CHAPTER 1

Cisco Virtual Security Gateway の概要

この章では、Cisco Nexus 1000V シリーズ スイッチおよび Cisco Nexus 1010 Virtual Services Appliance の Cisco Virtual Security Gateway（VSG）機能の概要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 Virtual Security Gateway に関する情報

ここでは、Cisco VSG の概要について説明します。内容は次のとおりです。

概要

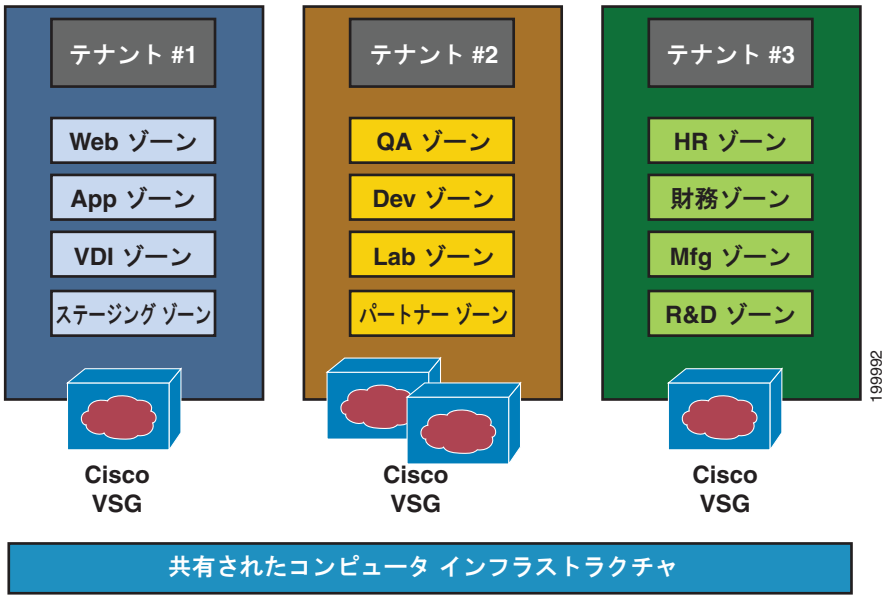
Cisco Virtual Security Gateway（VSG）は、仮想データセンターとクラウド環境への信頼性の高いアクセスを提供する仮想ファイアウォール アプライアンスです。Cisco VSG は、仮想データセンターのプライベート クラウドまたはパブリック クラウドで共通のコンピュータ インフラストラクチャを共有するためのさまざまなセキュリティ プロファイルを持つ、広範な組み合わせのマルチテナントの作業負荷を可能にします。個別の信頼ゾーンに 1 つ以上の仮想マシン（VM）を関連付けることにより、Cisco VSG では、確立されたセキュリティ ポリシーを介して信頼ゾーンへのアクセスが制御およびモニタされます。

Cisco VSG は、Cisco Nexus 1000V シリーズ スイッチ や Cisco Nexus 1010 と統合され、Cisco NX-OS オペレーティング システム上で実行されます。また、Cisco VSG には次の利点があります（図 1-1 を参照）。

- 信頼できるマルチテナント アクセス：法規制の遵守を強化し、監査を簡素化するための、マルチテナント（スケールアウト）環境におけるコンテキスト対応セキュリティ ポリシーによるゾーンベースの制御およびモニタリング。セキュリティ ポリシーは、セキュリティ プロファイル テンプレートへと組織され、多くの Cisco VSG の管理および配置を簡素化します。

- ダイナミック操作：VM がインスタンス化する間のセキュリティ テンプレートおよび信頼ゾーンのオンデマンド プロビジョニングと、異なる物理サーバ間で VM のライブ移行が発生するときのモビリティ トランスペアレントの適用およびモニタリング。
- 中断しない管理：セキュリティ全体およびサーバ チーム全体における管理分離。コラボレーションを提供し、管理者によるエラーを削除し、監査を簡素化します。

図 1-1　Cisco VSG をテナントごとに適用した信頼ゾーン ベースのアクセス コントロール



Cisco VSG には次の機能があります。

- 産業規制に準拠します。
- 仮想化環境の監査プロセスを簡略化します。
- 仮想データセンターまたはプライベート/パブリック クラウド コンピューティング環境などの共有されたコンピュータ インフラストラクチャ上で、複数のテナントにわたって仮想化された作業負荷をセキュアに配置することにより、コストを軽減します。

製品のアーキテクチャ

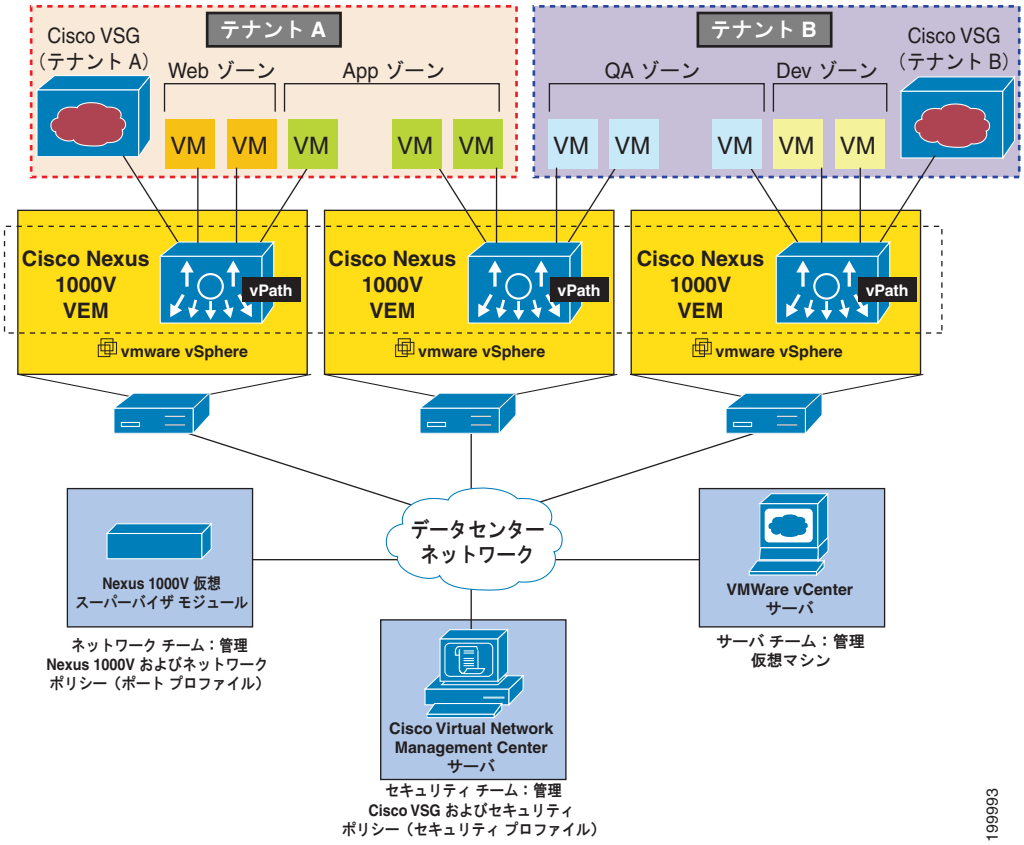
Cisco VSG は、VMware vSphere ハイパーバイザの Cisco Nexus 1000V とともに動作します。また、Cisco VSG は、Nexus 1000V 仮想イーサネット モジュール（VEM）に組み込まれている仮想ネットワーク サービス データパス（vPath）を活用します（図 1-2 を参照）。vPath は、トラフィックをテナントの Cisco VSG に誘導します（外部から VM、または VM から VM）。Cisco VSG では初期パケットの処理が行われ、ポリシーが評価および適用されます。ポリシーが決定すると、Cisco VSG は vPath への残りのパケットのポリシー適用をオフロードします。vPath は次の機能をサポートします。

