ゲートウェイプロファイル

ゲートウェイプロファイルは通常、ネットワークゲートウェイの設定に関連付けられます。これは、異なるネットワークに接続し、それらの間でトラフィックをルーティングするデバイスによって行われます。ゲートウェイプロファイルは、ネットワークゲートウェイの動作と機能を管理するために使用され、ネットワークのさまざまな部分の間の効率的で安全な通信を保証します。通常、これらのプロファイルには、次の保護対策が含まれているか、適用されます。

- ルーティング ポリシー
- Network Address Translation（NAT）
- 仮想プライベートネットワーク（VPN）設定
- Quality of Service（QoS）
- 認証とアクセス制御

これらのプロファイルは通常、Multicloud Defense Gateway、またはゲートウェイに関連付けられている VPN トンネルに適用されます。

- パケット キャプチャ プロファイル （1 ページ）
- ログ転送プロファイル （2 ページ）
- ゲートウェイメトリック転送プロファイル （4 ページ）
- ネットワーク タイム プロトコル プロファイル （6 ページ）
- IPSec プロファイル （7 ページ）
- BGP プロファイル （8 ページ）

パケット キャプチャ プロファイル

パケットキャプチャ（PCAP）は、ネットワークを介して送信されるデータパケットをキャプチャし、ネットワークトラフィックの詳細な分析を可能にします。PCAP を使用すると、キャプチャされたパケットを分析して、悪意のあるアクティビティの兆候がないかネットワークトラフィックをモニターできます。セキュリティシステムは、潜在的な脅威をリアルタイムで検出して対応し、インシデントにつながる一連のイベントを再構築し、攻撃の発生源と性質を特

定できます。この情報は、タイムラインの診断や、接続の問題、遅延、パケット損失などのイベントのトラブルシューティングに役立ちます。

新しいパケット キャプチャ プロファイルの作成

パケット キャプチャ プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）]** > **[プロファイル（Profiles）]** > **[パケットキャプチャ（Packet Capture）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 一意の [名前（Name）] を指定します。

ステップ 4 （任意）[説明（Description）]に説明を入力します。これは、似た名前の他のプロファイルを区別するのに役立ちます。

ステップ 5 [CSPアカウント（CSP Account）] を指定します。

ステップ 6 クラウドサービスプロバイダーのタイプによって、ストレージバケットのパラメータが決定される場合があります。次に示すクラウド サービス プロバイダーごとの要件に注意してください。

- **AWS**：S3 バケット。
- **Azure**：ストレージアカウント名、ブログコンテナ、およびストレージアクセスキー。
- **GCP**：ストレージバケット。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

ログ転送プロファイル

ログ転送プロファイルを使用すると、ゲートウェイ、VPC、および VNet ログのコレクションをサードパーティに送信できます。Multicloud Defense および選択したサードパーティの間の通信には、転送する必要があるログタイプと、ログを送信する宛先サーバープロファイルが含まれます。単一のプロファイル、または複数のエンドポイントに同時にログを送信するプロファイルグループを設定できます。

このプロファイルにはメトリックは含まれないことに注意してください。ログメトリックの転送に関する詳細については、ゲートウェイメトリック転送プロファイル （4 ページ）を参照してください。

スタンドアロンログ転送プロファイルの作成

ログを転送するスタンドアロンプロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [ログ転送（Log Forwarding）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）] に一意のプロファイル名を入力します。

ステップ 4 （任意）[説明（Description）] に説明を入力します。これは、同様の名前を持つ他のプロファイルと区別する場合に役立ちます。

ステップ 5 [タイプ（Type）] ドロップダウンメニューを展開し、[スタンドアロン（Standalone）] を選択します。

ステップ 6 [宛先（Destination）] ドロップダウンメニューを展開し、ログの送信先となるサードパーティ アプリケーションを選択します。

ステップ 7 ステップ 6 で選択した宛先のタイプに基づいて、プロンプトが表示されたら、ログを転送する最終エンドポイントを保護するための適切な情報を入力します。宛先のタイプによっては、すべてのオプションを使用できるわけではないことに注意してください。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

