Glossary

action

An *action* is a component of a security policy that resolves a condition. It is a terminal node in a condition branch. The firewall will enforce a specific action against any session requests that satisfy the condition branch leading to that action. Only two actions exist: ACCEPT and REJECT.

A condition evaluates a session request to determine whether that session satisfies the constraints identified by the user. The action determines whether to accept or reject the session. *See also* condition branch.

address

A unique hexadecimal number that identifies a computer on a network. *See also* IP address.

address classes

Predefined groupings of Internet addresses, with each class defining networks of a certain size. The range of numbers that can be assigned for the first octet in the IP address is based on the address class. Class A networks (values 1-126) are the largest, with over 16 million hosts per network. Class B networks (128-191) have up to 65,534 hosts per network, and Class C networks (192-223) can have up to 254 hosts per network. *See also* octet.

Address Resolution Protocol (ARP)

ARP is a protocol in the TCP/IP suite that provides IP address-to-MAC address resolution for IP-based network packets. *See also* media access control (MAC), IP address, and network packet.

administrative model
The model by which a system is administered. It specifies the abilities of the system to separate administrative actions into different administrative roles. An administrative model is made up of nodes (taken from graph theory), where each node has administrative actions associated with it and those nodes may differ. *See also* hierarchical administrative model and strict adherence administrative model.

agent
The fundamental building blocks of the Cisco Centri Firewall. Agents are designed to perform a specific task or collection of tasks. They provide specific services to other agents within the system.

anonymous FTP
The File Transfer Protocol (FTP) can be set up for anonymous access. Anonymous FTP allows any user on the network who does not have access to an account on your computer to access its files and databases using the account named "anonymous". *See also* FTP.

applet
Refers specifically to a Java-based program that requires a just-in-time compiler to operate correctly. Generically, an applet is a component of an application (e.g., the control panel is an application, all of the things in the control panel are applets.)

application layer firewall
An *application layer firewall* is a third-generation firewall technology that evaluates network packets for valid data at the application layer before allowing a connection. It examines the data in all network packets at the application layer and maintains complete connection state and sequencing information. In addition, an application layer firewall can validate other security items that only appear within the application layer, such as user passwords and service requests. Most application layer firewalls include specialized application software and proxy services. *See also* proxy services.

application proxy
The combination of a client proxy and a server proxy that both reside on an application layer firewall. *See also* proxy server and proxy client.

architecture
The design and structure of specific components of a computer system and how they connect and interact with one another.

ARPANET
Developed in the 1970's and funded by the Advanced Research Projects Agency, ARPANET is the network for which TCP/IP was originally developed. It is primarily used for military research and communications. *See also* DoD Internet.

auditing
Tracking activities of users by recording selected types of events in the security log of a server or workstation.

audit event
An action that causes an audit record to be recorded in the Windows NT Event Log.

audit policy
Defines the types of events that will be recorded for the purpose of improving security.

audit record
The information recorded in the Windows NT event log that describes an audit event including the user's ID, time of the event, session identifier, local port number, and other identifying information.

audit trail
Also referred to as audit logs, audit trails provide a method of accountability within a network application. It identifies who performed what tasks and when they did it. Audit events and audit records are instrumental to providing thorough audit trails. The more events that cause audit records to be recorded as well as the better the detail provided by an audit record, then the better the audit trail.

authentication
Validation of a user's logon information.

autonomous agent

An autonomous agent implies that it does not communicate directly with any other agent. Instead, an agent communicates only with the Security Knowledge Base. Agents communicate with each other indirectly by writing into and reading from the Security Knowledge Base data store. Agents only interact with the Security Knowledge Base. Because all interactions are well understood, this knowledge isolation facilitates rapid subsystem development. In addition, it lessens integration errors by isolating an agent's constraints. *See also* fixed agent and mobile agent.

backup domain controller (BDC)

In a Windows NT Server domain, a computer running Windows NT Server that receives a copy of the domain's directory database, which contains all account and security policy information for the domain. The copy is synchronized periodically and automatically with the master copy on the primary domain controller (PDC). BDCs also authenticate user's logons and can be promoted to function as PDCs as needed. Multiple BDCs can exist on a domain. *See also* primary domain controller.

bastion host

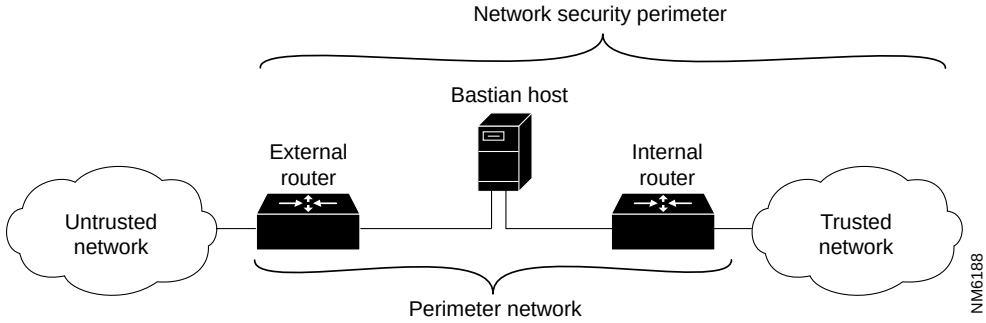
A *bastion host* is a computer that is critical to enforcing your organization's network security policy.

