Cisco Unified Communications Trusted Firewall Control - Version III

First Published: July 20, 2010

Cisco Unified Communications Trusted Firewall Control pushes intelligent services onto the network through a Trusted Relay Point (TRP) firewall. TRP is a Cisco IOS service feature, which is similar to the Resource Reservation Protocol (RSVP) agent. Firewall traversal is accomplished using Session Traversal Utilities for Network Adress Translation (STUN) on a TRP colocated with a Cisco Unified Communications Manager Express (Cisco Unified CME), Cisco Unified Border Element, and Media Termination Points (MTP).

This release supports the following:

- Session Initiation Protocol (SIP) session timer fully in the following Call Control Agents:
  - Time-division Multiplexing(TDM)-SIP Gateway
  - Cisco Unified CME for SIP trunk
  - Cisco Unified Border Element for both SIP to SIP and H.323 to SIP scenarios
- Unified Communication Trusted Firewall traversal for Cisco Unified CME SCCP line side and in CME as Survivable Remote Site Telephony (SRST) mode.
- Unified Communication Trusted Firewall traversal for Cisco Unified CME SIP line side and in CME as SRST mode.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Enhanced Firewall Traversal Cisco Unified CME" section on page 25.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://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

Contents

- Information About Enhanced Firewall Traversal for Cisco Unified Communications using STUN, page 3
- How to Configure Firewall Traversal for Cisco Unified CME SIP Line Side Endpoints, page 6
- Configuration Examples for Cisco Unified CME SIP Line Side EndPoints, page 7
- How to Configure Firewall Traversal for Cisco Unified CME SCCP Line Side Endpoints, page 11
- Configuring Firewall Traversal for Cisco Unified CME SCCP Line Side Endpoints, page 11
- How to Configure SIP Session Timer, page 18
- Configuring SIP Session Timer, page 18
- Additional References, page 23
- Feature Information for Enhanced Firewall Traversal Cisco Unified CME, page 25

Prerequisites for Cisco Unified Communications Trusted Firewall Control

- Ensure that you have the correct platform to support this feature. Cisco Unified Communications Trusted Firewall Control is supported on the Cisco 1861, 2801, 2811, 2821, 2851, 3825, and 3845 platforms.
- Cisco IOS Release 15.1(2)T
- All k9 images with voice support. Session Timer feature can run on any voice image and does not support the firewall traversal.
- uc-base and securityk9 licenses on Cisco 29xx and 39xx platforms. Session Timer feature does not require securityk9 licenses.

Restrictions for Enhanced Firewall Traversal for Cisco Unified Communications

Cisco IOS Release 15.1(2)T implements firewall traversal for media using STUN on TRP and is not supported for:

- RSVP flow support through the Firewall
- Traditional SRST mode
- H.323 trunk support for Unified Communication Trusted Firewall
- Media flow around on Cisco Unified Border Element
- IPv6
- IP Multicast
- Video calls on SCCP and SIP line side

Information About Enhanced Firewall Traversal for Cisco Unified Communications using STUN

Before you configure Enhanced Firewall Traversal using STUN, you should understand the following concepts:

- Overview of Firewall Traversal for Cisco Unified Communications, page 3
- SIP Session Timer, page 3
- Firewall Traversal for Soft Phone, page 4
- Firewall Traversal for Wireless Phone, page 4

Overview of Firewall Traversal for Cisco Unified Communications

In previous releases, firewall traversal implemented a new framework for IOS firewall traversal on Cisco Unified CME and Cisco Unified Border Element for SIP trunks.

For more information on Cisco trusted firewall traversal, see: *http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/feature/guide/EnhancedTrustedFirewallControll.html*

SIP Session Timer

The SIP Session Timer (RFC 4028) is the standard SIP keepalive mechanism that keeps the SIP session active. The SIP user agents send periodic re-INVITE or UPDATE requests (referred to as session refresh requests) to keep the session alive. The interval for the session refresh request is determined through a negotiation mechanism. Session Timer is used to allow SIP signaling through the IOS firewall. You must configure Access Control List (ACL) or partial SIP-Application Layer Gateway (ALG) on the Cisco IOS firewall to allow SIP signaling.

