ファイアウォール プロファイルおよびポリシー オブジェクトの設定

この章の内容は、次のとおりです。

- Intercloud Fabric ファイアウォール ポリシー オブジェクトに関する情報，1 ページ
- サービス ファイアウォールのロギングの設定，8 ページ
- Intercloud Fabric ファイアウォール設定の確認，8 ページ

Intercloud Fabric ファイアウォール ポリシー オブジェクトに関する情報

ここでは、Cisco Prime ネットワーク サービス コントローラ（Prime NSC）を使用して、Intercloud Fabric ファイアウォールでファイアウォール ポリシー オブジェクトを設定し管理する方法について説明します。

（注） Cisco PNSC を通じてのみ、Intercloud Fabric ファイアウォールを設定できます。 現在は、ファイアウォール ポリシー オブジェクトの帯域外の設定と管理はサポートしていません。

Intercloud Fabric ファイアウォール ポリシー オブジェクトおよびファイアウォール プロファイルに関する情報

Intercloud Fabric ファイアウォール ポリシー オブジェクトの設定の前提条件

Intercloud Fabric（ICF）ファイアウォール ポリシー オブジェクトには次の前提条件があります。

- ICF からデータと管理ポート プロファイルを作成する。
- PNSC から Intercloud Fabric ファイアウォールをインスタンス化する。

Intercloud Fabric ファイアウォール設定時の注意事項および制約事項

Intercloud Fabric（ICF）ファイアウォール（VSG）ポリシー オブジェクトおよびファイアウォール ポリシーには次の設定時の注意事項と制限事項があります。

- 管理 VLAN はクラウドに拡張する必要があります。
- 異なる IP サブネットで ICF ファイアウォールの管理およびデータ インターフェイスを設定します。

デフォルト設定

表 *1*： *Intercloud Fabric* ファイアウォール（*VSG*）のデフォルトのパラメータ設定

パラメータ	デフォルト
ルール ポリシー オブジェクト	drop

ゾーン

ゾーンは、VM の論理グループまたはホストです。 ゾーンは、ゾーン名を使用したゾーン属性に基づくポリシーの記述を許可することにより、ポリシーの記述を簡素化できます。 ゾーン定義により、ゾーンに VM がマッピングされます。 論理グループの定義は、VM 属性やネットワーク属性など、VMに関連付けられた属性に基づくことができます。 ゾーン定義は条件ベースのサブネットおよびエンドポイントの IP アドレスとして記述できます。

ゾーンおよびオブジェクト グループは異なる方向のさまざまなルール間で共有されるため、ゾーンで使用される属性は、方向付けされず、ニュートラルである必要があります。

ゾーンの例

次に、ネットワークのゾーンを表示する例を示します。

```
vsg# show running-config zone zone1
zone zone1
cond-match-criteria: match-any
condition 1 net.ip-address eq 1.1.1.1
condition 2 net.port eq 80
```

オブジェクト グループ

オブジェクト グループは、属性に関連する条件のセットです。 オブジェクト グループおよびゾーンは異なる方向のさまざまなルール間で共有されるため、オブジェクト グループ条件で使用される属性は、方向付けされず、ニュートラルである必要があります。 オブジェクト グループは、ファイアウォール ルールの記述を支援するセカンダリ ポリシー オブジェクトです。 ルール条件は、演算子を使用することによりオブジェクト グループを参照できます。

オブジェクト グループの例

次に、ネットワークのオブジェクト グループを表示する例を示します。

```
vsg# show running-config object-group g1
object-group g1 net.port
match 10 in-range protocol 6 port 10 30
match 11 eq protocol 6 port 21 inspect ftp
```

ルール

ファイアウォール ルールは複数の条件とアクショで構成できます。 ルールは、トラフィックをフィルタリングする条件としてポリシーで定義できます。 ポリシー エンジンは、Intercloud Fabric ファイアウォール（VSG）で受信したネットワーク トラフィックをフィルタリングする設定としてポリシーを使用します。 ポリシー エンジンは、ネットワーク トラフィックをフィルタリングする 2 種類の条件一致モデルを使用します。

