cisco Cisco WebEx Telepresence

Cisco WebEx Telepresence Firewall Requirements for SIP ALG

Table of Contents

Introduction

This document provides information about the Session Initiation Protocol (SIP) Application Level Gateway (ALG), which is a customer-side firewall feature, and why it must be disabled to ensure the proper operation of Cisco WebEx Telepresence.

Issue

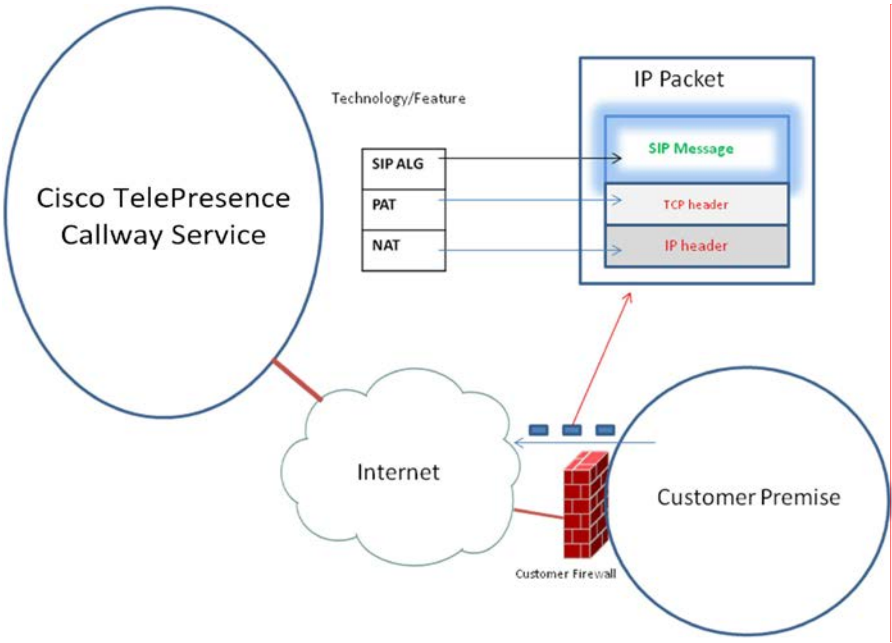
- Results from the Line Quality Test (LQT) tool (http://videotest.webex.com) indicate that the customer firewall settings are not compatible with the Cisco WebEx Telepresence service.
- Under the **What can I do section**, the LQT tool recommends the following course of action: "*Disable SIP/ALG feature. Do not use firewall vendor's built-in SIP aware rules.*"

Symptoms

- LQT tool results indicate that SIP ALG is enabled on the customer firewall.
- Some possible symptoms, which will vary depending on the environment and firewall type, are shown below:
  - o Device registration to the Cisco WebEx Telepresence service network fails.
  - o Device cannot receive and/or place calls.
  - o Calls connect as audio-only when calling other video devices.
  - o Calls drop after several minutes.

Overview of SIP ALG Operation

The following diagram illustrates an overview of the SLP ALG operation.



[JMS1]

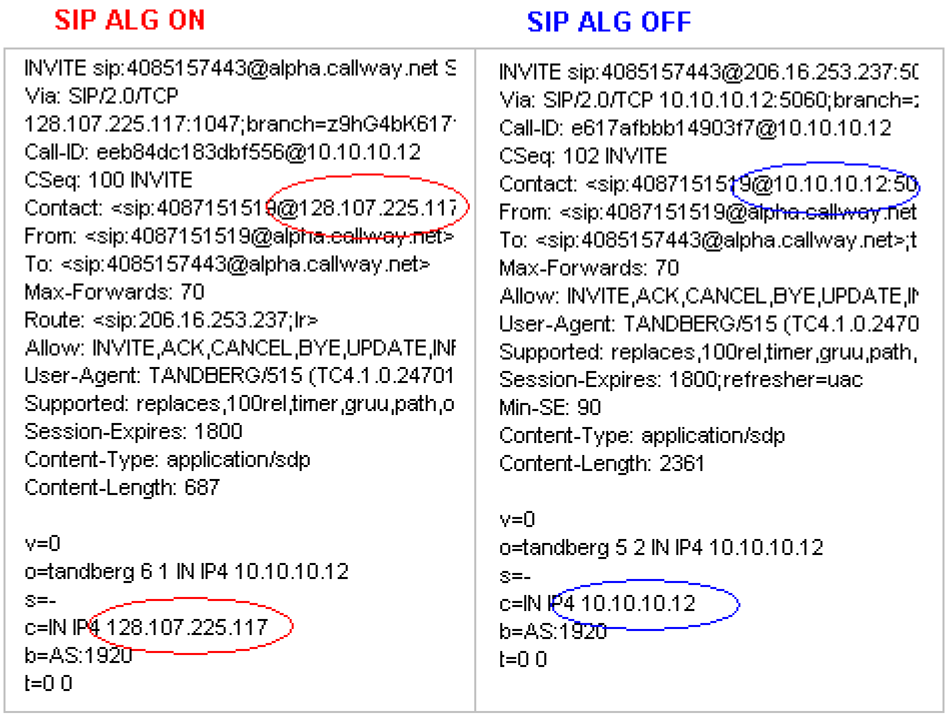
- Network Address Translation (NAT) translates IP address within the IP packet headers (Layer 3 of the OSI model).
- Port Address Translation (PAT) translates port information within the TCP/UDP headers (Layer 4 of the OSI model).

