



CHAPTER 3

VSD の設定

この章では、VSD を設定する方法を説明します。内容は次のとおりです。

- 「仮想サービス ドメインについて」 (P.3-1)
- 「注意事項および制約事項」 (P.3-3)
- 「デフォルト設定」 (P.3-4)
- 「VSD の設定」 (P.3-4)
- 「設定の確認」 (P.3-8)
- 「設定例」 (P.3-10)
- 「その他の関連資料」 (P.3-10)
- 「機能の履歴」 (P.3-11)

仮想サービス ドメインについて

仮想サービス ドメイン (VSD) を使用すると、ネットワーク サービスのためのトラフィックの分類と分離が可能になります。このネットワーク サービスの例としては、ファイアウォールやトラフィック監視があり、その他にコンプライアンス目標 (たとえば Sarbanes Oxley) の達成支援のためのサービスなどがあります。

サービス仮想マシン

Service VM (SVM; サービス仮想マシン) は、専門サービス、たとえばファイアウォール、ディープパケット インスペクション (アプリケーション認識型ネットワークング)、監視などを実行します。各 SVM には、次の 3 つの仮想インターフェイスがあります。

インターフェイス	説明
管理	SVM を管理する標準のインターフェイス 用途に応じて、レイヤ 2 またはレイヤ 3 接続を必要とします。

インターフェイス	説明
着信	VSD に着信するトラフィックを保護します。 VSD に着信するパケットはすべて、このインターフェイスを通過する必要があります。
発信	VSD から外部に発信されるトラフィックを保護します。 VSD から外部に発信されるパケットはすべて、SVM を通過する必要がありますが、発信インターフェイスから送出されます。

これらのインターフェイスでの送信元 MAC 学習は行われません。SVM はそれぞれ、セキュアな VSD を作成します。VSD 内のインターフェイスは、SVM によって防御されます。

ポート プロファイル

VSD は、セキュリティ サービスを実行する SVM によって保護されるインターフェイスの集合です。VSD に着信するトラフィックや VSD から発信されるトラフィックはすべて、SVM を通過する必要があります。

トラフィックの発信元と宛先の両方が同じ VSD の中にある場合は、そのトラフィックは安全と見なされるので、SVM を経由する必要はありません。

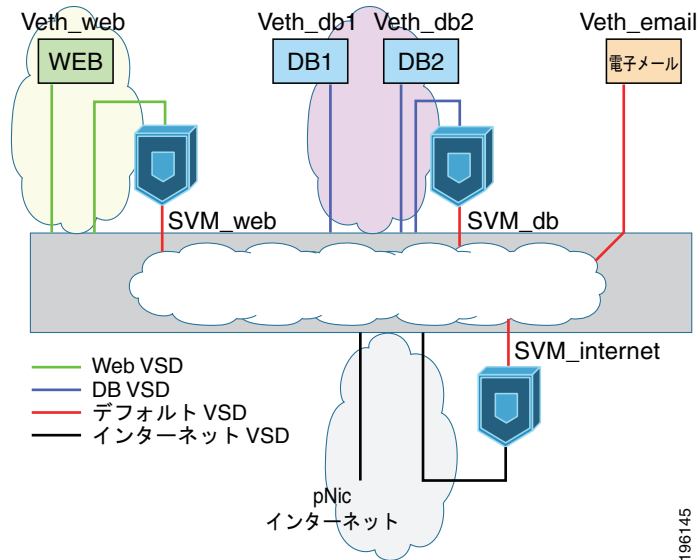
VSD を形成するには、次のポート プロファイルを作成します。

ポート プロファイル	説明
内側	VSD メンバーが発信元であるトラフィックは、内側ポートを通過して SVM に入り、外側ポートから出て宛先へ転送されます。
外側	宛先が VSD メンバーであるトラフィックは、外側ポートを通過して SVM に入り、内側ポートから出て宛先へ転送されます。
メンバ	個々の内側 VM が存在する場所。