AND モデル：ルール内のすべての属性が一致する場合、ルールは matched に設定されます。

OR モデル：属性は 5 つの異なるタイプのカラムに分類されます。 true になるルールの場合は、各カラムで少なくとも 1 つの条件が true である必要があります。 OR モデルの 5 つのカラムは下記のとおりです。

- 送信元カラム：送信元ホストを識別するための属性。
- 宛先カラム：宛先ホストを識別するための属性。
- サービス カラム：宛先ホストでサービスを識別するための属性。
- Ether タイプ カラム：リンク レベル プロトコルを識別するための属性。
- 送信元ポート カラム：送信元ポートを識別するための属性。

ルールの例

次に、ネットワークのルールを表示する例を示します。

```
vsg# show running-config rule r2
rule r2
cond-match-criteria: match-all
   dst-attributes
     condition 10 dst.zone.name eq z1@r2
   service/protocol-attribute
condition 11 net.service eq protocol 6 port 21 inspect ftp
action permit
```

ポリシー

ポリシーは Intercloud Fabric（ICF）ファイアウォール（VSG）でネットワーク トラフィックに適用されます。 ICF ファイアウォールで動作する主要コンポーネントはポリシー エンジンです。 ポリシー エンジンは、ICF ファイアウォールで受信されるネットワーク トラフィックに対して適用された場合に、ポリシーを設定として取得し、実行します。 ポリシーは、次のポリシー オブジェクトのセットを使用して構築されます。

- ルール
- 条件
- アクション
- オブジェクト グループ
- ゾーン

ポリシーは、一連の間接的な関連付けを使用して ICF ファイアウォールにバインドされます。 セキュリティ管理者は、セキュリティプロファイルを設定すると、セキュリティプロファイル内のポリシー名を参照できます。 セキュリティ プロファイルは、ICF ファイアウォールへのリファレンスを持つポート プロファイルに関連付けられます。

ポリシー例

次に、**show running-config** コマンド出力にポリシーが表示される例を示します。

```
vsg# show running-config policy p2@root/T1
policy p2@root/T1
  rule r2 order 10
```

次に、**show running-config** コマンド出力に条件が表示される例を示します。

```
condition 1 dst.net.ip-address eq 2.2.2.2
condition 2 src.net.ip-address eq 1.1.1.1
```

次に、**show running-config** コマンド出力にアクションが表示される例を示します。

```
action permit
```

Intercloud Fabric ファイアウォール属性

ここでは、Intercloud Fabric ファイアウォール（VSG）属性について説明します。

属性名表記に関する情報

方向属性

ファイアウォール ポリシーは、着信パケットまたは発信パケットに対して方向付けられています。 ルール条件内の属性は、送信元または宛先のいずれかに関連するように指定されたものが必要です。 src.、dst.のようなプレフィックス、または属性名は、方向付けに使用されます。

ニュートラル属性

オブジェクト グループおよびゾーンは異なる方向のさまざまなルール間で共有されるため、ゾーンで使用される属性は方向付けされません。 方向付けされていない属性（src. または dst. などの方向プレフィックスを提供 しない）は、ニュートラル属性と呼ばれます。

異なる方向の 2 つのルール条件は同じオブジェクト グループ定義を共有できます。 オブジェクト グループで使用されるニュートラル属性と net.ip-address は、src.net.ip-address および dst.net.ip-address のような異なるルールで使用される方向属性と関連付けることができます。

属性クラス

属性は、ポリシー ルールおよび条件の設定、またはゾーン定義で使用されます。

ニュートラル属性

オブジェクト グループおよびゾーンは異なる方向のさまざまなルール間で共有されるため、ゾーンで使用される属性は方向付けされません。 方向付けされていない属性（src. または dst. などの方向プレフィックスを提供 しない）は、ニュートラル属性と呼ばれます。

異なる方向の 2 つのルール条件は同じオブジェクト グループ定義を共有できます。 オブジェクト グループで使用されるニュートラル属性と net.ip-address は、src.net.ip-address および dst.net.ip-address のような異なるルールで使用される方向属性と関連付けることができます。

VM 属性

VM 属性は VM インフラストラクチャに関連し、次のクラスの VM 属性があります。

- 仮想インフラストラクチャ属性：これらの属性は Intercloud Fabric から取得され、名前にマッピングされます。
- ポート プロファイル属性：これらの属性は、ポート プロファイルに関連付けられます。
- カスタム属性：これらの属性は、サービス プロファイルで設定できます。

