Cisco Secure Firewall Threat Defense Container

目次

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、クラウドファイアウォールのニーズに対応するコンテナ化されたソリューションです。これは、企業が従来のデータセンターで使用してきたものと等しい堅牢なセキュリティをコンテナネットワークで提供します。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、最高クラスのセキュリティ制御によって、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。

製品の概要

Cisco Secure Firewall Threat Defense Container は、コンテナ環境において導入および拡張できるファイアウォールです。コンテナフォームファクタを使用すると、コンテナファイアウォールの展開、拡張、および管理が簡素化されます。Cisco Secure Firewall Threat Defense Container が提供する強力なステートフル L3/L4 ファイアウォール機能を設定して、ネットワーク、VPN を介したユーザーアクセス、およびコンテナがネットワークの残りの部分にアクセスする方法を保護できます。

ステートフル L3/L4 ファイアウォール機能に加えて、Cisco Secure Firewall Threat Defense Container には、仮想、物理、およびコンテナタイプの Cisco Secure Firewall ソリューションを管理する方法が簡素化される、ポリシーの一貫性を備えた強力な VPN 機能が含まれています。シスコ スマート ライセンシングにより、プライベート/パブリッククラウドで実行されているアプライアンスのコンテナ化されたインスタンスを簡単に展開、管理、追跡できます。

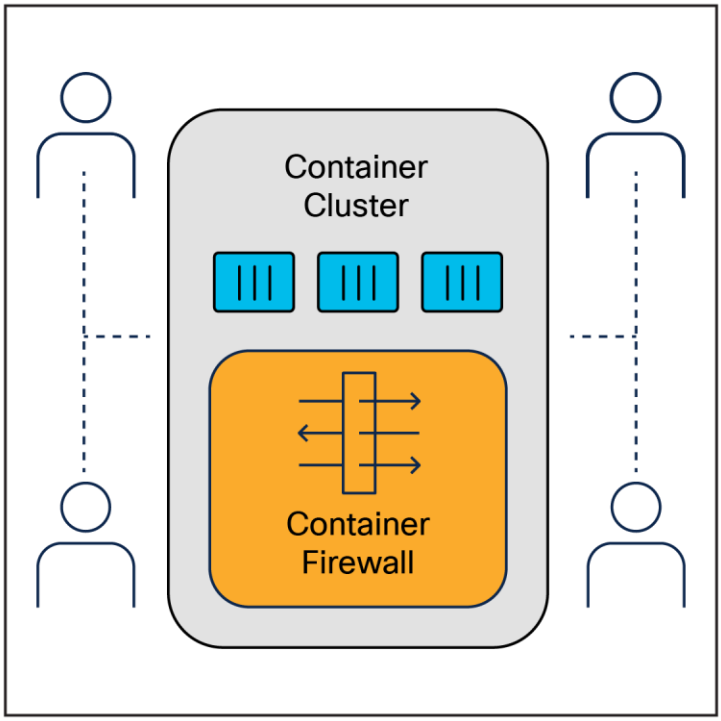

図 1.
パブリッククラウドまたはプライベートクラウドに展開された Cisco Secure Firewall Threat Defense Container

利点

L3/4 ファイアウォール機能

Cisco Secure Firewall Threat Defense Container は、堅牢なセキュリティとトラフィック管理を実現する L3/L4 ファイアウォール機能を提供します。顧客がネットワークトラフィックを正確にフィルタ処理および管理できるようにすることで、効率的なトラフィック制御を実現します。これにより、承認されたデータパケットのみが通過できるようになり、コンテナ環境が不正アクセスから保護されます。また、セキュアゾーンへのネットワーク セグメンテーションを可能にすることで、拡張可能なネットワーク セグメンテーションを実現し、カスタマイズされたセキュリティポリシーの適用により、機密性の高いワークロードを保護するとともに、全体的なセキュリティ態勢を強化します。

VPN ヘッドエンド

Cisco Secure Client は、従業員が自宅などあらゆる場所のあらゆるデバイスから、いつでも安全に作業できるようにします。企業ネットワークへの高度にセキュアなアクセスをユーザーに提供するとともに、インフラストラクチャにアクセスしているユーザーやデバイスを特定するための可視性と制御性をIT およびセキュリティチームに提供することができます。また、IT およびセキュリティチームがオフサイトの従業員や個人のデバイスをサポートする際の負担を軽減することもできます。Cisco Secure Firewall Threat Defense Container は、複数のデータセンターを接続するためのサイト間 VPN をサポートしています。

