vShield Zones の概要

vShield Zones 1.0

JA-000188-00

vmware®

最新情報を反映したテクニカル ドキュメントは、ヴイエムウェア Web サイトにてご覧いただけます。

http://www.vmware.com/jp/support/

ヴイエムウェア Web サイトでは、最新の製品アップデート情報も提供しています。

本書に関するコメントがございましたら、次のメールアドレスまでご連絡ください。

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

目次

本書について

本『vShield Zones の概要』では、VMware® vShield Zones の機能について説明します。

対象読者

本書は、vShield Zones のコンポーネントおよび機能について習得する必要のある方を対象としています。本書に記載されている情報は、Windows または Linux のシステム管理者としての経験があり、仮想マシン テクノロジーおよびデータ センターの操作に詳しい方を対象としています。

本書へのフィードバック

ドキュメントの向上にご協力ください。本書に関するコメントがございましたら、メール アドレス docfeedback@vmware.com までフィードバックをお寄せください。

vShield Zones のドキュメント

vShield Zones のドキュメント セットは、次のドキュメントで構成されています。

- vShield Zones 管理ガイド
- vShield Zones クイック スタート ガイド
- vShield Zones の概要

テクニカル サポートおよび教育リソース

次のセクションでは、お客様にご利用いただけるテクニカル サポート リソースを紹介します。本書およびその他の文書の最新バージョンは、http://www.vmware.com/jp/support/pubs でご覧いただけます。

オンライン サポートおよび電話によるサポート

テクニカル サポート リクエストの提出や、製品および契約情報の確認、製品の登録をオンラインで行うには、http://www.vmware.com/jp/support をご覧ください。

該当するサポート 契約を結んでいるお客様の場合、迅速な対応が必要な Severity1 の問題に関しては電話でのサポート をご利用ください。詳細は、http://www.vmware.com/jp/support/phone_support をご覧ください。

サポート サービス

お客様のビジネス ニーズに適した各種サポートの詳細については、
http://www.vmware.com/jp/support/services をご覧ください。

ヴイエムウェア プロフェッショナル サービス

ヴイエムウェア教育サービスの有償トレーニングでは、広範なハンズオン ラボやケース スタディをご紹介します。また、業務の際のリファレンスとしてお使いいただける資料も提供しています。トレーニングは、オンサイト、講義形式、およびライブ オンラインで受講できます。オンサイトのパイロット プログラムおよび実装のベスト プラクティスについては、ヴイエムウェア コンサルティング サービスがご使用の仮想環境の評価、計画、構築、および管理に役立つサービスを提供しています。教育トレーニング、認定プログラム、およびコンサルティング サービスについては、http://www.vmware.com/jp/services をご覧ください。

vShield Zones の概要

vShield Zones とは、VMware vCenter™ Server の統合のために構築されるアプリケーション対応のファイアウォールです。vShield Zones は、攻撃と不正使用から仮想化データ センターを保護するために不可欠なセキュリティ コンポーネントであり、コンプライアンスへの確実な準拠を可能にします。

この章には、次のトピックが含まれています。

vShield Zones のコンポーネント

vShield Zones には、トラフィックの分析と仮想マシンの保護に不可欠なコンポーネントとサービスが含まれています。vShield Zones は、Web ベースのユーザー インターフェイスとコマンド ライン インターフェイス（CLI）を使用して構成できます。

vShield Zones のコンポーネントは、OVF （Open Virtualization Format）ファイルとしてパッケージにまとめられています。vShield Zones を実行するには、1 つの vShield Manager OVF と 1 つの vShield OVF が必要です。

vShield Manager

vShield Manager は、ネットワークを一元的に管理する vShield Zones のコンポーネントであり、vCenter Server 環境にある任意の ESX™ ホストに仮想マシンとしてインストールされます。vShield Manager は、vShield インスタンスとは異なる ESX ホストで実行できます。

vShield Manager のユーザー インターフェイスには、Web ブラウザを使用してアクセスできます。管理者はユーザー インターフェイスを使用して vShield Zones 環境全体のインストール、構成、および保守を行うことができます。vShield Manager のユーザー インターフェイスには、VMware Infrastructure SDK を利用して vSphere Client のインベントリ パネルのコピーが表示され、ホストおよびクラスタ ビューとネットワーク ビューも表示されます。

