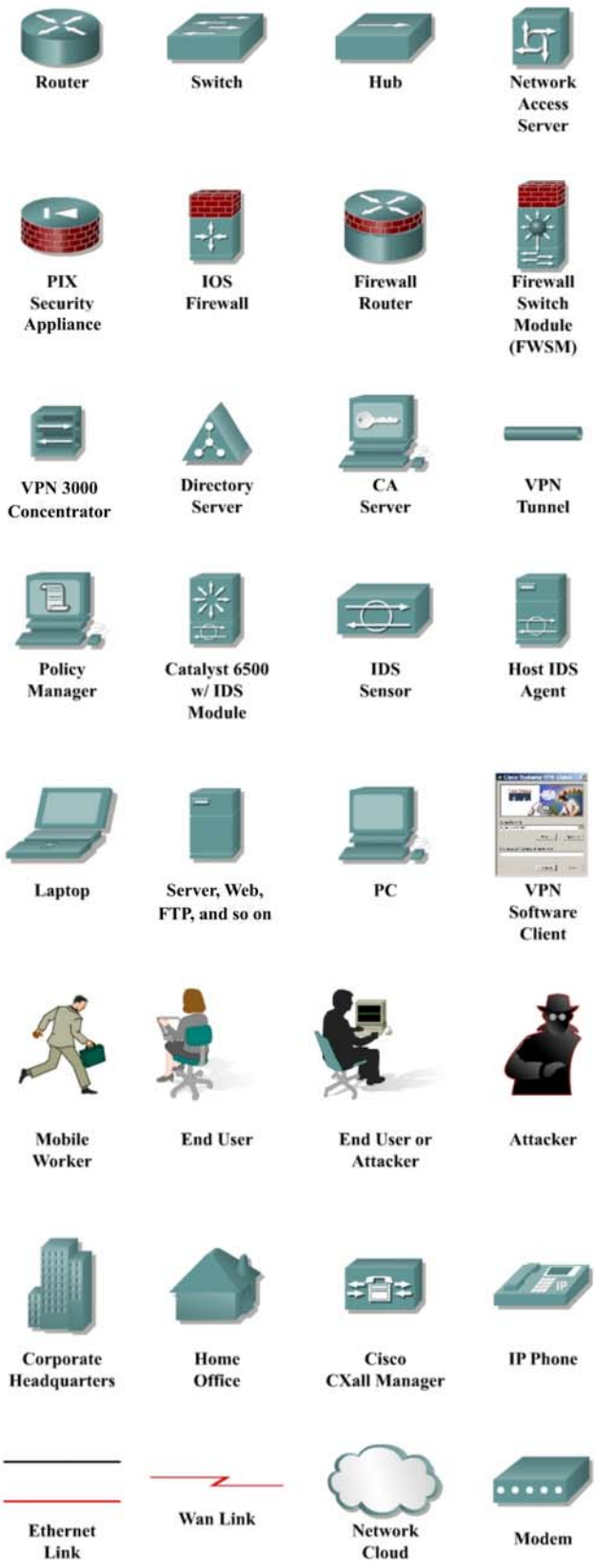
Fundamentals of Network Security Graphic Symbols

Overview


Router
Switch
Hub
Network Access Server
PIX Security Appliance
IOS Firewall
Firewall Router
Firewall Switch Module (FWSM)
VPN 3000 Concentrator
Directory Server
CA Server
VPN Tunnel
Policy Manager
Catalyst 6500 w/ IDS Module
IDS Sensor
Host IDS Agent
Laptop
Server, Web, FTP, and so on
PC
VPN Software Client
Mobile Worker
End User
End User or Attacker
Attacker
Corporate Headquarters
Home Office
Cisco CXall Manager
IP Phone
Ethernet Link
Wan Link
Network Cloud
Modem

Router

Figure 1: IOS Router icon and photos

A Router is an internetworking device which operates at OSI Layer 3. A Router interconnects network segments or entire networks and passes data packets between networks based on Layer 3 information. The router, by default, is an open device. Services must be turned off or secured.

Routing hardware provides everything from high-end routing platforms for building IP optimized backbones, to Ethernet LANs to WANs for the enterprise, medium and small businesses, and home offices.

Cisco router models include:

- 12000, 10000, and 7000 series for enterprise and service provider
- 3600, 2600, 2500, 1700 series for medium business and branch offices
- 70, 90, and 800 series for small business and home office

Switch

Figure 1: Switch icon and photos

Switches connect LAN segments, use a table of MAC addresses to determine the segment on which a datagram needs to be transmitted, and reduce traffic. Switches, which typically operate at Layer 2, can be categorized as stackable or chassis based.

The workgroup switch is typically a stackable switch and is placed in IDFs to provide LAN access to end device. In small networks, these switches can also be used for the core and distribution levels in addition to the access level.

