Augmenting Perimeter Security Networks With Cisco Self-Defending Networks

Mark Las

68-595

Security Project

Table of Contents

Abstract

Computer data networks are under constant attack and subject to an increasing variety of attacks. These attacks fall into several general categories that identify and separate them based on some key differences and methods. Many organizations have implemented perimeter security as a method for dealing with these threats and attacks. As attacks and threats have escalated and found ways through the perimeter, organizations have further extended the perimeter security approach with the concept of defense in depth, which provides a layered approach to protecting data networks beginning with the perimeter. Perimeter security is dependent on properly configured firewalls and routers. However, traditional packet-filtering firewalls only block network ports and computer addresses and do not address threats that occur at the application layer. Firewalls do not protect against traffic that is passed on open ports or encrypted VPN traffic. Other items not protected by firewalls or perimeter security include traffic that appears legitimate, weak passwords, or attacks once a network has been compromised.

As threats and attacks have continued to escalate and challenge perimeter security, Cisco has created a line of products designed to augment traditional perimeter security devices. To understand the benefit of these products and ensure their viability, it is important to understand the traditional types of attacks, defenses, and methods for augmenting with new Cisco Self-Defending products. The purpose of this paper is to address these topics.

Traditional Network Attacks

Computer networks are subject to an ever-growing number and variety of attacks on a daily basis. These attacks fall into several general categories of attacks. These attacks are listed below:

- Virus
- Worm
- Trojan horse
- Denial-of-service
- Distributed Denial-of-Service
- Spyware
- Phishing

These threats are constantly evolving as the amount of attacks is rapidly rising and in many cases, causing havoc on attacked systems. To understand how traditional network defenses, as well as advances in these defenses, can protect computer networks it is important to have an understanding of these attacks. [1]

Virus

A virus can be defined as "…a program that can 'infect' other programs by modifying them to include a, possibly evolved, copy of itself". [2] A virus is a software program that is considered malicious in nature, even though it may not actually cause any damage. Most viruses intend to cause serious damage and wreak havoc on a computer system. A virus infects other programs, including operating systems, by inserting itself into the chain of command so that attempting to launch a legitimate program results in the execution of the virus as well as (or instead of) the program.

A virus is traditionally composed of or can be dissected into three main sections. These sections are as follows:

Infection	Mechanism defined as the way or ways in which the virus spreads. A virus can be delivered via different methods, which include e-mail, e-mail attachments, physical transfer, Internet download, and macros.
Payload	Mechanism defined as what, if anything, the virus does apart from replication. This component defines what damage or harm the virus will deliver when triggered.
Trigger	Mechanism defined as the routine that decides whether now is the time to deliver the payload . In general, most viruses are

triggered during the execution of the virus program during the infection. However, in some cases, viruses can infect a program but be triggered at a later point in time or as a result of some predetermined action configured in the payload.

A virus that is triggered usually delivers or causes some form of damage. This damage can be one of the following:

- Deliberate damage inflicted by the virus payload mechanism, if it exists, such as the trashing or intentional corruption of files.
- Accidental damage caused when the virus attempts to install itself on the victim system (the newly infected host), such as corruption of system areas preventing the victim system from booting.
- Incidental damage that may not be obvious or severe but is nevertheless inherent in the fact of infection. Nearly all viruses cause damage in this category, since their presence involves loss of performance due to theft of memory, disk space, clock cycles, system modification, or a combination of two or more of these. BAT.Caya is a virus that was discovered on August 12, 2004 that takes up disk space and alters system files. When the virus is triggered, it copies itself to %system%\updateuser.bat, appends its code to batch located in several different locations including the %windir%(location for Windows system files), and will replicate itself on a system using Winzip, a third-party application, if it is installed. [3]

Worm

A worm is a destructive software program that scans for vulnerabilities or security holes on other computers in order to exploit a weakness and replicate itself. Worms are capable of initiating network connections to facilitate their replication to other unprotected hosts. The rapid growth of the Internet, combined with poorly patched and insecure hosts, has provided many potential targets for worms. Worms exhibit the potential for rapid, exponential growth capable of generating enough traffic to cripple data networks. This type of attack is also a form of distributed denial-of-service (DDoS).

It is very common to lump worms in the virus family but there are two main differences that separate worms from viruses:

- Viruses require a host to attach and execute; worms do not require a host.
- Viruses and worms typically cause different types of destruction.
    - Worms tend to be network-centric and can initiate network connections to send large amounts of data

- Viruses tend to be computer-centric and their payload tends to be limited to the infected host

Also, it is very common for worms to contain a data payload, which can relegate a target computer to the status of a zombie. A zombie is a computer that has been compromised and is now under control by the network attacker. In many cases, zombies are used to launch additional network attacks. A large grouping of these zombie computers is referred to as a botnet. It is not uncommon for botnets to be composed of more than 100,000 computers that were initially infected via a worm. In early 2004, a worm called MyDoom was unleashed that ultimately infected approximately 500,000 computers. MyDoom was designed to infect a system and harvest its e-mail address book. It would then establish a network connection and send itself to every e-mail address in the victim's address book. The original attack was launched from approximately 50,000 systems and quickly grew to 500,000. Ultimately, the intent of MyDoom was to launch a denial-of-service attack against SCO Group and Microsoft. [4] Currently, the largest botnet in the world is known as Srizbi. It controls an estimated 315,000 machines and has the capability to send out over 60 billion spam per day. [5]

Trojan Horse

A Trojan horse is detrimental software that masquerades itself as a legitimate application. In many cases, it masquerades itself as a game or screen saver. An unsuspecting user attempts to access the masqueraded software, assuming it is legitimate, and proceeds to execute the Trojan program. The Trojan program, once initiated, can perform activities such as formatting a hard drive or deleting files.

Denial-Of-Service/Distributed Denial-of-Service

Denial-of-service (DoS) is a network attack that results in a service provider, such as an application being requested from a web page, unable to deliver any service to the requester. Target systems such as servers must maintain state information and typically have expected buffer sizes and network packet contents for specific applications. DoS attacks exploit these types of vulnerabilities by sending packet sizes and data values that are not expected by the receiving application. DoS attempts to clog the network pipe so that legitimate traffic is unable to get through via network traffic.

DoS attacks usually take the form of one of the following:

- Consumption of system resources such as bandwidth, processing power, or disk space
- Disruption of device configuration information such as a routing table
- Disruption of connection state information
- Disruption of network components

- Obstructing the communication media between the intended users and the victim so that they no longer communicate adequately

DoS attacks can also execute malware that produce the following negative results:

- Max out the CPU's usage
- Trigger errors in the microcode of the machine
- Trigger errors in the sequencing of instructions
- Exploit errors in the operating system to cause resource starvation and/or thrashing
- Crash the operating system;

For example, CERT issued an advisory on December 18, 1996 which detailed a DoS attack in which an oversized ICMP packet could cause a system to crash, freeze, or reboot. [6]

Distributed Denial-of-Service (DDOS) attacks are very similar in nature to DoS attacks except that a DDoS attack originates from multiple source attack points. The DDoS attack is more complex and more difficult to defend against because it generates a greater amount of bogus network traffic as well as forcing the attacked system to identify and protect itself from several different, if not hundreds or thousands, attack points. The following, Table 1 [7], lists and describes several varieties of DoS/DD0S attacks:

Name of Attack	Flooding Capability	Short Description
Land	TCP SYN	Source and destination IP addresses are the same, causing the TCP response to loop.
SYN	TCP	Sends large numbers of TCP connection initiation requests to the target. The target system must consume resources to keep track of these partially opened connections.
Teardrop	TCP fragments	Sends overlapping IP fragments.
Smurf	Internet Control Message Protocol (ICMP)	Sends ICMP ping requests to a directed broadcast address. The forged source address of the request is the target of the attack. The recipients of the directed broadcast ping request respond to the request and flood the target's network.
Ping of Death	ICMP	Brings down a system by sending out more than 65536 ICMP packets.
Open/Close	TCP, UDP	Opens and closes connections at a high rate to any port serviced by an external service through inetd. The number of connections allowed is hard coded inside inetd (Internet super daemon, often used to run other services like FTP).

