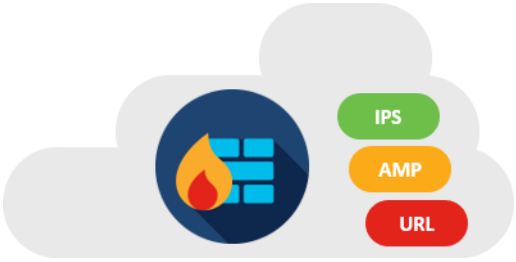
Cisco Firepower NGFW Virtual (NGFWv) アプライアンス データシート

目次

今日のビジネスは、ネットワークセキュリティの必要を満たす上で、物理的ソリューションと仮想ソリューションの組み合わせに依存しています。ビジネスには、ブランチオフィス、企業データセンター、および各拠点間のすべてのエントリポイントで一貫したポリシーを維持しつつ、さまざまな物理ファイアウォールと仮想ファイアウォールを幅広い環境に展開する柔軟な対応が必要です。データセンターの統合から、オフィスの移転、合併と買収、またはアプリケーションの需要がピークに達する時期に至るまで、シスコの仮想ファイアウォール ポートフォリオは、統一されたポリシーの利便性とあらゆる分野に展開できる柔軟性により、セキュリティ管理の簡素化に取り組むビジネスを支援します。

Cisco® 次世代ファイアウォール仮想（NGFWv）アプライアンスは、シスコの実績あるネットワーク ファイアウォールと高度な次世代 IPS、URL フィルタリング、マルウェア検出を組み合わせたものです。脅威を自動的に特定して排除し、セキュリティおよびネットワーク運用チームの負担を軽減します。さらに NGFWv は、物理環境、プライベートクラウド環境、およびパブリッククラウド環境におけるワークロードに一貫したセキュリティポリシーを適用することを可能にし、仮想環境の保護を簡素化します。ネットワークを詳細に可視化して、脅威の発生源とアクティビティを迅速に検出し、ビジネスに影響を与える前に攻撃を阻止します。シスコの仮想ファイアウォール製品は、世界有数のセキュリティ制御技術により、IT 部門に対する要求の大幅な変化を緩和し、ますます複雑化する脅威からワークロードを保護します。

製品の概要



NGFWv は、シスコの定評ある NGFW ソリューションの仮想化オプションであり、従来の物理データセンター、プライベートクラウド、およびパブリッククラウドでセキュリティを提供します。自動化されたリスクのランク付けと影響フラグを使用して脅威に優先順位を付け、即時の対応が必要なイベントにリソースを集中させます。ライセンス ポータビリティにより、すべてのアプライアンスで一貫したポリシーと一元的な管理を維持しつつ、オンプレミスのプライベートクラウドからパブリッククラウドへと柔軟に移行できます。シスコ スマート ソフトウェア ライセンシングにより、オンプレミスで実行されているアプライアンスの仮想インスタンスを簡単に展開、管理、追跡できます。

利点

パブリッククラウドとプライベートクラウドで同じ NGFW の機能を利用できます。その利点は次のとおりです。

自動化されたリスクのランク付けと影響フラグ

環境全体を詳細に可視化することで、脅威に優先順位を付けます。管理者による迅速な対応を必要とする影響の大きな事項に集中できるよう、イベントのノイズと量を減らします。Snort の最高水準のオープンソース侵入防御システム（IPS）を活用して、ホストプロファイルと脆弱性のレベルを関連付けるルールの推奨事項を設定し、影響分析を自動化し、データをコンテキスト化します。

クラウド間のライセンスポータビリティ

パブリッククラウドまたはプライベートクラウド（VMware、KVM、AWS、Azure、官公庁クラウド）間で仮想ソリューションをサポートする 1 つのライセンスのポータビリティを利用して、スーパーデータセンターからブランチオフィスに至るまで、あらゆる場所にアプライアンスを展開できます。1 つのライセンスで、ワークロードの拡張、縮小、または再配置を長期的に行い、複数のプライベートおよびパブリック クラウド インフラストラクチャに対応します。

一元的な管理と自動的な脅威の関連付け

高度なマルウェア防御（AMP）と URL フィルタリングにより、既知および未知のマルウェアを封じ込めることで、さらなる脅威を阻止します。統合されたツールの一元的な管理により、複数のセキュリティ製品を管理する作業の複雑さを軽減します。

機能と仕様

表 1. NGFWv の機能と仕様

機能	仕様
Cisco Firepower Device Manager（ローカル管理）	ESXi および KVM。Azure：バージョン 6.5 以降。AWS：6.6 以降
集中管理	集中型の設定、ロギング、モニタリング、およびレポートは、Cisco Firepower Management Center（オンプレミスおよび AWS と Azure を含むすべてのプラットフォーム）によって、または Cisco Defense Orchestrator を使用したクラウド（ESXi および KVM、Azure：バージョン 6.5 以降）で実行されます。
Application Visibility and Control（AVC）	標準。4,000 以上のアプリケーションと地理位置情報、ユーザ、および Web サイトをサポート
AVC：カスタム、オープンソース、アプリケーション検出機能で OpenAppID をサポート	標準
Cisco Security Intelligence	標準。IP、URL、および DNS の脅威インテリジェンス
Cisco Firepower 次世代型侵入防御システム（NGIPS）	使用可。エンドポイントとインフラストラクチャの脅威相関を受動的に検出可能。セキュリティ侵害指標（IoC）インテリジェンスを提供
ネットワーク向け Cisco Advanced Malware Protection（AMP）	使用可。標的型マルウェアや執拗なマルウェアの検出、ブロッキング、追跡、分析、封じ込めを行い、連続的な攻撃に攻撃中および攻撃後のいずれのタイミングでも対応可能。また、オプションで Cisco AMP for Endpoints による統合脅威相関機能を使用可能
Cisco AMP Threat Grid のサンドボックス	使用可。
URL フィルタリング：カテゴリの数	80 以上
URL フィルタリング：分類される URL の数	2 億 8000 万以上
自動化された脅威フィードと IPS シグネチャの更新	あり：Cisco Talos® グループ（https://www.cisco.com/c/ja_jp/products/security/talos.html）により、業界トップクラスの Collective Security Intelligence（CSI）を提供
サードパーティおよびオープンソースの	サードパーティ製品との統合を可能にするオープン API：Snort® および OpenAppID

