Cisco Secure Firewall Threat Defense Virtual

目次

はじめに

Cisco® Secure Firewall Threat Defense Virtual は、次世代のファイアウォール（NGFW）機能を実現したもので、パブリック、プライベート、ハイブリッドのクラウド環境に適用できます。物理的なハードウェアの制約を受けず、堅牢で拡張性のあるセキュリティとシンプルな管理を提供します。

Cisco Secure Firewall Threat Defense Virtualは、Cisco Hybrid Mesh Firewall アーキテクチャをクラウドに拡張し、AIを活用した脅威の検査と一貫したセキュリティポリシーの強化を、設置場所を問わずワークロード全体にわたって提供します。クラウドネイティブのネットワーク構造とシームレスに統合して、アプリケーションのパフォーマンスを向上させ、ユーザーやワークロードなどに信頼性の高いセキュアなアクセスを確保します。

表 1. Cisco Secure Firewall Threat Defense Virtual の主な機能

Cisco Secure Firewall Threat Defense Virtual	
堅牢な接続性とポータビリティ • データセンターから分散拠点まで、どこにでもアプライアンスを展開できます。1 つのライセンスのポータビリティを利用して、パブリックやプライベートのクラウドにまたがる仮想デプロイメントをサポートします。 • ネイティブ自動スケールサポートにより、リアルタイムの通信需要に応じてファイアウォールのキャパシティを自動的に拡張でき、またクラスタリングにより、分散クラウド環境全体で高性能のスループットとレジリエンスを提供します。	**優れた可視性** • AI を活用した暗号化可視性エンジン（EVE）にて Transport Layer Security（TLS）1.3 を含む暗号化通信に関するインサイトと制御を得て、通信を復号する必要性を排除します。 • SnortML によりゼロデイ脆弱性からネットワークを保護します。SnortMLは、業界をリードする Snort 3 Cisco Intrusion Prevention System（IPS）に統合され、Cisco Talos インテリジェンスグループを搭載した機械学習ベースのエクスプロイト検出テクノロジーです。
シンプルな管理 • オンプレミスでもクラウド提供プラットフォームでも使用可能な単一の統合マネージャを使用して、世界中のさまざまな支社や拠点にわたる、数百のファイアウォールを管理できます。 • Cisco Multicloud Defense により、パブリッククラウド環境全体にわたってファイアウォールのデプロイメントを迅速かつ簡素に行い、オーケストレーションの一元化、一貫したポリシー管理、運用の合理化を実現します。	**シームレスな統合** • Cisco Umbrella®、Cisco Secure Access、Cisco Endpoint Security をネイティブと統合し、包括的なエンドツーエンドの保護を実現します。 • ゼロタッチプロビジョニング（ZTP）によって高速化し、シームレスに統合した SD-WAN 機能により、アプリケーションの性能とユーザー体験を最適化します。

フレキシブルなパフォーマンスベースのライセンス

シスコの仮想ファイアウォール アプライアンスは、パブリック、プライベート、ハイブリッドの各クラウドの導入を含む、広範なインフラストラクチャ環境で導入の柔軟性を提供するように設計した、パフォーマンスベースのライセンスモデルを活用しています。

各パフォーマンスライセンス階層では、次の 2 つの主要なパラメータを適用しています。

- **スループット（レート制限）**：統合型レートリミッタを介して最大ファイアウォール インスペクション スループットを制御し、選択した階層に合わせた予測可能で一貫したパフォーマンスを提供します。
- **リモートアクセス（RA）VPN セッション制限：**ライセンス階層の下でサポートされる同時リモートアクセス VPN セッションの最大数を定義します。

表 2. パフォーマンスライセンス階層

パフォーマンス階層	スループット（レート制限）	RA VPN セッション制限
FTDv5	100 Mbps	50 セッション
FTDv10	1 Gbps	250 セッション
FTDv20	3Gbps	250 セッション
FTDv30	5 Gbps	250 セッション
FTDv50	10 Gbps	750 セッション
FTDv100	16 Gbps	10,000 セッション
FTDvU（無制限）	レートリミッタなし	32,000 セッション

重要：Cisco Secure Firewall Threat Defense Virtual パフォーマンス階層は、パブリッククラウド環境で選択した仮想アプライアンスや、コンピューティング インスタンスまたはシェイプに割り当てられた、基本的なコンピューティングリソース（vCPUとメモリ）には影響しません。割り当てられたコンピューティングリソースによりアプライアンスの機能の拡張性、すなわちルーティングテーブルのサイズやアクセス制御ルールなどが決まります。この分離型アプローチにより、お客様は特定の要件を満たすために必要なコンピューティングリソースを使用して仮想ファイアウォールを個別にサイズ指定する柔軟性を確保でき、スループットや VPN セッションのニーズに合わせたパフォーマンスライセンス階層を選択できます。

