SIP 검사가 설정된 경우 Expressway를 통한 통화에 대한 미디어 실패 문제 해결

목차

소개

이 문서에서는 ASA(Adaptive Security Appliance) 방화벽에서 SIP(Session Initiation Protocol) 검사를 비활성화하는 방법에 대해 설명합니다.

배경 정보

SIP 검사의 목적은 SIP 신호 처리 시 동적으로 포트를 열 수 있도록 SIP 헤더 및 본문에 주소 변환을 제공하는 것입니다.SIP 검사는 네트워크 내부에서 인터넷으로 전화를 걸 때 외부 네트워크에 내부 IP를 노출시키지 않는 추가적인 보호 계층입니다.예를 들어 Expressway-C를 통해 Cisco Unified Communications Manager(CUCM)에 등록된 디바이스에서 Business-to-Business로 전화하거나 다른 도메인을 다이얼하는 Expressway-E로 전화하는 경우 SIP 헤더의 개인 IP 주소가 방화벽의 IP로 변환됩니다. SIP 신호 처리를 검사하고 통화 실패 및 단방향 오디오 또는 비디오를 생성하는 ASA에서 많은 증상이 발생할 수 있습니다.

SIP 검사가 켜져 있을 때 Expressway를 통한 통화에 대한 미디어 실패

발신자가 미디어를 어디로 보낼지 파악하기 위해 오디오 및 비디오에 대한 SIP 협상 시 SDP(Session Description Protocol)에서 수신할 것으로 예상되는 항목을 전송합니다.Early Offer 시나리오에서는 이미지에 표시된 것처럼 200OK에서 받은 내용을 기반으로 미디어를 전송합니다.

ASA에서 SIP Inspection을 켜면 ASA는 SDP의 c 매개 변수(통화를 반환하기 위한 연결 정보) 또는 SIP 헤더에 IP 주소를 삽입합니다.다음은 SIP 검사가 켜져 있을 때 실패한 통화의 예입니다.

```
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
```

여기서 방화벽은 자신의 공용 IP 주소를 삽입하고 승인(ACK) 메시지 헤더의 도메인을 교체합니다.

```
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
```

방화벽의 공용 IP 주소가 이 SIP 신호 처리 프로세스 내의 아무 곳에나 삽입되면 통화가 실패합니다 .SIP 검사가 켜져 있으면 사용자 에이전트 클라이언트에서 다시 보낸 ACK가 없을 수 있으므로 통화 오류가 발생할 수 있습니다.

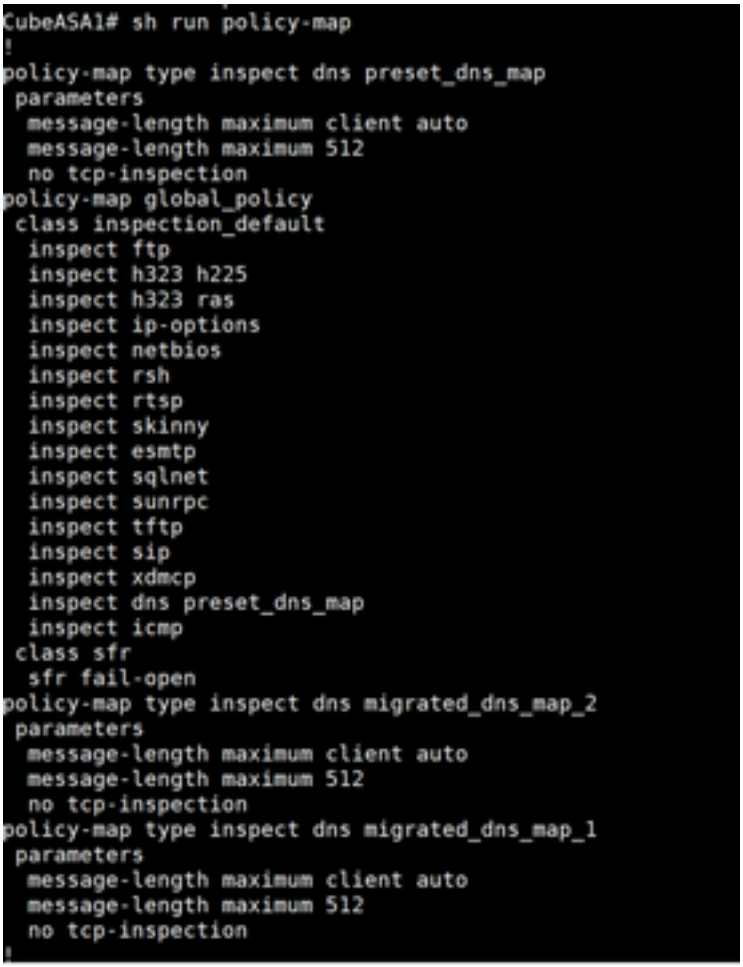
솔루션

ASA 방화벽에서 SIP 검사를 비활성화하려면

1단계. ASA의 CLI에 로그인합니다.

2단계. show **run policy-map 명령을 실행합니다**.

3단계. 이미지에 표시된 대로 inspect sip가 정책 맵 글로벌 정책 목록 아래에 있는지 확인합니다.



4단계. 이 경우 다음 명령을 실행합니다.

CubeASA1# policy-map global_policy

CubeASA1# 클래스 inspection_default

CubeASA1# 검사 sip 없음

관련 정보

- ASA 방화벽에서 SIP 검사를 사용하지 않는 것이 좋습니다(74페이지). 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
- SIP 검사에 대한 자세한 내용은 여기를 참조하십시오 .https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/firewall/asa-99-firewall-config/inspect-voicevideo.pdf
- **기술 지원 및 문서 – Cisco Systems**