Troubleshoot Media Failure for Calls Over Expressways When SIP Inspection Is Turned On

Contents

Introduction

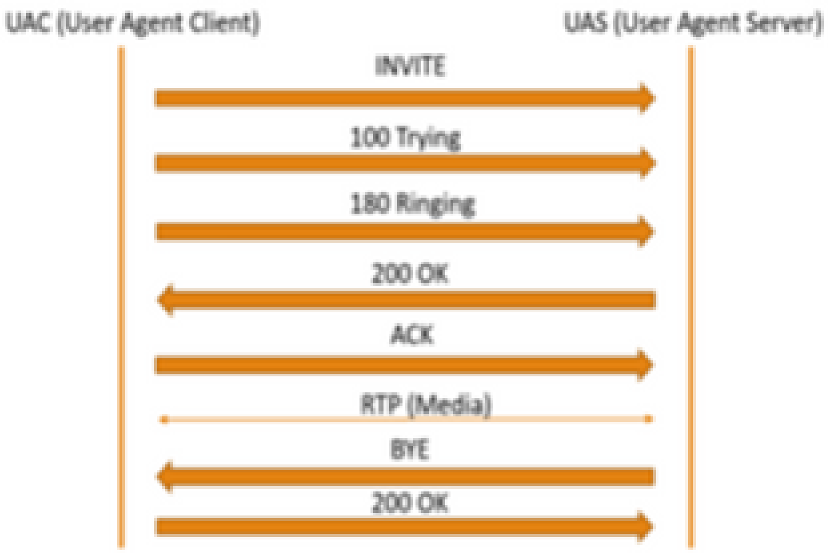
This document describes how to disable Session Initiation Protocol (SIP) inspection on Adaptive Security Appliance (ASA) firewalls.

Background Information

The purpose of SIP inspection is to provide address translation in the SIP header and body in order to allow for the dynamic opening of ports at the time of SIP signaling. SIP inspection is an extra layer of protection that does not expose internal IP’s to the external network when you make calls from inside the network to the internet. For example, in a Business-to-Business call from a device registered to the Cisco Unified Communications Manager (CUCM) through the Expressway-C and to the Expressway-E dialing a different domain, that private IP address in the SIP Header is translated to the IP of your firewall. Many symptoms can arise with ASA that inspect SIP signaling, creating call failures and one-way audio or video.

Media Failure for Calls Over Expressways When SIP Inspection Is Turned On

In order for the calling party to decipher where to send the media to, it sends what it expects to receive in a Session Description Protocol (SDP) at the time of the SIP negotiation for both audio and video. In an Early Offer scenario, it sends media based on what it received in the 200 OK as shown in the image.



When SIP Inspection is turned on by an ASA, the ASA inserts its IP address either in the c parameter of the SDP (connection information in order to return calls to) or the SIP Header. Here is an example of what a failed call looks like when SIP Inspection is turned on:

```
SIP INVITE:

|INVITE sip:7777777@domain SIP/2.0

Via: SIP/2.0/TCP *EP IP*:5060

Call-ID: faece8b2178da3bb

CSeq: 100 INVITE

Contact: <sip:User@domain;

From: "User" <sip:User@domain >;tag=074200d824ee88dd

To: <sip:7777777@domain>

Max-Forwards: 15

Allow: INVITE,ACK,CANCEL,BYE,INFO,OPTIONS,REFER,NOTIFY

User-Agent: TANDBERG/775 (MCX 4.8.12.18951) - Windows

Supported: replaces,timer,gruu

Session-Expires: 1800

Content-Type: application/sdp

Content-Length: 1961
```