After signaling, a pinhole is created. The firewall starts an inactivity timer, so that in case the user agents crashes or reboots during the call or the BYE message is lost, it can remove its states when the timer starts.

For the Cisco Unified CME SIP line side, by default, the endpoint sends periodic REGISTER messages on port 5060.

- A partial SIP-ALG keeps track of the endpoint registration and keeps the signaling pinhole open as far as the registration is active.
- An ACL tracks the User Datagram Protocol (UDP) / Transmission Control Protocol (TCP) messages that travel across the signaling port and keeps the signaling pinhole open.

However, the Cisco Unified CME SIP trunks do not exchange periodic SIP messages.The Cisco IOS firewall control sessions times out if no SIP messages are exchanged. The timed out SIP over UDP sessions are re-established with the next SIP message (for example, BYE). Timed out SIP over TCP sessions are not re-established and the subsequent SIP messages (for example, BYE) will be dropped.

Restrictions and Limitations for SIP Session Timer

SIP session timer does not support the following:

- Media modifications in responses to locally sent ReINVITE for session refresh
- Session timer in early dialog UPDATE

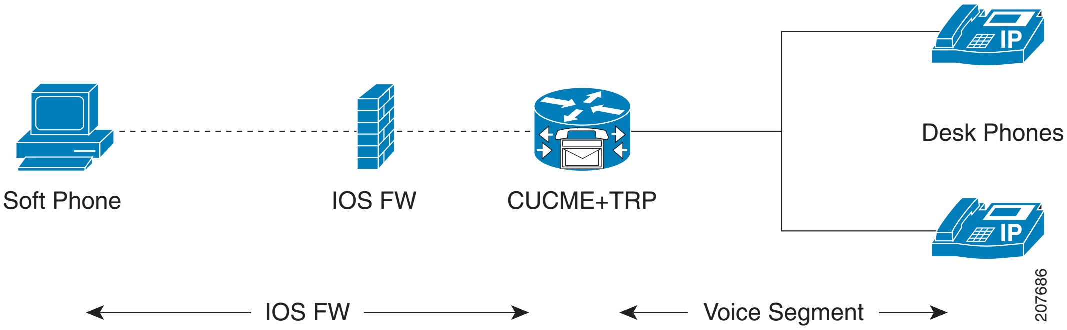
Firewall Traversal Deployment Scenarios

This section provides the firewall traversal scenarios for the Cisco Unified CME line side endpoints.

Firewall Traversal for Soft Phone

For Cisco Unified CME line side, you can deploy an IOS firewall that can be colocated or non colocated with the Cisco Unified CME.

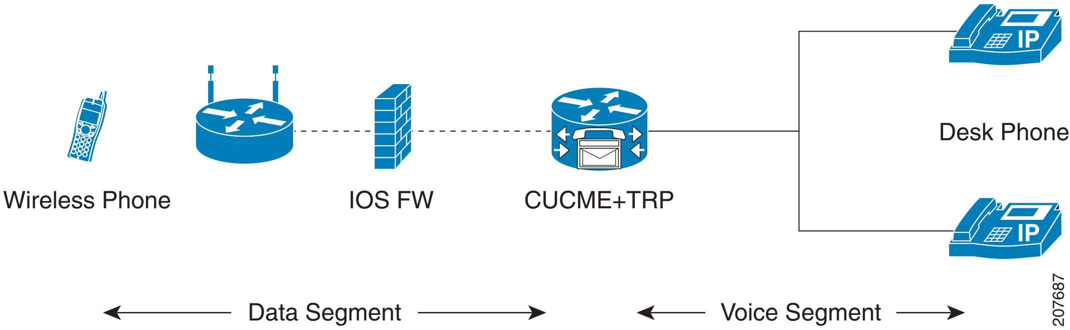
Figure 1 Soft Phone Communicating to Desktop Phones



This is a typical TRP-based trusted IOS firewall traversal deployment between a soft phone and the desk phones. In this scenario, a soft phone like CIPC in the data segment is registered to a Cisco Unified CME. When this soft phone communicates to a desktop IP phone in the voice segment that is registered to the same or different Cisco Unified CME, you can deploy an IOS firewall for the traffic sent between the desktop phone and the soft phone on the Cisco Unified CME line side.

