ネットワーク分析ポリシーの使用を開始するには

ここでは、ネットワーク分析ポリシーの使用を開始する方法について説明します。

ネットワーク分析ポリシーの基本

ネットワーク分析ポリシーは、多数のトラフィックの前処理オプションを制御し、アクセスコントロールポリシーの詳細設定で呼び出されます。ネットワーク分析に関連する前処理は、セキュリティ インテリジェンスによるブラックリスト化や SSL 復号化の後、侵入またはファイル検査の開始前に実行されます。

デフォルトでは、システムは *Balanced Security and Connectivity* ネットワーク分析ポリシーを使用して、アクセス コントロール ポリシーによって処理されるすべてのトラフィックを前処理します。ただし、この前処理を実行するために別のデフォルトのネットワーク分析ポリシーを選択できます。便宜を図るため、システムによっていくつかの変更不可能なネットワーク分析ポリシーが提供されます。これらのポリシーは、Cisco Talos Security Intelligence and Research Group（Talos）によってセキュリティおよび接続の一定のバランスがとれるように調整されています。カスタム前処理設定を使用して、カスタム ネットワーク分析ポリシーを作成することもできます。

ヒント システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。ネットワーク分析ポリシーと侵入ポリシーが連動してトラフィックを検査します。

複数のカスタムネットワーク分析ポリシーを作成し、それらに異なるトラフィックの前処理を割り当てることにより、特定のセキュリティ ゾーン、ネットワーク、VLAN 用に前処理オプションを調整できます。（ただし、ASA FirePOWER VLAN による前処理を制限することはできないことに注意してください）。

ネットワーク分析ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）]**、次に **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックします。 または **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]**、次に **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 ネットワーク分析ポリシーを管理します。

- [比較（Compare）] : [ポリシーの比較（Compare Policies）] をクリックします（ポリシーの比較 を参照）。
- 作成：新しいネットワーク分析ポリシーを作成する場合は、[ポリシーの作成（Create Policy）] をクリックして、カスタム ネットワーク分析ポリシーの作成 （3 ページ）で説明する手順を実行します。
- 削除：ネットワーク分析ポリシーを削除する場合は、削除アイコン（  ）をクリックして、ポリシーの削除を確認します。アクセス コントロール ポリシーが参照しているネットワーク分析ポリシーは削除できません。

  コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 展開：[展開（Deploy）] をクリックします（設定変更の導入 を参照）。

- 編集:既存のネットワーク分析ポリシーを編集する場合は、編集アイコン（）をクリックして、ネットワーク分析ポリシーの設定とキャッシュされた変更 （5 ページ）で説明する手順を実行します。

  代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- [レポート（Report）]：レポート アイコン（）をクリックします（現在のポリシー レポートの生成 を参照）。

カスタム ネットワーク分析ポリシーの作成

新しいネットワーク分析ポリシーを作成するときは、一意の名前を付け、基本ポリシーを指定し、インライン モードを選択する必要があります。

基本ポリシーはネットワーク分析ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

ネットワーク分析ポリシーのインライン モードでは、プリプロセッサでトラフィックを変更（正規化）したりドロップしたりして、攻撃者が検出を回避する可能性を最小限にすることができます。パッシブな展開では、インライン モードに関係なく、システムはトラフィック フローに影響を与えることができないことに注意してください。

関連トピック

基本レイヤ
インライン導入でのプリプロセッサによるトラフィックの変更 （8 ページ）
カスタム ネットワーク分析ポリシーの作成 （3 ページ）
ネットワーク分析ポリシーの編集 （6 ページ）

カスタム ネットワーク分析ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）]**、次に **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックします。 または **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]**、次に **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。別のポリシー内に未保存の変更が存在する場合は、[ネットワーク分析ポリシー（Network Analysis Policy）] ページに戻るかどうか尋ねられたときに [キャンセル（Cancel）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力します。

マルチドメイン展開では、ポリシー名をドメイン階層内で一意にする必要があります。システムは、現在のドメインでは表示できないポリシーの名前との競合を特定することができます。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 [基本ポリシー（Base Policy）] で最初の基本ポリシーを選択します。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

ステップ 6 プリプロセッサがインライン導入でのトラフィックに影響するようにする場合は、[インライン モード（Inline Mode）] を有効化します。

ステップ 7 ポリシーを作成します。

- 新しいポリシーを作成して [ネットワーク分析ポリシー（Network Analysis Policy）] ページに戻るには、[ポリシーの作成（Create Policy）] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度なネットワーク分析ポリシーエディタでそれを開いて編集するには、[ポリシーの作成と編集（Create and Edit Policy）] をクリックします。

