Risoluzione dei problemi relativi agli errori dei supporti per le chiamate su Expressways quando il controllo SIP è attivato

Sommario

Introduzione

In questo documento viene descritto come disabilitare l'ispezione SIP (Session Initiation Protocol) sui firewall ASA (Adaptive Security Appliance).

Premesse

Lo scopo dell'ispezione SIP è fornire la conversione degli indirizzi nell'intestazione e nel corpo del SIP in modo da consentire l'apertura dinamica delle porte al momento della segnalazione SIP. L'ispezione SIP è un ulteriore livello di protezione che non espone gli IP interni alla rete esterna quando si effettuano chiamate dall'interno della rete a Internet. Ad esempio, in una chiamata business-to-business da un dispositivo registrato in Cisco Unified Communications Manager (CUCM) tramite Expressway-C e Expressway-E per un dominio diverso, l'indirizzo IP privato nell'intestazione SIP viene convertito nell'indirizzo IP del firewall. L'appliance ASA può presentare molti sintomi che ispezionano la segnalazione SIP, creando errori di chiamata e audio o video unidirezionale.

Errore del supporto per le chiamate su Expressways quando il controllo SIP è attivato

Per decidere a chi inviare i media, il chiamante invia ciò che prevede di ricevere in un SDP (Session Description Protocol) al momento della negoziazione SIP per audio e video. In uno scenario di offerta anticipata, invia i supporti in base a quanto ricevuto nel 2009 OK, come mostrato nell'immagine.

Quando l'ASA attiva l'ispezione SIP, inserisce il proprio indirizzo IP nel parametro c dell'SDP (informazioni sulla connessione per la restituzione delle chiamate) o nell'intestazione SIP. Di seguito è riportato un esempio di una chiamata non riuscita quando è attivata l'ispezione 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
```

In questo modo, il firewall inserisce il proprio indirizzo IP pubblico e sostituisce il dominio nell'intestazione del messaggio di conferma (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
```

Se l'indirizzo IP pubblico del firewall è inserito in qualsiasi punto del processo di segnalazione SIP, le chiamate hanno esito negativo. Inoltre, se l'ispezione SIP è attivata, non è possibile inviare un ACK al client dell'agente utente, con conseguente errore di chiamata.

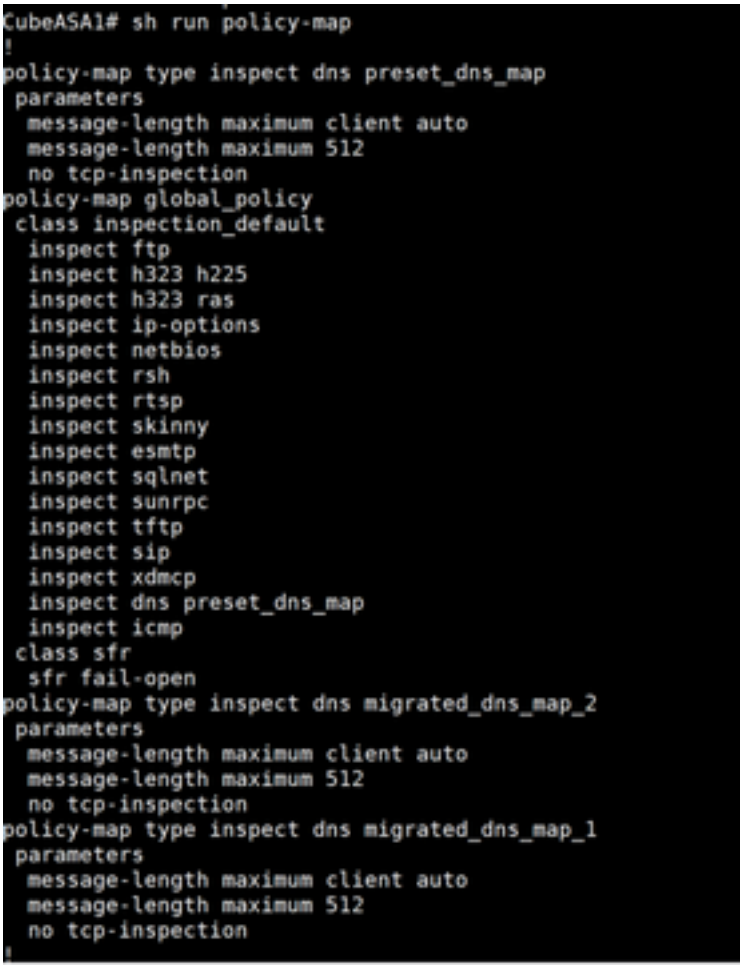
Soluzione

Per disabilitare l'ispezione SIP su un firewall ASA:

Passaggio 1. Accedere alla CLI dell'ASA.

Passaggio 2. Eseguire il comando **show run policy-map**.

Passaggio 3. Verificare che inspect sip sia incluso nell'elenco di criteri globali della mappa dei criteri, come mostrato nell'immagine.



Passaggio 4. In caso affermativo, eseguire i seguenti comandi:

CubeASA1# policy-map_global

CubeASA1# class_selection_default

CubeASA1# nessun sip di ispezione

Informazioni correlate

- Non si consiglia di usare l'ispezione SIP su un firewall ASA (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
- Maggiori informazioni sull'ispezione SIP sono disponibili qui; https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/firewall/asa-99-firewall-config/inspect-voicevideo.pdf
- **Documentazione e supporto tecnico – Cisco Systems**