Bastion hosts must be highly secured as they are vulnerable to attacks due to the fact that they are exposed to untrusted or unknown networks and are main points of contact for users of trusted networks. Often, bastion hosts provide services to external users, such as Web services and public access systems. Because these computers are very likely to be attacked, they are often referred to as *sacrificial hosts*.

In rarer cases, bastion hosts are used as one of three components to construct a firewall system—the component that inspects network traffic at protocol layers above the Internet layer. The remaining two components are routers: one known as the internal router (separating the perimeter network from the internal network) and the other known as the external router (separating the perimeter network from the external, or untrusted network). Because bastion hosts only contain one network interface card, this computer cannot protect

itself against IP spoofing attacks. Therefore, to prevent IP spoofing, the bastion host must be positioned between two routers; one router filters all requests from untrusted networks and the other filters all requests from the trusted networks to ensure that no spoofed packets reach the bastion host. These routers also verify that all network traffic that passes between them is addressed to the bastion host only. Figure C-1 depicts a firewall system that is constructed using a bastion host and two routers.

Figure C-1 A Bastion Host Configured as a Component in a Firewall System



Generally, a bastion host runs a general-purpose operating system, such as UNIX, VMS, Windows NT, rather than a ROM-based or firmware operating system. It gets its name from the highly fortified protections on the outer walls of medieval castles. *See also* dual-homed bastion host and firewall server.

break-in

A successful intrusion or attack on a computer that resides on your network.

bridge

A device used at the data link layer that selectively copies packets between networks of the same type.

circuit level firewall

A *circuit level firewall* is a second-generation firewall technology which validates the fact that a packet is either a connection request, or a data packet belonging to a connection, or virtual circuit, between two peer transport layers.

To validate a session, a circuit level firewall examines each connection setup to ensure that it follows a legitimate handshake for that transport layer protocol. The only widely used transport protocol that utilizes a handshake is TCP. In addition, data packets are not forwarded until the handshake is complete. For each connection that is established, the firewall maintains a table of valid connections (which includes complete session state and sequencing information) and lets network packets containing data pass through when network packet information matches an entry in the virtual circuit table. Once the connection is terminated, the table entry is removed, and that virtual circuit between the two peer transport layers is closed.

client
A system that uses NIS, NFS, or other services provided by another system. Web browsers, such as Netscape Navigator and Microsoft Internet Explorer, are also clients for Web servers.

client application
A networked application that requests network services directly from a server application.

client server
A program that has a client application and a server application. The server application presents network or information services to a client application upon request.

condition
A comparative test between user-defined values and the actual values of a session request. *See also* condition branch.

condition branch
A condition branch is one or more conditions terminated by two terminal nodes. Depending on whether the session request parameters satisfy the condition, the request is either accepted, rejected, processed by the next condition branch, or passed up to the next security policy for evaluation to find a condition that more closely matches the parameters of a particular session request.

Three explicit terminal nodes exist: ACCEPT, REJECT, or USE NEXT POLICY. ACCEPT and REJECT are actions. One implicit terminal node exists: continue to the next condition branch. The CONTINUE and USE NEXT POLICY statements differ from actions because they do not signal the end of the evaluation process.

When a condition continues to the next condition branch, we call this an implicit terminal node because we are continuing the evaluation directly with the next condition branch within the same security policy. When we continue to the next policy, we are explicitly stating that this security policy does not have the condition branches appropriate to satisfy the session request so we direct it to the next available security policy for further processing. *See also* action.

controlled host

Controlled hosts are computers that are the object of the activities of the agents. These hosts are controlled by decisions made by other agents. Computers executing product instances are examples of controlled hosts. Generally, fixed agents run on controlled hosts. *See also* controlling host.

controlling host

Controlling hosts are computers that run agents, but are not directly affected by the actions of the agents. Computers that run the administration agent are examples of controlling hosts. Generally mobile agents execute on controlling hosts. *See also* controlled host.

daemon

In UNIX, a server program. The term is from the Old English *daemon* meaning deified being, not *demon* meaning evil spirit.

DARPANET

The network used/created by the Department of Defense's Advanced Research Projects Agency.

datagram

Non-sequenced, self-contained network transmission unit at the IP level. The datagram is the fundamental unit for IP and UDP.

(Other) A packet of data and other delivery information that is routed through a packet-switched network or transmitted on a local area network.

decision tree
A decision tree comprises one or more condition branches. *See also* condition branch.

decapsulation
The process of removing headers and trailers from an incoming datagram as it travels up a network stack. It is the opposite process to encapsulation. Each layer strips off its header and/or trailer before passing the data up to the layer above. As information flows back up the network stack, information received from a lower layer is interpreted as both a header/trailer and data.

directory database
A database of security information, such as user account names and passwords, and the security policy settings. For Windows NT Workstation, the directory database is managed using User Manager. For a Windows NT Server domain, it is managed using User Manager for Domains. Other Windows NT documentation may refer to the directory database as the Security Accounts Manager (SAM) database.

DMZ
De-Militarized Zone. *See* perimeter network.

