Cisco IOS Firewall Support for Skinny Local Traffic and CME

Last Updated: January 20, 2012

The Cisco IOS Firewall Support for Skinny Local Traffic and CME feature enhances the Context-Based Access Control (CBAC) functionality to support Skinny traffic that is either generated by or destined to the router. When Cisco Call Manager Express (CME) is enabled on the Cisco IOS firewall router, the CME manages both VoIP and analog phones using Skinny Client Control Protocol (SCCP) over either an intranet or the Internet with flow-around and flow-through modes of CME.

In addition,the Firewall Support of Skinny Client Control Protocol feature extends the support of SCCP to accommodate video channels.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Cisco IOS Firewall Support for Skinny Local Traffic and CME

The Skinny inspection module is part of the inspection subsystem; thus, your router must be running an image that has firewall support.

Restrictions for Cisco IOS Firewall Support for Skinny Local Traffic and CME

This feature has the following restrictions:

- Skinny inspection will inspect only the SCCP sessions that have been established after the firewall is configured with Skinny inspection. That is, any SCCP sessions that were established through the firewall before the Skinny inspection was configured will not be inspected.
- This feature does not support Music on Hold (MOH) when a device other than the Call Manager (CM) is the music server. (This feature does support MOH when the CM is the music server.)
- This feature does not address either the multicast functionality of SCCP or the functionality of multiple active calls on a single Skinny client.

This feature does not support the following Skinny and firewall configurations.

The CM and the Skinny client cannot be on three different networks that are separated at the firewall. The firewall implementation does not inspect sessions that have devices residing on more than two distinct networks that are segregated at the firewall. That is, if more than two interfaces at the firewall, session inspection is not supported.

Information About Cisco IOS Firewall Support for Skinny Local Traffic and CME

Skinny Inspection Overview

Skinny inspection enables voice communication between two Skinny clients by using the Cisco CallManager. The Cisco CallManager uses the TCP port 200 to provide services to Skinny clients. A Skinny client connects to the primary Cisco CallManager by establishing a TCP connection and if available, connects to a secondary Cisco CallManager. After the TCP connection is established, the Skinny client registers with the primary Cisco CallManager, which will be used as the controlling Cisco CallManager until it reboots or a keepalive failure occurs. Thus, the TCP connection between the Skinny client and the Cisco CallManager exists forever and is used to establish calls coming to or from the client. If a TCP connection fails, the secondary Cisco CallManager is used. All data channels established with the initial Cisco CallManager remain active and will be closed after the call ends.

The Skinny protocol inspects the locally generated or terminated Skinny control channels and opens or closes pinholes for media channels that originate from or are destined to the firewall. Pinholes are ports that are opened through a firewall to allow an application controlled access to a protected network. The Skinny traffic that passes through and locally generated or terminated Skinny traffic is treated in the same way at the firewall.

The table below lists the set of messages that are necessary for the data sessions to open and close. Skinny inspection will examine the data sessions that are deemed for opening and closing the access list pinholes.

Table 1 Skinny Data Session Messages

Skinny Inspection Message	Description
StationCloseReceiveChannelMessage	Sent by Cisco CallManager instructing the Skinny client (on the basis of the information in this message) to close the receiving channel.
StationOpenReceiveChannelAckMessage	Contains the IP address and port information of the Skinny client sending this message. This message also contains the status of whether or not the client is willing to receive voice traffic.
StationStartMediaTransmissionMessage	Contains the IP address and port information of the remote Skinny client.
StationStopMediaTransmissionMessage	Sent by the Cisco CallManager instructing the Skinny client (on the basis of the information in this message) to stop transmitting voice traffic.
StationStopSessionTransmissionMessage	Sent by the Cisco CallManager instructing the Skinny client (on the basis of the information in this message) to end the specified session.
StationOpenMultiMediaReceiveChannelAckMessage	Contains the IP address and port information of the Skinny client sending this message. It also contains the status of whether the client is willing to receive video and data channels.
StationCloseMultiMediaReceiveChannel	Sent by the Cisco Unified Communications Manager to the Skinny endpoint to request the closing of the receiving video or data channel.
StationStartMultiMediaTransmitMessage	Sent by the Cisco Unified Communications Manager to the Skinny endpoint whenever Cisco Unified Communications Manager receives an OpenLogicalChannelAck message for the video or data channel.
StationStopMultiMediaTransmission	Sent to Skinny endpoints to request the stopping of the transmission of video or data channel.

