Cisco Unified Border Element(CUBE)Enterpriseと共存するゾーンベースファイアウォール(ZBFW)の設定

内容

概要

このドキュメントでは、Cisco Unified Border Element(CUBE)Enterpriseと共存するゾーンベースファイアウォール(ZBFW)を設定する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

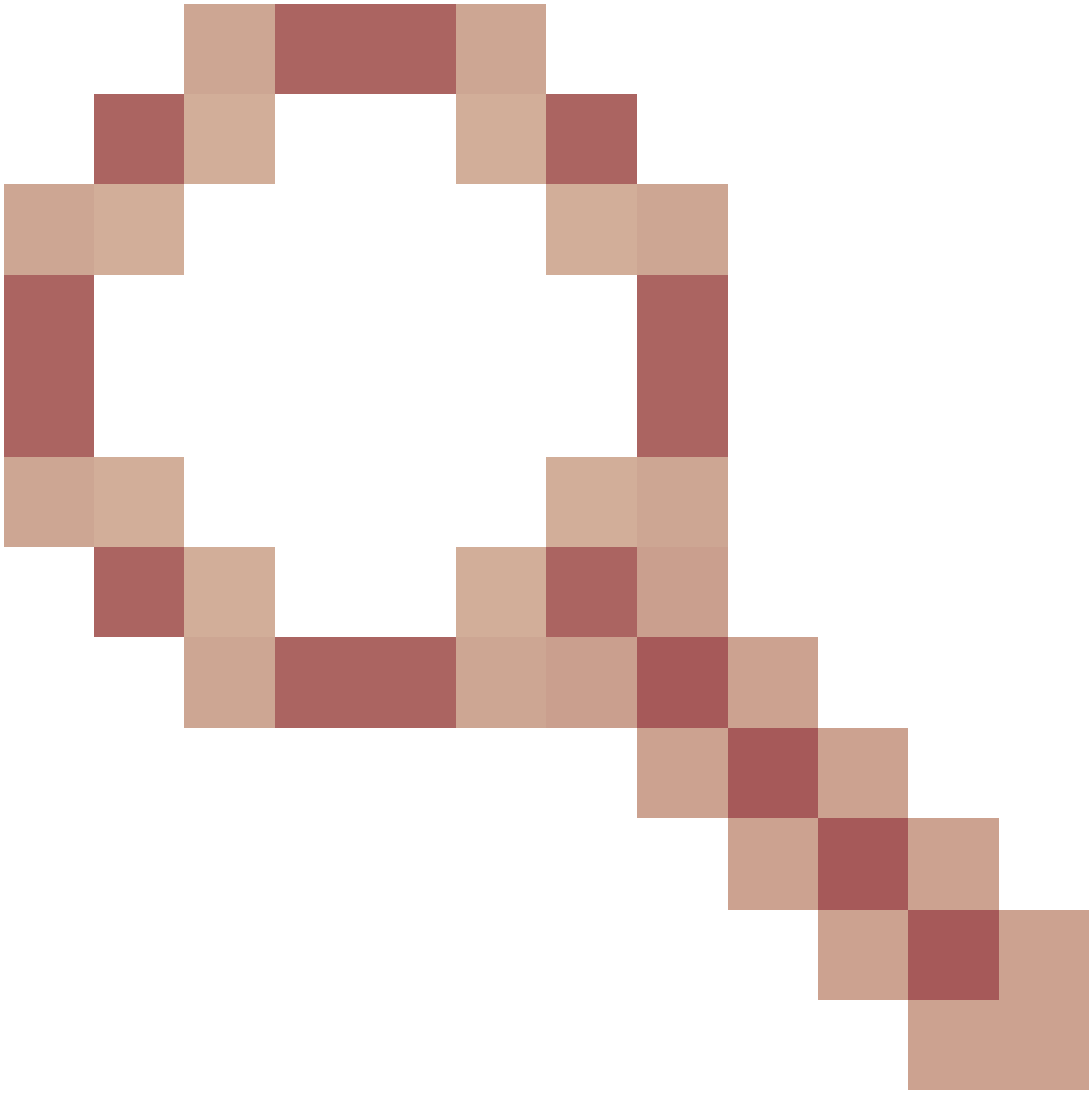
- Cisco IOS® XE 17.10.1aを実行するシスコルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

- CUBE EnterpriseとZBFWのコロケーションは、Cisco IOS XEでは16.7.1以降でサポートされていませんでした。

- CUBE EnterpriseはCUBE + ZBFW RTP-RTPメディアフローのみをサポートします。関連項目：



CSCwe66293

– このドキュメントは、CUBEメディアプロキシ、CUBEサービスプロバイダー、MGCPまたはSCCPゲートウェイ、Cisco SRSTまたはESRSTゲートウェイ、H323ゲートウェイ、またはその