関連トピック

カスタム ユーザ ロールの作成

ネットワーク分析ポリシーの管理

[ネットワーク分析ポリシー（Network Analysis Policy）] ページ（**[ポリシー（Policies）] > [アクセス コントロール（Access Control）]**、次に **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックします。、または**[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]**、次に **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックします。）で、現在のカスタム ネットワーク分析ポリシーを次の情報とともに確認できます。

- ポリシーが最後に変更された日時（ローカル時間）とそれを変更したユーザ

- プリプロセッサがトラフィックに影響を与えることを許可する [インライン モード（Inline Mode）] 設定が有効になっているかどうか
- トラフィックを前処理するためにアクセス コントロール ポリシーおよびデバイスがどのネットワーク分析ポリシーを使用しているか
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人（いれば）に関する情報

お客様が独自に作成するカスタム ポリシーに加えて、システムは初期インライン ポリシーと初期パッシブ ポリシーの2つのカスタム ポリシーを提供しています。これら2つのネットワーク分析ポリシーは、ベースとして「Balanced Security and Connectivity」ネットワーク分析ポリシーを使用します。両者の唯一の相違点はインライン モードです。インライン ポリシーではプリプロセッサによるトラフィックの影響が有効化され、パッシブ ポリシーでは無効化されています。これらのシステム付属のカスタム ポリシーは編集して使用できます。

ただし、Firepowerシステムのユーザアカウントの権限が侵入ポリシーまたは修正侵入ポリシーに限定されている場合は、ネットワーク分析ポリシーに加えて、侵入ポリシーを作成して編集できます。

関連トピック

カスタム ネットワーク分析ポリシーの作成 （3 ページ）
ネットワーク分析ポリシーの編集 （6 ページ）

ネットワーク分析ポリシーの設定とキャッシュされた変更

新しいネットワーク分析ポリシーを作成すると、そのポリシーには基本ポリシーと同じ設定が付与されます。

ネットワーク分析ポリシーの調整時、特にプリプロセッサを無効化するときは、プリプロセッサおよび侵入ルールによっては、トラフィックを特定の方法で最初にデコードまたは前処理する必要があることに留意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーのWebインターフェイスではプリプロセッサは無効のままになります。

（注） 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。

システムは、ユーザごとに1つのネットワーク分析ポリシーをキャッシュします。ネットワーク分析ポリシーの編集中に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。

関連トピック

ポリシーが侵入についてトラフィックを検査する仕組み
カスタム ポリシーの制限

ネットワーク分析ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）]**、次に **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックします。 または **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]**、次に **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックします。 を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 設定するネットワーク分析ポリシーの横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ネットワーク分析ポリシーを編集します。

- 基本ポリシーの変更：基本ポリシーを変更するには、[ポリシー情報（Policy Information）] ページの [基本ポリシー（Base Policy）] ドロップダウン リストから、ポリシーを選択します。
- ポリシー階層の管理：ポリシー階層を管理するには、ナビゲーション パネルで [ポリシー層（Policy Layers）] をクリックします。
- プリプロセッサの変更：プリプロセッサの設定有効または無効にするか、あるいは編集するには、ナビゲーション パネルで [設定（Settings）] をクリックします。
- トラフィックの変更：プリプロセッサがトラフィックを変更またはドロップできるようにするには、[ポリシー情報（Policy Information）] ページで [インライン モード（Inline Mode）] チェックボックスをオンにします。
- 設定の表示：基本ポリシーの設定を表示するには、[ポリシー情報（Policy Information）] ページで [基本ポリシーの管理（Manage Base Policy）] をクリックします。

ステップ 4 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] を選択して、[変更を確定（Commit Changes）] をクリックします。変更を確定せ

ずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- プリプロセッサでイベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、プリプロセッサのルールを有効にします。詳細については、侵入ルール状態の設定を参照してください。
- 設定変更を展開します。設定変更の導入を参照してください。

関連トピック

基本レイヤ
ベースポリシーの変更
ネットワーク分析ポリシーでのプリプロセッサの設定 （7 ページ）
インライン導入でのプリプロセッサによるトラフィックの変更 （8 ページ）
レイヤの管理
競合と変更：ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーでのプリプロセッサの設定

プリプロセッサは、トラフィックを正規化し、プロトコルの異常を識別することで、トラフィックの詳細な検査に備えます。プリプロセッサは、ユーザが設定したプリプロセッサ オプションをパケットがトリガーしたときに、プリプロセッサ イベントを生成できます。デフォルトで有効になるプリプロセッサや、それぞれのデフォルト設定は、ネットワーク分析ポリシーの基本ポリシーに応じて決まります。

（注） 多くの場合、プリプロセッサの設定には特定の専門知識が必要で、通常は、ほとんどあるいはまったく変更を必要としません。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。

プリプロセッサの設定を変更するには、その設定とネットワークへの潜在的影響を理解する必要があります。

トランスポート/ネットワーク プリプロセッサの詳細設定は、アクセス コントロール ポリシーを展開するすべてのネットワーク、ゾーン、VLANにグローバルに適用されることに注意してください。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