ICMP Unreachable	ICMP	The attacker sends ICMP unreachable packets from a spoofed address to a host. This causes all legitimate TCP connections on the host to be torn down to the spoofed address. This causes the TCP session to retry, and as more ICMP unreachable are sent, a denial-of-service (DoS) condition occurs.
ICMP redirect	ICMP	Causes data overload to the system being targeted.
ICMP Router Discovery Protocol (IRDP)	ICMP	Spoofing IRDP causes fake routing entries to be entered into a Windows machine. IRDP has no authentication. Upon startup, a system running MS Windows 95/98 will always send 3 ICMP Router Solicitation packets to the 224.0.0.2 multicast address. If the machine is NOT configured as a DHCP client, it ignores any Router Advertisements sent back to the host. However, if the Windows machine is configured as a DHCP client, any Router Advertisements sent to the machine will be accepted and processed.
ARP redirect	ARP	Attacks local subnet.
Looping User Datagram (UDP) ports	UDP	Spoofs two UDP services - chargen (port 19) and echo (port 7) - to send data to each other.
Fraggle	UDP	Same as Smurf, but uses UDP rather than ICMP to broadcast address for amplification.
UDP flood	UDP	Sends large numbers of UDP packets to the target system, thus tying up network resources.
TCP flood	TCP	Repeatedly establishes and abandons TCP connections, enabling a malicious host to tie up significant resources on a server.
UDP reflectors	UDP	All web servers, Domain Name System (DNS) servers, and routers are reflectors, because they will return SYN ACKs or RSTs in response to SYN or other TCP packets; query replies in response to query requests; or ICMP Time Exceeded or Host Unreachable in response to particular IP packets. By spoofing IP addresses from slaves, a massive DDoS attack can be arranged.

URL attacks	TCP	Attempts to overload an HTTP server with HTTP bombing (continuous requests for the same homepage or large web page) or by requesting the page with REFRESH to bypass any proxy server. Many of these attacks are not zombie attacks but rather human executed - by hundreds simultaneously.
Virtual Private Network (VPN) attacks	TCP	Using specially crafted Generic Routing Encapsulation (GRE) or IP in IP tunnel (IPIP) packets to attack the destination address of a VPN.

Table 1 *Generic DDoS Attacks*

Figure 1 [8] below illustrates the use of zombies in a coordinated DDoS attack against an enterprise web server:

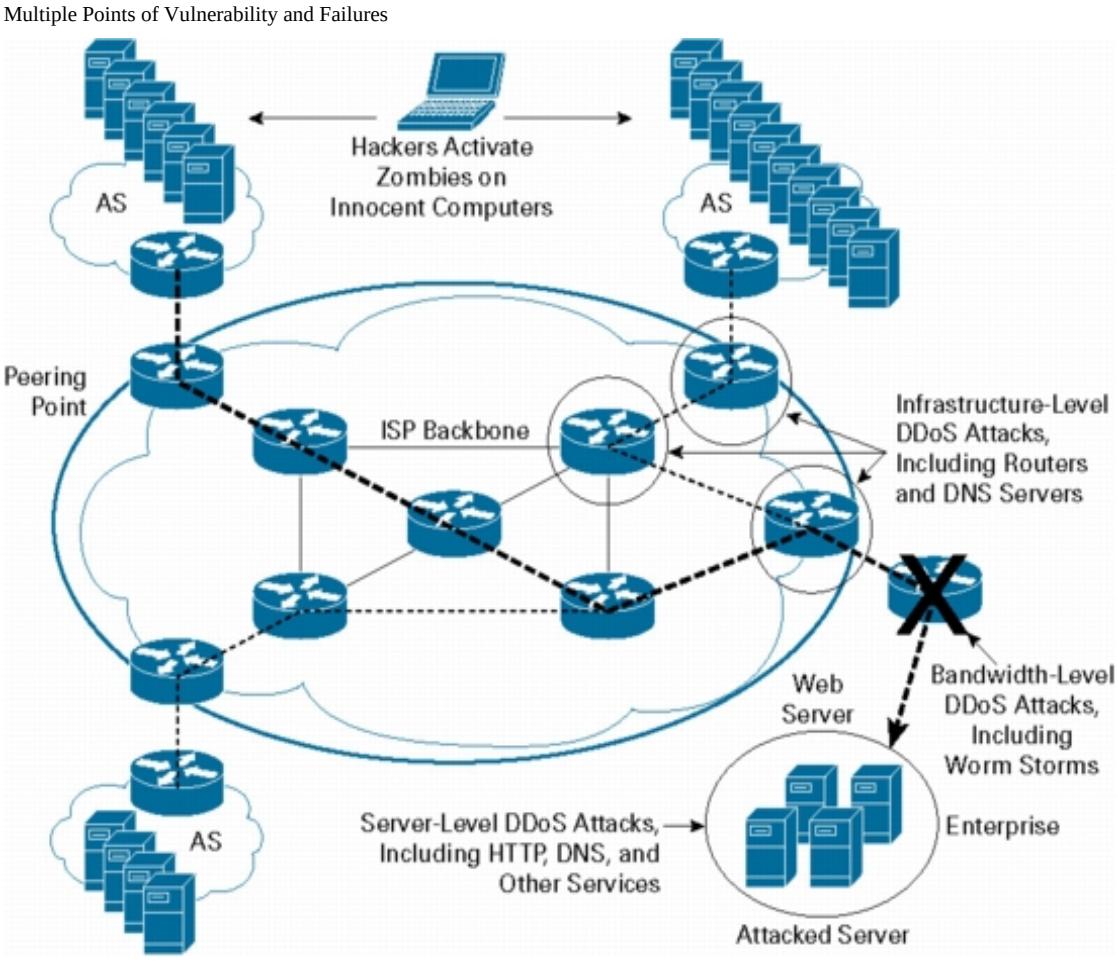


Figure 1. Use of zombies in a coordinated DD0S attack.

Spyware

Spyware is a group of applications that attempt to install themselves without the users express consent, and remain hidden on a targeted system. Spyware that is installed then attempts to run unobtrusively and collect data about a user and his computer activities. Also, spyware commonly tracks a user's web usage, e-mail account, as well as logging passwords. Attackers use the captured passwords and other information to gain entry to a network to launch a network attack. Adware is a form of spyware that installs itself onto a host and displays advertisements via web browser or messenger pop-ups.

Traditionally, spyware is installed onto a system via deception or exploitation of software vulnerabilities on a host. Spyware is commonly installed by program that disguises itself as a useful program, bundled with shareware, downloadable software, or packaged with another product such as a music CD, as well as through the manipulation of security features designed to prevent unwanted installations.

Phishing

Phishing is a network attack that is generated by an e-mail being sent to an unsuspecting user. These types of e-mails attempt to masquerade as a legitimate e-mail from a known and trusted institution such as an online merchant or financial institution. The e-mail attempts to convince the user to click on a link within the e-mail and have them logon to a web site and update their account information. What actually happens is the user is directed to false copy of the merchant or financial institutions web site where they enter legitimate personal and account information into a database a hacker implements to harvest data. This harvested data can be used to commit theft and fraud by impersonating the unsuspecting user.

Traditional Network Defenses/Defense-in-Depth

Computer network security is a core component of any data security strategy. Perimeter security has become the de facto standard for protecting computer networks from external attacks and threats. The following is a list of devices/services that are established components of perimeter security:

- Static packet filter
- Stateful firewall
- Proxy firewall
- IDS and IPS
- VPN Device

A further refinement to this approach is the concept of defense in depth. The US Military Dictionary defines defense in depth as the sitting of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver the reserve. This is a very strong and successful concept employed by the military adaptable to computer defenses. The purpose of Defense in Depth is to take the traditional network defense most organizations have in place and augment them with the following methods and products to strengthen network defense. This concept presumes that any defense can be breached so it calls for another layer of protection followed by another and another, to provide multiple levels of protection in case an outer layer is breached. Also, many organizations fail to protect themselves on the internal network or from internal hosts. It is presumed that an organization can trust its own systems and employees. Defense in depth attempts to strengthen the internal network to provide a more complete defense from attack. The layers of an onion are a common analogy used to describe the layering effect of this concept. Defense in depth is composed of the perimeter, as detailed above, the internal network, and the human factor. The human factor deals with policies and procedures detailing how information resource usage by people is managed and overseen. The internal network is composed of the following devices/services:

- Ingress and egress filtering on every router
- Internal firewalls to segregate resources
- IDS sensors to function as “canaries in a coal mine” and monitor the internal network
- Host-centric (personal) firewalls
- Antivirus software
- Operating system hardening
- Configuration management
- Audits

The above listed components help protect systems from internal attacks as well as those that breach perimeter security.