導入とシステム要件

Cisco Secure Firewall Threat Defense Virtual は、すべての主要なパブリッククラウド マーケットプレイスで利用でき、業界をリードするハイパーバイザ プラットフォームでのデプロイメントをサポートしています。

表 3. 導入環境の概要

カテゴリ	対応プラットフォーム
プライベートクラウドまたはオンプレミス	VMware、KVM、OpenStack、Nutanix、Microsoft Hyper-V
パブリック クラウド	AWS、Azure、GCP、OCI、Alibaba Cloud、Megaport、Equinix
最小システム要件	4 vCPU	8 GB RAM	100 GB ディスク
最大システム要件	64 vCPU	128 GB RAM	500 GB ディスク

表 4. 導入環境（パブリッククラウド）の互換性マトリックス

カテゴリ	AWS	Azure	GCP	OCI	Alibaba	Megaport	Equinix
所有ライセンス持ち込み（BYOL）	対応	対応	対応	対応	対応	対応	対応
PAYG（Pay As You Go、従量制）	対応	対応	非対応	非対応	非対応	非対応	非対応
自動スケール	対応	対応	対応	対応	非対応	非対応	非対応
高可用性（クラスタリング）	対応	対応	対応	非対応	非対応	非対応	非対応
Cisco Multicloud Defense を介したオーケストレーション	対応	対応	対応	非対応	非対応	非対応	非対応
Cisco Firewall Management Center を介した管理	対応	対応	対応	対応	対応	対応	対応
Cisco Firewall Device Manager を介した管理	対応	対応	対応	非対応	非対応	非対応	非対応

表 5. 導入環境（プライベートクラウド）の互換性マトリックス

カテゴリ	VMware	KVM	Nutanix	OpenStack	Hyper-V	HyperFlex
所有ライセンス持ち込み（BYOL）	対応	対応	対応	対応	対応	対応
高可用性（アクティブまたはスタンバイ）	対応	対応	対応	対応	対応	対応
高可用性（クラスタリング）	対応	対応	非対応	非対応	非対応	非対応
Firewall Management Center を介した管理	対応	対応	対応	対応	対応	対応
Firewall Device Manager を介した管理	対応	対応	対応	対応	非対応	対応

注：サポートされている各導入環境の詳細については、該当するスタートアップガイドと Cisco Secure Firewall Threat Defense 互換性ガイドを参照してください。

パフォーマンスとスケール

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、トラフィックの種類とプロファイル、CPU の種類、CPU の速度、キャッシュ、インターフェイスの数などを含む環境によって異なります。サポートされているコンピューティング インスタンスやシェイプの完全なリストについては、該当するスタートアップガイドを参照してください。

表 6. Cisco Secure Firewall Threat Defense Virtual（ESXi/KVM/OpenStack）バージョン 10.0 以降で Snort3 と SR-IOV を実行した場合のパフォーマンス仕様：

メトリック	4 x vCPU	8 x vCPU	12 x vCPU	16 x vCPU	32 x vCPU	64 x vCPU
スループット：FW + AVC（1024B）	5 Gbps	7.2Gbps	19 Gbps	26 Gbps	59 Gbps	90Gbps
スループット：FW + AVC + IPS（1024B）	4.5Gbps	7Gbps	18 Gbps	25Gbps	55 Gbps	85Gbps
IPSec VPN スループット（1024B TCP、ファストパス対応）	2.2Gbps	3.2Gbps	6Gbps	10.5Gbps	35Gbps	67Gbps
同時セッションの最大数（AVC を使用した場合）	100K	250K	500K	2M	4M	8M
1 秒あたりの最大新規接続数（AVC を使用した場合）	27K	44K	80 K	135K	300K	500K
VPN ピアの最大数	250	250	750	10K	20K	32K
最大仮想ルータインスタンス（VRF）	30	30	30	30	30	30

メトリック	4 x vCPU	8 x vCPU	12 x vCPU	16 x vCPU	32 x vCPU	64 x vCPU
クラスタリング*	対応	対応	対応	対応	対応	対応

表 7. Cicso Secure Firewall Threat Defense Virtual（AWS）バージョン 10.0 以降で Snort3 と SR-IOV を実行した場合のパフォーマンス仕様：

メトリック	4 x vCPU	8 x vCPU	16 x vCPU
	c5n.xlarge	c5n.2xlarge	c5n.4xlarge
スループット：FW + AVC（1024B）	4Gbps	4.1Gbps	12 Gbps
スループット：FW + AVC + IPS（1024B）	3 Gbps	4.1Gbps	12 Gbps
IPSec VPN スループット（1024B TCP、ファストパス対応）	2.5Gbps	2.5Gbps	7.2Gbps
同時セッションの最大数（AVC を使用した場合）	250K	250K	2M
1 秒あたりの最大新規接続数（AVC を使用した場合）	13K	30 K	80 K
VPN ピアの最大数	250	250	10K
クラスタリング	非対応	対応	対応