- インテリジェントなインターセプトとリダイレクション：テナント対応のフロー分類およびそれに続く指定した Cisco VSG のテナントへのリダイレクション
- 高速パスのオフロード：Cisco VSG によって vPath へオフロードされたフローの、テナントごとのポリシー適用

Cisco VSG および Nexus 1000V VEM には、次の利点があります（図 1-3 を参照）。

- 効率的な配置：各 Cisco VSG は複数の物理サーバにわたってアクセスおよびトラフィックを保護できます。これにより、物理サーバごとに仮想アプライアンスを配置する必要がなくなります。
- パフォーマンスの最適化：Cisco VSG は、高速パスを 1 つまたは複数の Cisco Nexus 1000V VEM vPath モジュールへオフロードすることにより、分散 vPath ベースの適用を介してネットワークのパフォーマンスを向上させます。
- 動作の簡易性：Cisco VSG は、複数のスイッチ作成や、一時的に異なるスイッチまたはサーバに VM を移行する必要がなく、ワンアーム モードで透過的に挿入できます。ゾーン拡張は、仮想アプライアンスに限定されている vNIC ではなく、セキュリティ プロファイルに基づきます。ゾーン拡張は物理サーバのアップグレードを簡素化します。セキュリティの漏洩やアプリケーションの停止はほとんど発生しません。
- ハイ アベイラビリティ：各テナントに対し、Cisco VSG をアクティブ/スタンバイ モードで配置し、可用性の高い動作環境を実現します。プライマリ Cisco VSG が使用できないときは、vPath によりパケットがスタンバイ Cisco VSG にリダイレクトされます。
- 独立したキャパシティ プランニング：Cisco VSG は、最大計算能力がアプリケーションの作業負荷に割り当てられるように、セキュリティ運用チームによって制御された専用サーバに配置できます。キャパシティ プランニングがサーバとセキュリティ チームにわたって独自に実行され、セキュリティ、ネットワークおよびサーバ チームにわたるオペレーション分離を維持できます。

図 1-2　Cisco Virtual Security Gateway の配置トポロジ



高速パスの接続タイムアウト

最初に VEM が保護された VM のパケットを検知すると、VEM は Cisco VSG にそのパケットをリダイレクトし、実行するアクションを決定します（例：許可、ドロップ、リセットなど）。アクションが決定されると、Cisco VSG と VEM の両方が接続情報およびアクションを一定期間保存します。この間、この接続のためのパケットは、追加のポリシー検索なしで同じアクションに従います。高速パスの接続としてこの接続を考慮します。トラフィックおよびアクションにより、接続が高速パスに留まる時間が異なります。表 1-1 に、高速パスの接続タイムアウトの詳細を示します

表 1-1　高速パスの接続タイムアウト

プロトコル	接続状態	タイムアウト
TCP	FIN および ACKACK で閉じる	VEM：4 秒 VSG：4 秒
	RST で閉じる	VEM：4 秒 VSG：4 秒
	アクションのドロップ	VEM：4 秒 VSG：4 秒
	アクションのリセット	VEM：4 秒 VSG：4 秒
	アイドル	VEM：36 ～ 60 秒 VSG：630 ～ 930 秒
UDP	アクションのドロップ	VEM：4 秒 VSG：4 秒
	アクションのリセット	VEM：4 秒 VSG：4 秒
	アイドル	VEM：8 ～ 12 秒 VSG：240 ～ 360 秒
	宛先 到達不要	VEM：4 秒 VSG：4 秒
L3/ICMP	アクションのドロップ	VEM：2 秒 VSG：2 秒
	アクションのリセット	VEM：2 秒 VSG：2 秒
	アイドル	VEM：8 ～ 12 秒 VSG：16 ～ 24 秒
L2（例：IPv6）	アクションのドロップ	VEM：2 秒 VSG：2 秒
	アクションのリセット	VEM：2 秒 VSG：2 秒
	アイドル	VEM：8 ～ 12 秒 VSG：12 ～ 18 秒

信頼できるマルチテナント アクセス

Cisco Nexus 1000V 分散仮想スイッチが配置された VMware vSphere 環境に Cisco VSG を透過的に挿入できます。Cisco VSG の 1 つ以上のインスタンスは、テナントごとに配置されます。これにより多くのテナントからなる大規模な配置が可能になります。テナントは相互に独立しているため、トラフィックはテナントの境界を越えることはできません。Cisco VSG は、テナント レベル、仮想データセンター（vDC）レベル、および vApp レベルで配置できます。