Firewall Traversal for Wireless Phone

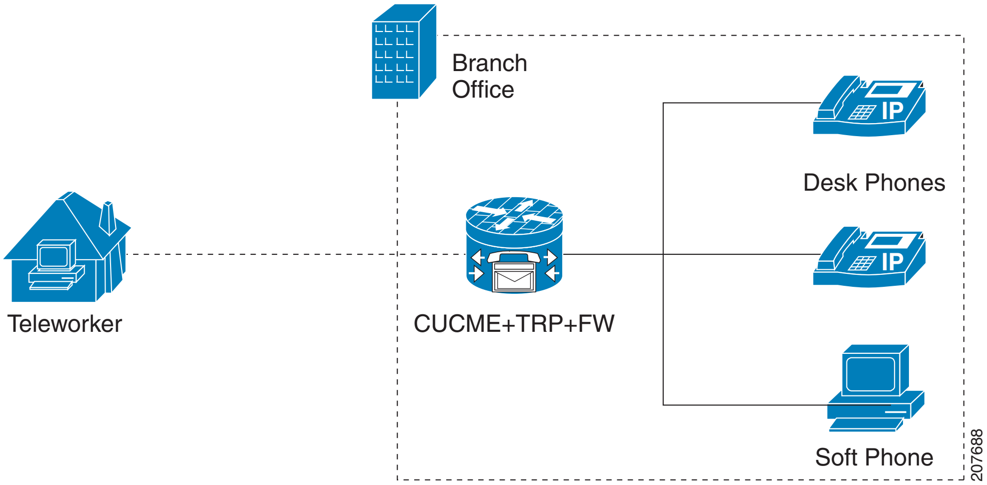
Figure 2 Wireless Phone Communicating to Wired Phones



In this scenario, the TRP-based trusted IOS firewall traversal is deployed between a wireless phone and desktop phones. A wireless (WiFi) phone like Cisco 792xG is registered to a Cisco Unified CME. When the wireless phone communicates to a wired phone that is registered to the same or different Cisco Unified CME, you can deploy an IOS firewall for the traffic sent between the wired and the wireless phone on the Cisco Unified CME line side.

Firewall Traversal for Teleworker

Figure 3 Teleworker Communicating to Central Office Desktop Phones



In this scenario, the teleworker phone is registered to a central or branch office and the Cisco Unified CME communicates to a phone which resides inside the central or branch office. You can deploy an IOS firewall for the traffic sent between the central/branch office and the teleworker phone on the Cisco Unified CME line side.

The teleworker can use the Transport Layer Security (TLS) and Secure Real-Time Protocol (SRTP) for making VoIP calls or establish a Virtual Private Network (VPN) tunnel to the central or branch office for making VoIP calls. In TLS/ SRTP case, the VPN engine/concentrator decrypts the signaling packets and passes the packets to the firewall for inspection. Hence, either a partial SIP ALG or ACL, along with TRP, can be deployed. In VPN case, the firewall will not have the key to decrypt the signaling packets. Hence, only ACL along with TRP can be deployed.

Configuration Prerequisites

The trusted firewall traversal for Cisco Unified CME SIP line side endpoints can be configured using TRP. The TRP must be configured under **voice service voip> stun** with the following information:

- Authorization agent-id
- Shared secret
- CAT life
- Keepalive interval

The *authorization agent-id* and *shared secret* are mandator commands and the *CATlife* and *Keepalive interval* are optional commands and can have default values.

In addition, the **stun-usage** command must to be configured as firewall traversal by using CISCO-STUN-FLOWDATA under **voice class stun-usage**

For detail configuration steps, see:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/feature/guide/EnhancedTrustedFirewallControll.html

How to Configure Firewall Traversal for Cisco Unified CME SIP Line Side Endpoints

To configure Firewall traversal for Cisco Unified CME SIP line side endpoints, enable the stun-usage under:

- Voice-register pool or voice-register template and apply under the voice register pool for SIP line side

This section contains the following procedures:

- Configuring Firewall Traversal for Cisco Unified CME SIP Line Side Endpoints, page 6
- Configuration Examples for Cisco Unified CME SIP Line Side EndPoints, page 7

Configuring Firewall Traversal for Cisco Unified CME SIP Line Side Endpoints

Perform these tasks to configure firewall traversal.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *phone-tag*
4. **voice-class stun-usage** *tag*
5. **end**

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	**voice register pool** *phone-tag* **Example:** `Router(config)# voice register pool 3`	Enters voice register pool configuration mode to set the phone-specific parameters for an SIP phone. • *phone-tag*—Unique sequence number that identifies the phone. Range is version and platform-dependent; type **?** to display range.

