特定の脅威の検出

次のトピックでは、特定の脅威を検出するためにネットワーク分析ポリシーでプリプロセッサを使用する方法について説明します。

特定の脅威の検出の概要

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

ネットワーク分析ポリシーでさまざまなプリプロセッサを使用して、モニター対象ネットワークへの特定の攻撃、たとえば、Back Orifice 攻撃、複数のポートスキャン タイプ、過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃などを検出できます。プリプロセッサに固有の GID 署名が有効になっている場合、Web 上のネットワーク分析ポリシーは無効と表示されます。ただし、プリプロセッサは、使用可能なデフォルト設定を使用しているデバイスでオンになります。

侵入ポリシーで設定する機密データ検出を使用して、センシティブな数値データの保護なし送信を検出することもできます。

特定の脅威の検出のライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

特定の脅威の検出の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

Back Orifice の検出

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

Firepower システムは、Back Orifice プログラムの存在を検出するプリプロセッサを提供しています。Back Orifice プログラムにより Windows ホストに対する管理者アクセス権を取得される可能性があります。

Back Orifice 検出プリプロセッサ

Back Orifice プリプロセッサは、UDP トラフィックを分析し、Back Orifice マジック クッキー「`*!*QWTY?`」を調べます。このクッキーは、パケットの最初の 8 バイトにあり、XOR で暗号化されています。

Back Orifice プリプロセッサには設定ページがありますが、設定オプションはありません。Back Orifice プリプロセッサが有効になっていても、プリプロセッサ ルールを有効にしなければ、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。。

表 *1 : Back Orifice GID:SID*

プリプロセッサ ルール **GID:SID**	説明
105:1	Back Orifice トラフィック検出
105:2	Back Orifice クライアント トラフィック検出
105:3	Back Orifice サーバー トラフィック検出
105:4	Back Orifice Snort バッファ攻撃検出

Back Orifice の検出

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（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 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 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 4 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [特定の脅威の検出（Specific Threat Detection）] の下の [Back Orifice の検出（Back Orifice Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

（注）
Back Orifice にユーザーが設定できるオプションはありません。

ステップ 6 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）] をクリックして、[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

- 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、Back Orifice 検出ルール 105:1、105:2、105:3、または 105:4 を有効にします。詳細については、「侵入ルールの状態」および「Back Orifice 検出プリプロセッサ （2 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開を参照してください。

ポートスキャン検出

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

ポートスキャンとは、攻撃者が攻撃の準備段階としてよく使用する、ネットワーク調査の形式です。ポートスキャンでは、攻撃者が特別に細工したパケットをターゲットホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーションプロトコルが実行されているかを、直接あるいは推論によって判断できます。

ポートスキャンは、それ自体では攻撃の証拠になりません。実際、攻撃者が使用するポートスキャン手法の中には、正当なユーザーがネットワークで使用する可能性があるものもあります。Cisco のポートスキャン ディテクタは、アクティビティのパターンを検出するという方法で、悪意のあるポートスキャンの可能性があるポートスキャンを判別できるように設計されています。

注目 内部リソースのデバイスの負荷分散試験。ポートスキャン検出が期待どおりに機能しない場合は、感度レベルを [高（High）] に設定する必要がある場合があります。

Snort 3 にアップグレードし、バージョン 7.2.0 で導入されたポートスキャン機能を使用することを強く推奨します。詳細については、Cisco Secure Firewall Management Center Snort 3 Configuration GuideおよびSnort 3 インスペクタリファレンスを参照してください。

ポートスキャン タイプ、プロトコル、フィルタリング感度レベル

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

攻撃者がネットワークを調査するために複数の手法を使用することはよくあります。通常、攻撃者は異なる複数のプロトコルを使用して、ターゲットホストからさまざまな応答を引き出します。その目的は、ブロックされた特定タイプのプロトコルを基に、使用できる可能性のあるプロトコルを絞り込んでいくことです。

表 *2:* プロトコル タイプ

プロトコル	説明
TCP	TCP プローブを検出します。たとえば、SYN スキャン、ACK スキャン、TCP connect() スキャン、およびXmas tree、FIN、NULL といった異常なフラグを組み合わせたスキャンなどです。
UDP	UDP プローブを検出します。たとえば、ゼロ バイトの UDP パケットなどです。
ICMP	ICMP エコー要求（ping）を検出します。
IP	IP プロトコル スキャンを検出します。これらのスキャンは、攻撃者が開いているポートを見つけようとしているのではなく、ターゲットホストでサポートされている IP プロトコルを発見しようとするためのスキャンであるため、TCP スキャンおよびUDP スキャンとは異なります。

一般に、ターゲットホストの数、スキャン側ホストの数、およびスキャン対象のポートの数に応じて、ポートスキャンは 4 つのタイプに分けられます。

表 *3:* ポートスキャン タイプ

タイプ	説明
ポート スキャン検出	1 対 1 のポートスキャン。攻撃者が 1 つまたは少数のホストを使用して、単一のターゲット ホスト上の複数のポートをスキャンする場合です。 1 対 1 の ポートスキャンには次のような特徴があります。 • 少数のホストを使用してスキャン • 単一のホストをスキャン • 多数のポートをスキャン このオプションでは、TCP、UDP、および IP ポートスキャンが検出されます。
ポートスイープ	攻撃者が少数のホストを使用して、複数の対象ホスト上で 1 つのポートをスキャンする 1 対複数のポートスイープ。 ポートスイープには次のような特徴があります。 • 少数のホストを使用してスキャン • 多数のホストをスキャン • 少数の固有のポートをスキャン このオプションでは、TCP、UDP、ICMP、および IP ポートスイープが検出されます。
デコイ ポートスキャン	攻撃者がスプーフィングされた送信元 IP アドレスと実際にスキャンされた IP アドレスとを組み合わせた 1 対 1 ポートスキャン。 デコイ ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 少数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン デコイ ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。