- Session Initiation Protocol (SIP) is the signaling protocol that is used by Cisco WebEx Telepresence devices to register with, make calls to, and receive calls from the Cisco WebEx Telepresence service network. SIP message headers and body also contain references to IP addresses and ports.
- Session Initiation Protocol Application Layer Gateway (SIP ALG) is a firewall feature that extends NAT and PAT. Specifically, SIP ALG is the function in the router that inspects and modifies the embedded IP address and port information within SIP messages according to the NAT/PAT settings. The original intended purpose of SIP ALG was to allow voice/video SIP calls to work through the firewall. SIP ALG is also known as protocol fixup or protocol inspection (the terminology may vary depending on the firewall vendor).

Because many implementations of SIP ALG are incomplete and do not consistently apply SIP ALG rules to all SIP messages, these implementations are not robust enough to allow voice/video calls to work seamlessly. Due to this fairly common inadequacy, Cisco recommends that SIP ALG be disabled on the customer firewall that serves Cisco WebEx Telepresence.

Example of SIP ALG Operation

In this example, 10.10.10.12 is the private IP address of the customer device and 128.107.225.117 is its public IP address. The below example compares a SIP INVITE, sent by the device from the perspective of the Cisco WebEx Telepresence service network, with SIP ALG enabled and disabled.



SIP ALG ON

```
INVITE sip:4085157443@alpha.callway.net S
Via: SIP/2.0/TCP
128.107.225.117:1047;branch=z9hG4bK617
Call-ID: eeb84dc183dbf556@10.10.10.12
CSeq: 100 INVITE
Contact: <sip:4087151519@128.107.225.117
From: <sip:4087151519@alpha.callway.net>
To: <sip:4085157443@alpha.callway.net>
Max-Forwards: 70
Route: <sip:206.16.253.237;lr>
Allow: INVITE,ACK,CANCEL,BYE,UPDATE,INF
User-Agent: TANDBERG/515 (TC4.1.0.24701
Supported: replaces,100rel,timer,gruu,path,o
Session-Expires: 1800
Content-Type: application/sdp
Content-Length: 687

v=0
o=tandberg 6 1 IN IP4 10.10.10.12
s=-
c=IN IP4 128.107.225.117
b=AS:1920
t=0 0
```

SIP ALG OFF

```
INVITE sip:4085157443@206.16.253.237:50
Via: SIP/2.0/TCP 10.10.10.12:5060;branch=
Call-ID: e617afbbb14903f7@10.10.10.12
CSeq: 102 INVITE
Contact: <sip:4087151519@10.10.10.12:50
From: <sip:4087151519@alpha.callway.net
To: <sip:4085157443@alpha.callway.net>;t
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,BYE,UPDATE,IN
User-Agent: TANDBERG/515 (TC4.1.0.2470
Supported: replaces,100rel,timer,gruu,path,
Session-Expires: 1800;refresher=uac
Min-SE: 90
Content-Type: application/sdp
Content-Length: 2361

v=0
o=tandberg 5 2 IN IP4 10.10.10.12
s=-
c=IN IP4 10.10.10.12
b=AS:1920
t=0 0
```

- The above example shows that, when SIP ALG is on, the customer NAT device performs the following translations:
  - Translates the IP address within the SIP contact header to the device public IP address based on NAT/PAT rules.
  - Translates the IP address embedded in the **c= line** within the Session Description Protocol (SDP) to the corresponding public IP address.

- With SIP ALG off, the customer NAT device does not translate the IP address within any of the contact headers or the SDP, as shown above.
  - o Allows the Cisco WebEx Telepresence service network to manage and perform all of the necessary SIP-specific translations, which is the desired behavior.

Solution - Disabling SLP ALG on the Customer Firewall

Because SIP ALG may interfere with the proper operation of Cisco WebEx Telepresence, it should be disabled.

Note: Be aware that the steps that are required to disable SIP ALG will differ depending on the type of firewall that is used. Cisco recommends that you refer to your specific product documentation before making any changes.

Below are the steps to follow to disable SIP ALG on some of the more common firewall types.