サポートされている次のいずれかの Web ブラウザを使用して、vShield Manager のユーザー インターフェイスに接続できます。

- Internet Explorer 5.x 以降
- Mozilla Firefox 1.x 以降
- Safari 1.x または 2.x

vShield

vShield は、vShield Zones のアクティブなセキュリティ コンポーネントです。個々の vShield インスタンスが、ネットワーク トラフィックを調べて一群のルールに基づきアクセスの権限を決定することにより、アプリケーション対応のトラフィック分析とステートフルなファイアウォール保護を提供します。vShield はトラフィックを保護ゾーンと非保護ゾーンに分け、トラスト ゾーンに基づいてトラフィックを制御します。vShield によって保護されている仮想マシンは保護ゾーンにあります。保護されている仮想マシンに送信されるすべてのトラフィックは、非保護ゾーンで受信されます。

vSphere Client を使用して、vShield OVF ファイルをテンプレートまたは仮想マシンとしてインストールできます。vSphere Client にパッケージをインストールしたあと、vShield Manager を使用してインストールを完了します。vShield パッケージをテンプレートとしてインストールした場合、vShield Manager からテンプレートを参照して、複数の vShield インスタンスを vCenter Server 環境に仮想マシンとしてインストールできます。vShield インスタンスは、物理 NIC に接続しているすべての vSwitch にインストールできます。ESX ホストには複数の物理 NIC を設定できるため、複数の vShield インスタンスを単一の ESX ホストにインストールできます。

vShield を参照テンプレートからインストールする際は、インストール プロセスによって次の手順が実行されます。

1 vSwitch ホストのクローンを作成します。

この vSwitch クローンに NIC は含まれません。vSwitch クローンの名前は、vSwitch ホスト名に _VS を付加した名前になります（例：vSwitch1_VS）。

2 保護ゾーンのポート グループ VSprot_vShield 名 を作成し、このポート グループを vSwitch ホストに追加します。

3 vShield インスタンスの管理インターフェイス用の vSwitch ホスト上に、管理ポートグループ VSmgmt_vShield 名を作成します。

4 保護ゾーンのポート グループ VSunprot_vShield 名を作成し、このポート グループを vSwitch クローンに追加します。

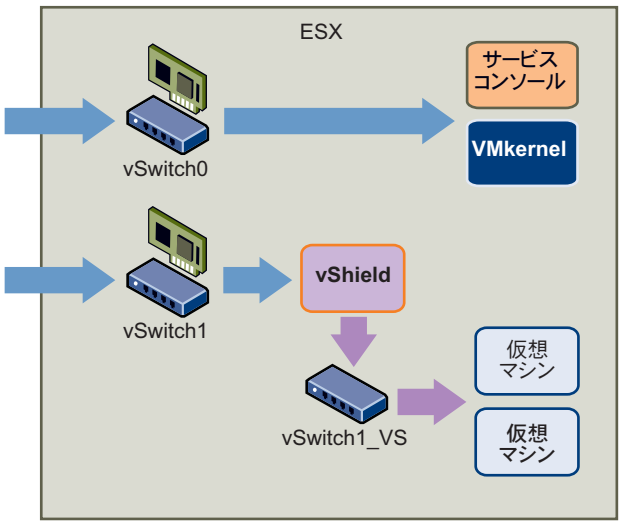
5 vShield インスタンスに接続し、インスタンスをパワーオンします。

6 vShield 上の仮想インターフェイスを非保護ポート グループと保護ポート グループに追加します。

7 仮想マシンを vSwitch ホストから vSwitch クローンに移動します。

同じ vSwitch 上に vShield Manager の仮想マシンがある場合、仮想マシンは移動されません。vShield Manager のインストール中に、vShield Manager を格納するための **`vsmgmt`** というポート グループを作成しました。vShield のインストールプロセスではこのポートグループ名が識別され、このポートグループ内のすべての仮想マシンが無視されます。

図 1. vSwitch への vShield のインストール



インストールされた個々の vShield インスタンスは、vSwitch ホスト上の仮想マシンと vSwitch クローン上の仮想マシンの間のトラフィックを含む、vSwitch ホスト上のすべての受信トラフィックと送信トラフィックを監視します。トラフィックが vShield を通過すると、データのカタログ化のために各セッション ヘッダーが調べられます。各仮想マシンについて、オペレーティング システム、アプリケーション、およびネットワーク通信に使用されるポートについて詳述したプロファイルが作成されます。vShield ではこの情報に基づいて、FTP や RPC のような動的プロトコルの通過が許可されて一時ポートを使用できるようになりますが 1024 以上のポートのロックダウンは維持されます。

