トランスポート層およびネットワーク層のプリプロセッサ

以下のトピックでは、トランスポート層およびネットワーク層プリプロセッサとそれらの設定方法について説明します。

トランスポート層およびネットワーク層のプリプロセッサの概要

トランスポート層およびネットワーク層のプリプロセッサは、IP フラグメンテーション、チェックサム検証、TCP および UDP セッションの前処理を悪用する攻撃を検出します。パケットがプリプロセッサに送信される前に、パケット デコーダはパケット ヘッダーとペイロードを、プリプロセッサおよび侵入ルールエンジンで簡単に使用できるフォーマットに変換し、パケットヘッダー内でさまざまな変則的動作を検出します。インライン正規化プリプロセッサは、パケットをデコードした後、他のプリプロセッサにパケットを送信する前に、インライン型展開を対象にトラフィックを正規化します。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、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が無効化されたままになりますが、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。

トランスポート層およびネットワーク層のプリプロセッサのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

トランスポート層およびネットワーク層のプリプロセッサの要件と前提条件

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

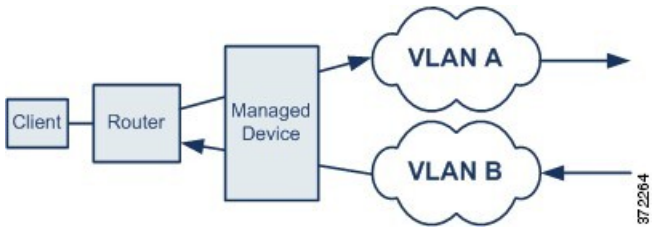
- 管理者
- 侵入管理者

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

トランスポート層とネットワーク層のプリプロセッサの詳細設定は、アクセス コントロール ポリシーが展開され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ます。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。

無視される **VLAN** ヘッダー

同じ接続で異なる方向に流れるトラフィックの VLAN タグが異なると、トラフィックのリアセンブルやルールの処理に影響を与える場合があります。たとえば、以下の図では、同じ接続のトラフィックを VLAN A で送信し、VLAN B で受信できます。



展開でパケットを正しく処理するため、VLANヘッダーを無視するようにシステムを設定できます。

侵入廃棄ルールでのアクティブ応答

廃棄ルールは、ルール状態が [ドロップしてイベントを生成する（Drop and Generate Events）] に設定された侵入ルールまたはプリプロセッサ ルールです。インライン展開では、システムは TCP または UDP 廃棄ルールに応答するために、トリガーしたパケットをドロップし、そのパケットが開始されたセッションをブロックします。

ヒント UDP データ ストリームは一般にセッションという観点では考慮されないため、ストリーム プリプロセッサはカプセル化 IP データグラム ヘッダーの送信元と宛先の IP アドレス フィールドと UDP ヘッダーのポート フィールドを使用してフローの方向を判別し、UDP セッションを識別します。

問題のあるパケットによって TCP または UDP 廃棄ルールがトリガーされた時点で、1 つ以上のアクティブ応答を開始して、より正確かつ明示的に TCP 接続または UDP セッションを閉じるようにシステムを設定することができます。アクティブ応答は、ルーテッド展開およびトランスペアレント展開を含むインライン展開で使用できます。アクティブ応答は、パッシブ展開には適していないか、またはサポートされていません。

アクティブ応答を設定するには、次の手順を実行します。

- TCP または UDP（**resp** キーワードのみ）の侵入ルールを作成または変更します。侵入ルール ヘッダー プロトコルを参照してください。
- 侵入ルールに **react** キーワードまたは **resp** キーワードを追加します。アクティブ応答のキーワードを参照してください。
- 必要に応じて、TCP 接続の場合は、送信する追加のアクティブ応答の最大数と、アクティブ応答の間に待機する秒数を指定します。トランスポート/ネットワーク プリプロセッサの詳細オプション （4 ページ）の「**アクティブ応答の最大数（Maximum Active Responses）**」および「**最小応答時間（秒）（Minimum Response Seconds）**」を参照してください。

アクティブ応答は、一致するトラフィックが廃棄ルールをトリガーとして使用したときに、次のように、そのセッションをクローズします。

- **TCP**：トリガーを使用したパケットを廃棄し、クライアントとサーバ両方のトラフィックに TCP リセット（RST）パケットを挿入します。
- **UDP**：セッションの両端に ICMP 到達不能パケットを送信します。

トランスポート/ネットワーク プリプロセッサの詳細オプション

接続の追跡時に VLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）

トラフィックの識別時に VLAN ヘッダーを無視するか、それとも考慮するかを指定します。次のようになります。

- このオプションを選択すると、VLANヘッダーが無視されます。この設定は、異なる方向に移動するトラフィックで同じ接続について異なる VLAN タグを検出する可能性がある展開済みデバイスに使用します。
- このオプションを無効にすると、VLANヘッダーが考慮されます。この設定は、異なる方向に移動するトラフィックで同じ接続について異なる VLAN タグを検出しない展開済みデバイスに使用します。

アクティブ応答の最大数（Maximum Active Responses）

TCP接続あたりのアクティブ応答の最大数を指定します。アクティブ応答が開始された接続でさらにトラフィックが発生し、前のアクティブ応答を送信してから [最小応答秒数（Minimum Response Seconds）] を超えるトラフィックが発生した場合、システムは指定された最大数に達するまで、別のアクティブ応答を送信します。0 を設定すると、**resp** または **react** ルールによってトリガーされる追加のアクティブ応答が無効になります。侵入廃棄ルールでのアクティブ応答 （3 ページ）およびアクティブ応答のキーワードを参照してください。

トリガーされた **resp** または **react** ルールは、このオプションの設定に関係なく、アクティブ応答を開始することに注意してください。

最小応答時間（秒）（Minimum Response Seconds）

[最大アクティブ応答数（Maximum Active Responses）] に達するまで、システムがアクティブ応答を開始した接続で発生した追加のトラフィックに対して次のアクティブ応答を送信するまで待機する時間を指定します。

トラブルシューティングオプション：セッション終了ロギングしきい値（Troubleshooting Options: Session Termination Logging Threshold）

⚠

注意 [セッション終了ロギングしきい値（Session Termination Logging Threshold）] は、サポート担当から指示されない限り変更しないでください。

トラブルシューティングの電話中に、個別の接続が指定したしきい値を超えた場合にメッセージを記録するようにシステムを設定することをサポートから依頼される場合があります。この

オプションの設定を変更するとパフォーマンスに影響するので、必ずサポートのガイダンスに従って実行してください。

このオプションは、ログに記録されるメッセージのバイト数を指定します。セッションが終了し、メッセージが指定のバイト数を超えた場合は、ログに記録されます。

（注） 上限は 1 GB ですが、管理対象デバイスでストリーム処理のために割り当てられるメモリの量によっても制限されます。

関連トピック

アクティブ応答のキーワード

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の構成

このタスクを実行するには、管理者、アクセス管理者、またはネットワーク管理者である必要があります。

手順

ステップ 1 アクセス制御ポリシーエディタで、変更するポリシーの **[編集（Edit）]**（✎） をクリックします。

ステップ 2 **[詳細（More）]** > **[詳細設定（Advanced Settings）]** の順にクリックし、[トランスポート/ネットワークプリプロセッサ設定（Transport/Network Preprocessor Settings）] セクションの横の **[編集（Edit）]**（✎） をクリックします。

ステップ 3 トラブルシューティング オプション [セッション終了のロギングしきい値（Session Termination Logging Threshold）] を除き、トランスポート/ネットワーク プリプロセッサの詳細オプション（4 ページ）の説明に従ってオプションを変更します。

注意 [セッション終了のロギングしきい値（Session Termination Logging Threshold）] は、サポートからの指示がない限り変更しないでください。

ステップ 4 [OK] をクリックします。

次のタスク

- 必要に応じて、アクセス コントロール ポリシーの編集の説明に従ってさらにポリシーを設定します。
- 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。

チェックサム検証

（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。

システムは、あらゆるプロトコル レベルのチェックサムを検証することで、IP、TCP、UDP、およびICMPによる送信データが完全に受信されていることを確認できます。さらに基本的なレベルで、パケットが転送中に改ざんされたり、誤って変更されたりしていないことも確認できます。チェックサムはアルゴリズムを使用して、パケットでのプロトコルの整合性を検証します。システムが終端のホストでパケットに書き込まれた値を計算し、それがチェックサムと同じであれば、そのパケットは変更されていないと見なされます。

チェックサムの検証を無効にすると、ネットワークが侵入攻撃にさらされる危険があります。システムは、チェックサム検証イベントを生成しないことに注意してください。インライン展開では、パケットのチェックサムが正しくない場合、そのパケットをドロップするようにシステムを設定できます。

チェックサム検証オプション

次のオプションは、いずれも、パッシブ展開またはインライン展開で [有効（Enabled）] または [無効（Disabled）] に設定することができます。インライン展開では [ドロップ（Drop）] に設定することもできます。

- **ICMP チェックサム（ICMP Checksums）**
- **IP チェックサム（IP Checksums）**
- **TCP チェックサム（TCP Checksums）**
- **UDP チェックサム（UDP Checksums）**