Switches can be configured via menu, command line, or web browser interfaces. Stackable switch models include the Catalyst 1900, 2900 and 3500 series. Chassis based switches include the Catalyst 4000, 5000, 6000, 8000, and 9000 series.

Hub

Figure 1: Hub icon and photos

Hubs, or multiport repeaters, are legacy devices which combine connectivity with the amplifying and re-timing properties of repeaters. Hubs operate at Layer one of the OSI. It is typical to see 4, 8, 12, and up to 24, ports on multiport repeaters. This allows many devices to be cheaply and easily interconnected.

Hubs have limited scalability due to shared bandwidth and high collision rates. Hubs are typically used for small office and home office environments.

Cisco offers the 1538 Hub series. Other network vendors provide a larger selection of Hub models and port configurations.

Network Access Server

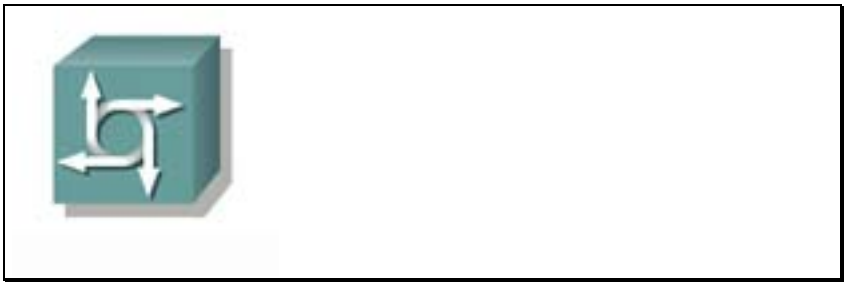


Figure 1: Network access server icon

Network Access Servers (NAS), such as a 2509 and 2511 router series, terminate remote access dial users for small and medium networks. Analog Modem Network Modules such as the NM-8AM and NM-16M can be used in 2600, 3600 and 3700 series routers to provide remote dial access as well.

The AS5300, AS5400, and AS5800 series are typically used in service provider and enterprise networks to provide the following services to users:

- Long Distance
- Prepaid Calling
- Local Access
- Hosted IP Telephony
- ASP Hosting and Termination
- Unified Communications
- Access VPN
- Dial Access

Hardware-based Firewall

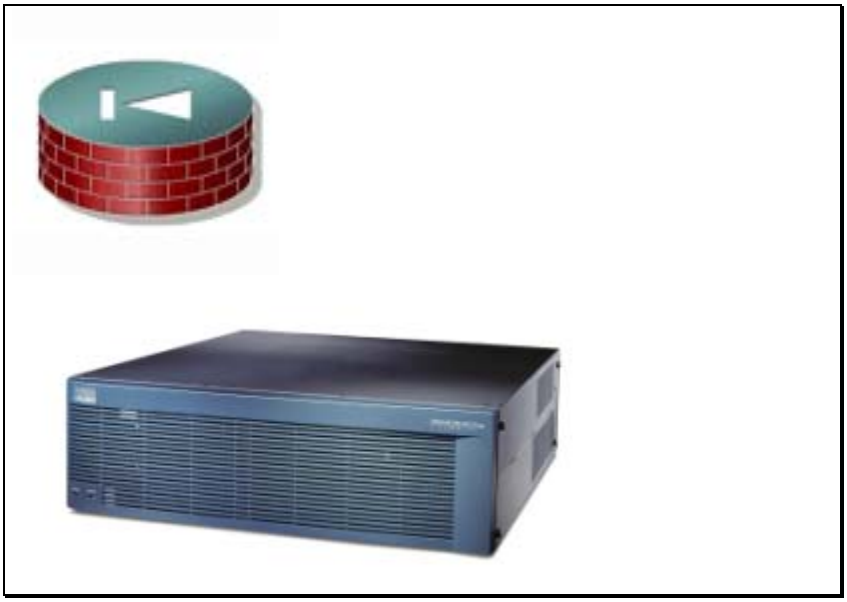


Figure 1: Firewall icon and photo

Hardware-based firewalls, or dedicated firewalls, are devices that have the software pre-installed on a specialized hardware platform. A firewall provides a single point of defense between two networks to protect one network from the other. Usually, a firewall protects the private network of a company from the public or shared networks to which it is connected. A dedicated firewall provides maximum configuration flexibility within a network.

The primary function of a firewall is to filter traffic based on Layer 4 connections. Many firewalls also provide encryption services to protect traffic, creating a secure Virtual Private Network (VPN).

The PIX Security Appliance, by default, is a closed device. Services must be turned on to allow traffic to pass. PIX Models, which scale from home office to service provider level, include the 501, 506E, 515E, 525, and 535.

IOS Firewall

Figure 1: IOS Firewall icon and photos

The Cisco IOS Firewall, provides robust, integrated firewall, intrusion detection, and VPN functionality for every perimeter of the network. The Firewall Feature Set is available for most Cisco routers including the 800, 1600, 1700, 2500, 2600, 3600, 7100, and 7200 series routers, however some features may not be available on low end and legacy router models.