Here the firewall inserts its own public IP address and replaces the domain in the header of the acknowledge (ACK) message:

```
SIP ACK:

|ACK sip:7777777@*Firewall IP 5062;transport=tcp SIP/2.0
```

```
Via: SIP/2.0/TLS +Far End IP*:7001

Call-ID: faece8b2178da3bb

CSeq: 100 ACK

From: "User" <sip:User@domain>;tag=074200d824ee88dd

To: <sip:7778400@domain>;tag=1837386~f30f6167-11a6-4211-aed0-632da1f33f58-61124999

Max-Forwards: 68

Allow: INVITE,ACK,CANCEL,BYE,INFO,OPTIONS,REFER,NOTIFY

User-Agent: TANDBERG/775 (MCX 4.8.12.18951) - Windows

Supported: replaces,100rel,timer,gruu

Content-Length: 0
```

If the Public IP address of the firewall is inserted anywhere within this SIP signaling process, calls fail. There could also be no ACK sent back from the User Agent Client if SIP inspection is turned on, which thereby results in call failure.

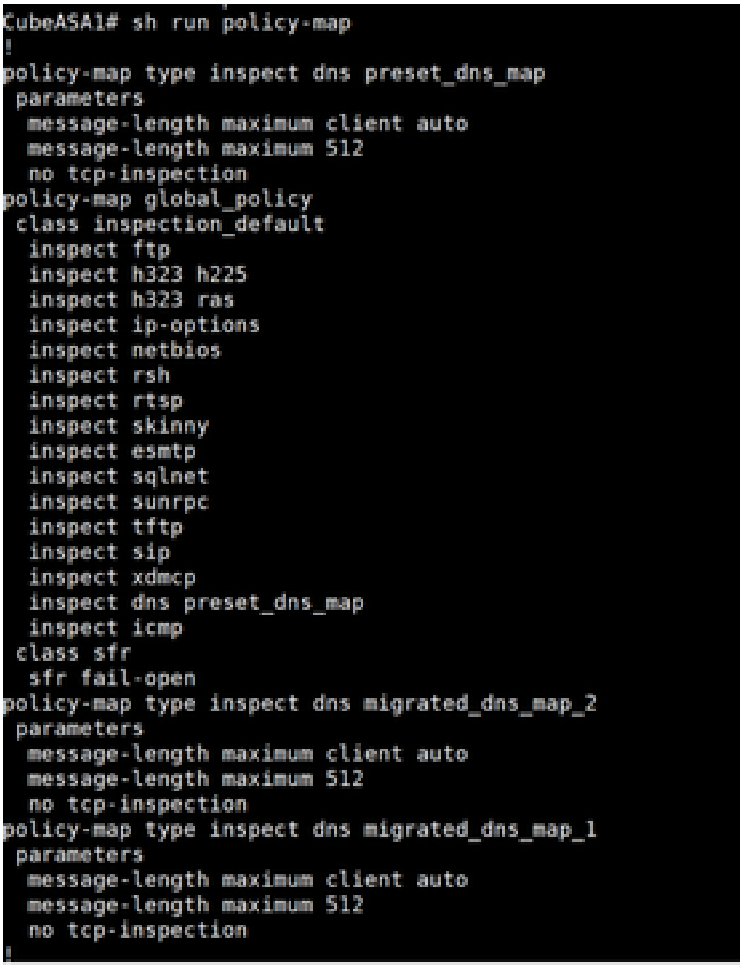
Solution

In order to disable SIP Inspection on an ASA Firewall:

Step 1. Log into the CLI of the ASA.

Step 2. Run command **show run policy-map**.

Step 3. Verify that inspect sip is under the policy map global-policy list as shown in the image.



```
CubeASA1# sh run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect dns preset_dns_map
  inspect icmp
 class sfr
  sfr fail-open
policy-map type inspect dns migrated_dns_map_2
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
!
```

Step 4. If it is, run these commands:

CubeASA1# policy-map global_policy

CubeASA1# class inspection_default

CubeASA1# no inspect sip

Related Information

- It is not recommended to use SIP inspection on an ASA firewall (Page 74); https://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-11/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-11-4.pdf
- More information regarding SIP insepction can be found here; https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/firewall/asa-99-firewall-config/inspect-voicevideo.pdf
- **Technical Support & Documentation - Cisco Systems**