CHAPTER 27

高度なファイアウォール保護の設定

この章では、保護機能を設定することによってネットワーク攻撃を防止する方法を説明します。この章には、次の項があります。

- 「脅威検出の設定」（P.27-1）
- 「接続の設定」（P.27-6）
- 「IP 監査の設定」（P.27-10）
- 「フラグメント サイズの設定」（P.27-18）
- 「Anti-Spoofing の設定」（P.27-20）
- 「TCP オプションの設定」（P.27-21）
- 「グローバル タイムアウトの設定」（P.27-23）

（注） [Configuration] > [Firewall] > [Advanced] 領域で設定する、Sun RPC サーバと暗号化トラフィック検査の設定値（およびこの章に含まれる多くの項目）については、第 24 章「アプリケーション レイヤ プロトコル インスペクションの設定」を参照してください。

脅威検出の設定

この項では、スキャン脅威検出と基本脅威検出を設定する方法について説明します。説明する内容は次のとおりです。脅威検出はシングル モードだけで使用できます。

この項では、次のトピックについて取り上げます。

- 「基本脅威検出の設定」（P.27-1）
- 「スキャン脅威検出の設定」（P.27-3）
- 「脅威統計情報の設定」（P.27-4）
- 「[Threat Detection] フィールドの説明」（P.27-5）

脅威検出の統計情報を表示するには、「[Firewall Dashboard] タブ」（P.1-17）を参照してください。

基本脅威検出の設定

基本脅威検出では、DoS 攻撃のような攻撃に関連している可能性があるアクティビティを検出します。基本脅威検出は、デフォルトでイネーブルになっています。

この項では、次のトピックについて取り上げます。

- 「基本脅威検出の概要」（P.27-2）
- 「基本脅威検出の設定」（P.27-2）

基本脅威検出の概要

セキュリティ アプライアンスは、基本脅威検出を使用して、次の理由でドロップしたパケットおよびセキュリティ イベントの割合を監視します。

- アクセス リストによる拒否
- 不正なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）
- 接続制限の超過（システム全体のリソース制限とコンフィギュレーションで設定されている制限の両方）
- DoS 攻撃の検出（無効な SPI、ステートフル ファイアウォール検査の不合格など）
- 基本ファイアウォール検査の不合格（このオプションは、ここに列挙されているファイアウォール関連のパケット ドロップすべてを含む総合レートです。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません）
- 疑わしい ICMP パケットの検出
- アプリケーション インスペクションに不合格のパケット
- インターフェイスの過負荷
- 検出されたスキャン攻撃（このオプションでは、スキャン攻撃をモニタします。たとえば、最初の TCP パケットが SYN パケットでないことや、TCP 接続で 3 ウェイ ハンドシェイクに失敗することなどです。フル スキャン脅威検出（「スキャン脅威検出の設定」（P.27-3）を参照）では、このスキャン攻撃レート情報を収集し、ホストを攻撃者として分類して自動的に排除することによって対処します）
- 不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）

セキュリティ アプライアンスは、脅威を検出するとただちにシステム ログ メッセージ（730100）を送信します。

基本脅威検出は、ドロップや潜在的な脅威があった場合に限りパフォーマンスに影響を与えます。この状況でも、パフォーマンスへの影響は大きくありません。

基本脅威検出の設定

基本脅威検出をイネーブルまたはディセーブルにするには、[Configuration] > [Firewall] > [Threat Detection] ペインで、[Enable Basic Threat Detection] チェックボックスをオンまたはオフにします。

このオプションはデフォルトで、パケット ドロップや不完全なセッションの検出など、特定のタイプのセキュリティ イベントの検出をイネーブルにします。必要に応じて、各イベント タイプのデフォルト設定を上書きできます。

イベント レートが超過すると、セキュリティ アプライアンスはシステム メッセージを送信します。セキュリティ アプライアンスは、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト レート間隔は、平均レート間隔の 1/60 と 10 秒のうち、いずれか大きいほうです。セキュリティ アプライアンスは、受信するイベントごとに平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、セキュリティ アプライアンスは、バースト期間におけるレート タイプごとに最大 1 つのメッセージの割合で 2 つの別々のシステム メッセージを送信します。

表 27-1 に、デフォルト設定を示します。

表 27-1　基本脅威検出のデフォルト設定

パケット ドロップの理由	トリガー設定	
	平均レート	バースト レート
• DoS 攻撃の検出 • 不正なパケット形式 • 接続制限の超過 • 疑わしい ICMP パケットの検出	直前の 600 秒間で 100 ドロップ/秒。	直前の 10 秒間で 400 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 320 秒間で 60 ドロップ/秒。
スキャン攻撃の検出	直前の 600 秒間で 5 ドロップ/秒。	直前の 10 秒間で 10 ドロップ/秒。
	直前の 3600 秒間で 4 ドロップ/秒。	直近の 60 秒間で 8 ドロップ/秒。
不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）（複合）	直前の 600 秒間で 100 ドロップ/秒。	直前の 10 秒間で 200 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 60 秒間で 160 ドロップ/秒。
アクセス リストによる拒否	直前の 600 秒間で 400 ドロップ/秒。	直前の 10 秒間で 800 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 60 秒間で 640 ドロップ/秒。
• 基本ファイアウォール検査に不合格 • アプリケーション インスペクションに不合格のパケット	直前の 600 秒間で 400 ドロップ/秒。	直前の 10 秒間で 1600 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 60 秒間で 1280 ドロップ/秒。
インターフェイスの過負荷	直前の 600 秒間で 2000 ドロップ/秒。	直前の 10 秒間で 8000 ドロップ/秒。
	直前の 3600 秒間で 1600 ドロップ/秒。	直近の 60 秒間で 6400 ドロップ/秒。

スキャン脅威検出の設定

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、セキュリティ アプライアンス のスキャンによる脅威の検出機能では、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、アクティビティを返さない接続、閉じられているサービス ポートへのアクセス、非ランダム IPID などの脆弱な TCP の動作、およびその他の疑わしいアクティビティを追跡します。

攻撃者に関するシステム ログ メッセージを送信するように セキュリティ アプライアンス を設定したり、自動的にホストを排除したりできます。

注意　スキャン脅威検出機能は、ホストベースとサブネットベースのデータ構造と情報を作成および収集する間、セキュリティ アプライアンスのパフォーマンスとメモリに大きな影響を与える可能性があります。

