Cisco Secure Firewall Threat Defense Virtual (旧称 FTDv/NGFWv)

目次

今日の組織は、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コントロールポイント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、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を支援します。

Cisco® Secure Firewall Threat Defense Virtual（旧称 FTDv/NGFWv）は、シスコの実績のあるネットワークファイアウォールと Snort IPS、URL フィルタリング、およびマルウェア防御を組み合わせています。物理、プライベート、およびパブリッククラウド環境で一貫したセキュリティポリシーを使用して、脅威からの保護を簡素化します。ネットワークを詳細に可視化し、脅威の発生源とアクティビティをすばやく検出します。検出後、運用に影響が及ぶ前に攻撃を阻止します。

製品の概要

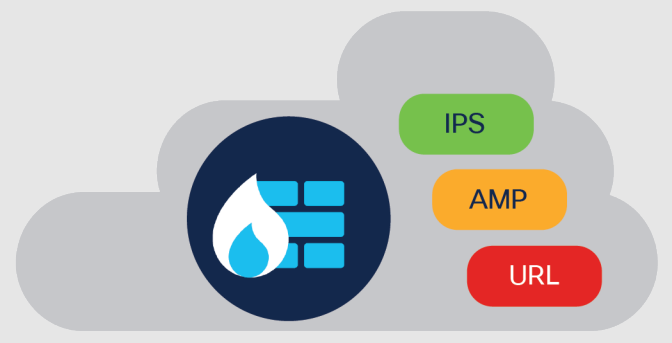

図 1.
Cisco Secure Firewall Threat Defense Virtual の概要

Secure Firewall Threat Defense Virtual は、人気の高い Secure Firewall Threat Defense（旧称 FTD）ソリューションの仮想化オプションです。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、仮想ファイアウォールのインスタンスを簡単に展開、管理、追跡できます。

利点

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。迅速な対応を必要とする影響の大きなアラートに集中できるよう、イベントのノイズと量を減らします。最高水準の Snort 3 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、OpenStack、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）、Oracle Cloud Infrastructure（OCI）、官公庁クラウド）間や、ハイパーコンバージド インフラストラクチャ（Cisco HyperFlex、Nutanix AHV）で仮想および物理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、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、および再配置を長期的に行い、物理、仮想、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

シスコの IPS ライセンス、マルウェア防御ライセンス、URL フィルタリングライセンスで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できます。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. Secure Firewall Threat Defense Virtual の機能と仕様

機能	仕様
Cisco Firewall デバイスマネージャ（ローカル管理）	ESXi、KVM、および OpenStack：バージョン 7.0 以降、Azure：バージョン 6.5 以降、AWS：6.6 以降、Cisco Hyperflex：バージョン 7.0 以降、Nutanix AHV：Version 7.0 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 Firewall Management Center（オンプレミスおよび AWS、Azure、GCP、OCI（6.7 以降）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、Cisco Hyperflex：バージョン 7.0 以降、 Nutanix AHV：Version 7.0 以降）で実行されます。
Application Visibility and Control（AVC）	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 サイトをサポートする標準
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 Secure Firewall の IPS ライセンス	使用可。Snort 3 IPS は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）を提供

機能	仕様
Cisco Secure Firewall の Malware Defense ライセンス	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 Secure Endpoint による統合脅威相関機能を使用可能。
Cisco Secure Malware Analytics サンドボックス分析	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エコシステム	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 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、Azure、GCP、OCI：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. Secure Firewall Threat Defense Virtual（ESXi/KVM/OpenStack）バージョン 7.0 以降のパフォーマンス仕様

