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

Virtual Service Domain（VSD; 仮想サービス ドメイン）を利用すると、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キング）、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、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。

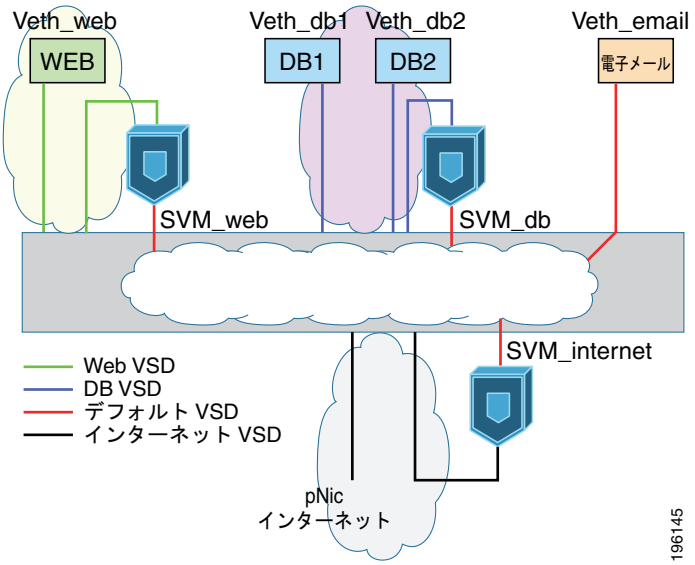
VSD を形成するには、次のポート プロファイルを作成します。

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、内側ポートを通って 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、外側ポートを通って SVM に入り、内側ポートから出て宛先へ転送されます。
メンバー	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ので、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 を再び稼動させます。

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
service-port default-action	転送
switchport trunk allowed vlan	All

VSD の設定

ここでは、次に示す手順を説明します。

- 「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。

始める前に

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 にログインしています。
- 設定エラーによるネットワークのフラッ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 を再び稼動させます。
- 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 フラッ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：
	`n1000v# config t`
	`n1000v(config)#`
		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：
	`n1000v(config)# port-profile webserver-inside`
	`n1000v(config-port-profile)#`
		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 プロファイル名の長さは最大 80 文字です。Cisco Nexus 1000V 上の各ポート プロファイルの名前は一意でなければなりません。

ステップ 3	**switchport mode trunk**
	
	例：
	`n1000v(config-port-profile)# switchport mode trunk`
	`n1000v(config-port-profile)#`
		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：
	`n1000v(config-port-profile)# switchport trunk allowed vlan all`
	`n1000v(config-port-profile)#`
		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：
	`n1000v(config-port-profile)# virtual-service-domain vsd1-webserver`
	`n1000v(config-port-profile)#`
		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：
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		プロファイル内のすべてのポートを管理目的でイネーブルにします。

ステップ 7	**vmware port-group** *pg-name*
	
	例：
	`n1000v(config-port-prof)# vmware port-group webservers-inside-protected`
	`n1000v(config-port-prof)#`
		ポート プロファイルが VMware ポート グループであることを指定します。
		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 接続が確立されると、Cisco Nexus 1000V で作成されたポート グループは、vCenter Server 上の仮想スイッチに配信されます。
		name：ポート グループ名。名前を指定しない場合は、ポート プロファイル名がポート グループ名となります。ポート プロファイルを別のポート グループ名にマッピングする場合は、pg-name オプションの後に別名を指定します。

	コマンド	目的
ステップ 8	**service-port** {**inside** | **outside**} [**default-action** {**drop** | **forward**}]	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。

	例：
	`n1000v(config-port-prof)# service-port inside default-action forward`
	`n1000v(config-port-prof)#`
		この例では、内側 VSD を設定します。この VSD では、サービス ポートがダウンした場合にパケットは転送されます。

	例：
	`n1000v(config-port-prof)# service-port outside default-action forward`
	`n1000v(config-port-prof)#`
		この例では、外側 VSD を設定します。この VSD では、サービス ポートがダウンした場合にパケットは転送されます。

