はじめに

Cisco Secure Workload の概要

現代のネットワークには、ベアメタル、仮想化、クラウドベース、およびコンテナベースのワークロードを使用し、ハイブリッドなマルチクラウド環境で実行されるアプリケーションが含まれています。重要な課題は、ネットワークの俊敏性を損なうことなく、アプリケーションとデータをより安全に保護する方法を実現することです。Cisco Secure Workload（旧称 Cisco Tetration）は、アプリケーションにふさわしいセキュリティを提供し、アプリケーションの動作に基づいてセキュリティ態勢を調整することで、包括的なワークロード保護を実現し、このセキュリティの課題に対処できるように設計されています。Secure Workload は、高度な機械学習および行動分析技術を使用してこれを達成します。プラットフォームには、次のセキュリティユースケースをサポートする、すぐに使用できるソリューションが用意されています。

- ゼロトラストモデルの実装を許可するマイクロセグメンテーションポリシー：ビジネス目的で必要なトラフィックのみを許可するポリシーを適用します。
- ワークロードの行動的ベースライン、分析、および異常の特定。
- 一般的な脆弱性とサーバーにインストールされたソフトウェアパッケージに関連したエクスポージャーの検出。
- 脆弱性の検出時にサーバーをプロアクティブに隔離し、通信をブロックするポリシーを適用可能。

ワークロードについて

ワークロードは IP アドレスです。

この製品では、「IPアドレス」と呼ばれる Secure Workload エージェントがインストールされていないホストと区別するために、「ワークロード」は特にエージェントがインストールされているホストを指す場合があります。

クイックスタートウィザード

オプションのウィザードを使用すると、範囲ツリーの最初のブランチを作成できます。これは、選択したアプリケーションのポリシーを生成して適用するための最初のステップです。その過程において、このウィザードはラベルと範囲の概念（およびその強力なメリット）を紹介します。

次のユーザーロールがこのウィザードにアクセスできます。

- サイト管理者
- カスタマーサポート
- ルート範囲の所有者

このウィザードにアクセスするには、次の手順を実行します。

- [整理（Organize）] > [範囲とインベントリ（Scopes and Inventory）] で範囲を定義することはできません

  （範囲が既に作成されている場合は、既存の範囲をすべて削除しない限り、このウィザードに再度アクセスすることはできません）。

- Cisco Secure Workload にサインインすると、このウィザードが表示されます。
- または、任意のページの上部で、青いバナー内のリンクをクリックします。
- または、ウィンドウの左側にあるメインメニューから [概要（Overview）] を選択します。

詳細情報：

- *Cisco Secure Workload Quick Start Guide*（https://cisco.com/go/secure-workload-quick-start-guide）[英語]
- ワークロードラベル
- 範囲とインベントリ
- ソフトウェアエージェントの展開
- セグメンテーション

マイクロセグメンテーションを使用する前に

以下の手順は非常に高度なものです。Secure Workloadを使用してマイクロセグメンテーションを設定するための出発点として使用してください。

マイクロセグメンテーション導入の一般的なプロセス

始める前に

要件を満たす。

ワークロードが実行されているプラットフォームとバージョン、およびポリシーに通知する重要な情報を提供するシステムをSecure Workloadがサポートしていることを確認します。https://www.cisco.com/go/secure-workload/requirements/agentsを参照してください。

ステップ1 ワークロードにエージェントをインストールします。

エージェントは、ワークロードをグループ化し適切なポリシーを決定するためにユーザーとSecure Workloadによって使用されるフローデータやその他の情報を収集します。その後準備ができた時点で、これらのエージェントは、ユーザーが承認したポリシーを適用します。サポートされているプラットフォームと要件のリストへのリンクを含む詳細については、「ソフトウェアエージェントの展開」を参照してください。

ステップ2 ワークロードを説明するラベルを収集するかアップロードします。

ラベルを使用すると、各ワークロードの目的やその他の重要な情報を容易に把握できるようになります。

この情報は、ワークロードをグループ化し、適切なポリシーを適用し、Secure Workloadによって提案されたポリシーを理解するために必要です。ラベルは、長期的なポリシー管理を簡素化するセルフメンテナンスグループの基盤です。詳細については、「ワークロードラベル」と「カスタムラベルのインポート」を参照してください。

ステップ3 ワークロードのラベルに基づいて範囲ツリーを作成します。

ラベルが作成に役立つワークロードの論理グループは「範囲」と呼ばれ、適切に選択されたラベルのセットは、範囲ツリーと呼ばれるネットワークの階層型マップを作成するのに役立ちます。ネットワーク上のワークロードの階層ビューは、ポリシーを効率的に作成およびメンテナンスするための鍵です。このビューを使用すると、ポリシーを1度作成するだけで、そのポリシーをツリーの該当するブランチのすべてのワークロードに自動的に適用できます。また、特定のアプリケーション（またはネットワークの一部）に関する責任を、それらのワークロードの正しいポリシーを決定するために必要な専門知識を持つ人員に委任することもできます。