違反パケットをドロップするには、オプションを [ドロップ（Drop）] に設定するだけでなく、関連付けられているネットワーク分析ポリシーの [インライン モード（Inline Mode）] を有効にし、確実にデバイスがインラインで展開されるようにする必要があります。

パッシブ展開またはタップ モードでのインライン展開で、これらのオプションを [ドロップ（Drop）] に設定することは、[有効（Enabled）] に設定するのと同じです。

注目 [TCP チェックサム（TCP checksums）] で、[無視（Ignore）] オプション（デフォルト）を選択すると、設定された Snort ルールがバイパスまたは無視されます。

すべてのチェックサム検証オプションは、デフォルトで、[有効（Enabled）] になっています。ただし、Threat Defense ルーテッド トランスペアレント インターフェイスでは、IP チェック

サム検証に失敗したパケットは常にドロップされます。Threat Defense ルーテッドおよびトランスペアレントインターフェイスが、パケットをSnortプロセスに渡す前に、正しくないチェックサムを使用して UDP パケットを修正することに注意してください。

関連トピック

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

チェックサムの確認

（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）]**、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**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policies]**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 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）]（👁） 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 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 [トランスポート層/ネットワーク層のプロセッサ（Transport/Network Layer Preprocessors）] の下にある [チェックサムの確認（Checksum Verification）] が無効になっている場合、[有効（Enabled）] をクリックします。

ステップ 6 [チェックサムの確認（Checksum Verification）] の横にある**[編集（Edit）]**（✎）をクリックします。

ステップ 7 チェックサム検証 （6 ページ） で説明されているオプションを変更します。

（注） [TCPチェックサム（TCP checksums）] で、[無視（Ignore）] オプション（デフォルト）を選択すると、設定された Snort ルールがバイパスまたは無視されます。

ステップ 8 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（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、最後の確定後にキャッシュされた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。

関連トピック

レイヤ管理
競合と変更：ネットワーク分析ポリシーと侵入ポリシー

インライン正規化プリプロセッサ

（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。

インライン正規化プリプロセッサは、インライン展開で攻撃者が検出を免れる可能性を最小限にするために、トラフィックを正規化します。

（注） システムでトラフィックに影響を与えるには、ルーテッド、スイッチド、または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 ペアを使用して、関連する設定を管理対象デバイスに展開する必要があります。

IPv4、IPv6、ICMPv4、ICMPv6、TCP トラフィックを任意に組み合わせて正規化を指定できます。ほとんどの正規化は、パケット単位で行われ、インライン正規化プリプロセッサによって処理されます。ただし、TCP ストリームプリプロセッサは、TCP ペイロードの正規化を含む、ほとんどの状態関連パケットおよびストリームの正規化を処理します。

インライン正規化は、パケットデコーダによるデコードの直後に行われます。その後で、別のプリプロセッサによる処理が行われます。正規化は、パケット層の内部から外部への方向で行われます。

インライン正規化プリプロセッサはイベントを生成しません。インライン正規化プリプロセッサの役割は、インライン展開の別のプリプロセッサおよびルールエンジンで使用できるようにパケットを準備することです。また、システムが処理するパケットが、ネットワーク上のホストで受信したパケットと同じであるようにする役割もあります。

（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たままインライン正規化プリプロセッサを設定することを推奨します。パッシブ展開では、adaptive profile updatesを使用することを推奨します。

関連トピック

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
アダプティブ プロファイルについて

インライン正規化オプション

最小 TTL（Minimum TTL）

[TTL のリセット（Reset TTL）] がこのオプションに設定する値以上の値に設定されている場合、このオプションは以下を指定します。

- [IPv4 の正規化（Normalize IPv4）] が有効にされている場合は、[IPv4 存続可能時間（TTL）（IPv4 Time to Live (TTL)）] フィールドの最小許容値。TTL のパケット値がこの値を下回る場合、[TTL のリセット（Reset TTL）] に設定された値に正規化されます。
- [IPv6 の正規化（Normalize IPv6）] が有効にされている場合は、[IPv6 ホップ リミット（IPv6 Hop Limit）] フィールドの最小許容値。ホップ リミットの値がこの値を下回る場合、[TTL のリセット（Reset TTL）] に設定された値に正規化されます。

このフィールドが空白の場合、システムは値が 1 であると想定します。

（注） Threat Defense ルーテッドおよびトランスペアレント インターフェイスの場合、[最小 TTL（Minimum TTL）] および [TTL のリセット（Reset TTL）] オプションは無視されます。接続の最大 TTL は最初のパケットの TTL によって決定します。後続パケットの TTL は削減できますが、増やすことはできません。システムは、TTL をその接続の以前の最小 TTL にリセットします。これにより、TTL 回避攻撃を阻止します。

パケット復号の [プロトコル ヘッダー異常の検出（Detect Protocol Header Anomalies）] オプションが有効になっている場合、デコーダ ルール カテゴリで次のルールを有効にして、このオプションに関する 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。を行うことができます。

- 指定の最小値を下回る TTL が設定された IPv4 パケットが検出された場合にトリガーするには、ルール 116:428 を有効にします。
- 指定の最小値を下回るホップ リミットが設定された IPv6 パケットが検出された場合にトリガーするには、ルール 116:270 を有効にします。

TTL のリセット（Reset TTL）

[最小 TTL（Minimum TTL）] の値以上の値を設定した場合、以下のフィールドが正規化されます。

- [IPv4 の正規化（Normalize IPv4）] が有効にされている場合は、[IPv4 TTL] フィールド
- [IPv6 の正規化（Normalize IPv6）] が有効にされている場合は、[IPv6 ホップ リミット（IPv6 Hop Limit）] フィールド

パケット値が [最小 TTL（Minimum TTL）] を下回る場合、システムはパケットの TTL またはホップ リミットの値をこのオプションに対して設定された値に変更して、パケットを正規化します。このフィールドを空白のままにするか、0 に設定するか、または [最小 TTL（Minimum TTL）] 未満の値に設定すると、このオプションは無効になります。

IPv4 の正規化（Normalize IPv4）

IPv4 トラフィックの正規化を有効にします。システムは、以下の場合にも必要に応じて TTL フィールドを正規化します。

- このオプションが有効になっていて、さらに、
- [TTL のリセット（Reset TTL）] に設定された値によって TTL の正規化が有効になっている。

このオプションを有効にすると、追加の IPv4 オプションを有効にすることもできます。

このオプションを有効にすると、システムは以下の基本の IPv4 正規化を実行します。

- 過剰なペイロードを持つパケットを、IP ヘッダーに指定されたデータグラム長まで切り捨てます。
- [差別化サービス（DS）（Differentiated Services (DS)）] フィールド（旧称 [タイプ オブ サービス（TOS）（Type of Service (TOS)）] フィールド）をクリアします。
- すべてのオプション オクテットを 1（[操作なし（No Operation）]）に設定します。

このオプションは Threat Defense ルーテッド インターフェイスとトランスペアレント インターフェイスでは無視されます。Threat Defense デバイスは、ルーテッド インターフェイスまたはトランスペアレント インターフェイスのルーテッド アラート、End of Options List（EOOL）、オペレーションなし（NOP）オプション以外の IP オプションを含んでいるすべての RSVP パケットをドロップします。

フラグメント禁止ビットの正規化（Normalize Don't Fragment Bit）

[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドの単一ビットの [フラグメント禁止（Don't Fragment）] サブフィールドをクリアします。このオプションを有効にすると、ダウンストリームのルータがパケットをドロップする代わりに、必要に応じてパケットをフラグメント化できます。また、このオプションを有効にすることで、ドロップされるパケットを巧妙に作成してポリシーを回避する試みを防ぐこともできます。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

IPv4 の正規化（Normalize Reserved Bit）

[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドの単一ビットの [予約済み（Reserved）] サブフィールドをクリアします。通常は、このオプションを有効にします。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

TOS ビットの正規化（Normalize TOS Bit）

1 バイトの [差別化サービス（Differentiated Services）]（旧称 [タイプ オブ サービス（Type of Service）]）フィールドをクリアします。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

余剰ペイロードの正規化（Normalize Excess Payload）

過剰なペイロードを持つパケットを、IP ヘッダーに指定されたデータグラム長にレイヤ 2（たとえば、イーサネット）ヘッダーを合計した長さにまで切り捨てます。ただし、最小フレーム長より小さく切り捨てることはしません。このオプションを選択するには、[IPv4 の正規化（Normalize IPv4）] を有効にする必要があります。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。過剰なペイロードを持つパケットは、常にこれらのインターフェイスでドロップされます。

IPv6 の正規化（Normalize IPv6）

[ホップバイホップ オプション（Hop-by-Hop Options）] および [宛先オプション（Destination Options）] 拡張ヘッダーに含まれるすべてのオプション タイプ フィールドを 00（スキップして処理を続行）に設定します。このオプションが有効にされていて、[Reset TTL] に設定された値が ホップ リミット正規化を有効にしている場合、システムは必要に応じてホップ リミット フィールドも正規化します。