An integrated firewall provides greater interoperability within the existing network. Either IOS Firewall or Firewall Router icon can be used to represent the Cisco IOS Firewall.

Firewall Services Module

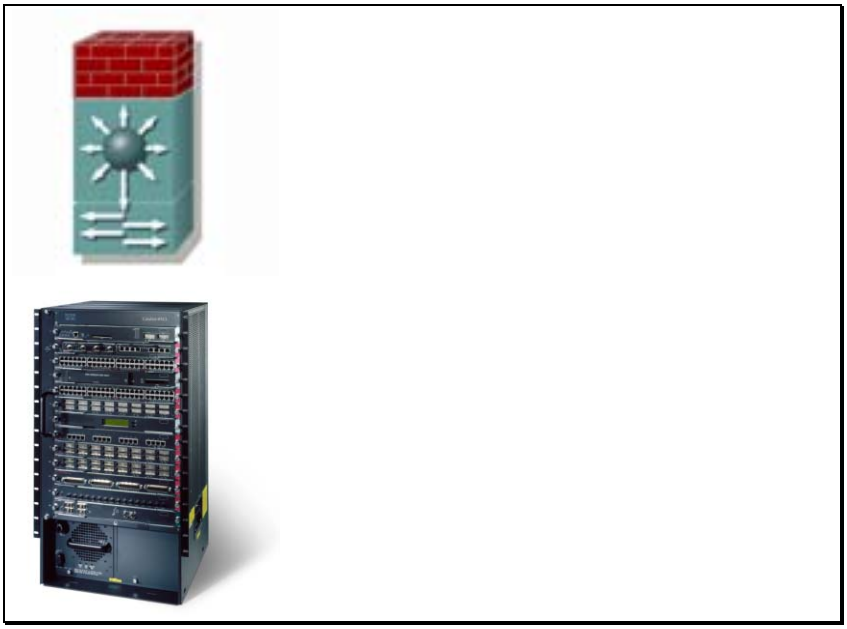


Figure 1: Firewall Services Module icon and photo

Cisco Firewall Services Module (FWSM) is a high-speed, integrated firewall module for Cisco Catalyst ® 6500 switches and Cisco 7600 Series routers, and provides a 5 Gbps throughput, 100,000 connections per second, and one million concurrent connections. Up to four FWSMs can be installed in a single chassis providing scalability to 20 Gbps per chassis. Based on Cisco PIX ® Firewall technology, the FWSM provides large enterprises and service providers with unmatched security, reliability, and performance within a switch chassis.

The traditional role of firewalls has changed. Firewalls now do more than protect a corporate network from unauthorized external access. They can also prevent unauthorized users from accessing a particular subnet, workgroup or LAN within a corporate network.

VPN 300 Series Concentrator

Figure: VPN 300 Series Concentrator icon and photo

Cisco VPN 3000 Series Concentrators is a family of purpose-built, remote access Virtual Private Network (VPN) platforms and client software that incorporates high availability, high performance and scalability with the most advanced encryption and authentication techniques available today.

Cisco VPN 3000 Series Concentrators include models to support a range of enterprise customers, from small businesses with 100 or fewer remote access users to large organizations with up to 10,000 simultaneous remote users.

The models include the 3005, 3015, 3030, 3060, and the 3080.

Directory Server

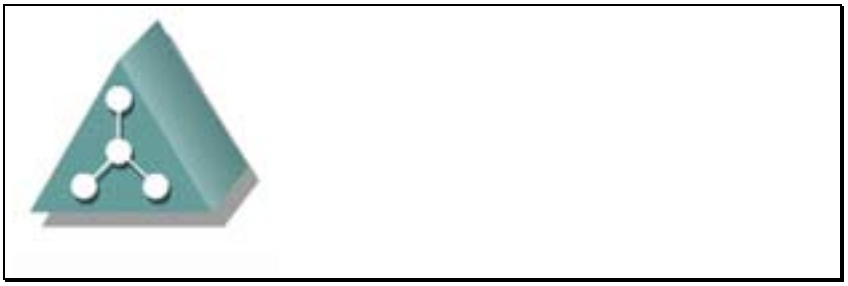


Figure 1: Director server icon

A directory server allows organizations to centrally manage and share information on network resources and users while acting as the central authentication point for the network. It is a central storage location for information assets such as users, applications, servers, computers, files, and printers. In large corporations, a directory server must maintain information on thousands of users, computers, servers, and files.

Some examples include Lightweight Directory Access Protocol (LDAP) servers, Microsoft Active Directory (AD) servers, and Novell Directory Services (NDS) servers.