タイプ	説明
分散型ポートスキャン	複数のホストが開いているポストに対して 1 つのホストをクエリする複数対 1 のポートスキャン。 分散型ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 多数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン 分散型ポートスキャン オプションでは、TCP、UDP、および IP プロトコル ポートスキャンが検出されます。

ポートスキャンディテクタは、主にプローブ対象ホストからの否定応答に基づいて、プローブに関する情報を取得します。たとえば、Web クライアントが Web サーバーに接続するときに、クライアントはサーバーのポート 80/tcp が開いていることを頼りに、そのポートを使用します。ただし、攻撃者がサーバーをプローブする場合、そのサーバーがウェブ サービスを提供するかどうかを攻撃者があらかじめ知っていることはありません。ポートスキャンディテクタは否定応答（つまり、ICMP 到達不能または TCP RST パケット）を見つけると、その応答を潜在的ポートスキャンとして記録します。否定応答をフィルタリングするデバイス（ファイアウォールやルータなど）の向こう側にターゲット ホストがある場合、このプロセスはさらに困難になります。この場合、ポートスキャンディテクタは、選択された機密レベルに基づいてフィルタリングされた ポートスキャン イベントを生成することができます。

表 *4*: 感度レベル

レベル	説明
Low	ターゲット ホストからの否定応答だけが検出されます。誤検出を抑えるためには、この機密レベルを選択します。ただし、特定のタイプのポートスキャン（時間をかけたスキャン、フィルタリングされたスキャン）が見逃される可能性があることに注意してください。 このレベルを使用すると、ポートスキャン検出の所要時間が最短になります。
Medium	ホストへの接続数に基づいてポートスキャンが検出されます。したがって、フィルタリングされたポートスキャンを検出できます。ただし、ネットワーク アドレス変換プログラムやプロキシなど、ホストが非常にアクティブな場合は、誤検出が発生する可能性があります。 [Ignore Scanned] フィールドにアクティブなホストの IP アドレスを追加すると、そのような誤検出を軽減できます。 このレベルを使用すると、ポートスキャン検出の所要時間が長くなります。

レベル	説明
High	期間に基づいてポートスキャンが検出されます。したがって、時間ベースのポートスキャンを検出できます。ただし、このオプションを使用する場合は、[スキャン済みの無視（Ignore Scanned）] および [スキャナの無視（Ignore Scanner）] フィールドに IP アドレスを指定するという方法で、時間をかけて慎重にディテクタを調整してください。 このレベルを使用すると、ポートスキャン検出の所要時間が大幅に長くなります。

ポートスキャン イベント生成

ポートスキャン検出が有効の場合、さまざまなポートスキャンおよびポートスイープを検出するには、ジェネレータ ID（GID）122 および SID 1 ～ 27 の [Snort ID]（SID）によりルールを有効にする必要があります。

（注） イベントがポートスキャン接続ディテクタによって生成された場合、プロトコル番号は255に設定されます。デフォルトでは、ポートスキャンに特定のプロトコルは関連付けられません。したがって、インターネット割り当て番号局（IANA）にはプロトコル番号が割り当てられません。IANA では 255 を予約番号として指定しているため、ポートスキャン イベントでは、そのイベントに関連付けられている番号がないことを示すために、この番号が使用されます。

表 *5*：ポートスキャン検出 *SID*（*GID 122*）

ポートスキャン タイプ	プロトコル	機密レベル	プリプロセッサ ルール SID
ポート スキャン検出	TCP	Low	1
	UDP	Medium または High	5
	ICMP	Low	21
	IP	Medium または High	イベントを生成しません。
		Low	イベントを生成しません。
		Medium または High	9
		Low	13
		Medium または High	

ポートスキャン タイプ	プロトコル	機密レベル	プリプロセッサ ルール SID
ポートスイープ	TCP UDP ICMP IP	Low Medium または High Low Medium または High Low Medium または High Low Medium または High	3、27 7 19 23 25 26 11 15
デコイ ポートスキャン	TCP UDP ICMP IP	Low Medium または High Low Medium または High Low Medium または High Low Medium または High	2 6 22 イベントを生成しません。 イベントを生成しません。 10 14
分散型ポートスキャン	TCP UDP ICMP IP	Low Medium または High Low Medium または High Low Medium または High Low Medium または High	4 8 20 24 イベントを生成しません。 イベントを生成しません。 12 16

ポートスキャン イベント パケット ビュー

関連するプリプロセッサ ルールを有効にすると、ポートスキャン ディテクタによって侵入イベントが生成されるようになります。生成されたイベントは、他のすべての侵入イベントと同じように表示できます。ただし、ポートスキャン イベントのパケット ビューに表示される情報は、他のタイプの侵入イベントとは異なります。

侵入イベント ビューを出発点に、ポートスキャン イベントのパケット ビューまでドリルダウンします。各ポートスキャンイベントは複数のパケットに基づくため、単一のポートスキャンパケットをダウンロードすることはできません。ただし、ポートスキャンパケットビューで、使用可能なすべてのパケット情報を確認できます。

任意の IP アドレスをクリックしてコンテキスト メニューを表示し、[whois（whois）] を選択して、そのIPアドレスでルックアップを実行するか、[ホストプロファイルの表示（View Host Profile）] を選択して、そのホストのホスト プロファイルを表示できます。

