Cisco IOS Firewall

Cisco IOS Firewall Overview

Q. What is Cisco IOS® Firewall?

A. Cisco IOS Firewall is a Common Criteria EAL4 certified stateful firewall solution integrated into Cisco IOS Software routers. By integrating with the industry's richest routing feature set with other security, voice, quality of service (QoS), and VPN capabilities, Cisco IOS Firewall provides a cost-effective and flexible firewall ideal for supporting telecommuter, small office, and enterprise branch office deployments where embedded security is desired in a distributed network topology.

Q. What are the two configuration models for Cisco IOS Firewall?

A. There are two configuration models for Cisco IOS Firewall. The traditional configuration model, Classic Firewall (formerly known as Context-Based Access Control, or CBAC), and the new configuration model, Zone-Based Policy Firewall.

Classic Firewall will continue to be maintained for the foreseeable future, but will not be significantly enhanced with new features. Instead, the strategic development direction for Cisco IOS Firewall is carried by Zone-Based Policy Firewall.

Q. What are the differences between Zone-Based Policy Firewall and Classic Firewall?

A. Zone-Based Policy Firewall introduces substantial changes to command-line interface (CLI) firewall configuration. In Classic Firewall configuration, firewall policy is applied on interfaces. In the Zone-Based Policy Firewall configuration, interfaces are assigned to security zones, and firewall policy is applied to traffic moving between the zones. For more details, refer to the following document: Conceptual Difference Between Cisco IOS Software Classic and Zone-Based Firewalls.

Q. Do all of the router platforms support the same Cisco IOS Firewall functions?

A. No. Cisco Integrated Services Routers (Cisco 800 Series Routers; Cisco 1800, 2800, and 3800 Series Integrated Services Routers), Cisco 7200 Series Routers, and the Cisco 7301 Router support both Classic Cisco IOS Firewall and Zone-Based Policy Firewall; Cisco ASR 1000 Series Aggregation Services Routers support only the Zone-Based Policy Firewall.

Q. Are all of the Cisco IOS Firewall functions available in all Cisco IOS Software release trains?

A. No. Cisco IOS Firewall capabilities are primarily available in mainline and technology (T) software release trains. The S train does not include many important performance and capability enhancements. Cisco IOS XE Software supports Zone-Based Policy Firewall on the Cisco ASR 1000 Series Aggregation Services Routers.

Zone-Based Policy Firewall

Q. What functional changes does Cisco IOS Software Zone-Based Policy Firewall offer compared to the Classic Cisco IOS Firewall?

A. The new Cisco IOS Software Zone-Based Policy Firewall offers a number of benefits:

- The Zone-Based Policy Firewall offers a default deny-all policy, similar to what ASA/PIX offers. Network services are allowed through the firewall with modular policy definitions.
- Firewall policy definition and audit are much more simple.
- Firewall policies can be configured to offer more precise control of network service access.
- Network service lists can be associated with a list of hosts and subnets to offer firewall policy configuration with object groups.
- The Zone-Based Policy Firewall is not dependent on access-control lists (ACLs) to define security policies, unlike what Classic Firewall offers.

Q. How does the Cisco IOS Software Zone-Based Policy Firewall simplify firewall policy configuration and audit?

A. Firewall policies are much clearer, as traffic encounters only one policy as it traverses from one zone to another. In the past, several inspection policies and access control lists had to be correlated to determine the policy that affected traffic flowing from one router interface to another.

Q. Which Cisco IOS Software release supports the Cisco IOS Software Zone-Based Policy Firewall?

A. Beginning with Release 12.4(6)T, Cisco Integrated Services Routers, Cisco 7200 Series Routers, and Cisco 7301 Router support the Zone-Based Policy Firewall.

Q. Does the Cisco IOS Zone-Based Policy Firewall work with stateful failover?

A. No. The Cisco IOS Zone-Based Policy Firewall does not work with stateful failover.

Classic Cisco IOS Firewall

Q. Does the Cisco IOS Firewall work on any type of router interface?

A. The Cisco IOS Firewall can be applied on any type of router interface, including LAN, WAN, sub-interfaces, generic routing encapsulation (GRE), and IP Security (IPsec) virtual tunnel interfaces.

Support for Secure Unified Communications

Q. Which voice-over-IP (VoIP) protocols are supported by the Cisco Zone-Based Policy Firewall?

A. The Zone-Based Policy Firewall supports the following VoIP protocols:

- **Session Initiation Protocol (SIP):** SIP packet inspection and pinholes opening, as well as protocol conformance and application security. For more information, consult SIP Enhancements: ALG and AIC.
- **H.323 V3 and V4:** Features such as call signaling (H.225) over User Datagram Protocol (UDP), multiple call signaling over a single TCP connection, T.38 fax over TCP, and address resolution using border elements are supported. Rate-limiting mechanism to monitor call attempt rate and call aggregation is also supported. For more information, consult H323 v3/v4 Support.
- **Skinny Client Control Protocol (SCCP):** This includes inspection of skinny control packets exchanged between a skinny client and the CallManager as well as skinny traffic that is either generated by or destined to the router. For more information, consult Support for Skinny Local Traffic and CME.