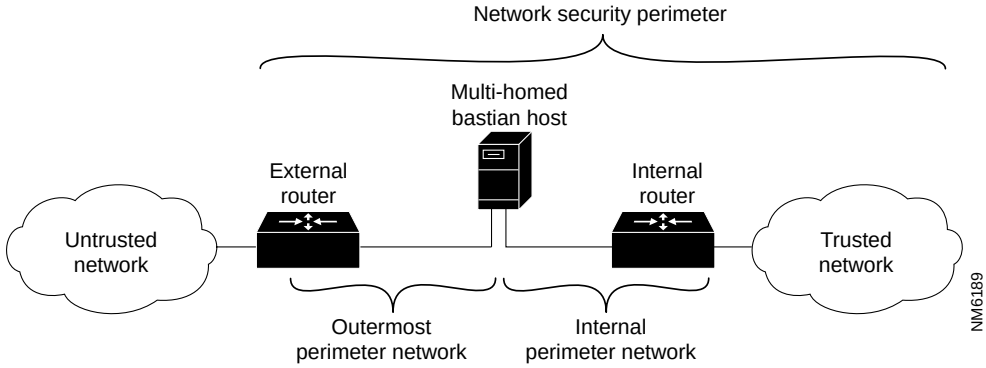
DoD Internet
Department of Defense (DoD) Internet. A wide area network to which the ARPANET belongs. *See also* Internet.

Domain Name Service (DNS)
One of three network-based systems for translating hostnames into Internet addresses. The other two are NIS (Sun Microsystems) and NetInfo (NeXT, Inc.). Of these three, DNS is a true distributed name resolving program that can access information at remote sites. DNS provides more functions than either NIS or NetInfo. DNS is principally used for the lookup of IP addresses based on hostnames.

dual-homed bastion host

A *dual-homed or multi-homed bastion host.* A computer with two (dual-homed) or more (multi-homed) network interface cards connecting it to two or more physical networks (see Figure C-2). This computer evaluates each network packet that it receives against a security policy definition file. A multi-homed bastion host can translate between two network access layer protocols (e.g., Ethernet to Token Ring) and check for IP spoofing attacks using trust tables. If positioned between two routers (an internal and external network pair), dual-homed bastion hosts allow for less complex rules in the routers, which increases performance. However, routers are not required with a dual-homed bastion host if it can provide the necessary routing and security functions.

Figure C-2 A Multi-Homed Bastion Host (Dual-Homed Here) Configured as a Component in a Firewall System



In firewall configurations, a dual-homed bastion host usually acts to block or filter some or all of the traffic trying to pass between the networks. IP traffic forwarding is usually disabled, restricting all traffic between the networks to whatever passes through some kind of security inspection mechanism. *See also* bastion host and firewall server.

dynamic packet filter

A *dynamic packet filtering firewall* is a fourth-generation firewall technology that allows the modification of the firewall security rule base on the fly. This type of technology is most useful for providing limited support for the UDP transport protocol. The UDP transport protocol is typically used for limited information requests and queries for exchanges by application layer protocols.

This firewall accomplishes its functional requirements by remembering all UDP packets that cross the security perimeter. If a response packet is generated and sent back to the original requester, then it is allowed through the firewall. This connection state is typically remembered for a short period of time and if no response packet is received within this time period, the association is invalidated. *See also* packet filter.

dynamic stack

Within Cisco Centri Firewall, a custom network stack comprising only applicable kernel proxies is dynamically constructed for each session. *See also* Kernel Proxy.

encapsulation

The process by which each layer in a network stack adds control information to an outgoing datagram (such as destination address, routing controls, and checksum) to ensure proper delivery. This control information is called a *header* and/or a *trailer* because it is placed in front of or behind the data to be transmitted. Each layer treats all of the information that it receives from the layer above it as data, and it places its own header and/or trailer around that information.

These wrapped messages are then passed into the layer below along with additional control information, some of which may be forwarded or derived from the higher layer. By the time a message exits the system on a physical link (such as a wire), the original message is enveloped in multiple, nested wrappers—one for each layer of protocol through which the data passed. *See also* decapsulation.

encryption
The transformation of a message into another type of message, using a mathematical function and an encryption password, called a key. The purpose of encryption is to make information indecipherable to protect it from unauthorized viewing or use, especially during transmission or when it is stored on a transportable magnetic medium.

Ethernet
A 10-megabit-per-second standard for local area networks (LANs) initially developed by Xerox. All hosts are connected by coaxial cable where they contend for network access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) paradigm.

File Transfer Protocol
See FTP.

fast Ethernet
A 100-megabit-per-second standard for local area networks.

firewall
A security system consisting of several components. Two components are filters and gateways. “Filters” block transmission of certain classes of traffic. A “gateway” is a machine or set of machines that provides relay services to compensate for the effects of the filters. A firewall may have one or more gateways.

firewall server
The *firewall server* is the actual computer on which the firewall software is running.

fixed agent
Fixed agents execute on a particular computer. For example, agents that are tightly integrated with a product instance are fixed to the same computer that is executing the product instance.