ICMPv4 の正規化（Normalize ICMPv4）

ICMPv4 トラフィックのエコー（要求）およびエコー応答メッセージで 8 ビットのコードフィールドをクリアします。

ICMPv6 の正規化（Normalize ICMPv6）

ICMPv6 トラフィックのエコー（要求）およびエコー応答メッセージで 8 ビットのコードフィールドをクリアします。

予約済みビットの正規化またはクリア（Normalize/Clear Reserved Bits）

TCP ヘッダーの予約ビットをクリアします。

オプション パディング バイトの正規化またはクリア（Normalize/Clear Option Padding Bytes）

TCP オプションのパディング バイトをクリアします。

URG=0 の場合に緊急ポインタをクリア（Clear Urgent Pointer if URG=0）

緊急（URG）制御ビットが設定されていない場合、16 ビットの TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドをクリアします。

空のペイロードに設定された緊急ポインタまたは URG をクリア（Clear Urgent Pointer/URG on Empty Payload）

ペイロードがない場合、TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドおよび URG 制御ビットをクリアします。

緊急ポインタが設定されていない場合 URG をクリア（Clear URG if Urgent Pointer is Not Set）

緊急ポインタが設定されていない場合、TCP ヘッダー URG 制御ビットをクリアします。

緊急ポインタの正規化（Normalize Urgent Pointer）

ポインタがペイロード長を上回る場合、2 バイトの TCP ヘッダー [緊急ポインタ（Urgent Pointer）] フィールドをペイロード長に設定します。

TCP ペイロードの正規化（Normalize TCP Payload）

再送信されるデータの一貫性が確保されるように [TCP データ（TCP Data）] フィールドの正規化を有効にします。正しく再構成できないセグメントはすべてドロップされます。

SYN に関するデータを削除（Remove Data on SYN）

TCP オペレーティング システム ポリシーが Mac OS 以外の場合、同期（SYN）パケットのデータを削除します。

また、このオプションにより、TCP ストリーム プリプロセッサの [ポリシー（Policy）] オプションが [Mac OS] に設定されていない場合にトリガー可能なルール 129:2 もまた無効になります。

RST に関するデータを削除（Remove Data on RST）

TCP リセット（RST）パケットからデータを削除します。

データをウィンドウにトリミング（Trim Data to Window）

[TCP データ（TCP Data）] フィールドを [ウィンドウ（Window）] フィールドに指定されたサイズにまで切り捨てます。

データを MSS にトリミング（Trim Data to MSS）

ペイロードが MSS より長い場合、[TCP データ（TCP Data）] フィールドを最大セグメント サイズ（MSS）にまで切り捨てます。

解決不可能な TCP ヘッダーの異常をブロック（Block Unresolvable TCP Header Anomalies）

このオプションを有効にすると、システムは無効になり受信ホストによってブロックされる可能性が高い異常な TCP パケット（正規化されている場合）をブロックします。たとえば、システムは確立されたセッションの後に送信された SYN パケットをブロックします。

また、システムは、ルールが有効にされているかどうかに関係なく、以下に示すTCP ストリーム プリプロセッサ ルールのいずれかに一致するパケットもドロップします。

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 ～129:19

[ブロックされたパケットの合計（Total Blocked Packets）] パフォーマンス グラフには、インライン展開でブロックされたパケットの数が示され、パッシブ展開とタップ モードでのインライン展開の場合は、インライン展開でブロックされる予想数が示されます。

明示的な混雑通知（ECN）（Explicit Congestion Notification）

明示的輻輳通知（ECN）フラグのパケット単位またはストリーム単位の正規化を以下のように有効にします。

- [パケット（Packet）] を選択すると、ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされます。
- [ストリーム（Stream）] を選択すると、ECN の使用がネゴシエートされていない場合、ストリーム単位で ECN フラグがクリアされます。

[ストリーム（Stream）] を選択した場合、この正規化が実行されるようにするには、TCP ストリーム プリプロセッサの [TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] オプションも有効にされている必要があります。

既存の TCP オプションをクリア（Clear Existing TCP Options）

[これらの TCP オプションを許可（Allow These TCP Options）] を有効にします。

これらの TCP オプションを許可（Allow These TCP Options）

トラフィックで許可する特定の TCP オプションの正規化を無効にします。

明示的に許可されたオプションは、正規化されません。オプションを [操作なし（No Operation）]（TCP オプション 1）に設定して明示的に許可していないオプションは、正規化されます。

[これらの TCP オプションを許可（Allow These TCP Options）] の設定に関係なく、次のオプションは最適な TCP パフォーマンスに一般的に使用されるため、システムは常にこれらのオプションを許可します。

- 最大セグメント サイズ（MSS）（Maximum Segment Size (MSS)）
- ウィンドウ スケール（Window Scale）
- タイム スタンプ TCP（Time Stamp TCP）

他のそれほど一般的に使用されないオプションについては、システムは自動的に許可しません。

特定のオプションを許可するには、オプション キーワード、オプション番号、またはこの両方のカンマ区切りリストを設定します。以下に、一例を示します。

```
sack, echo, 19
```

オプション キーワードを指定するということは、そのキーワードと関連付けられた 1 つ以上の TCP オプションの番号を指定することと同じです。たとえば、`sack` を指定することは、TCP オプション 4（Selective Acknowledgment Permitted）および TCP オプション 5（Selective Acknowledgment）を指定することと同じです。オプション キーワードでは、大文字と小文字が区別されません。

また、`any` を指定すると、すべての TCP オプションが許可されるため、実質的にすべての TCP オプションの正規化が無効にされます。

次の表に、許可する TCP オプションを指定する方法を要約します。フィールドを空のままにすると、システムは MSS、ウィンドウ スケール、およびタイムスタンプのオプションのみを許可します。

指定する内容	許可されるオプション
sack	TCP オプション 4（Selective Acknowledgment Permitted）および 5（Selective Acknowledgment）
echo	TCP オプション 6（Echo Request）および 7（Echo Reply）
partial_order	TCP オプション 9（Partial Order Connection Permitted）および 10（Partial Order Service Profile）
conn_count	TCP 接続数オプション 11（CC）、12（CC.New）、および 13（CC.Echo）
alt_checksum	TCP オプション 14（Alternate Checksum Request）および 15（Alternate Checksum）
md5	TCP オプション 19（MD5 Signature）
オプション番号 2 ～ 255	キーワードのないオプションを含む、特定のオプション

指定する内容	許可されるオプション
any	すべての TCP オプション（この設定は、実質的に TCP オプションの正規化を無効にします）

このオプションに any を指定しない場合、正規化には次のものが含まれます。

- MSS、ウィンドウ スケール、タイムスタンプ、およびその他の明示的に許可されたオプションを除き、すべてのオプションのバイトを [操作なし（No Operation）]（TCP オプション 1）に設定します。
- タイムスタンプは存在していても無効な場合、あるいは有効であってもネゴシエートされない場合、タイムスタンプ オクテットを [操作なし（No Operation）] に設定します。
- タイムスタンプがネゴシエートされるものの、存在しない場合、パケットをブロックします。
- 確認応答（ACK）制御ビットが設定されていない場合、[タイム スタンプ エコー応答（TSecr）（Time Stamp Echo Reply (TSecr)）] オプション フィールドをクリアします。
- SYN 制御ビットが設定されていない場合、[MSS] および [ウィンドウ スケール（Window Scale）] オプションを [操作なし（No Operation）]（TCP オプション 1）に設定します。

インライン正規化の設定

（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。

始める前に

- 問題を起こすパケットを正規化またはドロップするには、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の説明に従って [インライン モード（Inline Mode）] を有効にします。また、管理対象デバイスは、インラインで展開する必要があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（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**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policies]** 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 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）]（👁） 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 4 ナビゲーションパネルで [設定（Settings）] をクリックします（キャレットではなく、単語をクリックします）。

ステップ 5 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] で [インライン正規化（Inline Normalization）] 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 [インライン正規化（Inline Normalization）] の横にある **[編集（Edit）]**（✎） をクリックします。

ステップ 7 インライン正規化プリプロセッサ （8 ページ）で説明されているオプションを設定します。

ステップ 8 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（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、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- インライン正規化 [最小TTL（Minimum TTL）] オプションで侵入イベントを生成する場合は、パケットデコーダルール 116:429（IPv4）と 116:270（IPv6）のいずれかまたは両方を有効にします。詳細については、侵入ルール状態の設定およびインライン正規化オプション （9 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。

関連トピック

レイヤ管理
競合と変更：ネットワーク分析ポリシーと侵入ポリシー

IP 最適化プリプロセッサ

（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。

最大伝送ユニット（MTU）より大きいために IP データグラムが複数の小さい IP データグラムに分割されると、その IP データグラムはフラグメント化されたことになります。単一の IP データグラムフラグメントには、隠れた攻撃を識別するのに十分な情報が含まれない場合があ