また、侵入ポリシーではASCIIテキストのクレジット カード番号や社会保障番号などの機密データを検出する機密データ プリプロセッサを設定することにも注意してください。

関連トピック

- DCE/RPC プリプロセッサ
- DNP3 プリプロセッサ
- DNS プリプロセッサ
- FTP/Telnet デコーダ
- GTP プリプロセッサ
- HTTP Inspect プリプロセッサ
- IMAP プリプロセッサ
- インライン正規化プリプロセッサ
- IP 最適化プリプロセッサ
- Modbus プリプロセッサ
- パケット デコーダ
- POP プリプロセッサ
- 機密データ検出の基本
- SIP プリプロセッサ
- SMTP プリプロセッサ
- SSH プリプロセッサ
- SSL プリプロセッサ
- Sun RPC プリプロセッサ
- TCP ストリームの前処理
- UDP ストリームの前処理
- カスタム ポリシーの制限

インライン導入でのプリプロセッサによるトラフィックの変更

インライン導入（つまり、ルーテッド インターフェイス、スイッチド インターフェイス、トランスペアレント インターフェイス、あるいはインライン インターフェイスのペアを使用して関連する設定をデバイスに展開する導入）では、一部のプリプロセッサがトラフィックを変更およびブロックできます。次に例を示します。

- インライン正規化プリプロセッサは、パケットを正規化し、他のプリプロセッサおよび侵入ルールエンジンで分析されるようにパケットを準備します。ユーザは、プリプロセッサの [これらの TCP オプションを許可（Allow These TCP Options）] と [回復不能な TCP ヘッダーの異常をブロック（Block Unresolvable TCP Header Anomalies）] オプションを使用して、特定のパケットをブロックすることもできます。
- システムは無効なチェックサムを持つパケットをドロップできます。
- システムはレート ベースの攻撃防御設定に一致するパケットをドロップできます。

ネットワーク分析ポリシーに設定したプリプロセッサがトラフィックに影響を与えるようにするには、プリプロセッサを有効にして正しく設定するとともに、管理対象デバイスをインラインで正しく展開する必要があります。最後に、ネットワーク分析ポリシーの [インライン モード（Inline Mode）] 設定を有効にする必要があります。

ネットワーク分析ポリシーの注記におけるプリプロセッサの設定

ネットワーク分析ポリシーのナビゲーション パネルで [設定（Settings）] を選択すると、ポリシーによりタイプ別のプリプロセッサがリストされます。[設定（Settings）]ページで、ネットワーク分析ポリシーのプリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。

プリプロセッサを設定するには、それを有効にする必要があります。プリプロセッサを有効にすると、そのプリプロセッサに関する設定ページへのサブリンクがナビゲーション パネル内の [設定（Settings）] リンクの下に表示され、この設定ページへの [編集（Edit）] リンクが [設定（Settings）] ページのプリプロセッサの横に表示されます。

ヒント　プリプロセッサの設定を基本ポリシーの設定に戻すには、プリプロセッサ設定ページで[デフォルトに戻す（Revert to Defaults）] をクリックします。プロンプトが表示されたら、復元することを確認します。

プリプロセッサを無効にすると、サブリンクと [編集（Edit）] リンクは表示されなくなりますが、設定は保持されます。特定の分析を実行するには、多くのプリプロセッサおよび侵入ルールで、トラフィックをまず特定の方法でデコードまたは前処理する必要があることに注意してください。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

実際にトラフィックを変更せずに、設定がインライン展開でどのように機能するかを評価する場合は、インライン モードを無効にできます。タップ モードでのパッシブ展開またはインライン展開では、インライン モード設定に関係なくシステムがトラフィックに影響を及ぼすことはありません。

（注）　インライン モードを無効にすることで、侵入イベントのパフォーマンス統計グラフに影響を及ぼす可能性があります。インライン展開でインライン モードが有効の場合、侵入イベント パフォーマンス ページ（**[概要（Overview）]** > **[概要（Summary）]** > **[侵入イベント パフォーマンス（Intrusion Event Performance）]**）には、正規化し、ブロックされたパケットを示すグラフが表示されます。インライン モードが無効の場合、またはパッシブ展開である場合、多くのグラフによりシステムが正規化するか、またはドロップするトラフィックに関するデータが表示されます。

（注）　インライン展開では、インライン モードを有効にし、[TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にして、インライン正規化プリプロセッサを設定することをお勧めします。パッシブ展開では、アダプティブ プロファイルの更新を使用することをお勧めします。

関連トピック

トランスポート/ネットワーク プリプロセッサの詳細設定
チェックサム検証
インライン正規化プリプロセッサ
侵入イベントのパフォーマンス統計情報グラフの種類