開啟SIP檢查時，排除Expressway呼叫的介質故障

目錄

簡介

本檔案介紹如何在調適型安全裝置(ASA)防火牆上停用作業階段啟始通訊協定(SIP)檢查。

背景資訊

SIP檢查的目的是在SIP報頭和正文中提供地址轉換，以便允許在SIP信令時動態開啟埠。SIP檢查是額外的保護層，當您從網路內部呼叫到Internet時，不會將內部IP暴露給外部網路。例如，在從通過Expressway-C註冊到Cisco Unified Communications Manager(CUCM)的裝置到Expressway-E撥打其他域的業務到業務呼叫中，SIP報頭中的專用IP地址會轉換為防火牆的IP。檢查SIP信令、建立呼叫失敗和單向音訊或影片的ASA可能會出現許多症狀。

開啟SIP檢查時Expressway呼叫的媒體故障

為了讓主叫方破解將媒體傳送到何處，在音訊和影片的SIP協商時，主叫方會傳送它期望在會話描述協定(SDP)中接收的內容。在Early Offer場景中，它會根據在200 OK中接收的內容傳送媒體，如下圖所示。

當ASA開啟SIP檢測時，ASA會將其IP地址插入SDP的c引數（連線資訊以將呼叫返回到）或SIP報頭。以下是啟用SIP檢測時失敗呼叫的示例：

```
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
```

在此處，防火牆插入其自己的公用IP地址，並替換確認(ACK)消息的報頭中的域：

```
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
```

如果防火牆的公共IP地址插入此SIP信令流程中的任何位置，呼叫將失敗。如果啟用SIP檢查，則可能也沒有從使用者代理客戶端傳送回ACK，從而導致呼叫失敗。

解決方案

要在ASA防火牆上禁用SIP檢測，請執行以下操作：

步驟1.登入ASA的CLI。

步驟2.運行命令**show run policy-map**。

步驟3.驗證檢查sip是否位於策略對映全域性策略清單下，如下圖所示。

```
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
!
```

步驟4.如果是，請運行以下命令：

CubeASA1# policy-map global_policy

CubeASA1#類inspection_default

CubeASA1# no inspect sip

相關資訊

- 建議不要在ASA防火牆上使用SIP檢測（第74頁）；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
- 有關SIP檢查的更多資訊，請訪問此處；https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/firewall/asa-99-firewall-config/inspect-voicevideo.pdf
- **技術支援與文件 - Cisco Systems**