ります。そのため、攻撃者はエクスプロイトの検出を免れるために、フラグメント化されるパケットで攻撃データを送信する可能性があります。IP 最適化プリプロセッサは、ルール エンジンが IP データグラムに対してルールを実行する前に、パケットに仕込まれた攻撃をルールで識別しやすくするために、フラグメント化された IP データグラムを再構成します。フラグメント化されたデータグラムを再構成できない場合、それらのデータグラムに対しては、ルールが実行されません。

IP フラグメンテーション エクスプロイト

IP最適化を有効にすると、ネットワーク上のホストに対する攻撃（ティアドロップ攻撃など）や、システム自体に対するリソース消費攻撃（Jolt2 攻撃など）を検出するのに役立ちます。

ティアドロップ攻撃は、特定のオペレーティング システムのバグを悪用して、そのオペレーティング システムがオーバーラップした IP フラグメントを再構成しようとするとクラッシュするように仕掛けます。IP最適化プリプロセッサを有効にして、オーバーラップしたフラグメントを識別するように設定すれば、該当するフラグメントを識別できます。IP最適化プリプロセッサは、ティアドロップ攻撃などのオーバーラップ フラグメント攻撃で、最初のパケットを検出するだけで、同じ攻撃での後続のパケットは検出しません。

Jolt2 攻撃では、IP デフラグ機能を酷使させるという方法でサービス拒絶攻撃を仕掛けるために、フラグメント化された同じ IP パケットのコピーを大量に送信します。IP 最適化プリプロセッサでは、メモリ使用量の上限によって、このような攻撃を阻止し、包括的検査においてシステムを自己防衛状態にします。システムは攻撃によって過負荷にならず、運用可能な状態を維持し、ネットワーク トラフィックの検査を続行します。

フラグメント化されたパケットを再構成する方法は、オペレーティングシステムによって異なります。ホストがどのオペレーティングシステムで実行されているのかを攻撃者が特定できれば、その攻撃者はターゲットホストが特定の方法で再構成するように不正なパケットをフラグメント化することも可能です。モニター対象のネットワーク上でホストを実行しているオペレーティングシステムは、システムには不明です。したがって、プリプロセッサがパケットを誤った方法で再構成して検査し、それによってエクスプロイトが検出されないままパス スルーする可能性があります。このような攻撃を軽減するために、ネットワーク上のホストごとに適切な方法でパケットを最適化するよう、最適化プリプロセッサを設定できるようになっています。

パッシブ展開でadaptive profile updatesを使用することで、パケットのターゲット ホストのホスト オペレーティング システム情報に応じて、IP 最適化プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるようにすることもできます。

ターゲット ベースの最適化ポリシー

ホストのオペレーティングシステムは以下の3つの基準を使用して、パケットを再構成する際に優先するパケット フラグメントを決定します。

- オペレーティング システムがフラグメントを受信した順序
- フラグメントのオフセット（パケットの先頭からのそのフラグメントの距離（バイト単位））

- オーバーラップしているフラグメントとの相対開始位置と相対終了位置

これらの基準はすべてのオペレーティング システムで使用されているものの、フラグメント化されたパケットを再構成するときに優先するフラグメントは、オペレーティング システムによって異なります。したがって、ネットワーク上で異なるオペレーティング システムを使用する2台のホストが、同じオーバーラップ フラグメントをまったく異なる方法で再構成する場合も考えられます。

いずれかのホストのオペレーティング システムを認識している攻撃者が、オーバーラップしたパケット フラグメントに不正なコンテンツを忍ばせて送信することによって、エクスプロイトの検出を免れ、そのホストを悪用する可能性があります。このパケットが他のホストで再構成されて検査されても、パケットに害はないように見えますが、ターゲット ホストで再構成される場合には不正なエクスプロイトが含まれています。ただし、モニター対象のネットワーク セグメントで稼働するオペレーティング システムを認識するように IP 最適化プリプロセッサを設定すれば、このプリプロセッサがターゲット ホストと同じ方法でフラグメントを再構成することによって、攻撃を識別できます。

IP 最適化オプション

IP 最適化を有効または無効にすることだけを選択することもできますが、シスコでは、それよりも細かいレベルで、有効にする IP 最適化プリプロセッサの動作を指定することを推奨しています。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

次のグローバル オプションを構成できます。

事前に割り当てられたフラグメント（Preallocated Fragments）

プリプロセッサが一度に処理できる個々のフラグメントの最大数。事前割り当てするフラグメント ノードの数を指定すると、静的メモリ割り当てが有効になります。

⚠

注意 個々のフラグメントの処理には、約 1550 バイトのメモリが使用されます。プリプロセッサで個々のフラグメントを処理するために必要なメモリが、管理対象デバイスに事前定義された使用可能なメモリ量の制限を上回る場合は、管理対象デバイスのメモリ制限が優先されます。

IP 最適化ポリシーごとに、以下のオプションを設定できます。

ネットワーク

最適化ポリシーを適用するホスト（複数可）の IP アドレス。

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。デフォルト ポリシーを含め、合計で最大255個のプロファイルを指定できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニター対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

ポリシー

モニター対象ネットワーク セグメント上のホスト一式に使用する最適化ポリシー。

ターゲット ホストのオペレーティング システムに応じて、7 つの最適化ポリシーの 1 つを選択できます。以下の表に、7 つのポリシーと、それぞれのポリシーを使用するオペレーティング システムを記載します。First と Last というポリシー名は、これらのポリシーが元のオーバーラップ パケットまたは後続のオーバーラップ パケットのどちらを優先するかを反映しています。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

表 *1:* ターゲットベースの最適化ポリシー

ポリシー	オペレーティング システム
BSD	AIX FreeBSD IRIX VAX/VMS
BSD-right	HP JetDirect
First	Mac OS HP-UX
Linux	Linux OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

Timeout

プリプロセッサエンジンがフラグメント化されたパケットを再構成する際に使用できる最大時間（秒数）を指定します。指定された時間内にパケットを再構成できない場合、プリプロセッサ エンジンはパケットの再構成試行を停止し、受信したフラグメントを破棄します。

最小 TTL（Min TTL）

パケットに許容される最小 TTL 値を指定します。このオプションは、TTL ベースの挿入攻撃を検出します。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 123:11 を有効にします。

異常検知（Detect Anomalies）

オーバーラップ フラグメントのようなフラグメンテーション問題を識別します。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、次のルールを有効にすることができます：

- 123:1 ～ 123:4
- 123:5（BSD ポリシー）
- 123:6 ～ 123:8

オーバーラップ範囲（Overlap Limit）

セッション内で重複しているセグメントの設定された数が検出されると、そのセッションの最適化を停止することを指定します。

このオプションを設定するには、[異常検知（Detect Anomalies）] を有効にする必要があります。値が空白の場合、このオプションは無効になります。値 0 は、無制限の重複セグメント数を指定します。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。重複フラグメントは、それらのインターフェイスでは常にドロップされます。

このオプションに関するイベントを生成し、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、ルール 123:12 を有効にできます。

最小フラグメント サイズ（Minimum Fragment Size）

設定されたバイト数より小さい最後でないフラグメントが検出された場合、そのパケットは悪意のあるものとみなされることを指定します。

このオプションを設定するには、[異常検知（Detect Anomalies）] を有効にする必要があります。値が空白の場合、このオプションは無効になります。値0は、無制限のバイト数を指定します。

このオプションに関するイベントを生成し、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、ルール 123:13 を有効にできます。

IP 最適化の設定

（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。

始める前に

- カスタム ターゲットベース ポリシーで識別するネットワークが、親ネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、および VLAN のサブセットと一致するか、サブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定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）]**、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**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policies]**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 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）]（） 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 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 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] で [IP 最適化（IP Defragmentation）] 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 [IP最適化（IP Defragmentation）] の横にある **[編集（Edit）]**（） をクリックします。

ステップ 7 必要に応じて、[事前割り当て済みフラグメント（Preallocated Fragments）] フィールドに値を入力します。

ステップ 8 次の選択肢があります。

- サーバープロファイルの追加：ページの左側の [サーバー（Servers）] の横にある **Add** (＋) をクリックし、[ホストアドレス（Host Address）] フィールドに値を入力して、[OK] をクリックします。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。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。
- サーバー プロファイルの編集：ページの左側の [サーバー（Servers）] で設定済みのアドレスをクリックするか、[デフォルト（default）] をクリックします。
- プロファイルの削除：ポリシーの横にある[削除（Delete）]（🗑）をクリックします。

ステップ 9 IP 最適化オプション （18 ページ） で説明されているオプションを変更します。

ステップ 10 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（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、最後の確定後にキャッシュされた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、IP最適化ルール（GID 123）を有効にします。詳細については、「侵入ルール状態の設定」および「IP 最適化オプション （18 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。

関連トピック

レイヤの基本
競合と変更：ネットワーク分析ポリシーと侵入ポリシー

パケット デコーダ

（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。

キャプチャしたパケットをプリプロセッサに送信する前に、システムはパケットをパケットデコーダに送信します。パケット デコーダは、プリプロセッサやルール エンジンが容易に使用できる形式に、パケットヘッダーおよびペイロードを変換します。データリンク層から開始して、ネットワーク層、トランスポート層へと、各スタック層が順にデコードされます。

