Cisco Unified Communications Trusted Firewall Control-Version II

First Published: October 2, 2009

Introduction

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 NAT (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 focuses on the following:

- Noncolocated firewall for UC SIP trunks
- Support Firewall traversal for Cisco Unified Border Element call flows in which the media flow through the Media Termination Points such as MTP, Transcoder, or Conference bridge with Trust Relay Point (TRP) enabled.
- Firewall traversal for additional Cisco Unified Border Element call flows using STUN.

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 "stun flowdata shared-secret" section on page 18.

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

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 15.0(1)M
- All k9 images with voice support
- uc-base and securityk9 licenses on Cisco 29xx and 39xx platforms

Restrictions for Enhanced Firewall Traversal for Cisco Unified Communications using STUN

Cisco IOS Release 15.0(1)M implements firewall traversal for media using STUN on TRP and is supported on:

- Cisco Unified CME colocated with TRP
- Cisco Unified Border Element colocated with TRP
- Cisco Unified Media Termination Points colocated with TRP
- Cisco TDM-SIP Gateway colocated with TRP

TRP is supported for the following call control agents:

- Cisco Unified CME, Cisco Unified Border Element, Cisco TDM-SIP Gateway, and Cisco Unified Media Termination Points which are STUN-aware.

  Not Supported:

  - TRP based Cisco IOS firewall traversal on line side of Cisco Unified CME
  - RSVP
  - IPv6
  - Media flow around on Cisco Unified Border Element

Other restrictions:

- No prering support
  - No guarantee that STUN open pinhole packet reaches the Cisco IOS firewall before the first RTP packet. Possible initial RTP packet drops at the Cisco IOS firewall.
- Cisco IOS firewall control session timeout
  - ACLs or partial SIP-ALG must be configured on the Cisco IOS firewall to allow SIP signaling.
  - The Cisco IOS firewall control sessions timeout if no SIP messages are exchanged.
  - 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, causing subsequent SIP messages (for example, BYE) to be dropped.

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 Enhanced Firewall Traversal for Cisco Unified Communications using STUN, page 3
- Firewall Traversal Design, page 4

Overview of Enhanced Firewall Traversal for Cisco Unified Communications using STUN

Enhanced Firewall Traversal using STUN pushes intelligent services into the network through Trust Relay Point (TRP).

This document provides information related to TRP based Firewall traversal solution. It includes topologies, configurations and show/debug commands on the call agents (Cisco Unified CME /

Cisco Unified Border Element / Cisco TDM-SIP Gateway / MTP).

The following are the benefits of the solution:

- Increased firewall performance while opening firewall ports in the media path dynamically when a VoIP call is made between two endpoints
- Simplification of firewall policy configuration and integration of firewall policy generation with call control
- Solution to the above two problems without compromising on network security