スキャン脅威検出を設定するには、次の手順を実行します。

ステップ 1　スキャン脅威検出をイネーブルにするには、[Configuration] > [Firewall] > [Threat Detection] ペインで、[Enable Scanning Threat Detection] チェックボックスをオンにします。

デフォルトでは、ホストが攻撃者として識別されると、システム ログ メッセージ 730101 が生成されます。

セキュリティ アプライアンスは、スキャン脅威レートが超過すると、ホストを攻撃者またはターゲットとして特定します。セキュリティ アプライアンスは、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト イベント レートは、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の値です。スキャン攻撃の一部と見なされるイベントが検出されるたびに、セキュリティ アプライアンスは平均レート制限とバースト レート制限をチェックします。ホストから送信されるトラフィックがどちらかのレートを超えると、そのホストは攻撃者と見なされます。ホストが受信したトラフィックがどちらかのレートを超えると、そのホストはターゲットと見なされます。

表 27-2 に、スキャン脅威検出のデフォルトのレート制限を示します。

表 27-2　スキャンによる脅威の検出のデフォルトのレート制限

平均レート	バースト レート
直前の 600 秒間で 5 ドロップ/秒。	直前の 10 秒間で 10 ドロップ/秒。
直前の 3600 秒間で 5 ドロップ/秒。	直前の 60 秒間で 10 ドロップ/秒。

ステップ 2　（任意）ホストが セキュリティ アプライアンス によって攻撃者と判定された場合に自動的にそのホスト接続を終了するには、[Shun Hosts detected by scanning threat] チェックボックスをオンにします。

ステップ 3　（任意）ホストの IP アドレスを排除対象から外すには、[Networks excluded from shun] フィールドにアドレスを入力します。

複数のアドレスまたはサブネットは、カンマで区切って入力できます。IP アドレス オブジェクトのリストからネットワークを選択するには、[...] ボタンをクリックします。

脅威統計情報の設定

広範な統計情報を収集するようにセキュリティ アプライアンスを設定することができます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。デフォルトでは、アクセス リストの統計情報はイネーブルになっています。

脅威検出の統計情報を表示するには、「[Firewall Dashboard] タブ」（P.1-17）を参照してください。

注意　統計情報をイネーブルにすると、イネーブルにする統計情報のタイプに応じて、セキュリティ アプライアンスのパフォーマンスが影響を受けます。ホストの統計情報をイネーブルにすると、パフォーマンスに大きな影響があります。トラフィックの負荷が高い場合は、このタイプの統計情報は一時的にイネーブルにすることを検討してください。ポートの統計情報をイネーブルにしても影響はそれほどありません。

- すべての統計情報をイネーブルにするには、[Configuration] > [Firewall] > [Threat Detection] ペインで、[Enable All Statistics] オプション ボタンをオンにします。
- すべての統計情報をディセーブルにするには、[Configuration] > [Firewall] > [Threat Detection] ペインで、[Disable All Statistics] オプション ボタンをオンにします。
- 特定の統計情報だけをイネーブルにするには、[Configuration] > [Firewall] > [Threat Detection] ペインで、[Enable Only Following Statistics] オプション ボタンをオンにし、次のチェックボックスの中から 1 つ以上をオンにします。
  - [Hosts] : ホスト統計情報をイネーブルにします。ホストがアクティブで、スキャン脅威ホスト データベース内に存在する限り、ホスト統計情報は累積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます（統計情報もクリアされます）。
  - [Access Rules]（デフォルトでイネーブル）：アクセス ルールの統計情報をイネーブルにします。
  - [Port]：TCP/UDP ポートの統計情報をイネーブルにします。
  - [Protocol]：TCP/UDP 以外の IP プロトコルの統計情報をイネーブルにします。

[Threat Detection] フィールドの説明

[Threat Detection] ペインでは、基本脅威検出およびスキャン脅威検出を設定できます。

フィールド

- [Basic Threat Detection]：基本脅威検出では、DoS 攻撃のような攻撃に関連している可能性があるアクティビティを検出します。基本脅威検出は、デフォルトでイネーブルになっています。
  - [Enable Basic Threat Detection]：基本脅威検出をイネーブルにします。詳細については、「基本脅威検出の設定」（P.27-1）を参照してください。
- [Scanning Threat Detection]：スキャン脅威検出機能は、いつホストがスキャンを実行するかを決定します。
  - [Enable Scanning Threat Detection]：スキャン脅威検出をイネーブルにします。詳細については、「スキャン脅威検出の設定」（P.27-3）を参照してください。
  - [Shun Hosts detected by scanning threat] : セキュリティ アプライアンスがホストを攻撃者として識別すると自動的にホスト接続を終了します。

    [Networks excluded from shun]：ホスト IP アドレスを回避対象から除外します。複数のアドレスまたはサブネットは、カンマで区切って入力できます。IP アドレス オブジェクトのリストからネットワークを選択するには、[...] ボタンをクリックします。
- [Scanning Threat Statistics]：セキュリティ アプライアンスが広範な統計情報を収集できるようにします。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。デフォルトでは、アクセス リストの統計情報はイネーブルになっています。脅威検出の統計情報を表示するには、「[Firewall Dashboard] タブ」（P.1-17）を参照してください。

注意 統計情報をイネーブルにすると、イネーブルにする統計情報のタイプに応じて、セキュリティ アプライアンスのパフォーマンスが影響を受けます。ホストの統計情報をイネーブルにすると、パフォーマンスに大きな影響があります。トラフィックの負荷が高い場合は、このタイプの統計情報は一時的にイネーブルにすることを検討してください。ポートの統計情報をイネーブルにしても影響はそれほどありません。

- [Disable All Statistics]：すべての統計情報をディセーブルにします。
- [Enable All Statistics]：すべての統計情報をイネーブルにします。
- [Enable only following statistics]：特定の統計情報をイネーブルにします。

  [Hosts]：ホスト統計情報をイネーブルにします。ホストがアクティブで、スキャン脅威ホスト データベース内に存在する限り、ホスト統計情報は累積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます（統計情報もクリアされます）。

  [Access Rules]（デフォルトでイネーブル）：アクセス ルールの統計情報をイネーブルにします。

  [Port]：TCP/UDP ポートの統計情報をイネーブルにします。

  [Protocol]：TCP/UDP 以外の IP プロトコルの統計情報をイネーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