パケット デコーダ オプション

以下の説明でプリプロセッサルールが言及されていない場合、オプションにはプリプロセッサルールが関連付けられていません。

GTP データ チャネルのデコード（Decode GTP Data Channel）

カプセル化された GTP（General Packet Radio Service（GPRS）トンネリング プロトコル）データ チャネルをデコードします。デフォルトでは、デコーダはポート 3386 ではバージョン 0 のデータをデコードし、ポート 2152 ではバージョン 1 のデータをデコードします。`GTP_PORTS` デフォルト変数を使用して、カプセル化された GTP トラフィックを識別するポートを変更できます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:297 および 116:298 を有効にします。

[標準外ポートで Teredo を検知（Detect Teredo on Non-Standard Ports）]

ポート 3544 以外の UDP ポートで識別される IPv6 トラフィックの Teredo トンネリングを検査します。

IPv6 トラフィックが存在する場合、システムは常にこのトラフィックを検査します。デフォルトでは、IPv6 インスペクションには 4in6、6in4、6to4、および 6in6 トンネリング方式が含まれます。また、UDP ヘッダーがポート 3544 を指定している場合は、Teredo トンネリングも含まれます。

IPv4 ネットワークでは、IPv4 ホストが Teredo プロトコルを使用して、IPv4 ネットワーク アドレス変換（NAT）デバイスを介して IPv6 トラフィックをトンネリングできます。Teredo は、IPv6 パケットを IPv4 UDP データグラムにカプセル化して、IPv4 NAT デバイスの背後で IPv6 接続を許可します。システムは通常、UDP ポート 3544 を使用して Teredo トラフィックを識別します。ただし、攻撃者が検出を免れるために標準以外のポートを使用する可能性も考えられます。[非標準ポートでの Teredo の検出（Detect Teredo on Non-Standard Ports）] を有効にすることで、システムに Teredo トンネリングのすべての UDP ペイロードを検査させることができます。

Teredo のデコードは、外側のネットワーク層に IPv4 が使用されている場合に限り、最初の UDP 見出しに対してのみ行われます。UDP データが IPv6 データにカプセル化されるため、Teredo IPv6 層の後に 2 つめの UDP 層が存在する場合、ルール エンジンは UDP 侵入ルールを使用して、内側および外側の両方の UDP 層を分析します。

policy-other ルール カテゴリの侵入ルール 12065、12066、12067、および 12068 は Teredo トラフィックを検出しますが、デコードは行わないので注意してください。（任意）これらのルールを使用してインライン展開で Teredo トラフィックをドロップすることができます。ただし、[非標準ポートでの Teredo の検出（Detect Teredo on Non-Standard Ports）] を有効にする場合は、これらのルールを無効化するか、トラフィックをドロップせずにイベントを生成するように設定する必要があります。

[余長値の検知（Detect Excessive Length Value）]

パケットヘッダーが実際のパケット長を超えるパケット長を指定しているかどうかを検出します。

このオプションは、Threat Defense ルーテッド、トランスペアレント、およびインライン インターフェイスでは無視されます。超過ヘッダー長を持つパケットは常にドロップされます。ただし、このオプションは Threat Defense インライン タップおよびパッシブ インターフェイスに適用されます。

このオプションに関してイベントを生成し、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、ルール 116:6、116:47、116:97、および 116:275 を有効にできます。

[間違いな IP オプションを検知（Detect Invalid IP Options）]

無効な IP オプションを使用したエクスプロイトを識別するために、無効な IP ヘッダー オプションを検出します。たとえば、ファイアウォールに対するサービス妨害攻撃は、システムをフリーズさせる原因になります。ファイアウォールが無効なタイムスタンプおよび IP セキュリティ オプションを解析しようとして、ゼロ長のチェックに失敗すると、回復不可能な無限ループが発生します。ルールエンジンはゼロ長のオプションを識別し、ファイアウォールでの攻撃を軽減するために使用できる情報を提供します。

Threat Defense デバイスは、各ルーテッドまたはトランスペアレント インターフェイスのルータ アラート、End of Options List（EOOL）、およびオペレーションなし（NOP）オプションを持つ RSVP パケットをドロップします。インライン、インライン タップ、またはパッシブ インターフェイスについては、IP オプションは上記のように処理されます。

このオプションに関してイベントを生成し、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、ルール 116:4 および 116:5 を有効にします。

[実験的 TCP オプションを検知（Detect Experimental TCP Options）]

試験的な TCP オプションが設定された TCP ヘッダーを検出します。以下の表は、それらのオプションを示しています。

TCP オプション	説明
9	半順序接続許可（Partial Order Connection Permitted）
10	半順序サービス プロファイル（Partial Order Service Profile）
18	代替チェックサム要求（Alternate Checksum Request）
15	代替チェックサム データ（Alternate Checksum Data）
18	トレーラ チェックサム（Trailer Checksum）
20	スペース通信プロトコル標準（Space Communications Protocol Standards（SCPS））

TCP オプション	説明
21	選択的否定確認応答（Selective Negative Acknowledgements（SCPS））
22	レコードの境界（Record Boundaries（SCPS））
23	破損（Corruption（SPCS））
24	SNAP
26	TCP 圧縮フィルタ（TCP Compression Filter）

これらのオプションは試験的なものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。

（注） 上記の表に記載されている試験的オプションに加えて、26 より大きいオプション番号を持つ TCP オプションは、試験的オプションと見なされます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:58 を有効にします。

廃止された TCP オプションを検知

廃止された TCP オプションが設定された TCP ヘッダーを検出します。これらのオプションは廃止されたものであるため、一部のシステムでは考慮されず、悪用される恐れがあります。以下の表は、それらのオプションを示しています。

TCP オプション	説明
[6]	エコー（Echo）
7	エコー応答（Echo Reply）
16	Skeeter
17	Bubba
19	MD5 Signature（MD5 認証）
25	Unassigned（未定義）

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:57 を有効にします。

[T または TCP を検知（Detect T/TCP）]

CC.ECHO オプションが設定された TCP ヘッダーを検出します。CC.ECHO オプションは、TCP for Transactions（T/TCP）が使用されていることを確認します。T/TCP ヘッダー オプションは幅広く使用されていないため、一部のシステムでは考慮されず、悪用される恐れがあります。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 116:56 を有効にします。

[その他の TCP オプションを検知（Detect Other TCP Options）]

他の TCP デコード イベント オプションでは検出されない無効な TCP オプションが設定された TCP ヘッダーを検出します。たとえば、このオプションは、無効な長さ、またはオプション データが TCP ヘッダーに収まらない長さの TCP オプションを検出します。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。無効な TCP オプションを持つパケットは常にドロップされます。

このオプションに関してイベントを生成し、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、ルール 116:54、116:55、および 116:59 を有効にできます。

[プロトコルヘッダの異常を検知（Detect Protocol Header Anomalies）]

より具体的な IP および TCP デコーダ オプションでは検出されない他のデコード エラーを検出します。たとえば、このデコーダは、不正な形式のデータ リンク プロトコル ヘッダーを検出する場合があります。

このオプションは、Threat Defense ルーテッド、トランスペアレント、およびインライン インターフェイスでは無視されます。ヘッダー異常があるパケットは常にドロップされます。ただし、このオプションは Threat Defense インライン タップおよびパッシブ インターフェイスに適用されます。

このオプションに関するイベントを生成し、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、次のルールを有効にすることができます。

GID:SID	該当する場合にイベントを生成
116:467	パケットが Cisco FabricPath ヘッダーにカプセル化されるパケットの最小サイズより小さい。
116:468	ヘッダーの Cisco メタデータ（CMD）フィールドに、有効な CMD ヘッダの最小サイズより小さいヘッダー長が含まれている。CMD フィールドは、Cisco TrustSec プロトコルと関連付けられています。
116:469	ヘッダーの CMD フィールドに、無効なフィールド長が含まれている。

GID:SID	該当する場合にイベントを生成
116:470	ヘッダーのCMDフィールドに、無効なセキュリティ グループ タグ（SGT）オプションのタイプがあります。
116:471	ヘッダーのCMDフィールドに、値が予約されている SGT が含まれています。

その他のパケット デコーダ オプションに関連付けられていないパケット デコーダ ルールを有効にすることもできます。

関連トピック

定義済みデフォルト変数

パケット復号の設定

（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。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（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**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policies]**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 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）]（👁） 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 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 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] の下の [パケット復号（Packet Decoding）] 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 [パケット復号（Packet Decoding）] の横にある**[編集（Edit）]**（✎）をクリックします。

ステップ 7 パケット デコーダ オプション （23 ページ）で説明されているオプションを有効または無効にします。

ステップ 8 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（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、最後の確定後にキャッシュされた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、パケット デコーダ ルール（GID 116）を有効にします。詳細については、「侵入ルール状態の設定」および「パケット デコーダ オプション （23 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。

