打开SIP检测时，排除Expressway呼叫的介质故障

目录

[简介](#)
[背景信息](#)
[打开SIP检测时Expressway呼叫的媒体故障](#)
[解决方案](#)
[相关信息](#)

简介

本文档介绍如何在自适应安全设备(ASA)防火墙上禁用会话初始协议(SIP)检查。

背景信息

SIP检查的目的是在SIP报头和正文中提供地址转换，以便在SIP信令时允许动态打开端口。SIP检测是一种额外的保护层，当您从网络内部呼叫互联网时，它不会向外部网络暴露内部IP。例如，在从通过Expressway-C注册到Cisco Unified Communications Manager(CUCM)的设备到Expressway-E拨号到不同域的企业到企业呼叫中，SIP报头中的私有IP地址将转换为防火墙的IP。许多症状可能来自检查SIP信令的ASA，导致呼叫失败和一音频或视频。

打开SIP检测时Expressway呼叫的媒体故障

为了使主叫方解密将媒体发送到何处，它会发送在音频和视频的SIP协商时在会话描述协议(SDP)中预期接收的内容。在Early Offer场景中，它根据在200 OK时收到的内容发送媒体，如图所示。

当ASA打开SIP检查时，ASA会在SDP的c参数（返回呼叫的连接信息）或SIP报头中插入其IP地址

。以下是启用SIP检测时失败呼叫的示例：

```
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
```

在此，防火墙插入其自己的公有IP地址并替换确认(ACK)消息报头中的域：

```
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
```

如果防火墙的公有IP地址插入此SIP信令进程中的任何位置，则呼叫失败。如果SIP检测打开，则也

不会从用户代理客户端发回ACK，从而导致呼叫失败。

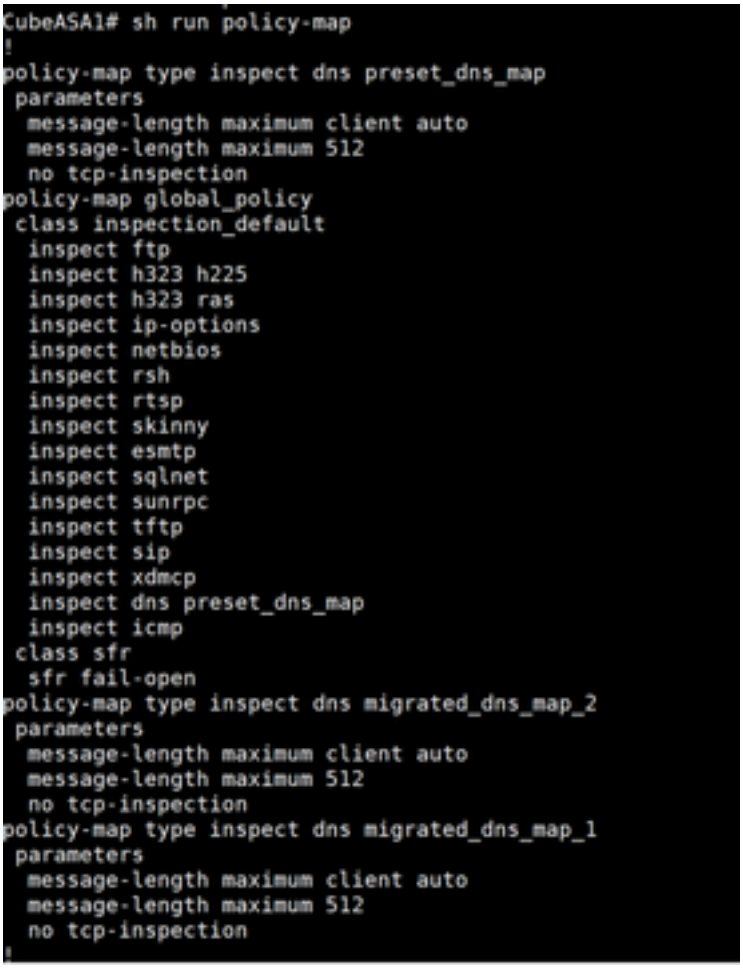
解决方案

要在ASA防火墙上禁用SIP检测，请执行以下操作：

步骤1.登录ASA的CLI。

步骤2.运行命令**show run policy-map**。

步骤3.验证检查sip是否在策略映射全局策略列表下，如图所示。



```
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
!
```

步骤4.如果是，请运行以下命令：

CubeASA1# policy-map global_policy

CubeASA1#类inspection_default

CubeASA1# no inspect sip

相关信息

- 不建议在ASA防火墙上使用SIP检测（第74页）；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
- 有关SIP检测的详细信息，请点击此处；https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/firewall/asa-99-firewall-config/inspect-voicevideo.pdf
- **技术支持和文档 - Cisco Systems**