Cisco Secure Firewall Cloud Native

目次

オンデマンドかつアジャイルで拡張性に優れたセキュリティサービスの必要性は、「どこからでも仕事ができる」という社風と、従業員が個人のデバイスから企業アプリケーションにアクセスする必要性に伴い、非常に高まっています。組織は通常、個々のコンポーネントを入手し、さまざまなベンダーのツールを使用してそれらを手動で自動化し、調整することで拡張性に優れたシステムを構築しています。このアプローチでは複雑さが生じて、スケーラブルなサービスのプロビジョニング、管理、およびトラブルシューティングが困難になります。

Cisco® Secure Firewall Cloud Native は、Kubernetes オーケストレーションを使用して、オンデマンドで、拡張性と復元力に優れたセキュリティサービスを導入するためのプラットフォームを提供します。拡張性、ロードバランシング、およびサービスの可用性に関連する複雑さを軽減します。これにより、SecOps チームはセキュリティポスチャの管理と適用に専念できます。

Secure Firewall Cloud Native を使用すると、組織に必要なパフォーマンスを柔軟に選択できます。パブリッククラウドとプライベートクラウドで、アジャイルで柔軟なセキュリティを提供します。スケーラブルで多機能な VPN 機能により、従業員、パートナー、サプライヤに対してセキュアなリモートアクセスが提供されるとともに、業界最先端のセキュリティ制御により、複雑化する脅威からワークロードが保護されます。

製品の概要

Secure Firewall Cloud Native は、セキュリティサービスの管理を簡素化する共通のフレームワークと、セキュリティサービスを自動的に拡張および制御するプラットフォームを提供します。お客様はプロビジョニングするサービスを選択できるため、チームは必要に応じてセキュリティを展開および拡張することができます。

拡張性と復元力を実現するために Kubernetes を使用します。お客様は、セキュリティサービス全体を設定するだけです。Secure Firewall Cloud Native は、ユーザ定義のメトリックに基づいてスケールアップまたはスケールダウンし、各サービスの正常性とパフォーマンスを監視します。任意の時点で実行されるサービスの各インスタンスの設定をカスタマイズし、イベントとログをユーザ設定のシンクに転送します。さらに、自動障害回復機能も提供します。

セキュリティポリシーは、Cisco Defense Orchestrator（CDO）、シンプルな GUI または REST API を使用した、機能豊富な Software-as-a-Service（SaaS）管理アプリケーションによって管理されます。Secure Firewall Cloud Native は、Infrastructure as Code として展開するオプションを含む、広範な自動化機能を提供します。

Secure Firewall Cloud Native は、リリース時に Amazon Web Services で利用でき、まもなく他のプラットフォームでも展開されます。

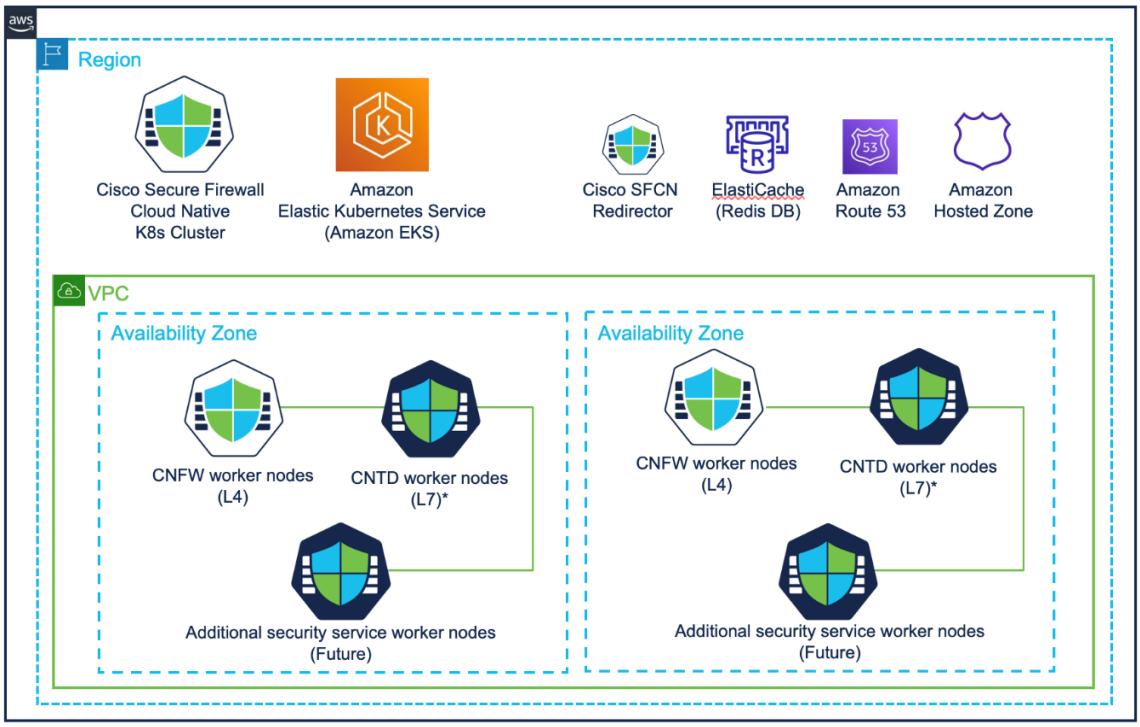

図 1.
Cisco Secure Firewall Cloud Native の概要

Secure Firewall Cloud Native を使用した拡張性の高い VPN サービス

拡張性に優れた VPN サービスを導入するには、クラウド ネイティブ ファイアウォール（CNFW）サービスを備えた Secure Firewall Cloud Native を導入します。

