CHAPTER 29

トランスポート層およびネットワーク層の前処理の設定

ネットワーク分析ポリシー内のネットワーク層プリプロセッサでほとんどのトランスポートを設定します。これにより、侵入ポリシーで有効になっているルールを使った検査に向けてトラフィックが準備されます。詳細については、ネットワーク分析ポリシーおよび侵入ポリシーについて（23-1 ページ）を参照してください。

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。詳細については、カスタム ポリシーに関する制約事項（23-13 ページ）を参照してください。

注意 カスタム ユーザ ロールを持つ一部のユーザは、標準メニュー パス（[ポリシー（Policies）] > [アクセス制御（Access Control）] > [ネットワーク分析ポリシー（Network Analysis Policy）]）からネットワーク分析ポリシーにアクセスできません。これらのユーザは、侵入ポリシーを介してネットワーク分析ポリシーにアクセスできます（[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] > [ネットワーク分析ポリシー（Network Analysis Policy）]）。カスタム ユーザ ロールの詳細については、カスタム ユーザ ロールの管理（61-56 ページ）を参照してください。

ネットワーク分析ポリシーで設定したトランスポート層/ネットワーク層プリプロセッサの設定を VLAN、ゾーン、またはネットワークによって調整できます。一部のトランスポート層およびネットワーク層の設定はすべてのトラフィックにグローバルに適用され、アクセス コントロール ポリシーでこれらを設定します。

トランスポート/ネットワークの詳細設定の構成

ライセンス：Protection

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 ポリシーが適用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。

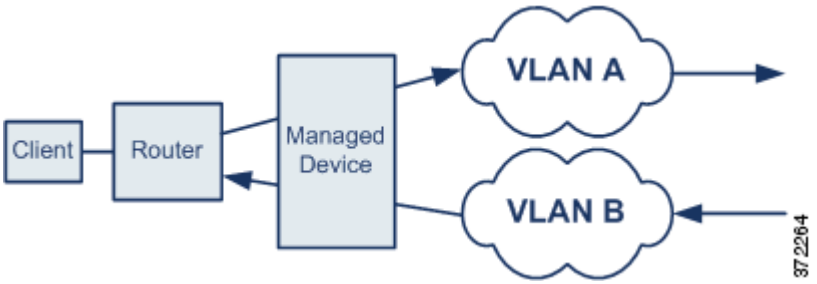
次の項では、これらの設定について説明します。

VLAN 見出しの無視

ライセンス：Protection

サポートされるデバイス：すべて（ASA FirePOWER を除く）

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、トラフィックの再アセンブリ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。



[接続を追跡するときに VLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）] を有効にすると、VLAN ヘッダーが無視されるので、展開に応じて適切にパケットを処理できます。

VLAN 見出しを無視するには、以下を行います。

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

手順 4　[転送またはネットワーク レイヤ プリプロセッサ設定（Transport/Network Layer Preprocessor Settings）] の横にある編集アイコン（）をクリックします。

[転送またはネットワーク レイヤ プリプロセッサ設定（Transport/Network Layer Preprocessor Settings）] ポップアップ ウィンドウが表示されます。

手順 5　次の選択肢があります。

- 展開されているデバイスが、異なる方向に流れるトラフィックで同じ接続に対して異なる VLAN タグを検出する可能性がある場合は、[接続を追跡するときに VLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）] チェック ボックスをオンにして、トラフィックを識別するときに VLAN ヘッダーを無視するようにします。
- 展開されているデバイスが、異なる方向に流れるトラフィックで同じ接続に対して異なる VLAN タグを検出する可能性がない場合は、[接続を追跡するときに VLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）] チェック ボックスをオフにして、トラフィックを識別するときに VLAN ヘッダーを考慮するようにします。

手順 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

侵入廃棄ルールでのアクティブ応答の開始

ライセンス：Protection

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。パッシブ展開の場合、システムがパケットをドロップすることはできません。また、セッションをブロックすることもありませんが、アクティブ応答を使用する場合はその限りではありません。

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 プリプロセッサがカプセル化 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別し、UDP セッションを識別する方法については、UDP ストリームの前処理の使用（29-35 ページ）で詳しく説明しています。

[最大アクティブ応答数（Maximum Active Responses）] オプションを設定することで、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ことができます。

