FortiGate VMX

VMware 環境の拡張セキュリティ制御機能を提供

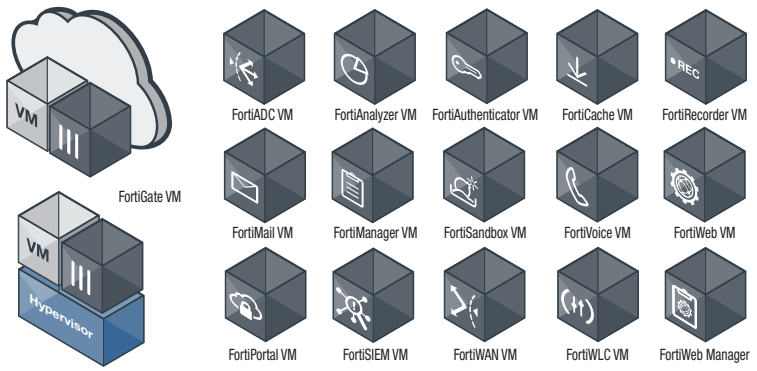
FortiGate VMX は、VMware 環境に特化したセキュリティソリューションで、VMware の Software-Defined Data Center（SDDC）の統合を可能にすることで、VMware NSX および vSphere との相互運用を実現します。FortiGate VMX は、API を直接統合することで仮想化されたネットワークトラフィックをハイパーバイザレベルで可視化し、保護できます。

導入 / 管理の自動化によってソフトウェア制御された動的なネットワークやインフラストラクチャでワークロードのセキュリティを確保し、確かな保護対策および法規制のコンプライアンスを可能にします。

仮想環境における豊富な実績

フォーティネットは2004年に仮想UTM（VDOM）テクノロジを発表して以来、サービスプロバイダおよび企業に仮想環境における強力なセキュリティソリューションを提供し続けています。2010年に初めてFortiGate VM仮想アプライアンスが製品ラインナップに加わったことで、選択の幅がさらに広がり、多くのお客様の既存の仮想化およびクラウドのインフラストラクチャにフォーティネットのセキュリティソリューションを柔軟に導入していただけるようになりました。

フォーティネットは、最初に発表したこの仮想環境向けセキュリティソリューション以降も継続的にソリューションの充実を図っており、FortiGate VMXが新たにポートフォリオに加わったことで、VMware環境に特化した16を超える豊富なソリューションをご利用いただけるようになりました。