Q. What is Cisco Unified Communications Trusted Firewall Control?

A. Cisco Unified Communications Trusted Firewall Control is a feature in Cisco IOS Firewall and Cisco IOS Software call control to tackle the following three commonly seen scenarios when voice protocols traverse the Cisco IOS Firewall:

- The Cisco IOS Firewall uses an Application Layer Gateway (ALG) to inspect voice protocols to open "pinholes" to allow media flows. When a newer version of the voice protocols is released, the Cisco IOS Firewall needs to update the ALG to conform to the protocol changes. Frequent voice protocol changes mean frequent updates to the ALG.
- The call signaling and media take different paths and do not traverse the same Cisco IOS Firewall. Hence the media flows for that call cannot traverse the Cisco IOS Firewall.
- The call signaling is encrypted and the Cisco IOS Firewall cannot determine the "pinholes" needed to be opened to allow the call.

Starting with Release 12.4(22)T, Cisco IOS Firewall incorporates Cisco Unified Communications Trusted Firewall, a feature that allows Cisco IOS Firewall to inspect, authenticate and authorize voice calls regardless which voice protocol version is in use; this essentially makes the Cisco IOS Firewall voice protocol inspection version independent, while maintaining highly secure encrypted signaling paths as well as asymmetric signaling and media paths.

Q. What is Trust Relay Point (TRP), and how does it relate to Cisco Unified Communications Trusted Firewall?

A. TRP is a Cisco IOS software function that provides multiple voice capabilities, and one of them is trusted firewall traversal. TRP eliminates the duplication of signaling intelligence: the deep packet inspection and the overhead associated with firewall inspection by signaling the firewall what traffic to permit.

The Cisco IOS Firewall enhances security for Unified Communications by establishing a trust relationship with Trust Relay Point (TRP). This is called Cisco Unified Communications Trusted Firewall.

With Trusted Firewall, firewall traversal for voice protocols is accomplished using STUN (Session Traversal Utilities for NAT) message from TRP to authenticate and authorize the voice calls. TRP communicates with the Cisco IOS Firewall and lets the firewall know what IP address and ports to open pinholes for and when to close them.

Q. How does Cisco Unified Communications Trusted Firewall Control work?

A.

1. A shared secret key is configured on the TRP (Trust Relay Point) as well as Cisco IOS Firewall and the key is used to generate a secure token.
2. A phone calls another phone across a Cisco IOS Firewall with the Trusted Firewall feature turned on.
3. The Cisco IOS Firewall uses partial ALG inspection to validate the signaling packets.
4. Cisco Unified CallManager or Cisco Unified CallManager Express receives the call signaling packets and knows that this call is TRP enabled.
5. Cisco Unified CallManager or Cisco Unified CallManager Express inserts TRP into the media path to make sure that the media flows through the TRP.
6. TRP generates the STUN (Session Traversal Utilities for NAT) message containing a highly secure token, the IP address, and port information for the media flow.

7. Trusted Firewall receives the STUN message, authenticates and authorizes the message based on the token (generated with the shared secret) to help ensure that it opens pinholes only for trusted TRP request.
8. The Trusted Firewall then opens a pinhole dynamically for the media flow based on the IP address and port information in the STUN message, and then the media path is established.
9. A STUN keep-alive is used to maintain the call session and prevent replay attacks.
10. Once the call is ended, Trusted Firewall will not receive any keep-alive messages from TRP, and then it will close the pinholes and the firewall session associated with this call.

Q. What are the other benefits of Cisco Unified Communications Trusted Firewall?

A. Besides keeping the unauthorized flows out, the Cisco Unified Communications Trusted Firewall also supports asymmetrical flows, where media and signaling packets do not follow the same path through the network. Trusted Firewall also supports encrypted Unified Communications signaling traffic, as it does not rely on finding the media information in the signaling flow. Trusted Firewall is also voice protocol version independent for firewall inspection.

Q. What keeps an attacker from faking a STUN packet to get the Cisco IOS Software Trusted Firewall to permit "bad" traffic?

A. The STUN message sent by the TRP is signed by a token generated with a shared secret, timestamp, length of message, and other parameters. The Cisco IOS Software Trusted Firewall only honors the STUN message after it has verified the token.