他のアナログ/TDM音声ゲートウェイには適用されません。

- TDM/アナログ音声ゲートウェイおよびZBFWについては、次のドキュメントを参照してください。https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html

ネットワーク図

設定例では、INSIDEとOUTSIDEという2つの論理ネットワークセグメントを示します。

INSIDEには1つのIPネットワークが含まれ、OUTSIDEには2つのIPネットワークが含まれます。

レイヤ3ネットワークトポロジ

```
Endpoint_A - Network A - Gig1 - CUBE - Gig3 - Network B - CUCM
                                          \_ Network C - Endpoint_B
```

レイヤ7コールフロー

```
Call Direction ======================================>
Endpoint_A > SIP > CUBE > SIP > CUCM > SIP > Endpoint_B
```

レイヤ7メディアフロー

```
Endpoint_A <> RTP <> CUBE <> RTP <> Endpoint_B
```

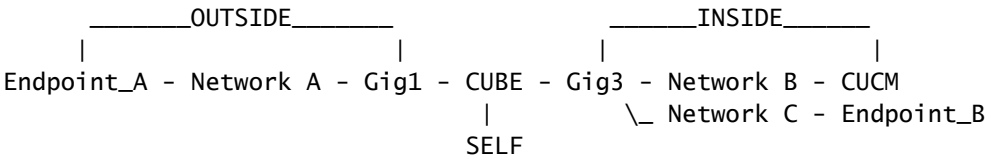
ZBFWクラッシュコースの概念

- ZBFWを設定する場合は、セキュリティゾーン名を設定します。このゾーン名は、次にインターフェイスで定義されます。この後、そのインターフェイスを行き来するすべてのトラフィックは、そのゾーン名に関連付けられます。
  - 同じゾーンとの間のトラフィックは常に許可されます。
  - 異なるゾーンを行き来するトラフィックは、管理者の設定で許可されていない限り廃棄されます。
- 許可されるトラフィックフローを定義するには、送信元と宛先のゾーン名を定義する単方向ゾーンペア設定を介してゾーンマッピングを作成する必要があります。
  - 次に、このゾーンペアマッピングは、検査されたトラフィックタイプ、許可されたトラフィックタイプ、および拒否されたトラフィックタイプをきめ細かく制御するために使用されるサービスポリシーに結び付けられます。
- CUBE Enterpriseは、特別なSELFゾーンで動作します。SELFゾーンには、ICMP、SSH、

NTP、DNSなど、ルータとの間でやり取りされるその他のトラフィックが含まれます。
    - CUBE LTIで使用するハードウェアPVDMはセルフゾーンに存在しないため、管理上設定されたゾーンにマッピングする必要があります。
- ZBFWはリターントラフィックを自動的に許可しないため、管理者はリターントラフィックを定義するようにゾーンペアを設定する必要があります。

次の3つの箇条書きを念頭に置いて、次のゾーンをL3ネットワークトポロジに重ねて追加できます。

- ネットワークA、Gig1は外部ゾーンです
- ネットワークB、ネットワークC、およびGig3は内部ゾーン
- CUBEはSELFゾーンの一部です



次に、CUBE+ZBFWを通過するトラフィックフローに必要な4つの単方向ゾーンペアマッピングを論理的に作成します。

出典	宛先	用途
OUTSIDE	セルフ	エンドポイントAからの着信SIPおよびRTPメディア
セルフ	INSIDE	CUBEからCUCMおよびエンドポイントBへの発信SIPおよびRTPメディア。
INSIDE	セルフ	CUCMおよびエンドポイントBからの着信SIPおよびRTPメディア。
セルフ	OUTSIDE	CUBEからエンドポイントAへの発信SIPおよびRTPメディア。

これらの概念を念頭に置いて、CUBEとして動作するCisco IOS XEルータでZBFWの設定を開始できます。

コンフィギュレーション

セキュリティゾーンの定義

2つのセキュリティゾーンINSIDEとOUTSIDEを設定する必要があることを思い出してください。selfはデフォルトであるため定義する必要はありません。

```
!
zone security INSIDE
zone security OUTSIDE
!
```