次の表に、Intercloud Fabric ファイアウォール（VSG）によってサポートされる VM 属性を示します。

説明	名前
VM の名前	src.vm.name dst.vm.name vm.name （注） vm.name はニュートラル属性です。

説明	名前
ゲスト OS のフルネーム（バージョン含む）	src.vm.os-fullname dst.vm.os-fullname vm.os-fullname （注） vm.os-fullname はニュートラル属性です。
特定の vNIC に関連付けられたポート プロファイルの名前	src.vm.portprofile-name dst.vm.portprofile-name vm.portprofile-name （注） vm.portprofile-name はニュートラル属性です。
関連付けられたポート グループのセキュリティ プロファイルからのカスタム属性。 （注） 一意のカスタム属性 xxx ごとに、合成された属性名は src.vm.custom.xxx または dst.vm.custom.xxx となります。ポリシーは合成された属性名を使用します。	src.vm.custom.xxx dst.vm.custom.xxx vm.custom.xxx （注） vm.custom.xxx はニュートラル属性です。

カスタム VM 属性は、サービス プロファイルの下で設定できるユーザ定義の属性です。

次に、ICF ファイアウォールの VM 属性を確認する例を示します。

```
firewall(config)# show vsg vm
VM uuid          : 47592090-c9c2-5e67-f044-9d6a39dc1696
VM attributes :
  name                        : didata1-cvm
  os-fullname                 : rhel 6.2 (64bit)


Zone(s) :

--------------------------------------------------------------------------------
VM uuid          : 503ee75f-437b-1fa0-f0f4-fe0da53bab7a
VM attributes :
  host-name                   : 10.36.6.9
  name                        : windowsvm-migrate
  os-fullname                 : microsoft windows server 2003 (32-bit)
  os-hostname                 : sg-w2k-rv-1
  resource-pool               : resources
  tools-status                : installed
```

ゾーン属性

表 *2*： ***Intercloud Fabric*** ファイアウォールでサポートされるゾーン属性

説明	名前
ゾーン名を指定します。 これは複数値属性で、複数のゾーンに同時に属することができます。	src.zone.name dst.zone.name zone.name （注） zone.name はニュートラル属性です。

セキュリティ プロファイル

セキュリティプロファイルは、ポリシーの記述に使用できるカスタム属性を定義します。 特定のポートプロファイルのタグが付いたすべての VM は、そのポートプロファイルに関連付けられたセキュリティプロファイルで定義されたファイアウォールポリシーおよびカスタム属性を継承します。 各カスタム属性は、state = CA のように名前と値のペアとして設定されます。

次に、Intercloud Fabric（ICF）ファイアウォールのセキュリティ プロファイルを確認する例を示します。

```
firewall(config-vnm-policy-agent)# show vsg security-profile table
--------------------------------------------------------------------------------
Security-Profile Name VNSP ID Policy Name
--------------------------------------------------------------------------------
default@root 1 default@root
sp10@root/tenant_d3338 9 ps9@root/tenant_d3338
sp9@root/tenant_d3338 10 ps9@root/tenant_d3338
sp2@root/tenant_d3338 11 ps1@root/tenant_d3338
sp1@root/tenant_d3338 12 ps1@root/tenant_d3338
```

次に、ICF ファイアウォールのセキュリティ プロファイルを確認する例を示します。

```
firewall(config-vnm-policy-agent)# show vsg security-profile
VNSP : sp10@root/tenant_d3338
VNSP id : 9
Policy Name : ps9@root/tenant_d3338
Policy id : 3
Custom attributes :
  vnsporg : root/tenant_d3338
VNSP : default@root
VNSP id : 1
Policy Name : default@root
Policy id : 1
Custom attributes :
  vnsporg : root
VNSP : sp1@root/tenant_d3338
VNSP id : 12
Policy Name : ps1@root/tenant_d3338
Policy id : 2
Custom attributes :
  vnsporg : root/tenant_d3338
location : losangeles
color9 : test9
```

```
color8 : test8
color7 : test7
color6 : test6
color5 : test5
color4 : test4
color3 : test3
color2 : test2
color13 : test13
color12 : test12
color11 : test11
color10 : test10
color1 : test1
color : red
VNSP : sp2@root/tenant_d3338
VNSP id : 11
Policy Name : ps1@root/tenant_d3338
Policy id : 2
Custom attributes :
  vnsporg : root/tenant_d3338
  location : sanjose
  color : blue
VNSP : sp9@root/tenant_d3338
VNSP id : 10
Policy Name : ps9@root/tenant_d3338
Policy id : 3
Custom attributes :
  vnsporg : root/tenant_d3338
```