	Command or Action (continued)	Purpose (continued)
Step 4	**voice-class stun-usage** *tag* **Example:** `Router(config-voice-register-pool)# voice-class stun-usage 1`	Enables voice-class stun-usage on the voice-registor pool. • This command can also be configured in voice-register-template configuration mode and applied to one or more SIP phones. The voice-register pool configuration has priority over the voice-register-template configuration.

Step 5	**end**
	Example:
	`Router(config-voice-register-pool)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Configuration Examples for Cisco Unified CME SIP Line Side EndPoints

This section provides the following sample configuration:

```
Router# show run

Building configuration...
!
! Last configuration change at 14:20:02 IST Thu Mar 25 2010 by cisco
! NVRAM config last updated at 15:10:47 IST Wed Mar 24 2010 by cisco
!
version 15.1
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname fidessrst
!
boot-start-marker
boot system tftp://9.13.40.15/kartk/c3845-adventerprisek9_ivs-mz.0_2_0_20091205
boot-end-marker
!
logging buffered 1000000
no logging console
enable secret 5 $1$GbsI$Ah0BLBHzFx4w/Hu7kyhrs1
enable password cisco
!
no aaa new-model
!
no process cpu autoprofile hog
clock timezone IST 5
!
dot11 syslog
ip source-route
!
no ip cef
!
no ip domain lookup
ip domain name yourdomain.com
no ipv6 cef
```

```
!
multilink bundle-name authenticated
!
template 10
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
voice service voip
 notify redirect ip2pots
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 stun
  stun flowdata agent-id 1 boot-count 45
  stun flowdata shared-secret 7 14141B180F0B7B79772B3A26211C564450
  stun flowdata catlife 70 keepalive 30
 sip
  session transport tcp
  registrar server expires max 600 min 60
!
voice class stun-usage 1
 stun usage firewall-traversal flowdata
!
voice register global
 mode cme
 source-address 192.168.0.1 port 5060
 max-dn 100
 max-pool 100
 load 7971 SIP70.8-5-2SR1S
 load 7970 SIP70.8-5-2SR1S
 load 7961 SIP41.8-5-2SR1S
 load 7960-7940 P0S3-8-12-00
 authenticate realm cisco.com
 tftp-path flash:
 create profile sync 0221764396482329
!
voice register dn  2
 number 999999
 pickup-group 333
 name 7970-2
 mwi
!
voice register dn  3
 number 777777
 pickup-group 333
 name 7970-3
 mwi
!
voice register dn  5
 number 2222
 name 7960-Camelot1
 mwi
!
voice register dn  6
 number 4444
 name 7960-Camelot2
 mwi
!
voice register dn  7
 number 6666
 name 7960-Camelot3
 mwi
!
```

```
voice register dn  8
 number 8888
 call-forward b2bua all 6666
 name 7960-Camelot4
 mwi
!
voice register dn  9
 number 101010
 call-forward b2bua all 1111
 name 7960-Camelot5
 mwi
!
voice register dn  10
 number 121212
 call-forward b2bua noan 6666 timeout 3
 name 7960-Camelot6
 mwi
!
voice register dn  11
 number 141414
 call-forward b2bua busy 1111
 name 7960-Camelot7
 huntstop channel 1
 mwi
!
voice register dn  50
number 15253545
name callgen-sip1
mwi
!
voice register dn  51
number 16263646
name callgen-sip2
mwi

voice register template  10
 voice-class stun-usage 1
 softkeys connected  Park Confrn Endcall Hold Trnsfer
!
voice register pool  2
 park reservation-group 1111
 id mac 0022.9059.81D9
 type 7970
 number 1 dn 2
 template 10
 codec g711ulaw
!
voice register pool  50
 id mac 0011.209F.5D60
 type 7960
 number 1 dn 50
 voice-class stun-usage 1