表 8. Cisco Secure Firewall Threat Defense Virtual（Azure）バージョン 10.0 以降で Snort3 と SR-IOV を実行した場合のパフォーマンス仕様：

メトリック	4 x vCPU	8 x vCPU	16 x vCPU
	Standard_D3_v2	Standard_D8_v5	Standard_D16_v5
スループット：FW + AVC（1024B）	2.7Gbps	5.7Gbps	11Gbps
スループット：FW + AVC + IPS（1024B）	2.6 Gbps	5.6 Gbps	10.5Gbps
IPSec VPN スループット（1024B TCP、ファストパス対応）	1.6 Gbps	3.4Gbps	8.5Gbps
同時セッションの最大数（AVC を使用した場合）	250K	250K	2M
1 秒あたりの最大新規接続数（AVC を使用した場合）	20K	38K	100K
VPN ピアの最大数	250	250	10K
クラスタリング	非対応	対応	対応

表 9. Cisco Secure Firewall Threat Defense Virtual（GCP）バージョン 10.0 以降で Snort3 と SR-IOV を実行した場合のパフォーマンス仕様：

メトリック	4 x vCPU	8 x vCPU	16 x vCPU
	C2-Standard-4	C2-Standard-8	C2-Standard-16
スループット：FW + AVC（1024B）	4.5Gbps	4.5Gbps	12.5Gbps
スループット：FW + AVC + IPS（1024B）	2.7Gbps	4.5Gbps	12 Gbps
IPSec VPN スループット（1024B TCP、ファストパス対応）	3 Gbps	3 Gbps	7.5Gbps
同時セッションの最大数（AVC を使用した場合）	250K	250K	2M
1 秒あたりの最大新規接続数（AVC を使用した場合）	13K	32K	95K
VPN ピアの最大数	250	250	10K
クラスタリング	非対応	対応	対応

表 10. Cisco Secure Firewall Threat Defense Virtual（OCI）バージョン 10.0 以降で Snort3 と SR-IOV を実行した場合のパフォーマンス仕様：

メトリック	VM.Standard3		VM.Standard.A1		
	8 x vCPU (4 x OCPU)	16 x vCPU (8 x OCPU)	4 x vCPU (4 x OCPU)	8 x vCPU (8 x OCPU)	16 x vCPU (16 x OCPU)
スループット：FW + AVC（1024B）	4Gbps	8.1Gbps	3 Gbps	4.5Gbps	13Gbps
スループット：FW + AVC + IPS（1024B）	4Gbps	8.1Gbps	3 Gbps	4.5Gbps	13Gbps
IPSec VPN スループット（1024B TCP、ファストパス対応）	3.5Gbps	7.9Gbps	1.8 Gbps	2.5Gbps	8Gbps
同時セッションの最大数（AVC を使用した場合）	250K	2M	100K	250K	2M
1 秒あたりの最大新規接続数（AVC を使用した場合）	40K	120K	20K	32K	100K
VPN ピアの最大数	250	10K	250	250	10K
クラスタリング	非対応	非対応	非対応	非対応	非対応

表 11. Cisco Secure Firewall Threat Defense Virtual（Alibaba）バージョン 10.0 以降で Snort3 と SR-IOV を実行した場合のパフォーマンス仕様：

メトリック	4 x vCPU	8 x vCPU	16 x vCPU
	g5ne.xlarge	g5ne.2xlarge	g5ne.4xlarge
スループット：FW + AVC（1024B）	3.1Gbps	3.7Gbps	9.6Gbps
スループット：FW + AVC + IPS（1024B）	2.1 Gbps	3.6Gbps	9Gbps
IPSec VPN スループット（1024B TCP、ファストパス対応）	2 Gbps	2.2Gbps	6.1Gbps
同時セッションの最大数（AVC を使用した場合）	250K	250K	2M
1 秒あたりの最大新規接続数（AVC を使用した場合）	10K	25K	70K
VPN ピアの最大数	250	250	10K
クラスタリング	非対応	非対応	非対応

発注情報

パフォーマンス階層型ライセンスは、Firewall Threat Defense Virtual バージョン 7.0 以降で使用できます。新しいライセンスモデルには、サブスクリプションとして基本ライセンスも含まれています。ライセンス、サブスクリプション、製品に関連するその他のオプションの詳細については、『ネットワークセキュリティ発注ガイド』を参照してください。

表 12. Cisco Secure Firewall Threat Defense Virtual の発注情報

製品 ID	説明
FTDV-SEC-SUB	Cisco Secure Firewall Threat Defense Virtual サブスクリプション
上記の PID を選択すると、適切なパフォーマンス階層と、1 つ以上の利用可能なアドオン サブスクリプション ライセンス（T-Threat、M-Malware Defense、URLフィルタリング）を選択できます。	

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」セクションには、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が掲載されています。

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 Secure Firewall（FTD）の全てがワンストップで分かる日本語サイト FTD How To 公開中！**
  https://cs.co/ftd

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

米国で印刷　C78-6090559-00　04/26