インライン展開でアクティブ応答が有効にされている場合、システムは TCP 廃棄ルールへの応答として、トリガーしたパケットをドロップし、クライアントとサーバの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。システムはパッシブ展開でパケットをドロップできません。アクティブ応答がパッシブ展開で有効になっている場合、システムは TCP 接続のクライアント側とサーバ側の両方に TCP リセットを送信することによって TCP 廃棄ルールに応答します。インライン展開またはパッシブ展開でアクティブ応答が有効にされていると、システムはセッションの両端に ICMP 到達不能パケットを送信することによって UDP セッションを閉じます。リセットは接続やセッションに影響を与えるのに間に合うまでに到着する可能性が高いため、アクティブ応答はインライン展開で最も効果を発揮します。

[最大アクティブ応答数（Maximum Active Responses）] オプションの設定方法によっては、接続またはセッションのいずれかの側からさらにトラフィックが発生しているようであれば、システムが追加のアクティブ応答を開始することもできます。システムは、指定された間隔（秒数）で、指定された最大回数まで追加のアクティブ応答を開始します。

アクティブ応答の最大数を設定する方法については、TCP グローバル オプションの選択（29-24 ページ）を参照してください。

[最大アクティブ応答数（Maximum Active Responses）] の設定とは関係なく、**resp** または **react** ルールがトリガーされた場合にも、アクティブ応答が開始されることに注意してください。ただし、[最大アクティブ応答数（Maximum Active Responses）] は、廃棄ルールに対するアクティブ応答の最大数を制御するのと同じ方法で、**resp** および **react** ルールに対して追加のアクティブ応答をシステムが開始するかどうかを制御します。詳細については、ルール キーワードを使用したアクティブ応答の開始（36-93 ページ）を参照してください。

`config response` コマンドを使用して、使用するアクティブ応答インターフェイス、およびパッシブ展開で試行する TCP リセットの回数を設定することもできます。詳細については、アクティブ応答のリセット試行とインターフェイスの設定（36-95 ページ）を参照してください。

プリプロセッサ ルールは、次のオプションに関連付けられていません。

最大アクティブ応答数（Maximum Active Responses）

TCP 接続あたりのアクティブ応答の最大数を 1 ～ 25 の範囲で指定します。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、廃棄ルールによってトリガーされるアクティブ応答が無効になり、**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も無効になります。詳細については、侵入廃棄ルールでのアクティブ応答の開始（29-3 ページ）およびルール キーワードを使用したアクティブ応答の開始（36-93 ページ）を参照してください。

最小応答秒数（Minimum Response Seconds）

[最小応答秒数（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 1 ～ 300 秒の範囲で指定します。

廃棄ルールでのアクティブ応答の開始方法：

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

手順 4　[転送またはネットワーク レイヤ プリプロセッサ設定（Transport/Network Layer Preprocessor Settings）] の横にある編集アイコン（）をクリックします。

[転送またはネットワーク レイヤ プリプロセッサ設定（Transport/Network Layer Preprocessor Settings）] ポップアップ ウィンドウが表示されます。

手順 5　次の選択肢があります。

- TCP 接続 1 つあたりの [最大アクティブ応答数（Maximum Active Responses）] を 1 ～ 25 の値で指定します。0 を設定すると、廃棄ルールによってトリガーされるアクティブ応答が無効になり、**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も無効になります。
- [最大アクティブ応答数（Maximum Active Responses）] が発生するか、またはシステムがアクティブ応答を開始した接続で追加のトラフィックが次のアクティブ応答をもたらすまで待機する [最小応答秒数（Maximum Active Responses）] を 1 ～ 300 の値で指定します。

手順 6　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

トラブルシューティング：セッション終了メッセージのロギング

ライセンス：Protection

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。

セッション終了メッセージの記録方法：

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

手順 4　[転送またはネットワーク レイヤ プリプロセッサ設定（Transport/Network Layer Preprocessor Settings）] の横にある編集アイコン（）をクリックします。

[転送またはネットワーク レイヤ プリプロセッサ設定（Transport/Network Layer Preprocessor Settings）] ポップアップ ウィンドウが表示されます。

手順 5　[トラブルシューティング オプション（Troubleshooting Options）] を展開します。

手順 6　[セッション終了ロギングしきい値（Session Termination Logging Threshold）] にメッセージの記録を開始するバイト数を指定します。セッションが終了し、そのバイト数を超えている場合はメッセージが記録されます。

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

手順 7　[OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

チェックサムの検証

ライセンス：Protection

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。

チェックサム検証の設定方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択して [アクセス コントロール ポリシー（Access Control Policy）] ページを表示し、[ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。

[ネットワーク分析ポリシー（Network Analysis Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシーの編集（Edit Policy）] ページが表示されます。