ライセンスのタイプ	FTDv5（100M）	FTDv10（1G）	FTDv20（3G）	FTDv30（5G）	FTDv50（10G）	FTDv100（16G）
仕様	**4 vCPU**	**4 vCPU**	**4 vCPU**	**8 vCPU**	**12 vCPU**	**16 vCPU**
スループット：FW + AVC（1024B）	100 Mbps	1 Gbps	3Gbps	5.5 Gbps	10 Gbps	15.5 Gbps
スループット：FW + AVC + IPS（1024B）	100 Mbps	1 Gbps	3Gbps	5.5 Gbps	10 Gbps	15.5 Gbps
スループット：FW + AVC（450B）	100 Mbps	1 Gbps	1.5 Gbps	3Gbps	5 Gbps	7 Gbps
スループット：FW + AVC + IPS（450B）	100 Mbps	1 Gbps	1 Gbps	2 Gbps	3Gbps	7 Gbps

ライセンスのタイプ	FTDv5（100M）	FTDv10（1G）	FTDv20（3G）	FTDv30（5G）	FTDv50（10G）	FTDv100（16G）
仕様	4 vCPU	4 vCPU	4 vCPU	8 vCPU	12 vCPU	16 vCPU
同時セッションの最大数	100,000	100,000	100,000	250,000	500,000	2,000,000
1 秒あたりの最大新規接続数	12,500	20,000	20,000	20,000	40,000	130,000
VPN ピアの最大数	250	250	250	250	750	10,000
IPSec VPN スループット（1024B TCP、ファストパス対応）	100 Mbps	1 Gbps	1.1 Gbps	2 Gbps	4 Gbps	6 Gbps 8 Gbps（QAT（ESXi / KVM）搭載）

表 3.　Threat Defense Virtual 7.0 以降のパフォーマンス仕様：AWS *

ライセンスのタイプ	FTDv5（100M）	FTDv10（1G）	FTDv20（3G）	FTDv30（5G）	FTDv50（10G）	FTDv100（16G）
AWS インスタンスのタイプ	c5.xlarge	c5.xlarge	c5.xlarge	c5.2xlarge	c5.4xlarge	c5.4xlarge
スループット：FW + AVC（1024B）	100 Mbps	1 Gbps	2.2 Gbps	4.3 Gbps	8.6 Gbps	8.6 Gbps
スループット：FW + AVC + IPS（1024B）	100 Mbps	1 Gbps	2.2 Gbps	4.3 Gbps	8.4 Gbps	8.4 Gbps
スループット：FW + AVC（450B）	100 Mbps	1 Gbps	830 Mbps	1.4 Gbps	3.8 Gbps	3.8 Gbps
スループット：FW + AVC + IPS（450B）	100 Mbps	1 Gbps	830 Mbps	1.4 Gbps	3.2 Gbps	3.2 Gbps
同時セッションの最大数	100,000	100,000	100,000	200,000	2M	2M
1 秒あたりの最大新規接続数	24,500	24,500	24,500	45,900	82,800	82,800
VPN ピアの最大数	250	250	250	250	750	10,000
IPSec VPN スループット（1024B TCP、ファストパス対応）	100 Mbps	1 Gbps	1.4 Gbps	1.4 Gbps	4 Gbps	4 Gbps

* 非階層型ライセンスの場合、4 vCPU インスタンスのパフォーマンスは FTDv20 と一致し、8 vCPU のパフォーマンスは FTDv30 と一致し、16 vCPU インスタンスのパフォーマンスは FTDv100 と一致します。