Firewall Traversal Design

TRP as Media Relay

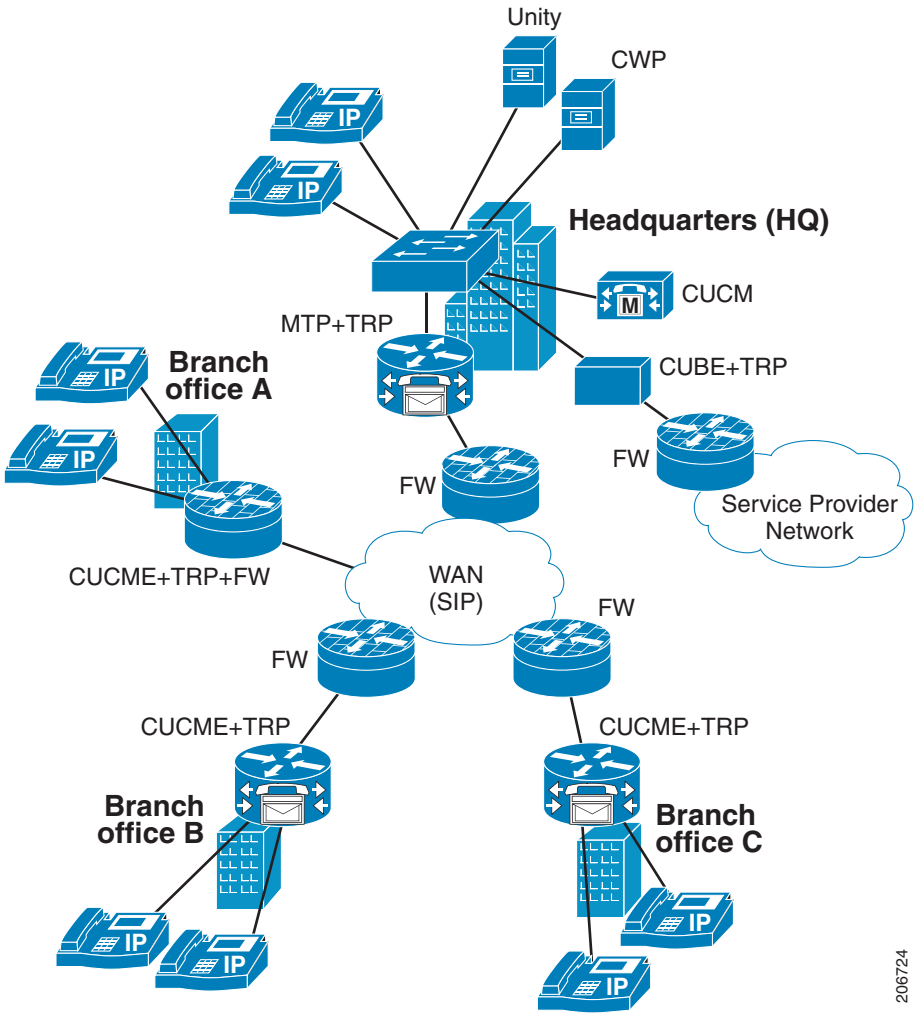

Figure x: Firewall Traversal Solution:

This is a typical TRP based Trusted IOS Firewall Traversal deployment for an Enterprise. In this scenario, the Headquarters (HQ) has a Cisco Unified CM cluster located in the Datacenter. There are two SIP trunks, one to the WAN establishing SIP connectivity with the Branch Offices and the other to the Service Provide (SP) Network. An IOS Firewall is deployed at the edge of the WAN and SP Network. The TRP colocated with the MTP and Cisco Unified Border Element performs the firewall traversal for media over the WAN and SP Network respectively.

Each branch office has a SIP trunk to the WAN which establishes the SIP connectivity with other Branch Offices and the HQ. The branch office has an IOS Firewall deployed at the edge of the WAN.

In Branch Office A, the IOS Firewall is colocated with Cisco Unified CME, whereas in Branch Offices B and C, it is noncolocated. At each branch the TRP colocated with the Cisco Unified CME performs the firewall traversal for media.

Firewall traversal using STUN

Firewall traversal is used to build intelligence into the firewall so that it can open a port dynamically when it receives a STUN request for a media flow. This request is authenticated/authorized by the firewall to ensure that it opens pin-holes only for genuine calls.

Cisco FlowData

Flowdata refers to CISCO-STUN-FLOWDATA, a comprehension-optional Cisco proprietary STUN attribute. If a STUN agent does not understand the attribute, the agent must ignore it. This attributes identifies an RTP or RTCP flow to the firewall and contains a Crypto Acceptance Token (CAT), which the firewall uses to authenticate the sender of the STUN message—the TRP. For more information, see RFC 5389.

How to Configure Firewall Traversal

The Cisco Unified Trusted Firewal Traversal can be configured using TRP. When you have Cisco Unified CM as the call control agent, enable TRP under the appropriate dspfarm profile. If you have Cisco Unified CME as the call control agent, enable TRP under the appropriate VoIP dial peer. For more information about enabling TRP on CUCM, refer to http://www.cisco.com/en/US/docs/voice_ip_comm/cucmbe/admin/7_1_2/ccmsys/a05media.html#wp1062136.