手順 3　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。

[設定（Settings）] ページが表示されます。

手順 4　[トランスポートまたはネットワーク レイヤ プロセッサ（Transport/Network Layer Preprocessors）] で [チェックサム検証（Checksum Verification）] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[チェックサム検証（Checksum Verification）] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）を参照してください。

手順 5　[チェックサム検証（Checksum Verification）] セクションの以下のオプションはいずれも、パッシブまたはインライン展開では [有効（Enabled）] または [無効（Disabled）] に設定できます。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)] に設定することに加え、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)] も有効にする必要があることに注意してください。詳細については、インライン展開で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(26-6 ページ)を参照してください。また、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)] に設定すると、オプションを [有効(Enabled)] に設定した場合と同じ効果があることに注意してください。

手順 6　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

インライン トラフィックの正規化

ライセンス: Protection

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。ネットワーク分析ポリシーでインライン正規化プリプロセッサを有効にすると、システムは次の 2 つの状態をテストして、ユーザがインライン展開を使用していることを確認します。

- [インライン モード(Inline Mode)] がポリシーで有効になっている。インライン展開で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(26-6 ページ)を参照してください。
- インライン正規化が有効化されているアクセス コントロール ポリシーは、インライン セットを使用しているインライン展開されたデバイスに適用されます。

上記の両方の条件に一致した場合のみ、プリプロセッサは指定されたトラフィックを正規化します。

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。

ヒント　インライン展開の場合、シスコでは、インライン正規化プリプロセッサの設定で [TCP ペイロードの正規化(Normalize TCP Payload)] オプションを有効にすることを推奨しています。パッシブ展開の場合、シスコでは、適応型プロファイルを設定することを推奨しています。詳細については、パッシブ展開における前処理の調整(30-1 ページ)を参照してください。

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 1 ～ 255 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。

  デコーダ ルール カテゴリで以下のルールを有効にすると、このオプションに対するイベントを生成できます。
- 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イベントを生成するには、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イベントを生成するには、ルール 116:270 を有効にします。

  詳細については、パケットのデコードの設定（29-21 ページ）のパケット デコーダの [プロトコル ヘッダーの異常の検出（Detect Protocol Header Anomalies）] オプションを参照してください。

TTL のリセット（Reset TTL）

このオプションに設定した値 1 ～ 255 が [最小 TTL（Minimum TTL）] 値を上回る場合、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。このオプションを値 0 または [最小 TTL（Minimum TTL）] を下回る値に設定すると、オプションは無効になります。このフィールドが空白の場合、システムは値が 0 であると想定します。

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。このオプションが有効にされていて、[TTL のリセット（Reset TTL）] に設定された値が TTL 正規化を有効にしている場合、システムは必要に応じて TTL フィールドも正規化します。このオプションを有効にする場合、[フラグメント禁止ビットの正規化（Normalize Don't Fragment Bits）] および [リザーブド ビットの正規化（Normalize Reserved Bits）] オプションも有効にすることができます。

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。

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。

リザーブド ビットの正規化（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。

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、[TTL のリセット（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。

このオプションによって、ルール 129:2 のイベント生成も無効になります。

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。

回復不能な TCP ヘッダーの異常をブロック（Block Unrecoverable 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。詳細については、侵入イベントのパフォーマンス統計グラフの生成（41-5 ページ）を参照してください。

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。詳細については、TCP ポリシーのオプションの選択（29-26 ページ）を参照してください。

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。

最大セグメント サイズ（MSS）、ウィンドウ スケール、およびタイムスタンプ TCP のオプションは TCP パフォーマンスを最適化するために一般的に使用されるため、システムは、これらのオプションを常に許可します。システムは、[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、これらの一般的に使用されるオプションを正規化します。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）
エコー	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）

指定する内容	許可されるオプション
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
任意	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。

インライン正規化プリプロセッサの設定方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択して [アクセス コントロール ポリシー（Access Control Policy）] ページを表示し、[ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。

[ネットワーク分析ポリシー（Network Analysis Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシーの編集（Edit Policy）] ページが表示されます。

手順 3　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。

[設定（Settings）] ページが表示されます。

手順 4　[トランスポートまたはネットワーク レイヤ プロセッサ（Transport/Network Layer Preprocessors）] で [インライン正規化（Inline Normalization）] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[インライン正規化（Inline Normalization）] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）を参照してください。

手順 5　インライン トラフィックの正規化（29-7 ページ）で説明されている任意のオプションを設定できます。

手順 6　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

IP パケットの最適化

ライセンス：Protection

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 最適化プリプロセッサのルールにイベントを生成させるには、これらのルール（ジェネレータ ID（GID）が 123 のルール）を有効にする必要があります。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