Static Packet Filtering

Static packet filtering is traditionally implemented on a router in the form of router access lists. The access list, or access control list (ACL) permits or denies network traffic based on predefined parameters including source IP address, destination IP address, as well as network service or port number. Every packet contains some key information and the router is aware of other information that is not contained in the packet. The main information [9] is:

- IP source address
- IP destination address
- Protocol (whether the packet is a TCP, UDP, or ICMP packet)
- TCP or UDP source port
- TCP or UDP destination port
- ICMP message type

In addition, the router knows things about the packet that aren't reflected in the packet headers, such as:

- The interface the packet arrives on
- The interface the packet will go out on

These lists are considered stateless because they do not maintain TCP connection state for each connection to the router. Rather, they analyze each packet as it comes across the network and permit or deny based on the configured rules in the ACL. Routers are considered edge or perimeter devices and serve as a base defense. Access control lists are also used to protect the network device itself. Packet filter traditionally operate at the network level (Level 3 of the OSI model) and only examine the header of each individual packet. The main advantage of a static packet filter is its ability to filter specific ports or protocols. However, static packet filters are susceptible to spoofing if source routing is enabled. A hacker can craft a packet to make it look like it originated on the network. [10] When a compromised system responds to this specially crafted packet, it will actually be responding to the spoofed address. Source routing is a method that allows a packet to carry information that tells a router its best path for return communications.

Stateful Firewall

A stateful firewall is a type of firewall that monitors the state of network connections traveling across it. Stateful firewalls examine a packet header. Every packet has a set of headers containing certain information. If it passes a static packet filter rule, it is passed and an entry to a state table is made. Any related packets that come to the firewall are matched against the state table and passed through the firewall. The most intense processing is performed on the initial packet at the time state is determined and recorded. Future packets for an established connection pass through the firewall leading to much faster, secure communications.

Proxy Firewall

A proxy firewall is a firewall that acts as a go-between for every network conversation. Instead of a host connecting directly with a destination via a network connection, the host establishes a connection to a proxy. The proxy establishes a network connection on behalf of the host. This provides a significant security benefit because it prevents any direct connections between systems on either side of the firewall,

Intrusion Detection System/Intrusion Prevention System

Intrusion Detection Systems (IDS) are passive devices that monitor a copy of network traffic as it flows through the network. The IDS attempts to detect a network attack based upon network traffic signatures or patterns of data in the network traffic. One of the main drawbacks of an IDS is that detects network attacks but does not prevent the attacks. It is considered an offline scanner because it works on a copy of the network traffic. Even though an IDS does not prevent an attack, it provides an early warning that a network attack has been initiated.

Intrusion Prevention Systems (IPS) operates exactly like an IDS but have the advantage of being an inline monitor, scanning live network traffic, and having the capability to detect and respond to attacks as they happen. IPS is divided into two main types: host intrusion prevention system (HIPS) and network intrusion prevention system (NIPS). HIPS are installed on an individual host and monitor the behavior of the host. If an attack attempts to alter or modify any files on the host, the HIPS system responds by blocking the change or requesting a course of action from the system administrator. A NIPS monitors network traffic and responds to events based on a configured security policy.

Virtual Private Network

Virtual Private Networks (VPNs) are a security layer applied to a public or private network in an effort to make the network connection secure. VPNs are extremely commonplace in the corporate world and are the de facto standard for remote access and connections between offices. VPNs use authentication mechanisms including one-time passwords and encryption such as 3DES or Advanced Encryption Standard (AES) to provide a secure layer on top of a network connection. VPNs can be found in the form of a hardware device, a component of a hardware device, such as a card, or as a software product, such as Microsoft VPN software-based technology that can be installed and managed via a server.

Benefits

- Cost Effective – A VPN can supply many levels of security to a shared network medium including improved confidentiality, integrity, and authentication. Organizations can limit the amount of dedicated circuits in use to establish a secure network by using VPN technology over existing Internet connections.
- Security – Provides encryption and authentication of varying levels that can be configured based on an organization's needs.
- Deployment – VPN technology leverages existing network hardware providing for quicker deployment.

Disadvantages

- Processing Overhead – Every packet of traffic over the VPN must be encrypted. Encryption involves complex mathematical computations that slow down the transmission of packets and slows performance of the gateway device and reduces the overall bandwidth of the VPN connection.
- Packet Overhead – All packets are encapsulated in another packet, called wrapping, which adds a new packet header containing VPN information. While the packet header is not exceptional in size, it does increase the packet size and can slow network performance.
- Implementation Issues – VPN technology is complex and may exhibit incompatibility with Network Address Translation, VPN pass-through usage, and maximum transmission unit size and design.
- Troubleshooting and Control Issues – Because packets are encrypted, it becomes more difficult to troubleshoot VPN communications until packets are decrypted. Common tools used to examine packet flow such as a network intrusion detection system are less effective because they cannot analyze an encrypted packet until after it has passed through the perimeter VPN device.

Ingress and Egress Filtering

Ingress and egress filtering is a strategy that is employed within the Defense in Depth model for advanced filtering of incoming and outgoing traffic at the border. In perimeter networks, there is always a border device, usually a router or firewall, which serves as the initial point of entry and last point of exit for network traffic. Traditionally, networks perform filtering on incoming network traffic but rarely filter outgoing traffic. Improperly destined traffic might be an internal address that hit your external interface or vice versa, and they can be addressed with ingress and egress filtering. Traffic coming in at the border with an internal address would be considered an attack and could be stopped by using ingress filtering. This type of filtering takes advantages of packet filter technology by expressly allowing or denying traffic based on its destination, port, and service type. Access lists are configured for incoming traffic that will deny all SMTP traffic on port 25 destined to any internal IP other than the organizations mail relay server. This is usually configured with two rules. One rule denies all SMTP traffic, and the other rule allows traffic only to the mail relay server. Also, an organization can implement the same concept on egress filtering. For example, a host on the internal network can become compromised by a virus and begin to send spam to external targets using SMTP over port 25. An egress filter or access list can deny all outbound traffic using SMTP over port 25 except for the mail relay which is authorized to send mail. The end result is that ingress and egress lists provide more control over what comes into a network and what goes out.

Internal Firewalls to Segregate Resources

Firewalls are traditionally used as border devices but can also be used to segment an internal network to provide increased levels of protection in case a host becomes compromised. Segmentation can occur across department of functional group lines. Internal networks can be physically carved up by IP address so each logical group would have a unique range of IP addresses or subnet. Then, with the implementation of internal firewalls, traffic can be configured across logical/physical groups. For example, if a host on a segment reserved for the customer service department becomes compromised, a hacker would not be able to access the accounting group's segment in an effort to access their payroll server, as illustrated in figure 2 below. Each firewall would be configured with strict rules governing internal network traffic. Customer service would not necessarily have a need to directly access the payroll application server, so a rule would be implemented on the firewall access list for the accounting group to block any attempt to access the server from subnet 192.168.2.0 or specifically from host 192.168.2.1.

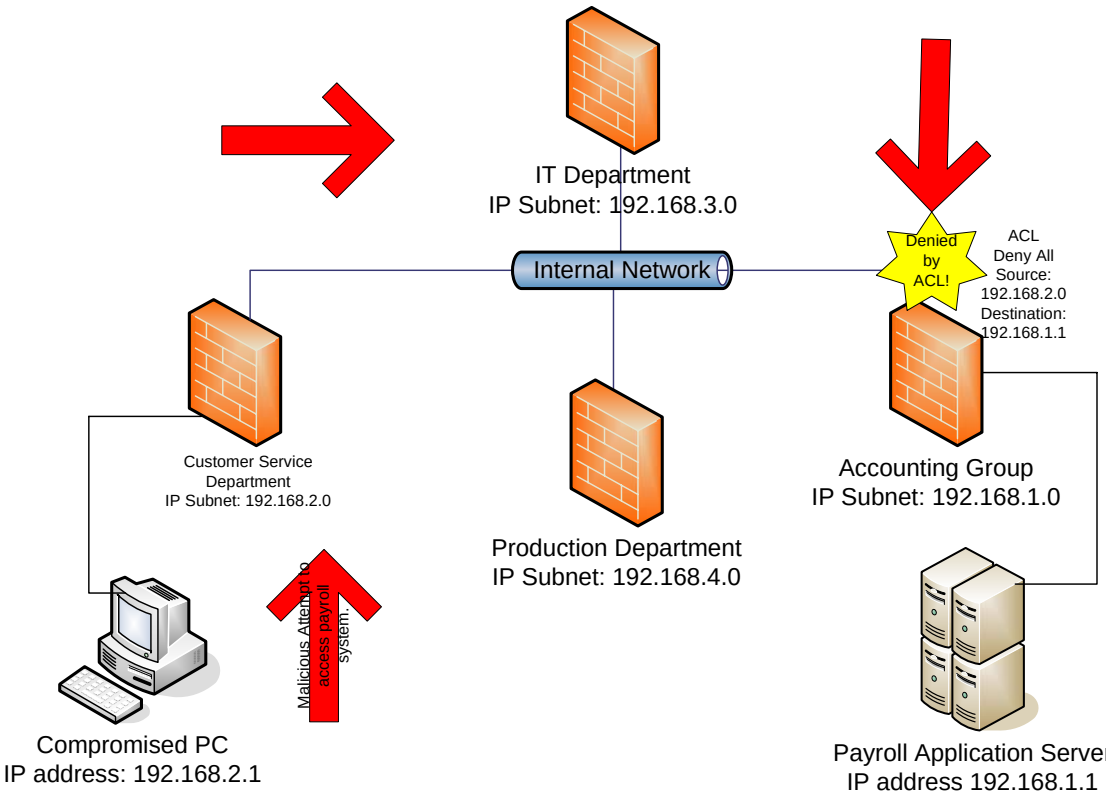


Figure 2. Using firewalls to segment a network.