This section contains the following procedures:

- Configuring Firewall Traversal, page 5
- Configuration Examples for Trusted Firewall Traversal using STUN, page 8

Configuring Firewall Traversal

Perform these tasks to configure firewall traversal.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **stun**
5. **stun flowdata agent-id** *tag*
6. **stun flowdata shared-secret** *string*
7. **stun flowdata keepalive** *seconds*
8. **exit**
9. **voice class stun-usage** *tag*
10. **stun usage firewall-traversal flowdata**
11. **exit**
12. **dial peer voice** *tag* **voip**

13. **destination pattern** *tag*
14. **voice-class stun-usage** *tag*
15. **end**
16. **dspfarm Profile**
17. **Stun firewall-traversal flowdata**
18. **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	**stun** **Example:** `Router(config-voi-serv)# stun`	Enters STUN configuration mode.
Step 5	**stun flowdata agent-id** *tag* **Example:** `Router(config-serv-stun)# stun flowdata agent-id 35`	Configure the STUN flowdata agent ID. • *tag*—Must match agent ID on the firewall
Step 6	**stun flowdata shared-secret** *string* **Example:** `Router(config-serv-stun)# stun flowdata shared-secret 123abc123abc`	Configures a secret shared on a call control agent. • *string*—Must match shared secret on the firewall.

Step 7	**stun flowdata keepalive** *seconds*
	
	Example:
	`Router(config)# voice service voip`
	`Router(config-serv-stun)# stun flowdata keepalive 5`
		(Optional) Changes the keepalive interval from the default value.
		• *seconds*—Range is 1 to 65535 seconds. Default is 10 seconds.

Step 8	**exit** **Example:** `Router(config-serv-stun)# exit`	Exits STUN configuration mode.

	Command or Action (continued)	Purpose (continued)
Step 9	**voice class stun-usage** *tag* **Example:** `Router(config)# voice-class stun-usage 10000`	Assigns identification tag to a voice class and enters voice class configuration mode.
Step 10	**stun usage firewall-traversal flowdata** **Example:** `Router(config-class)# stun usage firewall-traversal flowdata`	Enables firewall traversal using STUN.
Step 11	**exit** **Example:** `Router(config-class)# exit`	Exits voice class configuration mode.
Step 12	**Apply the voice-class on the dial peer in mode-1** **Example:** `Router(config)# dial-peer voice 1 voip`	Enters dial peer configuration mode to define a VoIP dial peer for firewall traversal.
Step 13	**destination-pattern** *tag* **Example:** `Router(config-dial-peer)# destination-pattern 2`	Defines the destination-pattern.
Step 14	**voice-class stun-usage** *tag* **Example:** `Router(config-dial-peer)# voice-class stun-usage 10000`	Enables firewall traversal for VoIP communications on this dial peer.
Step 15	**end** **Example:** `Router(config-dial-peer)# end`	Exits configuration mode and returns to privileged EXEC mode.

Step 16	**Enabling trusted firewal traversal on dspfarm in mode-2**
	`Router(config)# dspfarm profile 10 mtp`
	or
	`Router(config)# dspfarm profile 10 transcode`
	or
	`Router(config)# dspfarm profile 10 conference`
		Enters dspfarm configuration mode to define a dspfarm for firewall traversal for mtp.
		or
		Enters dspfarm configuration mode to define a dspfarm for firewall traversal for transcode.
		or
		Enters dspfarm configuration mode to define a dspfarm for firewall traversal for confernece.