 codec g711ulaw
!
voice register pool  51
 id mac 0011.209F.5D60
 type 7960
 number 1 dn 51
  voice-class stun-usage 1
 codec g711ulaw
license udi pid CISCO3845-MB sn FOC12373868
archive
 log config
```

```
  hidekeys
username cisco password 0 cisco
!
redundancy
!
ip ftp username test
ip ftp password test123
!

!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
 ip address 7.9.9.120 255.255.0.0

 duplex auto
 speed auto
 media-type rj45
 no keepalive
 no cdp enable
!
interface GigabitEthernet0/1
 ip address 192.168.0.1 255.255.255.0

 duplex auto
 speed auto
 media-type rj45
 no cdp enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 7.9.0.1
ip route 9.13.7.0 255.255.255.0 9.13.7.1
ip route 9.13.7.0 255.255.255.0 9.13.38.1
ip route 9.13.40.0 255.255.255.0 9.13.38.1
ip route 10.104.56.0 255.255.255.0 192.168.0.35
!

arp 10.104.56.54 0024.81b5.3302 ARPA
!
!
control-plane
!
call treatment on
!
voice-port 0/0/0
!
voice-port 0/0/1
!
!
mgcp fax t38 ecm
!
gateway
 timer receive-rtp 1200
!
sip-ua
!
!
alias exec showrtp show policy-map type inspect zone-pair sessions
!
line con 0
 exec-timeout 0 0
 login local
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

How to Configure Firewall Traversal for Cisco Unified CME SCCP Line Side Endpoints

To configure Firewall traversal for Cisco Unified CME SCCP line side endpoints, enable the stun-usage under:

- Ephone or ephone-template and apply under the ephone for SCCP line side

This section contains the following procedures:

- Configuring Firewall Traversal for Cisco Unified CME SIP Line Side Endpoints, page 6
- Configuration Examples for Cisco Unified CME SIP Line Side EndPoints, page 7

Configuring Firewall Traversal for Cisco Unified CME SCCP Line Side Endpoints

Note MTP should be enabled under ephones for SCCP CME line side endpoints

Perform these tasks to configure firewall traversal.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **mtp**
5. **voice-class stun-usage** *tag*
6. **end**

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	**`ephone`** *`phone-tag`*
	Example:
	`Router(config)# ephone 2`
		Enters ephone configuration mode to set phone-specific parameters for an SCCP phone.
		- *phone-tag*—Unique sequence number that identifies the phone. Range is version and platform-dependent; type **?** to display range.

Step 4	**`mtp`**
	Example:
	`Router(config-ephone)# mtp`
		Enables Media Termination Points (MTP) on this ephone.

Step 5	**`voice-class stun-usage`** *`tag`*
	Example:
	`Router(config-ephone)# voice-class stun-usage 10000`
	`device-security-mode none`
	`mac-address FCAC.3BAC.0001`
	`max-calls-per-button 2`
	`mtp`
	`type anl`
	`button  1:4`
		Enables voice-class stun-usage on this ephone.
		- This command can also be configured in ephone-template configuration mode and applied to one or more SCCP phones. The ephone configuration has priority over the ephone-template configuration.

Step 6	**`end`**
	Example:
	`Router(config-ephone)# end`
		Exits ephone configuration mode and returns to privileged EXEC mode.

Configuration Examples for Cisco Unified CME SCCP Line Side EndPoints

This section provides the following sample configuration:

```
Router#show run

Building configuration...
!
! Last configuration change at 14:20:02 IST Thu Mar 25 2010 by cisco
! NVRAM config last updated at 15:10:47 IST Wed Mar 24 2010 by cisco
```