VM は特定のテナントについてインスタンス化されるため、VM とセキュリティ プロファイルおよびゾーン メンバシップとの関連付けは、Cisco Nexus 1000V ポート プロファイルとのバインディングを介してただちに実行されます。各 VM は配置され論理的な信頼ゾーンへとインスタンス化されます（図 1-2 を参照）。セキュリティ プロファイルには、各ゾーンを出入りするトラフィックのアクセス ポリシーを指定するコンテキスト対応ルール セットが含まれています。セキュリティ管理者は、VM とネットワーク コンテキストに加え、セキュリティ プロファイルを介してゾーンを直接定義するためにカスタム属性を使用できます。ゾーンからゾーンへのトラフィックに加え、外部からゾーン（およびゾーンから外部）へのトラフィックにも制御が適用されます。ゾーン ベースの適用は VLAN 内で行われ、VLAN は頻繁にテナントの境界を識別します。Cisco VSG はアクセス コントロール ルールを評価した後、設定により、Cisco Nexus 1000V VEM vPath モジュールへの適用をオフロードする場合があります。Cisco VSG は。アクセスを許可または拒否できます。また、オプションのアクセス ログが生成される場合もあります。Cisco VSG は、アクセス ログを使用したポリシー ベースのトラフィック モニタリング機能も提供します。

Cisco VSG のテナントは、複数のハイパーバイザにまたがる VM を保護できます。各テナントは、重複（プライベート）IP アドレス空間が割り当てられます。IP アドレス空間はマルチテナント クラウド環境では重要です。

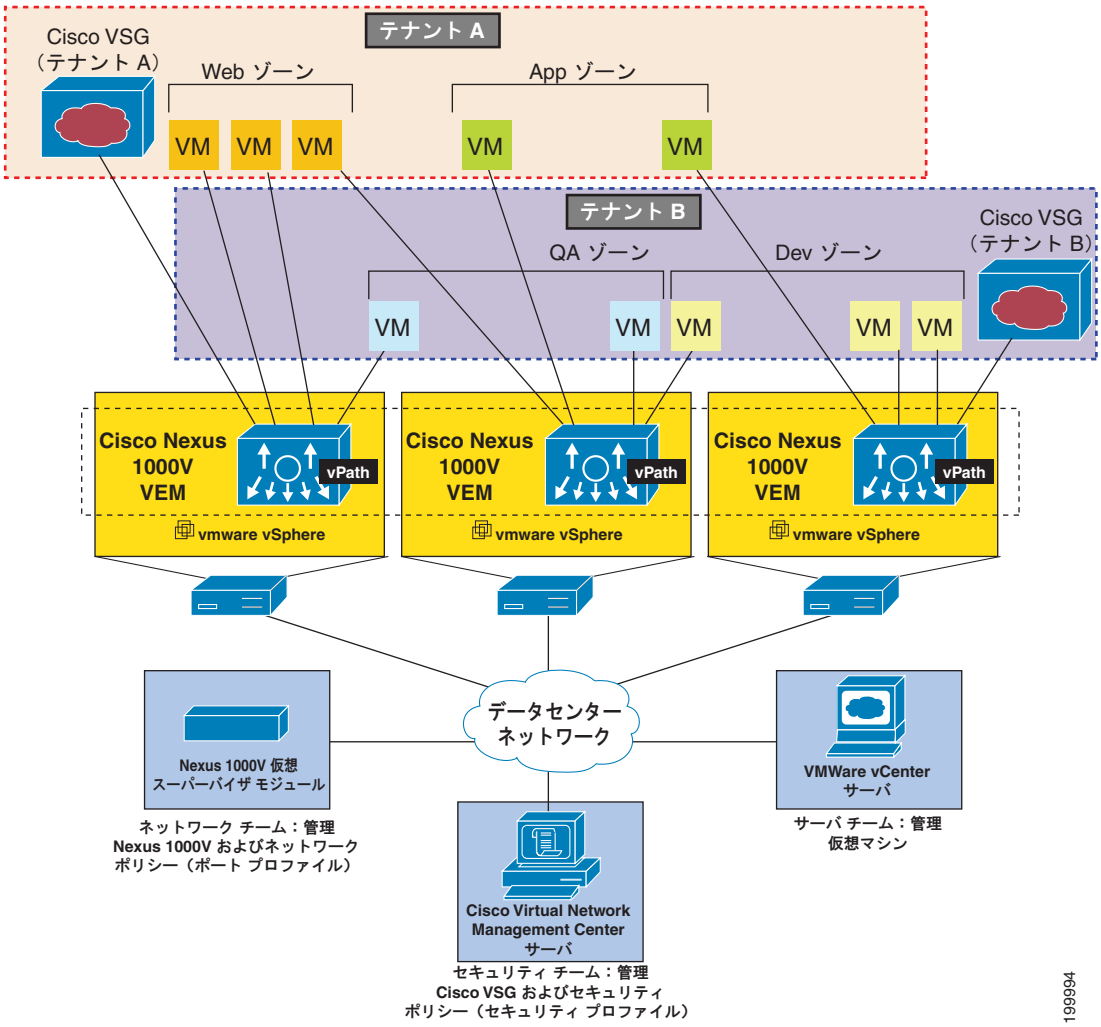
ダイナミック（仮想化対応）動作

仮想化環境はダイナミックであり、テナント全体と VM 全体で頻繁に追加、削除、および変更が行われます。また、VM のライブ移行は、手動またはプログラマチック vMotion イベントにより発生します。図 1-3 に、構造化環境（図 1-2 を参照）が、このダイナミック VM 環境により時間とともに変化する例を示します。

Cisco VSG は、Cisco Nexus 1000V（および vPath）とともに動作し、ダイナミック VM 環境をサポートします。通常、Cisco VSG（スタンドアロンまたはアクティブ / スタンバイ ペア）で Cisco Virtual Network Management Center（VNMC）にテナントを作成すると、関連するセキュリティ プロファイル（信頼ゾーン定義およびアクセス コントロール ルールを含む）が定義されます。各セキュリティ プロファイルは、Cisco Nexus 1000V ポート プロファイル（Cisco Nexus 1000V Virtual Supervisor Module（VSM）で作成され、VMware 仮想センターに発行されたもの）にバインドされます。サーバ管理者は、新しい VM がインスタンス化される際、VM の仮想イーサネット ポートにポート プロファイルを割り当てます。ポート プロファイルが一意にセキュリティ プロファイルと VM ゾーン メンバシップを参照するため、セキュリティ制御はただちに適用されます。VM は、異なるポート プロファイルまたはセキュリティ プロファイルを割り当てることにより再利用できます。

vMotion イベントがトリガされると、VM が物理サーバ間を横断します。Cisco Nexus 1000V はポート プロファイル ポリシーが VM に従うようにするため、関連するセキュリティ プロファイルもこれらの移動 VM に従い、セキュリティ適用およびモニタリングは vMotion イベントに対して透過的であり続けます。