サービス ファイアウォールのロギングの設定

『』の「Enabling Global Policy-Engine Logging」の項を参照してください。

Intercloud Fabric ファイアウォール設定の確認

Intercloud Fabric（ICF）ファイアウォール（VSG）設定を表示するには、**show running-config** コマンドを使用します。

```
firewall# show running-config

!Command: show running-config
!Time: Fri Sep 26 15:39:57 2014

version 5.2(1)VSG2(1)
feature telnet
no feature http-server

username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na. role network-operator
username admin password 5 $1$CbPcXmpk$l31YumYWiO0X/EY1qYsFB. role network-admin
username vsnbetauser password 5 $1$mr/jBgON$hoJsM9ACdPHRWPM3KpI6/1 role network-admin

banner motd #Nexus VSN#

ssh key rsa 2048
ip domain-lookup
ip domain-lookup
hostname firewall
snmp-server user admin auth md5 0x0b4894684d52823092c7a7c0b87a853d priv
0x0b4894684d52823092c7a7c0b87a853d localizedkey engineID 128:0:0:9:
3:0:0:0:0:0:0
snmp-server user vsnbetauser auth md5 0x272e8099cab7365fd1649d351b953884 priv
0x272e8099cab7365fd1649d351b953884 localizedkey engineID 128:
0:0:9:3:0:0:0:0:0:0

vrf context management
```

```
  ip route 0.0.0.0/0 10.193.72.1
vlan 1
port-channel load-balance ethernet source-mac
port-profile default max-ports 32

vdc vsg id 1
limit-resource vlan minimum 16 maximum 2049
limit-resource monitor-session minimum 0 maximum 2
limit-resource vrf minimum 16 maximum 8192
limit-resource port-channel minimum 0 maximum 768
limit-resource u4route-mem minimum 32 maximum 32
limit-resource u6route-mem minimum 16 maximum 16
limit-resource m4route-mem minimum 58 maximum 58
limit-resource m6route-mem minimum 8 maximum 8
interface mgmt0
  ip address 10.193.73.185/21
interface data0
cli alias name ukickstart copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-kickstart-mzg.VSG1.1.bin
bootflash:ukickstart
cli alias name udplug copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG1.1.bin
bootflash:ukickstart
cli alias name udplug copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG1.1.bin
bootflash:dplug
cli alias name uimage copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-mzg.VSG1.1.bin
bootflash:user_bin
line console
boot kickstart bootflash:/ukickstart sup-1
boot system bootflash:/user_bin sup-1
boot kickstart bootflash:/ukickstart sup-2
boot system bootflash:/user_bin sup-2
mgmt-policy TCP permit protocol tcp
  ha-pair id 25
security-profile profile1
  policy p2
security-profile profile2
  policy p1
custom-attribute state "texas"
object-group g1 net.port
  match 1 eq 80
  match 2 eq 443
zone zone1
  condition 1 net.ip-address eq 1.1.1.1
  condition 2 net.port eq 80
  condition 2 net.port eq 80
rule r2
  condition 1 dst.net.ip-address eq 2.2.2.2
  condition 2 src.net.ip-address eq 1.1.1.1
  condition 3 src.net.port eq 100
  condition 4 dst.net.port eq 80
  condition 5 net.protocol eq 6
  action 1 permit
rule r5
  condition 1 net.ethertype eq 0x800
  action 1 inspect ftp
rule r6
rule r7
policy p2
  rule r2 order 10
policy p1
  rule r2 order 10

service firewall logging enable
vnm-policy-agent
 registration-ip 10.193.73.190
 shared-secret **********
 log-level info
firewall#
```