表 4. Threat Defense Virtual 7.0 以降のパフォーマンス仕様：Azure*

ライセンスのタイプ	FTDv5（100M）	FTDv10（1G）	FTDv20（3G）	FTDv30（5G）	FTDv50（10G）	FTDv100（16G）
Azure VM のタイプ	**D3_v2、D3**	**D3_v2**	**D3_v2**	**D4_v2**	**D5_v2**	**D5_v2**
スループット：FW + AVC（1024B）	100 Mbps	1 Gbps	1.4 Gbps	1.5 Gbps	5.0 Gbps	5.0 Gbps
スループット：FW + AVC + IPS（1024B）	100 Mbps	1 Gbps	1.4 Gbps	1.5 Gbps	4.5 Gbps	4.5 Gbps
スループット：FW + AVC（450B）	100 Mbps	700 Mbps	700 Mbps	940 Mbps	1.0 Gbps	1.0 Gbps
スループット：FW + AVC + IPS（450B）	100 Mbps	700 Mbps	700 Mbps	920 Mbps	1.0 Gbps	1.0 Gbps
同時セッションの最大数	100,000	100,000	100,000	250,000	1.5 M	1.5 M
1 秒あたりの最大新規接続数	11,550	11,550	11,550	12,480	14,540	14,540
VPN ピアの最大数	250	250	250	250	750	10,000
IPSec VPN スループット（1024B TCP、ファストパス対応）	100 Mbps	830 Mbps	830 Mbps	1.6 Gbps	4 Gbps	4 Gbps

* Accelerated Networking（AN）が有効になっている仮想マシンで測定。非階層型ライセンスの場合、4 vCPU 仮想マシンのパフォーマンスは FTDv20 と一致し、8 vCPU のパフォーマンスは FTDv30 と一致し、16 vCPU のパフォーマンスは FTDv100 と一致します。

表 5. Threat Defense Virtual 7.0 以降のパフォーマンス仕様：GCP*

ライセンスのタイプ	FTDv5（100M）	FTDv10（1G）	FTDv20（3G）	FTDv30（5G）	FTDv50（10G）	FTDv100（16G）
GCP マシンタイプ	**c2-standard-4**	**c2-standard-4**	**c2-standard-4**	**c2-standard-8**	**c2-standard-16**	**c2-standard-16**
スループット：FW + AVC（1024B）	100 Mbps	1 Gbps	1.5 Gbps	5 Gbps	9.9 Gbps	9.9 Gbps
スループット：FW + AVC + IPS（1024B）	100 Mbps	1 Gbps	1.4 Gbps	5 Gbps	9.7 Gbps	9.7 Gbps
スループット：FW + AVC（450B）	100 Mbps	450 Mbps	450 Mbps	1.7 Gbps	2.3 Gbps	2.3 Gbps
スループット：FW + AVC + IPS（450B）	100 Mbps	450 Mbps	450Mbps	1.2 Gbps	2 Gbps	2 Gbps
同時セッションの最大数	100,000	100,000	100,000	250,000	2M	2M
1 秒あたりの最大新規接続数	12,000	12,000	12,000	45,000	84,000	84,000
VPN ピアの最大数	250	250	250	250	750	10,000

ライセンスのタイプ	FTDv5（100M）	FTDv10（1G）	FTDv20（3G）	FTDv30（5G）	FTDv50（10G）	FTDv100（16G）
GCP マシンタイプ	c2-standard-4	c2-standard-4	c2-standard-4	c2-standard-8	c2-standard-16	c2-standard-16
IPSec VPN スループット（1024B TCP、ファストパス対応）	100 Mbps	1 Gbps	1.5 Gbps	1.5 Gbps	4 Gbps	4 Gbps

* 非階層型ライセンスの場合、4 vCPU マシンのパフォーマンスは FTDv20 と一致し、8 vCPU のパフォーマンスは FTDv30 と一致し、16 vCPU のパフォーマンスは FTDv100 と一致します。