```
!
version 15.1
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname fidessrst
!
boot-start-marker
boot system tftp://9.13.40.15/kartk/c3845-adventerprisek9_ivs-mz.0_2_0_20091205
boot-end-marker
!
logging buffered 1000000
no logging console
enable secret 5 $1$GbsI$Ah0BLBHzFx4w/Hu7kyhrs1
enable password cisco
!
no aaa new-model
!
no process cpu autoprofile hog
clock timezone IST 5
!
dot11 syslog
ip source-route
!
no ip cef
!
no ip domain lookup
ip domain name yourdomain.com
no ipv6 cef
!
multilink bundle-name authenticated
!
template 10
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
voice service voip
 notify redirect ip2pots
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 stun
  stun flowdata agent-id 1 boot-count 45
  stun flowdata shared-secret 7 14141B180F0B7B79772B3A26211C564450
  stun flowdata catlife 70 keepalive 30
 sip
  session transport tcp
  registrar server expires max 600 min 60
!
voice class stun-usage 1
 stun usage firewall-traversal flowdata
!
!
license udi pid CISCO3845-MB sn FOC12373868
archive
 log config
  hidekeys
username cisco password 0 cisco
!
redundancy
!
ip ftp username test
ip ftp password test123
!

!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
 ip address 7.9.9.120 255.255.0.0

 duplex auto
 speed auto
 media-type rj45
 no keepalive
 no cdp enable
!
interface GigabitEthernet0/1
 ip address 192.168.0.1 255.255.255.0

 duplex auto
 speed auto
 media-type rj45
 no cdp enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 7.9.0.1
ip route 9.13.7.0 255.255.255.0 9.13.7.1
ip route 9.13.7.0 255.255.255.0 9.13.38.1
ip route 9.13.40.0 255.255.255.0 9.13.38.1
ip route 10.104.56.0 255.255.255.0 192.168.0.35
!

arp 10.104.56.54 0024.81b5.3302 ARPA
!
control-plane
!
call treatment on
!
voice-port 0/0/0
!
voice-port 0/0/1
!
!
mgcp fax t38 ecm
!
sccp local GigabitEthernet0/1
sccp ccm 192.168.0.1 identifier 1 version 7.0
sccp
!
gateway
 timer receive-rtp 1200
!
sip-ua
!
telephony-service
 sdspfarm units 3
 sdspfarm transcode sessions 12
 sdspfarm tag 2 HwConference
 sdspfarm tag 3 mtp00230471e381
 video
 srst mode auto-provision all
 srst ephone template 1
 srst dn line-mode dual
 max-ephones 262
 max-dn 500
 ip source-address 192.168.0.1 port 2000
 service directed-pickup gpickup
 max-conferences 8 gain -6
 call-park system application
 moh music-on-hold.au
 transfer-system full-consult
 create cnf-files version-stamp 7960 Mar 24 2010 15:09:20
!
ephone-template  1
voice-class stun-usage 1
 mtp
!
ephone-template  3
 voice-class stun-usage 1
!
ephone-dn  1  dual-line
 number 1000
 name vg1port1
!
ephone-dn  2  dual-line
 number 2000
 name vg1port2
!
ephone-dn  3  dual-line
 number 3000
 name vg2port1
!
ephone-dn  4  dual-line
 number 4000
 name vg2port2
 call-forward all 3000
!
ephone-dn  5  dual-line
 number 1111
 name sccpcamelot1
!
ephone-dn  6  dual-line
 number 3333
 name sccpcamelot2
!
ephone-dn  7  dual-line
 number 717818919
 description 717818919
 name 717818919
!
ephone-dn  8  dual-line
 number 6000
 label 6000
 description 6000
 name 6000
!
ephone-dn  9  dual-line
 number 5000
 label 5000
 description 5000
 name 5000
!
ephone-dn  10  dual-line
!
ephone-dn  11  dual-line
!
```