関連トピック

レイヤの基本
競合と変更：ネットワーク分析ポリシーと侵入ポリシー

TCP ストリームの前処理

（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。

TCP プロトコルは、接続で生じ得るさまざまな状態を定義します。各 TCP 接続は、送信元と宛先の IP アドレス、および送信元と宛先のポートによって識別されます。TCP では、接続パラメータ値が同じ接続は、一度に 1 つしか存在できません。

状態に関連する TCP エクスプロイト

侵入ルールに `established` 引数と組み合わせた `flow` キーワードを追加すると、侵入ルール エンジンはステートフル モードでルールとフロー ディレクティブに一致するパケットを検査します。ステートフル モードでは、クライアントとサーバの間で正当な 3 ウェイ ハンドシェイクによって確立されたTCPセッションの一部となっているトラフィックだけが評価されます。

確立された TCP セッションの一部として識別できない TCP トラフィックをプリプロセッサが検出するようにシステムを設定することは可能です。しかし、このようなイベントは、システムをすぐに過負荷状態に陥らせ、しかも意味のあるデータを提供しないため、通常の使用法では推奨されません。

Stick や Snot などの攻撃では、システムの自身に対する広範なルール セットとパケット インスペクションを悪用します。これらのツールは、Snort ベースの侵入ルールのパターンに基づいてパケットを生成し、ネットワークに送信します。ステートフルインスペクションに対して設

定するルールに `flow` または `flowbits` キーワードを含めなければ、パケットのそれぞれがルールをトリガーするため、システムが過負荷状態になります。ステートフルインスペクションを使用することで、確立された TCP セッションに含まれず、意味のある情報を提供しないこれらのパケットを無視できます。ステートフル インスペクションを実行すると、ルール エンジンは確立された TCP セッションに含まれる攻撃のみを検出するため、アナリストが stick や snot によって大量に生成されるイベントに時間を取られることがなくなります。

ターゲット ベースの TCP ポリシー

オペレーティング システムによって、TCP の実装方法は異なります。たとえば、セッションをリセットするために、Windowsやその他のオペレーティング システムの一部ではTCP リセットセグメントに正確なTCP シーケンス番号を割り当てる必要があるのに対し、Linuxや他のオペレーティング システムではシーケンス番号の範囲を使用できます。この例の場合、ストリーム プリプロセッサは、シーケンス番号に基づき、宛先ホストがリセットにどのように応答するかを正確に把握しなければなりません。ストリーム プリプロセッサがセッションの追跡を停止するのは、宛先ホストがリセットが有効であると見なした場合のみです。したがって、プリプロセッサがストリームの検査を停止した後は、パケットを送信することによって攻撃が検出を免れることはできません。TCP の実装方法の違いには、オペレーティング システムで TCP タイムスタンプ オプションを採用しているかどうか、採用している場合にはどのようにタイムスタンプを処理するか、そしてオペレーティング システムで SYN パケットのデータを受け入れるか、無視するかどうかも含まれます。

また、オーバーラップTCPセグメントを再構成する方法も、オペレーティング システムによって異なります。オーバーラップ TCP セグメントは、確認応答済み TCP トラフィックの通常の再送信を反映する場合があります。あるいは、ホストのオペレーティング システムを認識している攻撃者が、エクスプロイトの検出を免れるためにオーバーラップセグメントに不正なコンテンツを忍ばせて送信し、そのホストを悪用しようとしている場合もあります。ただし、モニター対象のネットワーク セグメント上で稼働するオペレーティング システムを認識するようにストリーム プリプロセッサを設定すれば、そのプリプロセッサがターゲット ホストと同じ方法でセグメントを再構成することによって、攻撃を識別できます。

モニター対象のネットワーク セグメント上のさまざまなオペレーティング システムに合わせてTCP ストリーム インスペクションおよび再構成を調整するために、1 つ以上の TCP ポリシーを作成することができます。ポリシーごとに、13 のオペレーティング システム ポリシーのうちの 1 つを特定します。異なるオペレーティング システムを使用するホストのいずれか、あるいはすべてを識別するために必要な数だけ TCP ポリシーを使用し、各 TCP ポリシーを特定の IP アドレスまたはアドレス ブロックにバインドします。デフォルトの TCP ポリシーは、他の TCP ポリシーで指定されていないモニタ対象ネットワーク上のすべてのホストに適用されます。したがって、デフォルトの TCP ポリシーに IP アドレスまたはアドレス ブロックを指定する必要はありません。

パッシブ展開で adaptive profile updates を使用することで、パケットのターゲット ホストのホスト オペレーティング システム情報に応じて、TCP ストリーム プリプロセッサに適用するターゲットベースのポリシーが動的に選択されるようにすることもできます。

TCP ストリームの再構成

ストリームプリプロセッサは、TCPセッションでのサーバからクライアントへの通信ストリーム、クライアントからサーバへの通信ストリーム、またはその両方の通信ストリームに含まれるすべてのパケットを収集して再構成します。これにより、ルール エンジンは、特定のストリームに含まれる個々のパケットだけを検査するのではなく、ストリームを再構成された単一のエンティティとして検査できます。

ストリームの再構成により、ルールエンジンは、個々のパケットを検査する場合には検出できない可能性のあるストリームベースの攻撃を識別できます。ルールエンジンの再アセンブリ対象とする通信ストリームは、ネットワークのニーズに応じて指定できます。たとえば、Web サーバー上のトラフィックをモニターする際に、独自の Web サーバーから不正なトラフィックを受信する可能性がほとんどないため、クライアント トラフィックだけを検査するという場合もあります。

各 TCP ポリシーに、ストリーム プリプロセッサが再構成するトラフィックを識別するポートのカンマ区切りのリストを指定できます。adaptive profile updates が有効にされている場合、再構成するトラフィックを識別するサービスを、ポートの代わりとして、あるいはポートと組み合わせてリストすることもできます。

ポート、サービス、またはその両方を指定できます。クライアント ポート、サーバ ポート、またはその両方を任意に組み合わせた個別のポートリストを指定できます。また、クライアント サービス、サーバ サービス、またはその両方を任意に組み合わせた個別のサービス リストを指定することもできます。たとえば、以下を再構成する必要があるとします。

- クライアントからの SMTP（ポート 25）トラフィック
- FTP サーバ応答（ポート 21）
- 両方向の Telnet（ポート 23）トラフィック

この場合、以下のように設定できます。

- クライアント ポートとして、`23, 25` を指定
- サーバ ポートとして、`21, 23` を指定

あるいは、以下のように設定することもできます。

- クライアント ポートとして、`25` を指定
- サーバー ポートとして、`21` を指定
- 両方のポートとして、`23` を指定

さらに、ポートとサービスを組み合わせた以下の設定例は、adaptive profile updates が有効にされている場合、有効になります。

- クライアント ポートとして、`23` を指定
- クライアント サービスとして、`smtp` を指定

- サーバー ポートとして、21 を指定
- サーバー サービスとして、telnet を指定

ポートを否定すると（!80など）、そのポートのトラフィックがTCPストリームプリプロセッサで処理されなくなり、パフォーマンスが向上します。

all を引数として指定して、すべてのポートに対して再構成を指定することもできますが、ではポートを all に**設定しない**よう推奨しています。この設定では、このプリプロセッサで検査するトラフィックの量が増え、不必要にパフォーマンスが低下するためです。

TCP再構成には、自動的かつ透過的にその他のプリプロセッサに追加するポートが含まれています。しかし、他のプリプロセッサの設定に追加した TCP 再構成リストにポートを明示的に追加する場合は、これらの追加したポートは通常処理されます。これには、次のプリプロセッサのポート リストが含まれています。

- FTP/Telnet（サーバ レベル FTP）
- DCE/RPC
- HTTP Inspect
- SMTP
- Session Initiation Protocol
- POP
- IMAP
- SSL

追加のトラフィック タイプ（クライアント、サーバー、両方）を再構成すると、リソースの需要が増大することに注意してください。

TCP ストリームのプリプロセス オプション

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

次のグローバル TCP オプションを構成できます。

パケット タイプ パフォーマンスの向上（Packet Type Performance Boost）

送信元ポートおよび宛先ポートの両方を any に設定した TCP ルールで、flow または flowbits オプションが使用されている場合を除き、有効化された侵入ルールに指定されていないポートおよびアプリケーション プロトコルのすべてについて、TCP トラフィックを無視するように設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

TCP ポリシーごとに、以下のオプションを設定できます。

ネットワーク（Network）

TCP ストリーム再アセンブリ ポリシーを適用するホストの IP アドレスを指定します。

単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニター対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

ポリシー

TCP ポリシーを適用するターゲット ホスト（複数可）のオペレーティング システムを識別します。[Mac OS] 以外のポリシーを選択すると、システムは同期（SYN）パケットからデータを削除し、ルール 129:2 に対するイベントの生成を無効にします。インライン正規化プリプロセッサの [SYN に関するデータを削除（Remove Data on SYN）] オプションを有効にすると、ルール 129:2 も無効になることに注意してください。

