CHAPTER 7

Cisco Virtual Security Gateway のファイアウォール プロファイルおよびポリシー オブジェクト

この章では、Cisco Virtual Security Gateway（VSG）のファイアウォール プロファイルおよびポリシー オブジェクトの設定方法について説明します。

この章では、次の内容について説明します。

- 「Cisco VSG のファイアウォール ポリシー オブジェクトに関する情報」（P.7-1）
- 「Cisco VSG ポリシー オブジェクト設定の前提条件」（P.7-2）
- 「デフォルト設定」（P.7-3）
- 「Cisco VSG のファイアウォール ポリシー オブジェクト」（P.7-1）
- 「サービス ファイアウォールのロギングの設定」（P.7-11）
- 「Cisco VSG の設定の確認」（P.7-11）
- 「設定の制限値」（P.7-13）

Cisco VSG のファイアウォール ポリシー オブジェクトに関する情報

Cisco VSG のすべての設定および管理は、Cisco Virtual Network Management Center（VNMC）を使用して行います。

（注） ポリシーエージェント（PA）がインストールされている場合、コマンドライン インターフェイス（CLI）は Cisco VSG のポリシー関連オブジェクトの設定に使用できません。PA をアンインストール（削除）すると、CLI から再度ポリシー（およびポリシー オブジェクト）を設定できます。ただし、Cisco VSG のファイアウォール ポリシー オブジェクトのすべての設定および管理には Cisco VNMC を使用することを推奨します。

Cisco VSG のファイアウォール ポリシー オブジェクト

この項では、次のトピックについて取り上げます。

- 「Cisco VSG ポリシー オブジェクト設定の前提条件」（P.7-2）

- 「Cisco VSG 設定時の注意事項および制限事項」（P.7-2）
- 「デフォルト設定」（P.7-3）
- 「ゾーン」（P.7-3）
- 「オブジェクト グループ」（P.7-3）
- 「ルール」（P.7-3）
- 「ポリシー」（P.7-4）
- 「セキュリティ プロファイル」（P.7-8）
- 「Cisco VNMC および Cisco VSG のセキュリティ プロファイルおよびポリシーの表示」（P.7-9）

Cisco VSG ポリシー オブジェクト設定の前提条件

Cisco VSG ポリシー オブジェクトには次の前提条件があります。

- Cisco Nexus 1000V シリーズ スイッチ に NEXUS_VSG_SERVICES_PKG ライセンスがインストールされている必要があります。
- 保護対象の ESX ホスト（VEM）の数に対して十分なライセンスがあることを確認してください。
- 仮想スーパーバイザ モジュール（VSM）上で、Cisco VSG のサービスおよび HA インターフェイスのポート プロファイルを作成してください。
- Cisco VSG ソフトウェアをインストールし、基本インストールを完了します。詳細については、『*Cisco Virtual Security Gateway, Release 4.2(1)VSG1(4.1) and Cisco Virtual Network Management Center, Release 2.0 Installation and Upgrade Guide*』を参照してください。
- データ IP アドレスおよび管理 IP アドレスを設定する必要があります。データ IP アドレスを設定するには、『*Cisco Virtual Security Gateway, Release 4.2(1)VSG1(4.1) and Cisco Virtual Network Management Center, Release 2.0 Installation and Upgrade Guide*』を参照してください。
- セキュリティ ポリシーに必要な属性の詳細を用意します。
- EXEC モードで Cisco VSG CLI にログインします。

Cisco VSG 設定時の注意事項および制限事項

Cisco VSG の設定に関する注意事項と制約事項は次のとおりです。

- 管理 VLAN は VM ネットワーク vSwitch 上にある必要があります。
- HA およびサービス VLAN はアップリンク ポート上に設定します。（システム VLAN 上にある必要はありません）。
- Cisco VSG の管理インターフェイスとデータ インターフェイス（data0）に同じネットワーク IP アドレスを設定しないでください。

設定および管理作業については、次の要件が満たされている必要があります。

- Cisco VSG ソフトウェアは 3 つのネットワーク アダプタで実行されている必要があります。ネットワーク ラベルは次のとおりです。
  - ポートプロファイルとして Service（eth0）
  - 管理 VLAN として Mgmt（Eth1）
  - ポートプロファイルとして HA（Eth2）

- Cisco VSG VM の電源をオンにし、データ インターフェイスの IP アドレス（data0 用）および管理インターフェイスの IP アドレスを設定します。

ネットワーク アダプタへのネットワーク ラベルの割り当てに関する詳細については、『*Cisco Virtual Security Gateway, Release 4.2(1)VSG1(4.1) and Cisco Virtual Network Management Center, Release 2.0 Installation and Upgrade Guide*』を参照してください。