FTP
File Transfer Protocol. A protocol that allows a user on one host to access and transfer files to and from another host over a network.

gateway

A *gateway* is a protocol converter between two peer network layers. Also commonly misused as a synonym for *firewall*.

handshake

A *handshake* is the exchange of control information during the session setup. A *connectionless protocol*, such as UDP, does not exchange control information (called a *handshake*) to establish an end-to-end connection before transmitting data. In contrast, a *connection-oriented protocol*, such as TCP, exchanges control information with the remote peer network layer to verify that it is ready to receive data before sending it. When the handshaking is successful, the peer network layers are said to have established a *connection*.

header

Information attached to the beginning of a datagram. Headers usually contain information about the following data to aid in processing it.

hierarchical administrative model

Within this administrative model, each higher-level node assumes the privileges and administrative authority of all lower-level nodes. This model allows for the "inheritance" of privileges as you move toward the top of the administrative domain.

From most perspectives, this model is the easiest to administer. It degenerates nicely into an administrative policy where one user is allowed to perform all administrative actions. If additional administrators are defined, they adopt limited roles within the administrative domain.

Within this model, an implicit list of privileges exists for each node. Any privileges that are associated with a particular node in the tree are implicitly associated with any higher-level nodes within the direct path of that node.

hijacking tool

Once an intruder has root access on a system, they can use a tool to dynamically modify the kernel. This modification allows them to hijack existing terminal and login connections for any user on the system.

In taking over system connections, an intruder can by-pass one-time passwords and other strong authentication schemes by tapping the connection after the authentication is complete. For example, a legitimate user connects to a remote site through a login or terminal session; the intruder hijacks the connection after the user has completed the authentication to the remote location; the remote site is now compromised.

hop count

A measure of distance between two points on the Internet.

host

A *host* is network object (such as a computer or network printer) attached to a network that is addressable on that network. As a host, it has the ability to process network packets at the Internet layer. The features of routers confuse this definition because they can act as both hosts (because they are addressable network objects when you are applying new routing tables) and network devices that translate between two peer network access layers. When translating between peer network access layers, routers do not process the network packets at the Internet layer. However, when you are configuring the routers, they act as hosts processing IP-based protocols (such as RIP) so that they can maintain information stored in their routing tables.

host ID

The portion of the IP address that identifies a computer within a particular network ID. *See also* IP address and network ID.

host-based firewall

A firewall where the security is implemented in software running on a general-purpose computer of some sort. Security in host-based firewalls is generally at the application level, rather than at a network level.

HTTP

Hypertext Transfer Protocol. The communication protocol used for transmitting data between servers and clients (browsers) on the World Wide Web. It also has variants, such as Secure HyperText Transfer Protocol (SHTTP) and one based on the Secure Sockets Layer (SLL) where URLs are addressed HTTPS.

HyperText Transfer Protocol
See HTTP.

ICMP
Internet Control Message Protocol. A network protocol that handles network errors and error messages. The **ping** command uses ICMP.

IETF
Internet Engineering Task Force. A loosely associated collection of individuals and organizations who are the protocol engineering and development arm of the Internet. It publishes specifications on Internet protocols, such as TCP/IP, using specifications and RFC (Request for Comment) documents.

Internet
A wide area network originally funded by the Department of Defense, which uses TCP/IP for data interchange. The term *Internet* is used to refer to any and all of ARPANET, DARPANET, DDN, or DoD Internets.

internetwork
A group of networks connected by routers.

IP
Internet Protocol. The network layer for the TCP/IP protocol suite. It is a connectionless, packet-switching protocol that allows host-to-host datagram delivery.

IP address
A unique number that identifies each node on a network and to specify routing information. Each node must be assigned a unique IP address. The address is made up of two distinct parts: a network ID, which identifies the network; and a host ID, which is typically assigned by the administrator. These addresses are typically represented in dotted-decimal notation, such as 138.58.11.27.

IP network
A unique number that identifies each IP network. IP network numbers are generalizations of IP addresses. *See also* net number.

IP packets

Packets of data forming the foundation of the TCP/IP protocol suite. Each packet contains a 32-bit source and destination address, option bits, a header checksum, and data.

IP spoofing protection

IP spoofing protection is a firewall feature that verifies that the source address of a network packet that originates on an untrusted network does not match a valid address or range of addresses that are reserved for a trusted network. It also verifies that trusted addresses do not match untrusted addresses or addresses of other trusted networks. However, IP spoofing protection does not prevent IP spoofing on the same network. In addition, it does not prevent other forms of packet spoofing, such as modifying user data.

IP spoofing

To gain access, intruders create packets with spoofed source IP addresses. This attack exploits applications that use authentication based on IP addresses and leads to unauthorized user and possibly root access on the targeted system. It is possible to route packets through filtering-router firewalls if they are not configured to filter incoming packets whose source address is in the local domain. It is important to note that the described attack is possible even if no reply packets can reach the attacker. Examples of configurations that are potentially vulnerable include the following:

— routers to external networks that support multiple interfaces

— routers with two interfaces that support subnets on the internal network

— proxy firewalls where the proxy applications use the source IP address for authentication

See also hijacking tool.

kernel mode

The privileged processor mode in which Windows NT system code runs. A thread running in kernel mode has access to system memory and to hardware. *Compare* user mode.

Kernel Proxy

Kernel Proxy is a fifth generation firewall architecture that provides modular, kernel-based, multi-layer session evaluation and runs in the Windows NT Executive, which is the kernel mode of Windows NT.