Support for Instant Messaging and Peer-to-Peer Applications

Q. Which instant messaging applications does the Cisco IOS Firewall support?

A. Cisco IOS Firewall Application Inspection Control (AIC) supports MSN Messenger, AOL Instant Messenger, Yahoo! Messenger, and ICQ.

Q. Are Cisco IOS Firewall's only options for instant messaging traffic control to block or allow traffic?

A. No, Cisco IOS Firewall AIC offers capability to limit instant messaging traffic to text-chat only, blocking other service-specific capabilities such as file transfer, and voice and video chat.

Q. Which peer-to-peer protocols does Cisco IOS Firewall support?

A. Cisco IOS Firewall AIC supports Gnutella, eDonkey, BitTorrent, KaZaA, Direct Connect, FastTrack, and WinMX.

Q. Are Cisco IOS Firewall's only options for peer-to-peer traffic control to block or allow traffic?

A. No, Cisco IOS Firewall AIC offers capabilities to limit peer-to-peer traffic to certain service-specific capabilities. Consult the "Zone-Based Policy Firewall Design and Application Guide" in the white paper section of http://www.cisco.com/go/iosfw.

Management

Q. What management tools are available to support the Zone-Based Policy Firewall?

A. Besides using the CLI, the GUI-based configuration tool Cisco Configuration Professional (CCP) or Security Device Manager (SDM, which is replaced by CCP) supports the zone-based configuration model. The network-based management tool Cisco Security Manager (CSM) will support the zone-based configuration model in the second half of 2009.

Q. What logging features are included with Cisco IOS Firewall?

A. Enhanced audit trail features use syslog mechanisms to track transaction-session termination time stamps, source host, destination host, ports used, and the total number of transmitted bytes. Real-time alerts send syslog notifications to central management consoles upon detection of suspicious activity. This setup gives network managers the ability to respond immediately to intrusions.

PCI Compliance

Q. How does Cisco IOS Firewall protect stored cardholder data?

A. Using the Cisco IOS Software Zone-Based Policy Firewall can facilitate deploying security for internal, external, and DMZ subnets on the network to prevent unauthorized access of cardholder data.

Q. How does Cisco IOS Firewall help me address PCI Data Security Standard (DSS) requirements?

A. The Cisco IOS Firewall is a full-featured firewall. It meets requirement number one, which states that organizations must install and maintain a firewall configuration to protect data.

Q. How do I know if my network is protecting cardholder data and if it is ever compromised?

A. The Cisco IOS Firewall addresses requirement number 10, which deals with alerts and monitoring using Cisco IOS Firewall's stateful traffic inspection and event syslog recording.

Q. What platforms does the Cisco IOS Firewall support?

A.

Product	Platforms Supported
Cisco 800 Series Routers	Cisco 831*, 836*, 837*, 851, 857, 860, 871, 876, 877, 878, 881, 888 and 891
Cisco 1700* Series Modular Access Routers	Cisco 1701, 1702, 1711, 1712, 1721, 1751, 1751-V, and 1760
Cisco 1800 Series Integrated Services Routers	Cisco 1801, 1802, 1803, 1811, 1812, 1841 and 1861
Cisco 1900 Series Integrated Services Routers	Cisco 1941 and 1941W
Cisco 2600* Series Multiservice Platforms	Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and 2691
Cisco 2800 Series Integrated Services Routers	Cisco 2801, 2811, 2821, and 2851
Cisco 2900 Series Integrated Services Routers	Cisco 2901, 2911, 2921, and 2951
Cisco 3600* Series Multiservice Platforms	Cisco 3660
Cisco 3700* Series Multiservice Access Routers	Cisco 3725 and 3745
Cisco 3800 Series Integrated Services Routers	Cisco 3825 and 3845
Cisco 3900 Series Integrated Service Routers	Cisco 3925 and 3945
Cisco 7200 Series Routers	Cisco 7201, 7204VXR, and 7206VXR
Cisco 7300 Series Routers	Cisco 7301
Cisco ASR 1000 Series Aggregation Services Routers	Cisco ASR 1001, 1001-X, 1002, 1002-X, 1004, 1006 and 1013

Q. How much memory does Cisco IOS Firewall use?

A. Cisco IOS Firewall consumes roughly 700 bytes per connection for basic inspection. More detailed application inspection will consume more memory: for example, FTP, HTTP and VoIP AIC.

Port-to-Application Mapping

Q. Can Cisco IOS Firewall inspect applications on ports other than those set as default ports?

A. Yes. Granular Protocol Inspection (Cisco IOS Software Release 12.3(14)T) introduced interoperability between Port to Application Mapping (PAM) and Cisco IOS Firewall. This includes support for a much larger list of protocols than was originally offered in the Cisco IOS Firewall and offers support for user-specified port numbers.