表 *6:* ポートスキャン パケット ビュー

情報	説明
デバイス	イベントを検出したデバイス。
時刻（Time）	イベントが発生した時刻。
Message	プリプロセッサによって生成されたイベント メッセージ。
送信元 IP	スキャン側ホストの IP アドレス。
Destination IP	スキャンされたホストの IP アドレス。
Priority Count	スキャンされたホストからの否定応答（TCP RST、ICMP 到達不能など）の数。否定応答の数が多ければ多いほど、プライオリティ カウントが高くなります。
Connection Count	ホスト上でアクティブな接続数。この値は、TCP や IP などの接続ベースのスキャンより正確です。
IP カウント	スキャン対象のホストに接続するIPアドレスが変更された回数。たとえば、最初の IP アドレスが 10.1.1.1、2 番目の IP アドレスが 10.1.1.2、 3 番目の IP アドレスが 10.1.1.1 の場合、IP カウントは 3 となります。 プロキシやDNS サーバーなどのアクティブ ホストでは、この数値はそれほど正確ではありません。
Scanner/Scanned IP Range	スキャン対象ホストまたはスキャン側ホスト（スキャンのタイプに依存）の IP アドレスの範囲。ポートスイープの場合、このフィールドにはスキャン対象ホストの IP アドレス範囲が示されます。ポートスキャンの場合は、スキャン側ホストの IP アドレス範囲が示されます。
Port/Proto Couont	TCP および UDP ポートスキャンの場合は、スキャン対象のポートが変更された回数です。たとえば、スキャンされた最初のポートが 80、2 番目のポートが 8080、3 番目のポートが再び 80 の場合、ポート カウントは 3 となります。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストに接続するために使用されたプロトコルが変更された回数です。

情報	説明
Port/Proto Range	TCP および UDP ポートスキャンの場合は、スキャンされたポートの範囲です。 IP プロトコル ポートスキャンの場合は、スキャン対象ホストへの接続試行で使用された IP プロトコル番号の範囲です。
Open Ports	スキャン対象ホストで開かれた TCP ポート。このフィールドは、ポートスキャンで1つ以上の開かれたポートが検出された場合にのみ表示されます。

ポートスキャン検出の設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

ポートスキャン検出の設定オプションを使用して、ポートスキャンディテクタによるスキャンアクティビティのレポート方法を微調整できます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** 見出し > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（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 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） 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 4 [設定（Settings）] をクリックします。

ステップ 5 [特定の脅威検出（Specific Threat Detection）] の下の [ポートスキャン検出（Portscan Detection）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [ポートスキャン検出（Portscan Detection）] の横にある [編集（Edit）]（） をクリックします。

ステップ 7 [プロトコル（Protocol）] フィールドで、有効にするプロトコルを指定します。

（注）
TCP を介してスキャンを検出するには TCP ストリーム処理が有効になっていること、UDP を介してスキャンを検出するには UDP ストリーム処理が有効になっていることを確認する必要があります。

ステップ 8 [スキャンタイプ（Scan Type）] フィールドで、検出するポートスキャンタイプを指定します。

ステップ 9 [重要度レベル（Sensitivity Level）] リストからレベルを選択します。ポートスキャンタイプ、プロトコル、フィルタリング感度レベル （5 ページ）を参照してください。

ステップ 10 特定のホストのポートスキャン アクティビティのサインをモニターする場合は、[IP の監視（Watch IP）] フィールドにホストの IP アドレスを入力します。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。すべてのネットワーク トラフィックを監視するには、フィールドを空白のままにします。

ステップ 11 ホストをスキャナとして無視するには、[スキャナの無視（Ignore Scanners）] フィールドにホストの IP アドレスを入力します。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。

ステップ 12 ホストをスキャンのターゲットとして無視するには、[スキャン対象の無視（Ignore Scanned）] フィールドにホストの IP アドレスを入力します。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。

ヒント
特にアクティブなネットワーク上のホストを示すには、[スキャナの無視（Ignore Scanners）] と [スキャン対象の無視（Ignore Scanned）] を使用します。このホスト リストは、時間経過とともに変更しなければならない場合があります。

ステップ 13 ミッドストリームでピックアップされたセッションのモニタリングを中断するには、[ACK スキャンの検出（Detect Ack Scans）] チェックボックスをオフにします。

（注）
ミッドストリームセッションの検出はACKスキャンの識別に役立ちますが、大量のトラフィックとパケットのドロップが発生するネットワークでは、誤ってイベントが生成される可能性があります。

ステップ 14 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）] をクリックして、[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

- さまざまなポートスキャンおよびポートスイープを検出するためにポートスキャン検出を行う場合は、ルール 122:1 ～ 122:27 を有効にします。詳細については、「侵入ルールの状態」および「ポートスキャン イベント生成 （8 ページ）」を参照してください。
- 設定変更を展開します設定変更の展開を参照してください。

レート ベースの攻撃防御

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

レート ベース攻撃とは、接続の頻度または攻撃を行うための反復試行に依存する攻撃のことです。レート ベースの検出基準を使用することで、レート ベース攻撃が行われていることを検出し、攻撃が発生するごとに対応できます。また、攻撃が収まった後は、通常の検出設定に戻すことができます。

レート ベース フィルタを含めたネットワーク分析ポリシーを設定することで、ネットワーク上のホストを対象とした過剰なアクティビティを検出できます。インライン モードで展開されている管理対象デバイスでこの機能を使用すると、指定の期間だけレートベース攻撃をブロックし、その後イベントだけを生成してトラフィックをドロップしない状態に戻せます。

ネットワークのホストを SYN フラッドから保護するには、SYN 攻撃防止オプションを利用します。一定期間中に認められたパケットの数を基準に、個々のホストまたはネットワーク全体を保護することができます。パッシブ導入のデバイスでは、イベントを生成できます。インライン導入のデバイスでは、不正なパケットをドロップすることもできます。タイムアウト期間の満了時にレート条件に達しなくなっていれば、イベントの生成およびパケットのドロップが停止します。

たとえば、1 つの IP アドレスからの SYN パケットの最大許容数を設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