接続の設定

この項では、TCP と UDP の最大接続数、最大初期接続数、クライアントあたりの最大接続数、接続タイムアウト、デッド接続検出を設定する方法、および TCP シーケンスのランダム化をディセーブルにする方法について説明します。この項では、TCP 正規化を設定する方法についても説明します。TCP 正規化によって、異常なパケットを識別する基準を指定できます。セキュリティ アプライアンスは、異常なパケットが検出されるとそれらをドロップします。

この項では、次のトピックについて取り上げます。

- 「接続制限値の概要」（P.27-7）
- 「接続設定と TCP 正規化のイネーブル化」（P.27-8）

（注） NAT コンフィギュレーションで最大接続数、最大初期接続数、および TCP シーケンス ランダム化を設定することもできます。両方の方法を使用して同じトラフィックにこれらの設定を行う場合は、セキュリティ アプライアンスは低い方の制限を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

接続制限値の概要

この項では、接続を制限する目的について説明します。次の項目を取り上げます。

- 「TCP 代行受信の概要」（P.27-7）
- 「クライアントレス SSL VPN の互換性を目的とした管理パケットの TCP 代行受信のディセーブル化」（P.27-7）
- 「デッド接続検出の概要」（P.27-7）
- 「TCP シーケンスランダム化概要」（P.27-8）

TCP 代行受信の概要

初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、クライアントあたりの制限値と初期接続の制限を利用して TCP 代行受信を開始します。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。TCP 代行受信では、SYN クッキー アルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、セキュリティ アプライアンスはサーバのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。セキュリティ アプライアンスがクライアントから ACK を受信すると、クライアントを認証し、サーバへの接続を許可できます。

クライアントレス SSL VPN の互換性を目的とした管理パケットの TCP 代行受信のディセーブル化

デフォルトでは、TCP 管理接続では TCP 代行受信が常にイネーブルになっています。TCP 代行受信は、イネーブルになると 3 ウェイ TCP 接続確立ハンドシェイク パケットを代行受信するため、セキュリティ アプライアンスはクライアントレス（ブラウザベースの）SSL VPN からのパケットを処理できなくなります。クライアントレス SSL VPN では、3 ウェイ ハンドシェイク パケットを処理し、選択的な ACK とクライアントレス SSL VPN 接続への TCP オプションを提供できなければなりません。管理トラフィックの TCP 代行受信をディセーブルにするには、初期接続制限を設定します。初期接続制限に達した後にだけ TCP 代行受信をイネーブルにできます。

デッド接続検出の概要

デッド接続検出（DCD）では、デッド接続を検出し、トラフィックをまだ処理できる接続を期限切れにすることなく、デッド接続を期限切れにできます。DCD は、アイドル状態でも有効な接続を維持する場合に設定します。

DCD をイネーブルにすると、アイドル タイムアウト動作が変化します。アイドル タイムアウトになると、DCD プローブが 2 つのエンドホストそれぞれに送信され、接続の有効性が判断されます。設定された間隔でプローブが送信された後にエンドホストが応答を返さないと、その接続は解放され、リセット値が設定されていれば各エンドホストに送信されます。両方のエンドホストが応答して接続の有効性が確認されると、アクティビティ タイムアウトが現在の時間に更新され、それに応じてタイムアウトが再スケジュールされます。

TCP シーケンスランダム化概要

それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

- 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
- セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
- セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

接続設定と TCP 正規化のイネーブル化

接続設定値と TCP 正規化を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] ペインで、第 23 章「サービス ポリシー ルールの設定」に従ってサービス ポリシーを設定します。

新しいサービス ポリシー ルールの一部として接続制限を設定できます。または、既存のサービス ポリシーを編集することもできます。

ステップ 2　[Rule Actions] ダイアログボックスで、[Connection Settings] タブをクリックします。

ステップ 3　最大接続数を設定するには、[Maximum Connections] 領域で次の値を設定します。

- [TCP & UDP Connections]：トラフィック クラスのすべてのクライアントで同時に接続される TCP および UDP 接続の最大数を 65,536 までの範囲で指定します。どちらのプロトコルともデフォルトは **0** で、接続可能な最大許容数に設定されています。
- [Embryonic Connections]：ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。
- [Per Client Connections]：クライアントごとに、同時接続できる TCP 接続と UDP 接続の最大数を指定します。クライアントあたりの最大接続数の接続をすでに開いているクライアントが新しい接続を試みると、セキュリティ アプライアンスは、その接続を拒否してパケットをドロップします。
- [Per Client Embryonic Connections]：クライアントごとに、同時接続できる TCP 初期接続の最大数を指定します。クライアントあたりの最大初期接続数の接続をセキュリティ アプライアンスからすでに開いているクライアントが新しい TCP 接続を要求すると、セキュリティ アプライアンスは、その要求の処理を TCP 代行受信機能に代行させ、接続を阻止します。

ステップ 4　TCP タイムアウトを設定するには、[TCP Timeout] 領域で次の値を設定します。

- [Connection Timeout]：接続スロットを解放するまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。この期間は 5 分以上にする必要があります。デフォルトは **1 時間**です。
- [Send reset to TCP endpoints before timeout]：セキュリティ アプライアンスが、接続スロットを解放する前に接続のエンドポイントに TCP リセット メッセージを送信するように指定します。
- [Embryonic Connection Timeout]：初期接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。デフォルトは **30 秒**です。
- [Half Closed Connection Timeout]：ハーフ クローズ接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。この期間は 5 分以上にする必要があります。デフォルトは **10 分**です。

ステップ 5　シーケンス番号のランダム化をディセーブルにするには、[Randomize Sequence Number] をオフにします。

別のインライン ファイアウォールで TCP イニシャル シーケンス番号のランダム化をイネーブルにしている場合は、そのランダム化をディセーブルにできます。2 つのファイアウォールで同じ動作を実行する必要はないからです。ただし、両方のファイアウォールで ISN ランダム化をイネーブルにしたままにしてもトラフィックには影響しません。

それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスでは、発信方向に通過する TCP SYN の ISN をランダム化します。同一セキュリティ レベルの 2 つのインターフェイス間の接続の場合、ISN は双方向の SYN でランダム化されます。