To perform its function of inspecting the actual network packets and enforcing security policies, this architecture uses dynamic, custom TCP/IP-based stacks. These stacks are session dependent, which means that they are constructed on-the-fly when a new session request arrives at the firewall. Unlike normal TCP/IP stacks, these stacks are constructed out of kernel-level proxies.

These custom stacks comprise only those protocol proxies that are relevant to the session for which they were built, which allows customization of the level of stringency used to evaluate all packets belonging to a single network session.

The Kernel Proxy technology performs security checks in the kernel as the data is passing up or down the network stack. These in-line inspections increase performance and prevent the possibility of passing invalid network packets up the network stack into application space.

The dynamic stacks that comprise the kernel proxies makes it possible to examine and modify each network packet at every layer as the packet travels up the custom network stack, obviating the need to pass the packet from kernel to application space and back again.

As a network packet passes through each proxy layer, the packet is evaluated to ensure that both it and its data are valid. If a packet fails to pass the evaluation of any proxy layer, it is dropped without propagating through the remainder of the stack.

Cisco Centri Firewall's separate dynamic stacks are positioned between the native Windows NT TCP/IP stack and the device driver layer that provides access to all installed network adapter cards.

LAN

Local area network.

local communications bus (LCB)
Within Cisco Centri Firewall, a secure application-layer communications channel used to quickly and efficiently exchange system data among application-layer agents of the security system.

local communications channel (LCC)
Within Cisco Centri Firewall, a secure kernel-layer communications channel used to quickly and efficiently exchange system data between kernel-layer agents and application-layer agents of the security system.

MAC address
A unique 49-bit number assigned to the network interface card (NIC) by the manufacturer. MAC addresses, which are physical addresses, are used for mapping in TCP/IP network communications. *See also* media access control and ARP.

media access control (MAC)
MAC is a layer in the network architecture that deals with network access and collision detection.

mobile agent
A free agent that can execute on any computer that matches its resource and security requirements.

NDIS
See network device interface specification.

network device interface specification (NDIS)
In Windows networking, the Microsoft/3Com specification for the interface of network device drivers. All transport drivers call the NDIS interface to access network adapter cards. All network drivers and protocol drivers that are shipped with Windows NT Workstation and Windows NT Server conform to NDIS.

network number
A number that InterNIC assigns to your network. The net number forms the first part of a host's IP address. Also referred to as a registered IP address.

network mask
A number used by software applications to separate additional network information (called the “subnet”) from the host part of an IP address. The network mask is also referred to as a subnet mask or netmask.

Netscape Navigator
A graphical interface and HTTP client used to access sites, or servers, on the World Wide Web.

network
A *network* is a group of two or more network objects connected to each other by a cable, over telephone lines, or through wireless communication.

network adapter
A physical adapter that allows a host to use network services.

network adapter card
A physical piece of hardware that is installed in a computer and allows that computer to connect to a network via a physical wire or dialup connection. For the purposes of the Cisco Centri Firewall, network adapter cards include Ethernet cards, modems, Token Ring cards, etc.

network administrator
The person in charge of operations on either a wide area network or local area network. The duties of a network administrator (also called a system administrator) can be broad and might include such tasks as installing new workstations and other devices, adding and removing authorized users, archiving files, overseeing passwords and other security measures, monitoring usage of shared resources, and handling multifunctioning equipment.

network application
A program that is primary to the network. It was designed specifically for the network, such as FTP. Within Cisco Centri Firewall, network applications are constructed using other networked applications and/or network services that define the services required to support a specific networked application. They serve as usable wrappers for a collection of services and network applications that collectively define the services required for a specific user application.

network ID
The portion of the IP address that identifies a group of computers and devices located along the same logical network.

network interface
A combination of the hardware and software that is required to communicate across a physical network medium.

network object
A *network object* is an entity on a network that is addressable via an IP address, an IP address and subnet mask, or a hostname. An address is similar to phone numbers for people on the global telephone network. If you dial a phone number, you can contact the person to whom that number belongs. Likewise, a network object can be contacted using its address.

network packet
A *network packet* is the fundamental unit of communication on the network. It is a transmission unit of fixed maximum size that consists of binary information representing both data and a header containing an ID number, source and destination addresses, and error-control data.

network packet header
The part of a network packet that contains an identification number, source and destination addresses, and sometimes, error control data. *See also* network packet, decapsulation, and encapsulation.

network protocol
Sets of rules that explain how software and hardware should interact within a network to transmit information.

network security perimeter
A typical network security perimeter includes a collection of trusted networks, or intranetworks, and a collection of perimeter networks, or De-Militarized Zones (DMZs). Any networks that are not classified as trusted or perimeter networks should be classified as either untrusted networks or unknown networks (a term used to indicate remaining networks on the Internet).

network security policy

A *network security policy* focuses on controlling the network traffic and usage. It identifies a network's resources and threats, defines network use and responsibilities, and details action plans for when the security policy is violated. When you deploy a network security policy, you want to strategically enforce them at defensible boundaries within your network. These strategic boundaries are called *perimeter networks*.

network security stance

A network security stance is a high-level statement on the security policies and procedures that are enforced for a network of systems.

network service

Most often, a *network service* defines the particular properties of a network protocol and port mappings that satisfies the requirements of a specific service, such as Domain Name Server TCP Service, which is well defined at port 53 on TCP. Within Cisco Centri Firewall, a network service is a descriptive wrapper for the actual configuration details of a protocol-to-port mapping.

network session

A complete communication exchange between two network objects. *See also* session.