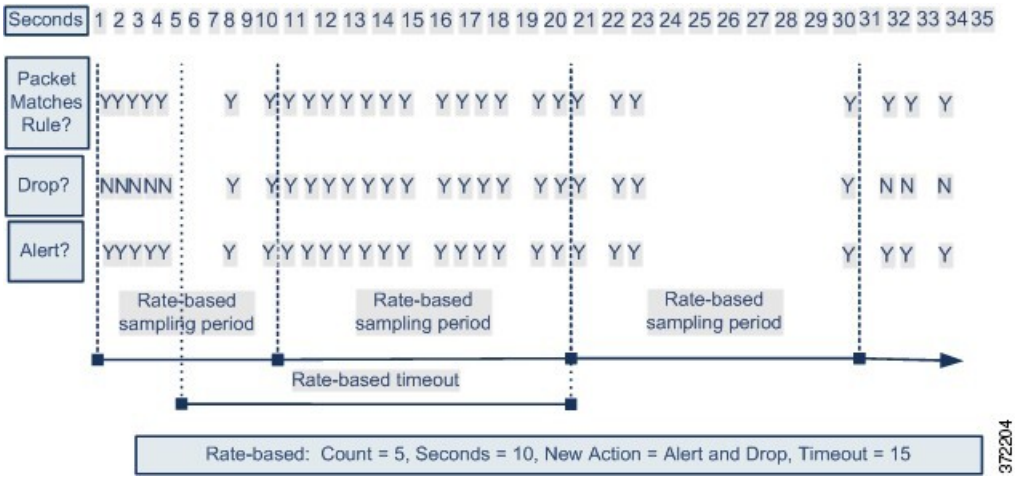
ネットワーク上のホストでの TCP/IP 接続数を制限することで、サービス妨害（DoS）攻撃や、ユーザーによる過剰なアクティビティを防止できます。システムが、指定の IP アドレスまたはアドレス範囲で正常に行われている接続が設定された許容数に達したことを検出すると、以降の接続に対してイベントを生成します。タイムアウト期間が満了するまでは、レート条件に達しなくなっても、レートベースのイベント生成が続行されます。インライン導入では、レート条件がタイムアウトになるまでパケットをドロップするように設定できます。

たとえば、1 つの IP アドレスからの同時接続の最大許容数を 10 に設定し、このしきい値に達すると、その IP アドレスからの以降の接続を 60 秒間ブロックするように設定できます。

（注） デバイスは、内部リソースにインスペクションの負荷を分散させます。レートベースの攻撃防御を設定する際は、デバイスごとではなく、リソースごとのトリガー レートを設定します。レート ベースの攻撃防御が期待どおりに機能しない場合、トリガー レートを下げなければならないことが考えられます。ユーザーにより規定の時間間隔内に送信された接続試行が多すぎると、アラートがトリガーされます。そのため、ルールをレート制限することを推奨します。正しいレートを決定する際に支援が必要な場合は、サポートに連絡してください。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レート ベースの攻撃防御が設定されたルールをトリガーします。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する（Drop and Generate Events）] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値を超えている場合は、新しいアクションが続行されます。新しいアクションが元の「イベントの生成」アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



関連トピック

動的侵入ルール状態

レート ベースの攻撃防御の例

トラフィック自体またはシステムが生成するイベントをフィルタリングする手段としては、`detection_filter` キーワード、しきい値および抑制機能も使用できます。レートベースの攻撃防御は、単独で使用することも、しきい値構成、抑制、または `detection_filter` キーワードと任意に組み合わせて使用することもできます。

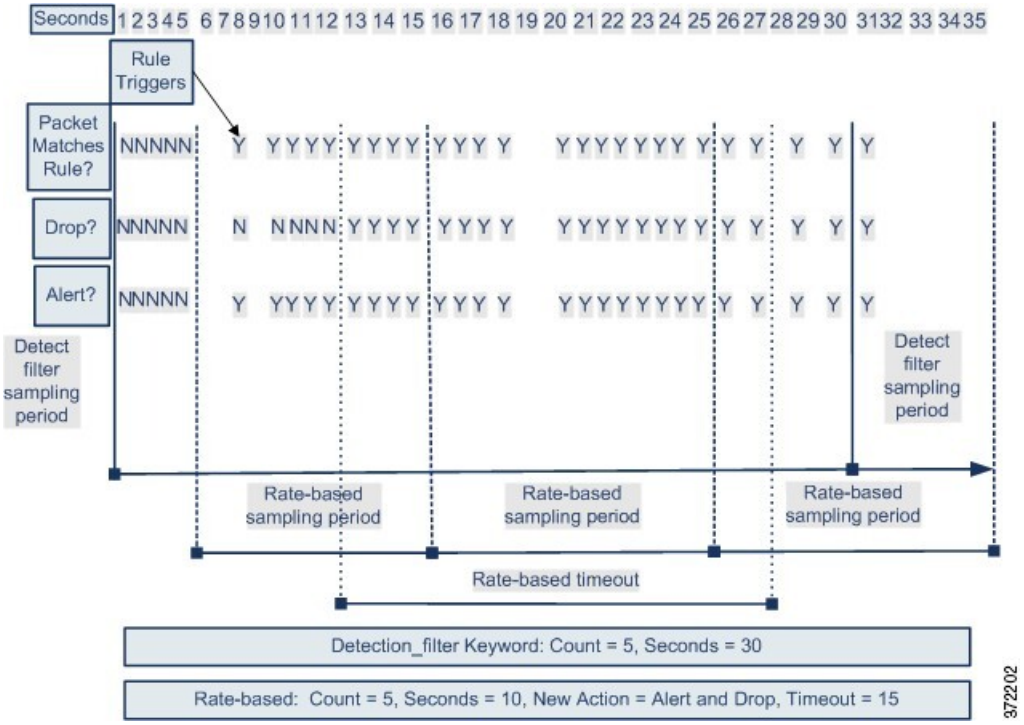
detection_filter キーワード、しきい値構成または抑制、およびレートベースの基準のすべてが同じトラフィックに適用される場合もあります。抑制をルールに適用すると、レートベースの変更が発生しても、指定の IP アドレスに対するイベントの生成は抑制されます。

detection_filter キーワードの例

以下に、攻撃者がブルートフォースログインを仕掛ける例を示します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された detection_filter キーワードも含むルールがトリガーされます。このルールには、レートベース攻撃防止が設定されています。10 秒以内にルールに 5 回ヒットすると、レートベースの設定により、ルール属性が 20 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベントは生成されません。それは、レートが detection_filter キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レートベースの基準によって新しいアクション [ドロップしてイベントを生成する（Drop and Generate Events）] がトリガーされることはありません。