機能	仕様
エコシステム	のコミュニティリソースにより、新しい脅威および特定の脅威に対応
高可用性とクラスタリング	アクティブ/スタンバイ（ESXi および KVM のみ）
展開モード	ルーテッド、透過的（インラインセット：IPS のみ）、パッシブ。AWS および Azure：ルーテッドモードのみ

注： パフォーマンスは、アクティブになっている機能、ネットワークトラフィックのプロトコルミックス、およびパケットサイズの特性によって変化します。パフォーマンスは新しいソフトウェアのリリース時に変化することがあります。サイジングの詳細なガイダンスについては、シスコの担当者にお問い合わせください。

製品パフォーマンスのガイドライン

注： パフォーマンスは以下と異なる場合があります。これらは一般的なガイドラインと見なす必要があります。実際のパフォーマンスは、CPU タイプ、CPU 速度、キャッシュ、インターフェイス数など、テスト環境によって異なります。

表 2. NGFWv のパフォーマンス仕様

仕様	4 vCPU	8 vCPU	12 vCPU
スループット：**FW + AVC（1024B）**	3 Gbps	5.5 Gbps	10 Gbps
スループット：**FW + AVC + IPS（1024B）**	3 Gbps	5.5 Gbps	10 Gbps
スループット：**FW + AVC（450B）**	1.5 Gbps	3 Gbps	5 Gbps
スループット：**FW + AVC + IPS（450B）**	1 Gbps	2 Gbps	3 Gbps
同時セッションの最大数	100,000	250,000	500,000
1 秒あたりの最大新規接続数	20,000	20,000	40,000
VPN ピアの最大数	250	250	750

システム要件

表 3. NGFWv のシステム要件

仕様	説明
VMware および KVM：仮想 CPU およびメモリ（6.4 以降）	• 4 vCPU/8GB • 8 vCPU/16GB • 12 vCPU/24GB
VMware および KVM：仮想 CPU およびメモリ（6.3 以前）	4 vCPU/8GB
ストレージ	すべての FTDv 構成で 50GB
ハイパーバイザ サポート	ESXi 6.0、6.5、6.7。KVM

仕様	説明
AWS サポート	• インスタンス：c3.xlarge、c4.xlarge • インスタンス：c5.xlarge、c5.2xlarge、および c5.4xlarge（6.6 以降） • 政府/自治体市場 • 中国市場 • 自動スケール • 拡張ネットワーキング
Azure サポート	• インスタンス：D3、D3_v2 • インスタンス：D4_v2 および D5_v2（6.5 以降） • 政府/自治体市場 • 中国市場 • 自動スケール

発注情報

表 4. NGFWv の発注情報

部品番号	説明
FPRTD-V-K9	Cisco Firepower Threat Defense（TD）仮想アプライアンス
L-FPRTD-VT	Cisco Firepower TD 仮想による脅威からの保護
L-FPRTD-V-TM	Cisco Firepower TD 仮想による脅威およびマルウェアからの保護
L-FPRTD-V-TC	Cisco Firepower TD 仮想による脅威からの保護と URL
L-FPRTD-V-TMC	Cisco Firepower TD 仮想による脅威、マルウェア、および URL フィルタリング
L-FPRTD-V-AMP	Cisco Firepower TD 仮想によるマルウェアからの保護
L-FPRTD-V-URL	Cisco Firepower Threat Defense 仮想 URL フィルタリング

シスコの環境保全への取り組み

シスコの企業の社会的責任（CSR）レポートの「環境保全」セクションでは、製品、ソリューション、運用・拡張運用、サプライチェーンに対する、シスコの環境保全ポリシーとイニシアチブを掲載しています。

次の表に、環境保全に関する主要なトピック（CSR レポートの「環境保全」セクションに記載）への参照リンクを示します。

持続可能性に関するトピック	参照先
製品の材料に関する法律および規制に関する情報	材料
製品、バッテリ、パッケージを含む電子廃棄物法規制に関する情報	WEEE 適合性

シスコでは、パッケージデータを情報共有目的でのみ提供しています。これらの情報は最新の法規制を反映していない可能性があります。シスコは、情報が完全、正確、または最新のものであることを表明、保証、または確約しません。これらの情報は予告なしに変更されることがあります。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、およびサードパーティの補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

シスコによるセキュリティの利点

シスコでは、一貫した可視性、ポリシーの整合性、強力なユーザおよびデバイス認証を備えた、世界有数のセキュリティ制御をあらゆる場所に提供できるセキュリティプラットフォームを構築しています。シスコは、ネットワーキングに関するリーダーシップと最先端のセキュリティ技術を組み合わせます。結果として、ネットワーク全体をファイアウォールの延長として機能させ、かつてないセキュアなアーキテクチャを実現することが可能になりました。最新世代の Cisco Firepower NGFW は、脅威に対して先手を打つために必要な能力と柔軟性を備えています。Cisco NGFW を使用することで、俊敏性と統合性の両方を備えたセキュリティの基盤に投資し、現在および将来、考え得る最も強力なセキュリティポスチャを実現できます。

お問い合せ先

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C78-742858-04JA 20.09