

Falla de medios del Troubleshooting para las llamadas sobre las autopistas cuando se gira el examen del SORBO

Contenido

[Introducción](#)

[Antecedentes](#)

[Falla de medios para las llamadas sobre las autopistas cuando se gira el examen del SORBO](#)

[Solución](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo inhabilitar el examen del Session Initiation Protocol (SIP) en los Firewall adaptantes del dispositivo de seguridad (ASA).

Antecedentes

El propósito del examen del SORBO es proporcionar la traducción de la dirección en la encabezado y el cuerpo del SORBO para tener en cuenta la apertura dinámica de los puertos a la hora de la señalización del SORBO. El examen del SORBO es una capa adicional de protección que no exponga los IP internos a la red externa cuando usted hace las llamadas por dentro de la red a Internet. Por ejemplo, en una llamada interempresarial de un dispositivo registró a las Comunicaciones unificadas de Cisco al administrador (CUCM) con Expressway-C y a Expressway-e que marca un diverso dominio, ese IP Address privado en la encabezado del SORBO se traduce al IP de su Firewall. Muchos síntomas pueden presentarse con el ASA que examinan la señalización del SORBO, creando las fallas de llamada y audio unidireccional o vídeo.

Falla de medios para las llamadas sobre las autopistas cuando se gira el examen del SORBO

Para que la parte llamadora descifre donde enviar los media a, envía lo que espera recibir en un protocolo session description (SDP) a la hora de la negociación del SORBO para el audio y el vídeo. En un escenario temprano de la oferta, envía los media basados en lo que recibió en la AUTORIZACIÓN 200 tal y como se muestra en de la imagen.



Cuando el examen del SORBO es girado por un ASA, el ASA inserta su dirección IP en el parámetro c del SDP (información de conexión para volver las llamadas a) o de la encabezado del SORBO. Aquí está un ejemplo de una que llamada fallida parece cuando se gira el examen del SORBO:

```

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 a su propio IP Address público y substituye el dominio en la encabezado del mensaje del 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 insertan al IP Address público del Firewall dondequiera dentro de este proceso de señalización del SORBO, las llamadas fallan. No podría también haber ACK devuelto del cliente del agente de usuario si se gira el examen del SORBO, que de tal modo da lugar a la falla de llamada.

Solución

Para inhabilitar el examen del SORBO en un Firewall ASA:

Paso 1. Registro en el CLI del ASA.

Paso 2. Ejecute el directiva-**mapa del** comando show run.

Paso 3. Verifique que examina el sorbo está conforme a la lista de la política global de la correspondencia de políticas tal y como se muestra en de la imagen.

```

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
!

```

Paso 4. Si es, funcione con estos comandos:

Global_policy del directiva-mapa CubeASA1#

Inspection_default de la clase CubeASA1#

CubeASA1# ningunos examinan el sorbo

Información Relacionada

- No se recomienda para utilizar el examen del SORBO 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
- Más información con respecto al insepction del SORBO se puede encontrar 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](#)