```
ephone-dn  13  dual-line
 number 919886087486
 name blacforestvg0
!
ephone-dn  14  dual-line
 number 919886087487
 name blacforestvg1
!
ephone-dn  15  dual-line
 number 919886087488
 name blacforestvg2
!
ephone-dn  16  dual-line
 number 919886087489
 name blacforestvg3
!
ephone-dn  41  dual-line
 number 9876
 conference meetme
 preference 1
 no huntstop
!
ephone-dn  42  dual-line
 number 9876
 conference meetme
 preference 2
 no huntstop
!
ephone-dn  43  dual-line
 number 9876
 conference meetme
 preference 3
 no huntstop
!
ephone  1
 voice-class stun-usage 1
 device-security-mode none
 mac-address FCAC.3BAE.0000
 max-calls-per-button 2
 mtp
 type anl
 button  1:1
!
ephone  2
 voice-class stun-usage 1
 device-security-mode none
 mac-address FCAC.3BAE.0001
 max-calls-per-button 2
 mtp
 type anl
 button  1:2
!
ephone  3
 voice-class stun-usage 1
 device-security-mode none
 mac-address FCAC.3BAC.0000
 max-calls-per-button 2
 type anl
 button  1:3
!
ephone  4
 voice-class stun-usage 1
 device-security-mode none
 mac-address FCAC.3BAC.0001
 max-calls-per-button 2
 mtp
 type anl
 button  1:4
!
ephone  5
 voice-class stun-usage 1
 device-security-mode none
 mac-address 1234.1234.1111
 max-calls-per-button 2
 mtp
 type 7960
 button  1:5
!
ephone  6
 voice-class stun-usage 1
 device-security-mode none
 mac-address 1234.1234.3333
 ephone-template 3
 max-calls-per-button 2
 codec g729r8 dspfarm-assist
 mtp
 type 7960
 button  1:6
!
ephone  7
 device-security-mode none
 mac-address FCAC.3B79.0001
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:14
!
ephone  8
 device-security-mode none
 mac-address 001B.D584.E274
 ephone-template 1
 button  1:7
!
ephone  9
 device-security-mode none
 mac-address FCAC.3B7F.0001
 ephone-template 1
 button  1:8
!
ephone  10
 device-security-mode none
 mac-address FCAC.3B7F.0000
 ephone-template 1
 button  1:9
!
ephone  11
 device-security-mode none
 mac-address FCAC.3B79.0002
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:15
!
ephone  13
 device-security-mode none
 mac-address FCAC.3B79.0000
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:13
!
ephone  14
 device-security-mode none
 mac-address FCAC.3B79.0003
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:16
!
alias exec showrtp show policy-map type inspect zone-pair sessions
!
line con 0
 exec-timeout 0 0
 login local
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

How to Configure SIP Session Timer

This section contains the following procedures:

- Configuring SIP Session Timer, page 18
- Configuration Examples for SIP Session Timer, page 20
- Session Timer Call Flows, page 21

Configuring SIP Session Timer

Perform these tasks to configure SIP session timer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **min-se** *string* **session-expire***s string*
6. **session refresh**

7. **dial-peer voice** *tag* **voip**
8. **voice-class sip session refresh** [**system**]
9. **end**

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	**`voice service voip`**
	Example:
	`Router(config)# voice service voip`
		Enters voice-service configuration mode and specifies a voice-encapsulation type.

Step 4	**`sip`**
	Example:
	`Router(config-voi-serv)# sip`
		Enters SIP configuration mode.

Step 5	**`min-se`** *`string`* **`session-expires`** *`string`*
	Example:
	`Router(conf-serv-sip)#min-se 90 session-expires 100`
		Configures the minimum session expires (min-se) and session-expires.
		- *min se— 90 to 86400*

Step 6	**`session refresh`**
	Example:
	`Router(conf-serv-sip)#session refresh`
		Enables SIP session timer globally.

Step 7	**`dail-peer voice`** *`tag`* **`voip`**
	Example:
	`Router(config)# dial-peer voice 1 voip`
		Enters dial peer configuration mode to define a VoIP dial peer.

Step 8	**`voice-class sip session refresh`**
	Example:
	`Router(config-dial-peer)# voice-class sip session refresh`
		Enables SIP session refresh at dial-peer level.

