SIPインスペクションがオンの場合のExpressway経由のコールのメディア障害のトラブルシューティング

内容

概要

このドキュメントでは、適応型セキュリティアプライアンス(ASA)ファイアウォールでSession Initiation Protocol(SIP)インスペクションを無効にする方法について説明します。

背景説明

SIPインスペクションの目的は、SIPシグナリング時にポートを動的にオープンできるようにするために、SIPヘッダーと本文にアドレス変換を提供することです。SIPインスペクションは、ネットワーク内部からインターネットにコールを発信するときに、内部IPを外部ネットワークに公開しない追加の保護層です。たとえば、Expressway-Cを介してCisco Unified Communications Manager(CUCM)に登録されたデバイスから別のドメインをダイヤルするExpressway-EへのBusiness-to-Business(B2B)コールでは、SIPヘッダーのプライベートIPアドレスがファイアウォールにに変換されます音声またはビデオの方法。

SIPインスペクションがオンの場合のExpressway経由のコールのメディア障害

発信側は、メディアの送信先を解読するために、音声とビデオの両方のSIPネゴシエーション時にセッション記述プロトコル(SDP)で受信すると想定するものを送信します。早期オファーのシナリオでは、図に示すように、200 OKで受信した内容に基づいてメディアを送信します。

ASAがSIPインスペクションをオンにすると、ASAはSDP（コールを返す接続情報）のcパラメータまたはSIPヘッダーのいずれかにIPアドレスを挿入します。SIPインスペクションをオンにすると、失敗したコールがどのように表示されるかの例を次に示します。

```
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
```

ここで、ファイアウォールは自身のパブリックIPアドレスを挿入し、確認応答(ACK)メッセージのヘッダー内のドメインを置き換えます。

```
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
```

ファイアウォールのパブリックIPアドレスがこのSIPシグナリングプロセス内のどこかに挿入されると、コールは失敗します。また、SIPインスペクションがオンの場合にユーザエージェントクライアントからACKが返信されず、コールが失敗する可能性があります。

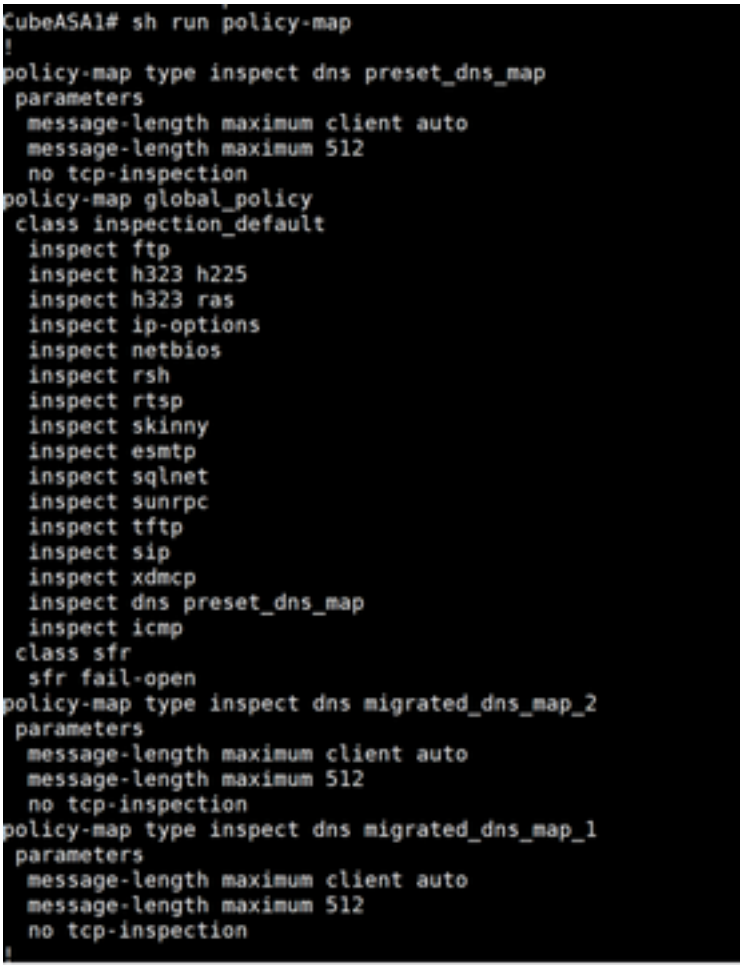
解決方法

ASAファイアウォールでSIPインスペクションを無効にするには、次の手順を実行します。

ステップ1:ASAのCLIにログインします。

ステップ2：コマンド**show run policy-mapを実行します**。

ステップ3：図に示すように、inspect sipがポリシーマップglobal-policyリストの下にあることを確認します。



ステップ4：該当する場合は、次のコマンドを実行します。

CubeASA1# policy-map global_policy

CubeASA1# class inspection_default

CubeASA1# no inspect sip

関連情報

- ASAファイアウォールでSIPインスペクションを使用することは推奨されません（74ページ）。
  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
- SIPインスペクションの詳細については、こちらを参照してください。
  https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/firewall/asa-99-firewall-config/inspect-voicevideo.pdf
- テクニカル サポートとドキュメント – Cisco Systems