ラベルに基づくクエリに基づいて、ワークロードを範囲にグループ化します。たとえば、「Application = Email-app」および「Environment = Production」というラベルを持つすべてのワークロードを含む「Email-app」という範囲を作成できます。「Environment = Production」というクエリを使用して、この範囲の親範囲を作成できます。Production（実稼働）範囲には、実稼働Emailappと、「Environment = Production」とラベル付けされた他のすべてのワークロードが含まれます。

詳細については、「範囲とインベントリ」を参照してください。

ステップ 4 ポリシーを適用する範囲ごとにワークスペースを作成します。

ワークスペースは、範囲内の全ワークロードのポリシーを管理する場所です。詳細については、「ワークスペース」を参照してください。

ステップ 5 ネットワーク全体に広く適用されるポリシーを手動で作成します。

たとえば、すべての内部ワークロードからNTPサーバーへのアクセスを許可し、すべての外部トラフィックを拒否するか、明示的に許可されていない限り、すべての非内部ホストからのアクセスを拒否することができます。より詳細に適用されるポリシーでオーバーライドできない絶対ポリシーと、より具体的なポリシーが存在する場合にオーバーライドできるデフォルトポリシーを作成できます。通常、これらのポリシーは、ツリーの最上部に近い範囲に関連付けられたワークスペースで作成します。

ステップ 6 範囲ツリー内の下位の範囲に関するポリシーを自動的に検出します。

Secure Workload は、ワークロード間のトラフィックを分析して、動作に基づいてワークロードをグループ化し、既存のトラフィックパターンに基づいて一連のポリシーを提案します。

一般に、長期間にわたるフローデータが多いほど、より正確なポリシー提案が作成されます。

ポリシーは繰り返し検出できます（下記を参照）。

詳細については、「自動ポリシー検出」を参照してください。

ステップ 7 Secure Workload によって提案されたポリシーを確認して分析します。

提案されたポリシーを確認して、各ワークロードに関連付けられたラベルに基づき、それらが意味をなすかどうかを確かめます。Secure Workload でポリシー分析やその他のツールを使用して、組織がビジネスを実施するために必要なトラフィックが提案されたポリシーに許可されているかどうかを判断します。たとえば、「ライブ分析」を参照してください。

- 範囲内のワークロードのクラスタリングを理解します。

  クラスタは 1 つの範囲内で密接に関連しているワークロードのグループであり、クラスタでは、範囲全体を対象としたポリシーよりもカスタマイズされたポリシーの方が正当とされる可能性があります。

- 継承の影響を考慮します。

  ポリシーの結果を分析するときは、階層に含まれる各範囲の上位の範囲に属するワークスペースのポリシーが、同じブランチの下位の範囲のワークロードに影響を与える可能性があることに注意してください。

組織内の対象分野の専門家と協力して、組織のニーズと提案されたポリシーの適切性を判断してください。

ステップ 8 必要に応じて繰り返しポリシーを検出します。

トラフィックフローデータが多いほどポリシーの提案がより正確になるため（たとえば、毎月実行されるレポートがある場合、3 週間分のデータでもすべての重要なトラフィックをキャプチャできていない可能性があります）、ポリシーの検出を継続し、新たに検出されたポリシー提案を確認し分析できます。検出を実行するたびに、その時点における既存のトラフィックフローに基づいてポリシーが提案されます。

自動ポリシー検出を再実行する前に、上書きしないポリシーを承認できます。

「自動ポリシー検出の再実行」を参照してください。

ステップ 9 準備ができたら、ポリシーを承認して適用します。

ワークスペース（および関連付けられた範囲）に関連付けられたポリシーが適切であり、重要なサービスを中断せずに不要なトラフィックをブロックすると判断したら、それらのポリシーを承認して適用できます。

ポリシーは繰り返し適用できます。たとえば、最初は手動で作成したポリシーのみを適用し、その後、時間の経過とともに、確認し承認した検出済みのポリシーを適用していくことができます。

ベアメタルまたは仮想マシンで実行されるワークロードのマイクロセグメンテーションを設定する

ステップ 1 ネットワーク上のワークロードの IP アドレスの収集を開始します。

ワークロードごとに、アプリケーション名、アプリケーションの所有者、環境（本番または非本番）、および適用するポリシーを決定するその他の情報（地理的地域など）も必要になります。

構成管理データベース（CMDB）がない場合は、この情報をスプレッドシートで収集できます。

開始するには、焦点を合わせる単一のアプリケーションを選択します。

ステップ 2 サポートされているベアメタルベースまたは仮想ワークロードにエージェントをインストールします。

「ソフトウェアエージェントの展開」を参照してください。

ステップ 3 これらのワークロードを説明するラベルをアップロードします。

「ワークロードラベル」と「カスタムラベルのインポート」を参照してください。

必要に応じて、初回ウィザードを実行して、選択したアプリケーションのラベルと範囲ツリーの最初のブランチを作成できます。ウィザードを実行した後、ポリシーの作成にスキップできます。ウィザードの詳細については、「クイックスタートウィザード」を参照してください。