詳細については、次の各項を参照してください。

- IP フラグメンテーションのエクスプロイトについて（29-13 ページ）
- ターゲットベースの最適化ポリシー（29-14 ページ）
- 最適化オプションの選択（29-15 ページ）
- IP 最適化の設定（29-17 ページ）

IP フラグメンテーションのエクスプロイトについて

ライセンス：Protection

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 最適化機能を酷使させるという方法でサービス妨害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。詳細については、ターゲットベースの最適化ポリシー（29-14 ページ）を参照してください。

適応型プロファイルを使用することで、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ができます。詳細については、パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

ターゲットベースの最適化ポリシー

ライセンス：Protection

ホストのオペレーティング システムは、パケットを再構成する際に優先するパケット フラグメントを判断するために、3 つの基準を使用します。それは、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フラグメントの距離（バイト単位））、オーバーラップ フラグメントとの相対開始位置および終了位置です。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。

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うちのいずれかを使用するように IP 最適化プリプロセッサを設定できます。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。

表 29-1　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
ファースト	Mac OS
	HP-UX
Linux	Linux
	OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

最適化オプションの選択

ライセンス：Protection

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。

[事前に割り当てられたフラグメント（Preallocated Fragments）] グローバル オプションを設定できます。

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。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-24 ページ）を参照してください。

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。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となる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、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）を参照してください。

ポリシー

モニタ対象ネットワーク セグメント上のホスト一式に使用する最適化ポリシー。7 つのポリシー（BSD、BSD-Right、First、Linux、Last、Solaris、Windows）の中から選択できます。これらのポリシーの詳細については、ターゲットベースの最適化ポリシー（29-14 ページ）を参照してください。

タイムアウト（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（Minimum 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。

このオプションのイベントを生成するには、ルール 123:1 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

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。

以下のルールを有効にすることで、このオプションに対するイベントを生成できます。

- 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）

セッションで最適化を停止する条件とする、セッションでのオーバーラップ セグメントの検出数を 0（無制限）～ 255 の範囲で指定します。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。

このオプションのイベントを生成するには、ルール 123:12 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

最小フラグメント サイズ（Minimum Fragment Size）

パケットを不正と見なす条件とする、検出されたフラグメント（最後のフラグメントを除く）の最小サイズを 0（無制限）～ 255 バイトの間で指定します。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。

このオプションのイベントを生成するには、ルール 123:13 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

IP 最適化の設定

ライセンス：Protection

IP 最適化プリプロセッサを設定するには、次の手順を実行します。IP 最適化プリプロセッサの設定オプションの詳細については、最適化オプションの選択（29-15 ページ）を参照してください。

IP 最適化の設定方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択して [アクセス コントロール ポリシー（Access Control Policy）] ページを表示し、[ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。

[ネットワーク分析ポリシー（Network Analysis Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシーの編集（Edit Policy）] ページが表示されます。

手順 3　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。

[設定（Settings）] ページが表示されます。

手順 4　[トランスポートまたはネットワーク レイヤ プロセッサ（Transport/Network Layer Preprocessors）] で [IP 最適化（IP Defragmentation）] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[IP 最適化（IP Defragmentation）] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）を参照してください。

手順 5　必要に応じて、[グローバル設定（Global Settings）] ページ領域にある [事前に割り当てられたフラグメント（Preallocated Fragments）] の設定を変更できます。

手順 6　次の 2 つの対処法があります。

- 新しいターゲットベースのポリシーを追加します。ページの左側で [サーバ（Servers）] の横にある追加アイコン（ ）をクリックします。[ターゲットの追加（Add Target）] ポップアップ ウィンドウが表示されます。[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、[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。FireSIGHT システムで IP アドレス ブロックを使用する方法については、IP アドレスの表記規則（1-24 ページ）を参照してください。

ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となる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、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）を参照してください。

ページの左側にあるターゲットのリストに新しいエントリが表示されます。このエントリは、強調表示によって選択された状態であることが示されます。また、[設定（Configuration）] セクションが更新されて、追加したポリシーの現在の構成が反映されます。

- 既存のターゲットベースのポリシーの設定を変更します。ページの左側の [ホスト（Hosts）] に追加されているポリシーの設定済み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。

  選択したエントリが強調表示され、[設定（Configuration）] セクションが更新されて、選択したポリシーの現在の設定が表示されます。既存のターゲットベースのポリシーを削除するには、削除するポリシーの横にある削除アイコン（ ）をクリックします。

