VMware vShield Edge

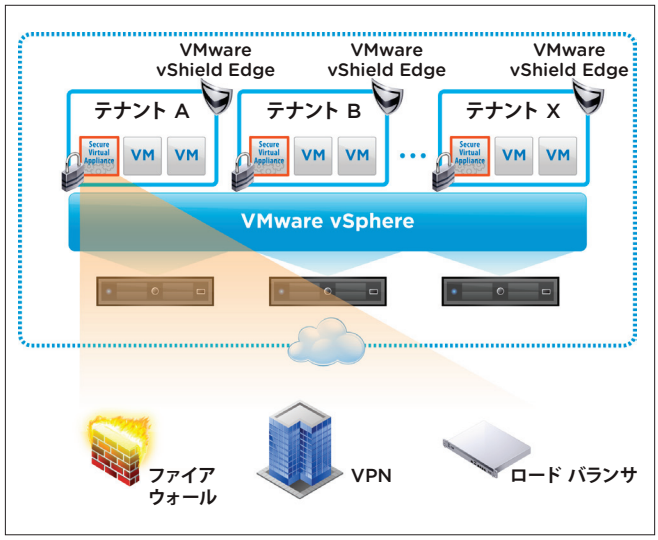
データセンターのネットワーク境界の保護

概 要

VMware vShield™ Edge は、仮想セキュリティを提供する VMware vShield 製品ファミリの 1 つとして、仮想データセンターに包括的な境界ネットワーク セキュリティを提供します。vShield Edge は VMware vSphere® とシームレスに連携し、企業がクラウド インフラストラクチャの規模を迅速かつ安全に変更するための、ネットワーク ゲートウェイ サービスを提供します。

主なメリット

- 複数の専用アプライアンスの使用を排除し、ネットワーク ゲートウェイ サービスを迅速にプロビジョニングすることにより、コストと複雑性を低減
- 組み込みのエッジ ネットワーク セキュリティとサービスによるポリシー適用の保証
- 組織やテナントごとに 1 つの境界を設定することで、スケーラビリティとパフォーマンスが向上
- 詳細なログ機能による IT コンプライアンスへの準拠の簡素化
- VMware vCenter™ Server および業界をリードするエンタープライズ セキュリティ ソリューションと連携する、完全な機能を備えたインターフェイスを使用して、管理を効率化



vShield Edge は、組み込みの境界セキュリティによって、仮想データセンター間のトラフィックを保護します。

vShield Edge について

vShield Edge は、仮想データセンター向けのエッジ ネットワーク セキュリティ ソリューションです。ネットワーク セキュリティ ゲートウェイ サービスなどの重要なセキュリティ機能と、パフォーマンスと可用性のための Web のロード バランシング機能を提供します。このソリューションは vSphere に直接組み込まれ、フォルト トレランスや高可用性などの vSphere の機能を活用して、比類のない回復性を実現します。

管理者は、vShield Edge に含まれる vShield Manager コンソールを使用して、vShield Edge 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、vShield Edge は VMware vCloud™ Director と連携しており、マルチテナント クラウド インフラストラクチャにおける仮想データセンターのプロビジョニングの自動化と安全性を強化します。セキュリティ管理者と仮想インフラストラクチャの管理者の業務を分離することにより、許可を受けたリソースのみにアクセスが制限されます。

vShield Edge の仕組み

vShield Edge は仮想アプライアンスとして展開され、ファイアウォール、VPN、Web ロード バランサ、ネットワーク アドレス変換（NAT）、および DHCP サービスを提供して、送信元および送信先の IP アドレスが含まれるパケットのヘッダを監視します。また、ポリシーに基づいて、接続の拒否または許可、VPN セッションの開始および終了、ネットワーク アドレスの変換、送信元および送信先のポートやプロトコル タイプ（TCP または UDP）単位でのデータの検査を実行します。