デフォルト設定

表 7-1 に、Cisco VSG パラメータのデフォルト設定を示します。

表 7-1　デフォルト パラメータ

パラメータ	デフォルト
ルール ポリシー オブジェクト	ドロップ

ゾーン

ゾーンは、仮想マシン（VM）またはホストの論理グループです。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、vCenter に定義された VM 属性など、VM またはホスト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、オブジェクト グループで使用される属性は、方向付けされていない、ニュートラル属性である必要があります。

次に、**show running-config** コマンド出力にゾーンが表示される例を示します。

```
vsg# show running-config zone zone1
zone zone1
   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、属性に関連する一連の条件です。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。

次に、**show running-config** コマンド出力にオブジェクト グループが表示される例を示します。

```
vsg# show running-config object-group g1
object-group g1 net.port
  match 1 eq 80
  match 2 eq 443
```

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、ポリシー内で、条件ベースのサブネット、またはエンド ポイントの IP アドレスおよび VM 属性として定義できます。

アクションはポリシー評価の結果です。指定したルール内で、次のアクションを 1 つまたは複数定義して関連付けることができます。

- 許可
- ドロップ パケット
- ログ
- インスペクション

次に、**show running-config** コマンド出力にルールが表示される例を示します。

```
vsg# show running-config rule r2
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
```

ポリシー

ファイアウォール ポリシーは、特定のポリシーにルールをバインドし、ルール間にランクを作成します。ポリシーは、Cisco VSG 上のネットワーク トラフィックを適用します。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 Cisco VSG 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、Cisco VSG 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。

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
policy p2
  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 1 permit
```

Cisco Virtual Security Gateway の属性

ここでは、Cisco Virtual Security Gateway の属性について説明します。

この項では、次のトピックについて取り上げます。

- 「属性名表記に関する情報」（P.7-5）
- 「属性クラス」（P.7-5）

属性名表記に関する情報

この項では、次のトピックについて取り上げます。

- 「方向属性」（P.7-5）
- 「ニュートラル属性」（P.7-5）

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、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

Cisco VSG 属性は、次のクラスに分類されます。

- 「ネットワーク属性」（P.7-5）
- 「VM 属性」（P.7-6）
- 「ゾーン属性」（P.7-8）

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。ゾーンは、VM 属性を使用して定義することもできます。

ネットワーク属性

ここでは、VSG ネットワーク属性について説明します（表 7-2 を参照）。

表 7-2　ネットワーク属性

説明	名前
送信元 IP アドレス	src.net.ip-address
送信元ポート	src.net.port
宛先 IP アドレス	dst.net.ip-address
宛先ポート	dst.net.port
IP アドレス[1]	net.ip-address

表 7-2　ネットワーク属性 （続き）

説明	名前
ポート[1]	net.port
IP プロトコル 9[1]	net.protocol
レイヤ 2 モードのフレームの EtherType[1]	net.ethertype

1. ニュートラル属性

VM 属性

VM 属性は、仮想マシンのインフラストラクチャに関連する属性で、次の VM 属性のクラスを含みます。

- 仮想インフラストラクチャ属性：これらの属性は、VMware vCenter から取得され、表 7-3 にリストされている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。

表 7-3 に、サポートされる VM 属性を示します。

表 7-3　VM 属性

説明	名前
VM の名前	src.vm.name dst.vm.name vm.name[1]
親ホスト（ESX ホスト）の名前	src.vm.host-name dst.vm.host-name vm.host-name[1]
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[1]
関連付けられた仮想アプリケーションの名前	src.vm.vapp-name dst.vm.vapp-name vm.vapp-name[1]
関連付けられたクラスタの名前	src.vm.cluster-name dst.vm.cluster-name vm.cluster.name[1]
VM のインベントリ パス	src.vm.inventory-path dst.vm.inventory-path vm.inventory-path[1]

表 7-3　VM 属性 （続き）

説明	名前
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[1]
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[1]

1. ニュートラル属性

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、Cisco VSG の VM 属性を確認する例を示します。

```
vsg# show vsg vm

VM uuid          : 421c2a2d-5e7c-3bdb-51e7-f7528163b021
VM attributes :
    name                      : centos5.3_3_vem1_clone
    vapp-name                 : apps
    os-fullname               : red hat enterprise linux 4 (32-bit)
    tools-status              : installed
    host-name                 : 10.193.75.20
    cluster-name              : dc_dm1_clu1
```

ゾーン属性

表 7-4 に、Cisco VSG がサポートするゾーン属性を示します。

表 7-4　ゾーン属性

説明	名前
ゾーン名。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[1]

1. ニュートラル属性

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、Cisco VSG のセキュリティ プロファイルを確認する例を示します。

```
vsg_d3338(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、Cisco VSG のセキュリティ プロファイルを確認する例を示します。

