Resolución de problemas de fallo de medios para llamadas a través de Expressway cuando se activa la inspección SIP

Contenido

Introducción

Este documento describe cómo deshabilitar la inspección del protocolo de inicio de sesión (SIP) en los firewalls Adaptive Security Appliance (ASA).

Antecedentes

El propósito de la inspección de SIP es proporcionar la traducción de direcciones en el encabezado y cuerpo de SIP para permitir la apertura dinámica de puertos en el momento de la señalización SIP. La inspección SIP es una capa adicional de protección que no expone las IP internas a la red externa cuando realiza llamadas desde dentro de la red a Internet. Por ejemplo, en una llamada de empresa a empresa desde un dispositivo registrado a Cisco Unified Communications Manager (CUCM) a través de Expressway-C y a Expressway-E marcando un dominio diferente, esa dirección IP privada en el encabezado SIP se traduce a la IP del firewall. Pueden surgir muchos síntomas con ASA que inspeccionan la señalización SIP, crean fallos de llamadas y audio o vídeo unidireccional.

Fallo de medios para llamadas a través de Expressway cuando se activa la inspección SIP

Para que la parte que llama pueda decidir a dónde enviar los medios, envía lo que espera recibir en un protocolo de descripción de sesión (SDP) en el momento de la negociación SIP para audio y vídeo. En un escenario de oferta anticipada, envía medios basados en lo que recibió en 200 OK, como se muestra en la imagen.

Cuando una ASA enciende la inspección de SIP, el ASA inserta su dirección IP en el parámetro c de la SDP (información de conexión para devolver llamadas a) o en el encabezado SIP. A continuación se muestra un ejemplo de cómo se ve una llamada fallida cuando se activa la inspección SIP:

```
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
```

Aquí el firewall inserta su propia dirección IP pública y reemplaza el dominio en el encabezado del mensaje de reconocimiento (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
```

Si la dirección IP pública del firewall se inserta en cualquier lugar dentro de este proceso de señalización SIP, las llamadas fallan. Tampoco puede haber ningún ACK enviado de vuelta desde el Cliente de agente de usuario si se activa la inspección SIP, lo que da como resultado una falla de llamada.

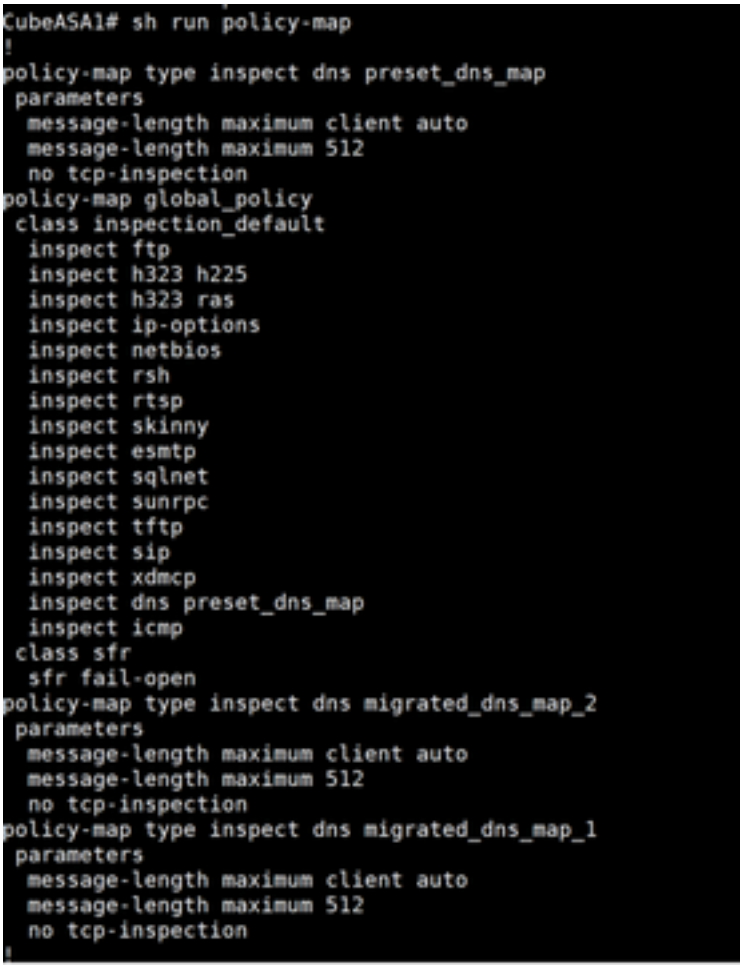
Solución

Para inhabilitar la inspección SIP en un firewall ASA:

Paso 1. Inicie sesión en la CLI del ASA.

Paso 2. Ejecute el comando **show run policy-map**.

Paso 3. Verifique que inspect sip esté en la lista de políticas globales del mapa de políticas como se muestra en la imagen.



Paso 4. Si es así, ejecute estos comandos:

CubeASA1# policy-map global_policy

CubeASA1# class inspection_default

CubeASA1# sin inspección sip

Información Relacionada

- No se recomienda utilizar la inspección SIP en un firewall ASA (página 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
- Puede encontrar más información sobre la inspección SIP aquí; https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/firewall/asa-99-firewall-config/inspect-voicevideo.pdf
- **Soporte Técnico y Documentación - Cisco Systems**