手順 7　オプションで、[設定（Configuration）] ページ領域にあるオプションのいずれかを変更できます。

手順 8　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

パケットのデコードについて

ライセンス：Protection

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。

注意すべき点として、パケット デコーダのルールにイベントを生成させるには、これらのルール（ジェネレータ ID（GID）が 116 のルール）を有効にする必要があります。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

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。詳細については、定義済みのデフォルトの変数の最適化（3-20 ページ）を参照してください。

このオプションのイベントを生成するには、ルール 116:297 および 116:298 を有効にします。

非標準ポートでの Teredo の検出（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 ヘッダー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 つ目の 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。詳細については、「侵入ポリシー内のルールのフィルタリング（32-11 ページ）」と「ルール状態の設定（32-23 ページ）」を参照してください。

過剰な長さの値の検出（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。

このオプションのイベントを生成するには、ルール 116:6、116:47、116:97、および 116:275 を有効にします。

無効な IP オプションの検出（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。

このオプションのイベントを生成するには、ルール 116:4 および 116:5 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

試験的な TCP オプションの検出（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）
14	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））
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。

このオプションのイベントを生成するには、ルール 116:58 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

廃止された TCP オプションの検出（Detect Obsolete TCP Options）

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）

このオプションのイベントを生成するには、ルール 116:57 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

T/TCP の検出（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。

このオプションのイベントを生成するには、ルール 116:56 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

その他の TCP オプションの検出（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。

このオプションのイベントを生成するには、ルール 116:54、116:55、および 116:59 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

プロトコル ヘッダー異常の検出（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。

このオプションに対するイベントを生成するには、他のパケット デコーダ オプションに明示的に関連付けられていないパケット デコーダのルールを有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

異常な IPv6 トラフィックによってトリガーされるイベントを生成するルールは、116:270 ～ 116:274、116:275 ～ 116:283、116:291、116:292、116:295、116:296、116:406、116:458、116:460、116:461 です。

インライン正規化プリプロセッサの [最小 TTL（Minimum TTL）] オプションに関連する以下のルールについても注意してください。

- 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イベントを生成するには、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イベントを生成するには、ルール 116:270 を有効にします。

詳細については、インライン トラフィックの正規化（29-7 ページ）のインライン正規化の [最小 TTL（Minimum TTL）] オプションを参照してください。

パケットのデコードの設定

ライセンス：Protection

パケットのデコードは、[パケット デコーディング（Packet Decoding）] 設定ページで設定できます。パケットのデコード設定オプションの詳細については、パケットのデコードについて（29-18 ページ）を参照してください。

パケットのデコードの設定方法:

アクセス: Admin/Intrusion Admin

手順 1　[ポリシー(Policies)] > [アクセス制御(Access Control)] を選択して [アクセス コントロール ポリシー(Access Control Policy)] ページを表示し、[ネットワーク分析ポリシー(Network Analysis Policy)] をクリックします。

[ネットワーク分析ポリシー(Network Analysis Policy)] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

[ポリシーの編集(Edit Policy)] ページが表示されます。

手順 3　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。

[設定(Settings)] ページが表示されます。

手順 4　[トランスポートまたはネットワーク レイヤ プロセッサ(Transport/Network Layer Preprocessors)] で [パケット デコーディング(Packet Decoding)] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[パケット デコーディング(Packet Decoding)] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

手順 5　[パケット デコーディング(Packet Decoding)] ページの任意の検出オプションを有効または無効にできます。詳細については、パケットのデコードについて(29-18 ページ)を参照してください。

手順 6　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

TCP ストリームの前処理の使用

ライセンス: Protection

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。

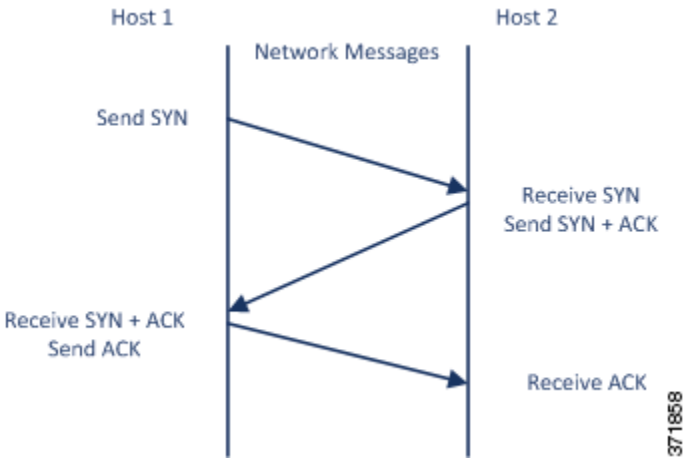
TCP ストリーム プリプロセッサのルールにイベントを生成させるには、それらのルール(ジェネレータ ID(GID)が 129 のルール)を有効にする必要があります。詳細については、ルール状態の設定(32-23 ページ)を参照してください。