図 1-3　ダイナミック VM 環境の Cisco VSG セキュリティ（VM のライブ移行を含む）



Cisco Nexus 1010 Virtual Services Appliance 上の Cisco VSG

Cisco Virtual Security Gateway（VSG）は、Cisco Nexus 1010 Virtual Services Appliance 上でホスティングできます。Cisco Nexus 1010 は、Cisco Network Analysis Module（NAM）、Virtual Supervisor Module（VSM）、または Cisco VSG として設定できる最大 6 つの仮想サービス ブレード（VSB）をホストします。VMware 仮想マシンでホストされた VSM は、Cisco VSG として Cisco Nexus 1010 上でホスティングできます。

Cisco VSG のソフトウェアは、別の Cisco Nexus 1010 用ソフトウェア（キックスタート イメージとハイパーバイザを含む）にバンドルされています。Cisco Nexus 1010 上で Cisco VSG を実装するためのソフトウェアは VSB 作成用のソフトウェアに付属しており、ブートフラッシュ リポジトリに格納されています。

図 1-4 では、Cisco Nexus 1010 上で VSM と Cisco VSG を実行した場合と、仮想マシン上で VSM と Cisco VSG を実行した場合を比較しています。

図 1-4　VM と Cisco Nexus 1010 の比較

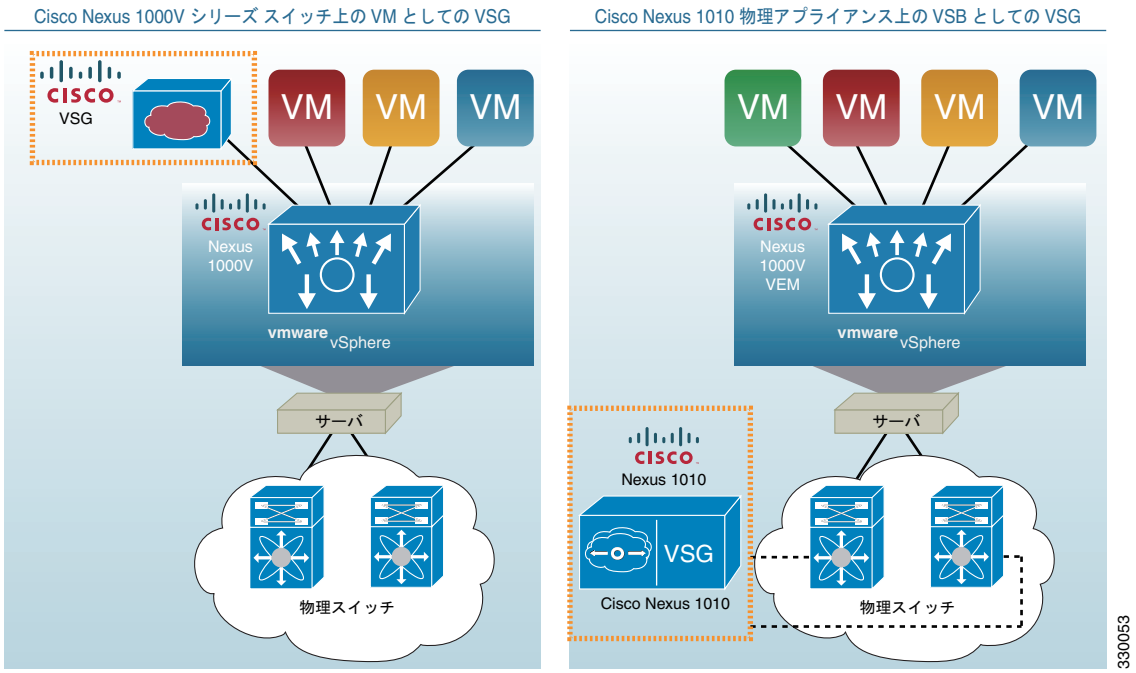
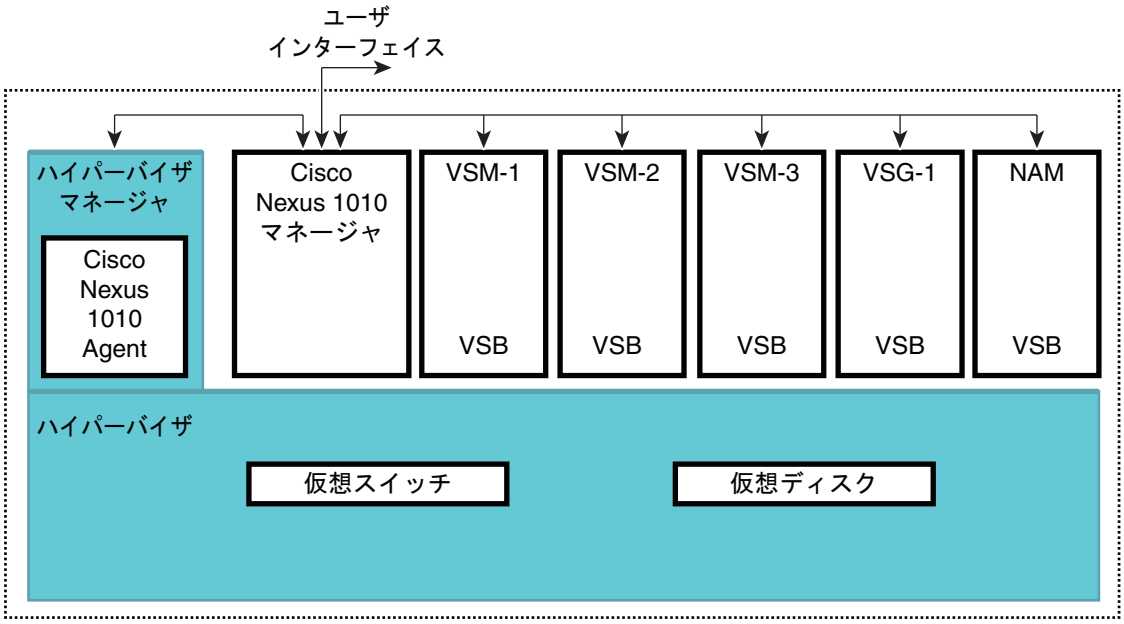


