Fehlerbehebung bei Medienausfällen für Anrufe über Expressways bei eingeschalteter SIP-Inspektion

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die SIP-Inspektion (Session Initiation Protocol) auf ASA-Firewalls (Adaptive Security Appliance) deaktiviert wird.

Hintergrundinformationen

Die SIP-Prüfung dient der Adressumwandlung in den SIP-Header und -Text, um das dynamische Öffnen von Ports zum Zeitpunkt der SIP-Signalisierung zu ermöglichen. SIP-Inspektion ist eine zusätzliche Schutzebene, die keine internen IPs für das externe Netzwerk verfügbar macht, wenn Sie Anrufe vom Netzwerk zum Internet tätigen. Beispielsweise wird bei einem Business-to-Business-Anruf von einem Gerät, das beim Cisco Unified Communications Manager (CUCM) über den Expressway-C und beim Expressway-E registriert ist und eine andere Domäne wählt, diese private IP-Adresse im SIP-Header in die IP-Adresse Ihrer Firewall übersetzt. Bei ASA-Geräten können zahlreiche Symptome auftreten, die die SIP-Signalisierung überprüfen und Anrufausfälle sowie unidirektionale Audio- oder Videofunktionen verursachen.

Medienfehler für Anrufe über Expressways bei eingeschalteter SIP-Inspektion

Damit der anrufende Teilnehmer feststellen kann, an wen die Medien gesendet werden sollen, sendet er zum Zeitpunkt der SIP-Aushandlung sowohl für Audio als auch für Video das, was er von einem Session Description Protocol (SDP) erwartet. Bei einem Frühangebot werden Medien basierend auf dem im 200 OK erhaltenen Inhalt gesendet, wie im Bild gezeigt.

Wenn die SIP-Inspektion von einer ASA aktiviert wird, fügt die ASA ihre IP-Adresse entweder im c-Parameter des SDP (Verbindungsinformationen zur Rückgabe von Anrufen) oder im SIP-Header ein. Im Folgenden sehen Sie ein Beispiel für einen fehlgeschlagenen Anruf, wenn die SIP-Inspektion aktiviert ist:

```
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
```

Hier fügt die Firewall ihre eigene öffentliche IP-Adresse ein und ersetzt die Domäne im Header der Bestätigungsnachricht (ACK):

```
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
```

Wenn die öffentliche IP-Adresse der Firewall an einer beliebigen Stelle innerhalb dieses SIP-Signalisierungsprozesses eingefügt wird, schlagen Anrufe fehl. Wenn die SIP-Inspektion aktiviert ist, kann es auch sein, dass keine ACK vom Benutzer-Agent-Client zurückgesendet wird, was zu einem Anrufausfall führt.

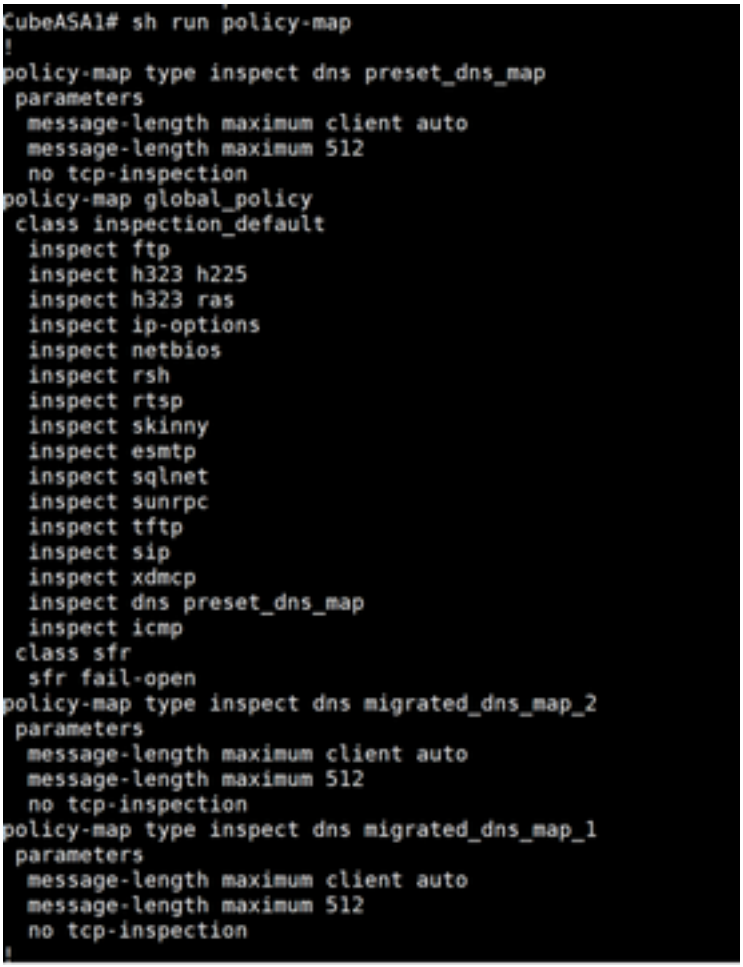
Lösung

So deaktivieren Sie die SIP-Inspektion auf einer ASA-Firewall:

Schritt 1: Melden Sie sich bei der CLI der ASA an.

Schritt 2: Führen Sie den Befehl **show run policy-map aus**.

Schritt 3: Stellen Sie sicher, dass inspect sip unter der globalen Richtlinienzuweisungsliste aufgeführt ist, wie im Bild gezeigt.



Schritt 4: Wenn ja, führen Sie folgende Befehle aus:

CubeASA1#-Richtlinienzuweisung global_policy

CubeASA1# class Inspection_default

CubeASA1# no inspect sip

Zugehörige Informationen

- Es wird nicht empfohlen, SIP-Inspektion auf einer ASA-Firewall zu verwenden (Seite 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
- Weitere Informationen zur SIP-Inspektion finden Sie hier. https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/firewall/asa-99-firewall-config/inspect-voicevideo.pdf
- **Technischer Support und Dokumentation - Cisco Systems**