NT executive

The portion of the Windows NT operating system that run in kernel mode. It provides process structure, interprocess communication, memory management, object management, thread scheduling, intercept processing, I/O capabilities, networking, and object security.

NT kernel

The component of the NT executive that manages the processor. It performs thread scheduling and dispatching, interrupt and exception handling, and multiprocessor synchronization and provides primitive objects that the NT executive uses to create user-mode objects.

OBDC

See Open Database Connectivity.

object
A single runtime instance of an NT-defined object type. It contains data that can be manipulated only by using a set of services provided for the objects of its type.

octet
In programming, an octet refers to eight bits or one byte. For example, IP addresses are typically represented in dotted-decimal notation, where the decimal value of each octet of the address is separated by a period. *See also* IP address.

Open Database Connectivity (OBDC)
A standard method of sharing data between databases and other programs. ODBC drivers use the standard Structured Query Language (SQL) to store data in sources outside of Cisco Centri Firewall's Security Knowledge Base. Cisco Centri Firewall supports any ODBC 2.0 compliant drivers for popular database formats.

operating system
Software that controls the input and output and that loads and runs other programs.

packet
See network packet.

packet filter firewall
A *packet filter firewall* is a first-generation firewall technology that analyzes network traffic at the transport protocol layer. Each IP network packet is examined to see if it matches one of a set of rules defining which data flows are allowed. These rules identify whether communication is allowed based upon information contained within the internet and transport layer headers and the direction that the packet is headed (internal to external network or vice-versa).

If a matching rule is found, and if the rule permits the packet, then the firewall allows the packet through, from one network to another. If a matching rule denies the packet, then the packet is dropped. If there is no matching rule, then the packet is dropped.

packet spoofing protection

Packet spoofing protection is a firewall feature that prevents an attack scenario whereby an intruder modifies some portion of a network packet. Network packets may be modified at any layer in the Internet reference model.

perimeter network

A *perimeter network* is a network added between a protected, trusted network and an external, untrusted network in order to provide an additional layer of security (defense in depth).

policy inheritance

Policy inheritance refers to Cisco Centri Firewall's ability to use recursive lists of security policies. If a policy on a lower node of a tree has the action Use Next Policy applied to a condition branch, then the next policy up and in the direct path of that node is applied. This ability is transferred all the way up to the Trusted Network, Logical Network, or Internet node if the policies below those nodes use the Use Next Policy action. Dominance is an attribute of the lowest node to which a security policy is applied. If the parameters of a session request match two security policies within a direct path, the one applied to the lowest node in that path is applied to that session.

primary domain controller (PDC)

In a Windows NT Server domain, the computer running Windows NT Server that authenticates domain logons and maintains the directory database for a domain. The PDC tracks changes made to accounts of all computers on a domain. It is the only computer to receive these changes directly. A domain has only one PDC. *See also* directory database and backup domain controller.

proxy

An entity that has the authority to act for another. *See also* proxy client and proxy server.

proxy client

A *proxy client* is part of a user application that talks to the real server on the external network on behalf of the real client. When a real client requests a service, the proxy server evaluates that request against the policy rules defined for that proxy and determines whether to approve it. If it approves the request, the proxy server forwards that request to the proxy client. The proxy client then

contacts the real server on behalf of the client (thus the term “proxy”) and proceeds to relay requests from the proxy server to the real server and to relay responses from the real server to the proxy server. Likewise, the proxy server relays requests and responses between the proxy client and the real client.

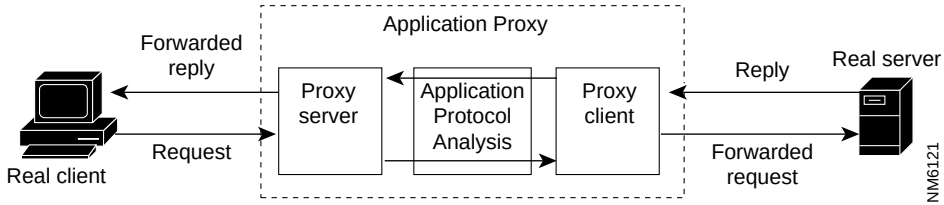
proxy server

A *proxy server* acts as the end server for all connection requests originated on a trusted network by a real client. That is, all communication between internal users and the Internet passes through the proxy server rather than allowing users to communicate directly with other users and servers on the Internet. An internal user, or client, sends a request to the proxy server for connecting to an external service, such as FTP or Telnet. The proxy server evaluates the request and decides to permit or deny the request based on a set of rules that are managed for the individual network service. Proxy servers understand the protocol of the service that they are evaluating, and therefore, they only allow those packets through that comply with the protocol definitions. They also enable additional benefits, such as detailed logging of session information and user authentication.

proxy service

A *proxy service* is a software program that connects a user to a remote destination through an intermediary gateway. They are special-purpose programs that manage traffic through a firewall for a specific service, such as HTTP or FTP, that is able to enforce security as well as provide valuable services such as logging. Proxy services tend to be specific to the protocol they are designed to forward, and they can provide increased access control, careful checks for valid data, and generate audit event records about the traffic that they transfer (see Figure C-3). In addition, proxy services tend to offer certain common features such as authentication, data caching, and application layer protocol validation.