Pregenerated Session Handling

When two phones register with the CME running on Cisco IOS firewall, two control channels terminated on the CME box. These two control channels are TCP connections and are inspected by the Firewall

Skinny module. When pinholes are opened for the media traffic, a total of four pre-gen sessions are created, two for each control session.

With the flow-through mode of operation of CME, the four pregenerated sessions are converted to two active sessions. The same number of active sessions is retained because there are two media sessions, one from each phone terminating on CME.

With the flow-around mode of operation of CME, the CME is bypassed as there is a direct connection between the two phones. In this mode, there are two possible scenarios:

- When both phones are on the same side of the CME, there is no exchange of media packets between the two phones. However, exchange of media packets is possible with pass-through traffic. In this case, the pre-gen sessions will timeout because the media traffic will not reach the router itself.
- When both phones are located on either side of the CME, the media traffic goes through the CME box. The four pre-gen sessions that are created are converted to one active session. Instead of creating four pre-gen sessions, only two pre-gen sessions are created. These two pre-gen sessions are converted to one active session when you see the media traffic.

NAT with CME and the Cisco IOS Firewall

In typical deployments, both Cisco IOS firewall and Network Address Translator (NAT) will be running on the same router. When CME is also running, typically in the case of an Integrated Services Router (ISR), some complexities and limitations exist.

- If two Skinny phones are registered to CME that is on the Cisco IOS firewall with NAT. When Phone 1 attempts to communicate with Phone 2, the IP and port (mostly private IP) of Phone 1 will be exchanged with Phone 2 over the already established TCP connection.
- If NAT is configured on the outside interface to translate all the private addresses to the router's global address. Some private addresses are exchanged over a TCP connection between the router and the remote phone. If NAT is able to translate the addresses in such flows where one endpoint is the router itself, then NAT and CME running on the same box will not cause any problems. If not, the following scenarios are possible:
- In flow-through mode of operation, the voice data channels, Real-time Transport Protocol (RTP) stream over User Datagram Protocol (UDP), from Phone 1 and Phone 2, both terminate on CME. So, there will be one RTP over UDP connection from Phone 1 to the CME and a second from Phone 2 to the CME. The CME relays the voice data over the two channels. In this case, there should not be any problem with NAT running on the CME box, as the connection is terminated on the router from Phone 2 and the address used for that connection is the global address of the router.
- In flow-around mode of operation, there is a direct connection (RTP over UDP) between Phone1 and Phone 2 for carrying voice data traffic. If NAT does not translate the private IP of Phone 1, then the voice data channel will not be established successfully because the private IP of Phone 1 is shared in the control channel. In such a scenario, the running of CME with NAT breaks down.

New Registry for Locally Generated Traffic

A new registry is created in the Skinny local media traffic path. This path differs from the regular switching path code, where all the controlling and pass-through media traffic is inspected. The Skinny module sends the locally generated traffic using the "fastsend" application program interface (API) which does not put the packet in the regular switching path, but sends it directly (to Layer 2 drivers). This new registry resets the timeouts for the media channels and also reports the number of Skinny media sessions that are established such as the output of **show** commands.

Note The above API is used to update the Firewall sessions when the media channel is active. Firewall will not attempt to protect the CME box based on the nonexistence of pregen. Therefore, the firewall will not drop media packets for which there is no pre-gen/active session. The MTP module in CME protects itself by dropping the packets that do not match the source IP and source port numbers.

How to Configure Cisco IOS Firewall Support for Skinny Local Traffic and CME

Creating a ZonePair Between a Zone and the Self Zone

To inspect the traffic that is destined to the router or the traffic originating from the router, you need to create a zonepair between a zone (containing the incoming/outgoing interface) and the self zone.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **alert** {**on** | **off**}
5. **audit-trail** {**on** | **off**}
6. **class-map type inspect** protocol-name [**match-any**| **match-all**] class-map-name
7. **policy-map type inspect** *policy-map-name*
8. **class type inspect** *class-map-name*
9. **zone security** *name*
10. **zone security** *name*
11. exit
12. **zone-pair security** *zone-pair-name* {**source** *source-zone-name*| **self}** **destination** [**self** | *destination-zone-name*]
13. **service-policy type inspect** *policy-map-name*
14. **interface** *type number*
15. **zone-member security** *zone-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect** *parameter-map-name* **Example:** `Router(config)# parameter-map type inspect insp-pmap`	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action. • Enters parameter-map type inspect configuration mode.