保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

ステップ 6　TCP 正規化を設定するには、[Use TCP Map] をオンにします。

ドロップダウン リストから既存の TCP マップを選択するか（選択可能な場合）、[New] をクリックして新しい TCP マップを追加します。

[Add TCP Map] ダイアログボックスが表示されます。

a. [TCP Map Name] フィールドで、名前を入力します。

b. [Queue Limit] フィールドで、異常なパケットの最大数を 0 ～ 250 の範囲で指定します。

c. [Reserved Bits] 領域で、[Clear and allow]、[Allow only]、または [Drop] をクリックします。

[Allow only] を指定すると、TCP ヘッダーに予約ビットのあるパケットだけが許可されます。

[Clear and allow] を指定すると、TCP ヘッダーの予約ビットをクリアしてパケットを許可します。

[Drop] を指定すると、TCP ヘッダーに予約ビットのあるパケットをドロップします。

d. 次のいずれかのオプションをオンにします。

- [Clear Urgent Flag]：セキュリティ アプライアンスを通じて URG ポインタを許可またはクリアします。
- [Drop Connection on Window Variation]：予想外のウィンドウ サイズの変更が発生した接続をドロップします。
- [Drop Packets that Exceed Maximum Segment Size]：ピアで設定した MSS を超過したパケットを許可またはドロップします。
- [Check if transmitted data is the same as original]：再送信データ チェックをイネーブルおよびディセーブルにします。
- [Drop SYN Packets With Data]：データを持つ SYN パケットを許可またはドロップします。

- [Enable TTL Evasion Protection]：セキュリティ アプライアンスの TTL 回避保護をイネーブルまたはディセーブルにします。
- [Verify TCP Checksum]：チェックサム検証をイネーブルおよびディセーブルにします。

e. TCP オプションを設定するには、次のいずれかのオプションをオンにします。

- [Clear Selective Ack]：[selective-ack TCP] オプションを許可するかクリアするかを示します。
- [Clear TCP Timestamp]：TCP タイムスタンプ オプションを許可するかクリアするかを示します。
- [Clear Window Scale]：ウィンドウ スケール タイムスタンプ オプションを許可するかクリアするかを示します。
- [Range]：有効な TCP オプションの範囲を示します。正しい範囲は 6 ～ 7 と 9 ～ 255 です。下限境界値は上限境界値以下でなければなりません。

f. [OK] をクリックします。

ステップ 7　存続可能時間を設定するには、[Decrement time to live for a connection] をオンにします。

ステップ 8　[OK] または [Finish] をクリックします。

IP 監査の設定

IP 監査機能は、基本的な IPS 機能を提供します。サポートされるプラットフォームで高度な IPS 機能を実現する場合には、AIP SSM をインストールできます。

この機能により、名前付き監査ポリシーを作成し、パケットが事前定義済みの攻撃シグニチャまたは情報シグニチャと一致する場合に実行するアクションを特定できます。シグニチャは、既知の攻撃パターンに一致するアクティビティです。たとえば、DoS 攻撃に一致するシグニチャがあります。セキュリティ アプライアンスは、パケットをドロップ、アラームを生成、または接続をリセットするように設定できます。

IP Audit Policy

[IP Audit Policy] パネルでは、監査ポリシーを追加し、そのポリシーをインターフェイスに割り当てられます。攻撃ポリシーと情報ポリシーは、各インターフェイスに割り当てられます。攻撃ポリシーにより、パケットが攻撃シグニチャに一致するときに実行するアクションが決まります。そのパケットは、DoS 攻撃など、ネットワークでの攻撃の一部である可能性があります。情報ポリシーにより、パケットが情報シグニチャに一致するときに実行するアクションが決まります。そのパケットは、現時点ではネットワークを攻撃していなくても、ポート スイープなどの情報収集アクティビティの一部になる可能性があります。すべてのシグニチャのリストについては、IP 監査のシグニチャ リストを参照してください。

フィールド

- [Name]：定義済み IP 監査ポリシーの名前を示します。このテーブルには名前付きポリシーのデフォルト アクションが一覧表示されていますが（「--Default Action--」）、インターフェイスに割り当てることができる名前付きポリシーではありません。デフォルト アクションは、ポリシーでアクションを設定しない場合に、名前付きポリシーによって使用されます。デフォルト アクションを変更するには、そのアクションを選択して [Edit] ボタンをクリックします。
- [Type]：ポリシー タイプ（[Attack] または [Info]）を示します。

- [Action]：ポリシーに一致するパケットに対して実行されるアクション（[Alarm]、[Drop]、または [Reset]）を示します。複数のアクションが一覧表示されることもあります。
- [Add]：新しい IP 監査ポリシーを追加します。
- [Edit]：IP 監査ポリシーまたはデフォルト アクションを編集します。
- [Delete]：IP 監査ポリシーを削除します。デフォルト アクションは削除できません。
- [Policy-to-Interface Mappings]：攻撃および情報ポリシーを各インターフェイスに割り当てます。
  - [Interface]：インターフェイス名を表示します。
  - [Attack Policy]：使用できる攻撃監査ポリシー名を一覧表示します。リストにある名前をクリックして、ポリシーをインターフェイスに割り当てます。
  - [Info Policy]：使用できる情報監査ポリシー名を一覧表示します。リストにある名前をクリックして、ポリシーをインターフェイスに割り当てます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit IP Audit Policy Configuration

[Add/Edit IP Audit Policy Configuration] ダイアログボックスでは、インターフェイスに割り当てられる名前付き IP 監査ポリシーを追加または編集し、シグニチャ タイプごとにデフォルト アクションを変更できます。

フィールド

- [Policy Name]：IP 監査ポリシー名を設定します。ポリシー名は、追加した後では変更できません。
- [Policy Type]：ポリシー タイプを設定します。ポリシー タイプは、追加した後では変更できません。
  - [Attack]：ポリシー タイプを攻撃として設定します。
  - [Information]：ポリシー タイプを情報として設定します。
- [Action]：パケットがシグニチャに一致するときに実行するアクションを 1 つ以上設定します。アクションを選択しない場合には、デフォルト ポリシーが使用されます。
  - [Alarm]：パケットがシグニチャに一致したことを示すシステム メッセージを生成します。すべてのシグニチャのリストについては、「IP 監査のシグニチャ リスト」を参照してください。
  - [Drop]：パケットをドロップします。
  - [Reset]：パケットをドロップし、接続を閉じます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