IDS Sensors

Intrusion detection systems are mainly used to analyze a copy of network traffic originating from an external source as it enters the internal network. Defense in depth takes this a step further by incorporating IDS sensors on the internal network. IDS is already in place within the organization, so extending it, or tuning the sensors to also track internal network traffic, is not much more difficult. By placing sensors on the internal network, the organization may receive an early warning benefit if a host is compromised. In many cases, organizations trust their internal hosts and users, making it difficult to track and identify an internal host that is compromised. An IDS sensor can identify traffic originating on the internal network that is potentially malicious and also identify the host, helping prevent a potential security problem.

Host-centric (personal) Firewalls

Personal firewalls are a core feature of defense in depth and help augment perimeter security. Personal firewalls are implemented as software programs on host computers that monitor all traffic as it enters and leaves the system. Personal firewalls work much like network firewalls and perform packet filtering at the host level. Personal firewalls can be configured to grant or deny access to services, web sites, and

applications as well as control incoming connections. Examples of personal firewalls include Microsoft Windows Firewall and Zone Labs ZoneAlarm.

Antivirus Software

Antivirus software is a core component of any security solution, especially when implementing defense in depth. Antivirus software analyzes data on a host as well in memory in an effort to detect and safely remove any virus-infected files or programs that are running. Antivirus software also prevents malicious code from being downloaded or executing on a host system.

Operating System Hardening

Operating system hardening is also known as host hardening and is an important part of defense in depth. Host hardening is the process of tightening the configuration of the host's OS and applications with the purpose of securing any unnecessary openings on the system. Host hardening is done by regularly downloading and applying patches for an operating system, device drivers, and applications. Host hardening also requires the setting of strict file system permissions, disabling unnecessary services, and enforcing password restrictions. Host hardening is the last layer of protection after every other layer has been breached so its role is critical to the security of a host. A personal firewall may be viewed as a component of system hardening but it is important to recognize that a personal firewall is focused on filtering traffic coming and going from a host whereas host hardening is an approach to enforcing security through proactively maintaining the host and related components such as software drivers that may have inherent bugs or flaws that need to be patched. This approach also attempts to minimize the role of the host in an effort to reduce the potential for attack.

Configuration Management

Configuration management is the process of establishing and maintaining a known configuration for systems and devices that are on a network. Configuration management attempts to remove any uniqueness from an environment, with the hopes of limiting any damage from a security breach. Configuration management establishes a baseline for all hosts within an organization that documents all applications, services, and service packs, etc. that are allowed to be installed and can run on a host. Implementation can vary from large scale automation using a product like Norton Ghost, which can image a large number of hosts in a short amount of time, to manual implementation and management. Ultimately, one of the key features of configuration management is the prevention of unwanted applications from being installed.

Audits

Audits are a core feature of defense in depth because they allow an organization to analyze its network and ensure its security systems are, in fact, working. Audits can be conducted by external consultants or internal employees. Typically, several meetings are held to determine expectations and establish costs, risks, levels of cooperation, deliverables, time frames, as well as authorization. An initial audit report is created, and the staff is usually given an opportunity to respond to this report or address any concerns raised. Once addressed, a final report is completed and given to senior management for review. Follow-up is expected to occur on a regular basis to ensure that security systems continue to function.

Human Factor

The human factor of defense in depth involves the non-technical aspects of network security. The non-technical revolves around policies and awareness of security within an organization. A security policy documents an organizations approach to security and drives the design and implementation of technical products to achieve and sustain that approach. A good policy is composed of the following items [11]:

- Authority – Who is responsible
- Scope – Who it affects
- Expiration – When it ends
- Specificity – What is required
- Clarity – Can everyone understand it

Awareness is a key component of defense-in-depth because a user base with a heightened sense of security can reduce risk and help support defense-in-depth by following the security policy. Users can be made to sign an acceptable use policy which details the organizations security policy and practices. A user base with a sense of security is also less susceptible to social-engineering attacks.

Cisco Self-Defending Networks

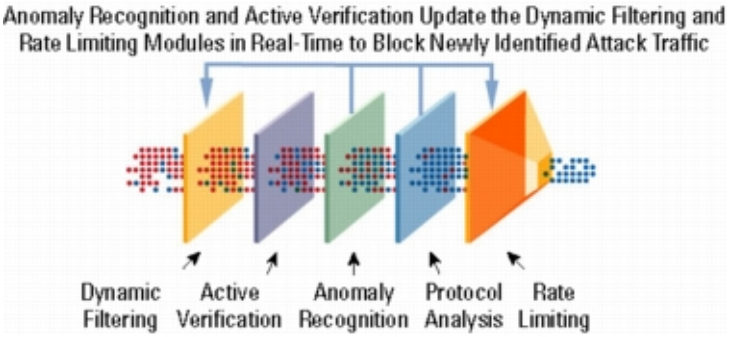
Cisco has created a suite of products, consisting of both hardware and software, which claim to augment and support traditional network defenses designed and implemented with the defense in depth concept. Cisco's new suite falls into a new concept known as self-defending networks. According to Cisco, self-defending networks are different from traditional defenses because they provide some level of automatic protection. Traditional defenses tend to be manually configured and maintained, leaving them susceptible to a host of threats and problems. Cisco's intent is to deliver a set of adaptive products to protect complex corporate networks from the attacks used to exploit them. The key abilities of these adaptive solutions are that they:

- Remain active at all times
- Perform unobtrusively
- Minimize propagation of attacks
- Quickly respond to as-yet unknown attacks

These adaptive solutions include DDoS mitigation, Adaptive Security Appliances, Incident Control Services, Network Admission Control, 802.1x, Host Intrusion Prevention, as well as Cisco Security Centralized Management. The following sections provide an overview of each of these products.

DDoS Mitigation

Cisco distributed denial-of-service (DDoS) mitigation solution is composed of two key components: Cisco Traffic Anomaly Detector and Cisco Guard. Both technologies are based on the patented Multi-Verification Process (MVP) architecture. This MVP architecture, illustrated in Figure 3 [12] below with an explanation of each component of MVP, allows both products to leverage the latest analysis and attack recognition techniques to detect and remove network attack traffic while scrubbing and reinjecting valid network traffic to its proper destination.



· Active verification-This module verifies that packets entering the system have not been spoofed. The Cisco Guard XT uses numerous unique, patent-pending source-authentication mechanisms to stop spoofed packets

from reaching the victim. The active verification module also has several mechanisms to help ensure proper identification of legitimate traffic, virtually eliminating the risk of valid packets being discarded.

· Anomaly recognition-This module monitors all traffic that was not stopped by the filter or the active verification modules and compares it to baseline behavior recorded over time, looking for deviations that would identify the source of malicious packets. The basic principle behind the operation of this module is that the pattern of traffic originating from a "black-hat" daemon residing at a source differs dramatically from the pattern generated by legitimate sources during normal operation. This principle is used to identify the attack source and type, as well as to provide guidelines for blocking traffic or performing more detailed analysis of the suspected data.

· Protocol analysis-This module processes flows that anomaly recognition finds suspicious in order to identify application-specific attacks, such as HTTP error attacks. Protocol analysis then detects any misbehaving protocol transactions, including incomplete transactions or errors.

· Rate limiting-This module provides another enforcement option and prevents misbehaving flows from overwhelming the target while more detailed monitoring is taking place. The module performs per-flow traffic shaping, penalizing sources that consume too many resources (for example, bandwidth or connections) for too long a period.

Figure 3. Cisco Systems MVP Architecture

Traffic Anomaly Detector analyzes network traffic during what would be considered a normal traffic pattern. Based on this normal traffic pattern, a network traffic baseline is established. This baseline is reviewed, and appropriate mitigation policies are then created and applied to this product. It begins to monitor live network traffic, and if a policy is violated or threshold crossed, it diverts all network traffic to the Cisco Guard.