Certificate Authority Server

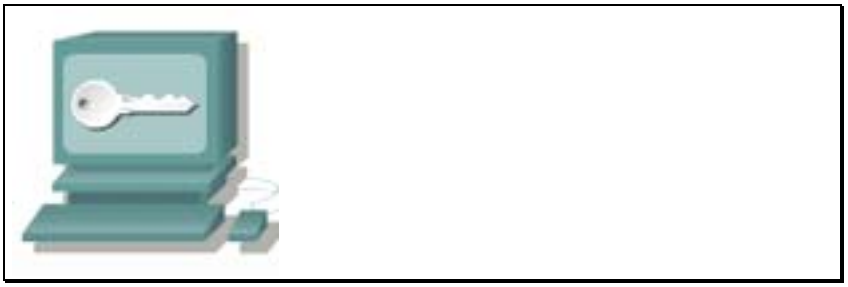


Figure 1: CA Server icon

A Certificate Authority (CA) Server issues digital certificates to network devices. Digital certificates are used to authenticate devices and users when creating a VPN connection or tunnel.

There are several CA vendors that interoperate with Cisco IOS software on Cisco routers. They include Entrust, VeriSign, Baltimore, and Microsoft. Several CA vendors support the simple certificate enrollment protocol (SCEP) for enrolling Cisco routers and PIX Security Appliances.

Virtual Private Network Tunnel

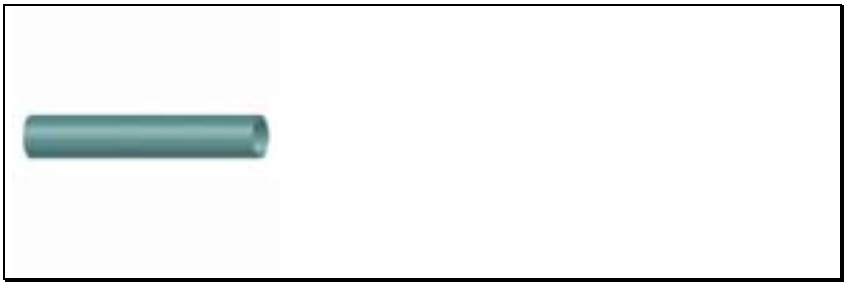


Figure 1: VPN tunnel

A Virtual Private Network (VPN) tunnel is created between two network devices. The devices can include servers, software clients, VPN routers, concentrators, and PIX Security Appliances. The tunnel can be created using various technologies including:

- Generic Router Encapsulation (GRE)
- IP Security (IPSec)
- Layer 2 Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)
- Multi-Protocol Label Switching (MPLS)

VPN tunnels can provide confidentiality, integrity, and authenticity between two devices depending on the technology utilized to create the tunnel.

Policy Manager or Policy Director

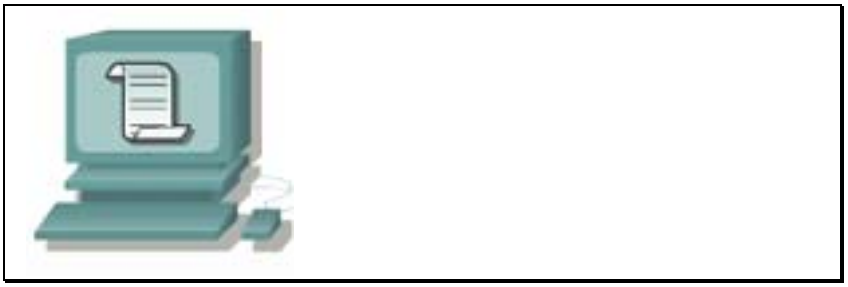


Figure 1: Policy manager or director icon

One of the greatest challenges of network security is management and monitoring of hundreds or thousands of VPNs, routers, firewalls, and intrusion detection sensors. A policy manager or director server is used to manage enterprise level security for medium to large networks. Cisco provides two director platforms:

- Cisco Secure Policy Manger (CSPM)
- VPN Management Solution (VMS)

Catalyst 6500 Series Intrusion Detection System Services Module

Figure 1: Catalyst 6500 Series Intrusion Detection System Services Module icon and photo

The Cisco Catalyst 6500 Series Intrusion Detection System (IDSM) Services Module is a key network based intrusion protection solution for safeguarding organizations from costly and debilitating network breaches such as malicious Internet worms, Denial of Service attacks, and application attacks.

The second generation Cisco IDSM-2 is designed to protect switched environments by integrating full-featured IDS functionality directly into the network infrastructure through the widely deployed Cisco Catalyst® 6500 Series chassis. This integration allows the user to monitor traffic directly off the switch back-plane - a logical platform for additional services such as firewall, virtual private network (VPN) and IDS services.

The Cisco IDSM-2 is works in concert with other components to increase the operating efficiency of intrusion protection to secure data infrastructure.