ログ転送グループの作成

ログを転送するプロファイルグループを作成するには、次の手順を実行します。

始める前に

- このプロファイルを作成する前に、メトリックの転送先となるサードパーティ アプリケーションを少なくとも 1 つ用意してください。
- 少なくとも 2 つのスタンドアロンメトリック転送プロファイルを作成しておく必要があります。詳細については、スタンドアロンログ転送プロファイルの作成 （3 ページ）を参照してください。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [ログ転送（Log Forwarding）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）] に一意のプロファイル名を入力します。

ステップ 4 （任意）[説明（Description）] に説明を入力します。これは、同様の名前を持つ他のプロファイルと区別する場合に役立ちます。

ステップ 5 [タイプ（Type）] ドロップダウンメニューを展開し、[グループ（Group）] を選択します。

ステップ 6 [グループの詳細（Group Details）] で、プロファイルに追加する必要がある新しい行ごとに [追加（Add）] をクリックします。

ステップ 7 各行のドロップダウンメニューを展開して、グループに追加するプロファイルを選択します。保存する前に、任意の時点でプロファイルを削除する場合は、プロファイルのチェックボックスをオンにして強調表示してから、[削除（Remove）] を選択します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

ゲートウェイメトリック転送プロファイル

このプロファイルは、データのモニタリングと分析のために Multicloud Defense Gateway によって生成されたゲートウェイメトリックを転送することを目的としています。メトリックはゲートウェイによって生成されますが、メトリックをサードパーティの分析アプリケーションに転送するのは Multicloud Defense Controller です。この転送プロファイルを使用すると、Multicloud Defense にログインせずにゲートウェイメトリックをモニター、分析、および整理できます。この情報を使用してゲートウェイ環境のパフォーマンスと動作を評価できます。この情報は環境のトラブルシューティングにも利用できます。

（注） Multicloud Defense Controller バージョン 23.09 の時点では、Datadog のみがサードパーティ分析アプリケーションとしてサポートされています。

Datadog をはじめとする使用可能な分析アプリケーションのほとんどで、ツールの API とレンダリングされたデータにアクセスするには承認ユーザーである必要があります。

スタンドアロンメトリック転送プロファイルの作成

スタンドアロンプロファイルを作成し、メトリックを転送してサードパーティによって処理されるようにするには、次の手順を実行します。

始める前に

このプロファイルを作成する前に、メトリックの転送先となるサードパーティアプリケーションを少なくとも 1 つ用意してください。

手順

ステップ 1 **[管理（Manage）]** > **[プロファイル（Profiles）]** > **[メトリック転送（Metrics Forwarding）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）] に一意のプロファイル名を入力します。

ステップ 4 （任意）[説明（Description）]に説明を入力します。これは、同様の名前を持つ他のプロファイルと区別する場合に役立ちます。

ステップ 5 [タイプ（Type）] ドロップダウンメニューを展開し、[スタンドアロン（Standalone）] を選択します。

ステップ 6 [宛先（Destination）] ドロップダウンメニューを展開し、メトリックを処理して分析するサードパーティアプリケーションを選択します。

ステップ 7 [エンドポイント（Endpoint）]に、メトリックのエンドポイントの場所として使用するエンドポイントを入力します。

ステップ 8 [保存（Save）] をクリックします。

分析アプリケーションとして Datadog を選択した場合、[エンドポイント（Endpoint）] にはデフォルトで HTTPS ウェブフックが入力されます。この入力は、デフォルトで設定されている場合、プロファイルを保存する前に変更できます。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

グループメトリック転送プロファイルの作成

このプロセスでは、プロファイルを作成し、そのプロファイルを特定のゲートウェイに割り当てます。グループプロファイルは、最大5つのスタンドアロンメトリック転送プロファイルを組み合わせたもので、単一のゲートウェイに割り当てることができます。グループ化したメトリック転送プロファイルを作成するには、次の手順を実行します。