図 3-1 では、ただ 1 つの VEM がいくつもの vswitch の役割を果たしています。SVM によって次の VSD が定義されます。

VSD	SVM (保護)	内側ポート プロファイル	外側ポート プロファイル	メンバー ポート プロファイル
DB VSD	SVM_db	SVM_db_inside	SVM_db_outside	vEth_db1 vEth_db2
Web VSD	SVM_web	SVM_web_inside	SVM_web_outside	vEth_web
インターネット VSD	SVM_Internet	SVM_internet_inside	SVM_internet_outside	
デフォルト		SVM VSD		vEth Email

図 3-1 仮想サービス ドメイン (VSD) の例



注意事項および制約事項

仮想サービス ドメイン (VSD) に関する注意事項と制約事項は次のとおりです。

- トラフィックの遅延を防ぐために、トラフィックのセキュリティ維持の手段は VSD だけを使用してください。
- ホストあたり最大 6 個の VSD を設定できます。VSM 上には最大 64 個を設定できます。
- VSD あたり最大 214 個のインターフェイスが 1 つのホスト上でサポートされ、VSM 上では 2048 個のインターフェイスがサポートされます。
- Vmotion は、SVM に対してはサポートされないため、ディセーブルにしてください。
- VSM リロードやネットワーク中断の後にネットワーク ループが発生するのを防ぐには、SVM のすべてのポート プロファイルにおいて制御 VLAN とパケット VLAN をディセーブルにする必要があります。
- SVM に対して設定されたポート プロファイルにサービス ポートが指定されていない場合は、ネットワーク上でパケット フラッディングが発生します。
- SVM に対してポート プロファイルを設定するときは、初めにその SVM を停止させてください。このようにすれば、ポート プロファイルがサービス ポートを持たないように誤って設定されても、ネットワーク上でパケット フラッディングが発生することはありません。設定と確認が完了したら、SVM を再び稼働させます。
- VShield 4.1 は VSD をサポートしません。VSD 機能は、VShield 4.1 とともに使用する場合は予想どおりに機能しません。

デフォルト設定

次の表に、Telnet のデフォルトを示します。

パラメータ	デフォルト
<code>service-port default-action</code>	forward
<code>switchport trunk allowed vlan</code>	all

VSD の設定

ここでは、次の手順について説明します。

- 「内側または外側 VSD ポート プロファイルの設定」(P.3-4)
- 「メンバー VSD ポート プロファイルの設定」(P.3-7)

内側または外側 VSD ポート プロファイルの設定

ここでは、SVM に入る接続および SVM から出る接続を定義するポート プロファイルを設定する手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 設定エラーによるネットワークのフラグディングを防ぐために、SVM を停止させてください。設定と確認が完了したら、SVM を再び稼働させます。
- サービス ポートが設定されていない場合は、SVM は通常の VM として起動するので、ネットワーク上でパケット フラグディングが発生します。
- 選択 VLAN フィルタリングは、このコンフィギュレーションではサポートされません。代わりに、デフォルトを使用してください。デフォルトでは、すべての VLAN がポート上で許可されます。


手順の概要

1. `config t`
2. `port-profile name`
3. `switchport mode trunk`
4. `switchport trunk allowed vlan vlanID`
5. `virtual-service-domain name`
6. `no shut`
7. `vmware port-group pg-name`
8. `service-port {inside | outside} [default-action {drop | forward}]`
9. `state enabled`
10. `show virtual-service-domain name`