ステップ 4 ラベルに基づいて範囲ツリーを作成します。

「範囲とインベントリ」を参照してください。

ステップ 5 ポリシーを適用する範囲ごとにワークスペースを作成します。

「ワークスペース」を参照してください。

ステップ 6 ネットワーク全体に広く適用される手動ポリシーを作成します。

範囲に関連付けられたワークスペースですべてのポリシーを作成します。

ステップ 7 下位レベルの範囲に関連付けられたワークスペースのポリシーを自動的に検出します。

「自動ポリシー検出」を参照してください。

ステップ 8 提案されたポリシーを確認して分析します。

たとえば、「ライブ分析」を参照してください。

ステップ 9 必要に応じて繰り返しポリシーを検出します。

「自動ポリシー検出の再実行」を参照してください。

ステップ 10 準備ができたら、ポリシーを承認して適用します。

各ワークスペースのポリシーの動作に問題がなければ、ポリシーを適用できます。

ワークスペースとエージェントでポリシーの適用を有効にする必要があります。

クラウドベースのワークロードに対するマイクロセグメンテーションの設定

ステップ 1 （オプション）クラウドベースのワークロードにエージェントをインストールします。

Cloud Connector が提供する VPC/VNet レベルの粒度よりも細かいレベルでポリシーの検出と適用が必要な場合は、サポートされているプラットフォームにエージェントをインストールします。

クラウドサービスが実行されているオペレーティング システムに基づいて、エージェントをインストールします。「ソフトウェアエージェントの展開」を参照してください。

ステップ 2 Cloud Connector を設定して、ラベルとフローデータを収集します。

その場合は、次のトピックを参照してください。

- AWS コネクタ。
- Azure コネクタ。

ステップ 3 コネクタによって作成された範囲のワークスペースを作成します。

「ワークスペース」を参照してください。

ステップ 4 ポリシーを自動的に検出します。

VPC/VNet で定義された範囲ごとに（該当する場合は、より細かい範囲ごとに）ポリシーを検出します。

「自動ポリシー検出」を参照してください。

ステップ 5 提案されたポリシーを確認して分析します。

たとえば、「ライブ分析」を参照してください。

ステップ 6 必要に応じて、ポリシーを繰り返し検出、レビュー、分析します。

「自動ポリシー検出の再実行」を参照してください。

ステップ 7 準備ができたら、各範囲のポリシーを承認して適用します。

該当するワークスペースと各 VPC または VNet のコネクタ、および/または個々のワークロードにインストールされているエージェントの適用を有効にする必要があります。

- AWS ベースのワークロードについては、「AWS インベントリにセグメンテーションポリシーを適用するときのベストプラクティス」を参照してください。
- Azure ベースのワークロードについては、「Azure インベントリにセグメンテーションポリシーを適用するときのベストプラクティス」を参照してください。

Kubernetes ベースのワークロードに対するマイクロセグメンテーションの設定

ステップ 1 Kubernetes ベースのワークロードにエージェントをインストールします。

要件および前提条件を確認してください。

「Kubernetes/Openshift エージェント：優れた可視性と適用」を参照してください。

エージェントは、該当する Kubernetes サービスによって管理される将来のすべてのワークロードに自動的にインストールされます。

ステップ 2 Kubernetes ベースのワークロードのラベルを収集します。

Kubernetes の展開に応じて、以下を参照してください。

- （シンプルな Kubernetes およびオープンソースワークロードの場合）Kubernetes 外部オーケストレータ。
- AWS で実行されるマネージド Kubernetes サービスの Cloud Connector。
- Azure Kubernetes Services（AKS）の Cloud Connector。
- GCP（GKE）で実行されるマネージド Kubernetes サービス のC loud Connector。

ステップ 3 ラベルに基づいて範囲ツリーを作成します。

「範囲とインベントリ」を参照してください。

ステップ 4 ポリシーを適用する範囲ごとにワークスペースを作成します。

「ワークスペース」を参照してください。

ステップ 5 各低レベル範囲のポリシーを自動的に検出します。

「自動ポリシー検出」を参照してください。

ステップ 6 提案されたポリシーを確認して分析します。

たとえば、「ライブ分析」を参照してください。

ステップ 7 必要に応じて、ポリシーを繰り返し検出、レビュー、分析します。

「自動ポリシー検出の再実行」を参照してください。

ステップ 8 準備ができたら、各範囲のポリシーを承認して適用します。

ワークスペースとエージェントでポリシーの適用を有効にする必要があります。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。