SD-WAN CLIテンプレートからのZBFWの設定

内容

はじめに

このドキュメントでは、Cisco Catalyst SD-WAN ManagerからCLIアドオン機能テンプレートを使用して、ゾーンベースファイアウォール(ZBFW)ポリシーを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Catalystソフトウェア定義型ワイドエリアネットワーク(SD-WAN)
- ゾーンベースファイアウォール(ZBFW)の基本動作

使用するコンポーネント

- Cisco Catalyst SD-WAN Manager 20.9.3.2
- Cisco IOS® XE Catalyst SD-WANエッジ17.6.5a

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。

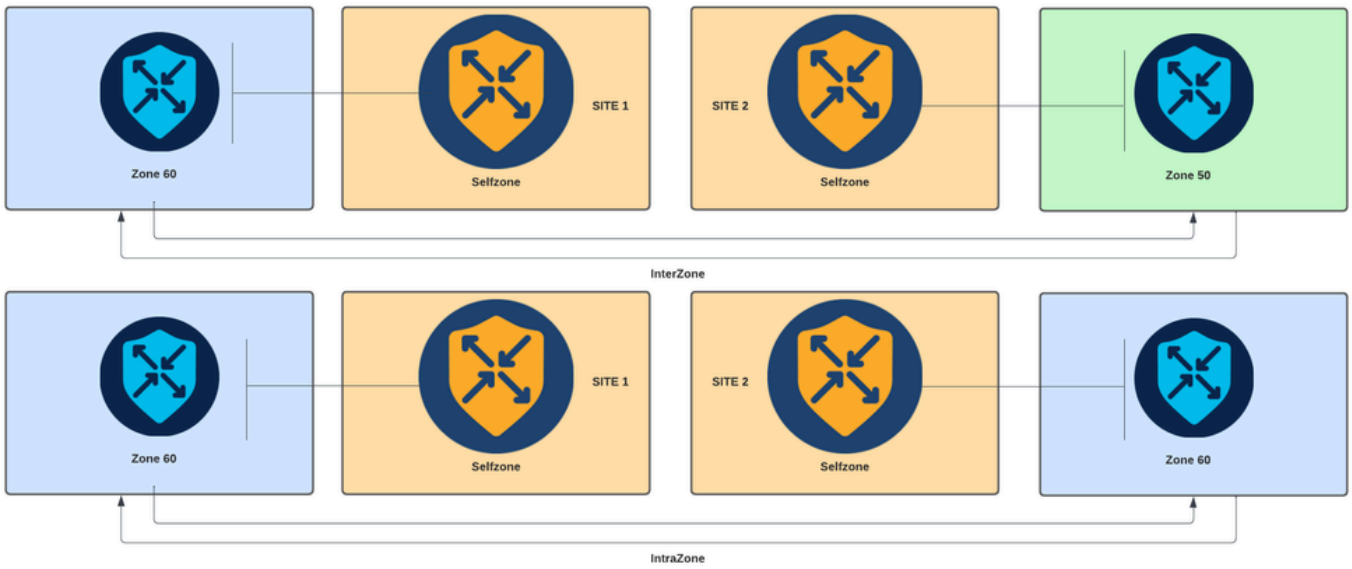
背景説明

ファイアウォールポリシーは、TCP、UDP、およびICMPデータトラフィックフローのステート

フルインスペクションを可能にする一種のローカライズされたセキュリティポリシーです。これはゾーンの概念を使用します。したがって、特定のゾーンで発信されるトラフィックフローは、2つのゾーン間のポリシーに基づいて別のゾーンに進むことができます。