信頼できるトラフィック用のアクセスリスト、クラスマップ、ポリシーマップの作成

どのトラフィックを制御するために、ルータが照合して許可する方法を設定する必要があります。

そのために、トラフィックを検査する拡張アクセスリスト、クラスマップ、およびポリシーマップを作成します。

わかりやすくするために、着信トラフィックと発信トラフィックの両方をマッピングするポリシーを各ゾーンに作成します。

match protocol sipやmatch protocol sip-tlsなどの設定が使用される場合もありますが、説明のためにIP/ポートがすでに設定されています

外部の拡張アクセスリスト、クラスマップ、ポリシーマップ

<#root>

```
! Define Access List with ACLs for OUTSIDE interface


ip access-list extended TRUSTED-ACL-OUT
 10 remark Match SIP TCP/UDP 5060 and TCP TLS 5061
 11 permit tcp 192.168.1.0 0.0.0.255 any range 5060 5061
 12 permit tcp any 192.168.1.0 0.0.0.255 range 5060 5061
 13 permit udp 192.168.1.0 0.0.0.255 any eq 5060
 14 permit udp any 192.168.1.0 0.0.0.255 eq 5060
 !
 20 remark Match RTP Port Range, IOS-XE and Remote Endpoints
 21 permit udp 192.168.1.0 0.0.0.255 any range 8000 48198
 22 permit udp any 192.168.1.0 0.0.0.255 range 8000 48198
!

! Tie ACL with Class Map


class-map type inspect match-any TRUSTED-CLASS-OUT
```

```
 match access-group name TRUSTED-ACL-OUT
!
! Tie Class Map with Policy and inspect


policy-map type inspect TRUSTED-POLICY-OUT
 class type inspect TRUSTED-CLASS-OUT
  inspect
 class class-default
  drop log
!
```

内部拡張アクセスリスト、クラスマップ、ポリシーマップ

```
!
ip access-list extended TRUSTED-ACL-IN
 1 remark SSH, NTP, DNS
 2 permit tcp any any eq 22
 3 permit udp any any eq 123
 4 permit udp any any eq 53
 !
 10 remark Match SIP TCP/UDP 5060 and TCP TLS 5061
 11 permit tcp 192.168.2.0 0.0.0.255 any range 5060 5061
 12 permit tcp any 192.168.2.0 0.0.0.255 range 5060 5061
 13 permit udp 192.168.2.0 0.0.0.255 any eq 5060
 14 permit udp any 192.168.2.0 0.0.0.255 eq 5060
 !
 20 remark Match RTP Port Range, IOS-XE and Remote Endpoints
 21 permit udp 192.168.2.0 0.0.0.255 any range 8000 48198
 22 permit udp any 192.168.2.0 0.0.0.255 range 8000 48198
 23 permit udp 192.168.3.0 0.0.0.31 any range 8000 48198
 24 permit udp any 192.168.3.0 0.0.0.31 range 8000 48198
!
class-map type inspect match-any TRUSTED-CLASS-IN
 match access-group name TRUSTED-ACL-IN
!
policy-map type inspect TRUSTED-POLICY-IN
 class type inspect TRUSTED-CLASS-IN
  inspect
 class class-default
  drop log
!
```

ゾーンペアマッピングの作成

次に、表の前半で説明した4つのゾーンペアマッピングを作成する必要があります。

これらのゾーンペアは、先ほど作成したポリシーマップが適用されたサービスポリシーを参照します。

```
! INSIDE <> SELF


zone-pair security IN-SELF source INSIDE destination self
 service-policy type inspect TRUSTED-POLICY-IN
zone-pair security SELF-IN source self destination INSIDE
 service-policy type inspect TRUSTED-POLICY-IN
!

! OUTSIDE <> SELF


zone-pair security OUT-SELF source OUTSIDE destination self
 service-policy type inspect TRUSTED-POLICY-OUT
zone-pair security SELF-OUT source self destination OUTSIDE
 service-policy type inspect TRUSTED-POLICY-OUT
!
```

インターフェイスへのゾーンの割り当て

<#root>

```
! Assign Zones to interfaces


int gig1
 zone-member security INSIDE
!
int gig3
 zone-member security OUTSIDE
!
```

確認

サンプルパケットフロー – コール

この時点で、エンドポイントBからCUBEへのCUCM宛てのコールにより、次のシーケンスが呼び出されます。

1. 5060上のCUBEへの着信TCP SIPパケットはGIG 1に入り、外部ソースゾーンにマッピングされる
2. CUBEはSELFゾーンで動作するため、OUTSIDE to SELFゾーンペアが使用されます(OUT-SELF)。
3. service-policy/policy-map TRUSTED-POLICY-OUT は、TRUSTED-CLASS-OUT クラスマップとTRUSTED-ACL-OUTアクセスリストに基づいてトラフィックを検査するために使用されます
4. その後、CUBEはローカルコールルーティングロジックを使用して、コールの送信先と使用する出力インターフェイスを決定します。この例では、CUCMの出力インターフェイスはGIG 3です。
    1. CUBEコールルーティングの概要については、次のドキュメントを参照してください