	Command or Action (continued)	Purpose (continued)
Step 17	**Apply the stun for dspfarm** `Router(config-dspfarm-profile)#stun firewall-traversal flowdata`	Defines the stun usage firewall-traversal flowdata command under dspfarm profile.
Step 18	**end** **Example:** `Router(config-dspfarm-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuration Examples for Trusted Firewall Traversal using STUN

This section provides the following sample configuration:

```
Router#sh run

Building configuration...



Current configuration : 4446 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service internal
!
hostname CUBE1-3825
!
boot-start-marker
boot system flash:c3825-adventerprisek9_ivs-mz.21aug08
boot-end-marker
!
logging buffered 9999999
no logging console
!
no aaa new-model
clock timezone IST 5
no network-clock-participate slot 1
!
dot11 syslog
ip source-route
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
!
!
```

```
!
!
voice-card 0
!
voice-card 1
 dsp services dspfarm
!
!
!
voice service voip
 allow-connections sip to sip
 stun

  stun flowdata agent-id 15 boot-count 1
  stun flowdata shared-secret 7 110A1016141D1B0D17393C2079616676
  stun flowdata catlife 70 keepalive 30
 sip
  midcall-signaling passthru
!
voice class stun-usage 100
 stun usage firewall-traversal flowdata
!
voice class stun-usage 10000
 stun usage firewall-traversal flowdata
!
!
!
voice iec syslog
!
!
!
!
!
!
license udi pid CISCO3825 sn FHK1029F0TB
archive
 log config
  hidekeys
no memory lite
!
!
ip ftp username test
ip ftp password test123
!
!
!
!
!
interface Loopback0
 no ip address
!
interface GigabitEthernet0/0
 ip address 9.13.24.6 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
```

```
 no keepalive
 no cdp enable
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 9.13.24.1
ip route 1.1.1.0 255.255.255.0 9.13.24.7
ip route 9.13.23.0 255.255.255.0 9.13.24.7
ip route 9.13.23.233 255.255.255.255 9.13.24.1
!
!
!
control-plane
!
call treatment on
!
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
sccp local GigabitEthernet0/0
sccp ccm 9.13.24.2 identifier 2 version 7.0
sccp ccm 9.13.24.50 identifier 1 version 6.0
sccp
!
sccp ccm group 1
 associate ccm 2 priority 1
 associate profile 100 register TRPMode2
 keepalive retries 1
 keepalive timeout 10
 switchover method immediate
 switchback method immediate
!
dspfarm profile 100 conference
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 stun firewall-traversal flowdata <<< To enable mode 2 TRP>>>
 maximum sessions 5
 associate application SCCP
!
dspfarm profile 10 mtp
 codec g711ulaw
 shutdown
!
dial-peer voice 1 voip
 destination-pattern 2...
 session protocol sipv2
 session target ipv4:9.13.23.6
 voice-class stun-usage 10000 <<< To enable mode 1 TRP>>>
 codec g711ulaw
!
dial-peer voice 2 voip
 destination-pattern 9...
 session protocol sipv2
 session target ipv4:9.13.24.50
 codec g711ulaw
!
```

```
!
!
sip-ua
 protocol mode ipv4
!
!
telephony-service
 sdspfarm units 1
 sdspfarm tag 1 mtp1234
 em logout 0:0 0:0 0:0
 max-ephones 10
 max-dn 10
 ip source-address 9.13.23.6 port 2000
 max-conferences 12 gain -6
 transfer-system full-consult
 create cnf-files version-stamp 7960 May 29 2008 11:57:23
!
alias exec t test stun
alias exec dp show run | sec dial
alias exec voice show run | sec voice
alias exec route show run | sec route
alias exec profile show run | sec dspfarm profile
alias exec sccp show run | sec sccp
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 no login
 transport input none
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
no process cpu autoprofile hog
ntp server 9.13.0.10
end
```

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 using STUN

Table 1 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 1 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 1 Feature information for Enhanced Firewall Traversal using STUN

Feature Name	Releases	Feature Information
Cisco Unified Communications Trusted Firewall Control.	15.0(1)M	Cisco Unified Communications Trusted Firewall Control using STUN pushes intelligent services into the network through Trust Relay Point (TRP). The **stun flowdata catlife** commands is introduced by this feature.