IP Audit Signatures

[IP Audit Signatures] ペインでは、監査シグニチャをディセーブルにできます。正規のトラフィックが頻繁にシグニチャに一致する場合には、シグニチャをディセーブルにしてみてください。リスクが伴うことを承知でシグニチャをディセーブルにすると、多数のアラームを回避できます。

すべてのシグニチャのリストについては、「IP 監査のシグニチャ リスト」を参照してください。

フィールド

- [Enabled]：イネーブルになっているシグニチャを一覧表示します。
- [Disabled]：ディセーブルになっているシグニチャを一覧表示します。
- [Disable]：選択したシグニチャを [Disabled] ペインに移動します。
- [Enable]：選択したシグニチャを [Enabled] ペインに移動します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

IP 監査のシグニチャ リスト

表 27-3 に、サポートされているシグニチャおよびメッセージ番号の一覧を示します。

表 27-3　シグニチャ ID とシステム メッセージ番号

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1000	400000	IP options-Bad Option List	Informational	IP データグラム ヘッダーの IP オプションのリストが不完全であるか、または不正な形式になっている IP データグラムを受信するとトリガーされます。IP オプションのリストには、さまざまなネットワーク管理タスクまたはデバッグ タスクを実行するオプションが 1 つ以上含まれています。
1001	400001	IP options-Record Packet Route	Informational	データグラムの IP オプション リスト中にオプション 7（記録パケット ルート）を含む IP データグラムを受信するとトリガーされます。
1002	400002	IP options-Timestamp	Informational	データグラムの IP オプション リスト中にオプション 4（タイムスタンプ）を含む IP データグラムを受信するとトリガーされます。
1003	400003	IP options-Security	Informational	データグラムの IP オプション リスト中にオプション 2（セキュリティ オプション）を含む IP データグラムを受信するとトリガーされます。
1004	400004	IP options-Loose Source Route	Informational	データグラムの IP オプション リスト中にオプション 3（緩慢な送信元ルート）を含む IP データグラムを受信するとトリガーされます。
1005	400005	IP options-SATNET ID	Informational	データグラムの IP オプション リスト中にオプション 8（SATNET ストリーム ID）を含む IP データグラムを受信するとトリガーされます。
1006	400006	IP options-Strict Source Route	Informational	データグラムの IP オプション リスト中にオプション 2（厳密な送信元ルーティング）を含む IP データグラムを受信するとトリガーされます。
1100	400007	IP Fragment Attack	Attack	オフセット フィールドのオフセット値が 0 より大きく 5 未満になっている IP データグラムを受信するとトリガーされます。
1102	400008	IP Impossible Packet	Attack	送信元と宛先が同じアドレスになっている IP パケットが到着するとトリガーされます。このシグニチャは、いわゆる Land Attack を捕捉します。

表 27-3　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1103	400009	IP Overlapping Fragments（Teardrop）	Attack	同じ IP データグラム内に含まれている 2 つのフラグメントのオフセット値が、そのデータグラム内の位置決めを共有していることを示す場合にトリガーされます。これは、フラグメント A がフラグメント B によって完全に上書きされること、またはフラグメント A がフラグメント B によって部分的に上書きされることを意味します。オペレーティング システムによっては、このように重複するフラグメントが正しく処理されず、重複フラグメントを受信すると例外をスローしたり、他の不適切な動作を行ったりします。Teardrop 攻撃では、これにより DoS 状態を引き起こします。
2000	400010	ICMP Echo Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 0（エコー応答）に設定された IP データグラムを受信するとトリガーされます。
2001	400011	ICMP Host Unreachable	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 3（ホスト到達不能）に設定された IP データグラムを受信するとトリガーされます。
2002	400012	ICMP Source Quench	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 4（ソース クエンチ）に設定された IP データグラムを受信するとトリガーされます。
2003	400013	ICMP Redirect	Informational	P ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 5（リダイレクト）に設定された IP データグラムを受信するとトリガーされます。
2004	400014	ICMP Echo Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 8（エコー要求）に設定された IP データグラムを受信するとトリガーされます。
2005	400015	ICMP Time Exceeded for a Datagram	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 11（データグラムの超過時間）に設定された IP データグラムを受信するとトリガーされます。

表 27-3　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2006	400016	ICMP Parameter Problem on Datagram	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 12（データグラムのパラメータ問題）に設定された IP データグラムを受信するとトリガーされます。
2007	400017	ICMP Timestamp Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 13（タイムスタンプ要求）に設定された IP データグラムを受信するとトリガーされます。
2008	400018	ICMP Timestamp Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 14（タイムスタンプ応答）に設定された IP データグラムを受信するとトリガーされます。
2009	400019	ICMP Information Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 15（情報要求）に設定された IP データグラムを受信するとトリガーされます。
2010	400020	ICMP Information Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 16（ICMP 情報応答）に設定された IP データグラムを受信するとトリガーされます。
2011	400021	ICMP Address Mask Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 17（アドレス マスク要求）に設定された IP データグラムを受信するとトリガーされます。
2012	400022	ICMP Address Mask Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 18（アドレス マスク応答）に設定された IP データグラムを受信するとトリガーされます。
2150	400023	Fragmented ICMP Traffic	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、他にも 1（ICMP）に設定されたフラグメント フラグが存在するか、またはオフセット フィールドにオフセット値が指定されている IP データグラムを受信するとトリガーされます。
2151	400024	Large ICMP Traffic	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、IP 長が 1024 より大きくなっている IP データグラムを受信するとトリガーされます。