図 1-5 に、Cisco Nexus 1010 ソフトウェア コンポーネントと Cisco VSG との関連を示します。

図 1-5　Cisco Nexus 1010 ソフトウェア コンポーネント



Cisco Nexus 1010 の詳細については、『*Cisco Nexus 1010 Software Configuration Guide*』を参照してください。

Cisco VSG の配置シナリオ

Release 4.2(1)VSG1(3.1) 以前のリリースでは、Cisco VSG は VEM へのレイヤ 2 隣接に配置する必要があります。このように配置された場合、このマニュアルでは、Cisco VSG がレイヤ 2 モードで動作すると表現されます。

現在のバージョンは Cisco VSG のレイヤ 3 モードでの配置をサポートします。Cisco VSG および VEM は同じレイヤ 2 ネットワーク内にある必要はありません。VEM および Cisco VSG は、Virtual Kernel NIC（vmknic）という特殊な仮想ネットワーク インターフェイスを介して相互に通信します。この vmknic は、管理者により作成されます。

（注）　VEM への隣接は、vPath および Cisco VSG が同じレイヤ 2 ネットワークに属しているため、vPath がルータなしでレイヤ 2 の Cisco VSG と対話できることを意味します。

レイヤ 3 モードの Cisco VSG の VEM インターフェイス

VEM にレイヤ 3 モードの Cisco VSG に保護された VM がある場合、VEM は、レイヤ 3 モードの Cisco VSG パケットを終端させるために少なくとも 1 つの IP/MAC ペアが必要です。VEM はルータではなく IP ホストとして機能し、IPv4 アドレスだけをサポートします。

VEM のレイヤ 3 コントロールの設定と同様に、レイヤ 3 モードの Cisco VSG との通信に使用する IP アドレスは、**capability l3-vn-service** コマンドを持つ vmknic にポート プロファイルを割り当てることによって設定されます。

vmknic インターフェイス VEM の使用を設定するために、ポート プロファイル コンフィギュレーションの **capability l3-vn-service** コマンドを使用してポート プロファイルを割り当てることができます。

vPC-HM MAC ピン接続が必要なサーバ コンフィギュレーションの複数のアップリンク（またはサブグループ）上で、レイヤ 3 モードの Cisco VSG のトラフィックを伝送するために、最大 4 つの vmknic を設定できます。同じ ESX/ESXi ホスト内の、レイヤ 3 モードの VXLAN vmknic すべてを、**capability l3-vn-service** パラメータを使用してポート プロファイルに割り当てることを推奨します。

ローカル vEthernet インターフェイスで送信され、Cisco VSG にリダイレクトされる必要のあるレイヤ 3 モードのトラフィックは、フレーム内の送信元 MAC に基づき、この vmknic 間で分散されます。VEM は、レイヤ 3 モードの複数の vmknic を自動的にピン接続し、アップリンクを分割します。アップリンクに障害が発生すると、VEM は vmknic を動作中のアップリンクに自動的に再度ピン接続します。

Cisco VSG 宛てのカプセル化されたトラフィックが vmknic サブネット以外の異なるサブネットに接続されている場合、VEM は VMware ホスト ルーティング テーブルを使用しません。代わりに、vmknic はリモート Cisco VSG IP アドレスに対して ARP を開始します。アップストリーム ルータは、プロキシ ARP 機能を使用して応答するように設定する必要があります。

Virtual Extensible LAN

現在のリリースでは、Cisco Nexus 1000v は Virtual Extensible LAN（VXLAN）機能をサポートします。これは 24 ビット LAN セグメント ID を定義し、クラウド スケールのセグメンテーションを提供します。

VXLAN は次をイネーブル化します。

- 異なるサブネット上に配置された仮想マシン間で拡張される論理ネットワーク。
- 異なるサブネットに追加される新しいサーバ。
- 異なるサブネット内のサーバ間を移行する仮想マシン。

同じ VXLAN に存在する VM は、Cisco VSG で保護できます。

（注）　Cisco VSG は、VLAN 内に存在する必要があります。

ネットワークのための Cisco Virtual Security Gateway の設定

ここでは、ネットワークのための Cisco Virtual Security Gateway の設定について説明します。次の項目を取り上げます。

- 「Cisco VSG および VLAN のセットアップ」（P.1-9）
- 「Cisco VSG の設定の概要」（P.1-10）
- 「レイヤ 2 モードの Cisco VSG を設定する場合のシーケンス」（P.1-13）

Cisco VSG および VLAN のセットアップ

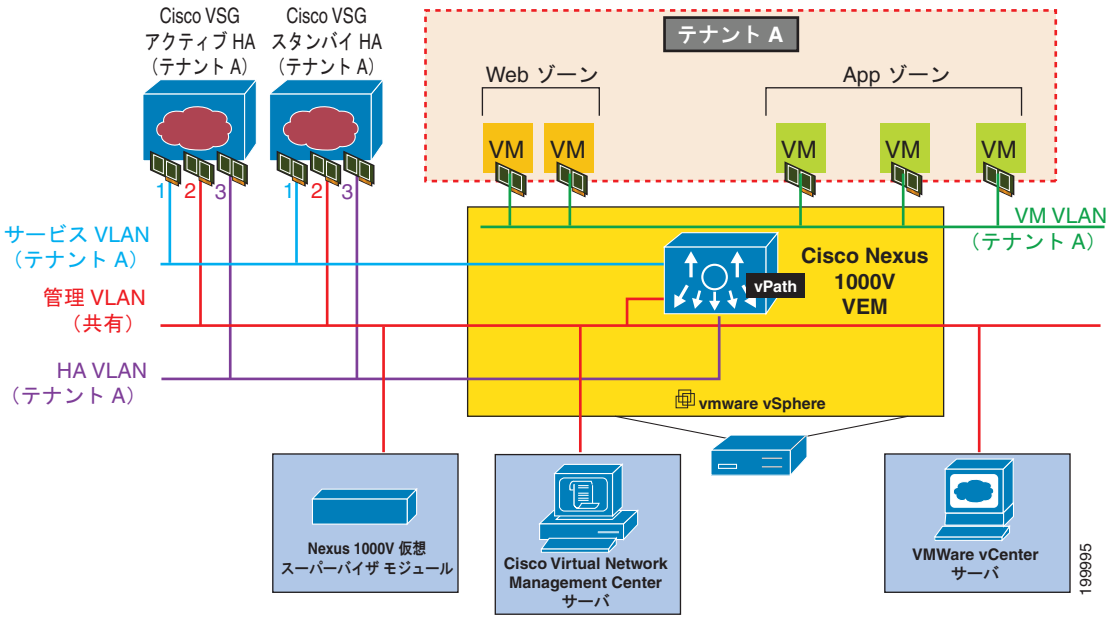
Cisco VSG は、その位置にかかわらず VM が Cisco VSG に到達できるようにセットアップされます。Cisco Nexus 1000V VEM の vPath コンポーネントは、VM からのパケットを代行受信し、さらなる処理を行うために Cisco VSG に送信します。