レートベースの基準に一致すると、イベントが生成されて、パケットがドロップされます。これは、レートベースのタイムアウト期間が満了し、かつレートがしきい値未満になるまで続きます。20 秒が経過すると、レートベース アクションがタイムアウトになります。タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。タイムアウトが発生した時点で、サンプリングされたレートは前のサンプリング期間のしきい値レートを超過しているため、レートベースのアクションは続行されます。



この例には示されていませんが、[ドロップしてイベントを生成する（Drop and Generate Events）] ルール状態を `detection_filter` キーワードと組み合わせて使用することで、ルールのヒット数が指定のレートに達するとトラフィックのドロップが開始されるようにすることができることにも注意してください。ルールにレート ベースの設定を使用するかどうかを決定する際は、ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] に設定した場合の結果と `detection_filter` キーワードを含めた場合の結果が同じであるかどうか、あるいは侵入ポリシーでレートとタイムアウトの設定を管理する必要があるかどうかを検討してください。

関連トピック

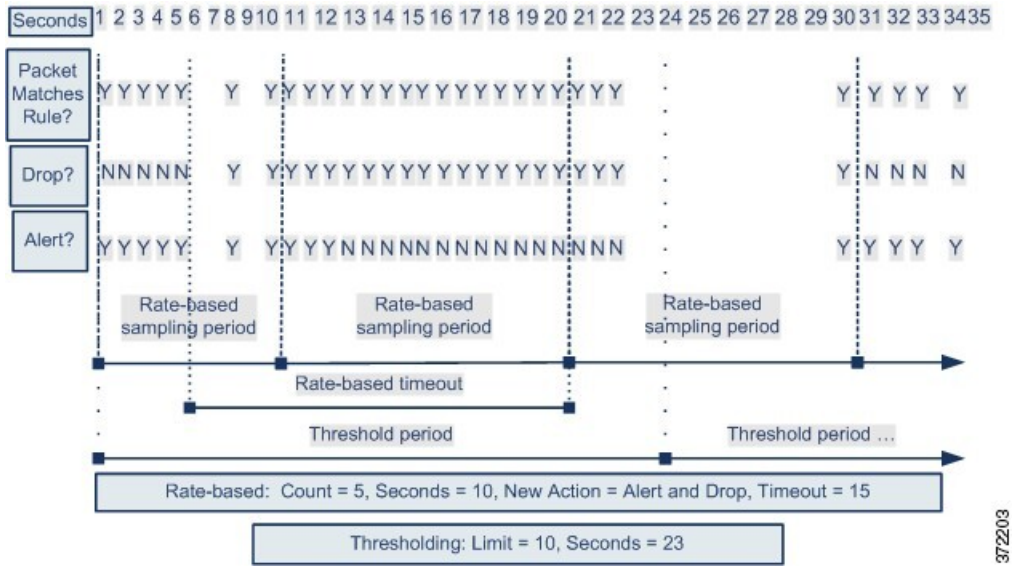
侵入ルールの状態

ダイナミック ルール状態のしきい値構成または抑制の例

以下に、攻撃者がブルート フォース ログインを仕掛ける例を示します。パスワードを特定する試みが繰り返されると、レートベースの攻撃防止が設定されているルールがトリガーされます。10 秒以内にルールに 5 回ヒットすると、レートベースの設定により、ルール属性が 15 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。さらに、上限しきい値により、ルールで生成可能なイベントの数が 23 秒間で 10 に制限されます。

図に示されているように、最初の 5 個のパケットが一致すると、ルールはイベントを生成します。5 個のパケットがルールに一致した後、レートベースの基準が新しいアクションとして [ドロップしてイベントを生成する（Drop and Generate Events）] をトリガーし、次の 5 個のパケットがルールに一致した時点でイベントが生成され、パケットをドロップします。10 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成することなくドロップします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。新しいアクションが元の [Generate Events] アクションに戻されるのは、サンプリング期間の完了時にサンプルリング レートがしきい値を下回っている場合のみです。