以下の表に、オペレーティング システム ポリシーとそれを使用するホスト オペレーティング システムをリストします。

表 *2: TCP* オペレーティング システム ポリシー

ポリシー	オペレーティング システム
First	不明な OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 カーネル Linux 2.6 カーネル
Old Linux	Linux 2.2 以前のカーネル
Windows	Windows 98 Windows NT Windows 2000 Windows XP
Windows 2003	Windows 2003

ポリシー	オペレーティング システム
Windows Vista	Windows Vista
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 以降
HPUX 10	HP-UX 10.2 以前
Mac OS	Mac OS 10（Mac OS X）

ヒント First オペレーティング システム ポリシーは、ホストのオペレーティング システムが不明な場合にはある程度の保護対策になります。ただし、攻撃を見逃す可能性もあります。オペレーティング システムが既知であれば、ポリシーを編集して、その正しいオペレーティング システムを指定してください。

Timeout

侵入ルール エンジンが非アクティブなストリームを状態テーブルで保持する秒数（1 ～ 86400 秒）。指定された期間内にストリームが再アセンブルされない場合、侵入ルール エンジンはそのストリームを状態テーブルから削除します。

（注） ネットワーク トラフィックがデバイスの帯域幅制限に到達しやすいセグメントに、管理対象デバイスが展開されている場合は、処理のオーバーヘッド量を削減するために、この値を大きい値（たとえば、600 秒）に設定することを検討してください。

Threat Defense デバイスはこのオプションを無視します。その代りに高度なおアクセス制御の **Threat Defense サービス ポリシー**の設定を使用します。詳細については、サービス ポリシー ルールの設定を参照してください。

最大 TCP ウィンドウ（Maximum TCP Window）

受信側ホストで指定されている TCP ウィンドウの最大許容サイズを 1 ～ 1073725440 バイトの範囲で指定します。値を 0 に設定すると、TCP ウィンドウ サイズのチェックが無効になります。

⚠

注意 上限は RFC で許可される最大ウィンドウ サイズです。これは、攻撃者が検出を回避できないようにすることを目的としていますが、あまりにも大きな最大ウィンドウ サイズを設定すると、システム自体がサービス妨害を招く可能性があります。

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効になっている場合は、ルール 129:6 を有効にして、このオプションに対しイベントを生成し、インライン展開では、違反パケットをドロップします。 することができます。

オーバーラップ範囲（Overlap Limit）

セッションで許容するオーバーラップ セグメントの数を 0（無制限）～ 255 の範囲で指定します。セッションで、この指定された値に達すると、セグメントの再構成が停止します。[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされていて、それに付随するプリプロセッサ ルールが有効にされている場合、イベントも生成されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:7 を有効にします。

ファクタをフラッシュ（Flush Factor）

インライン展開では、ここで設定するサイズ減少なしのセグメントの数（1 ～ 2048）の後にサイズが減少したセグメントが検出されると、システムは検出用に累積されたセグメントデータをフラッシュします。値を 0 に設定すると、要求または応答の終わりを示す可能性のあるこのセグメントパターンの検出が無効になります。このオプションを有効にするには、インライン正規化の [TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にする必要があることに注意してください。

ステートフル インスペクションの異常（Stateful Inspection Anomalies）

TCP スタックの異常な動作を検出します。付随するプリプロセッサ ルールが有効にされている場合、TCP/IP スタックが不完全に作成されていると、多数のイベントが生成される可能性があります。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、次のルールを有効にすることができます：

- 129:1 ～ 129:5
- 129:6（Mac OS のみ）
- 129:8 ～ 129:11
- 129:13 ～ 129:19

次の点に注意してください。

- ルール 129:6 でトリガーするには、さらに [最大 TCP ウィンドウ（Maximum TCP Window）] に 0 より大きい値を設定する必要があります。
- ルール 129:9 および 129:10 でトリガーするには、さらに [TCP セッションのハイジャック（TCP Session Hijacking）] を有効にする必要があります。

TCP セッションのハイジャック（TCP Session Hijacking）

3 ウェイ ハンドシェイク中に TCP 接続の両端から検出されたハードウェア（MAC）アドレスの有効性を、セッションで受信した後続のパケットに照合して検査することにより、TCP セッション ハイジャックを検出します。[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされていて、2 つの対応するプリプロセッサ ルールのいずれかが有効にされている場合、接続のどちらかの側の MAC アドレスが一致しないと、システムがイベントを生成します。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションに対しイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、ルール 129:9 および 129:10 を有効にします。これらのルールのいずれかを使用してイベントを生成するには、[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] を有効にする必要があります。

連続した小型セグメント（Consecutive Small Segments）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされている場合、連続する小さな TCP セグメントの許容数を 1 ～ 2048 の範囲で指定します。値を 0 に設定すると、連続する小さな TCP セグメントのチェックが無効になります。

このオプションは、[小さなセグメント サイズ（Small Segment Size）] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。通常は、それぞれのセグメントの長さが 1 バイトであったとしても、ACK が介在することなく 2000 個もの連続するセグメントを受信することはないので注意してください。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:12 を有効にします。

小型セグメントのサイズ（Small Segment Size）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）] が有効にされている場合、小さいと見なされる TCP セグメントのサイズを 1 ～ 2048 バイトの範囲で指定します。値を 0 に設定すると、小さいセグメントのサイズの指定が無効になります。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

このオプションは、[連続する小さなセグメント（Consecutive Small Segments）] オプションと同時に設定し、両方とも無効にするか、両方にゼロ以外の値を設定する必要があります。2048 バイトの TCP セグメントは、標準的な 1500 バイトのイーサネット フレームより大きいことに注意してください。

小型セグメントを無視したポート（Ports Ignoring Small Segments）

[ステートフル インスペクションの異常（Stateful Inspection Anomalies）]、[連続する小さなセグメント（Consecutive Small Segments）]、および [小さなセグメント サイズ（Small Segment Size）] が有効になっている場合は、小さい TCP セグメントの検出を無視する 1 つ以上のポートのカンマ区切りリストを指定します。このオプションを空白のままにすると、ポートはすべて無視されないように指定されます。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

リストには任意のポートを追加できますが、このリストが適用されるのは、TCP ポリシーの [ストリーム再構成を実行（Perform Stream Reassembly on）] ポート リストに指定されているポートのみです。

TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）

TCP スリーウェイ ハンドシェイクの完了時に確立されたセッションだけを処理することを指定します。パフォーマンスを向上させ、SYN フラッド攻撃から保護し、部分的に非同期の環境での運用を可能にするには、このオプションを無効にします。確立された TCP セッションには含まれていない情報を送信して誤検出を発生させようとする攻撃を回避するには、このオプションを有効にします。

このオプションにイベントを生成し、インライン展開では、違反パケットをドロップします。するには、ルール 129:20 を有効にします。

3 ウェイ ハンドシェイク タイムアウト（3-Way Handshake Timeout）

[TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] が有効にされている場合、ハンドシェイクを完了するまでの時間制限を 0（無制限）～ 86400 秒（24 時間）の範囲で指定します。このオプションの値を変更するには、[TCP 3 ウェイ ハンドシェイク必須（Require TCP 3-Way Handshake）] を有効にする必要があります。

Firepower ソフトウェア デバイスと Threat Defense インライン、インラインタップ、およびパッシブ インターフェイスの場合、デフォルトは 0 です。Threat Defense のルーティッド インターフェイスおよびトランスペアレント インターフェイスの場合、タイムアウトは常に 30 秒であり、ここで設定した値は無視されます。

パケット サイズ パフォーマンスの向上（Packet Size Performance Boost）

再アセンブリ バッファで大きいパケットをキューに入れないようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。1 ～ 20 バイトの小さなパケットを使用した検出回避の試行から保護するには、このオプション

を無効にします。すべてのトラフィックが非常に大きなパケットからなるため、そのような攻撃は起こらないと確信できる場合は、このオプションを有効にします。

レガシー再構成（Legacy Reassembly）

パケットを再構成する際に、廃止されたストリーム4プリプロセッサをエミュレートするようにストリーム プリプロセッサを設定します。これにより、ストリーム プリプロセッサで再構成されたイベントを、ストリーム4プリプロセッサで再構成された、同じデータ ストリームに基づくイベントと比較できます。

非同期ネットワーク（Asynchronous Network）

モニター対象ネットワークが非同期ネットワーク（システムにトラフィックの半分だけが見えるネットワーク）であるかどうかを指定します。このオプションを有効にすると、システムはTCP ストリームを再構成しないため、パフォーマンスが向上します。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

クライアント ポートでのストリーム再構成の実行（Perform Stream Reassembly on Client Ports）

接続のクライアント側のポートに基づくストリームの再アセンブリを有効にします。つまり、Web サーバー、メール サーバー、または一般に $HOME_NET で指定された IP アドレスによって定義されたその他の IP アドレスを宛先とするストリームが再構成されます。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

クライアント サービスでのストリーム再構成の実行（Perform Stream Reassembly on Client Services）

接続のクライアント側のサービスに基づくストリームの再アセンブリを有効にします。不正なトラフィックがクライアントから発生する可能性がある場合は、このオプションを使用します。

選択するクライアント サービスごとに、1つ以上のクライアントディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。関連するクライアントアプリケーションに有効にされているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタをアプリケーションに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーションに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