詳細については、次の各項を参照してください。

状態関連の TCP エクスプロイトについて

ライセンス：Protection

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 セッションの一部であるトラフィックだけが評価されます。以下の図に、3 ウェイ ハンドシェイクを示します。



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。

TCP グローバル オプションの選択

ライセンス: Protection

TCP ストリーム プリプロセッサには、TCP ストリーム プリプロセッサの動作を制御するグローバル オプションが 1 つあります。

プリプロセッサ ルールは、このオプションに関連付けられていません。

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。

ターゲットベースの TCP ポリシーについて

ライセンス: Protection

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、CIDR ブロック、またはプレフィックス長を指定する必要はありません。

適応型プロファイルを使用することで、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ができます。詳細については、パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

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 29-2　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
ファースト	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
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。

TCP ポリシーのオプションの選択

ライセンス：Protection

以下に、ストリーム プリプロセッサの検査対象とする TCP トラフィックを識別して制御するために設定できるオプションをリストし、説明します。

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。

ネットワーク（Network）

TCP ストリーム再構成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。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-24 ページ）を参照してください。

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。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となる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、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）を参照してください。

ポリシー（Policy）

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。

詳細については、ターゲットベースの TCP ポリシーについて（29-24 ページ）を参照してください。

タイムアウト（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構成されない場合、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。

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。

このオプションのイベントを生成するには、ルール 129:6 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

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。

このオプションのイベントを生成するには、ルール 129:7 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

フラッシュ ファクタ（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。詳細については、インライン トラフィックの正規化（29-7 ページ）を参照してください。

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。

以下のルールを有効にすることで、このオプションに対するイベントを生成できます。

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

詳細については、ルール状態の設定（32-23 ページ）を参照してください。

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。

このオプションのイベントを生成するには、ルール 129:9 および 129:10 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

連続する小さなセグメント（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。

このオプションのイベントを生成するには、ルール 129:12 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

小さなセグメント 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、[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。

小さなセグメントを無視するポート（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）] が有効にされている場合、必要に応じて、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。

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。

このオプションのイベントを生成するには、ルール 129:20 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

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。

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

再構成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。

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

ストリーム プリプロセッサの再構成対象とするトラフィックを識別するクライアント ポート、サーバ ポート、またはその両方のカンマ区切りリストを指定します。ストリーム再構成のオプションの選択（29-30 ページ）を参照してください。

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

ストリーム プリプロセッサの再構成対象とするトラフィックで識別するクライアント サービス、サーバ サービス、またはその両方のサービスを指定します。ストリーム再構成のオプションの選択（29-30 ページ）を参照してください。

トラブルシューティング オプション：最大キューイング 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。

TCP ストリームの再構成

ライセンス：Protection

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。

詳細については、次の各項を参照してください。

- ストリームベースの攻撃について（29-30 ページ）
- ストリーム再構成のオプションの選択（29-30 ページ）

ストリームベースの攻撃について

ライセンス：Protection

ストリーム再構成により、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 エンジンの再構成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 サーバ上のトラフィックをモニタする際に、独自の Web サーバ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。

ストリーム再構成のオプションの選択

ライセンス：Protection

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。適応型プロファイル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。適応型プロファイルを有効にして使用する方法については、パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

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 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、適応型プロファイル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 ポートとして、21 を指定
- サーバ 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、シスコではポートを 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、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。

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。

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構成を有効にします。つまり、Web サーバ、メール サーバ、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。

クライアント サービスでのストリーム最高性の実行（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再構成を有効にします。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、少なくとも 1 つのクライアント ディテクタを有効にする必要があります（ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照）。デフォルトでは、シスコ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シスコ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、Protection および Control ライセンスが必要です。

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）

接続のサーバ側のポートに基づくストリーム再構成のみを有効にします。つまり、Web サーバ、メール サーバ、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。

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

接続のサーバ側のサービスに基づくストリーム再構成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。

選択するサービスごとに、少なくとも 1 つのディテクタを有効にする必要があります（ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照）。デフォルトでは、シスコ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シスコ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、Protection および Control ライセンスが必要です。

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。

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。

選択するサービスごとに、少なくとも 1 つのディテクタを有効にする必要があります（ディテクタのアクティブ化と非アクティブ化（46-30 ページ）を参照）。デフォルトでは、シスコ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シスコ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、Protection および Control ライセンスが必要です。