Step 4	**alert** {**on** | **off**}
	Example:
	`Router(config-profile)# alert on`
		(Optional) Turns on and off Cisco IOS stateful packet inspection alert messages that are displayed on the console.

Step 5	**audit-trail** {**on** | **off**}
	Example:
	`Router(config-profile)# audit-trail on`
		(Optional) Turns audit trail messages on or off.

Step 6	**class-map type inspect** protocol-name [**match-any**| **match-all**] class-map-name
	Example:
	`Router(config-profile)# class-map type inspect skinnycmap match-any protocol skinny`
		Creates a class map for the Skinny protocol so that you can enter match criteria.
		• Enters class-map configuration mode.

Step 7	**policy-map type inspect** *policy-map-name* **Example:** `Router(config-profile)# policy-map type inspect skinnypmap`	Creates a policy map so that you can enter match criteria. • Enters policy map configuration mode.

	Command or Action	Purpose
Step 8	**class type inspect** *class-map-name* **Example:** `Router(config-profile)#` **class type inspect** *skinnycmap*	Specifies the name of the class on which an action is to be performed. • The value of the *class-map-name* argument must match the appropriate class name specified via the **class-map type inspect** command.
Step 9	**zone security** *name* **Example:** `Router(config-profile)# zone security z1`	Creates a zone for phone 1. • Enters global configuration mode.
Step 10	**zone security** *name* **Example:** `Router(config-profile)# zone security z2`	Creates a zone for phone 2.
Step 11	exit **Example:** `Router(config-profile)#exit`	Exits profile configuration mode.
Step 12	**zone-pair security** *zone-pair-name* {**source** *source-zone-name*| **self}** **destination** [**self** | *destination-zone-name*] **Example:** `Router(config)# zone-pair security z1-self source z1 destination self`	Creates a zone-pair. • Enters security zone-pair configuration mode.
Step 13	**service-policy type inspect** *policy-map-name* **Example:** `Router(config-sec-zone-pair)# service-policy type inspect skinnypmap`	Attaches a firewall policy map to the destination zone-pair. • If a policy is not configured between a pair of zones, traffic is dropped by default. • Enters global configuration mode.
Step 14	**interface** *type number* **Example:** `Router(config)# interface FastEthernet4/1`	Specifies the type of interface to be configured and the port, connector, or interface card number.

	Command or Action	Purpose
Step 15	**zone-member security** *zone-name* **Example:** `Router(config-sec-zone-pair)#` **zone-member security** *z1*	Specifies the name of the security zone to which an interface is attached.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Firewall support of SCCP	"Firewall Support of Skinny Client Control Protocol (SCCP)" chapter in th e *Cisco IOS Security Configuration Guide*
Firewall commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco IOS Firewall Support for Skinny Local Traffic and CME

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 Feature Information for Cisco IOS Firewall Support for Skinny Local Traffic and CME

Feature Name	Releases	Feature Information
IOS Firewall Support for Skinny Local Traffic and CME	12.4(20)T	The Cisco IOS Firewall Support for Skinny Local Traffic and CME feature enhances the Context-Based Access Control (CBAC) functionality to support ‘router generated/destined to router’ Skinny traffic. When CME is enabled on the IOS firewall router, it manages both VoIP and analog phones using Skinny Client Control Protocol (SCCP) over intranet or internet with flow-around and flow-through modes of CME. The following commands were introduced or modified: **class-map type inspect, class type inspect, interface, parameter-map type inspect, policy-map type inspect, service-policy type inspect, zone-member security, zone-pair security.**
IOS Zone-Based Firewall SCCP Video Support	15.1(2)T	The IOS Zone-Based Firewall SCCP Video Support (SCCP) feature extends support to accommodate video channels.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.