。https://www.cisco.com/c/en/us/support/docs/voice/ip-telephony-voice-over-ip-voip/211306-In-Depth-Explanation-of-Cisco-IOS-and-IO.html

5. CUBEは新しいTCPソケットとSIP INVITEをすべてGIG 3（内部）から作成します。CUBEはSELFゾーンで動作するため、これはSELF-OUTゾーンペアを使用します
6. service-policy/policy-map TRUSTED-POLICY-IN は、TRUSTED-CLASS-IN クラスマップとTRUSTED-ACL-INアクセスリストに基づいてトラフィックを検査するために使用されます
7. このフローのリターントラフィックに対して、IN-SELFゾーンとSELF-OUTゾーンでコールの応答を送信します。

show コマンド

show zone-pair security

- このコマンドは、すべてのゾーンペアマッピングと適用されたサービスポリシーを表示します。
- source、destinationキーワードを使用すると、特定のゾーンペアマッピングを定義して多数のゾーンペアが存在するかどうかを確認できます。

<#root>

```
Router#
```

show zone-pair security

```
Zone-pair name IN-SELF 2
    Source-Zone INSIDE Destination-Zone self
    service-policy TRUSTED-POLICY-IN
Zone-pair name OUT-SELF 4
    Source-Zone OUTSIDE Destination-Zone self
    service-policy TRUSTED-POLICY-OUT
Zone-pair name SELF-IN 5
    Source-Zone self Destination-Zone INSIDE
    service-policy TRUSTED-POLICY-IN
Zone-pair name SELF-OUT 6
    Source-Zone self Destination-Zone OUTSIDE
    service-policy TRUSTED-POLICY-OUT

Router#
```

show zone-pair security source INSIDE destination self

```
Zone-pair name IN-SELF 2
    Source-Zone INSIDE Destination-Zone self
    service-policy TRUSTED-POLICY-IN
```

show call active voice compact

- このコマンドは、CUBEの観点からリモートメディア接続を表示します>

<#root>

Router#

show call active voice com | i NA|VRF

```
       <callID> A/O FAX   T<sec>  Codec       type        Peer Address   IP R:<ip>:<udp>              V
       467      ANS       T2      g711ulaw    VOIP        Psipp          192.168.1.48:16384
       468      ORG       T2      g711ulaw    VOIP        P8675309       192.168.3.59:16386           NA
```

show voip rtp connections

- このコマンドは、リモートとローカルの両方のメディア接続情報をCUBEの観点から表示します

<#root>

Router#

show voip rtp con | i NA|VRF

```
No. CallId     dstCallId  LocalRTP RmtRTP   LocalIP                                    RemoteIP
1     467        468        8120     16384    192.168.1.12                                192.168.1.48
2     468        467        8122     16386    192.168.2.58                               192.168.3.59
```

show call active voice brief

- このコマンドをvoice service voipで設定されたmedia bulk-statsコマンドと組み合わせると、コールレッグの送信(TX)および受信(RX)統計情報が表示されます。
- メディアがCUBEおよびZBFWを通過する場合、TXはピアコールレッグのRXと一致する必要があります（109 RX、109 TXなど）。

<#root>

Router#

show call active voice br | i dur

```
 dur 00:00:03 tx:107/24156 rx:109/24592 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 dur 00:00:03 tx:109/24592 rx:107/24156 dscp:0 media:0 audio tos:0xB8 video tos:0x0
```

show sip-ua connections tcp detail

- このコマンドは、CUBE経由のアクティブなSIP TCP接続の詳細を表示します
- show sip-ua connections udp detailやshow sip-ua connections tcp tls detailなどのコマンドを使用すると、UDP SIPとTCP-TLS SIPで同じ詳細を表示できます

<#root>

```
Router#

show sip-ua connections tcp detail

Total active connections      : 2
[..truncated..]
Remote-Agent:192.168.3.52, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address                Tenant
  =========== ======= =========== =========== ======================================= ======
         5060      51 Established           0 192.168.2.58:51875                         0

Remote-Agent:192.168.1.48, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address                Tenant
  =========== ======= =========== =========== ======================================= ======
        33821      50 Established           0 192.168.1.12:5060                          0
[..truncated..]
```

show policy-firewall sessions platform（ダウンロード）

- このコマンドは、ZBFWの観点からコールを表示します。
- RTPとRTCPには、SIPセッションとサブフローがあります。
- この出力のセッションIDは、後でZBFWをデバッグするときに使用できます。
- show policy-firewall sessions platform detailを使用すると、さらに多くのデータを表示できます。