CNFW サービスの一部として展開される 3 つの主要コンポーネントは次のとおりです。

1. **コントロールプレーンポッド：**コントロールプレーンポッドは、VPN サービスの設定を行います。管理アプリケーションまたは REST API から設定を受け入れます。これらのポッドは、設定を検証し、適用ポイントに配布します。
2. **適用ポイントポッド：**適用ポイントポッドは、VPN セッションの実際の終了とトラフィックの転送を行います。
3. **リダイレクタポッド：**リダイレクタポッドは、各適用ポイントポッドの負荷のリアルタイム評価に基づいて、適用ポイントポッド間のセッションのスマートロードバランシングを行います。

Secure Firewall Cloud Native をインストールすると、すべてのコンポーネントが自動的に展開されます。お客様は、プラットフォームに導入する必要がある適用ポイントポッドの数に基づいてサイジングを決定することを推奨します。この推奨事項は、予想されるピーク VPN スループットと平均 VPN スループットに基づいています。システムは高い拡張性と弾力性を考慮して設計されており、見積もりはいつでも簡単に調整できるため、最初の見積もりが正確でなくても心配する必要はありません。

AWS のリソース使用率の詳細

各コンポーネントは、AWS 上の特定のインスタンスタイプで実行するように最適化されています。次の表に、各コンポーネントのインスタンスタイプの詳細を示します。

コンポーネント	インスタンス タイプ
コントロールプレーンポッド	m5.xlarge
適用ポイント ポッド	m5.xlarge
リダイレクタポッド[1]	m5.xlarge

[1] リダイレクタ機能には Redis データベースが必要で、デフォルトで m5. large インスタンスにインストールされます。デフォルトは簡単に変更でき、より大きなまたはより小さなインスタンスタイプを使用して、より多くの（または少ない）メモリを割り当てることができます。

インストーラは、適切なインスタンスタイプで各コンポーネントを展開します。

評価指標

Cisco Secure Firewall Cloud Native の VPN のパフォーマンスは、各適用ポイントポッドのパフォーマンスの合計に等しくなります。システムは柔軟性が高く、現在のパフォーマンス要件に基づいて適用ポイントポッドを動的に追加または削除します。次の表に、各適用ポイントポッドのテスト済み VPN パフォーマンスを示します。

機能	パフォーマンス
IPsec VPN スループット（AES 450B UDP テスト）[1]	1.5 Gbps
IPsec VPN ピア数	2000
Cisco AnyConnect® またはクライアントレス VPN のユーザセッション数	2000

[1] VPN スループットとセッション数は、設定と VPN のトラフィックパターンによって異なります。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ります。

ポッドごとのパフォーマンスに基づいて、スケーリングの制限を設定できます。

1. 適用ポイントポッドの最小数：常にプロビジョニングされるポッドの数。
2. 適用ポイントポッドの最大数：任意の時点でプロビジョニングできるポッドの最大数。

Secure Firewall Cloud Native は、指定された VPN パラメータを使用して負荷をモニタし、負荷に基づいて指定された範囲内のポッドの数を動的に決定します。

コンポーネントの拡張性

次の表に、テストされた各コンポーネントの拡張性の制限を示します。

属性	拡張性
Secure Firewall Cloud Native の 1 つのインスタンスに展開できる適用ポッドの最大数	75*
1 つのコントロールプレーンポッドで管理できる適用ポッドの最大数	75*

* これらの数値は、シスコを通じてテストおよび検証されています。テスト済みのものよりも規模が大きい場合は、シスコの営業担当者にお問い合わせください。

Cisco Secure Firewall Cloud Native のライセンス

Cisco Secure Firewall Cloud Native で実行されるサービスにはライセンスが付与されます。各サービスは、サービスに割り当てられた CPU コアの数に基づき、シスコスマートライセンシングを使用してライセンスが付与されます。

CNFW サービスでは、展開されている適用ポイントポッドごとに、Cisco スマートライセンスアカウントで 4 つのライセンスを使用できる必要があります。

スマート ソフトウェア ライセンシング

シスコのスマート ソフトウェア 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。Secure Firewall Cloud Native はクラウドのシスコサーバ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、企業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 CNFW 適用ポイントポッドがインスタンス化されると、プールから各 CPU コアの権限が減少します。ライセンス済みの CNFW 適用ポイントポッドが停止された場合、または Smart Software Manager でインスタンス化が解除された場合は、権限がプールに戻されます。

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 Cloud Native 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。

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。

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

C78-744973-00JA 21.10