設計上、各 vShield インスタンスでは、最大 40,000 の同時セッションが可能です。

サービス コンソールや VMkernel は仮想マシンではないため、vShield を使用して保護することはできません。

主な機能

vShield Zones は、仮想マシンとの間で送受信されるトラフィックについての情報を提供し、仮想データ センター内の仮想マシンを保護するための豊富な機能群を提供します。

ファイアウォール保護

vShield Zones は、導入された vShield インスタンス全体にグローバルおよびローカルのアクセス制御ポリシーを適用することによって、ファイアウォール保護を提供します。vShield Zones を使用すると、全般的なトラフィックの方向、アプリケーション プロトコルとポート、および特定の送信元と宛先のパラメータに基づいてファイアウォールのルールを作成できます。

vShield Manager のユーザー インターフェイス内の **[VM Wall]** タブに、vShield Zones のファイアウォール機能が表示されます。VM Wall は階層構造の一元的なアクセス コントロール リストです。これらのコンテナに複数の vShield インスタンスにまたがる一貫したルール セットを適用することで、VM Wall のアクセス ルールをデータ センターおよびクラスタ レベルで管理できます。これらのコンテナ内の仮想マシンのメンバーシップは動的に変化することができるため、アクセス ルールを再構成しなくても、vShield Zones によって既存のセッションの状態が維持されます。

デフォルトのルール

VM Wall は、デフォルトではトラフィックがすべての vShield インスタンスを通過できるルール セットを適用します。これらのルールは VM Wall テーブルの **[Default Rules]** セクションに表示されます。デフォルトのルールは削除することも追加することもできません。ただし、各ルールの **[Action]** 要素については、**[Allow]** から **[Deny]** に変更することができます。

レイヤー 4 ルールおよびレイヤー 2/ レイヤー 3 ルール

[VM Wall] タブには、L4（レイヤー 4）ルールと L2 / L3（レイヤー 2 / レイヤー 3）ルールという、構成可能な 2 組のルールがあります。ここでのレイヤーは、OSI（Open Systems Interconnection）参照モデルのレイヤーを指します。

レイヤー 4 ルールは、レイヤー 7 の TCP トランスポートおよび UDP トランスポート、つまりアプリケーション固有のトラフィックを管理します。VM Wall ルールのほとんどの操作は、レイヤー 4 ルールの管理が中心です。

レイヤー 2/ レイヤー 3 ルールは、ICMP、ARP、およびその他のレイヤー 2 プロトコルとレイヤー 3 プロトコルを監視します。レイヤー 2 とレイヤー 3 を制御する VM Wall ルールは、デフォルトではすべてのトラフィックの通過を許可します。レイヤー 2/ レイヤー 3 ルールはデータ センター レベルでのみ適用されます。

VM Wall ルールの階層

個々の vShield インスタンスは VM Wall ルールを上から順に適用します。vShield は、VM Wall テーブル内の上位ルールと照合し、テーブル内の後続のルールに移る前に各トラフィック セッションをチェックします。テーブル内のルールのうち、トラフィック パラメータと一致する最初のルールが適用されます。

VM Wall は、コンテナ レベルおよびカスタムの優先順位構成を提供します。

- コンテナ レベルの優先順位では、クラスタ レベルよりもデータ センター レベルの方が優先度が高いと認識します。ルールがデータ センター レベルで構成されるときは、すべてのクラスタおよびその中に含まれるすべての vShield インスタンスにそのルールが継承されます。クラスタ レベルのルールは、クラスタ内の vShield インスタンスにのみ適用されます。
- カスタムの優先順位とは、データ センター レベルで作成されたルールに高い優先順位や低い優先順位を割り当てるオプションを指します。**データ センターの高優先順位ルール**は、コンテナ レベルの優先順位ルールと同じように機能します。**データ センターの低優先順位ルール**は**クラスタ レベルのルール**より優先度が低いですが、事前構成済みの**デフォルトのルール**より優先されます。このように柔軟性が高いため、適用された優先順位の複数のレイヤーを認識することができます。

VM Wall テーブルでは、次の階層に従ってルールが適用されます。

1 **データ センターの高優先順位ルール :** グローバル アクセス ルールのセット。データ センター レベルで作成され、最も優先順位が高いルールです。

2 **クラスタ レベルのルール :** クラスタ固有のアクセス ルール セット。データ センターの高優先順位ルールより優先順位は低くなります。

3 **データ センターの低優先順位ルール :** グローバル アクセス ルールのセット。データ センター レベルで作成され、クラスタ レベルのルールよりも優先順位が低いルールです。