IDS Sensor

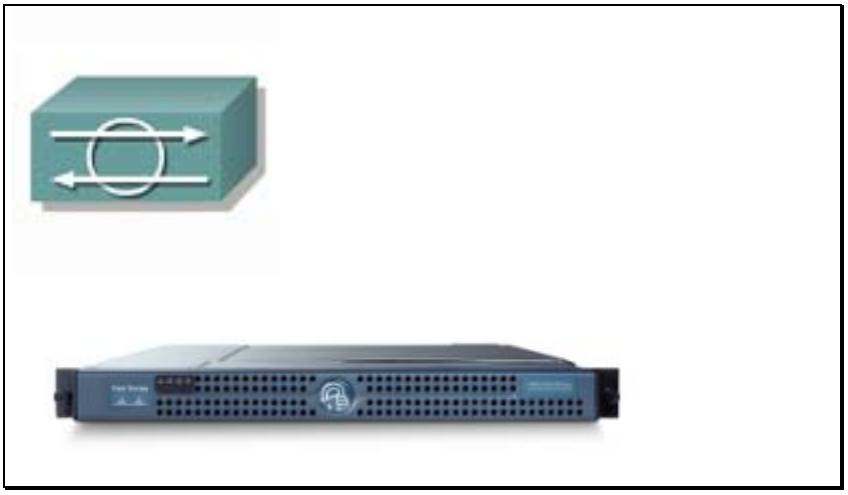


Figure 1: IDS Sensor

A IDS Sensor is a network appliance which monitors traffic flowing across a network segment. IDS Sensors respond to any attacks in real time by resetting any traffic which matches an attack signature, and sending alarms to a central monitoring server.

IDS Sensors are purpose-built, high-performance network security “appliances” that protect against unauthorized, malicious activity traversing the network, such as attacks by hackers.

The Cisco IDS 4200 Series of appliance sensors includes three products: the Cisco IDS 4210, the Cisco IDS 4235, and the Cisco IDS 4250. Each appliance sensor addresses the bandwidth requirements at one of a variety of performance marks, from 45 Mbps to 1 Gbps.

Host Intrusion Detection Agent

Figure 1: Host intrusion detection agent icon

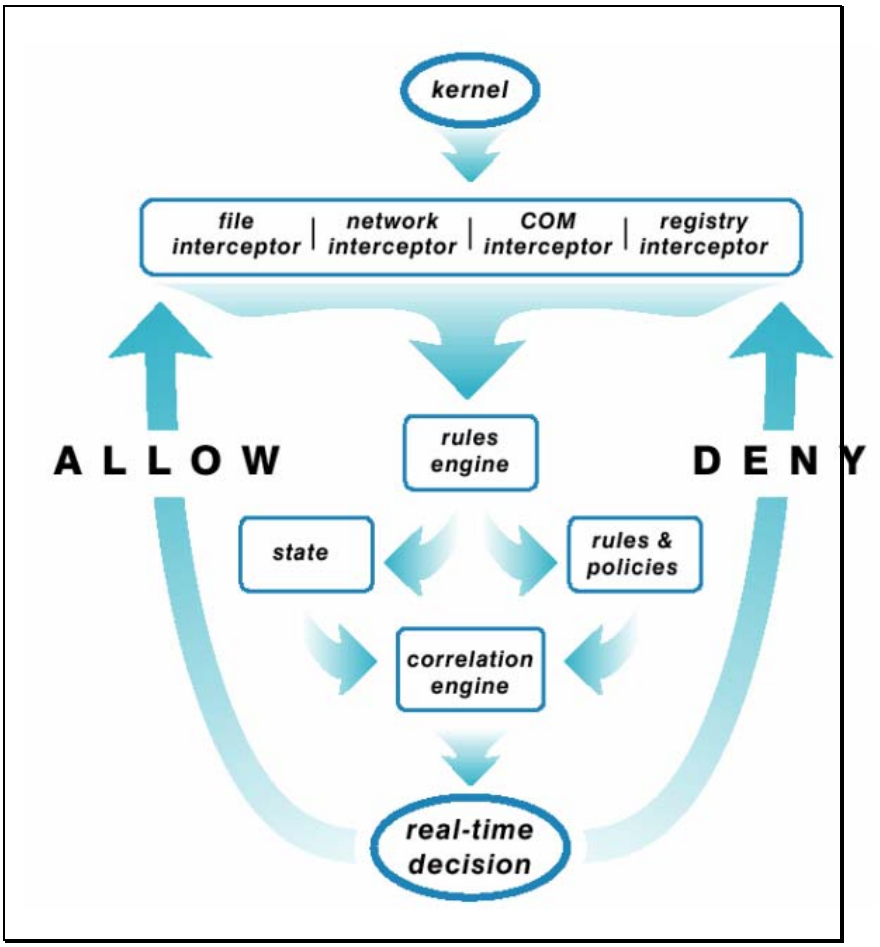


Figure 2: Component object model

Host based intrusion detection software should be installed on mission critical desktops and servers. Most of the attacks today are targeted towards public servers.