Step 9	**`end`**
	Example:
	`Router(config-dial-peer)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Configuration Examples for SIP Session Timer

This section provides the following sample configuration:

```
Router# show run
show running-config
Building configuration...
Current configuration : 2284 bytes
!
! Last configuration change at 13:50:48 IST Sun Mar 14 2010
! NVRAM config last updated at 16:21:46 IST Fri Mar 12 2010
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname CUBE1-Fides3
!
boot-start-marker
boot-end-marker
!
!
logging buffered 1000000
no logging console
!
no aaa new-model
no process cpu autoprofile hog
clock timezone IST 5
!
ip source-route
!
ip cef
!
no ip domain lookup
ip domain name yourdomain.com
no ipv6 cef
multilink bundle-name authenticated
!
voice service voip
allow-connections sip to sip
sip
min-se 90 session-expires 100
session refresh
!
voice-card 0
!
license udi pid CISCO2821 sn FHK1143F0UK
archive
log config
hidekeys
no memory lite
username cisco privilege 15 secret 5 $1$p0H/$eUuiG4gFjfFQFVvUzoDd3/
!
redundancy
!
ip ftp username test
ip ftp password test123
!
interface GigabitEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
ip address 7.9.9.106 255.255.0.0
duplex auto
```

```
speed auto
no cdp enable
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
no cdp enable
!
ip forward-protocol nd
!
ip http server
ip http access-class 23
ip http authentication local
ip http timeout-policy idle 60 life 86400 requests 10000
ip route 0.0.0.0 0.0.0.0 7.9.0.1
!
control-plane
!
mgcp fax t38 ecm
!
!
dial-peer voice 100 voip
huntstop
destination-pattern 1000000000
b2bua
session protocol sipv2
session target ipv4:7.9.9.9
incoming called-number 2000000000
voice-class sip session refresh
codec g711ulaw
!
sip-ua
retry invite 2
!
!
gatekeeper
shutdown
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
access-class 23 in
privilege level 15
login local
transport input telnet
line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

Session Timer Call Flows

Table 1 shows who will be sending the session refresh requests for all combinations of User Agent Clients (UAC) / User Agent Server (UAS) support for session timer.

Table 1 Session Timer on CUBE for SIP-SIP Call Flows

S.No	UAC Support	UAS Support	Command Line Interface Enabled on IN leg	Command Line Interface Enabled on OUT leg	Action
1	Yes	Yes	Yes	Yes	UAC/UAS will send the session refresh requests and the Call Control Agent will pass it across.
2	Yes	Yes	No	Yes	
3	Yes	Yes	Yes	No	
4	Yes	Yes	No	No	UAC/UAS may send session refresh requests and the Call Control Agent will pass it across.
5	Yes	No	Yes	Yes	If the incoming INVITE has no “refresher” or “refresher=uac”, UAC will send the session refresh requests and the Call Control Agent will pass it across. The Call Control Agent will also start the session expiration timer on the IN LEG. If the incoming INVITE has “refresher=uas”, the Call Control Agent will send the session refresh requests on the appropriate leg(s).
6	Yes	No	No	Yes	
7	Yes	No	Yes	No	
8	Yes	No	No	No	UAC may send the session refresh requests and the Call Control Agent will pass it across.
9	No	Yes	Yes	Yes	If the 2xx response from UAS has “refresher=uas”, UAS will send the session refresh requests and the Call Control Agent will pass it across. The Call Control Agent will also start the session expiration timer on the OUT LEG. If the 2xx response from UAS has no “refresher” or has “refresher=uac”, the Call Control Agent will the send session refresh requests on the appropriate call leg(s).
10	No	Yes	No	Yes	
11	No	Yes	Yes	No	
12	No	Yes	No	No	UAS may send the session refresh requests and the Call Control Agent will pass it across.
13	No	No	Yes	Yes	Call Control Agent will send the session refresh requests on the appropriate call leg(s).
14	No	No	No	Yes	
15	No	No	Yes	No	
16	No	No	No	No	No session timer.

Additional References

The following sections provide references related to the Enhanced Firewall Traversal using STUN feature.

Related Documents

Related Topic	Document Title
	•
	•

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	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

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Enhanced Firewall Traversal Cisco Unified CME

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, and Cisco IOS XE, software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature information for Firewall Traversal for Cisco Unified CME

Feature Name	Releases	Feature Information
Cisco Unified Communications Trusted Firewall Control.	15.1(2)T	Cisco Unified Communications Trusted Firewall Control using STUN pushes intelligent services into the network through Trust Relay Point (TRP). The **session refresh** and **voice-class sip session refresh** commands are introduced in this release.

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.