Probleemoplossing bij media-falen voor oproepen via expressies wanneer SIP-inspectie is ingeschakeld

Inhoud

Inleiding

Dit document beschrijft hoe u Session Initiation Protocol (SIP)-inspectie uit kunt schakelen voor adaptieve security applicatie (ASA) firewalls.

Achtergrondinformatie

Het doel van de SIP-inspectie is adresomzetting in de SIP-kop en -instantie te bieden, zodat poorten op het moment van SIP-signalering dynamisch kunnen worden geopend. SIP-inspectie is een extra beschermingslaag die geen interne IP's aan het externe netwerk blootstelt wanneer u vanuit het netwerk naar het internet belt. In een Business-to-Business-gesprek van een apparaat dat is geregistreerd voor Cisco Unified Communications Manager (CUCM) via de sneltoets-C en het sneldraaien van een ander domein, wordt dat privé IP-adres in de SIP-header vertaald naar IP van uw firewall. Veel symptomen kunnen zich voordoen met ASA die SIP-signalering inspecteert, oproepen-uitvallen en audio- of video-eenrichtingen creëert.

Mediafouten bij oproepen via expressies wanneer SIP-inspectie wordt ingeschakeld

Om de oproepende partij te laten ontcijferen waar de media naar moeten worden gestuurd, stuurt zij wat zij verwacht te ontvangen in een Session Description Protocol (SDP) op het tijdstip van de SIP-onderhandeling voor zowel audio als video. In een scenario voor een vroege aanbieding stuurt het media die zijn gebaseerd op wat het in 2000 OK heeft ontvangen zoals in de afbeelding wordt getoond.

Wanneer de SIP-inspectie door een ASA is ingeschakeld, voegt de ASA zijn IP-adres in de c-parameter van de SDP (verbindingsinformatie om oproepen naar terug te sturen) of de SIP-header toe. Hier is een voorbeeld van hoe een mislukt gesprek eruit ziet wanneer SIP-inspectie wordt ingeschakeld:

```
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 voegt de firewall zijn eigen openbare IP-adres in en vervangt u het domein in de header van het ACK-bericht:

```
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
```

Als het openbare IP-adres van de firewall binnen dit SIP-signaalproces ergens is ingevoegd, mislukt de vraag. Er kan ook geen ACK worden verzonden vanuit de client van de gebruikersagent als de SIP-inspectie is ingeschakeld, wat resulteert in een storing van de oproep.

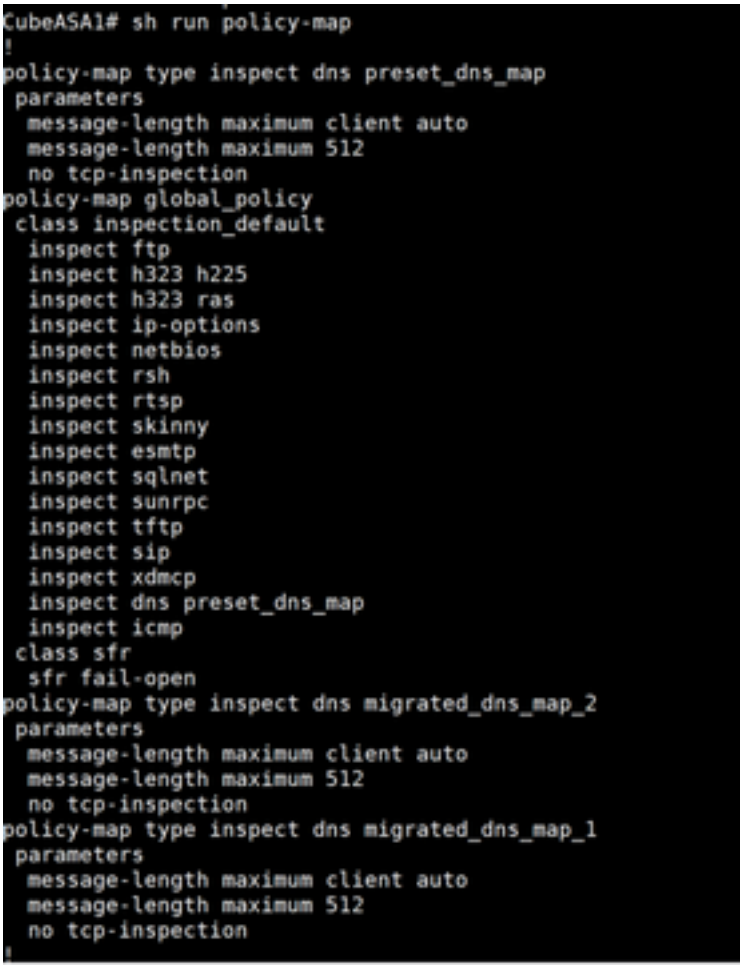
Oplossing

Zo schakelt u SIP-inspectie op een ASA-firewall uit:

Stap 1. Meld u aan bij de CLI van de ASA.

Stap 2. Laat de opdracht uitvoeren om beleid-kaart uit te voeren.

Stap 3. Controleer dat de optie VIP-inspectie onder de algemene beleidslijst staat zoals in de afbeelding.



Stap 4. Als dit het geval is, voert u deze opdrachten uit:

CubeASA1# beleids-map global_policy

CubeASA1# class inspection_default

CubeASA1# geen inspectie-stap

Gerelateerde informatie

- Het wordt niet aanbevolen om SIP-inspectie op een ASA-firewall te gebruiken (pagina 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
- Hier vindt u meer informatie over de SIP-inspectie; https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/firewall/asa-99-firewall-config/inspect-voicevideo.pdf
- **Technische ondersteuning en documentatie – Cisco Systems**