Cisco provides host based intrusion detection using the Cisco Security Agent, which resides between the applications and the kernel. The agent intercepts all system calls to file, network, and registry sources, as well as to dynamic, run-time resources such as memory pages, shared library modules, and Component Object Model (COM) objects. The agent correlates behaviors of these system calls, based on rules that define appropriate or acceptable behavior for a specific application. Then the software permits

or denies the action and sends an alarm to a central monitoring server or agent manager when an attack is detected.

Laptops

Figure 1: Laptop icon and photo

Laptops are present on almost every network today. They are becoming standard desktop replacements in many corporations. Users can work at the office, from home, or any other location with Internet access.

Two trends which greatly increased the use of laptops include wireless LANs and VPNs. Both are critical productivity factors, however these must be securely implemented to avoid network breaches. Laptop theft is also a big problem which must be considered as well. Many anti-theft hardware and software solutions are available.

Viruses, Trojan horses, hostile applets, and worms pose a great problem to laptop computers and network systems. Anti-virus software should be installed on laptops. Furthermore, operating systems must be continually updated with security patches and fixes to remain as secure as possible.

Server

Figure 1: Server icon and photo

In most networks, servers are the brains of the operation while networking devices provides the nervous system of the business. It is very important that these resources are protected against attacks. Some of the common server platforms include:

- Microsoft Windows NT and 2000 Server
- Sun Solaris
- LiNux

Servers provide critical functions including:

- File, Email and Web Services
- Print Services
- Storage
- Voice Call Management
- Database Services
- Directory Services

Personal Computer

Figure 1: PC icon and photo

The Personal Computer (PC) has only been around for 25 years and has greatly changed the world. Functionality, performance, and storage have greatly increased. With the advent of the Internet, PCs have become commonplace in governments, businesses, schools, and homes. Unfortunately, with increased capabilities and connectivity, security vulnerabilities in applications and operating systems are a big problem. It is these vulnerabilities, which are exploited by hackers today. With broadband services such as DSL and Cable, the attacks have increased dramatically.

Viruses, Trojan horses, hostile applets, and worms pose a great problem to computers and network systems. Anti-virus software is very important in a networked world. Furthermore, operating systems must be continually updated with security patches and fixes to remain as secure as possible.

VPN Client Software

Figure 1: VPN Client software

VPN Client software, which is installed on a PC or laptop, enables users to create a secure tunnel to the corporate intranet. This allows telecommuters the ability to access internal corporate resources such as email, voice, video, web, and file services which are not available to the public.

Simple to deploy and operate, the Cisco VPN Client enables a secure, end-to-end encrypted tunnel. This software client can be terminated on several VPN products including the VPN router, PIX Security Appliance, and the Cisco VPN 3000 Series Concentrator.

There are other VPN clients available including the native Microsoft VPN client and other 3rd party clients.

Mobile Worker

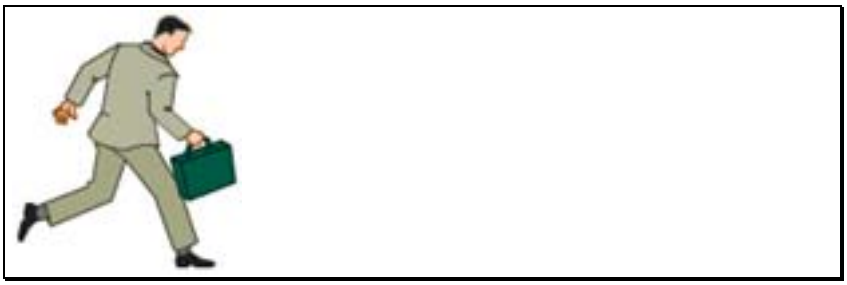


Figure 1: Mobile worker icon

Mobile workers can include staff within a company. Virtually every occupation and business has workers who are mobile.

For many years, the challenge was connectivity to the corporate network, especially when dial-up access was the only way to connect. Today, users can connect by way of

56K dial-up, ISDN, DSL, Cable, and any LAN connected to the Internet. Connectivity is no longer a big concern. Security is.

Wireless LANs have also created a new workplace where workers can move around the office as needed and maintain connectivity. With wireless LANs, people can easily access the Internet while at home, in a hotel, at the airport, at the coffee shop, and in many public areas. Unfortunately, without security measures in place, hackers have access as well.

