Dépanner les défaillances de support pour les appels sur les autoroutes lorsque l'inspection SIP est activée

Contenu

Introduction

Ce document décrit comment désactiver l'inspection SIP (Session Initiation Protocol) sur les pare-feu ASA (Adaptive Security Appliance).

Informations générales

L'inspection SIP a pour but de fournir la traduction d'adresses dans l'en-tête et le corps SIP afin de permettre l'ouverture dynamique des ports au moment de la signalisation SIP. L'inspection SIP est une couche supplémentaire de protection qui n'expose pas les adresses IP internes au réseau externe lorsque vous passez des appels depuis l'intérieur du réseau vers Internet. Par exemple, dans un appel entre entreprises d'un périphérique enregistré auprès de Cisco Unified Communications Manager (CUCM) via l'Expressway-C et l'Expressway-E qui compose un domaine différent, cette adresse IP privée dans l'en-tête SIP est traduite en adresse IP de votre pare-feu. De nombreux symptômes peuvent survenir avec l'ASA qui inspecte la signalisation SIP, créant des pannes d'appel et un signal audio ou vidéo unidirectionnel.

Panne de support des appels sur les autoroutes lorsque l'inspection SIP est activée

Pour que l'appelant puisse déterminer où envoyer le support, il envoie ce qu'il attend de recevoir dans un protocole SDP (Session Description Protocol) au moment de la négociation SIP pour l'audio et la vidéo. Dans un scénario d'offre anticipée, il envoie le support en fonction de ce qu'il a reçu dans le 200 OK, comme l'illustre l'image.

Lorsque l'inspection SIP est activée par un ASA, l'ASA insère son adresse IP soit dans le paramètre c du SDP (informations de connexion afin de renvoyer les appels), soit dans l'en-tête SIP. Voici un exemple de l'état d'un appel en échec lorsqu'une inspection SIP est activée :

```
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
```

Ici, le pare-feu insère sa propre adresse IP publique et remplace le domaine dans l'en-tête du message accuser réception (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 l'adresse IP publique du pare-feu est insérée n'importe où dans ce processus de signalisation SIP, les appels échouent. Il peut également n'y avoir aucun ACK renvoyé par le client Agent utilisateur si l'inspection SIP est activée, ce qui entraîne une défaillance d'appel.

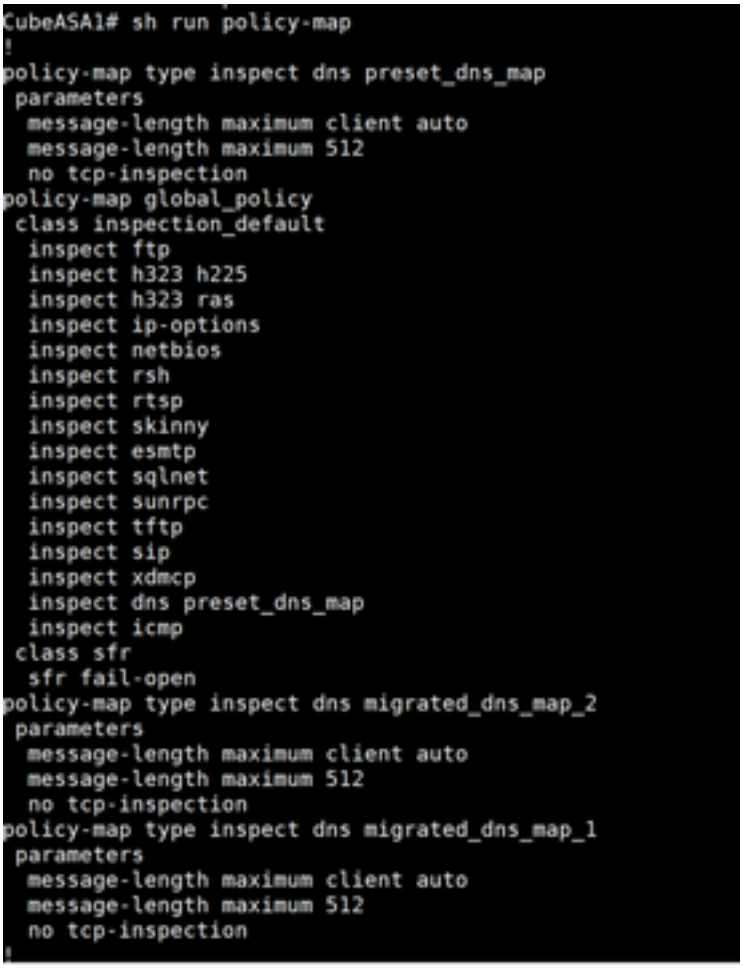
Solution

Afin de désactiver l'inspection SIP sur un pare-feu ASA :

Étape 1. Connectez-vous à l'interface de ligne de commande de l'ASA.

Étape 2. Exécutez la commande **show run policy-map**.

Étape 3. Vérifiez que inspect sip se trouve sous la liste des politiques globales de la carte de stratégie, comme l'illustre l'image.



Étape 4. Si tel est le cas, exécutez les commandes suivantes :

CubeASA1# policy-map global_policy

CubeASA1# class inspection_default

CubeASA1# no inspect sip

Informations connexes

- Il n'est pas recommandé d'utiliser l'inspection SIP sur un pare-feu ASA (page 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
- Pour plus d'informations sur l'inspection SIP, cliquez ici ; https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/firewall/asa-99-firewall-config/inspect-voicevideo.pdf
- **Support et documentation techniques - Cisco Systems**