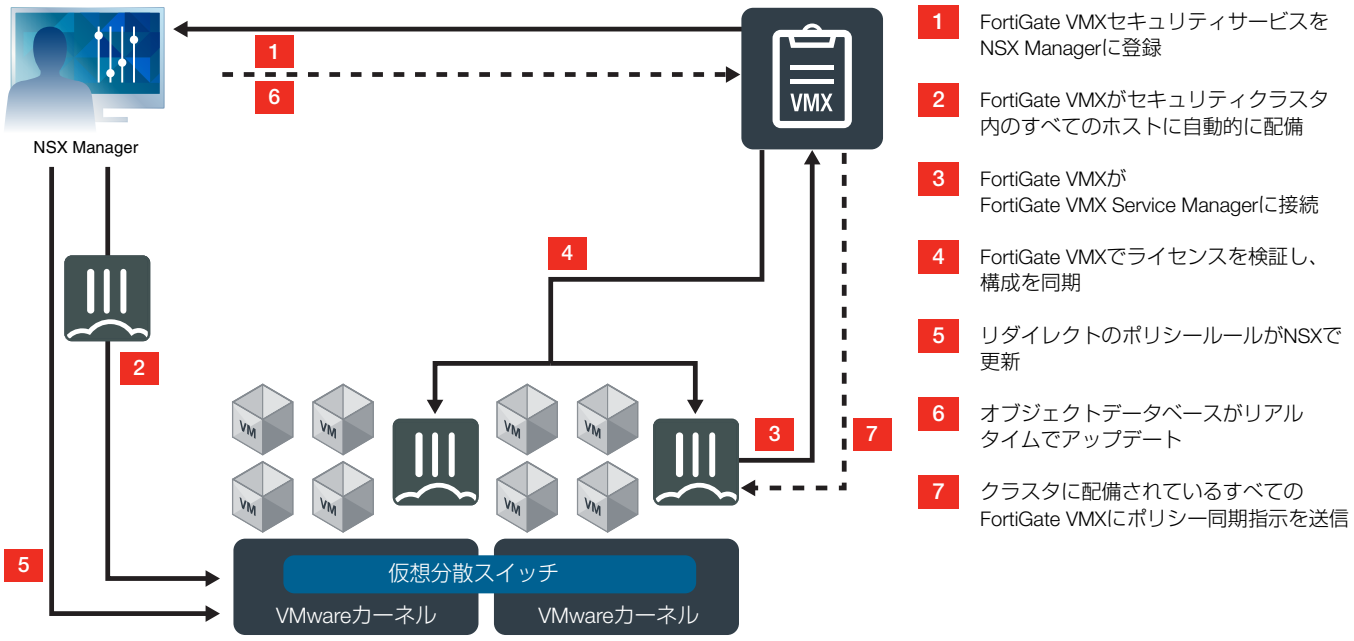


フォーティネットの包括的仮想アプライアンス製品（日本で未販売の製品も含まれます）

ハイライト

- すべてのvSphere仮想ネットワークトラフィックを可視化
- FortiGate VMXセキュリティノードを新しいESXiホストに自動的に配備 / プロビジョニング可能
- 新しいVMワークロードを瞬時にリアルタイムで保護
- ライブマイグレーションイベント（vMotion）間でセッション状態を維持
- マルチテナント環境をサポート
- 次世代セキュリティ機能が1つのプラットフォームに集約された総合ソリューション

導入例



1. FortiGate VMX をセキュリティサービスとして登録

登録プロセスでは、FortiGate VMX Service Manager と NSX Manager との双方向通信を可能にするために、NetX（Network Extensible）管理プレーン API を使用します。

2. FortiGate VMX をクラスタ内のすべての ESXi ホストに自動配備

NSX Manager が登録時に指定された URL から FortiGate VMX イメージを収集し、FortiGate VMX のインスタンスをクラスタ内の各々の ESXi ホストにインストールします。

3. FortiGate VMX と FortiGate VMX Service Manager の間の接続を確立

ライセンス情報を取得するために、FortiGate VMX は FortiGate VMX Service Manager への接続を開始します。

4. FortiGate VMX の構成を同期

FortiGate VMX Service Manager が FortiGate VMX のステータスを確認し、構成を同期します。

5. リダイレクトルールの有効化

NSX ネットワークイントロスペクションサービスのセキュリティポリシールールが有効化され、ポリシーで指定された通信フローがすべて FortiGate VMX にリダイレクトされてトラフィックが保護されます。

6. オブジェクトのリアルタイムアップデート

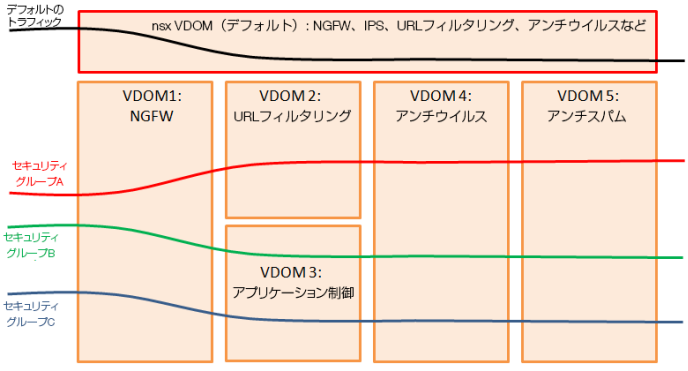
NSX Manager は、仮想環境内の変更に伴う更新内容を FortiGate VMX Service Manager に送信します。