11. copy running-config startup-config

手順の詳細

	コマンド	目的
ステップ 1	config t 例: <pre>n1000v# config t n1000v(config)#</pre>	CLI グローバル コンフィギュレーション モードを開始します。
ステップ 2	port-profile name 例: <pre>n1000v(config)# port-profile webserver-inside n1000v(config-port-profile)#</pre>	<p>ポート プロファイルを作成し、このポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。</p> <p>ポート プロファイルには最大 80 文字の名前を設定できます。ポート プロファイル名は、Cisco Nexus 1000V 上の各ポート プロファイルに対して一意である必要があります。</p>
ステップ 3	switchport mode trunk 例: <pre>n1000v(config-port-profile)# switchport mode trunk n1000v(config-port-profile)#</pre>	インターフェイスがスイッチ トランク ポートであることを指定します。
ステップ 4	switchport trunk allowed vlan vlanID 例: <pre>n1000v(config-port-profile)# switchport trunk allowed vlan all n1000v(config-port-profile)#</pre>	すべての VLAN をポート上で許可します。
ステップ 5	virtual-service-domain name 例: <pre>n1000v(config-port-profile)# virtual-service-domain vsd1-webserver n1000v(config-port-profile)#</pre>	このポート プロファイルに VSD 名を追加します。
ステップ 6	no shutdown 例: <pre>n1000v(config-port-prof)# no shutdown n1000v(config-port-prof)#</pre>	管理上の目的でプロファイル内のすべてのポートをイネーブルにします。
ステップ 7	vmware port-group pg-name 例: <pre>n1000v(config-port-prof)# vmware port-group webserver-inside-protected n1000v(config-port-prof)#</pre>	<p>VMware ポート グループとしてポート プロファイルを指定します。</p> <p>ポート プロファイルは、同じ名前の VMware ポート グループにマッピングされます。vCenter Server 接続が確立すると、Cisco Nexus 1000V で作成されたポート グループは、vCenter Server の仮想スイッチに配信されます。</p> <p>name : ポート グループ名。pg-name を指定しない場合、ポート グループ名は、ポート プロファイル名と同じになります。ポート プロファイルを異なるポート グループ名にマッピングする場合は、pg-name オプションのあとに別の名前を続けます。</p>

	コマンド	目的												
ステップ 8	service-port {inside outside} [default-action {drop forward}] 例： <pre>n1000v(config-port-prof)# service-port inside default-action forward n1000v(config-port-prof)#</pre> 例： <pre>n1000v(config-port-prof)# service-port outside default-action forward n1000v(config-port-prof)#</pre>	インターフェイスを内側 (inside) または外側 (outside) として設定するとともに、サービスポートがダウンした場合にパケットを転送するかドロップするかを指定します (default-action)。 default-action を省略すると、デフォルトでは forward 設定が使用されます。  注意 サービスポートが設定されていない場合は、SVM は通常の VM として起動するので、ネットワーク上でパケットフラッディングが発生します。												
ステップ 9	state enabled 例： <pre>n1000v(config-port-prof)# state enabled n1000v(config-port-prof)#</pre>	VSD ポート プロファイルをイネーブルにします。 このポート プロファイルの設定が、割り当てられたポートに適用されます。また、vCenter Server 上の VMware vSwitch 内にポート グループが作成されます。												
ステップ 10	show virtual-service-domain name 例： <pre>n1000v(config-port-prof)# show virtual-service-domain vsd1-webserver Default Action: forward</pre> <table border="1" data-bbox="342 1289 688 1478"> <thead> <tr> <th>Interface</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>Vethernet1</td> <td>Member</td> </tr> <tr> <td>Vethernet2</td> <td>Member</td> </tr> <tr> <td>Vethernet3</td> <td>Member</td> </tr> <tr> <td>Vethernet7</td> <td>Inside</td> </tr> <tr> <td>Vethernet8</td> <td>Outside</td> </tr> </tbody> </table> <pre>n1000v(config-port-prof)#</pre>	Interface	Type	Vethernet1	Member	Vethernet2	Member	Vethernet3	Member	Vethernet7	Inside	Vethernet8	Outside	(任意) この VSD ポート プロファイルの設定を表示します。この表示を使用して、ポート プロファイルが正しく設定されていること確認します。
Interface	Type													
Vethernet1	Member													
Vethernet2	Member													
Vethernet3	Member													
Vethernet7	Inside													
Vethernet8	Outside													
ステップ 11	copy running-config startup-config 例： <pre>n1000v(config-port-prof)# copy running-config startup-config [#####] #] 100% n1000v(config-port-prof)#</pre>	(任意) リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。												

