製品データシート

VMware vShield Zones

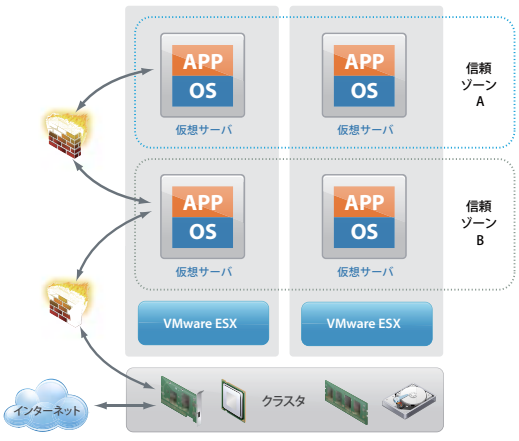
ポリシ ベースのネットワーク監視および仮想マシンへのポリシーの適用

概　要

VMware® vShield Zones を使用すると、クラウド コンピューティングの効率性と柔軟性を維持しながら、セキュリティ ポリシーおよび業界規制へのネットワーク コンプライアンスの遵守が可能になります。VMware vShield Zones は、複数の共有物理リソースにまたがる仮想データ センター内に論理ゾーンを作成します。各ゾーンには、異なるレベルの信頼性と機密性を設定できます。

メリット

- トラフィックを物理アプライアンスに転送させることなく、仮想マシン間の通信におけるネットワークの視認性を提供
- シンプルなゾーン ベースのアクセス ルールにより、管理を容易にし、ポリシー エラーを削減
- VMware VMotion™ イベントおよび仮想マシンのライフサイクル イベントすべてに一貫したポリシーを適用
- 物理ネットワークに関係なく、仮想インフラストラクチャ内のセキュリティ状態を監査



VMware ESX ホスト間およびインターネットに対し、論理的で信頼される組織的な境界を作成

VMware vShield Zones について

VMware vShield Zones は、VMware vSphere™ 導入環境にネットワーク アクティビティの視認性を提供し、ポリシーの適用を行うセキュリティ仮想アプライアンスです。これにより企業のセキュリティ ポリシーや、PCI やサーベンス オクスリー法などの業界規制に準拠できます。これまで、このレベルの視認性を得てポリシーの適用を行うには、VMware ESX™ ホストから外部の物理アプライアンスへトラフィックを転送し、リソース プールを分断されたクラスタへと分割する必要がありました。また、これは共有のコンピューティング プールやクラウドの柔軟性や効率性に影響を与えるものでした。VMware vShield Zones を使用すると、仮想データ センターのすべての物理リソースにわたる論理ゾーンを作成し、異なるレベルの信頼性、プライバシー、機密性を維持できます。

VMware vShield Zones は次の機能を提供します。

- 論理的で信頼される境界または組織的な境界に基づいた、ブリッジ、ファイアウォール、または分離された仮想マシン ゾーン
- 既存の VMware vCenter Server コンテナを使用した直観的なネットワーク アクセス ルールの作成
- アプリケーション ベースのプロトコルによる、許可または禁止されたアクティビティのログおよびレポートの作成
- 確認したネットワーク フローを正確なアクセス ルールへ容易に変換

VMware vShield Zones の企業での活用

VMware vShield Zones を使用すると、次のことが可能になります。

仮想 DMZ の統合。VMware vShield Zones では、DMZ（demilitarized zone）を仮想化するほか、インターネット トラフィックを内部サーバから完全に分離したままで、DMZ と内部ネットワークのコンピューティング リソースの共有が可能になります。DMZ ファイアウォールが仮想環境に持ち込まれるため、DMZ 専用の VMware ESX ホストは不要になります。これらの VMware ESX ホストは、可用性および使用率向上のために再利用できます。

機密データのネットワーク分離のための PCI コンプライアンスの遵守。PCI（Payment Card Industry）標準は、消費者保護のために、クレジットカードのデータを処理するサーバが存在するネットワークをセグメント化して、ほかのシステムから切り離すものです。VMware vShield Zones では、クレジットカード情報を処理する仮想マシンと、ほかの信頼できないネットワークやマシンとの間にファイアウォール ポリシーを作成できます。これは、PCI のデータ セキュリティ標準の要件です。HIPAA や SOX のようなほかの業界標準でも同様に、患者の健康情報や企業の財務状況など機密データのプライバシー保護に対応するには、ファイアウォール設定とネットワークのセグメント化の制御が重要であるとしています。VMware vShield Zones では、仮想環境にこれらの制御を提供できます。

主な機能

外部クラウドまたはプライベート クラウドのマルチテナント分離の適用。 VMware vShield Zones では、分離および制限されたデータ センター ゾーンを作成できます。これにより、1 つのクラウド インフラストラクチャを共有する複数のテナントにわたり、ネットワークからのデータやユーザー アクティビティの漏えいを防ぐことが可能です。個別の仮想スイッチおよび仮想 LAN（VLAN）によって生じる非常に複雑なネットワークや管理を必要とせずに、何百ものテナントへ分離を拡張できます。