4 **デフォルトのルール :** デフォルト のグローバル アクセス ルール セット。最も 優先順位が低いルールです。

全般的な指針として、優先順位の低いルールが優先順位の高いルールと競合しないようにしてください。

VM Wall ルールの適用計画

VM Wall を使用すると、自社のネットワーク ポリシーに基づいて許可ルールと拒否ルールを構成できます。VM Wall の一般的な構成は、次の指針に従って行われます。

- デフォルト のルールを維持してすべてのトラフィックを許可し、トラフィックの統計や手動の構成に基づいてデータ センターレベルとクラスタ レベルで拒否ルールを追加する。このシナリオでは、セッションがどのカスタムの拒否ルールにも 一致しない場合、vShield はトラフィックの通過を許可します。
- デフォルト のルールのステータスを **[Allow]** から **[Deny]** に変更し、特定のシステムとアプリケーションについて、データ センター レベルとクラスタ レベルで許可ルールを追加する。このシナリオでは、セッションがどのカスタムの許可ルールにも 一致しない場合、vShield はセッションを宛先に届く 前にドロップします。デフォルト のルールをすべて変更し、許可ルールを作成せずにすべてのトラフィックを拒否するようにした場合、vShield はすべての受信トラフィックと 送信トラフィックをドロップします。

トラフィックの分析

vShield は通過する個々のパケットのヘッダーを調べ、仮想マシンとの間の各セッションに関する情報を収集します。セッションの詳細には、送信元、宛先、方向、および要求されているサービスが含まれます。導入済みのすべての vShield インスタンスによって収集されたトラフィックのデータは、vShield Manager のユーザー インターフェイスに集約されます。

vShield Manager の **[VM Flow]** タブにトラフィックの分析データが表示されます。このデータには、セッション数、パケット 数、および送受信されたバイト 数が含まれます。VM Flow は、不正なサービスの検出、送受信のセッションの検査、および VM Wall のアクセス ルールの作成を行う ためのフォレンジック ツールとして便利です。トラフィックのデータは、サービスまたはクライアント によるトラフィック使用率の高低を検出するなど、ネットワークのトラブルシューティングにも 使用できます。

[VM Flow] タブには、データ センター内またはクラスタ コンテナ内のすべてのアクティブな vShield インスタンスから返されたスループットの統計、または個々の仮想マシン レベルにおける単一の vShield インスタンスのスループットの統計が表示されます。VM Flow は、クライアントとサーバ間の通信に使用されるアプリケーション プロトコルに照らして統計を 3 つのチャートに整理します。チャート内の各色は、それぞれ異なるアプリケーション プロトコルを表します。このチャート手法を使用すると、サーバのリソースをアプリケーションごとに追跡できます。

デフォルトでは、VM Flow には最近 7 日間に調べられたすべてのフローのトラフィックの統計が表示されます。

VM Flow には、トラフィック データの包括的なレポートがセッション単位で含まれています。このレポートのデータを掘り下げて、特定の送信元と宛先の組み合わせに関する統計を表示することができます。このデータに基づいて、VM Wall の詳細な許可ルールと拒否ルールを作成できます。

仮想マシンの検出

インストールの完了後、通過するすべてのネットワーク トラフィックが各 vShield によって調べられ、オペレーティング システム、アプリケーション、および各仮想マシン上の開いているポートのインベントリが作成されます。この調査プロセスは「検出」と呼ばれます。vShield Manager は、検出された仮想マシンのインベントリを **[VM Inventory]** タブに表示します。

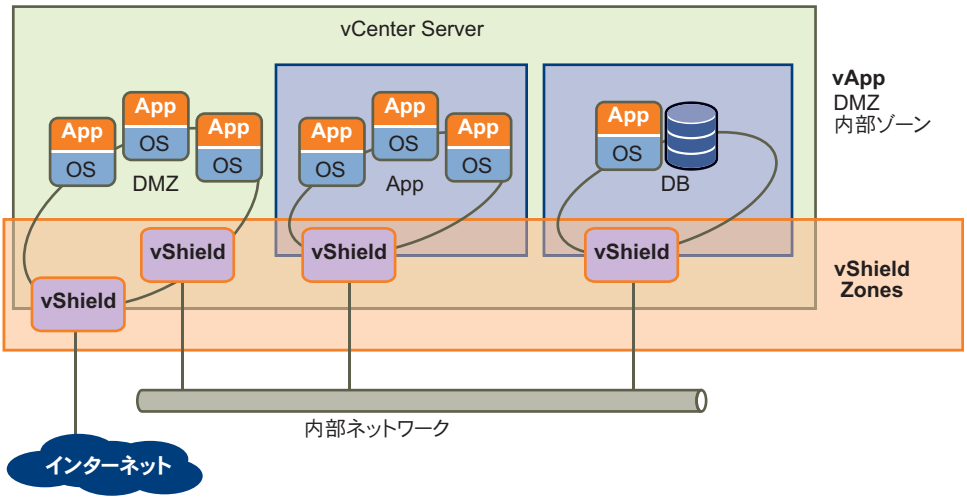
保護されていない仮想マシンへのトラフィックが vShield によって検出されると、その仮想マシンは vShield Manager のユーザー インターフェイスのインベントリパネルで赤色に強調表示されます。これにより、脆弱なサーバを速やかに識別し、それらを新規の vShield または既存の vShield で保護することができます。保護されていないと検出プロセスで判断された個々の仮想マシンは、vShield Manager のインベントリ パネルに赤の枠線で強調表示されます。これにより、すべての仮想マシンを識別して保護することができます。