Figure C-3 Proxy Service



Each proxy service requires two components that are typically implemented as a single executable: a proxy server and a proxy client. *See also* proxy server and proxy client.

Remote Access Service (RAS)

A service that provides remote networking for telecommuters, mobile workers, and system administrators who monitor and manage servers at multiple branch offices. Users with RAS on a Windows NT computer can dial in to remotely access their networks for services, such as file and printer sharing, e-mail, scheduling, and SQL database access.

reusable passwords

The simplest form of authentication. It requires the user to enter a text string that only he or she knows. Every time a user needs to authenticate himself, he enters the same password. However, reusable passwords are vulnerable to packet sniffers and common password attacks. Therefore, reusable passwords are not considered a reliable authentication mechanism. For this reason, we do not recommend that you use reusable passwords, and we strongly recommend that you do not use reusable passwords to gain access from untrusted networks or for the firewall administrator account.

RFC

Request for Comments. The naming convention for specifications produced by the IETF that are made publicly available for comments.

router-based firewall

A firewall where the security is implemented using screening routers as the primary means of protecting the network.

router

A router helps LANs and WANs achieve interoperability and connectivity and can link LANs that have different network topologies, such as Ethernet and Token Ring. Routers match network packet headers to a LAN segment and chose the best path for the network packet, optimizing network performance. *See also* bridge, network packet, and routing.

routing

The process of forwarding packets to other routers until the packet is eventually delivered to a router connected to the specified destination. *See also* network packet and router.

S/Key

An authentication method that uses a one-time password system developed at Bellcore. Under this system, the user generates a set of passwords based on a "seed" word or phase. When the firewall server prompts the user for authentication information, it provides a challenge based on the result of an algorithm applied iteratively to the seed value. The user must enter the password appropriate for that challenge. While S/Key is able to validate the user's current response, it has no way of predicting the user's next response. Each time users attempt to log in, they are prompted for a different password.

screened subnet

A firewall architecture in which a "sand box" or "demilitarized zone" network is set up between the protected network and the Internet, with traffic between the protected network and the Internet blocked. Conceptually, a subnet is similar to a dual-homed gateway, except for the fact that an entire network, rather than a single host, is reachable from the outside.

screening router

A router that is used to implement part of the security of a firewall by configuring it to selectively permit or deny traffic at a network level.

SecureNetKey (SNK)

An authentication method that uses a random challenge password to authenticate users. When a user attempts to log in, the firewall server provides a random challenge. The user enters his personal identification number and the challenge into a software-based calculator on his computer. The calculator

encrypts the challenge and, using a special cipher and encryption key, determines and displays the encrypted result. The user then submits this result to the authentication service as his response to the challenge. Packet sniffers cannot gain access to your network because any password they may have been able to steal is not reusable. And since neither the user's personal identification number nor the encryption key pass over the Internet, SNK is relatively safe from common password attacks.

Security Knowledge Base

A proprietary knowledge-based system that persistently stores configuration information, as well as audit events generated by the security system. It combines knowledge representation technology from the artificial intelligence community with object-oriented technology from the programming community to enable agents within the Cisco Centri Firewall to communicate with each other and to store information using a flexible representation.

security policy

A network security policy specifies which network objects are allowed to communicate with each other. You can specify which internal network objects can communicate with which external network objects and vice versa.

Within Cisco Centri Firewall, a security policy is represented by a decision tree. This decision tree contains conditions against which session requests are compared to determine whether a session matches the conditions defined within the policy. If the conditions match, then the action associated with a particular condition is applied to that session.

server

A system that provides services to the network. These services can include Web servers, FTP servers, Gopher servers, proxy services, NFS file system and NIS database access.

server application

A networked application that provides network services directly to a client application.

session

(Centri) A *session* is the act of two network objects communicating. It is a four step process that includes a session request, a session acceptance, communication of data, and a close request. Within Cisco Centri Firewall, sessions are created for all network service protocols. A session is similar to two people conversing on a telephone. They greet each other to indicate the beginning (hello) and end (goodbye) of a conversation. *See also* session request.

(Other) A communication between two users using TCP or UDP to make and manage the connection. TCP sessions are started with a connection request, followed by connection acceptance, and are closed by a close request. UDP sessions are started by an attempt to transmit a UDP datagram from a local UDP port to a remote UDP port and are closed implicitly when the calling application closes its handle to the UDP protocol stack.

session request

A *session request* is the initial request by a network object to begin a session with another network object. *See also* handshake.

session control

A *session control* is a particular setting or characteristic about a session that you can use to provide stricter control over what is and what is not allowed during a session and to act upon a session. Session controls are specific to a network service.

Two types of session controls exist within the Cisco Centri Firewall: run-time and static. *Run-time session controls* are those session controls that can be modified at the time the session request is received by the firewall. Run-time session controls are defined using security policies. Static session controls are those controls that are fixed for all sessions of a particular type. They are defined in the panels presented within the Services tree.