図 1-6 に、Cisco VSG を示します。この図では、Cisco VSG に 3 つの異なる VLAN（管理 VLAN、サービス VLAN、および HA VLAN）が接続されています。Cisco VSG には 3 つの vNICS が設定され、各 vNIC が VLAN のいずれかに接続されます。VLAN の機能は次のとおりです。

- 管理 VLAN は VMware vCenter、Cisco Virtual Network Management Center、および Cisco Nexus 1000V VSM などの管理プラットフォームや、管理対象の複数の Cisco VSG を接続します。
- サービス VLAN は、Cisco Nexus 1000V VEM と複数の Cisco VSG との間の通信を提供します。すべての Cisco VSG は、サービス VLAN の一部であり、VEM はこの VLAN を使用して Cisco VSG と通信します。
- HA VLAN は、ハートビート メカニズムで、マスター / スレーブ関係を識別します。

VM から VM への通信のために、1 つまたは複数の VM データ VLAN を割り当てることができます。マルチテナント環境では、管理 VLAN はすべてのテナント間で共有され、サービス VLAN、HA VLAN、および VM データ VLAN はテナントごとに割り当てられます。ただし、VLAN のリソースが少ない場合は、サービスおよび HA 機能用の単一の VLAN を使用することもできます。

図 1-6　Cisco Virtual Security Gateway の VLAN 使用状況



（注）　Cisco VSG は VXLAN 上にはありません。Cisco VSG は VXLAN のデータ トラフィックだけをサポートします。詳細については、『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

Cisco VSG の設定の概要

ここでは、Cisco VSG の設定の概要について説明します。次の項目を取り上げます。

- 「Cisco Nexus 1000V シリーズ スイッチ VSM」（P.1-10）
- 「ポート プロファイル」（P.1-11）
- 「Virtual Security Gateway」（P.1-11）
- 「セキュリティ プロファイル」（P.1-11）
- 「ファイアウォール ポリシー」（P.1-12）

Cisco VSG を仮想化されたデータセンター ネットワークにインストールした場合は、Cisco Nexus 1000V シリーズ スイッチ VSM および Cisco VSG の設定を変更する必要があります。

Cisco Nexus 1000V シリーズ スイッチ VSM

VSM は、論理的なモジュラ スイッチです。1 つの VSM が複数の VEM を制御します。VSM は、物理的なライン カード モジュールの代わりに、サーバ内のソフトウェアで実行される VEM をサポートします。設定は VSM を介して実行され、VEM に自動的に反映されます。1 つのホスト上のハイパーバイザ内にあるソフト スイッチを一度に設定する代わりに、VSM が管理するすべての VEM 上で、ただちに使用するための設定を定義できます。

ポート プロファイル

Cisco Nexus 1000V シリーズ スイッチ では、ポート プロファイルを使用してインターフェイスを設定します。VSM の管理インターフェイスを介して、複数のインターフェイスにポート プロファイルをすべて同じ設定で割り当てることができます。ポート プロファイルを変更すると、そのポート プロファイルが割り当てられているすべてのインターフェイスの設定に自動的に反映されます。

VMware vCenter Server では、ポート プロファイルはポート グループとして表されます。vEthernet インターフェイスまたは Ethernet インターフェイスは、vCenter Server で次の機能のポート プロファイルに割り当てられます。

- ポリシーによるポート設定の定義。
- 単一のポリシーの多数のポートへの適用。
- vEthernet ポートと Ethernet ポートの両方のサポート。

アップリンクとして設定されていないポート プロファイルは、VM 仮想ポートに割り当てられます。セキュリティ プロファイルと Cisco VSG の IP アドレスをバインドすると、VM ポート プロファイルは、Cisco VSG によって提供されるセキュリティ サービス（VM セグメンテーション用など）のプロビジョニングに使用できます。

Virtual Security Gateway

Cisco Nexus 1000V シリーズ スイッチ用 Cisco VSG は、仮想データセンターとクラウド環境への信頼されたアクセスを提供する仮想ファイアウォール アプライアンスです。管理者はホスト上でサービス VM として Cisco VSG をインストールし、セキュリティ プロファイルとファイアウォール ポリシーで設定できます。これにより、VM セグメンテーションおよび他のファイアウォール機能を提供し、VM へのアクセスを保護します。

セキュリティ プロファイル

Cisco Nexus 1000V シリーズ スイッチ ポート プロファイルは、各 VM のネットワーク パラメータをダイナミックにプロビジョニングします。同じポリシーのプロビジョニングは、VM がポート プロファイルに接続された場合、各 VM がネットワーク サービス ポリシーとダイナミックにプロビジョニングされるようにネットワーク サービスの設定情報を伝達します。このプロセスは、ポート プロファイルでの ACL または QoS ポリシーの関連付けと同様です。ネットワーク サービスの設定に関する情報は、セキュリティ プロファイルと呼ばれる独立したプロファイル内に作成され、ポート プロファイルに接続されます。セキュリティ管理者は、Cisco VSG にセキュリティ プロファイルを作成し、これをネットワーク管理者が VSM の適切なポート プロファイルに関連付けます。

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で設定されます。ネットワーク管理者はまた、特定のポート プロファイルに関連付けられている Cisco VSG をバインドします。ポート プロファイルに関連付けられている Cisco VSG は、そのポート プロファイルにバインドされるアプリケーション VM のネットワーク トラフィックのファイアウォール ポリシーを適用します。同じ Cisco VSG は、アプリケーション VM の位置に関係なく使用されます。このため、VMotion 手順を実行中でもポリシーは一貫して適用されます。トラフィックがサービス プロファイルにバインドされている場合、そのサービス プロファイルに関連付けられたポリシーが実行されるように、サービス プロファイル固有のポリシーをバインドすることもできます。サービス プレーンおよび管理プレーンは、両方ともマルチテナント機能の要件をサポートします。異なるテナントは、独自の Cisco VSG（または複数の Cisco VSG のセット）を持ち、個別に定義されたポリシーを適用できます。各 ESX ホストの vPath は、適切な Cisco VSG にテナント トラフィックをインテリジェントにリダイレクトできます。