7. ESXi クラスタに配備されているすべての FortiGate VMX インスタンスにポリシーの同期指示を送信

新しく作成されたセキュリティポリシーは、すべての FortiGate VMX セキュリティノードに送信されます。クラスタに配備されているすべての FortiGate VMX に同じポリシーセットが送信されます。

仮想セグメンテーション機能

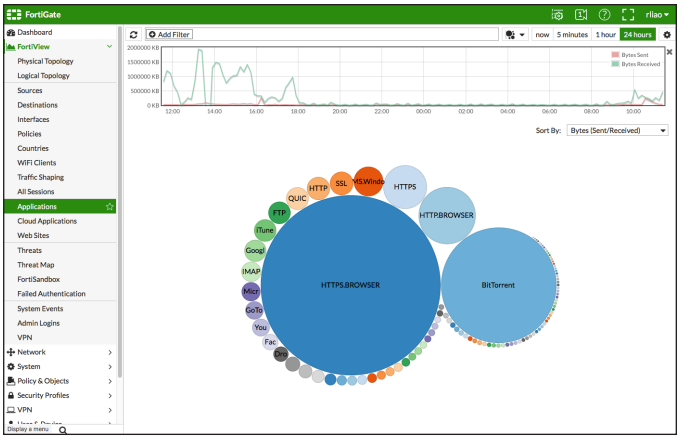
フォーティネットの仮想 UTM（VDOM）テクノロジを FortiGate VMX へと拡張することで、セキュリティ機能のセグメント化とマルチテナント環境のサポートが可能になります。フォーティネットの仮想 UTM（VDOM）に NSX サービスプロファイルをマッピングすることにより、ポリシーを分割して特定のトラフィックフローに適用できます。これにより、環境内でホスティングされている各テナント向けに特定のセキュリティソリューションを登録する複雑な作業の負荷が大幅に軽減されます。



ソフトウェア

FortiOS

直感的なオペレーティングシステムで、FotiGate プラットフォーム全体にわたるセキュリティおよびネットワーク機能をすべて一元制御できます。これによって完全統合された次世代セキュリティプラットフォームが実現し、運用経費や時間を抑制することが可能になります。



- 真の統合セキュリティプラットフォームにより、すべてのFortiGate プラットフォームのあらゆるセキュリティおよびネットワークサービスが 1 つの OS で一元制御できます。
- 業界最先端の保護機能：NSS Labs の「Recommended（推奨）」評価および VB100 アワード獲得、AV Comparatives および ICSA 認定の優れたセキュリティとパフォーマンスが提供されます。
- 数千ものアプリケーションの制御、最新のエクスプロイトのブロック、そして数百万規模の URL のリアルタイム評価に基づく Web トラフィックのフィルタリングが可能です。
- 高度な脅威保護フレームワークとの統合により、わずか数分で巧妙な攻撃を自動的に検知し、ブロックします。
- ルーティング、スイッチング、WiFi、LAN、WAN など多様なネットワーキング機能を提供し、企業のあらゆるニーズに対応します。
- 市場最速のファイアウォールプラットフォームにおいて、必要なセキュリティ機能すべての SPU による高速実行を可能にします。

詳細は、www.fortinet.co.jp で公開している「FortiOS データシート」をご覧ください。

サービス

FortiGuard セキュリティサービス

FortiGuard Labs は、脅威の最新状況に関するリアルタイムの情報を駆使してフォーティネットのさまざまなソリューション向けに包括的なセキュリティアップデートを提供します。セキュリティに対する脅威の研究者、エンジニア、犯罪科学のスペシャリストで構成されるチームが、脅威の監視を手掛ける世界有数の機関やネットワーク / セキュリティ分野を代表するベンダー、世界各国の捜査機関と協力して、優れたサービスをお届けします。

- **リアルタイムアップデート** — 24 時間 365 日対応のグローバルな体制で、フォーティネットのすべてのプラットフォームにフォーティネット分散ネットワーク経由でセキュリティインテリジェンスを提供します。
- **セキュリティ調査** — FortiGuard Labs はこれまでに 170 種のゼロデイ脆弱性を発見した実績があり、毎月公開している自動化されたシグネチャアップデートの累計は数百万件に達しています。
- **検証済みのセキュリティインテリジェンス** — FortiGuard インテリジェンスに基づくフォーティネットのネットワークセキュリティプラットフォームは、世界有数の第三者検証機関や世界中のお客様によって検証され、その有効性が確認されています。