表 27-3　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2154	400025	Ping of Death Attack	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、Last Fragment ビットが設定され、（IP オフセット * 8）+（IP データ長）> 65535 になっている（つまり、IP オフセット（元のパケットでのこのフラグメントの開始位置、8 バイト単位）と残りのパケットの合計が IP パケットの最大サイズより大きくなっている）IP データグラムを受信するとトリガーされます。
3040	400026	TCP NULL flags	Attack	SYN、FIN、ACK、または RST のいずれのフラグも設定されていない 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3041	400027	TCP SYN+FIN flags	Attack	SYN および FIN のフラグが設定されている 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3042	400028	TCP FIN only flags	Attack	1 つの孤立 TCP FIN パケットが特定のホストの特権ポート（ポート番号が 1024 未満）に送信されるとトリガーされます。
3153	400029	FTP Improper Address Specified	Informational	要求側ホストと異なるアドレスを指定して port コマンドが発行された場合にトリガーされます。
3154	400030	FTP Improper Port Specified	Informational	1024 未満または 65535 より大きい値のデータ ポートを指定して port コマンドが発行された場合にトリガーされます。
4050	400031	UDP Bomb attack	Attack	指定されている UDP 長が、指定されている IP 長より短い場合にトリガーされます。この不正な形式のパケット タイプは、サービス拒絶攻撃と関連付けられています。
4051	400032	UDP Snork attack	Attack	送信元ポートが 135、7、または 19 のいずれかで、宛先ポートが 135 になっている UDP パケットが検出されるとトリガーされます。
4052	400033	UDP Chargen DoS attack	Attack	このシグニチャは、送信元ポート 7 および宛先ポート 19 において UDP パケットが検出されるとトリガーされます。
6050	400034	DNS HINFO Request	Informational	DNS サーバから HINFO レコードへのアクセスが試みられるとトリガーされます。
6051	400035	DNS Zone Transfer	Informational	送信元ポートが 53 の通常の DNS ゾーン転送が実行されるとトリガーされます。
6052	400036	DNS Zone Transfer from High Port	Informational	送信元ポートが 53 以外のときに不正な DNS ゾーン転送が発生するとトリガーされます。
6053	400037	DNS Request for All Records	Informational	すべてのレコードに対する DNS 要求があるとトリガーされます。
6100	400038	RPC Port Registration	Informational	ターゲット ホストで新しい RPC サービスを登録する試みがあるとトリガーされます。

表 27-3　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
6101	400039	RPC Port Unregistration	Informational	ターゲット ホストで既存の RPC サービスを登録解除する試みがあるとトリガーされます。
6102	400040	RPC Dump	Informational	ターゲット ホストに対して RPC ダンプ要求が発行されるとトリガーされます。
6103	400041	Proxied RPC Request	Attack	ターゲット ホストのポートマッパーにプロキシ RPC 要求が送信されるとトリガーされます。
6150	400042	ypserv (YP server daemon) Portmap Request	Informational	YP サーバ デーモン（ypserv）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6151	400043	ypbind (YP bind daemon) Portmap Request	Informational	YP バインド デーモン（ypbind）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6152	400044	yppasswdd (YP password daemon) Portmap Request	Informational	YP パスワード デーモン（yppasswdd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6153	400045	ypupdated (YP update daemon) Portmap Request	Informational	YP 更新デーモン（ypupdated）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	Informational	YP 転送デーモン（ypxfrd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6155	400047	mountd (mount daemon) Portmap Request	Informational	マウント デーモン（mountd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6175	400048	rexd (remote execution daemon) Portmap Request	Informational	リモート実行デーモン（rexd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6180	400049	rexd (remote execution daemon) Attempt	Informational	rexd プログラムの呼び出しが行われるとトリガーされます。リモート実行デーモンは、プログラムをリモート実行する役割を担うサーバです。rexd プログラムの呼び出しは、システム リソースへの不正アクセスの試みを示唆している場合があります。
6190	400050	statd Buffer Overflow	Attack	サイズの大きな statd 要求が送信されるとトリガーされます。これは、バッファをオーバーフローさせてシステムへアクセスしようとする試みの可能性があります。

フラグメント サイズの設定

デフォルトでは、セキュリティ アプライアンスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、フラグメントがセキュリティ アプライアンスを通過できないようにすることをお勧めします。フラグメント化されたパケットは、DoS 攻撃によく使われます。

フィールド

- [Fragment] テーブル：
  - [Interface]：セキュリティ アプライアンスの使用可能なインターフェイスを一覧表示します。
  - [Size]：リアセンブリを待機する IP リアセンブリ データベースに格納可能なパケットの最大数を設定します。デフォルトは 200 です。
  - [Chain Length]：1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。デフォルトは 24 パケットです。
  - [Timeout]：フラグメント化されたパケット全体の到着を待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。デフォルトは 5 秒です。
- [Edit]：[Edit Fragment] ダイアログボックスを開きます。
- [Show Fragment]：パネルが開き、セキュリティ アプライアンスのインターフェイスごとに現在の IP フラグメント データベースの統計情報が表示されます。

フラグメント パラメータの変更

インターフェイスの IP フラグメント データベースのパラメータを変更するには、次の手順を実行します。

ステップ 1　[Fragment] テーブルで変更するインターフェイスを選択し、[Edit] をクリックします。[Edit Fragment] ダイアログボックスが表示されます。

ステップ 2　[Edit Fragment] ダイアログボックスで、[Size]、[Chain]、および [Timeout] の値を必要に応じて変更し、[OK] をクリックします。間違った場合は、[Restore Defaults] をクリックします。

ステップ 3　[Fragment] パネルの [Apply] をクリックします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Show Fragment

[Show Fragment] パネルには、IP フラグメント リアセンブリ モジュールの動作データが表示されます。

フィールド

- [Size]：*表示専用*。リアセンブリを待機する IP リアセンブリ データベース内のパケット数を表示します。デフォルトは 200 です。
- [Chain]：*表示専用*。1 つの完全な IP パケットにフラグメント化できる最大パケット数を表示します。デフォルトは 24 パケットです。
- [Timeout]：*表示専用*。フラグメント化されたパケットの全体の到着を待機する最大秒数を表示します。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。パケットのすべてのフラグメントが表示の秒数内に到着しないと、すでに受信しているパケットのフラグメントはすべて破棄されます。デフォルトは 5 秒です。
- [Threshold]：*表示専用*。IP パケットのしきい値、つまりその値を超えるとリアセンブリ モジュールで新しいチェーンを作成できなくなる限界を表示します。
- [Queue]：*表示専用*。キュー内でリアセンブリを待機している IP パケットの数を表示します。
- [Assembled]：*表示専用*。正常にリアセンブリされた IP パケットの数を表示します。
- [Fail]：*表示専用*。リアセンブリの失敗試行回数を表示します。
- [Overflow]：*表示専用*。オーバーフロー キュー内の IP パケットの数を表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Edit Fragment

[Edit Fragment] ダイアログボックスでは、選択したインターフェイスの IP フラグメント データベースを設定できます。

フィールド

- [Interface]：[Fragment] パネルで選択したインターフェイスを表示します。[Edit Fragment] ダイアログボックスでの変更内容は、表示されたインターフェイスに適用されます。
- [Size]：リアセンブリを待機する IP リアセンブリ データベースに格納可能なパケットの最大数を設定します。
- [Chain Length]：1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。
- [Timeout]：フラグメント化されたパケット全体の到着を待機する最大秒数を設定します。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。