Cisco IOS Routers

Step Number	Description
Step 1	Execute global disable sip inspection on your Cisco IOS device by entering the following commands: ios_router# ios_router#**conf t** Enter configuration commands, one per line. End with CNTL/Z. ios_router(config)# ios_router(config)#**no ip nat service sip tcp port 5060** ios_router(config)#**do show run | inc nat service sip** no ip nat service sip tcp port 5060 ios_router(config)#

Netgear

Step Number	Description
Step 1	Navigate to the **Advanced > WAN Setup** menu.
Step 2	Uncheck the **Disable SIP ALG** option.

Cisco ASA CLI (Example uses 5505 and asa824-k8.bin)

Step Number	Description
Step 1	Disable SIP ALG/inspection within the policy-map that is being used. Policy-maps may be applied either globally or to an interface in the Adaptive Security Appliance (ASA) firewall (or both).
Step 2	To check where the policy-map is applied, issue the following command: ASA# **show run | inc service-policy**

	service-policy global_policy global

The above configuration uses a globally applied policy-map.

For an example of disabling SIP inspection under the global-policy policy-map applied at the global level, see the below configuration:

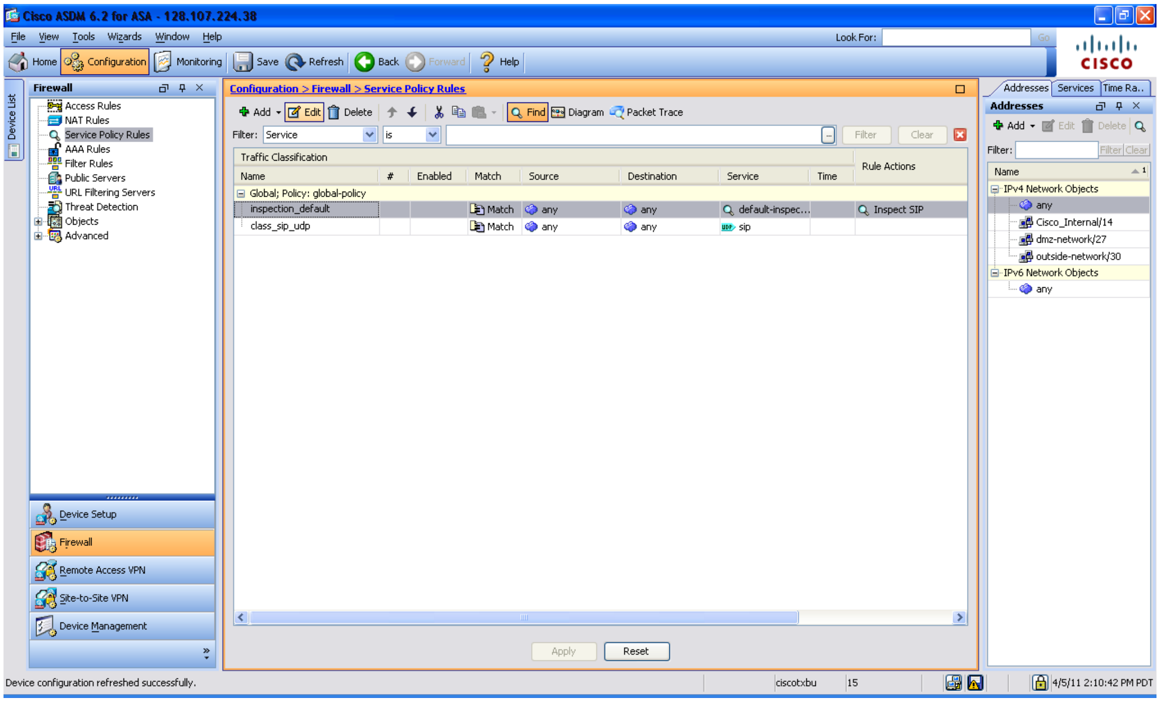
```
ASA#
ASA# conf t
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# no inspect sip
ASA(config-pmap-c)#end
ASA# show run | inc policy-map global-policy|inspect sip
policy-map global-policy
```

To “clear xlate” on your ASA and clear the inspection cache, enter the following command:

```
ASA# clear xlate local <callway_endpoint_private_ip>
```

Cisco ASA SDM (Example uses asa824-k8.bin, and asdm-625.bin)

Step Number	**Description**
Step 1	From a web browser, open https://ip_of_your_asa/admin.
Step 2	Click **Run ADSM**
Step 3	Navigate to **Configuration > Firewall > Service Policy Rules**
Step 4	Select **policy**; then, click **Edit**