The Cisco Guard maintains an updated routing table in the event that an attack occurs. It takes the suspect data, analyzes the traffic to determine what is legitimate traffic and what is considered actual attack traffic, and scrubs the DoS/DDoS traffic and routes the valid traffic back to the destination zone. This process is illustrated in Figure 4 [13] below.

Cisco Protection in an Enterprise Environment. Only Traffic Destined for the Targeted Device Is Diverted to the Cisco Guard XT, Which Returns "Clean" Transactions Back to the System.

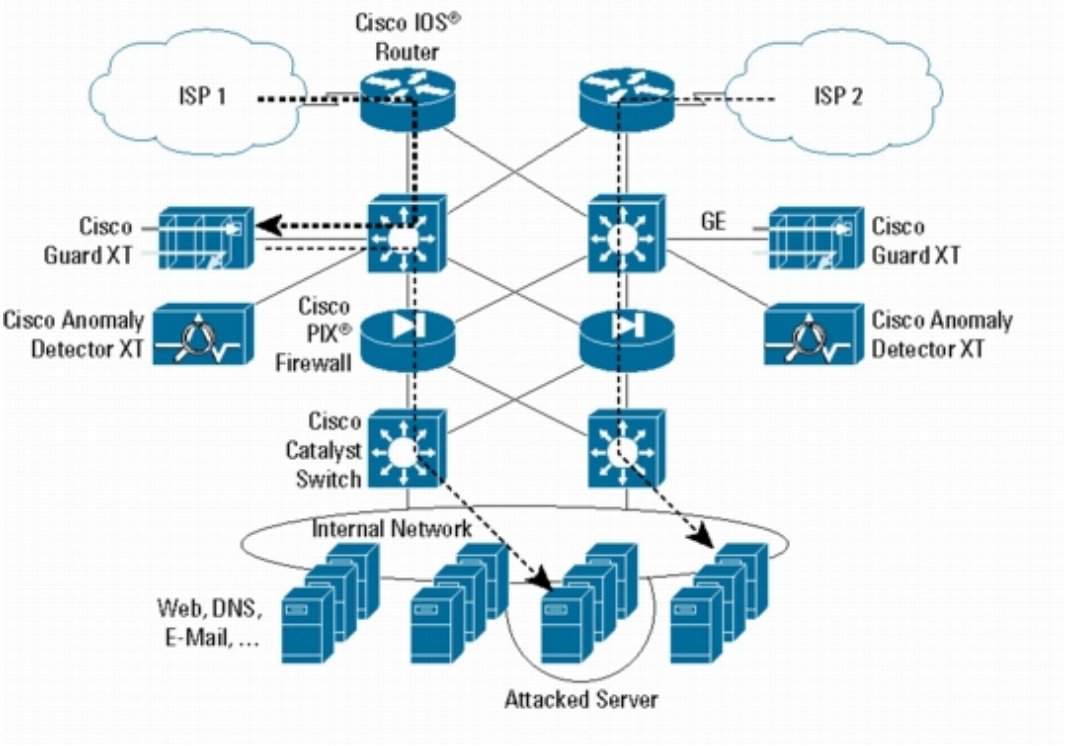


Figure 4. Cisco Guard processing DoS/DDoS traffic.

Adaptive Security Appliances (ASA)

Adaptive Security Appliances (ASA) is a product designed by Cisco that combines multiple functions into a single appliance. It is an adaptive appliance that can have various features activated to establish and maintain the best fit for an organization's security needs. The ASA appliance combines the functions of a firewall, Virtual Private Network, and an intrusion protection system into one appliance. The ASA appliance is also extensible and can be used to add self-defending capabilities that include antivirus, antiphishing, antispam, and antispyware. Many of the above listed features replicated traditional network defense components that are enhanced by the following features:

- Antispoofing
- Intrusion Prevention Service
- Protocol Inspection Services
- HTTP Inspection Engine
- TCP Map/HTTP Map
- Content and Control Security

The following sections detail these self-defending components of the ASA appliance.

Antispoofing

Antispoofing protects a network by verifying that the source of network traffic is valid. This feature creates filters that verify the source address as well as the integrity of the router. A command line interface function, ip verify reverse-path, performs a route lookup on the source address of the packet and drops the packet if a valid return route does not exist. Legitimate traffic will always have a valid return route.

Intrusion Prevention Services

The intrusion prevention service on an ASA device takes the form of an inline Prevention Security Service on the Advanced Inspection and Protection Security Services Module (AIP-SSM). This module is capable of identifying and dropping the IP packets of an active network attack. Being inline means that the module inspects live traffic versus a copy of network traffic like a traditional IDS, however, because it is analyzing live traffic, there is a slight performance penalty as the ASA, which is routing the packet already, performs some analysis. The IPS takes the form of a software module that is uploaded to the ASA device.

Protocol Inspection Services

Incoming network packets can be generated by many different protocols, and the ASA appliance has the capability to analyze packet contents to determine the protocol in use. The ASA can identify and defend itself from potential attack by looking for certain protocols that might try to take advantage of a vulnerability in a network protocol.

HTTP Inspection Engine

The ASA analyzes all network traffic coming in on TCP port 80 which is the HTTP port. The ASA is capable of mitigating potential network attacks that seek to exploit HTTP protocol vulnerabilities.

TCP Map/HTTP Map

The TCP and HTTP Map components allow an organization to tailor how TCP connections can be policed and normalized. The TCP normalization feature lets you specify criteria that identify abnormal packets, which the security appliance drops when they are detected. TCP/HTTP map scans TCP packets and based on the results of normalization, identifies fields in the packet that may not be normal or standard. Packets that are determined to not be normal or standard can be allowed, reset, or dropped.

Content and Control Security

A partnership between Cisco and Trend Micro has led to the development of the Content Security and Control Security Service Module (CSC-SSM) which is an optional component that can be installed on an ASA. It incorporates the following functions:

- Antivirus
- Antiphising
- Antispam
- Antispyware
- URL filtering/blocking
- Content filtering
- File Blocking

These functions are core features of a defense-in-depth approach and attempt to mitigate many of the traditional attacks described above.

Incident Control Services (ICS)

Traditionally, antivirus, antispam, and antispyware are critical components of a defensive strategy but tend to be behind the attacker, not able to defend until a signature can be determined and delivered for a new attack. In an effort to increase the speed with which signatures can be updated, Cisco has partnered with Trend Micro to create Incident Control Services (ICS). ICS is a centrally managed product that manages an automated IPS signature update service provided by Trend Micro. ICS is capable of deploying a broad access control list that can stop the spread of a newly identified infection through the network. These broad ACLs are known as Outbreak Prevention Access Control Lists (OPACLS). After detection of a new network incident, Trend Micro analyzes it and a specific signature designed to mitigate the threat is devised. ICS than takes this signature and deploys it IOS routers with IPS protection. These special signatures are known as Outbreak Prevention Signatures (OPSigs).

Typical list of events that transpire to control the network incident includes the following items [14]:

1. Trend Micro's TrendLabs identifies a new network threat or attack.
2. Trend Micro's TrendLabs create an outbreak management task file. This outbreak management task file contains a broad OPACL that will prevent the outbreak from spreading throughout the network.
3. Cisco ICS cab automatically download this outbreak management task file for the new network threat.
4. The OPACL in the task file can be either automatically deployed or manually deployed after human intervention. There is also an exception list that will prevent Cisco ICS from applying an ACL for a specific port for common network traffic, such as an HTTP (TCP Port 80).
5. TrendLabs releases an OPSig to enable IPS devices to detect the new network threat. Typically the OPSig is released within a few hours of the release of the outbreak management task file with the OPACL.
6. Cisco ICS downloads the OPSig, either automatically or manually.
7. The original OPACL expires after the download of the OPSig.
8. Cisco ICS uses IPS events to determine if a host is sending network traffic that is considered to be a network threat and could possibly be infected. If a host is infected, the infected host is added to the watch list in Cisco ICS.