Q. What does PAM do?

A. PAM enables the Cisco IOS Firewall to support applications that run on nonstandard TCP or UDP ports: that is, ports different from the registered or well-known ports associated with an application. Using PAM, network administrators can customize access control for specific applications and services to meet the distinct needs of their networks.

PAM uses the port information to establish a table of default port-to-application mapping information at the Cisco IOS Firewall. The PAM table initially is populated with system-defined mapping information when the Cisco IOS Firewall router first starts. As mapping information is customized, the PAM table is modified with new mapping information. The information in the PAM table enables the Cisco IOS Firewall supported services to run on nonstandard ports.

PAM also supports host-specific or subnet-specific port mapping, which allows PAM to be applied to a single host or subnet using ACLs. Host or subnet specific port mapping is done using standard ACLs.

Q. When is PAM used?

A. To apply nonstandard port numbers for a service or application:

- When a specific host or subnet uses a port number for an application that is different than the default port number established in the PAM table.
- When different hosts use the same port number for different applications.

Q. What limitations exist with PAM?

A. PAM can only recognize applications based on default and configured protocol and port numbers. PAM cannot recognize applications that use dynamic destination ports.

Authentication Proxy

Q. What protocols are available for Authentication Proxy to authenticate users?

A. Authentication Proxy can employ HTTP and HTTPS for web GUI-based authentication; FTP and Telnet are available for CLI authentication.

Q. How does the Authentication Proxy feature benefit users behind a Cisco router equipped with Cisco IOS Firewall?

A. The Authentication Proxy capability in Cisco IOS Firewall provides dynamic, per-user authentication and authorization for network users. Previously, if user identity and related authorized access were not determined by the user's IP address, then the security policy had to be applied to a user group or subnet. With the addition of Authentication Proxy, per-user policy can be downloaded dynamically to the router from the TACACS+ or RADIUS authentication server.

Q. Does Authentication Proxy function when the targeted web server is the router on which the proxy is running?

A. No. Authentication Proxy does not intercept packets that are destined to the router. Router-targeted HTTP packets are typically authenticated as specified by the router login configuration or the “ip http server authentication” method configuration.

Q. Can Authentication Proxy be used for specific users or subnets?

A. Yes. Standard ACLs can be used to specify which networks or hosts need to authenticate before a specific user profile is applied at the Cisco IOS Firewall.

Q. Can Authentication Proxy be triggered by HTTP if it is configured to run on a nonstandard port?

A. No. Authentication Proxy intercepts only HTTP traffic destined for port 80.

Miscellaneous

Q. Does Cisco IOS Firewall support Oracle's application proxy, SQLNet?

A. Yes. SQLNet is a multichannel protocol with the client and the server. From a quick look, the interactions are as follows:

- Client connects to the TNS listener on port 1521 (TCP).
- We look for the REDIRECT message and extract the following.
  - host ip: ip addr of the server
  - protocol (tcp/udp)
  - port: port that the server will use
  - client ip, (client port range) ----> host ip extracted, port, protocol
- This requires more a detailed understanding of application activity. The port is opened from client to a host IP rather than the destination IP address. This indicates that the destination (TNS listener) and the Oracle server could be on different machines.

Q. Does Cisco IOS Firewall support Point-to-Point Tunneling Protocol (PPTP)?

A. The following configuration must be completed to support PPTP:
(PPTP Client) ======== [firewall] ========= (PPTP Server)

- Allow for TCP port 1723 from the PPTP client to the PPTP server.
- Allow for IP protocol 47 (GRE) from the PPTP client to the PPTP server.

Q. Can the Cisco IOS Firewall and TCP Intercept be enabled at the same time?

A. No. TCP Intercept and Cisco IOS Firewall (the zone-based firewall or Context-Based Access Control (CBAC)) are incompatible features. Configuring TCP intercept along with NAT and/or IOS Firewall is not supported.

Q. Does the Cisco IOS Firewall work in environments with asymmetric routing?

A. No. Asymmetric routing is not supported on the Cisco IOS Firewall. Refer to the link http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5710/ps1018/white_paper_using_cisco_ios_zone_based_classic_fw.html for more information.

Q. Can rate limiting be applied for Cisco IOS Firewall policies?

A. Yes. The Cisco IOS Firewall provides the ability to control the bandwidth that is used by an application or a set of traffic through the firewall. This serves as a limiting factor to DoS attacks by preventing excessive bandwidth from being consumed by the packets from the DoS attack.

Please note this Q&A guide is to inform you mostly asked questions regarding Cisco IOS Firewall. This list of Q&A is intended to provide a general idea of the supported applications, protocols and usage scenario that is needed to use and troubleshoot Cisco IOS Firewall. For specific Cisco platform performance and scalability concerns please contact a Cisco representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C67-607150-01 09/14