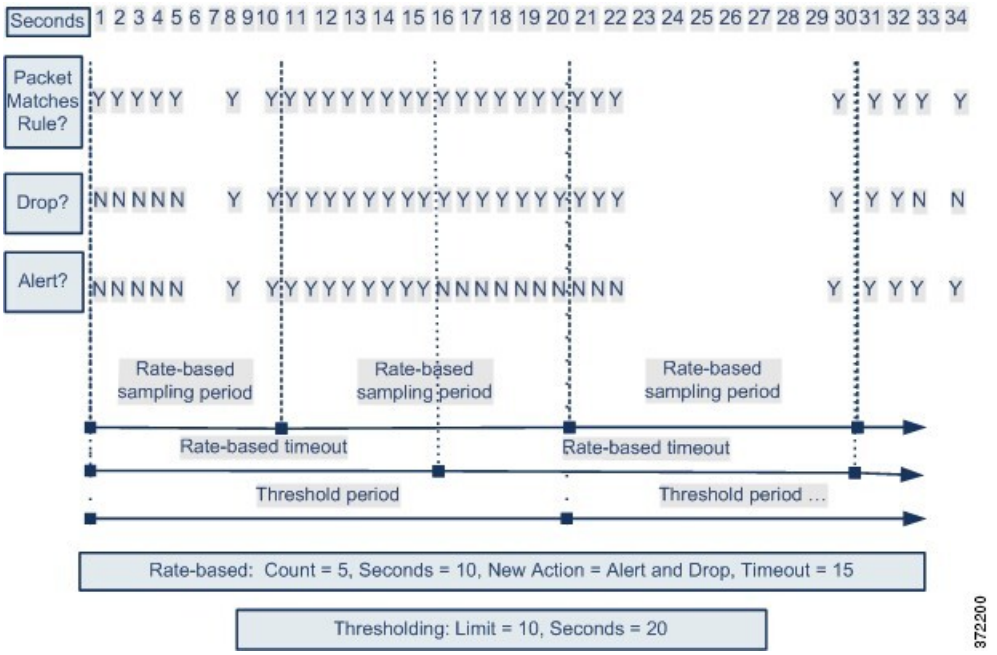
この例には示されていませんが、しきい値に達した後に、レートベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [イベントを生成する（Generate Events）] から [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す11番目のイベントを生成します。

ポリシー全体のレート ベース検出としきい値構成または抑制の例

以下に、ネットワーク上のホストに対して、攻撃者がサービス妨害（DoS）攻撃を仕掛ける例を示します。同じ送信元から多数のホストに対して同時接続が行われると、ポリシー全体の [同時接続の制御（Control Simultaneous Connections）] 設定がトリガーされます。この設定は、1 つの送信元からの接続数が 10 秒間で 5 つに達すると、イベントを生成して悪意のあるトラフィックをドロップします。さらに、グローバル上限しきい値により、ルールまたは設定で生成可能なイベントの数が 20 秒間で 10 件に制限されます。

この図に示されているように、ポリシー全体の設定により、一致する最初の 10 個のパケットに対してイベントが生成され、トラフィックがドロップされます。10個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリングされたレートが、現在または前のサンプリング期間のしきい値レートを超過している場合、レートベースのアクションによるイベントの生成とトラフィックのドロップが続行されます。レート ベース アクションが停止するのは、サンプリング期間が完了した時点で、サンプリングされたレートがしきい値レートを下回っている場合のみです。



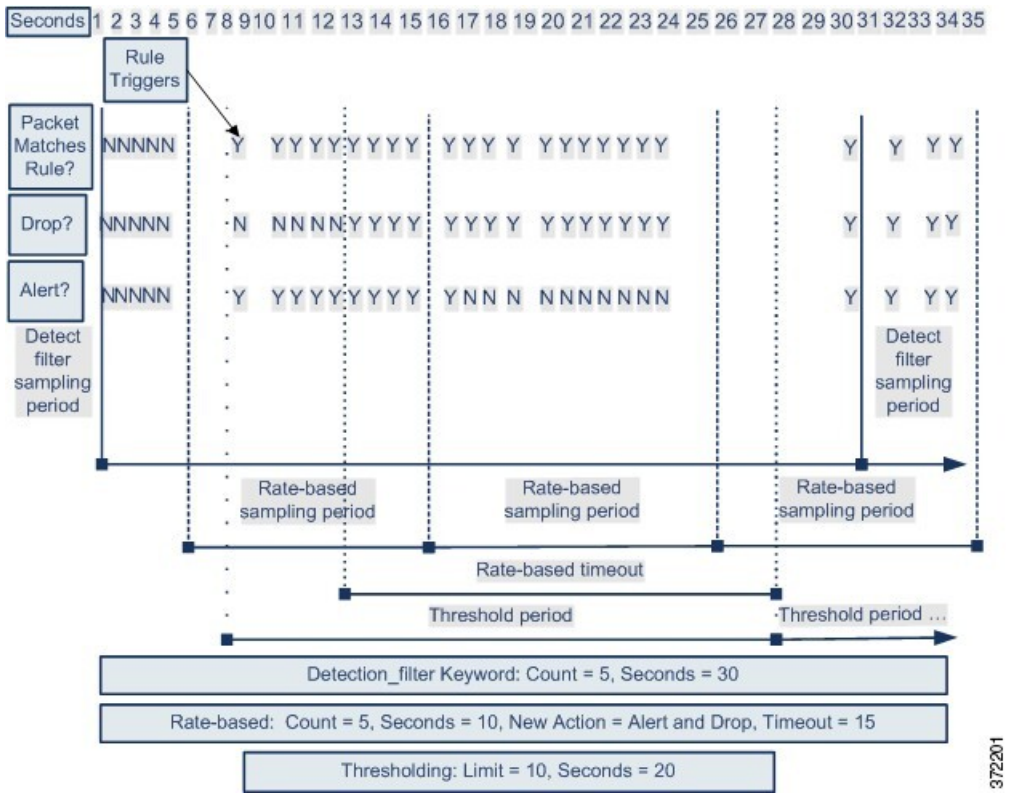
この例には示されていませんが、しきい値に達した後に、レートベースの基準によって新しいアクションがトリガーされた場合、システムはアクションが変更されたことを示す単一のイベントを生成することに注意してください。したがって、たとえば上限しきい値の 10 に達してシステムがイベントの生成を停止し、14 番目のパケットでアクションが [ドロップしてイベントを生成する（Drop and Generate Events）] に変更されると、システムはアクションが変更されたことを示す 11 番目のイベントを生成します。