Network Admission Control (NAC)

Network Admission Control is based on the concept of Network Access Control; the terms are synonymous. NAC attempts to control access to a network with policies that limit the affect of worms and viruses. While perimeter security and defense in depth go to great lengths to protect a network, worms and viruses continue to infiltrate networks. Noncompliant users are frequently to blame for various reasons including the following [cite]:

- A user might choose to wait and install a new update later because they don't have the time
- A contractor, partner, or guest needs network access; however, the business may not control the endpoint
- The endpoints are not managed
- The business lacks the capability to monitor the endpoints and determine whether they are updated to conform to the business's security policy

Cisco provides two solutions for network admission control: NAC Appliance and NAC Framework. The NAC Framework allows organizations to leverage their existing Cisco network products as well as any third-party vendor products such as anti-virus, security, and identity-based software. The NAC appliance is a dedicated appliance solution that is also marketed as Cisco Clean Access (CCA) and provides a dedicated server and management appliance that is not dependent on any existing network components. Figure 5 [15] illustrates the typical customer profile for each solution:

NAC Framework	NAC Appliance
Uses an integrated framework approach, leveraging existing security solutions from other vendors	Prefers bundled, out-of-the-box functionality with preinstalled support for antivirus and Microsoft updates
Complex network environment, leveraging many types of Cisco network access products	Heterogeneous network infrastructure
Longer, phased-in deployment model	Rapid deployment model
Can integrate with 802.1x	Independent of 802.1x

Figure 5. NAC Customer profile.

NAC Framework offers many benefits [16] including the following:

- Protect corporate assets – Enforces the corporate security software compliance policy for endpoints.
- Provides comprehensive span of control – All the access methods that endpoints use to connect to the network are covered, including campus switching, wireless, router WAN links, IP security (IPSEC), and remote access.
- Controls endpoint admission – Validates all endpoints regardless of their operating system, and it doesn't matter which agents are running. Also provides the ability to exempt certain endpoints from having to be authenticated or checked.
- Offers a multivendor solution – NAC is the result of a multivendor collaboration between leading security vendors, including antivirus, desktop management, and other market leaders. NAC supports multiple security and patch software vendors through APIs.
- Leverages existing technologies and standards – NAC extends the use of existing communications protocols and security technologies, such as Extensible Authentication Protocol (EAP), 802.1x, and RADIUS services.
- Leverages existing network and antivirus investments – NAC combines existing investments in network infrastructure and security technology to provide a secure admission control solution.

The NAC Framework is composed of several components that work in concert to provide the benefits listed above. The key components include an endpoint security application, posture agent, network access devices, Cisco Policy server, optional servers that operate as policy server decision points and audit servers, as well as optional management and reporting tools. These components are deployed across an entire organization and protect all access points including WAN, LAN, IPSEC, remote access links, as well as wired and wireless connections. Figure 6 [17] illustrates the location of each of these components and their role in providing NAC:

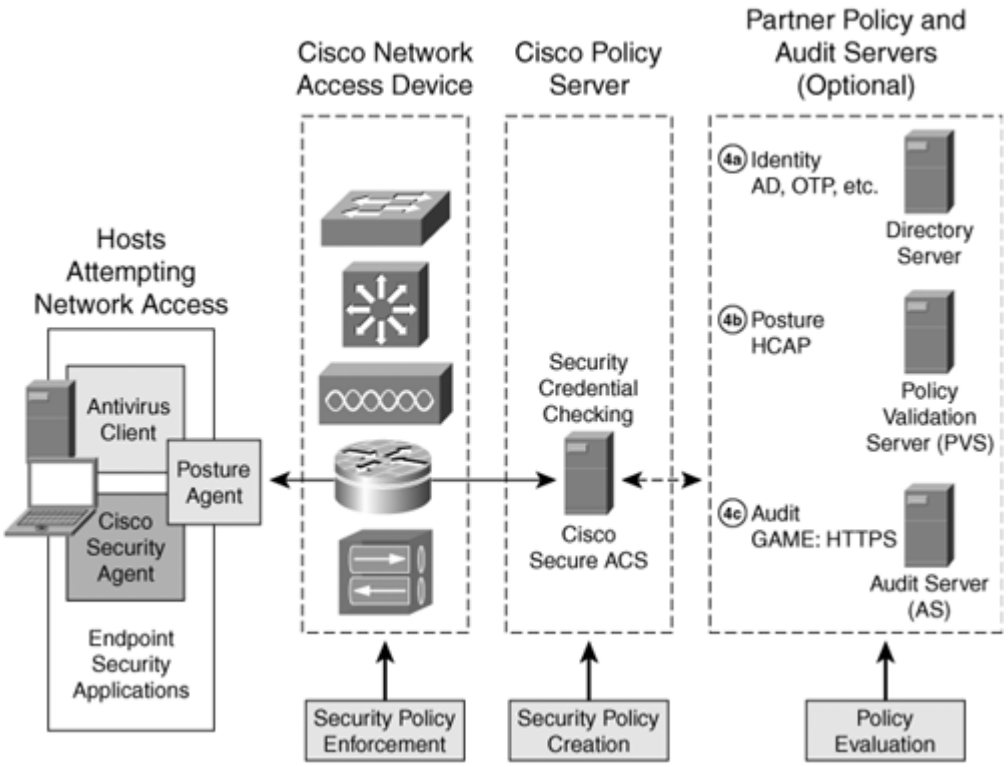


Figure 6. NAC Architecture

The endpoint security application is software that resides on a host and provides many functions that include antivirus scanning, a personal firewall, and HIPS. All these functions are managed by a posture agent which is a piece of middleware that resides on the host and maintains security state information from all the NAC-enabled security applications on the host. The posture agent is called the Cisco Trust Agent (CTA). The CTA maintains the security state information and communicates it to a Cisco Secure Access Control Server (ACS) which maintains and enforces the security policies installed with the NAC Framework.

Network access devices are components such as routers, switches, wireless access points and firewalls that help enforce admission control policy. Each of these devices request security credentials and relay this information to policy servers where network access decisions are made. These decisions include permit, deny, quarantine, or restrict. These are devices are frequently referred to as security policy enforcement points (PEP).

The Cisco Policy server receives endpoint security information and evaluates this information to make an access determination. The Cisco Secure ACS is an authentication, authorization, and accounting device that provides an area for the creation of the admission security policy as well as a location to determine the

endpoint device's compliance condition or posture. The Cisco Secure ACS device can also work with other policy and audits servers to provide additional admission validations [18]:

- Identity – User authentication can be validated with an external directory server and the result is communicated to Cisco Secure ACS. Examples include Microsoft Active Directory and one-time password (OTP) servers.
- Posture – Third-party, vendor-specific credentials such as antivirus and spyware can be forwarded using the Host Credential Authorization Protocol (HCAP) to NAC-enabled Policy Validation Servers (PVS) for further evaluation. This enables businesses to leverage existing policies maintained in their PVS to validate and forward the software compliance result to Cisco Secure ACS, ensuring that a consistent policy is applied across the entire organization.
- Audit – Determines the posture for a NAC Agentless Host (NAH), which is a host without the presence of a posture agent such as Cisco Trust Agent. The Audit server works out of band performs several functions:
    - Collects posture information from an endpoint.
    - Acts as a posture validation server to determine compliance of an endpoint and determine the appropriate compliance result in the form of a posture.
    - Communicate the result to Cisco Secure ACS using Generic Authorization Message Exchange (GAME) over an HTTPS session. GAME uses an extension of Security Assertion Markup Language (SAML), a vendor-neutral language enabling Web services to exchange authentication and authorization information.

The following list is a summary of the admission process for a noncompliant endpoint shown in Figure 7 [19]:

1. An endpoint attempts to access the network.
2. The NAC notifies the policy server (Cisco Secure ACS) that an endpoint is requesting network access.
3. Cisco Secure ACS checks the NAC policy to determine whether the endpoint is compliant.
4. Cisco Secure ACS forwards specific information to other partner policy servers.
    a. Identity information is sent to a directory server for authentication validation.
    b. Host credentials are sent to an antivirus policy server for posture determination.
5. Cisco Secure Access uses information from the all-policy servers and decides the endpoints authorization. In this example, the endpoint is not compliant and is assigned a quarantine posture.
6. Quarantine enforcement actions are sent from Cisco Secure ACS to the NAC servicing the endpoint.
7. NAC enforces admission actions and communicates posture to Posture Agent.
8. Posture Agent notifies the user that the endpoint is quarantined.