FortiCare サポートサービス

FortiCare カスタマーサポートチームは、全てのフォーティネット製品に関する技術サポートをグローバルに提供します。FortiCare は南北アメリカ、ヨーロッパ、中東、アジアの各地域にサポートスタッフを配備しており、あらゆる規模の企業ニーズに最適なサービスを提供します。

- **Enhanced Support（拡張サポート）** — 現地の営業時間内のみの対応を必要とされるお客様向け。
- **Comprehensive Support（総合サポート）** — ハードウェアの迅速な交換を含む 24 時間対応のミッションクリティカルサポートを必要とされるお客様向け。
- **Advanced Services（アドバンスサポート）** — 専任のテクニカルアカウントマネージャ、高レベルの SLA、広範囲のソフトウェアサポート、優先順位のエスカレーション、オンサイトでの作業などをグローバルまたはそれぞれの地域で必要とされるお客様向け。
- **プロフェッショナルサービス** — アーキテクチャ / 設計サービス、実装 / 導入サービス、運用サービスなどを必要とする、複雑なセキュリティ実装環境のお客様向け。

エンタープライズバンドル

FortiGuard Labs は、FortiGate ファイアウォールプラットフォームと併せてご利用いただける、多数のセキュリティインテリジェンスサービスを提供しています。FortiGuard エンタープライズバンドルを利用することで、FortiGate の保護機能を簡単に最適化できます。このバンドルには、FortiGuard のすべてのセキュリティサービスに加えて、最も柔軟で広範な保護を 1 つのパッケージにまとめた、FortiCare サポートサービスが含まれます。

ソリューション

可視性

セキュリティ仮想アプライアンスをトラフィックのフローに配置してポリシーを実行する必要がある従来型の導入環境とは異なり、FortiGate VMX では仮想スイッチポートとワークロード VM そのものの仮想 NIC（vNIC）の間で送受信されるトラフィックを可視化できます。

配備 / プロビジョニングの自動化

FortiGate VMX Service Manager は、VMware の NSX Manager と直接通信し、フォーティネットのセキュリティサービスに関する情報を取得し、登録します。これにより、VMware 環境において FortiGate VMX セキュリティノードが該当するクラスタ内の各 VMware ESXi ホストに自動的に配備されるようになります。FortiGate VMX Service Manager と FortiGate VMX セキュリティノード間でのライセンス認証とセキュリティポリシーの実行も自動的に行われます。

オブジェクトベースの保護

FortiGate VMX セキュリティポリシーは、動的な NSX セキュリティグループおよび関連するオブジェクトに基づいて適用されます。NSX Manager におけるセキュリティグループに対する追加や変更の内容は、該当する適切な FortiGate VMX と自動的に関連付けが行われるため、FortiGate VMX Service Manager での変更作業は必要ありません。ポリシーはサービスするドメインや接続ポートに依存せず、適切なオブジェクトに適用されます。ライブマイグレーション（vMotion）のイベント中にホストが移動した場合も、該当する VM のワークロードへのポリシー適用が継続されます。

ポリシーのリダイレクト

VMware NSX API および NSX Service Composer との統合により、独自のリダイレクトセキュリティポリシーを有効化して、指定された ESXi クラスタ内の特定の VM ワークロードで送受信されるアプリケーショントラフィックを FortiGate VMX セキュリティサービスで保護することができます。手作業によるネットワークフローの構成は不要です。

リアルタイムの保護

新しい VM ワークロードが作成されると、NSX の動的なセキュリティグループベースのポリシーに基づいて、該当するセキュリティポリシーがリアルタイムで自動的に関連付けられます。これにより、ポリシーの作成から実行までのタイムラグ、あるいはデータセンター管理者とセキュリティ管理者の間のやり取りにおいて発生するミスを回避することができます。

