データシート

Cisco Public

Cisco Secure Firewall Threat Defense Container

目次

はじめに

今日の急速に変化するデジタル環境では、さまざまな組織が、コンテナ化されたアプリケーションの迅速な導入により、比類のない拡張性、柔軟性、および効率性を実現しています。ただし、コンテナの導入が進むにつれて、それらを保護することの複雑さも増していきます。従来のセキュリティ対策では、多くの場合、こうした動的な環境に必要な保護を十分に提供できません。そこで、専用のコンテナファイアウォールが不可欠になります。

Cisco® Secure Firewall Threat Defense Container（FTDc）は、AI を利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による次世代ファイアウォール機能（NGFW）を提供し、Cisco Hybrid Mesh Firewall アーキテクチャをコンテナネットワークに拡張します。これにより、組織に最適なパフォーマンスレベルを選択できます。スケーラブルな VPN 機能により、組織のリソースへの安全なアクセスを確保しながら、進化し続ける複雑な脅威からワークロードを保護できます。

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

Cisco Secure Firewall Threat Defense Container	
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およびコンテナデプロイメントをサポートします。 • HELM チャートを介したコンテナのライフサイクル管理。 • Sidecar を介したロータッチプロビジョニング（LTP）。 • 従来のネットワーク構造とコンテナ固有の属性に基づくレイヤ 3 からレイヤ 7 のファイアウォール機能。	**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フォームファクタでも使用可能な単一の統合管理コンソールを使用して、世界中のさまざまな支社や拠点にわたる、数百の物理ファイアウォール、仮想ファイアウォール、またはコンテナファイアウォールを管理できます。	**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。

フレキシブルなパフォーマンスベースのライセンス

シスコのコンテナファイアウォールは、仮想フォームファクタと同じパフォーマンスベースのライセンスモデルを利用しており、さまざまなインフラストラクチャ環境で導入の柔軟性を実現するように設計しています。この統合型ライセンスアプローチにより、単一の PID セットで、パブリックとプライベートの両クラウド環境にわたって、仮想デプロイメントとコンテナ化デプロイメントの両方に対応できます。

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
FTDc5	100 Mbps	50 セッション
FTDc10	1 Gbps	250 セッション
FTDc20	3Gbps	250 セッション
FTDc30	5 Gbps	250 セッション
FTDc50	10 Gbps	750 セッション
FTDc100	16 Gbps	10,000 セッション
FTDcU (無制限)	レートリミッタなし	32,000 セッション

重要：FTDc 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コンテナアプライアンスや、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コンテナ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

表 3. 導入環境の概要

カテゴリ	サポート対象環境
プライベートクラウドまたはオンプレミス	
コンテナランタイム	Docker：26.1.3 以降
Kubernetes のバージョン	Kubernetes - 1.29.15 以降、1.31.14 まで
オペレーティングシステムとバージョン	Ubuntu - 20.04 LTS 以降、22.04 LTS まで
CNI（コンテナ ネットワーク インターフェイス）	Macvlan、SR-IOV
パブリック クラウド	
AWS	EKS（Elastic Kubernetes Service）- 1.30 以降、1.31 まで

カテゴリ	サポート対象環境
システムと導入要件	
最小システム要件	4 vCPU	8 GB RAM	50 GB ディスク
最大システム要件	32 vCPU	64 GB RAM	500 GB ディスク
構成モード	ルーテッド
ハイ アベイラビリティ	今後のリリースで提供予定
クラスタリング	今後のリリースで提供予定

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 4. FTDc（Docker/Kubernetes）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
スループット：FW + AVC（1024B）	5 Gbps	7.2Gbps	19 Gbps	26 Gbps	59 Gbps
スループット：FW + AVC + IPS（1024B）	4.5Gbps	7Gbps	18 Gbps	25Gbps	55 Gbps
IPSec VPN スループット（1024B TCP、ファストパス対応）	2.2Gbps	3.2Gbps	7Gbps	10.5Gbps	35Gbps
同時セッションの最大数（AVC を使用した場合）	100K	250K	500K	2M	4M
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
VPN ピアの最大数	250	250	750	10K	20K
最大仮想ルータインスタンス（VRF）	30	30	30	30	30
高可用性 – アクティブまたはスタンバイ	今後のリリースで提供予定				
高可用性 – クラスタリング	今後のリリースで提供予定				

発注情報

パフォーマンス階層型ライセンスは、Firewall Threat Defense 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 5. Cisco Secure Firewall Threat Defense Container の発注情報

製品 ID	説明
FTDV-SEC-SUB	Cisco Secure Firewall Threat Defense Virtual / Container 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　C78-6064201-00　04/26