<#root>

```
Router#

show policy-firewall sessions platform

--show platform hardware qfp active feature firewall datapath scb any any any any any all any --
[s=session  i=imprecise channel c=control channel  d=data channel u=utd inspect A/D=appfw action allow/
Session ID:0x000000A8 192.168.2.58 51875 192.168.3.52 5060 proto 6 (-global-:0:-global-:0) (0x16:sip) [
 +-Session ID:0x000000AA 192.168.2.58 0 192.168.3.52 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)  [
 +-Session ID:0x000000A9 192.168.3.52 0 192.168.2.58 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)  [
Session ID:0x000000AC 192.168.3.59 16386 192.168.2.58 8122 proto 17 (-global-:0:-global-:0) (0x2:udp) [
Session ID:0x000000AD 192.168.1.48 16384 192.168.1.12 8120 proto 17 (-global-:0:-global-:0) (0x3a:sip r
Session ID:0x000000A6 192.168.1.48 33821 192.168.1.12 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)
 +-Session ID:0x000000AE 192.168.1.48 16385 192.168.1.12 8121 proto 17 (-global-:0:-global-:0) (0x3a:si
 +-Session ID:0x000000AD 192.168.1.48 16384 192.168.1.12 8120 proto 17 (-global-:0:-global-:0) (0x3a:si
 +-Session ID:0x000000AB 192.168.1.48 0 192.168.1.12 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)
 +-Session ID:0x000000A7 192.168.1.12 0 192.168.1.48 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)
```

show policy-map type inspect zone-pair sessions

- このコマンドは、show policy-firewall sessions platformと同様のデータを表示しますが、デバッグに便利なゾーンペアマッピングも出力に含まれています。

```
Router# show policy-map type inspect zone-pair sessions | i Zone-pair|Session ID
  Zone-pair: IN-SELF
```

```
        Session ID 0x000000AD (192.168.1.48:16384)=>(192.168.1.12:8120) sip-RTP-data SIS_OPEN
        Session ID 0x000000A6 (192.168.1.48:33821)=>(192.168.1.12:5060) sip SIS_OPEN
        Session ID 0x000000A7 (192.168.1.12:0)=>(192.168.1.48:5060) sip SIS_PREGEN
        Session ID 0x000000AE (192.168.1.48:16385)=>(192.168.1.12:8121) sip-RTP-data SIS_PREGEN
        Session ID 0x000000AB (192.168.1.48:0)=>(192.168.1.12:5060) sip SIS_PREGEN
  Zone-pair: OUT-SELF
        Session ID 0x000000AC (192.168.3.59:16386)=>(192.168.2.58:8122) udp SIS_OPEN
  Zone-pair: SELF-IN
  Zone-pair: SELF-OUT
        Session ID 0x000000A8 (192.168.2.58:51875)=>(192.168.3.52:5060) sip SIS_OPEN
        Session ID 0x000000AA (192.168.2.58:0)=>(192.168.3.52:5060) sip SIS_PREGEN
        Session ID 0x000000A9 (192.168.3.52:0)=>(192.168.2.58:5060) sip SIS_PREGEN
```

トラブルシュート

Cisco IOS XEゾーンベースファイアウォールのトラブルシューティングについては、次のドキュメントを参照してください。

https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/117721-technote-iosfirewall-00.html

CUBEローカルトランスコーディングインターフェイス(LTI)+ ZBFW

- CUBEがマザーボードまたはネットワークインターフェイスモジュール(NIM)のハードウェアPVDMリソースで設定されている場合、これらはCUBE LTIの目的で使用できます。
- PVDMのバックプレーンインターフェイスには、PVDMの配置に対応する静的なservice-engine x/y/zが含まれます。たとえば、service-engine 0/4は、マザーボードのPVDM/DSPスロットです。
- このサービスエンジンはゾーンで設定する必要があり、セルフゾーンには存在しません。

次の設定では、CUBE LTIで使用されるサービスエンジンを、ZBFWの目的でINSIDEゾーンにマッピングします。

```
!
interface Service-Engine0/4/0
 zone-member security INSIDE
!
```

ハードウェアPVDM/DSPベースのSCCPメディアリソースとSCCPバインドインターフェイスでも、サービスエンジンのゾーンペアマッピングに同様のロジックを使用できますが、このトピックについてはこのドキュメントでは説明しません。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。