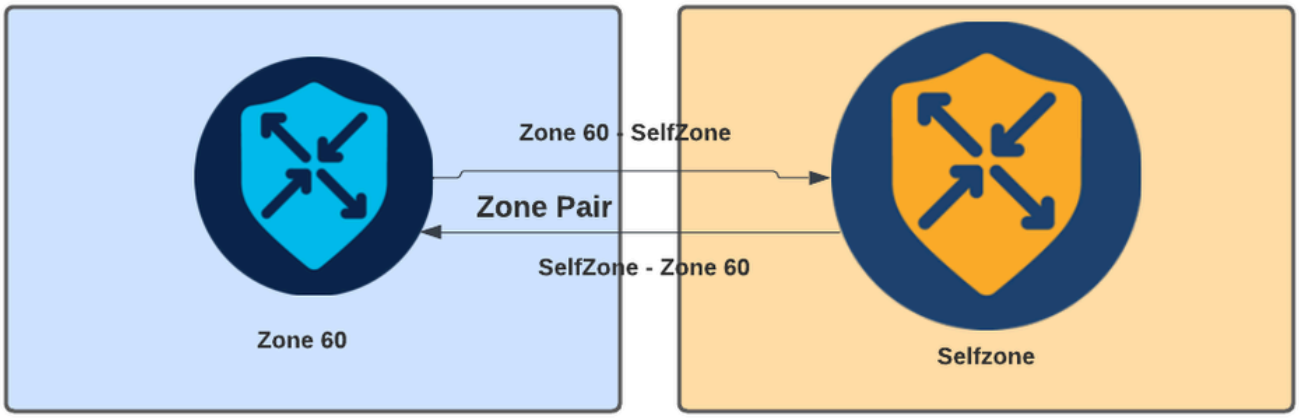
ゾーンは、1つ以上のVPNのグループです。ZBFWに存在するゾーンのタイプは次のとおりです。

- 送信元ゾーン：データトラフィックフローを発信するVPNのグループ。VPNは1つのゾーンにのみ属することができます。
- 宛先ゾーン：データトラフィックフローを終端するVPNのグループ。VPNは1つのゾーンにのみ属することができます。
- Interzone：異なるゾーン間をトラフィックが流れる場合（デフォルトでは通信は拒否されます）、これをinterzoneと呼びます。
- ゾーン内:トラフィックが同じゾーンを通過する場合（デフォルトでは通信は許可されます）、ゾーン内と呼ばれます。
- Selfzone:ルータ自体を送信元または宛先とするトラフィックの制御に使用されます（システムによって作成および事前設定されたデフォルトゾーン。デフォルトでは、通信は許可されます）。



ゾーンベースファイアウォールの図

ZBFWで使用されるもう1つの概念はゾーンペアです。これは、ソースゾーンを宛先ゾーンに関連付けるコンテナです。ゾーンペアは、2つのゾーン間を流れるトラフィックにファイアウォールポリシーを適用します。