クラスタベースの拡張

FortiGate VMX は VMware 環境内のセキュリティサービスであるため、セキュアな ESXi クラスタに追加されたすべての新しいホストに対して瞬時に同じセキュリティポリシーが適用されます。FortiGate VMX セキュリティノードは新しい ESXi ホストに自動的に配備されるため、手作業による設定などは一切必要ありません。

総論

FortiGate アプライアンスは、高度な機能を備えた FortiOS オペレーティングシステムの活用によって、Software-Defined Datacenter（SDDC）が直面する多様なセキュリティの脅威を効率的に無力化します。FortiGate アプライアンスは、最前線の防御を目的とするエッジへの導入（FortiGate ハードウェアアプライアンス）、ゾーン間セキュリティや VPN 終端の仮想インフラストラクチャにおけるアプリケーションへの導入（FortiGate VM）、または VM 間での使用や高度なハイパーバイザベースのセキュリティ（FortiGate VMX）のいずれの用途においても、今日最も有効なセキュリティテクノロジを活用し、お客様のインフラストラクチャを確実に保護します。

技術仕様

	ソリューション	サポートするバージョン
フォーティネット		
	FortiGate VMX Service Manager	v5.4およびそれ以降
	FortiGate VMX Security Node	v5.4およびそれ以降
	FortiAnalyzer（オプション）	v5.2.4およびそれ以降
VMware		
	vCenter Server	v5.5 Update 2およびそれ以降
	ESXi	v5.5 Update 2およびそれ以降
	NSX	v6.1.3およびそれ以降

注：上の表に記載されているすべてのコンポーネントに関する最新の互換性マトリックスについては、「VMware Compatibility Guide（VMware 互換性ガイド）」のフォーティネット製品セクションをご参照ください。
https://www.vmware.com/resources/compatibility/detail.php?deviceCategory=security&productid=41557&vcl=true
https://www.vmware.com/resources/compatibility/detail.php?deviceCategory=security&productid=40673&vcl=true

システム性能情報

	FortiGate VMX	
技術仕様		
仮想 CPU 数（最小 / 最大）	1 / 無制限	
メモリ（最小 / 最大）	1 GB / 無制限	
仮想 UTM（VDOM：標準 / 最大）	10 / 250	
ファイアウォールポリシー（VDOM / システム）	50,000 / 100,000	
ユーザー数無制限ライセンス	○	
システム性能	**2 vCPU / 4 GB RAM**	**4 vCPU / 6 GB RAM**
ファイアウォール同時セッション（TCP）	RAM に依存（上限なし）	RAM に依存（上限なし）
ファイアウォール新規セッション / 秒（TCP）	30,000	30,000
ファイアウォールスループット（HTTP 1 M）	15.0 Gbps	15.0 Gbps
IPS スループット（HTTP / エンタープライズトラフィック混合）[1]	9.5 / 1.75 Gbps	12.5 / 3.1 Gbps
アプリケーション制御スループット[2]	3.1 Gbps	5.3 Gbps
NGFW スループット[3]	1.4 Gbps	2.5 Gbps
脅威保護スループット[4]	1.4 Gbps	2.3 Gbps

注：数値はすべて「最大」の性能値であり、システム構成に応じて異なります。上記の数値は、14 コア Intel Xeon CPU E5-2630v4 2.60 GHz を搭載する Dell PowerEdge R630 サーバー上で、VMware ESXi 6.0.0 を実行して測定されています。1. IPS パフォーマンスは、1 M バイト HTML ファイルとエンタープライズトラフィック混合を用いて測定されています。2. アプリケーション制御パフォーマンスは、64 K バイト HTML ファイルのトラフィックを用いて測定されています。3. NGFW パフォーマンスは、IPS およびアプリケーション制御有効、エンタープライズトラフィック混合の状態のトラフィックを用いて測定されています。4. 脅威保護パフォーマンスは、IPS、アプリケーション制御、およびマルウェア保護有効、エンタープライズトラフィック混合の状態のトラフィックを用いて測定されています。

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.co.jp/contact

お問い合わせ