End User

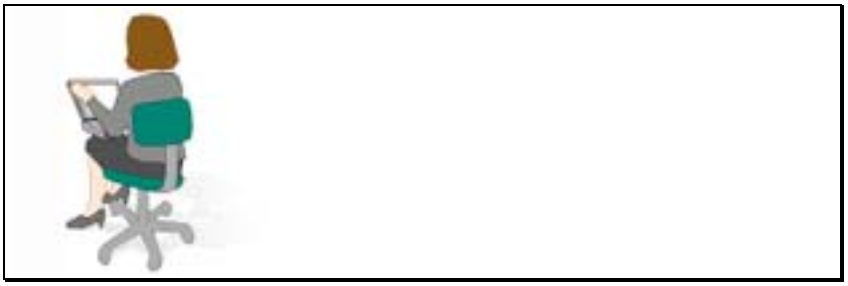


Figure 1: End user icon

End users are workers who are connected to the network through a PC, laptop, or other mobile devices. Users are what drive the business. Without people, a business cannot survive. Unfortunately, they also can be responsible for security breaches. Some users carelessly use easy to guess passwords, write them on a note near the computer, or simple give their passwords when asked.

Users also inadvertently download viruses, Trojans horses, and hostile java and active-x code from various web sites. Many users delete files accidentally or may email confidential information without thinking twice. And on occasion, some users connect a wireless access point on the corporate network without and security mechanism in place.

End User or Attacker

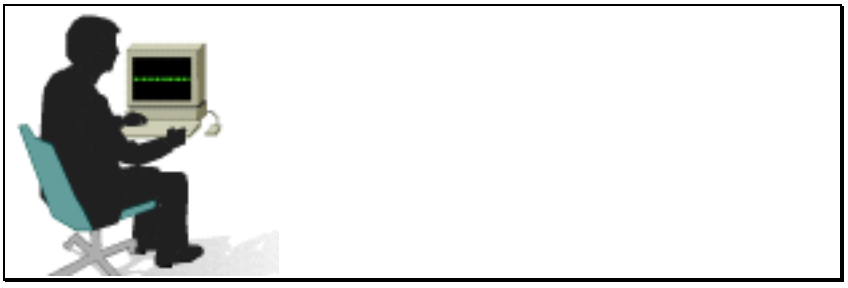


Figure 1: End user or attacker icon

At one point, some end users can become the attacker. Many times, there is a fine line between network use and hacking, for example, a user in the marketing department accessing confidential data in the human resources department.

Almost 75 percent of the network attacks come from inside the network.

Attacker

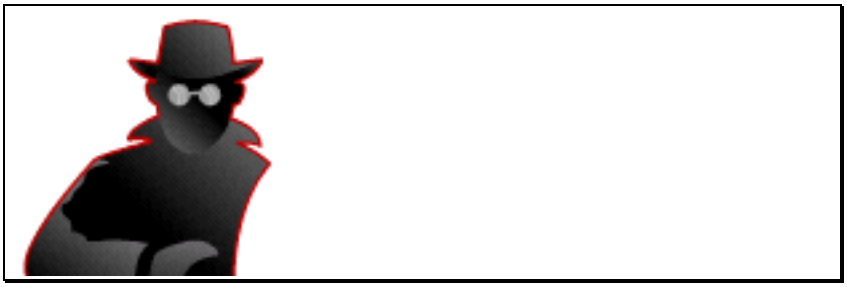


Figure 1: Attacker

An attacker, also know as a hacker, is an end user who is attempting to:

- Discover the network
- Access the network
- Damage the network

Attackers access the network either internally or externally. Remember that 75 percent of the attacks come from within the network. Attackers can be curious users, corporate spies, government operatives, careless users, disgruntled employees, or elite hackers.

Corporate Headquarter

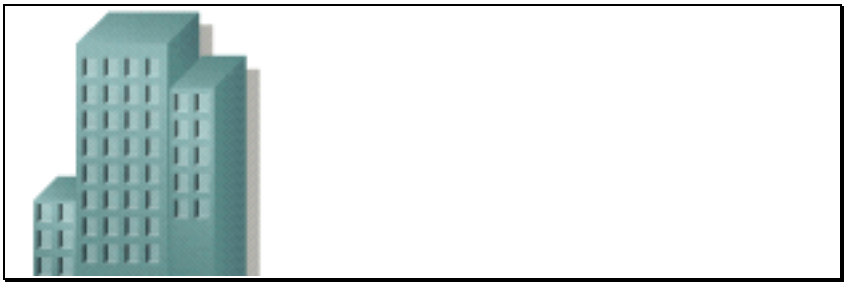


Figure 1: Corporate headquarter icon

The Corporate Headquarter (HQ) is where the primary network resides. The HQ is a central point of connection between branch offices, business partners, remote users, and the Internet. Devices located at the HQ are most critical to protect.

Home Office

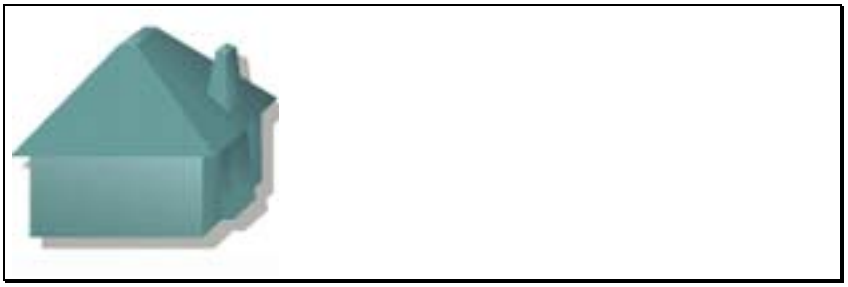


Figure 1: Home office icon

The Home Office has become an extension to the corporate network. More and more users are working remotely from home. This has greatly increased worker productivity and reduced corporate overhead.