また、vShield の検出処理を利用して仮想マシンをスキャンし、セキュリティ リスクが存在する可能性のあるオープンなアプリケーションを識別することもできます。

導入のシナリオ

vShield Zones を使用すれば、さまざまな仮想マシン環境に安全なゾーンを作成できます。仮想マシンは、特定のアプリケーション、VLAN セグメント、またはカスタム コンプライアンスの各要素に基づいて隔離することができます。ゾーン作成ポリシーを決めたら、vShield Zones を導入して個々のゾーンにアクセス ルールを適用できます。

図 2. vShield Zones を使用した仮想ネットワーク内の特定ゾーンのセキュリティ保護



DMZ の保護

DMZ は混在型のトラスト ゾーンです。クライアントが Web および E メール サービス用のインターネットから接続する一方で、DMZ 内のサービスは内部ネットワークへのアクセスを必要とする場合があります。内部サービスを必要とする DMZ サービスの典型例は Microsoft Exchange です。OWA （Microsoft Outlook Web Access）は通常は DMZ クラスタに存在します。一方、Microsoft Exchange バック エンドは内部クラスタに存在します。内部クラスタでは、VM Wall ルールを作成して DMZ からの Exchange 関連の要求だけを許可し、特定の送信元と宛先のパラメータを識別することができます。DMZ クラスタからは、HTTP、FTP、または SMTP を使用して特定の宛先に送信する場合のみ DMZ への外部アクセスを許可するルールを作成できます。

VLAN の隔離

トラフィックのセグメント化に VLAN タグを使用する場合、VM Wall を使用してより有用なアクセス ポリシーを作成できます。物理ファイアウォールの代わりに VM Wall を使用すると、共有 ESX クラスタ内でトラスト ゾーンを閉じたり混在させたりできます。それにより、別々に断片化したクラスタを置く代わりに、DRS や HA などの機能を使用して使用率を最適化し、統合を行うことができます。ESX 環境全体を単一のプールとして管理すると、個別にプールを置いて管理する場合ほど作業が複雑ではありません。

たとえば、VLAN を使用して仮想マシンのゾーンを論理境界、組織の境界、またはネットワーク境界に基づいてセグメント化するとします。Virtual Infrastructure SDK を使用して、vShield Manager のインベントリ パネルのネットワーク ビューに VLAN ネットワークのビューが表示されます。各 VLAN ネットワーク用のアクセス ルールを作成して仮想マシンを隔離し、それらのマシン宛のタグなしのトラフィックをドロップすることができます。

VMware View™ ユーザーのセグメント化

VMware View ユーザーも、VM Wall のアクセス ポリシーのメリットを活用できます。一方向（たとえば外部から内部へ）のトラフィック、RDP などの動的アプリケーション、または View のさまざまなポート グループにまたがるアクセス制御を提供する同様の要求に基づいて、アクセス ルールを作成することができます。たとえば、従業員のステータス（正社員や契約社員）に基づいてユーザーを隔離するためのポート グループを作成できます。グループの作成後に VM Wall ルールを使用して、それらのポート グループから内部ネットワークへのアクセス、および仮想マシンからインターネットへの接続について決定することができます。

次の手順

vShield Zones のドキュメントとその内容について、表 1 に示します。

VMware 製品のドキュメントは、http://www.vmware.com/jp/support/pubs/index.html から入手できます。

表 1. ドキュメント

タスク	ドキュメント
vShield Zones のインストール	vShield Zones クイック スタート ガイド
vShield Zones の構成、監視、および保守 vNetwork 分散スイッチ環境での vShield Zones のインストール	vShield Zones 管理ガイド