TCP ストリームの前処理の設定

ライセンス：Protection

TCP ポリシーを含め、TCP ストリームの前処理を設定できます。TCP ストリーム プリプロセッサの設定オプションの詳細については、TCP ポリシーのオプションの選択（29-26 ページ）を参照してください。

TCP セッションを追跡するストリーム プリプロセッサを設定する方法:

アクセス: Admin/Intrusion Admin

手順 1　[ポリシー(Policies)] > [アクセス制御(Access Control)] を選択して [アクセス コントロール ポリシー(Access Control Policy)] ページを表示し、[ネットワーク分析ポリシー(Network Analysis Policy)] をクリックします。

[ネットワーク分析ポリシー(Network Analysis Policy)] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

[ポリシーの編集(Edit Policy)] ページが表示されます。

手順 3　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。

[設定(Settings)] ページが表示されます。

手順 4　[トランスポートまたはネットワーク レイヤ プロセッサ(Transport/Network Layer Preprocessors)] で [TCP ストリームの構成(TCP Stream Configuration)] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集(Edit)] をクリックします。
- 設定が無効である場合、[有効(Enabled)] をクリックし、[編集(Edit)] をクリックします。

[TCP ストリームの構成(TCP Stream Configuration)] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(24-1 ページ)を参照してください。

手順 5　必要に応じて、[グローバル設定(Global Settings)] の下にある [パケット タイプ パフォーマンスの向上(Packet Type Performance Boost)] を変更します。詳細については、TCP グローバル オプションの選択(29-24 ページ)を参照してください。

手順 6　次の 2 つの対処法があります。

- 新しいターゲットベースのポリシーを追加します。ページの左側の [ホスト(Hosts)] の横にある追加アイコン( )をクリックします。[ターゲットの追加(Add Target)] ポップアップ ウィンドウが表示されます。[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、[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。FireSIGHT システムで IP アドレス ブロックを使用する方法については、IP アドレスの表記規則(1-24 ページ)を参照してください。

  ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となる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、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ(25-3 ページ)を参照してください。

  ページの左側にあるターゲットのリストに新しいエントリが表示されます。このエントリは、強調表示によって選択された状態であることが示されます。また、[設定(Configuration)] セクションが更新されて、追加したポリシーの現在の構成が反映されます。

- 既存のターゲットベースのポリシーの設定を変更します。ページの左側の [ホスト(Hosts)] に追加されているポリシーの設定済み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。

選択したエントリが強調表示され、[設定（Configuration）] セクションが更新されて、選択したポリシーの現在の設定が表示されます。既存のターゲットベースのポリシーを削除するには、削除するポリシーの横にある削除アイコン（ ）をクリックします。

手順 7　必要に応じて、[設定（Configuration）] にある任意の TCP ポリシー オプションを変更します。

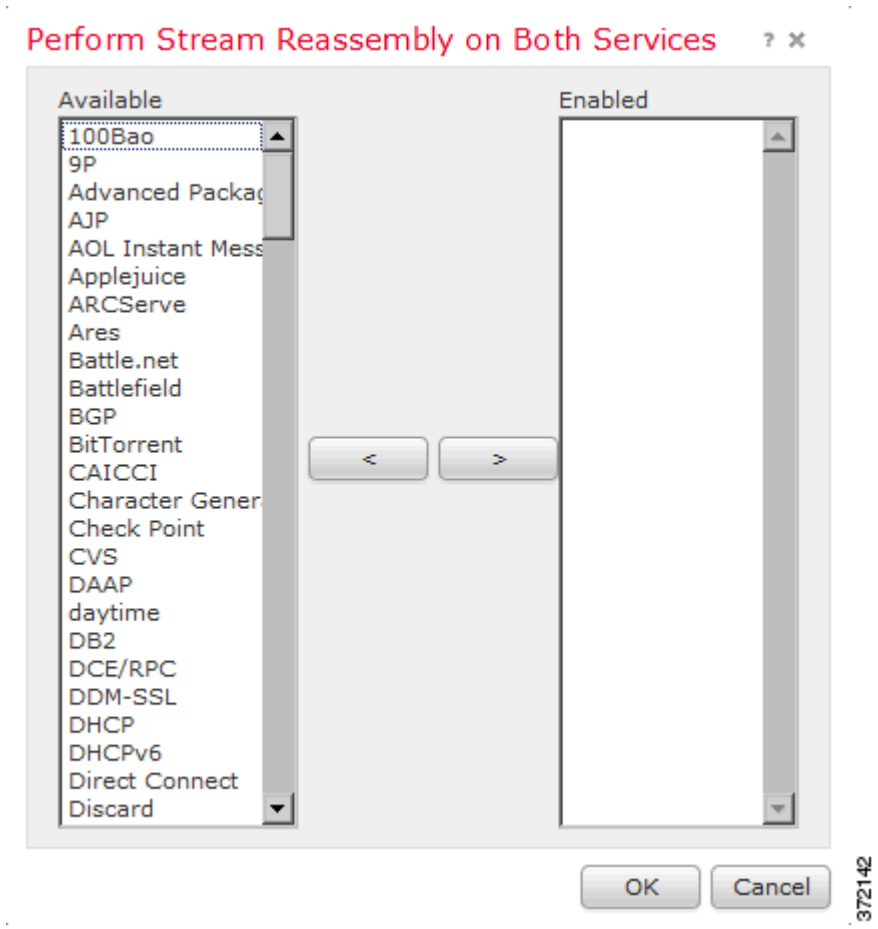
クライアント サービス、サーバ サービス、またはその両方に基づくストリーム再構成の設定を変更するには、ステップ 8 に進みます。そうでない場合は、ステップ 11 に進みます。