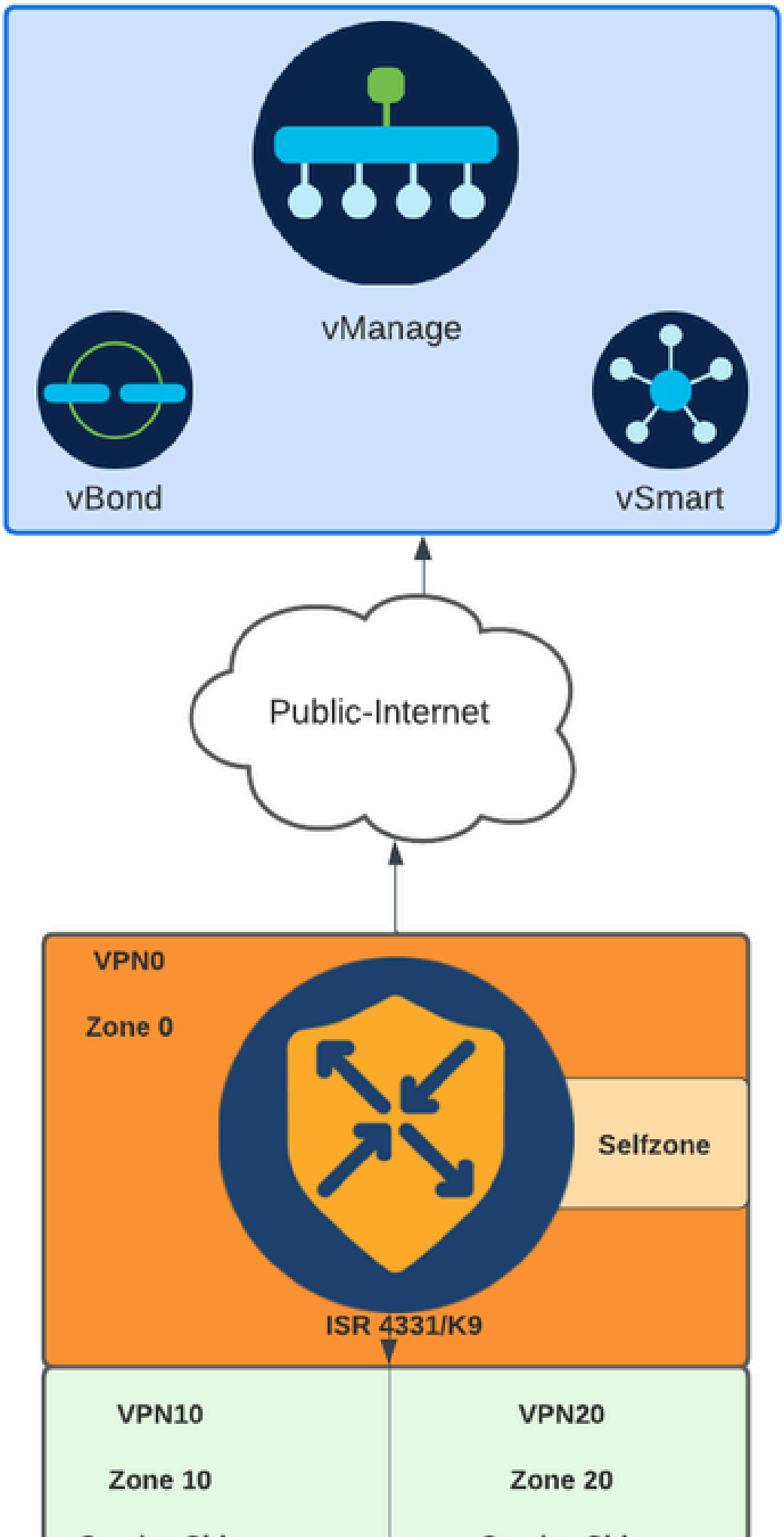
ゾーンペアの例

ゾーンペアを定義した後、フローに適用されるアクションは次のとおりです。

- ドロップ：単にフローに一致するパケットを廃棄します。
- 合格：アクセスリストのpermitアクションと同様に、ステートフルインスペクションを使用しないパケットフローを許可します。 フローにパスアクションが設定されているかどうかにかかわらず、そのフローのリターンパスが必要です。
- Inspect：送信元から宛先ゾーンへのトラフィックフローのステートフルインスペクションを可能にし、トラフィックフローが戻ってくることを自動的に許可します。

設定

ネットワーク図


vManage
vBond
vSmart
Public-Internet
VPN0
Zone 0
Selfzone
ISR 4331/K9
VPN10
Zone 10
VPN20
Zone 20

```
 multi-tenancy
 vpn zone security
  alert on
  log dropped-packets
  max-incomplete tcp timeout
```

max-incomplete tcp
コンフィギュレーションコマンドは、TCPセッションがドロップされるまでの不完全な接続の最大数を指定するために使用されます。

multi-tenancy設定コマンドは、ZBFW設定に必要なグローバルパラメータです。SD-WAN Manager GUIを使用してZBFWを設定すると、デフォルトで回線が追加されます。コマンドラインインターフェイス(CLI)でZBFWを設定する場合は、この行を追加する必要があります。

2. WANゾーンを作成します。

```
zone security wan
vpn 0
```

注：セルフゾーンはデフォルトで作成されるため、設定する必要はありません。

---

3. 送信元アドレスと宛先アドレスのオブジェクトグループを設定します。

```
object-group network CONTROLLERS
 host 172.18.121.103
 host 172.18.121.106
 host 192.168.20.152
 host 192.168.22.203
object-group network WAN_IPs
 host 10.122.163.207
```

4. IPアクセスリストを作成します。

```
ip access-list extended self-to-wan-acl
 10 permit tcp object-group WAN_IPs object-group CONTROLLERS
 20 permit udp object-group WAN_IPs object-group CONTROLLERS
 30 permit ip object-group WAN_IPs object-group CONTROLLERS
ip access-list extended wan-to-self-acl
 10 permit tcp object-group CONTROLLERS object-group WAN_IPs
 20 permit udp object-group CONTROLLERS object-group WAN_IPs
 30 permit ip object-group CONTROLLERS object-group WAN_IPs
```