- [Restore Defaults]：工場出荷時のデフォルト設定に戻します。
  - [Size] は 200 です。
  - [Chain] は 24 パケットです。
  - Timeout は 5 秒です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Anti-Spoofing の設定

[Anti-Spoofing] ウィンドウでは、インターフェイスで Unicast Reverse Path Forwarding（Unicast RPF; ユニキャスト逆経路転送）をイネーブルにできます。Unicast RPF は、ルーティング テーブルに従い、すべてのパケットが正しい発信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護します。

通常、セキュリティ アプライアンスは、パケットの転送先を判定するときに宛先アドレスだけを調べます。Unicast RPF は、送信元アドレスも調べるようにセキュリティ アプライアンスに指示します。そのため、逆経路転送（Reverse Path Forwarding）と呼ばれます。セキュリティ アプライアンスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートをセキュリティ アプライアンスのルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、セキュリティ アプライアンスはデフォルト ルートを使用して Unicast RPF 保護の条件を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティング テーブルにない場合、セキュリティ アプライアンスはデフォルト ルートを使用して、外部インターフェイスを発信元インターフェイスとして正しく識別します。

ルーティング テーブルにあるアドレスから外部インターフェイスにトラフィックが入り、このアドレスが内部インターフェイスに関連付けられている場合、セキュリティ アプライアンスはパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合は、一致するルート（デフォルト ルート）が外部インターフェイスを示しているため、セキュリティ アプライアンスはパケットをドロップします。

Unicast RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルート ルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

フィールド

- [Interface]：インターフェイス名を一覧表示します。

- [Anti-Spoofing Enabled]：インターフェイスで Unicast RPF がイネーブルになっているかどうかを、Yes または No で示します。
- [Enable]：選択したインターフェイスに対する Unicast RPF をイネーブルにします。
- [Disable]：選択したインターフェイスに対する Unicast RPF をディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	•	—

TCP オプションの設定

[TCP Options] ペインでは、TCP 接続のパラメータを設定できます。

フィールド

- [Inbound and Outbound Reset]：着信および発信トラフィックの拒否された TCP 接続をリセットするかどうかを設定します。
  - [Interface]：インターフェイス名を表示します。
  - [Inbound Reset]：着信 TCP トラフィックのインターフェイスのリセット設定を、Yes または No で示します。この設定をイネーブルにすると、セキュリティ アプライアンスは、セキュリティ アプライアンスの通過を試み、アクセス リストまたは AAA の設定に基づいてセキュリティ アプライアンスにより拒否されたすべての着信 TCP セッションについて TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。
  - [Outbound Reset]：発信 TCP トラフィックのインターフェイスのリセット設定を、Yes または No で示します。この設定をイネーブルにすると、セキュリティ アプライアンス は、セキュリティ アプライアンス の通過を試み、アクセス リストまたは AAA の設定に基づいて セキュリティ アプライアンス により拒否されたすべての発信 TCP セッションについて TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。
  - [Edit]：インターフェイスの着信および発信のリセット設定値を設定します。
- [Other Options]：追加の TCP オプションを設定します。
  - [Send Reset Reply for Denied Outside TCP Packets]：セキュリティ レベルが最も低いインターフェイスで終了し、またアクセス リストまたは AAA の設定に基づいてセキュリティ アプライアンスにより拒否された TCP パケットのリセットをイネーブルにします。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。セキュリティ レベルが最も低いインターフェイスの Inbound Resets をイネーブルにする場合（TCP Reset Settings を参照）は、この設定もイネーブルにする必要はありません。Inbound Resets は、セキュリティ アプライアンスへのトラフィックとともに、セキュリティ アプライアンスを通過するトラフィックも処理します。

- [Force Maximum Segment Size for TCP] : 最大 TCP セグメント サイズを 48 から最大数の範囲のバイト数で設定します。デフォルト値は 1380 バイトです。この機能は、0 バイトに設定することによってディセーブルにできます。ホストとサーバが最初に接続を確立するときに、両方で最大セグメント サイズを設定できます。どちらかの最大値がここで設定する値を超えると、セキュリティ アプライアンスはその最大値を無効化し、ユーザが設定した値を挿入します。たとえば、ユーザが最大サイズを 1200 バイトに設定した場合に、ホストが最大サイズとして 1300 バイトを要求すると、セキュリティ アプライアンスは 1200 バイトを要求するようにパケットを変更します。
- [Force Minimum Segment Size for TCP] : 48 から最大数の間で、ユーザが設定したバイト数未満にならないように最大セグメント サイズを上書きします。この機能は、デフォルトでディセーブルです（0 に設定）。ホストとサーバが最初に接続を確立するときに、両方で最大セグメント サイズを設定できます。いずれかの最大値が [Force Minimum Segment Size for TCP Proxy] フィールドで設定した値未満になる場合、セキュリティ アプライアンスはその最大値を無効化し、ユーザが設定した「最小」値を挿入します（最小値は、実際には許容される最大値の中での最小の値です）。たとえば、ユーザが最小サイズを 400 バイトに設定した場合に、ホストが最大値として 300 バイトを要求すると、セキュリティ アプライアンスは 400 バイトを要求するようにパケットを変更します。
- [Force TCP Connection to Linger in TIME_WAIT State for at Least 15 Seconds] : 最後の標準 TCP クローズダウン シーケンスの後、最低でも 15 秒間、各 TCP 接続が短縮 TIME_WAIT 状態に保持するように強制します。エンド ホスト アプリケーションのデフォルト TCP 終了シーケンスが同時クローズである場合に、この機能を使用することを推奨します。セキュリティ アプライアンスのデフォルトの動作では、シャットダウン シーケンスが追跡され、2 つの FIN と最後の FIN セグメントの ACK の後で接続が解放されます。この即時解放ヒューリスティックにより、セキュリティ アプライアンスでは、標準クローズ シーケンスと呼ばれる最も一般的なクロージング シーケンスに基づいて、高い接続レートを維持できます。ただし、一方の端が閉じ、もう一方の端が確認応答してから独自のクロージング シーケンスを開始する標準クローズ シーケンスとは異なり、同時クローズでは、トランザクションの両端がクロージング シーケンスを開始します（RFC 793 を参照）。したがって、同時クローズでは、接続の一方の側が即時解放によって強制的に CLOSING 状態に保持されます。多くのソケットを CLOSING 状態にすると、エンド ホストのパフォーマンスが低下する可能性があります。たとえば、一部の WinSock メインフレーム クライアントはこの動作を示し、メインフレーム サーバのパフォーマンスを低下させることが知られています。この機能を使用すると、同時クローズダウン シーケンスを完了するためのウィンドウが作成されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