詳細については、TCP ポリシーのオプションの選択（29-26 ページ）およびストリーム再構成のオプションの選択（29-30 ページ）を参照してください。

手順 8　クライアント サービス、サーバ サービス、またはその両方に基づくストリーム再構成の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。

選択したフィールドのポップアップ ウィンドウが表示されます。

たとえば、次の図は、[両サービスでのストリーム再構成の実行（Perform Stream Reassembly on Both Services）] ポップアップ ウィンドウを示しています。



適応型プロファイルを有効にすることで、ネットワークで検出されたサービスに基づいてストリーム プリプロセッサが再構成するトラフィックをモニタできます。詳細については、サーバの使用（50-39 ページ）と パッシブ展開における前処理の調整（30-1 ページ）を参照してください。

手順 9　次の 2 つの選択肢があります。

- モニタするサービスを追加するには、左側の [選択可能（Available）] リストで 1 つまたは複数のサービスを選択してから、右矢印（>）ボタンをクリックします。
- サービスを削除するには、右側の [有効（Enabled）] リストで削除するサービスを選択してから、左矢印（<）ボタンをクリックします。

複数のサービス ディテクタを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。また、クリック アンド ドラッグ操作で、複数の隣接するサービス ディテクタを選択することもできます。

手順 10　[OK] をクリックして、選択した項目を追加します。

[TCP ストリームの構成（TCP Stream Configuration）] ページが表示され、サービスが更新されます。

手順 11　任意で、サポートによって求められた場合にのみ、[トラブルシューティング オプション（Troubleshooting Options）] を展開し、TCP ストリーム前処理ポリシー設定のいずれかを変更します。詳細については、TCP ポリシーのオプションの選択（29-26 ページ）を参照してください。

手順 12　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

UDP ストリームの前処理の使用

ライセンス：Protection

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（TCP または UDP クライアントまたはサーバ フローへのルールの適用（36-57 ページ）を参照）が含まれる場合です。

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

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。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。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。セッションは、設定可能なタイマーが超過したとき、または他のエンドポイントが到達不能であるか要求されたサービスが使用不可であるという ICMP メッセージをエンドポイントが受信したときに終了します。

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。パケット デコーダによって生成されるイベントについては、パケットのデコードについて（29-18 ページ）を参照してください。

UDP ストリームの前処理の設定

ライセンス：Protection

UDP ストリームの前処理を設定できます。

UDP セッションを追跡するストリーム プリプロセッサを設定する方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択して [アクセス コントロール ポリシー（Access Control Policy）] ページを表示し、[ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。

[ネットワーク分析ポリシー（Network Analysis Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシーの編集（Edit Policy）] ページが表示されます。

手順 3　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。

[設定（Settings）] ページが表示されます。

手順 4　[トランスポートまたはネットワーク レイヤ プロセッサ（Transport/Network Layer Preprocessors）] で [UDP ストリームの構成（UDP Stream Configuration）] が有効にされているかどうかによって、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[UDP ストリームの構成（UDP Stream Configuration）] ページが表示されます。ページ下部のメッセージは、設定を含むポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）を参照してください。

手順 5　必要に応じて、[タイムアウト（Timeout）] 値を設定し、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期間を 1 ～ 86400 秒の範囲で指定します。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。

手順 6　必要に応じて、[パケット タイプ パフォーマンスの向上（Packet Type Performance Boost）] を選択し、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。

手順 7　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。