Some session controls allow you to modify the data of network packets that are part of a particular session while others allow you to determine whether or not to allow a session. Example session controls are date, time, type of service, port number, user authentication requirements, and Java and Active X filtering.

Site

Sites represent a network that is trusted, untrusted, or unknown, and they are tied to a network adapter card. Because more than one network can be assigned to a network adapter card, sites represent the relationships among networks. When a network packet arrives at the firewall server, it arrives from a particular site. The site that it arrives from determines which network security policy is applied to that packet.

Sites determine how security policies are applied, how networks are organized, and how network address translation works within the firewall server. All data passes through the firewall's central site, which is where Centri's Security Kernel resides. How a network packet travels across two sites determines which security polices are applied. It identifies the source and destination of the packet. If a network packet does not change sites, then no security policy is applied to the network packet.

SMTP

Simple Mail Transfer Protocol. Used to transfer electronic mail between computers.

strict adherence administrative model

Within this model, each node is assigned a discrete set of administrative actions and privileges, and only those users associated with that node are allowed to perform administrative actions at that level.

This model presents a more complex administrative policy to manage and implement. It requires administrative actions to be well defined, the responsibility for that administrative action to be well understood, and for different users to be associated with the various product instances.

This policy is the most secure and produces a system that isolates damage from any employee that may attack an internal system. Each individual is allowed to only perform a subset of the administrative procedures (for example, examining the reports generated by the Monitoring Subsystem).

Within this model, each node has an explicit list of actions associated with it. No actions are implicitly associated with a node—they must be explicitly defined.

subnet number
A part of the Internet address that designates a subnet. Ignored for the purpose of Internet routing, it is used for intranet routing.

system administrator
See network administrator.

task
Tasks are the ordered collection of specific actions into a meaningful relationship. Tasks signify the ordered completion of actions that must be performed to conclude a higher goal.

TCP
Transmission Control Protocol. A sequenced, bi-directional network protocol commonly used for services on the Internet such as Telnet, FTP, SMTP, NNTP and HTTP. The TCP protocol is considered reliable because transmitted data is resubmitted until its receipt is acknowledged by the receiver.

TCP/IP
Transmission Control Protocol/Internet Protocol. The suite of applications and transport protocols that runs over IP. These protocols include FTP, Telnet, SMTP, and UDP (a transport layer protocol).

Telnet
The Internet standard protocol for remote terminal connection service.

trusted network
Trusted networks are the networks inside your network security perimeter, with the exception of virtual private networks (VPNs). These networks are the ones that you are trying to protect. Often, you or someone in your organization administers the computers that compose these networks, and your organization controls their security measures.

UDP
A non-sequenced and unreliable network protocol. UDP sends and receives datagrams. UDP is at the same layer as TCP, but it does not acknowledge transmissions, and therefore, it is unreliable.

Uniform Resource Locator
A method of specifying an address for a network server on the world-wide web (WWW).

UNIX
An operating system developed by Bell Laboratories that supports multi-user and multitasking operations.

unknown network
Unknown networks are those networks that are neither trusted nor untrusted. They are unknown quantities to the firewall because you cannot explicitly tell the firewall server that this network is a trusted or an untrusted network. Unknown networks exist outside of your security perimeter. By default, all unknown networks are assumed to be untrusted networks.

untrusted network
Untrusted networks are the networks that are known to be outside your security perimeter. They are untrusted because they are outside of your control. You have no control over the administration or security policies for these sites. They are the private and shared networks from which you are trying to protect your network. However, you still need and want to communicate with these networks even though they are untrusted.

user mode
The non-privileged mode in which application code runs. A thread running in user mode can gain access to the system only by calling system services. *Compare* kernel mode.

virtual circuit
A virtual communication channel between two computers. Multiple network sessions are multiplexed across a single virtual circuit.

virtual private network (VPN)

A trusted network that transmits data across an untrusted network infrastructure. For the purposes of our discussion, the network packets that originate on a VPN are considered to originate from within your internal perimeter network. This origin is logical because of how VPNs are established. For communications that originate on a VPN, security mechanisms must exist by which the firewall server can authenticate the origin, data integrity, and other security principles contained within the network traffic according to the same security principles that you enforce on your trusted networks.

World Wide Web (WWW)

The software, protocols ,conventions, and information that enable hypertext and multimedia publishing among disparate computers.

Windows Internet Names Service (WINS)

A name resolution service that resolves Windows networking computer names to IP addresses in a routed environment. A WINS server handles name registrations, queries, and releases. *See also* IP address and routing.

Windows NT Workstation

The high-end operating system, introduced by Microsoft Corporation in 1993, that is optimized to run user applications. Along with Windows 95, Window NT Workstation acts as a client in the Windows NT client-server model. It is a portable 32-bit, preemptive multitasking operating system that features networking, symmetric multiprocessing, multithreading, and security.

Windows NT Server

A superset of the Windows NT Workstation operating system that is optimized to run server-based applications that are shared among multiple users and acts as the server in the Windows NT client-server model. It provides centralized, domain-based network management and security. It also offers advanced fault-tolerance features, such as disk mirroring, and additional connectivity.