複数のフィルタリング方法によるレート ベース検出の例

以下に、攻撃者がブルートフォース ログインを仕掛ける例で、`detection_filter` キーワード、レートベースのフィルタリング、およびしきい値が相互作用する場合を説明します。パスワードの検出試行が繰り返されると、カウントが 5 に設定された `detection_filter` キーワードを含むルールがトリガーされます。このルールには、レート ベースの攻撃防御も設定されています。その設定では、15 秒間にルールのヒット数が 5 に達すると、ルール属性が 30 秒間、[ドロップしてイベントを生成する（Drop and Generate Events）] に変更されます。さらに、上限しきい値により、ルールによって生成されるイベントは 30 秒間で 10 件に制限されます。

図に示されているように、最初の 5 個のパケットがルールに一致しても、イベント通知は行われません。それは、`detection_filter` キーワードで指定されたレートを超過するまで、ルールはトリガーされないためです。ルールがトリガーされると、イベント通知が開始されますが、さらに 5 個のパケットが通過するまでは、レート ベースの基準によって新しいルールとして [ドロップしてイベントを生成する（Drop and Generate Events）] がトリガーされることはありません。レート ベースの基準が満たされると、システムは 11 個目から 15 個目のパケットに対してイベントを生成し、パケットをドロップします。15 個目のパケットがルールに一致すると、上限しきい値に達するため、システムは残りのパケットについてはイベントを生成せずにドロップします。

レート ベースのタイムアウトが発生した後は、それに続くレート ベースのサンプリング期間中、パケットが引き続きドロップされることに注意してください。サンプリング レートが前回のサンプリング期間中にしきい値レートを超えた場合は、新しいアクションが続行されます。



レート ベースの攻撃防御オプションと設定

レート ベース攻撃の防御では、異常なトラフィック パターンを識別して、そのトラフィックが正当な要求に与える影響を最小限に抑えるようにします。一般に、レート ベース攻撃には次のいずれかの特性があります。

- 任意のトラフィックに、ネットワーク上のホストに対して過剰な未完了接続が含まれています。これは、SYN フラッド攻撃を意味します。
- 任意のトラフィックには、ネットワーク上のホストに対して過剰な接続が含まれています。これは、TCP/IP 接続フラッド攻撃を意味します。
- 1 つ以上の特定の宛先 IP アドレスへのトラフィック、または 1 つ以上の特定の送信元 IP アドレスからのトラフィックで、ルールとの一致が過剰に発生します。
- すべてのトラフィックで、特定のルールとの一致が過剰に発生します。

ネットワーク分析ポリシーでは、ポリシー全体に対して SYN フラッドまたは TCP/IP 接続フラッドのいずれかの検出を設定することができます。または個々の侵入ルールもしくはプリプロセッサ ルールに対してレート ベース フィルタを設定できます。GID 135 ルールに手動でレート ベース フィルタを追加すること、またはルールの状態を変更することはできない点に注意してください。GID 135 のルールでは、クライアントを送信元の値、サーバーを宛先の値として使用します。

[SYN攻撃防止（SYN Attack Prevention）] が有効になっている場合、定義されたレート条件を超えるとルール 135:1 がトリガーされます。

[同時接続の制御（Control Simultaneous Connections）] が有効になっている場合、定義されたレート条件を超えるとルール 135:2 がトリガーされ、セッションがクローズまたはタイムアウトするとルール 135:3 がトリガーされます。

（注） デバイスは、内部リソースにインスペクションの負荷を分散させます。レートベースの攻撃防御を設定する際は、デバイスごとではなく、リソースごとのトリガー レートを設定します。レート ベースの攻撃防御が期待どおりに機能しない場合、トリガー レートを下げなければならないことが考えられます。ユーザーにより規定の時間間隔内に送信された接続試行が多すぎると、アラートがトリガーされます。そのため、ルールをレート制限することを推奨します。正しいレートを決定する際に支援が必要な場合は、サポートに連絡してください。

各レート ベース フィルタには、以下のコンポーネントが含まれます。

- ポリシー全体またはルール ベースの送信元/宛先の設定の場合、ネットワーク アドレスの指定
- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超過した場合に実行する新しいアクション

  ポリシー全体に対してレート ベースを設定すると、システムはレート ベース攻撃を検出した時点でイベントを生成します。インライン展開では、トラフィックをドロップすることもできます。個々のルールにレート ベース アクションを設定する場合は、[イベントの生成（Generate Events）]、[イベントのドロップと作成（Drop and Generate Events）]、[無効（Disable）] の 3 つの利用可能なアクションから選択できます。
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウト期間が満了し、レートがしきい値を下回っている場合、ルールのアクションはそのルールに最初に設定されたアクションに戻ります。ポリシー全体に適用される設定の場合、アクションは、トラフィックと一致する個々のルールのアクションに戻ります。一致するアクションがなければ、アクションは停止されます。

インライン展開のレートベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定が使用されていない場合、ルールが [イベントの生成（Generate Events）] に設定されていればイベントが生成されますが、そのルールのパケットがドロップされることはありません。ただし、攻撃トラフィックが、レートベースの基準が設定されているルールに一致した場合、それらのルールが当初 [イベントのドロップおよび生成（Drop and Generate Events）] に設定されていないとしても、レート アクションがアクティブである期間は、パケットがドロップされる場合があります。

（注） レート ベース アクションでは、無効にされたルールを有効にすることも、無効にされたルールに一致するトラフィックをドロップすることもできません。ただし、ポリシー レベルでレート ベース フィルタを設定すると、指定した期間内の過剰な数のSYNパケットまたはSYN/ACKインタラクションを含むトラフィックに対してイベントを生成するか、イベントを生成してトラフィックをドロップすることができます。

同じルールに複数のレート ベース フィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベース フィルタ アクションが競合する場合は、最初のレート ベース フィルタのアクションが実行されることに注意してください。同様に、ポリシー全体に対するレート ベース フィルタと個々のルールに設定されたレート ベース フィルタが競合する場合は、ポリシー全体のレート ベース フィルタが優先されます。

