VMware vShield App

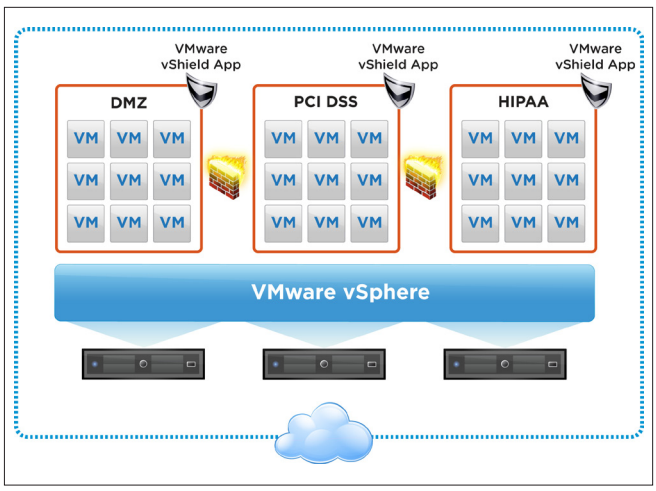
ネットワーク ベースのセキュリティ攻撃からのアプリケーションの保護

概 要

VMware vShield™ App は、VMware vShield 仮想化セキュリティ製品ファミリの一部です。仮想データセンター内のアプリケーションをネットワーク ベースの攻撃から保護します。これにより、仮想マシン間のネットワーク通信の視認性と管理性が向上します。ポリシーの適用は、IP アドレスなどの物理構成のみではなく、VMware vCenter™ Server のコンテナや vShield セキュリティ グループなどの論理構成も基準にしているため迅速に行われます。vShield App は、ハードウェアや VLAN などの従来の制御方法に依存しないため、ハードウェアやポリシーの急増を抑制できます。これにより、物理セキュリティの制限を超える費用対効果に優れたソリューションが実現します。この製品には、ファイルのアンチウイルス スキャン処理の負荷を軽減し、アンチウイルスの頻繁な起動を最小限に抑える VMware vShield Endpoint も含まれています。

主なメリット

- 仮想マシン間のネットワーク通信の視認性と管理性の向上
- 各セキュリティ グループを分離するための専用ハードウェアと VLAN の必要性を排除
- ハードウェア リソースの使用を最適化しながら、強力なセキュリティを維持
- すべての仮想マシン ネットワーク アクティビティを包括的に記録する機能により、コンプライアンスへの準拠を簡素化



vShield App では、セキュリティ グループを使用して、詳細にポリシーを適用します。

vShield App について

vShield App は、仮想データセンター向けに開発された、ハイパーバイザー ベースのアプリケーション対応ファイアウォール ソリューションです。

この製品は VMware vSphere® に直接組み込まれ、社内ネットワークベースの脅威からアプリケーションを保護し、企業のセキュリティ境界内のポリシー違反を低減します。これを実現するため、アプリケーション対応ファイアウォールと、送信元および送信先 IP アドレスに基づく詳細なパケット検査および接続制御を使用しています。

vShield App では、業務に関連するセキュリティ グループを迅速に作成することで、ポリシー制御を簡素化できます。また、フロー監視制御機能により、仮想マシンのネットワーク トラフィック分析や、セキュリティ グループ ポリシーの動的な適用が可能となります。管理者は、vShield App に含まれる vShield Manager コンソールを使用して、vShield App を統合管理できます。vShield Manager コンソールは VMware vCenter Server とシームレスに連携するため、仮想データセンターの統合セキュリティ管理が容易になります。

また、ハードウェアや VLAN などの従来の制御方法に依存しないため、ハードウェアやポリシーの急増を抑制できます。これにより、物理的なセキュリティの制限を超える費用対効果に優れたソリューションが実現します。

vShield App の仕組み

vShield App は各 vSphere ホストにインストールされ、ホスト上のすべてのネットワーク トラフィックを管理および監視します。これには、物理ネットワーク インターフェイス カード（NIC）を経由しないパケットも含まれます。物理的な境界や、アプリケーションの展開に関する静的な前提条件の代わりに、管理者が定義した業務に関連するセキュリティ グループに基づいて、ポリシーの作成および適用が可能です。

また、vCenter Server を利用した統合インターフェイスを提供しているため、仮想データセンター内の複数の vSphere ホストにこれらのポリシーを一括で適用できます。

vShield App の活用

- **アプリケーション対応の保護機能：**管理者は、仮想 NIC を経由するすべてのトラフィックに対し、詳細なポリシーを定義して適用することができます。これにより、社内の仮想データセンターのトラフィックに対する視認性が向上し、物理ファイアウォールへの迂回路が排除されます。
- **変更に対応した保護機能の維持：**vShield App では、仮想マシンがホスト間で移行しても引き続きファイアウォールで保護されるため、ネットワーク トポロジを変更してもアプリケーションのセキュリティには影響しません。