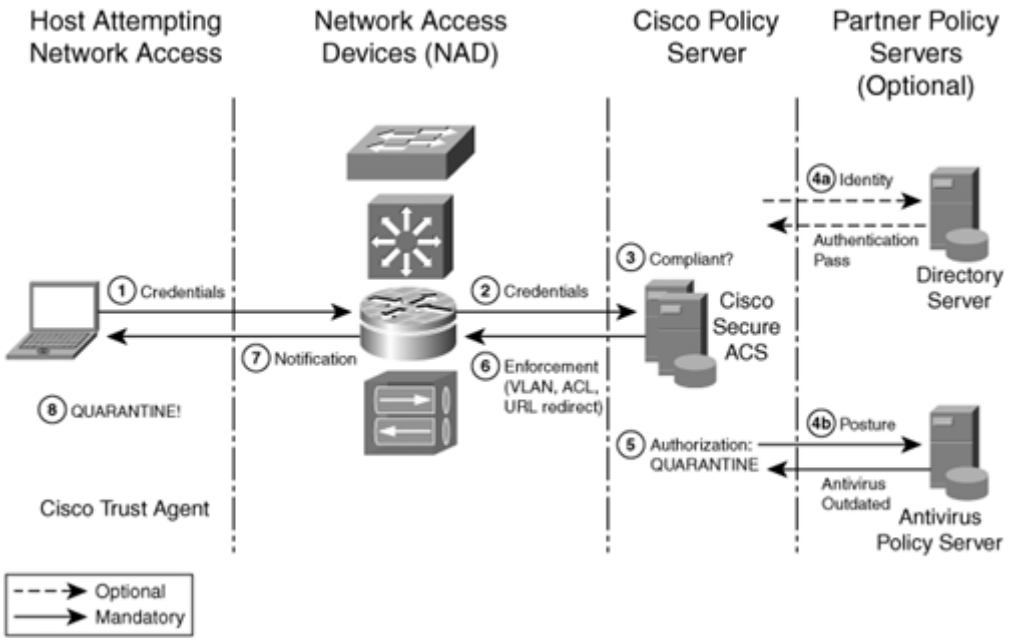


Figure 7. Admission process for noncompliant endpoint

The Cisco NAC appliance is a NAC deployment option that provides admission control functions including authentication, posture validation, and remediation. The appliance is composed of a server, a manager component, and an optional client agent that runs on Windows hosts. The NAC appliance does not use existing routers or switches on the network and does not require 802.1x as a port-based user authentication mechanism. In general, the NAC appliance does everything the Framework can do with the main differences being in the architecture of each solution.

802.1x

802.1x is a public standard that defines port-based user authentication. It is a standard that applies to wired and wireless network infrastructures and involves the use of several different Extensible Authorization Protocol (EAP) types. EAP types define how authentication is implemented on a network. Traditional port security involves specifying what MAC addresses are allowed access to a network. 802.1x is comprised of three major components [20]:

- Authentication Server – The authentication server is an 802.1x server and often contains other user authentication services like Remote Authentication Dial-in User Service (RADIUS). The authentication server often provides user authentication services for both 802.1x and other access methods like remote access IPSec VPNs. Cisco Secure Access Control Server (ACS) is an example of an authentication server.
- Authenticator – The authentication client, or authenticator, is the network component that receives the initial request for port-based user authentication. The authenticator is typically a switch or wireless access-point.
- Supplicant – The supplicant resides on the end-device, like a laptop, desktop computer, or PDA. Some end-device platforms, including the pervasive Microsoft XP, contain a native 802.1x supplicant. Full-featured 802.1x supplicants can also be purchased from third parties for Windows and other platforms, including Linux and MacOS.

The following diagram [21] shows the relationship between the three components of 802.1x and their role in the authentication process. The supplicant is the end user in this process and is the initiator of the request that requires authentication. The supplicant request is sent to the authenticator which receives the request and forwards it to the authenticator which verifies the supplicant's credentials.

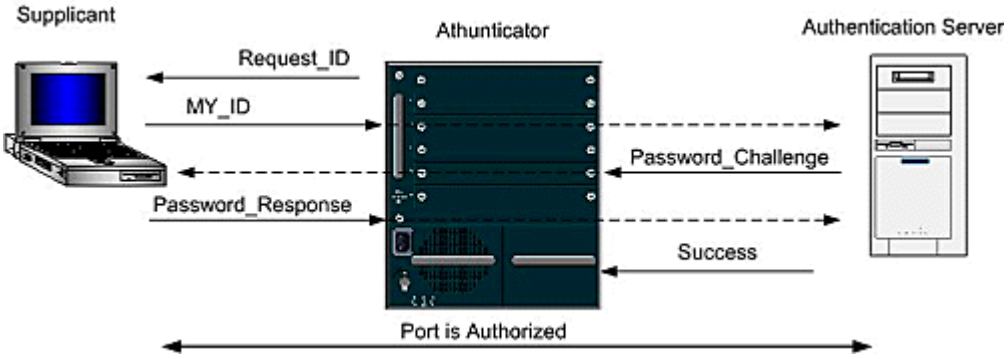


Figure 8. Cisco 802.1x Authentication Process

Cisco's implementation of 802.1x is built upon traditional port security and provides greater features and functionality. Cisco Identity-Based Networking Services (IBNS) provides a mechanism for implementing 802.1x identity-based networking on Cisco networks. It is composed of the following components [22]:

- Machine Authentication – Provides a mechanism for machine authentication during system boot prior to dynamic IP address assignment and port-based user authentication. This feature is only supported by Microsoft Windows because it requires an Active Directory server to validate the machine name.
- 802.1x and NAC – 802.1x can use information including the machine name, client-side digital certificate, and username and password to identify and authenticate a user onto a port in the network. NAC is a form of authentication that is considered a superset of 802.1x and uses port authentication as a base for identity authentication, and then extending the authentication process to check security posture of the device. 802.1x can be incorporated with the Cisco NAC solution to achieve port, identity, and posture authentication and verification.
- VPN and 802.1x – Port-based user-authentication is very useful in a remote-access or teleworker environment. Typically, an organization cannot control a user's home network, and it is not uncommon for a home system to be infected with a virus which then compromises the organization's network. This solution requires a home router that is IOS-based and includes an embedded 802.1x authenticator. The 802.1x supplicant on the home system sends information to the 802.1x authenticator on the router which then forwards the authentication request to the authentication server at the corporate network. This method will allow a trusted machine access to the corporate network while denying connections to other, untrusted systems on the home network.

Host Intrusion Prevention

The Cisco Security Agent (CSA) is a software-based solution that serves as the last line of defense in a layered self-defending network. The CSA is installed directly on the host system. Supported host systems include PCs, laptop, or servers on the network. The CSA operates by monitoring the OS kernel and requests to the file system, network resources, and registry keys. CSA stops an attack by looking at the symptoms of an attack instead of looking for a signature of a known attack. CSA will not necessarily identify a virus that is attempting to delete a system file but would stop the attempt and notify the user that something was trying to delete a system file. This solution works well against what are known as zero-day attacks. Zero-day attacks are attacks in which vulnerability is manipulated before a vendor can release a patch to the public. On February 16, 2007, Microsoft announced a new zero-day attack [23] where attackers are using specially crafted Word files that exploit a recently discovered vulnerability in Microsoft Office 2000 and XP. In this example, hackers have known about this vulnerability and have been exploiting it before Microsoft has been able to issue a patch to secure the application. CSA management is incorporated into the Cisco Management Center which is discussed below. CSA also provides

qualifications, or support, for many different operating systems. CSA includes the following features and qualifications [24]:

- Zero-day protection against certain attacks
- Host intrusion prevention
- Protection against buffer overflows
- Port scan detection
- Distributed personal firewall protection
- Protection against spyware/adware
- Application inventory
- Location-based policies depending upon whether the machine is on a home network or the corporate network
- Policies to restrict access to removable media, including USB devices
- Support for International Windows
- Native end-station Cisco Security Agent Panel support for French, German, Japanese(Kanji), Chinese, Italian, Spanish, and Korean
- Application inventory and use-tracking
- Hot fix and Service Pack (SP) checking
- File and directory protection
- Enforcing security policies for data on Clipboard
- Antivirus DAT checking
- Windows XP Home Edition support
- Embedded Cisco Trust Agent in Cisco Security Agent
- Auto-enrollment group for Windows, Solaris, and Linux
- QoS marking of applications from Cisco Security Agent
- VMWare qualification
- Tablet PC qualification
- Solaris 9

CSA also contains an optional component known as the network shim. The network shim provides end-station protection against attacks by detecting SYN floods, port scans, and malformed packets at the shim layer on the OS at the end station. These types of attacks are network driven and are usually detected and defended by network devices.

Cisco Security Centralized Management

Centralized management is an effective tool that ensures all components of a layered defense are working together to execute the same plan. Centralized management can also interact with a support organization by providing notification when a layered defense is not functioning correctly or is under attack. The Cisco Security Manager (CSM) serves as the centralized management tool for all components of the Cisco Self-Defending Network. It provides mechanisms for monitoring all components as well as mitigating threats. It also provides a configuration mechanism. The CSM is composed of the following three components [25]:

- Device view – This view allows the administrator to manage all devices on the network, providing mechanisms for configuring interface roles, creating ACLs, applying these roles and ACLs across multiple devices as well as some device auditing.
- Map view – Provides an interface for viewing devices and components on the network based on their location instead of by device view; provides the same details as the Device view.
- Policy view – Allows an administrator to view all policies in place across the network and all devices in the self-defending solution. It serves as an auditing tool and is helpful when incorporating the human factor component of the defense-in-depth model.