ファイアウォール ポリシー

ファイアウォール ポリシーを使用して、Cisco VSG のネットワーク トラフィックを適用できます。Cisco VSG の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、Cisco 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。

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。

- 「オブジェクト グループ」（P.1-12）
- 「ゾーン」（P.1-12）
- 「ルール」（P.1-12）
- 「アクション」（P.1-12）
- 「ポリシー」（P.1-13）

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。

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、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。

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。

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

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
- リセット
- ログ
- インスペクション

ポリシー

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。Cisco VSG 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、Cisco VSG で受信したネットワーク 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 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。

サービス ファイアウォールのロギング

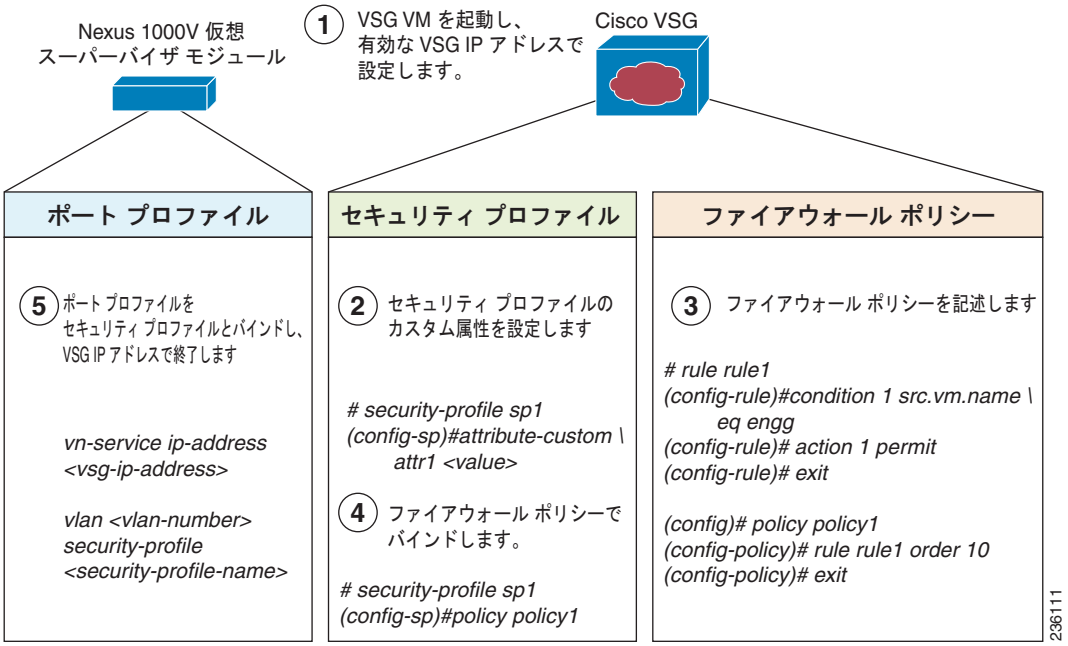
サービス ファイアウォールのログは、ポリシーのテストおよびデバッグを行うツールです。ポリシーの評価中に、ポリシー エンジンによりポリシー評価のポリシー結果が表示されます。このツールは、ポリシーをトラブルシューティングするユーザとポリシー記述者双方に役立ちます。

レイヤ 2 モードの Cisco VSG を設定する場合のシーケンス

ここでは、管理者としてレイヤ 2 モードの Cisco VSG を設定する場合に従う必要のあるシーケンスの概要について説明します （図 1-7 を参照）。

1. Cisco VSG サービス VM をインストールおよびセットアップし、有効な IP アドレスで Cisco VSG を設定します。
2. ファイアウォール ポリシーでカスタム属性を使用する場合は、Cisco VSG のセキュリティ プロファイル設定の一連のカスタム属性を作成します。
3. オブジェクト グループ、ゾーン、ルール、条件、アクション、ポリシーなどの適切なポリシー オブジェクトを使用して Cisco VSG 上でファイアウォール ポリシーを記述します。
4. ファイアウォール ポリシーを作成したら、以前に作成したセキュリティ プロファイルにポリシーをバインドします。この手順は、セキュリティ プロファイル管理インターフェイスを使用します。
5. セキュリティ プロファイルとファイアウォール ポリシーが完全に構築されると、VSM 上のポート プロファイル管理インターフェイスを介して、Cisco VSG 提供のアクセス保護を要求する VM ポート プロファイルとこのセキュリティ プロファイルをバインドできます。また、Cisco VSG を VM ポート プロファイルのセットとバインドする必要があります。