5. クラスマップを作成します。

```
class-map type inspect match-all self-to-wan-cm
 match access-group name self-to-wan-acl
class-map type inspect match-all wan-to-self-cm
 match access-group name wan-to-self-acl
```

6. ゾーンペアに追加するポリシーマップを作成します。

```
policy-map type inspect wan-to-self-pm
 class type inspect wan-to-self-cm
  inspect
 class class-default
policy-map type inspect self-to-wan-pm
 class type inspect self-to-wan-cm
  inspect
 class class-default
```

7. ゾーンペアを作成してポリシーマップをリンクします。

```
zone-pair security self-to-wan source self destination wan
 service-policy type inspect self-to-wan-pm
zone-pair security wan-to-self source wan destination self
 service-policy type inspect wan-to-self-pm
```

コントロールプレーンフローが許可されたら、データプレーン設定を適用できます。

制御接続を検証するには、EXECコマンドを使用します。

<#root>

Device#

show sdwan control connections

セルフゾーンとWANゾーンのZBFWが正しく設定されていないと、デバイスは制御接続を失い、次のようなコンソールエラーを受け取ります。

<#root>

Oct 30 19:44:17.731: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:00000004865486441431 %FW-6-

データ プレーン

1. 必要なVirtual Routing and Forwarding(VRF)ごとにセキュリティゾーンを作成します。

```
zone security user
vpn 10
zone security server
vpn 20
```

3. 送信元アドレスと宛先アドレスのオブジェクトグループを設定します。

```
 object-group network USER
 host 10.10.10.1
 host 10.10.10.2
 host 10.10.10.3
object-group network SERVER
 host 10.20.20.1
 host 10.20.20.2
```

4. IPアクセスリストを作成します。

```
ip access-list extended user-to-server-acl
 10 permit tcp object-group USER object-group SERVER
 20 permit udp object-group USER object-group SERVER
 30 permit ip object-group USER object-group SERVER
ip access-list extended server-to-user-acl
 10 permit tcp object-group SERVER object-group USER
 20 permit udp object-group SERVER object-group USER
 30 permit ip object-group SERVER object-group USER
```

5. クラスマップを作成します。

```
class-map type inspect match-all user-to-server-cm
 match access-group name user-to-server-acl
class-map type inspect match-all server-to-wan-cm
 match access-group name server-to-user-acl
```

6. ゾーンペアに追加するポリシーマップを作成します。

```
policy-map type inspect user-to-server-pm
 class type inspect user-to-server-cm
```

```
  inspect
 class class-default
policy-map type inspect server-to-user-pm
 class type inspect server-to-user-cm
  inspect
 class class-default
```

7. ゾーンペアを作成してポリシーマップをリンクします。

```
zone-pair security user-to-server source user destination server
 service-policy type inspect user-to-server-pm
zone-pair security server-to-user source server destination user
 service-policy type inspect server-to-user-pm
```

注:CLIテンプレートの使用の詳細については、「CLIアドオン機能テンプレート」および「CLIテンプレート」を参照してください。

確認

設定されたinspect class-mapを検証するには、EXECコマンドを使用します。

<#root>

Device#

show class-map type inspect

設定されたinspect policy-mapを検証するには、EXECコマンドを使用します。

<#root>

Device#

show policy-map type inspect

設定されたゾーンペアを検証するには、EXECコマンドを使用します。

<#root>

Device#

show zone-pair security

設定されたアクセスリストを検証するには、EXECコマンドを使用します。

```
<#root>

Device#

show ip access-list
```

設定されたオブジェクトグループを検証するには、EXECコマンドを使用します。

```
<#root>

Device#

show object-group
```

ZBFWセッションのステータスを表示するには、EXECコマンドを使用します。

```
<#root>

Device#

show sdwan zonebfwdp sessions

 SRC DST TOTAL TOTAL UTD
SESSION SRC DST SRC DST VPN VPN NAT INTERNAL INITIATOR RESPONDER APPLICATION POLICY
ID STATE SRC IP DST IP PORT PORT PROTOCOL VRF VRF ID ID ZP NAME CLASSMAP NAME FLAGS FLAGS BYTES BYTES T
----------------------------------------------------------------------------------------------------

8 open 172.18.121.106 10.122.163.207 48960 32168 PROTO_L4_UDP 0 0 0 65534 wan-to-self wan-to-self-cm - 0


5 open 10.122.163.207 172.18.121.106 32168 32644 PROTO_L4_UDP 0 0 65534 0 self-to-wan self-to-wan-cm - 0

7 open 10.122.163.207 172.18.121.103 32168 32168 PROTO_L4_UDP 0 0 65534 0 self-to-wan self-to-wan-cm - 0


6 open 172.18.121.106 10.122.163.207 60896 32168 PROTO_L4_UDP 0 0 0 65534 wan-to-self wan-to-self-cm - 0
9 open 10.122.163.207 172.18.121.106 32168 34178 PROTO_L4_UDP 0 0 65534 0 self-to-wan self-to-wan-cm - 0
```