表 6. Threat Defense Virtual 7.0 以降のパフォーマンス仕様：OCI*

ライセンスのタイプ	FTDv5（100M）	FTDv10（1G）	FTDv20（2G）/ FTDv 30（5G）	FTDv50（10G）	FTDv100（16G）
OCI のシェイプタイプ	VM.Standard2.4	VM.Standard2.4	VM.Standard2.4	VM.Standard2.8	VM.Standard2.8
スループット：FW + AVC（1024B）	100 Mbps	1 Gbps	1.2 Gbps	2.4 Gbps	2.4 Gbps
スループット：FW + AVC + IPS（1024B）	100 Mbps	1 Gbps	1.2 Gbps	2.4 Gbps	2.4 Gbps
スループット：FW + AVC（450B）	100 Mbps	410 Mbps	410 Mbps	920 Mbps	920 Mbps
スループット：FW + AVC + IPS（450B）	100 Mbps	390 Mbps	390 Mbps	910 Mbps	910 Mbps
同時セッションの最大数	250,000	250,000	250,000	2M	2M
1 秒あたりの最大新規接続数	4900	4900	4900	10,000	10,000
VPN ピアの最大数	250	250	250	750	10,000
IPSec VPN スループット（1024B TCP、ファストパス対応）	100 Mbps	1 Gbps	1.2 Gbps	1.5 Gbps	1.5 Gbps

* 準仮想化インターフェイスで測定。非階層型ライセンスの場合、4 つの OCPU シェイプタイプのパフォーマンスは FTDv30 と一致し、8 つの OCPU シェイプタイプのパフォーマンスは FTDv100 と一致します。

システム要件

表 7. Secure Firewall Threat Defense Virtual 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 • 16 vCPU/32GB（Threat Defense Virtual バージョン 7.0 以降）
VMware および KVM：仮想 CPU およびメモリ（6.3 以前）	4 vCPU/8GB
VMware および KVM：Intel QuickAssist Technology（QAT）のサポート（7.0 以降）	UCS M5 サーバで認定された Intel QAT 8970 PCI アダプタ。FTDv100 でのみサポートされます。
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、7.0 KVM、Openstack、Nutanix AHV：AOS バージョン 5.20、AHV バージョン 20201105.2030。Cisco HyperFlex：データ プラットフォーム バージョン 4.5.1a-39020
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 • Accelerated Networking
GCP のサポート（6.7 以上）	• インスタンス：c2-standard-4、c2-standard-8、c2-standard-16、n1-standard-4、n1-standard-8、n1-standard-16、n2-standard-4、n2-standard-8、n2-standard-16、n1-highcpu-8、n2-highcpu-8、n1-highcpu-16、n2-highmem-4、n2-highmem-8、n2-highmem-16、n2-highcpu-16
OCI のサポート（6.7 以上）	• インスタンス：VM.Standard2.4、VM.Standard2.8

発注情報

表 8. Secure Firewall Threat Defense Virtual バージョン 7.0（階層ライセンス）の発注情報

部品番号	説明
FTDV-SEC-SUB	Cisco Firepower TD 仮想サブスクリプション
上記の PID を選択すると、次の階層型ベースおよび階層型脅威、マルウェア、URL フィルタリング サブスクリプションから選択できます。	
FTD-V-(X)S-BSE-K9*	Cisco Firepower TD 仮想の基本ライセンス
FTD-V-(X)S-T*	Cisco Firepower TD 仮想による脅威からの保護
FTD-V-(X)S-TM*	Cisco Firepower TD 仮想による脅威およびマルウェアからの保護
FTD-V-(X)S-TC*	Cisco Firepower TD 仮想による脅威からの保護と URL
FTD-V-(X)S-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
FTD-V-(X)S-AMP*	Cisco Firepower TD 仮想によるマルウェアからの保護
FTD-V-(X)S-URL*	Cisco Firepower Threat Defense 仮想 URL フィルタリング

* 「X」は、特定の階層モデル番号 5、10、20、30、50、および 100 を示します。

表 9. Secure Firewall Threat Defense Virtual （非階層型 ）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 Secure Firewall 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 Secure Firewall を使用すると、セキュリティの基盤に投資することになります。Secure Firewall には Cisco SecureX の権限が含まれており、すべてのシスコセキュリティ製品を一元的に可視化して、俊敏性と統合性の両方を備えたセキュリティを提供します。

ください。

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

C78-742858-09JA 22.02