図 1-7　Cisco Virtual Security Gateway のレイヤ 2 設定フロー



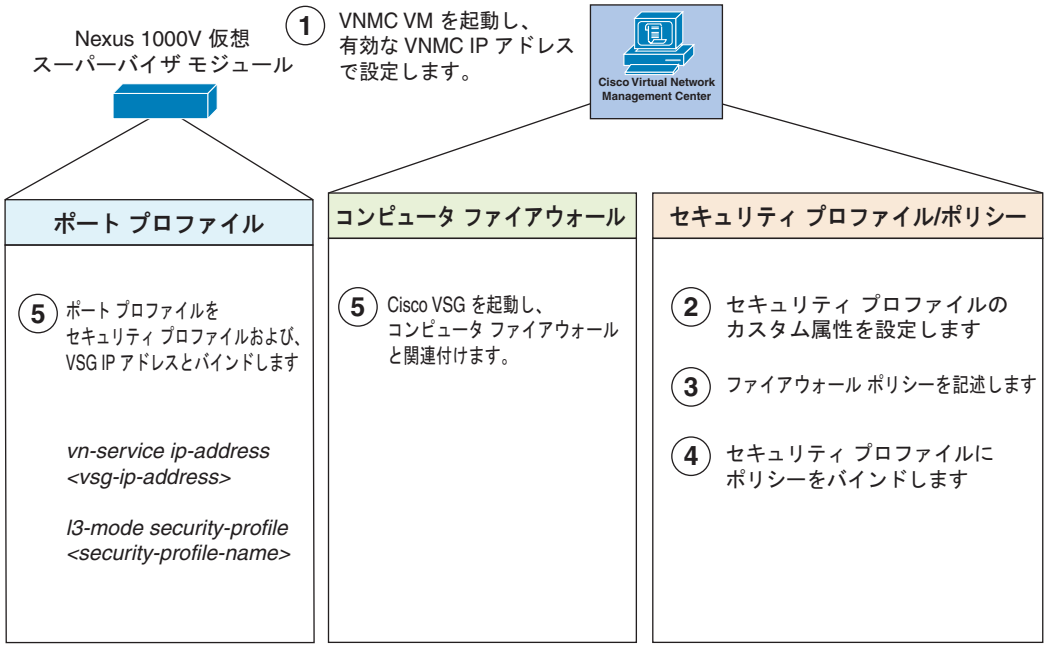
レイヤ 3 モードの Cisco VSG を設定する場合のシーケンス

レイヤ 3 モードの Cisco VSG を設定する前に、L# vmknic を作成します。詳細については、「レイヤ 3 モード VSG カプセル化のための vmknic の設定」（P.3-5）を参照してください。

ここでは、レイヤ 3 モードの Cisco VSG を設定する場合に従う必要のあるシーケンスの概要について説明します（図 1-8（P.1-15）を参照）。

1. Cisco VSG サービス VM をインストールおよびセットアップし、有効な IP アドレスで Cisco VSG を設定します。
2. 管理者としてファイアウォール ポリシーでカスタム属性を使用する場合は、Cisco VSG のセキュリティ プロファイル設定の一連のカスタム属性を作成します。
3. 管理者として、オブジェクト グループ、ゾーン、ルール、条件、アクション、ポリシーなどの適切なポリシー オブジェクトを使用して Cisco VSG 上でファイアウォール ポリシーを記述します。
4. ファイアウォール ポリシーを作成したら、管理者として、以前に作成したセキュリティ プロファイルにポリシーをバインドします。この手順は、セキュリティ プロファイル管理インターフェイスを使用します。
5. セキュリティ プロファイルとファイアウォール ポリシーが完全に構築されると、管理者として、VSM 上のポート プロファイル管理インターフェイスを介して、Cisco VSG 提供のアクセス保護を要求する VM ポート プロファイルとこのセキュリティ プロファイルをバインドできます。管理者として、Cisco VSG を VM ポート プロファイルのセットとバインドする必要があります。

図 1-8　Cisco Virtual Security Gateway のレイヤ 3 設定フロー



レイヤ 2 モードからレイヤ 3 モードへの移行

前提条件

1. ルータ（仮想または物理）には、2 つのレッグがあります
   - 1 つは L3 vmknic vlan (vlan 10) 5.5.5.x ネットワークにあります（下の例を参照）
   - もう 1 つは既存の Layer 2 Cisco VSG service vlan (vlan 5) 6.6.6.x ネットワークにあります（下の例を参照）
   - プロキシ ARP は、ルータの vlan 10 interface/leg でイネーブルになります
2. セットアップは 1.3 VNMC、1.3 Cisco VSG、および CN VSM/VEM にアップグレードされます

手順

ステップ 1　すべての VEM（vlan 10）に vmknic L3 を追加します。

a. アップリンク ポートの L3 vmknic vlan をプロビジョニングします。
b. l3 機能および vlan 10 を使用してポート プロファイルを作成します。
c. vmknic を作成し、b で作成されたポート プロファイルを vmknic と関連付けます。
d. 各 VEM ホストで手順 3 を繰り返します。

ステップ 2　VEM から VEM、VEM から VSG の L3 vmknic 接続を確認します。

a. 各 VEM からそのピアまで、VEM から VEM への vmkping を実行します。

```
[root@sg-dmastrop-sd4 Storage1 (1)]# vmkping 5.5.5.2
PING 5.5.5.2 (5.5.5.2): 56 data bytes
```

```
64 bytes from 5.5.5.2: icmp_seq=0 ttl=64 time=0.467 ms
```

b. VSM で ping vsn を実行し、VEM から VSG の接続を確認します。

```
vsm-d16-bl434(config-vnm-policy-agent)# ping vsn ip 6.6.6.99 src-module all
ping vsn 6.6.6.99 vlan 0 from module 3 4, seq=0 timeout=1-sec
  module(usec)   :  3(434)  4(434)


ping vsn 6.6.6.99 vlan 0 from module 3 4, seq=1 timeout=1-sec
  module(usec)   :  3(356)  4(481)


ping vsn 6.6.6.99 vlan 0 from module 3 4, seq=2 timeout=1-sec
  module(usec)   :  3(341)  4(448)


ping vsn 6.6.6.99 vlan 0 from module 3 4, seq=3 timeout=1-sec
  module(usec)   :  3(368)  4(466)


ping vsn 6.6.6.99 vlan 0 from module 3 4, seq=4 timeout=1-sec
  module(usec)   :  3(346)  4(414)
```

ステップ 3　ステップ a. または ステップ b に進みます（この手順の実行中に、ポート プロファイルを使用した VM からの新しいトラフィックの速度が低下するため、トラフィックが一時中断される場合があります。既存のフローは影響を受けません）。

a. 既存のレイヤ 2 モードのポート プロファイルを変更してレイヤ 3 モードをサポートします（新しいセッションは中断されます）。

1. レイヤ 2 モードのポート プロファイルで no-vn-service を実行し、既存の Layer 2 vn-service 設定を削除します。
2. 新しい vn-service を設定します。

```
Vn-service <same ip address> l3-mode security-profile  <same security-profile
name>
```

例：

```
vn-service ip-address 6.6.6.99 l3-mode security-profile L3mode2
```

b. 新しいレイヤ 3 モードのポート プロファイルを作成し、既存のレイヤ 2 モードのポート プロファイルはそのままにします。

1. 新しいレイヤ 3 モードのポート プロファイルを作成します。

例：

```
port-profile type vethernet L3_vlan121_VM
  vmware port-group
  switchport mode access
  switchport access vlan 121   <<< access vlan for the traffic VM
  org root/L3_mode/dc2
  no shutdown
  vn-service ip-address 6.6.6.99 l3-mode security-profile L3mode2
  state enabled
```

2. トラフィック VM のポート プロファイルを新しいレイヤ 3 モードのポート プロファイルに変更します（新しいセッションは中断されます）。