始める前に

- このプロファイルを作成する前に、メトリックの転送先となるサードパーティアプリケーションを少なくとも 1 つ用意してください。
- 少なくとも2つのスタンドアロンメトリック転送プロファイルを作成しておく必要があります。詳細については、スタンドアロンメトリック転送プロファイルの作成（4ページ）を参照してください。

手順

ステップ 1 Multicloud Defense Controller インターフェイスで、**[管理（Manage）] > [プロファイル（Profiles）] > [メトリック転送（Metrics Forwarding）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）] に一意のプロファイル名を入力します。

ステップ 4 （任意）[説明（Description）]に説明を入力します。これは、似た名前のプロファイルを区別するのに役立ちます。

ステップ 5 [タイプ（Type）] ドロップダウンメニューを展開し、[グループ（Group）] を選択します。

ステップ 6 [グループの詳細（Group Details）] で、プロファイルに追加する必要がある新しい行ごとに [追加（Add）] をクリックします。

ステップ 7 各行のドロップダウンメニューを展開して、グループに追加するプロファイルを選択します。保存する前に、任意の時点でプロファイルを削除する場合は、プロファイルのチェックボックスをオンにして強調表示してから、[削除（Remove）] を選択します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

ネットワーク タイム プロトコル プロファイル

ネットワーク タイム プロトコルは、電話モデム、ラジオ、および衛星を介してコンピュータのクロックを相互に同期させ、国際標準に同期させます。プロファイルとして、特に分散システム内では、アクションを調整し、分散プロセスがシームレスに連携することを保証するために、時刻が同期されていることが不可欠です。デバイス間で一貫性のある時間は、モニタリングや障害対応などのネットワーク管理タスクに理想的です。これにより、さまざまなデバイスからのログを正確に関連付けることができ、ネットワークのスムーズで安全な運用が保証されます。

プロファイルの作成

NTP プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [NTP]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 一意の [名前（Name）] を指定します。

ステップ 4 （任意）[説明（Description）] に説明を入力します。これは、似た名前の他のプロファイルを区別するのに役立ちます。

ステップ 5 NTP サーバーの [リスト（List）] を指定します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

IPSec プロファイル

仮想トンネルインターフェイスにインターネット プロトコル セキュリティ（IPSec）プロファイルを使用すると、リモートアクセスを保護する必要がある場合の設定プロセスを簡素化できます。IPSec プロファイルには、2 つのサイト間 VPN ピア間をセキュアで論理的な通信パスでつなぐために必要なセキュリティプロトコルとアルゴリズムが含まれています。VPN はネットワーク間、ホスト - ネットワーク間、およびホスト間通信の IPsec トンネルに依存するため、これはトンネルの作成時に必要なコンポーネントです。IPSec プロファイルを使用すると、IKE パラメータと IPSec パラメータの両方を 1 ヵ所で設定して、セキュリティと暗号化保護を強化できます。

サイト間トンネル設定内に IPSec プロファイルを含めることを選択した場合、このプロファイルは、ネットワーク上のポイント間を移動するデータを暗号化および認証することにより、堅牢なネットワークセキュリティを提供するだけでなく、サイト間、クライアント - サイト間、およびクライアント間のトンネルとの互換性という柔軟性も提供します。

IPSec プロファイルの作成

Multicloud Defense Controller ダッシュボードから IPSec プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [IPSec]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）] に一意のプロファイル名を入力します。