The CSM also provides a module for management of the IPS solution.

Summary

After reviewing the major types of attacks and traditional defenses employed to protect against them, it is important to understand the placement of Cisco's Self-Defending products into this process. The Cisco line of self-defending products replicate many of the components defined as network defenses or defense-in-depth components. These Cisco products also augment and improve on these defenses and strategies. The following matrix shows the relationship between Cisco's solutions and the traditional network defenses and components of the defense-in-depth strategy:

	Cisco Solutions	DDoS Mitigation	ASA	ICS	NAC	802.1x	HIP	CSSM
Traditional Defenses	Static Packet Filter	X	X	X	X	X	X	X
	Stateful Firewall	X	X		X		X	X
	Proxy Firewall				X		X	X
	IDS/IPS		X	X	X		X	X
	VPN Device		X		X	X		X
Defense-in-Depth	Ingress/Egress Filtering		X		X	X		X
	IDS Sensors		X		X		X	X
	Host-Centric Firewalls				X		X	X
	Antivirus Software		X	X	X	X	X	X
	Operating System Hardening				X	X		X
	Configuration Management				X	X		X
	Audits	X	X	X	X	X	X	X

Table 2. Cisco Solution/Traditional Network Defense Matrix

In general, the ASA device serves as the heart of the perimeter defense and provides the primary component of the Self-Defending network. Many of the traditional network defenses such as static packet filtering, a stateful firewall, VPN services, and IDS/IPS are available with this appliance. Once this device is installed, an organization can begin to add more components and layer additional levels of security. The following diagram [26] illustrates a typical corporate network and the placement of Cisco Self-Defending components:

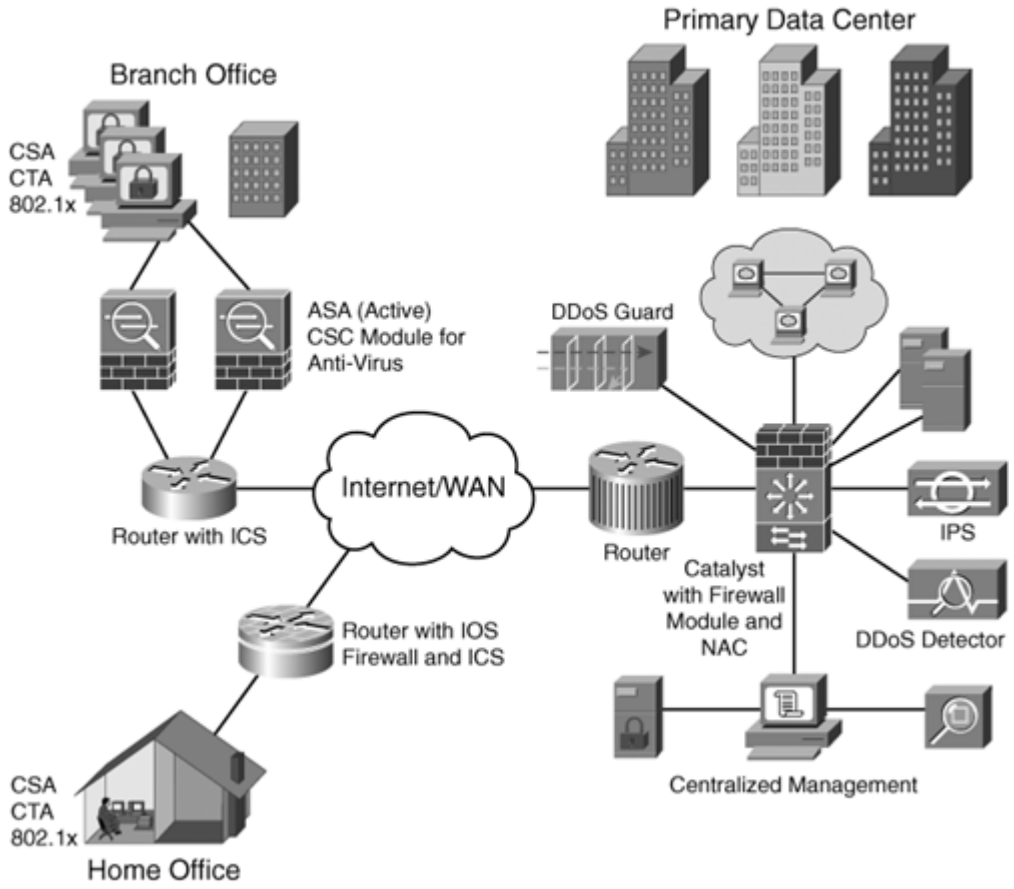


Figure 9. Cisco Self-Defending Network Diagram

It is also important to note that Cisco does not provide solutions for all factors of network defense and defense-in-depth. Audits, operating system hardening, and anti-virus, which are key components of defense-in-depth, are not expressly provided for by Cisco and are dependent on other vendors and different solutions. However, it is clear the Cisco products play a key role in augmenting perimeter security and play a key role in providing layers of defense as prescribed in the defense-in-depth model.

References

[1] De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pgs. 3-7.

[2] Cohen, Fred (1984). Retrieved March 17, 2008 from Fred Cohen and Associates web site: http://all.net/books/virus/part2.html

[3] Andres, Rodney (2007). Retrieved April 19, 2008 from Symantec Security Response Center web site: http://www.symantec.com/business/security_response/writeup.jsp?docid=2004-081215-0934-99&tabid=2

[4] Newsweek (2004). Retrieved April 19, 2008 from http://www.newsweek.com/id/52912/page/1

[5] Jackson Higgins, Kelly (2008). *New Massive BotNet Twice the Size of Storm*. Retrieved April 19, 2008 from http://www.darkreading.com/document.asp?doc_id=150292&WT.svl=news1_1

[6] Carnegie Mellon University (1996). *CERT® Advisory CA-1996-26 Denial-of-Service Attack via ping.* Retrieved April 19, 2008 from http://www.cert.org/advisories/CA-1996-26.html

[7] De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pgs. 19-21.

[8] Cisco, Inc. Defeating DDoS Attacks. Retrieved April 18, 2008 from http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/prod_white_paper0900aecd8011e927.html

[9] Chapman, D. Brent; Zwicky, Elizabeth D. (1996). *Firewall Design: Here's a practical guide on how to protect your network*. Retrieved April 18, 2008 from http://sunsite.uakom.sk/sunworldonline/swol-01-1996/swol-01-firewall.html

[10] M4k3 (2006). Spoofing Tutorial. Retrieved April 19, 2008 from http://www.elitehackers.info/forums/archive/index.php/t-3993.html

[11] Northcutt, Stephen (2005). *Inside Network Perimeter Security*. Indianapolis IN: Sams Publishing, pg 20.

[12] Cisco Systems, Inc. (2008). Defeating DDoS Attacks. Retrieved April 18, 2008 from http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/prod_white_paper0900aecd8011e927_ns615_Networking_Solutions_White_Paper.html

[13] Cisco Systems, Inc. (2008). Defeating DDoS Attacks. Retrieved April 18, 2008 from http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/prod_white_paper0900aecd8011e927_ns615_Networking_Solutions_White_Paper.html

[14] De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pgs. 80-81.

[15] De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pg 120.

[16] De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pgs. 120-121.

[17] De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pg. 122.

[18]De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pg. 123-124.

[19]De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pg. 125.

[20] De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pgs. 110.

[21] McQuerry, Steven (2002). IEEE 802.1X: Practical Port Control for Switches. Retrieved April 27, 2008 from http://www.ciscopress.com/articles/article.asp?p=29600&seqNum=2.

[22] De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pgs. 111-115.

[23] Kirk, Jeremy (2007). Attacks seize on new zero-day in Word. Retrieved April 27, 2008 from http://www.infoworld.com/article/07/02/15/HNzerodayinword_1.html

[24] De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pgs. 163-164.

[25] De Capite, Duane (2007). *Self-Defending Networks: The next Generation of Network Security*. Indianapolis, IN: Cisco Press, pgs. 180-202.

[26] Cisco (2008). Introducing Cisco Self-Defending Networks. Retrieved April 27, 2008 from http://safari.ciscopress.com/1587052539/ch01lev1sec3