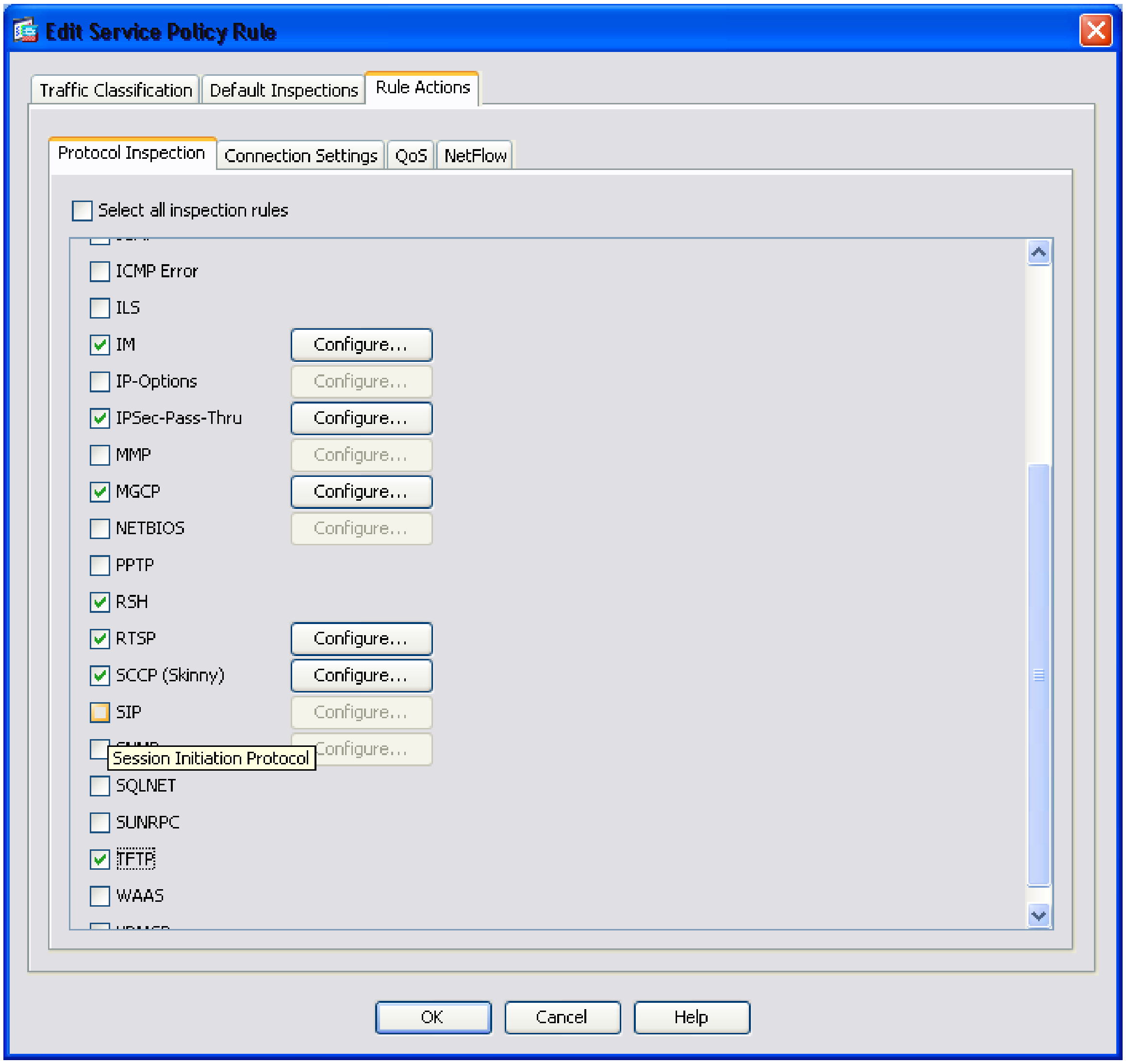
Configuration > Firewall > Service Policy Rules

Filter: Service is

Traffic Classification								Rule Actions
Name	#	Enabled	Match	Source	Destination	Service	Time	
Global; Policy: global-policy								
inspection_default			Match	any	any	default-inspec...		Inspect SIP
class_sip_udp			Match	any	any	sip		

Device configuration refreshed successfully. ciscotxbu 15 4/5/11 2:10:42 PM PDT

Step Number	Description
Step 5	Select the **Rule Actions** tab, as shown below
Step 6	Make sure that **SIP** is *not* checked
Step 7	Click **OK**



Edit Service Policy Rule

□ Select all inspection rules

- □ ICMP Error
- □ ILS
- ☑ IM — Configure...
- □ IP-Options — Configure...
- ☑ IPSec-Pass-Thru — Configure...
- □ MMP — Configure...
- ☑ MGCP — Configure...
- □ NETBIOS — Configure...
- □ PPTP
- ☑ RSH
- ☑ RTSP — Configure...
- ☑ SCCP (Skinny) — Configure...
- □ SIP — Configure...
- □ SNMP — Configure...
- □ SQLNET
- □ SUNRPC
- ☑ TFTP
- □ WAAS

Session Initiation Protocol