Home offices can be connected through various WAN technologies such as dial-up, ISDN, DSL, Cellular, Satellite, and Cable. In many instances, the Internet connection is "always on". This increases the chances that the devices connected within the home office become targets of attack. In some cases, these devices become launch points of attacks without the end users knowledge.

Many homes now have small networks including multiple PCs, a router, and a switch. Wireless LAN devices are becoming very popular connection methods for home offices. Without proper security attackers easily breach home networks.

CallManager

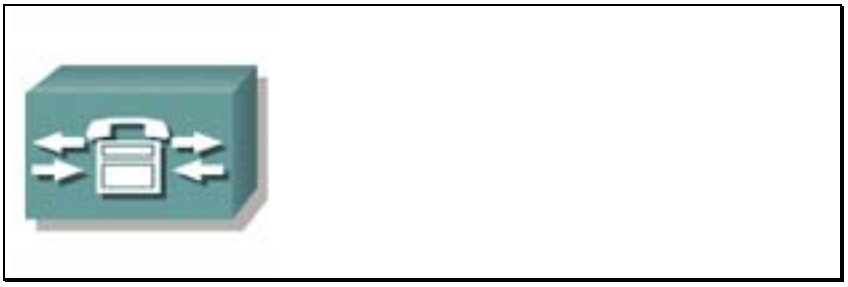


Figure: CallManager icon

Cisco CallManager is the software-based call-processing component of the Cisco IP telephony solution, part of Cisco AVVID (Architecture for Voice, Video and Integrated Data). The software extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems interact with the IP telephony solution through Cisco CallManager`s open telephony application programming interface (API). Cisco CallManager is installed on the Cisco Media Convergence Server (MCS).

IP Phone

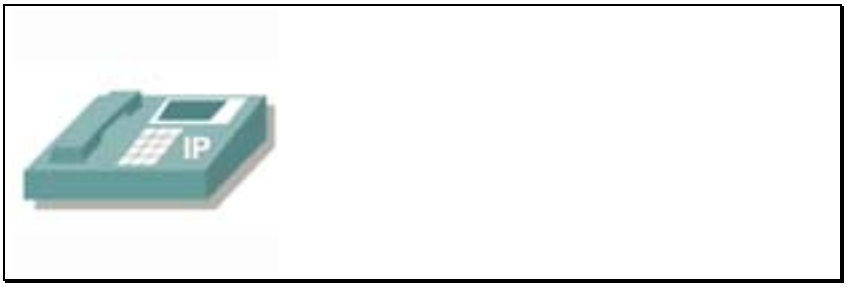


Figure 1: IP phone icon

IP Phones provides voice communication systems over the data network. IP Phones are designed to enhance productivity and leverage the existing data network. The Cisco IP Phones 7960G and 7940G feature a large, pixel-based LCD display and can support additional information services including Extensible Markup Language (XML) capabilities. XML-based services can be customized to provide users with access to a array of information such as stock quotes, employee extension numbers, or any Web-based content. Models including the 7960G, 7940G, 7910G and 7910G + SW, can accept in-line power from a card integrated with a Catalyst switch or a Catalyst in-line power patch panel.

IP Phones must have a central control server called a Call Manager Server to operate on a data network.

Ethernet Link

Figure 1: Ethernet link

Ethernet Links provide connectivity for the entire network. These links interconnect routers, switches, printers, PCs, laptops, servers, and other end devices. Current Ethernet links operate at from 10Mbps to 10Gbps. Ethernet can run over fiber and copper.

Other common LAN link options include access via 802.11a, 802.11b, and 802.11g wireless technologies.

WAN Link

Figure 1: WAN link

WAN Links provide connectivity to the Internet. WAN technologies can be classified as packet switched, circuit switched or cell switched. Technologies include dial-up, ISDN, X.25, xDSL, Satellite, Cellular, Cable, Frame Relay, SMDS, ATM, SONET. Speeds range from 28Kbps to 10Gbps.

Network Cloud

Figure 1: Network cloud

The Network Cloud represents a wide area network (WAN) or the Internet. Network traffic can traverse private and public links depending on the established service and connections. Also, data can traverse a single Internet service provider (ISP) or multiple ISPs.

Modem

Figure 1: Modem

A modem is a device which provides connectivity to the ISPs network access server. A modem can terminate dial-up connections, xDSL, or Cable connections.

A device, which terminates a permanent circuit such as a T1 or T3, is usually called a CSU/DSU.