TCP Reset Settings

このダイアログボックスでは、インターフェイスの着信および発信のリセット設定値を設定します。

フィールド

- [Send Reset Reply for Denied Inbound TCP Packets] : セキュリティ アプライアンスの通過を試み、アクセス リストまたは AAA の設定に基づいてセキュリティ アプライアンスにより拒否されたすべての着信 TCP セッションについて TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。

  アイデンティティ要求（IDENT）接続をリセットする必要がある場合は、着信トラフィックに対して明示的にリセットを送信できます。拒否されたホストに TCP RST（TCP ヘッダーのリセット フラグ）を送信すると、RST によって着信 IDENT プロセスが停止されるため、IDENT がタイムアウトするのを待機する必要がなくなります。外部ホストは IDENT がタイムアウトするまで SYN を継続的に再送信するため、IDENT がタイムアウトするのを待機するとトラフィックの速度低下の原因となる可能性があります。そのため、**service resetinbound** コマンドによってパフォーマンスが向上する可能性があります。

- [Send Reset Reply for Denied Outbound TCP Packets] : セキュリティ アプライアンスの通過を試み、アクセス リストまたは AAA の設定に基づいてセキュリティ アプライアンスにより拒否されたすべての発信 TCP セッションについて TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。このオプションは、デフォルトで有効です。たとえば、トラフィック ストーム時に CPU の負荷を軽減するためなどに発信リセットをディセーブルにできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

グローバル タイムアウトの設定

[imeouts] ペインでは、セキュリティ アプライアンスで使用するタイムアウトの期間を設定できます。すべての期間は、hh:mm:ss の形式で表示されます。さまざまなプロトコルの接続スロットと変換スロットのアイドル時間を設定します。指定したアイドル時間の間スロットが使用されなかった場合、リソースは空いているプールに戻されます。TCP 接続スロットは、標準接続クローズ シーケンスのおよそ 60 秒後に解放されます。

（注）　カスタマー サポートによる指示がない限り、これらの値を変更しないことをお勧めします。

フィールド

[Authentication absolute] と [Authentication inactivity] を除くすべての場合において、チェックボックスをオフにすることはタイムアウト値を指定しないことを意味します。これら 2 つの場合にチェックボックスをオフにすることは、新しい接続ごとに再認証することを意味します。

- [Connection]：接続スロットが解放されるまでのアイドル時間を変更します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。この期間は 5 分以上にする必要があります。デフォルトは 1 時間です。
- [Half-closed]：TCP ハーフクローズ接続がクローズするまでのアイドル時間を変更します。最小値は 5 分です。デフォルトは 10 分です。ハーフクローズ接続のタイムアウトをディセーブルにするには、0:0:0 と入力します。
- [UDP]：UDP プロトコル接続がクローズするまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。タイムアウトをディセーブルにするには、0:0:0 と入力します。
- [ICMP]：全般的な ICMP 状態がクローズするまでのアイドル時間を変更します。
- [H.323]：H.323 メディア接続がクローズするまでのアイドル時間を変更します。デフォルトは 5 分です。タイムアウトをディセーブルにするには、0:0:0 と入力します。
- [H.225]：H.225 シグナリング接続がクローズするまでのアイドル時間を変更します。H.225 のデフォルトのタイムアウトは 1 時間（01:00:00）です。値を 00:00:00 にすると、この接続はクローズされません。すべての呼び出しがクリアされた後にこの接続をすぐにクローズするには、値を 1 秒（00:00:01）にすることをお勧めします。
- [MGCP]：MGCP メディア ポートがクローズするまでのアイドル時間を表す MGCP のタイムアウト値を変更します。MGCP のデフォルト タイムアウトは 5 分（00:05:00）です。タイムアウトをディセーブルにするには、0:0:0 と入力します。
- [MGCP PAT]：MGCP PAT 変換が削除されるまでのアイドル時間を変更します。デフォルトは 5 分（00:05:00）です。最小時間は 30 秒です。デフォルト値に戻すには、チェックボックスをオフにします。
- [SUNRPC]：SunRPC スロットが解放されるまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 10 分です。タイムアウトをディセーブルにするには、0:0:0 と入力します。
- [SIP]：SIP シグナリング ポート接続がクローズするまでのアイドル時間を変更します。この期間は 5 分以上にする必要があります。デフォルトは 30 分です。
- [SIP Media]：SIP メディア ポート接続がクローズするまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 2 分です。
- [SIP Invite]：PROVISIONAL 応答とメディア xlate のピンホールがクローズされるまでのアイドル時間を変更します。最小値は 0:1:0 で、最大値は 0:30:0 です。デフォルト値は 0:03:00 です。
- [SIP Disconnect]：CANCEL または BYE メッセージで 200 個の OK を受信しない場合に、SIP セッションを削除するまでのアイドル時間を変更します。最小値は 0:0:1 で、最大値は 0:10:0 です。デフォルト値は 0:02:00 です。
- [Authentication absolute]：認証キャッシュがタイムアウトになり、新しい接続を再認証する必要が生じるまでの期間を変更します。この期間は、変換スロット値よりも短い必要があります。システムは、新しい接続を開始して再びプロンプトが表示されるまで待機します。新しい接続のすべてでキャッシングと再認証をディセーブルにするには、0:0:0 と入力します。

（注） 接続でパッシブ FTP を使用する場合は、この値を 0:0:0 に設定しないでください。

- [Authentication inactivity]：認証キャッシュがタイムアウトになり、ユーザが新しい接続を再認証する必要が生じるまでのアイドル時間を変更します。この期間は、変換スロット値よりも短い必要があります。

- [Translation Slot]：変換スロットが解放されるまでのアイドル時間を変更します。この期間は 1 分以上にする必要があります。デフォルトは 3 時間です。タイムアウトをディセーブルにするには、0:0:0 と入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—