メンバー VSD ポート プロファイルの設定

ここでは、個々のメンバーが存在する場所である VSD ポート プロファイルを設定する手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- メンバー VSD ポート プロファイルを SVM に対して設定しないでください。

メンバー VSD ポート プロファイルはサービス ポートを持たないので、SVM に対して設定されると、ネットワーク上でパケットフラッディングが発生します。

手順の概要

1. `config t`
2. `port-profile name`
3. `switchport access vlan vlanID`
4. `switchport trunk allowed vlan vlanID`
5. `virtual-service-domain name`
6. `no shut`
7. `state enabled`
8. `show virtual-service-domain name`
9. `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	config t 例： <pre>n1000v# config t n1000v(config)#</pre>	CLI グローバル コンフィギュレーション モードを開始します。
ステップ 2	port-profile name 例： <pre>n1000v(config)# port-profile vsdl-member n1000v(config-port-profile)#</pre>	ポート プロファイルを作成し、このポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。 ポート プロファイルには最大 80 文字の名前を設定できます。ポート プロファイル名は、Cisco Nexus 1000V 上の各ポート プロファイルに対して一意である必要があります。
ステップ 3	switchport access vlan vlanID 例： <pre>n1000v(config-port-profile)# switchport access vlan 315 n1000v(config-port-profile)#</pre>	このポート プロファイルのアクセス ポートに VLAN ID を割り当てます。

	コマンド	目的																
ステップ 4	virtual-service-domain name 例: <pre>n1000v(config-port-profile)# virtual-service-domain vsd1-webserver n1000v(config-port-profile)#</pre>	VSD 名をこのポート プロファイルに割り当てます。																
ステップ 5	no shutdown 例: <pre>n1000v(config-port-prof)# no shutdown n1000v(config-port-prof)#</pre>	管理上の目的でプロファイル内のすべてのポートをイネーブルにします。																
ステップ 6	state enabled 例: <pre>n1000v(config-port-prof)# state enabled n1000v(config-port-prof)#</pre>	VSD ポート プロファイルをイネーブルにします。 このポート プロファイルの設定が、割り当てられたポートに適用されます。また、vCenter Server 上の VMware vSwitch 内にポート グループが作成されます。																
ステップ 7	show virtual-service-domain name 例: <pre>n1000v(config-port-prof)# show virtual-service-domain vsd1-webserver Default Action: forward</pre> <table border="1"> <thead> <tr> <th>Interface</th> <th>Type</th> </tr> </thead> <tbody> <tr><td>Vethernet1</td><td>Member</td></tr> <tr><td>Vethernet2</td><td>Member</td></tr> <tr><td>Vethernet3</td><td>Member</td></tr> <tr><td>Vethernet6</td><td>Member</td></tr> <tr><td>Vethernet7</td><td>Inside</td></tr> <tr><td>Vethernet8</td><td>Outside</td></tr> <tr><td>n1000v(config-port-prof)#</td><td></td></tr> </tbody> </table>	Interface	Type	Vethernet1	Member	Vethernet2	Member	Vethernet3	Member	Vethernet6	Member	Vethernet7	Inside	Vethernet8	Outside	n1000v(config-port-prof)#		(任意) この VSD ポート プロファイルの設定を表示します。この表示を使用して、ポート プロファイルが正しく設定されていることを確認します。
Interface	Type																	
Vethernet1	Member																	
Vethernet2	Member																	
Vethernet3	Member																	
Vethernet6	Member																	
Vethernet7	Inside																	
Vethernet8	Outside																	
n1000v(config-port-prof)#																		
ステップ 8	copy running-config startup-config 例: <pre>n1000v(config-port-prof)# copy running-config startup-config [#####] #] 100% n1000v(config-port-prof)#</pre>	(任意) リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。																