vShield Edge の活用

- **エッジ セキュリティ ハードウェアの統合：** vShield Edge を使用すると、既存の vSphere リソースを使用してエッジ セキュリティ サービスをプロビジョニングできます。vSphere ホストを「エアギャップ」するための、エッジ セキュリティ ハードウェアは必要ありません。
- **仮想データセンターの境界を迅速かつ安全に設置：** vShield Edge を使用すると、企業は仮想データセンター環境の周辺に、ハードウェアに依存しないセキュアな論理的境界（エッジ）を容易に設置できます。これにより、マルチテナント IT インフラストラクチャ内の共有ネットワーク リソースを容易に利用できるようになります。
- **共有ネットワーク上でデータの機密性を保護：** vShield Edge では、256 ビットの暗号化を使用したサイト間の VPN 機能を提供しています。これにより、仮想データセンターの境界を越えて転送されるすべてのデータの機密性が維持されます。

- **Web サービスのパフォーマンスと可用性の保証：** vShield Edge は、仮想マシン クラスタ間の受信 Web トラフィックを効率的に管理します。また、エッジ セキュリティとともに展開することも、単独で展開することも可能な、Web のロード バランシング機能が含まれます。
- **コンプライアンス管理の促進：** vShield Edge は、イベントの詳細なログ記録やフローの統計情報などの重要な管理機能を備えています。これらは、企業ポリシーや業界および政府の規制に遵守していることを証明するために必要な機能です。

主な機能

ファイアウォール

- 境界（レイヤー 3）ファイアウォール。ネットワーク アドレス変換（NAT）は不要
- ステートフル インスペクション ファイアウォール。次のパラメータに基づくルールを使用して、受信および送信接続を制御
  - IP アドレス：送信元および送信先の IP アドレス
  - ポート：送信元および送信先のポート
  - プロトコル：タイプ別（TCP または UDP）

ネットワーク アドレス変換

- 仮想環境で送受信される IP アドレスの変換
- 信頼できない場所へは、仮想データセンターの IP アドレスをマスカレードして送信

DHCP

- vSphere 環境内の仮想マシンに対する IP アドレス プロビジョニングの自動化
- 管理者が定義するパラメータ（アドレス プール、リース期間、専用 IP アドレスなど）

サイト間の VPN

- 仮想データセンター（またはエッジ セキュリティ仮想マシン）間の通信の保護
- IKE（Internet Key Exchange）プロトコルに基づく IPsec VPN（証明書認証および共有キー）をサポート

Web のロード バランシング

- Web トラフィック（HTTP）を含むすべてのトラフィックの受信ロード バランシング
- ラウンド ロビン アルゴリズム
- 「スティッキー」セッションのサポート

エッジ フロー統計情報

- テナントに起因する仮想データセンター リソースの使用率の測定
- REST（Representational State Transfer）API を通じてアクセスでき、サービス プロバイダのチャージバック アプリケーションで利用される統計情報

ポリシー管理

- vShield Manager を使用した完全な管理機能。多くの機能が vCenter Server インターフェイスから利用可能
- REST API を使用した管理のための、カスタマイズ可能なインターフェイス
- 企業の IT セキュリティ管理ツールとの連携をサポート

ログの記録と監査

- 業界標準の Syslog フォーマットに基づく
- REST API および vShield Manager ユーザー インターフェイスを通じて利用可能
- 管理者は主なエッジ セキュリティ イベント（エラー、警告など）用のログ記録のオン / オフを次のレベルで定義可能
  - ファイアウォール：ルール レベル
  - NAT：ルール レベル
  - VPN：サイト間の接続名
  - Web ロード バランサ：プール レベル。URL やフォルダなどの特定の Web 要求
  - DHCP：サービス レベル。バインディング（リリースおよび更新）

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、ネットワーク ベースの攻撃からアプリケーションを保護する vShield App、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、端末のセキュリティとパフォーマンスの向上を実現する VMware 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 サイトから、『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 製品の詳細情報については、
http://vmware.com/jp/products をご覧ください。

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