ゾーンペアの統計情報を表示するには、EXECコマンドを使用します。

```
<#root>

Device#

show sdwan zbfw zonepair-statistics

zbfw zonepair-statistics user-to-server
```

```
src-zone-name user
dst-zone-name server
policy-name user-to-server-pm
fw-traffic-class-entry user-to-server-cm
zonepair-name user-to-server

class-action Inspect


pkts-counter 0
bytes-counter 0
attempted-conn 0

current-active-conn 0


max-active-conn 0
current-halfopen-conn 0
max-halfopen-conn 0
current-terminating-conn 0
max-terminating-conn 0

time-since-last-session-create 0
```

ZBFWドロップ統計情報を表示するには、EXECコマンドを使用します。

<#root>

```
Device#

show sdwan zbfw drop-statistics

zbfw drop-statistics catch-all                          0
zbfw drop-statistics l4-max-halfsession                 0
zbfw drop-statistics l4-session-limit                   0
zbfw drop-statistics l4-scb-close                       0




zbfw drop-statistics insp-policy-not-present            0


zbfw drop-statistics insp-sess-miss-policy-not-present 0


zbfw drop-statistics insp-classification-fail           0
zbfw drop-statistics insp-class-action-drop             0
```

```
zbfw drop-statistics insp-policy-misconfigure          0

zbfw drop-statistics l4-icmp-err-policy-not-present    0

zbfw drop-statistics invalid-zone                      0

zbfw drop-statistics ha-ar-standby                     0
zbfw drop-statistics no-forwarding-zone                0

zbfw drop-statistics no-zone-pair-present            105 <<< If no zone-pair configured
```

QuantumFlow Processor(QFP)廃棄の統計情報を表示するには、EXECコマンドを使用します。

<#root>

```
Device#
show platform hardware qfp active statistic drop

Last clearing of QFP drops statistics: never
-------------------------------------------------------------------------
Global Drop Stats                          Packets               Octets
-------------------------------------------------------------------------

BFDoffload                                   194                 14388

FirewallBackpressure                           0                     0
FirewallInvalidZone                            0                     0

FirewallL4                                     1                    74
```

```
FirewallL4Insp                              372                40957
FirewallL7                                    0                    0

FirewallNoForwardingZone                      0                    0


FirewallNoNewSession                          0                    0


FirewallNonsession                            0                    0
FirewallNotFromInit                           0                    0
FirewallNotInitiator                      11898               885244

FirewallPolicy                                0                    0
```

QFPファイアウォールのドロップを表示するには、EXECコマンドを使用します。

<#root>

```
Device#

show platform hardware qfp active feature firewall drop all

-----------------------------------------------------------------------------
Drop Reason                                                        Packets
-----------------------------------------------------------------------------
TCP out of window                                                        0
TCP window overflow                                                      0
<snipped>
TCP - Half-open session limit exceed                                     0
Too many packet per flow                                                 0
<snipped>
ICMP ERR PKT:no IP or ICMP                                               0
ICMP ERR Pkt:exceed burst lmt                                            0
ICMP Unreach pkt exceeds lmt                                             0
ICMP Error Pkt invalid sequence                                          0
ICMP Error Pkt invalid ACK                                               0
ICMP Error Pkt too short                                                 0
Exceed session limit                                                     0
Packet rcvd in SCB close state                                           0
Pkt rcvd after CX req teardown                                           0
CXSC not running                                                         0

Zone-pair without policy                                                 0 <<< Existing zone-pair, but not


Same zone without Policy                                                 0 <<< Zone without policy configu


<snipped>

No Zone-pair found                                                     105 <<< If no zone-pair configured
```

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。