- **動的なポリシーを効率的に管理：**変化するビジネス ニーズに応じて社内ファイアウォール ポリシーの定義や調整を行うための、豊富なコンテキストを管理者に提供します。
- **ボットネット攻撃によるリスクの低減：**信頼できるアプリケーションに対する動的なポートの割り当てが可能なため、セキュリティ管理者はボットネットやその他の攻撃を防ぐことができます。
- **共有リソースへのアクセスの制御：**セキュリティ管理者はストレージやバックアップなど、vSphere ホスト上の共有サービスへのアクセスを IP アドレスに基づいて制限できます。
- **IT コンプライアンスへの準拠の促進：**仮想マシンのネットワーク セキュリティの視認性と管理性が向上します。また、ログの記録および監査制御機能により、企業は社内ポリシーや外部の規制要件へ準拠していることを証明できます。

主な機能

ファイアウォール

- ハイパーバイザー レベルのファイアウォール：ハイパーバイザーの検査により受信接続および送信接続を仮想 NIC レベルで制御し、マルチホーム仮想マシンをサポート
- レイヤー 2 のファイアウォール：透過型ファイアウォールとも呼ばれるレイヤー 2 のファイアウォールにより、パスワード スニフィング、DHCP スヌーピング、ARP（Address Resolution Protocol）偽装やポイズニング攻撃など、さまざまな種類の攻撃からの保護を実現。この機能により、SNMP トラフィックは完全に分離されます。
- ネットワーク、アプリケーション ポート、プロトコル タイプ（TCP、UDP）、またはアプリケーション タイプに応じて保護を適用
- 仮想マシン移行時の動的な保護を実現
- IP ベースのステートフルなファイアウォールおよびアプリケーション レイヤー ゲートウェイ：Oracle、Sun RPC（Remote Procedure Call）、Microsoft RPC などの広範なプロトコルに対応。ゲートウェイは、必要な場合にのみセッション（ポート）を開くことでセキュリティを強化します。サポート対象プロトコルの一覧については、『VMware vShield Administration Guide』（英語）を参照してください。

フローの監視

- 詳細なレポート作成機能：管理者は、アプリケーション トラフィック（アプリケーション、セッション数、バイト数）の詳細なレポートにより、仮想マシン間のネットワーク アクティビティを確認し、ファイアウォール ポリシーの定義と変更、ボットネット攻撃の特定、およびビジネス プロセスの保護を実現

セキュリティ グループ

- 管理者は、業務に関連する仮想マシンのグループを仮想 NIC ごとに定義可能

ポリシー管理

- vShield Manager により製品の機能を管理。多くの機能は、vCenter Server インターフェイスから利用可能に
- 管理者によるセキュリティ グループ、vCenter Server グループ、および TCP 5-tuple（送信元 IP、送信先 IP、送信元ポート、送信先ポート、プロトコル）へのポリシーの適用
- REST（Representational State Transfer）API は、管理およびポリシー適用のためのプログラム可能なインターフェイスを提供
- 企業のセキュリティ管理ツールとの連携をサポート

IP アドレス

- 複数のテナント ゾーンで同一の IP アドレスを使用するなど、柔軟な IP アドレス指定によりプロビジョニングを簡素化

ログの記録と監査

- 業界標準の Syslog フォーマットに基づいてログを記録
- REST API と vShield Manager により、ログおよび監査ツールが利用可能
- ファイアウォールのログ記録のオンまたはオフを、管理者がルール レベルで定義可能

サポート対象の製品

サポート対象の vSphere 環境の製品リリースについては、http://vmware.com/jp/products を参照してください。

関連製品

vShield セキュリティ製品ファミリには、vShield App の機能に加えて機密データの検出を行う vShield App with Data Security、境界をセキュリティ保護する vShield Edge、端末のセキュリティとパフォーマンスを強化する vShield Endpoint、vShield Manager、およびすべての製品を含む vShield Bundle があります。

詳細情報

製品仕様とシステム要件の詳細については、次の Web サイトで、『VMware vShield Administration Guide』（英語）を参照してください。
http://www.vmware.com/pdf/vshield_41_admin.pdf

vShield 製品の詳細な情報については、次のサイト
http://vmware.com/jp/products を参照してください。

ヴイエムウェア株式会社 〒105-0013 東京都港区浜松町 1-30-5 浜松町スクエア 13F www.vmware.com/jp