関連トピック

[ルール（Rule）] ページからの動的ルール状態の設定

レートベースの攻撃防御、検出フィルタリング、しきい値処理または抑制

キーワード `detection_filter` により、ルールに一致するしきい値が指定の時間内に発生するまで、ルールのトリガーを阻止します。ルールに `detection_filter` キーワードが含まれている場合、システムは指定の期間、ルールのパターンに一致する着信パケットの数を追跡します。システムはそのルールについて、特定の送信元 IP アドレスからのヒット数、または特定の宛先 IP アドレスからのヒット数をカウントできます。レートがルールのレートを超過すると、そのルールに関するイベント通知が開始されます。

しきい値処理と抑制を用いて、ルール、送信元または宛先に関するイベント通知数を制限することまたはそのルールをすべて一緒に通知を抑制することで、過剰なイベントを低減できます。また、オーバーライドする特定のしきい値がない各ルールに適用するグローバル ルールのしきい値を設定できます。

ルールに抑制を提供する場合、ポリシー全体またはルールにより指定されたレート ベースの設定であるため、レート ベースでアクションの変更が発生した場合でも、システムは、すべての適用可能な IP アドレスのそのルールのイベント通知を抑制します。

関連トピック

侵入イベントしきい値
侵入ポリシー抑制の設定
グローバル ルールのしきい値の基本

レートベース攻撃防止の設定

（注） このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

ポリシー レベルでレートベース攻撃防止を設定することで、SYN フラッド攻撃を阻止できます。特定の送信元からの過剰な接続、または特定の宛先への過剰な接続を阻止することもできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[アクセス制御（Access Control）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policy）]** をクリックするか、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]** を選択してから **[ネットワーク分析ポリシー（Network Analysis Policies）]**をクリックします。

（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 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

ステップ 3 編集するポリシーの横にある [編集（Edit）]（✎） をクリックします。

代わりに [表示（View）]（👁） 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 4 [設定（Settings）] をクリックします。

ステップ 5 [特定の脅威検出（Specific Threat Detection）] の下の [レートベース攻撃防止（Rate-Based Attack Prevention）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 6 [レートベース攻撃防止（Rate-Based Attack Prevention）] の横にある[編集（Edit）]（✎）をクリックします。

ステップ 7 次の 2 つの選択肢があります。

- ホストのフラッディングを目的とする不完全な接続を防ぐには、[SYN 攻撃の防止（SYN Attack Prevention）] の下にある [追加（Add）] をクリックします。
- 過剰な数の接続を防ぐには、[同時接続の制御（Control Simultaneous Connections）] の下にある [追加（Add）] をクリックします。

ステップ 8 トラフィックを追跡する方法を指定します。

- 特定の送信元または送信元の範囲からのすべてのトラフィックを追跡するには、[追跡対象（Track By）] ドロップダウン リストから [送信元（Source）] を選択し、[ネットワーク（Network）] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。
- 特定の宛先または宛先の範囲へのすべてのトラフィックを追跡するには、[追跡対象（Track By）] ドロップダウン リストから [宛先（Destination）] を選択し、[ネットワーク（Network）] フィールドに単一の IP アドレスまたはアドレス ブロックを入力します。

（注）
- すべてのサブネットまたは IP をモニターするために、[ネットワーク（Network）] フィールドに IP アドレス 0.0.0.0/0 を入力しないでください。システムは、（通常、

すべてのサブネットまたはIPを識別するために使用される）このIPアドレスをレートベースの攻撃防御ではサポートしていません。

- システムは、[ネットワーク（Network）] フィールドに含まれる各IPアドレスのトラフィックを個別に追跡します。ある特定のIPアドレスからの設定されたレートを超過するトラフィックがある場合、そのIPアドレスに関するイベントだけが生成されることになります。例として、ネットワーク設定で`10.1.0.0/16`の送信元CIDRブロックを設定し、10個の同時接続が開始された時点でイベントを生成するようにシステムを設定するとします。10.1.4.21から8つの接続が開始され、10.1.5.10から6つの接続が開始されている場合、いずれの送信元も開始されている接続がトリガーを引き起こす数になっていないため、システムはイベントを生成しません。一方、10.1.4.21から11個の同時接続が開始されている場合、システムは10.1.4.21からの接続に対してだけイベントを生成します。

ステップ9 レート追跡設定をトリガーとして使用するレートを指定します。

- SYN攻撃に対する構成の場合は、[レート（Rate）] フィールドに、一定の秒数あたりのSYNパケット数を入力します。
- 同時接続に対する構成の場合は、[カウント（Count）] フィールドに、接続数を入力します。

デバイスは、内部リソースにインスペクションの負荷を分散させます。レートベースの攻撃防御を設定する際は、デバイスごとではなく、リソースごとのトリガー レートを設定します。レート ベースの攻撃防御が期待どおりに機能しない場合、トリガー レートを下げなければならないことが考えられます。ユーザーにより規定の時間間隔内に送信された接続試行が多すぎると、アラートがトリガーされます。そのため、ルールをレート制限することを推奨します。正しいレートの決定する方法については、サポートに問い合わせてください。

ステップ10 レートベース攻撃防止設定に一致するパケットをドロップするには、[ドロップ（Drop）]チェックボックスをオンにします。

ステップ11 [タイムアウト（Timeout）] フィールドに、イベント生成のタイムアウト期間を入力します。この期間を経過すると、SYNまたは同時接続のパターンに一致するトラフィックに対するイベント生成が（該当する場合はドロップも）停止されます。

注意
インライン展開では、大きいタイムアウト値を指定するとホストへの接続が完全にブロックされる可能性があります。

ステップ12 [OK] をクリックします。

ステップ13 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）] をクリックして、[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

- 設定変更を展開します設定変更の展開を参照してください。

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。