ステップ 9	**state enabled**
	例：
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		VSD ポート プロファイルをイネーブルにします。
		割り当てられたポートに、このポート プロファイルの設定が適用され、ポート グループが vCenter Server 上の VMware vSwitch 内に作成されます。

ステップ 10	**show virtual-service-domain** *name*
	例：
	`n1000v(config-port-prof)# show virtual-service-domain vsd1-webserver`
	`Default Action: forward`
	`_____________________________`
	`Interface Type`
	`_____________________________`
	`Vethernet1 Member`
	`Vethernet2 Member`
	`Vethernet3 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確認します。

ステップ 11	**copy running-config startup-config**
	例：
	`n1000v(config-port-prof)# copy running-config startup-config`
	`[########################################] 100%`
	`n1000v(config-port-prof)#`
		（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーし、リブートと再起動を行って、永久的に保存します。

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。

始める前に

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 にログインしています。
- 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：
	`n1000v# config t`
	`n1000v(config)#`
		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 1	**port-profile** *name*
	
	例：
	`n1000v(config)# port-profile vsd1-member`
	`n1000v(config-port-profile)#`
		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 プロファイル名の長さは最大 80 文字です。Cisco Nexus 1000V 上の各ポート プロファイルの名前は一意でなければなりません。

ステップ 2	**switchport access vlan** *vlanID*
	
	例：
	`n1000v(config-port-profile)# switchport access vlan 315`
	`n1000v(config-port-profile)#`
		このポート 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 3	**virtual-service-domain** *name*
	
	例：
	`n1000v(config-port-profile)# virtual-service-domain vsd1-webserver`
	`n1000v(config-port-profile)#`
		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 4	**no shutdown**
	
	例：
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		プロファイル内のすべてのポートを管理目的でイネーブルにします。

ステップ 5	**state enabled**
	
	例：
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		VSD ポート プロファイルをイネーブルにします。
		
		割り当てられたポートに、このポート プロファイルの設定が適用され、ポート グループが vCenter Server 上の VMware vSwitch 内に作成されます。

ステップ 6	**show virtual-service-domain** *name*
	
	例：
	`n1000v(config-port-prof)# show virtual-service-domain vsd1-webserver`
	`Default Action: forward`
	
	`_____________________________`
	`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確認します。

ステップ 7	**copy running-config startup-config**
	
	例：
	`n1000v(config-port-prof)# copy running-config startup-config`
	`[########################################] 100%`
	`n1000v(config-port-prof)#`
		（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーし、リブートと再起動を行って、永久的に保存します。

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。
module vem *module_number* **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。
show virtual-service-domain brief	すべての VSD 設定の要約を表示します。
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。

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 4.0(4)SV1(3)*』を参照してください。

例 3-1　　show vsd

```
n1000v# module vem 3 execute vemcmd show vsd
 ID  Def_Act ILTL  OLTL  NMLTL  State    Member LTLs
  1   DROP    48    49     4     ENA    54,52,55,53
  2   FRWD    50    51     0     ENA
vsim-cp# module vem 3 execute vemcmd show vsd ports
  LTL   IfIndex    VSD_ID     VSD_PORT_TYPE
   48   1b020000     1          INSIDE
   49   1b020010     1          OUTSIDE
   50   1b020020     2          INSIDE
   51   1b020030     2          OUTSIDE
   52   1b020040     1          REGULAR
   53   1b020050     1          REGULAR
   54   1b020060     1          REGULAR
   55   1b020070     1          REGULAR
n1000v#
```

例 3-2　　show virtual-service-domain brief

```
n1000v# show virtual-service-domain brief
Name             default action    in-ports    out-ports   mem-ports
vsd1             drop              1           1           4
vsd2             forward           1           1           0
vsim-cp# 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
vsim-cp# show virtual-service-domain name vsd1
Default Action: drop

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

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.3-10）
- 「標準規格」（P.3-10）

関連資料

関連項目	マニュアル タイトル
ポート プロファイル	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)*』
CLI	『*Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)*』 『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

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)	この機能が追加されました。