ステップ 4 （任意）[説明（Description）] に説明を入力します。これは、同様の名前を持つ他のプロファイルと区別する場合に役立ちます。

ステップ 5 プロンプトで要求されたら、適切な IKE 情報を入力します。

a) [DHグループ（DH Group）]：Diffie-Hellman（DH）グループは、キー交換プロセスで使用されるキーの強度を決定します。ドロップダウンメニューを展開して、プロファイルに適したグループを選択します。

b) [認証（Authentication）]：ドロップダウンメニューを展開して、このトンネルに必要な認証のタイプを選択します。

c) [暗号化（Encryption）]：代行受信されたスタックでは、暗号化と復号が必要です。ドロップダウンメニューを展開して、暗号化の方法を選択します。

d) [ハッシュ（Hash）]：SHA1 は、160 ビットダイジェストを作成する一方向のハッシュアルゴリズムです。ドロップダウンメニューを使用して、適切なオプションを選択します。

e) [キーの有効期間（Key Lifetime）]：キーの存続時間を秒単位で入力します。使用可能な値は 60 ～ 86400 秒です。

f) [IKEバージョン（IKE Version）]：Internet Key Exchange（IKE）は、IP パケットの堅牢な認証と暗号化を提供する IPSec プロトコルスイートでセキュリティ アソシエーションを設定するために使用されるプロトコルです。ドロップダウンメニューを使用して、IKE バージョン 1 またはバージョン 2 を選択します。バージョン間で大きな違いがあるため、ご使用の環境に最も適したバージョンを選択してください。

ステップ 6 プロンプトで要求されたら、適切な IPSec 情報を入力します。

a) [認証（Authentication）]：ドロップダウンメニューを展開して、認証方式（[なし（None）]、[SHA256]、[SHA]、または [ヌル（Null）]）を選択します。

b) [暗号化（Encryption）]：ドロップダウンメニューを展開し、キーのタイプ（AES GCM 256、AES GCM 192、または AES GCM）を選択します。これにより、接続されたデバイス間で一意のキー交換が生成され、各デバイスは他のデバイスのメッセージを復号できるようになります。

c) [モード（Mode）]：ドロップダウンメニューを展開して、IPSec ポリシー認証プロトコルを選択します。複数選択できます。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

BGP プロファイル

ボーダー ゲートウェイ プロトコル（BGP）はインターネット技術特別調査委員会（IETF）の標準規格であり、すべてのルーティングプロトコルの中で最も高い拡張性があります。BGP は、グローバルインターネットおよびサービスプロバイダープライベートネットワークのルーティングプロトコルです。BGP を使用すると、VPN ゲートウェイと BGP ネイバーは、ルートを交換して、関連するゲートウェイまたはルータの可用性を接続の両側のゲートウェイに通知することができます。

別のプラットフォームまたはデバイスへのサイト間 VPN トンネル接続を確立する場合は、BGP プロファイルを作成してゲートウェイに追加することを**強く**お勧めします。BGP プロファイル

を使用して展開すると、ネットワークとクラウドサービスプロバイダー間で BGP を使用したダイナミックルーティングを使用するゲートウェイが展開されます。

BGP プロファイルの作成

Multicloud Defense Controller ダッシュボードから BGP プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [BGP]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）] に一意のプロファイル名を入力します。

ステップ 4 （任意）[説明（Description）] に説明を入力します。これは、同様の名前を持つ他のプロファイルと区別する場合に役立ちます。

ステップ 5 [LocalAS] 値を入力します。この値は、BGP4 デバイスが存在するローカル自律システム（AS）を表します。

ステップ 6 [ネイバーの追加（Add Neighbor）] をクリックして、少なくとも 1 つのピアをプロファイルに追加します。

ステップ 7 [ネイバー（Neighbor）] に関する次の情報を追加します。

a) [IPアドレス（IP Address）]：単一のアドレスまたは IP アドレスの範囲と BGP ピアグループを入力します。複数のアドレスを追加する場合は、各アドレスを**スペース**で区切ります。

b) [自律システム（Autonomous System）]：ネイバーが存在する [LocalAS] を入力します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

BGP プロファイルを Multicloud Defense Gateway に追加します。新しいゲートウェイを作成するか、または既存のゲートウェイを編集して新しいプロファイルを含めることができます。

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。