```
vsg_d3338(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
```

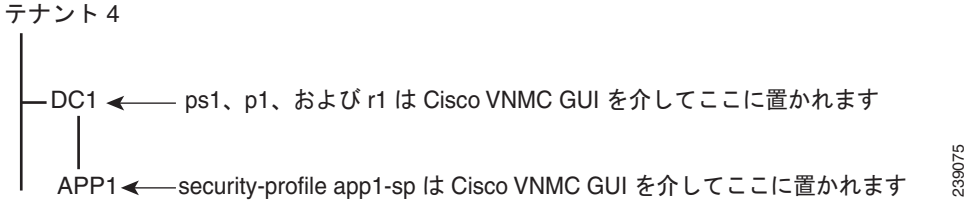
Cisco VNMC および Cisco VSG のセキュリティ プロファイルおよびポリシーの表示

Cisco VNMC GUI を使用すると、Cisco VSG のセキュリティ ポリシー オブジェクトを表示できます。Cisco VNMC GUI で表示されるポリシー オブジェクトは、**show running-config** コマンドを入力して Cisco VSG CLI に表示される組織のパス位置と必ずしも同じ位置に表示されるわけではありません。

たとえば、Cisco VNMC GUI では、仮想データセンター DC1 がテナントの下にあり、アプリケーション APP1 が DC1 の下にある場合、APP1 レベルの vvnsp app1-sp は DC レベルのポリシー セット ps1 を指します。

図 7-1 に、Cisco VNMC GUI の組織構造を示します。

図 7-1　　テナント、データセンター、およびアプリケーションの Cisco VNMC 組織階層




```
security-profile app1-sp@root/tenant4/DC1/APP1
  policy ps1@root/tenant4/DC1/APP1
  custom-attribute loc "sunnyvale"
  custom-attribute vnsporg "root/tenant4/dc1/app1"
```

show running-config コマンドの出力は、ポリシー セットおよびそのオブジェクトが、セキュリティ プロファイルが定義されている APP1 レベルから解決されることを示しています。Cisco VNMC GUI のオブジェクトの実際の場所は DC1 レベルです。

```
policy ps1@root/tenant4/DC1/APP1
rule p1/r1@root/tenant4/DC1/APP1 order 101
```

Cisco VSG の **show running-config** コマンド出力で表示されるポリシー オブジェクト DN は、DN（*解決される*場所と関連する DN）とともに表示されます。ポリシー オブジェクト DN は、Cisco VNMC の組織階層に実際のポリシー オブジェクトがある場所にはありません。

ただし、セキュリティ プロファイルは、Cisco VNMC の組織階層に実際のセキュリティ プロファイルが作成された場所に DN とともに表示されます。

ポリシー オブジェクトは、Cisco VNMC の組織階層にセキュリティ プロファイルが置かれている場所の上で解決されます。

例

次の例では、Cisco VSG が次の仕様で設定されています。

- セキュリティ プロファイル（VNSP）sp1 に、ルール r1 を含むポリシー p1 のあるポリシーセット ps1 があります。
- ポリシーセット ps1 が Cisco VNMC の組織ツリー内のルートに置かれています。
- ポリシー p1 が Cisco VNMC の組織ツリー内のルートに置かれています。
- ルール r1 が Cisco VNMC のポリシー p1 内に置かれています（Cisco VNMC ではルール オブジェクト自体を作成できません）。
- セキュリティ プロファイル sp1 が Cisco VNMC の tenant_d3337/dc1 に置かれています。

tenant_d3337 のすべての Cisco VSG には、次の **show-running config** コマンド出力があります（この設定はリーフ パス内のすべての Cisco VSG に複製されます）。

```
security-profile sp1@root/tenant_d3337/dc1
  policy ps1@root/tenant_d3337/dc1
  custom-attribute vnsporg "root/tenant_d3337/dc1"

policy p1@root/tenant_d3337/dc1
  rule p1/r1@root/tenant_d3337/dc1 order 101
```

（注）　上のポリシー オブジェクトは、実際は Cisco VNMC の組織ツリーの DC1 レベルには存在しませんが、Cisco VNMC 組織ツリー内のその位置から解決されます。

サービス ファイアウォールのロギングの設定

『*Cisco Virtual Security Gateway, Release 4.2(1)VSG1(4.1) and Cisco Virtual Network Management Center, Release 2.0 Installation and Upgrade Guide*』の「Enabling Global Policy-Engine Logging」の項を参照してください。

Cisco VSG の設定の確認

Cisco VSG の設定を表示するには、**show running-config** コマンドを使用します。

```
vsg# show running-config

!Command: show running-config
!Time: Wed Jan 26 15:39:57 2011

version 4.2(1)VSG1(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 vsg
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

vsg#
```

設定の制限値

表 7-5 に、Cisco VSG を設定する場合の制限値を示します。

表 7-5　設定の最大制限値

機能	上限
Cisco VSG の各ゾーン	16 カウント
ポリシーごとのルール	1000 カウント
Cisco VSG ごとのポリシー セット	16 カウント
ルールごとの属性	10
ルールごとの条件	10
Cisco VSG ごとの最大ルール数	1000 カウント