仮想データ センター内の不正アクセスの監視。 広範囲にわたるオープンな内部ネットワークは、マルウェアや不正なアクティビティの蔓延を助長します。VMware vShield Zones は、アプリケーション プロトコル レベルで、仮想マシン間のトラフィックとインターネットへのトラフィックを監視し、ログを記録します。ワームや不正アクセスの可能性がある異常なアクティビティは、グラフィカルなレポートまたは表形式のレポートで確認できます。また、特定のネットワーク フローが、個別のマシンまたは統合された複数のマシン レベルで、正しいブロック ルールに迅速に変換されます。

VMware vShield Zones の仕組み

VMware vShield Zones は、VMware vSphere™ 環境を安全で制限された複数のアクティビティ ゾーンにパーティショニングする負担を低減します。これにより仮想化を使用して、機密性の高いデータ センター領域に高い効率性、使用率、可用性を提供できます。このとき、ユーザーやデータがリスクにさらされたり、ネットワーク制御に関するセキュリティやコンプライアンス要件に違反することもありません。VMware vShield Zones は、仮想化およびアプリケーションに高度に対応したコンテキスト内で、ネットワーク監視およびアクセス管理を実現します。これにより管理者は、既存の VMware vCenter Server 管理階層およびネットワーク トポロジーで表示される、論理的なトラスト ゾーン、または組織的なゾーンの境界に直感的にマッピングされるアクセス ポリシーを定義できます。

VMware vShield Zones は、VMware vShield Manager および VMware vShield Zones アプライアンスで構成されています。VMware vShield Manager は、導入環境全体にわたる監視およびアクセス ポリシーの統合管理を行い、VMware vShield Zones アプライアンスは、ランタイムの適用を行います。VMware vShield Manager は仮想アプライアンスとして導入され、自動的に VMware vCenter Server に統合されます。これにより、既存の仮想マシン、ネットワーク、ホスト、およびクラスタのコンテキストにポリシーとイベントが提供されます。

VMware vShield Zones 仮想アプライアンスは、VMware ESX ホスト上の仮想スイッチでインラインに分散および展開され、実行時の視認性を提供し、トラフィックの適用を行います。ゾーン間、および外部に対するネットワーク アクティビティは、ログに記録され、アプリケーションのネットワーク プロトコルに従って分類されます。そしてパケットをインラインでフィルタすることで、不正なプロトコルやアクセスをすべてブロックします。イベントは VMware vShield Manager 内に統合されます。ここでは、データ センター全体にわたるアクティビティのログの記録、参照、およびサード パーティ製管理ソリューションへのエクスポートが行われます。

VMware vShield Zones の主な機能

論理ゾーンの境界およびセグメントの統合管理

- 既存の仮想インフラストラクチャ コンテナ（ホスト、仮想スイッチ、VLAN）を、論理的なトラスト ゾーン、または組織的なゾーンとして活用
- ゾーン境界間でネットワーク トラフィックをブリッジ、ファイアウォール設定、または分離するポリシーを定義
- VMware vCenter Server 環境全体で、ポリシーを管理および適用
- VMware vCenter Server との統合と、既存の仮想ネットワークにおける自動的な展開
- 仮想マシン上で実行している既存のアプリケーションをスキャンおよび検出し、アプリケーション プロトコルを特定

ネットワークの適用とフローの監視

- ネットワークまたはアプリケーション プロトコル（HTTP、RDP、SNMP など）ごとにトラフィックを分類
- SPI（stateful packet inspection）による、高機能なトラフィックのフィルタリング
- FTP などのプロトコルの動的なポート接続をトラッキング
- VMware VMotion を使用した移行イベント全体のネットワーク接続をトラッキング
- 確認したネットワーク フローを正確なネットワーク適用ルールに容易に変換
- 許可または禁止されたアクティビティを監視

管理およびレポート作成

- Web ベースの vShield Manager インターフェイスに、あらゆる Web ブラウザからリモート アクセス可能
- VMware vCenter Server に共通の管理者、または業務と役割を明確に分けた管理者の設定
- 個別の仮想マシン レベルまたは全体的なレベルでアクティビティを階層的に表示し、グラフィカルなレポートまたは表形式のレポートを作成
- アーカイブおよびコンプライアンスへの準拠に使用するログ データを保持
- syslog フォーマットを使用したイベントおよびデータのエクスポート

詳細情報

VMware 製品のご購入、または詳細情報については、弊社営業部門に電話（03-4334-5600）またはメールでお問い合わせいただくか、次の製品 Web サイトをご覧ください。
www.vmware.com/jp/products/vshield-zones/
製品仕様およびシステム要件の詳細については、VMware vShield Zones のインストールおよび構成ガイドをご覧ください。

VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
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 Tel: 03-4334-5600 Fax: 03-4334-5601 www.vmware.com/jp