サーバ ポートでのストリーム再構成の実行（Perform Stream Reassembly on Server Ports）

接続のサーバー側のポートに基づくストリームの再アセンブリのみを有効にします。つまり、Web サーバー、メール サーバー、または一般に $EXTERNAL_NET で指定された IP アドレスによって定義されたその他の IP アドレスから発信されたストリームが再構成されます。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

（注） サービスを徹底的に検査するには、Perform Stream Reassembly on Server Ports フィールドにポート番号を追加することに加えて、Perform Stream Reassembly on Server Services フィールドにサービス名を追加します。たとえば、HTTP サービスを検査するには、Perform Stream Reassembly on Server Ports フィールドにポート番号 80 を追加することに加えて、Perform Stream Reassembly on Server Services フィールドに **'HTTP'** サービスを追加します。

サーバー サービスでのストリーム再構成の実行（Perform Stream Reassembly on Server Services）

接続のサーバー側のサービスに基づくストリームの再アセンブリのみを有効にします。サーバ側の攻撃を監視する必要がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

1 つ以上のディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。サービスに有効にされているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタを関連するアプリケーション プロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーション プロトコルに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）

接続のクライアント側とサーバー側の両方のポートに基づくストリーム再構成を有効にします。同じポートで、不正なトラフィックがクライアントとサーバ間のいずれの方向でも移動する可能性がある場合は、このオプションを使用します。ポートを指定しないことによって、このオプションを無効にできます。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

両方のサービスでのストリーム再構成の実行（Perform Stream Reassembly on Both Services）

接続のクライアント側とサーバー側の両方のサービスに基づくストリーム再構成を有効にします。同じサービスで、不正なトラフィックがクライアントとサーバー間のいずれの方向でも移

動する可能性がある場合は、このオプションを使用します。サービスを指定しないことによって、このオプションを無効にできます。

1 つ以上のディテクタを有効にする必要があります。デフォルトでは、Cisco が提供するすべてのディテクタはアクティブになっています。関連するクライアントアプリケーションまたはアプリケーションプロトコルに対して有効になっているディレクタがない場合、システムは自動的に Cisco 提供のすべてのディテクタをアプリケーションまたはアプリケーションプロトコルに対して有効にします。そのようなディテクタが提供されていない場合は、最後に変更されたユーザ定義のディテクタをアプリケーションまたはアプリケーションプロトコルに対して有効にします。

この機能には、保護ライセンスと制御ライセンスが必要です。

このオプションは、Threat Defense ルーテッドおよびトランスペアレント インターフェイスでは無視されます。

トラブルシューティング オプション：最大キューイング バイト（Troubleshooting Options: Maximum Queued Bytes）

トラブルシューティングの電話中に、TCP接続の片側でキューイングできるデータの量を指定するようにサポートから依頼される場合があります。値 0 は、無制限のバイト数を指定します。

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

トラブルシューティングオプション：最大キューイング セグメント（Troubleshooting Options：Maximum Queued Segments）

トラブルシューティングの電話中に、TCP 接続の片側でキューイングできるデータ セグメントの最大バイト数を指定するようにサポートから依頼される場合があります。値0は、無制限のデータ セグメント バイト数を指定します。

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

関連トピック

ディテクタのアクティブ化と非アクティブ化
レイヤ管理
競合と変更：ネットワーク分析ポリシーと侵入ポリシー

TCP ストリームの前処理の設定

（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。

始める前に

- カスタム ターゲットベースのポリシーで指定するネットワークが一致しているか、または親のネットワーク分析ポリシーで処理されるネットワーク、ゾーン、および VLAN のサブセットであることを確認します。詳細については、ネットワーク分析プロファイルの詳細設定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）]**、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**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policies]**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 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 変更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）]（） 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 4 左側のナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 5 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] の下の [TCPストリームの構成（TCP Stream Configuration）] 設定が無効になっている場合は、[有効化（Enabled）] をクリックして有効にします。

ステップ 6 [TCPストリームの構成（TCP Stream Configuration）] の横にある **[編集（Edit）]**（） をクリックします。

ステップ 7 [グローバル設定（Global Settings）] セクションの [パケット タイプ パフォーマンス ブースト（Packet Type Performance Boost）] チェックボックスをオンまたはオフにします。

ステップ 8 次の操作を実行できます。

- [ターゲット（Targets）] セクションの [ホスト（Hosts）] の横にある **Add** () をクリックします。[ホスト アドレス（Host Address）] フィールドに 1 つまたは複数の IP アドレスを指定します。単一の IP アドレスまたはアドレス ブロックを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のターゲットベースのポリシーを作成できます。作業が完了したら [OK] をクリックします。

- 既存のターゲットベースのポリシーの編集：[ホスト（Hosts）]の下で、編集するポリシーのアドレスをクリックするか、またはデフォルトの構成値を編集します。
- TCP ストリームの前処理オプションの変更：TCP ストリームのプリプロセス オプション（31 ページ）を参照してください。

注意 サポートから指示がない限り、[最大キュー済みバイト（Maximum Queued Bytes）]または [最大キュー済みセグメント（Maximum Queued Segments）] を変更しないでください。

ヒント クライアント サービス、サーバー サービス、またはその両方に基づくストリームリアセンブル設定を変更するには、変更するフィールドの内側をクリックするか、そのフィールドの横にある [編集（Edit）] をクリックします。ポップアップウィンドウで矢印を使用して、サービスを [利用可能（Available）] リストと [有効化（Enabled）] リスト間で移動し、[OK] をクリックします。

- 既存のターゲットベースのポリシーの削除：削除するポリシーの横にある [削除（Delete）]（🗑） をクリックします。

ステップ 9 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（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、最後の確定後にキャッシュされた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、SMTP ストリーム プリプロセッサ ルール（GID 129）を有効にします。詳細については、「侵入ルール状態の設定」および「TCP ストリームのプリプロセス オプション （31 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。

関連トピック

レイヤ管理
競合と変更：ネットワーク分析ポリシーと侵入ポリシー

UDP ストリームの前処理

（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。

UDP ストリームの前処理が行われるのは、ルール エンジンがパケットを処理するために使用する UDP ルールに、以下の引数のいずれかを使用した `flow` キーワードが含まれる場合です。

- `Established`
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDPデータ ストリームは一般に、セッションという観点で考慮されません。UDPはコネクションレス型プロトコルであり、2つのエンドポイントが通信チャネルを確立してデータを交換し、チャネルを終了する手段は提供していません。ただし、ストリームプリプロセッサは、カプセル化 IP データグラム ヘッダーの送信元および宛先 IP アドレス フィールドと、UDP ヘッダーのポート フィールドを使用して、フローの方向を判断し、セッションを識別します。セッションが終了するのは、設定可能なタイマーの時間を超えた場合、または一方のエンドポイントで、もう一方のエンドポイントが到達不能、あるいは要求されたサービスが利用不可という内容の ICMP メッセージを受け取った場合です。

システムは UDP ストリームの前処理に関連するイベントを生成しないことに注意してください。ただし、関連するパケット デコーダ ルールを有効にすることで、UDP プロトコル ヘッダーの異常を検出することができます。

関連トピック

TCP ヘッダー値とストリーム サイズ

UDP ストリームのプリプロセス オプション

Timeout

プリプロセッサが非アクティブなストリームを状態テーブルに保持する秒数を指定します。指定した時間内に追加のデータグラムが現れなかった場合、プリプロセッサはそのストリームを状態テーブルから削除します。

Threat Defense デバイスはこのオプションを無視します。その代りに高度なおアクセス制御の **Threat Defense サービス ポリシー**の設定を使用します。詳細については、サービス ポリシー ルールの設定を参照してください。

パケット タイプ パフォーマンスの向上（Packet Type Performance Boost）

送信元および宛先ポートの両方を `any` に設定した UDP ルールで `flow` または `flowbits` オプションが使用されている場合を除き、有効化されたルールに指定されていないポートおよびアプリケーション プロトコルのすべてについて、UDP トラフィックを無視するようにプリプロセッサを設定します。このオプションはパフォーマンスを向上させますが、攻撃を見逃す可能性があります。

UDP ストリームの前処理の設定

（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。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（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**[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policies]**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 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）]（👁）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 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 [トランスポートまたはネットワーク レイヤ プリプロセッサ（Transport/Network Layer Preprocessors）] の下の [UDP ストリームの構成（UDP Stream Configuration）] 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 [UDPストリームの設定（UDP Stream Configuration）] の横にある**[編集（Edit）]**（✎）をクリックします。

ステップ 7 UDP ストリームのプリプロセス オプション （42 ページ）で説明されているオプションを設定します。

ステップ 8 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報（Policy Information）] をクリックし、[変更の確定（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、最後の確定後にキャッシュされた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、関連するパケット デコーダ ルール（GID 116）を有効にします。詳細については、「侵入ルール状態の設定」および「パケット デコーダ （22 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。

関連トピック

レイヤ管理

競合と変更：ネットワーク分析ポリシーと侵入ポリシー

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。