delay. However because PIX is Cisco proprietary, the OSI constraints can be bypassed and made to allow cut-through proxy to operate.

Since the PIX is a security device, limiting access to the PIX to only those who need it is critical. This task should include

- Restricting remote access to the PIX to the management hosts only
- Deactivating all unused services and unused features
- Activating idle session timeouts
- Making sure the PIX Firewall is physically secure
- Activate system logging to an external syslog server

The Cisco PIX Firewall Manager performs network security management providing a clear view of the network security policies that are enforced on the network. PIX Firewall Manager can be used to centralize administration of the PIX firewalls on a network by providing a GUI to manage the security rules on the PIX. The management interface also supports a syslog server that can be used to centralize the logging information generated by all PIX firewalls, up to a maximum of ten. Alarms can then be configured based on the logs generated from the firewall.

Cisco Secure Intrusion Detection Systems

Once a security solution is designed and implemented, it needs to be evaluated. Intrusion detection can be done at the host level or at the network level by listening in on the network and looking for signature attacks in the IP packets traveling on the wire.

Cisco offers different tools to manage and implement intrusion detection. Cisco Secure Scanner is a network-scanning utility that can be used for regular security-monitoring purposes by actively probing the devices on the network to gather information. The user instructs the scanner to scan a network based on supplied IP address details . TCP/UDP port interrogation and SNMP queries are used to gather information that is compiled into a database.

The Cisco Secure Scanner will identify which IP addresses are alive and will also extract the operating system, version number, domain name and IP setting for all hosts including internetworking devices such as routers, switches and remote access servers. Major Internet servers such as Web, FTP and SMTP will also be identified. The detailed information that is obtained from the active devices is compared against a list of well-known security threats and common vulnerabilities. This vulnerability information is collated from the Network Security Database (NSDB) that contains current well-known security vulnerabilities grouped by operating system. Regular updates to the vulnerability scanner are easy to download and install directly from the Cisco website. Cisco employs a team called the Cisco Countermeasure Research Team, or C-CRT, who work to ensure that Secure Scanner is up-to-date. Further information on common vulnerabilities and security exposures is available at http://cve.mitre.org

Once the data has been collated and any vulnerabilities identified the application allows the creation of numerous charts and reports. Three types of HTML reports can be generated from Secure Scanner: executive, brief technical and full technical. Each type of report is aimed at different groups of people with the executive presenting a high-level summary whereas the full technical provides an in-depth review of all security vulnerabilities found on the network.

Cisco Secure Scanner is most effective when run during varying traffic loads. Running the Scanner session when the network traffic levels are low as well as during busy hours when all devices are powered up will afford a more comprehensive set of results. Run unscheduled scans to increase the likelihood of catching devices that may be switched on only occasionally. As soon as new devices are added to the network, a scan should be run. This process should be integrated into a company change management program. Report any anomalies or new vulnerabilities that you may have found to Cisco Systems using the NSDB reporting mechanism. For a thorough guide on usage of Secure Scanner look at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csscan/csscan2/csscug/**.**

Intrusion detection can be defined as detecting, reporting, and terminating unauthorized activity on the network. The Cisco Secure Intrusion Detection System (formerly NetRanger) is the dynamic security component of Cisco's end-to-end security product line that responds to intrusions in real-time by utilizing sensors to capture traffic and monitor syslog traffic from a Cisco router to detect network intrusions.

The Cisco Secure IDS uses a security database for signature analysis that provides information about exploits as well as countermeasures. Updates to the security database are made available through Cisco's website. Custom attack signatures can also be defined. For further details, have a look at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm

The Cisco Secure IDS consists of three major components. The Intrusion Detection Sensor is a network plug-and-play device that interprets IP traffic into meaningful

security events. These events are then passed to the Intrusion detection Director for analysis.

The sensor is a specialized device that uses a rule-based inference engine to process large volumes of traffic in order to identify security issues in real-time. The sensor is either a ready-made appliance that is purchased directly from Cisco or it can be a software-based one installed on an x86 or SPARC Solaris 2.6 station.

After capturing packets, Cisco Secure Intrusion Detection Sensor reassembles the packet and compares the data received against a rule base that contains signatures of common network intrusions. Both packet header and packet data are analyzed against the rule set to catch the varying types of attacks.

If an attack or security event is detected by the sensor, Cisco Secure IDS can respond by generating alarms, logging the event, resetting TCP connections or by dynamically reconfiguring a network device's access control list to block the source of an attack in real-time.

The Cisco Secure Intrusion Detection Director is responsible for the initial configuration, monitoring and remote management of the CSIDS sensors. Additionally, collection of data and its subsequent analysis is performed by the Director using software with a built-in set of SQL-compliant queries that can be run against data collected by the sensors.

The CSIDS Director can be programmed with user-defined actions such as running a UNIX script to lock down specific services.

The CSIDS Post Office is the communication backbone that allows Cisco Secure IDS services and hosts to communicate with each other. This messaging facility between Director and sensors uses a proprietary UDP transport protocol for communication.

Staying up-to-date on Cisco Perimeter Security and Cisco Intrusion Detection can be challenging. A new software version comes out, new bugs are found, the exploit is published and the software vendor sends out a patch. As a network security manager, keeping in touch with the most current information is crucial .The Cisco Product Security Incident response Web page reports useful information on security incidents related to Cisco products and can be visited at www.cisco.com/warp/public/707/sec_incident_response.shtml.

Works Cited

Cisco Systems. "Improving Security on Cisco Routers"
URL: http://www.cisco.com/warp/public/707/21
Cisco Systems. " Cisco Secure PIX 500 Firewalls" URL: www.cisco.com/go/pix.
CERT Coordination Center. " Denial of Service Attacks" URL:
www.cert.org/tech_tips/denial_of_service.html
The MITRE Corporation . "Common Vulnerabilities and Exposures (CVE)" URL:
http://cve.mitre.org
Cisco Systems. "Cisco Secure Scanner User Guide Version 2.0" URL:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csscan/csscan2/csscug/
Cisco Systems. "Cisco Secure Intrusion Detection System" URL:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm
Cisco Systems. "Cisco Product Security Incident Response "
URL: www.cisco.com/warp/public/707/sec_incident_response.shtml.

References Used

Andrew G. Mason and Mark J. Newcomb, *Cisco Secure Internet Security Solutions*, Cisco Press, February 2001
Russell Lusignan, Oliver Steudler and Jacques Allison, *Managing Cisco Network Security*, Syngress Publishing, 2000

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event