設定の確認

VSD 設定を表示するには、次のコマンドを使用します。

コマンド	目的
show virtual-service-domain name vsd-name	特定の VSD の設定を表示します。 例 3-1 (P.3-9) を参照してください。
show virtual-service-domain brief	すべての VSD 設定の要約を表示します。 例 3-2 (P.3-9) を参照してください。

コマンド	目的
show virtual-service-domain interface	すべての VSD のインターフェイス設定を表示します。 例 3-3 (P.3-9) を参照してください。
module vem <i>module_number</i> execute vemcmd show vsd	VEM の VSD 設定を表示するために、リモートの Cisco Nexus 1000V から VEM にコマンドを送信します。 例 3-4 (P.3-10) を参照してください。
module vem <i>module_number</i> execute vemcmd show vsd ports	VEM の VSD ポート設定を表示するために、リモートの Cisco Nexus 1000V から VEM にコマンドを送信します。 例 3-5 (P.3-10) を参照してください。

これらのコマンドの出力の詳しい説明については、『Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)』を参照してください。

例 3-1 show virtual-service-domain name *vsd_name*

```
n1000v## show virtual-service-domain name vsd1
Default Action: drop
```

Interface	Type
Vethernet1	Member
Vethernet2	Member
Vethernet3	Member
Vethernet6	Member
Vethernet7	Inside
Vethernet8	Outside

```
n1000v#
```

例 3-2 show virtual-service-domain brief

```
n1000v# show virtual-service-domain brief
Name vsd-id default action in-ports out-ports mem-ports Modules with
VSD Enabled
zone 1 forward 1 1 2 4
n1000v#
```

例 3-3 show virtual-service-domain interface

```
n1000v# sho virtual-service-domain interface
```

Name	Interface	Type	Status
vsd1	Vethernet1	Member	Active
vsd1	Vethernet2	Member	Active
vsd1	Vethernet3	Member	Active
vsd1	Vethernet6	Member	Active
vsd1	Vethernet7	Inside	Active
vsd1	Vethernet8	Outside	Active
vsd2	Vethernet9	Inside	Active
vsd2	Vethernet10	Outside	Active

例 3-4 `module module_number execute vemcmd show vsd`

```
n1000v# module vem 4 execute vemcmd show vsd
ID Def_Act ILTL OLTTL NMLTL State Member LTLs
1 FRWD 51 50 1 ENA 49
n1000v#
```

例 3-5 `module module_number execute vemcmd show vsd ports`

```
n1000v# module vem 4 execute vemcmd show vsd ports
LTL IfIndex VSD_ID VSD_PORT_TYPE
49 1c000010 1 REGULAR
50 1c000040 1 OUTSIDE
51 1c000030 1 INSIDE
n1000v#
```

設定例

次に、VSD を設定する例を示します。

```
port-profile vsd1_member
  vmware port-group
  switchport access vlan 315
  virtual-service-domain vsd1
  no shutdown
  state enabled
port-profile svm_vsd1_in
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 310-319
  virtual-service-domain vsd1
  service-port inside default-action drop
  no shutdown
  state enabled
port-profile svm_vsd1_out
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 310-319
  virtual-service-domain vsd1
  service-port outside default-action drop
  no shutdown
```

その他の関連資料

VSD の設定に関連する詳細情報については、次の項を参照してください。

- 「[関連資料](#)」(P.3-11)
- 「[標準](#)」(P.3-11)

関連資料

関連項目	参照先
ポート プロファイル	『Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)』
CLI	『Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)』 『Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

機能の履歴

ここでは、VSD のリリース履歴を示します。

機能名	リリース	機能情報
VSD	4.0(4)SV1(2)	この機能が導入されました。