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、カーネルベース仮想マシン（KVM）と Hyper-V、OpenStack、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）、Oracle Cloud Infrastructure（OCI）、官公庁クラウド）間の 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、パブリッククラウドに至るまで、あらゆる場所に Cisco Secure Firewall Threat Defense Container 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、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。

ロータッチ導入

アプリケーションまたは VPN の計画外もしくは季節的な需要増に対応するために、追加の Cisco Secure Firewall Threat Defense Container アプライアンスをコンテナクラスタに迅速に導入できます。新しい仮想マシンをスピンアップすることで、リモートオフィスの帯域幅や保護を強化できます。さらに保護が必要な場合は、よりパフォーマンスの高いモデル（オプション）を選択できます。

スマート ソフトウェア ライセンシング

シスコ スマート ライセンシングにより、シスコのライセンスの購入、展開、追跡、更新が容易になります。以下のようなメリットがあります。

- 仮想アプライアンスのより簡単な購入とアクティベーション
- ライセンスプーリングにより、ライセンス管理と仮想アプライアンスのレポートが容易
- 仮想アプライアンスのプロビジョニング時の自動ライセンス アクティベーション

お客様、セレクトパートナー、およびシスコは、Cisco Smart Software Manager で製品の権限とサービスを閲覧できます。設定とアクティベーションは、単一のトークンで行います。Cisco Secure Firewall Threat Defense Container はクラウドのシスコサーバーに自己登録するため、製品アクティベーションキー（PAK）で製品を登録する必要はありません。スマート ソフトウェア ライセンシングでは、PAK またはライセンスファイルを使用する代わりに、組織全体で使用できるソフトウェアライセンスまたは権限のプールを確立します。お客様の社内で仮想アプライアンスがインスタンス化されると、プールから権限が減少します。仮想アプライアンスが停止された場合、または Smart Software Manager でインスタンス化が解除された場合は、権限がプールに追加されます。

Smart Software Manager を使用すれば、企業全体のライセンス展開を簡単かつ迅速に管理できます。また、スマート ソフトウェア ライセンシングをサポートするシスコの複数の製品を管理することもできます。

Cisco Secure Firewall Threat Defense Container は、スマート ソフトウェア ライセンシングを排他的に使用します。以前の形式のライセンシングはサポートしていません。

すべての Cisco Secure Firewall Threat Defense Container ライセンスは、サポートされているすべての FTDc vCPU/メモリ構成で使用できます。この機能により、顧客は、さまざまな VM リソースフットプリントで実行できるようになります。また、サポート対象の AWS、Azure、GCP、および OCI インスタンスタイプの数も増えます。Cisco Secure Firewall Threat Defense Container VM を構成する場合、サポートされる最大 vCPU 数は 16 個です。また、サポートされる最大メモリ容量は 128 GB RAM です。

表 1. K8s および Docker 上のスタンドアロン FTDc

スタンドアロン **FTDc**	
FTDc vCPU/メモリ	**1 vCPU/2 GB**

スタンドアロン FTDc	
FTDc vCPU/メモリ	**1 vCPU/2 GB**
ステートフル インスペクション スループット（最大）[1]	1 Gbps
スループット：**FW（450B）**	500 Mbps
IPsec VPN スループット（**AES 450B UDP** テスト）[2]	250 Mbps
1 秒あたりの接続数	6000
並列セッション	100,000
VLAN	50
ブリッジ グループ	25
IPsec VPN ピア数	250
Cisco Secure Client またはクライアントレス **VPN** のユーザーセッション数	250
仮想 **CPU** コアの割り当て[3]	1
メモリ割り当て	2 GB

[1] 記載されたリソース割り当ては、各階層の記載されたパフォーマンスの数字を達成するために必要。割り当て数が少ない場合もサポートされるが、パフォーマンスが低下する可能性がある。

[2] スループットは、最適なテスト条件下で 1500B User Datagram Protocol（UDP）トラフィックを使って計測。

[3] VPN スループットとセッション数は、FTD のデバイス設定と VPN のトラフィックパターンによって異なる。これらの要素はキャパシティプランニングの一環として考慮する必要がある。

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。

Printed in USA C78-5121851-00 04/25