CHAPTER 24

ネットワーク攻撃の防止

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。次の項で構成されています。

Connection Settings（透過モードのみ）

Configuration > Properties > Connection Settings

Connection Settings ペインでは、TCP および UDP の最大接続数や最大初期接続数を設定し、透過ファイアウォール モードでの発信トラフィック（内部から外部へ）の TCP シーケンスのランダム化をディセーブルにすることができます。

（注）　最大接続数、最大初期接続数、および TCP シーケンスのランダム化は、Service Policy Rules でも設定できます。サービス ポリシー ルールにより、これらの制限値の適用方法をより柔軟に制御し、発信接続だけでなく両方向のトラフィックの制限値を設定することができます。同じトラフィックに対して両方の方法でこれらの設定値を設定した場合、セキュリティ アプライアンスは小さい方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、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。

接続と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、初期接続の制限を利用して TCP 代行受信を発生させます。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 シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合だけにします。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、1 つはサーバが生成します。セキュリティ アプライアンスは、ホスト / サーバによって生成される ISN をランダム化します。少なくとも 1 つの ISN をランダムに生成して、攻撃者が次の ISN を予想してセッションを乗っ取ることができないようにする必要があります。

フィールド

- Interface：接続制限がイネーブルになっているインターフェイスを示します。外部インターフェイスでは接続制限はサポートされていないため、このインターフェイスは常に内部インターフェイスとなります。
- Address：接続制限を適用するアドレスを示します。
- Maximum TCP Connections：最大 TCP 接続数を示します。値の 0 は、接続を制限しないことを意味します。
- Embryonic Limit：最大初期接続数を示します。値の 0 は、接続を制限しないことを意味します。
- Maximum UDP Connections：最大 UDP 接続数を示します。値の 0 は、接続を制限しないことを意味します。
- Randomize Sequence Number：TCP シーケンスのランダム化がイネーブルになっているかディセーブルになっているかを、Yes または No で示します。
- Add：接続制限ルールを追加します。
- Edit：接続制限ルールを編集します。
- Delete：接続制限ルールを削除します。

モード

次の表に、この機能を使用できるモードを示します。

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
—	•	•	•	—

Set/Edit Connection Settings

Configuration > Properties > Connection Settings > Set/Edit Connection Settings

Set/Edit Connection Settings ダイアログボックスでは、透過ファイアウォール モードでの発信トラフィック（内部から外部へ）の接続制限ルールを定義できます。

フィールド

- Host/Network：接続制限を設定するホストまたはネットワークを設定します。
  - Interface : 接続制限を設定するインターフェイスを設定します。内部インターフェイスのみを選択します。
  - IP Address：接続制限を設定する IP アドレスを設定します。
  - Mask : サブネット マスクを設定します。フィールドにマスクを入力するか、またはリストから共通マスクを選択できます。
  - Browse : Select host/network ダイアログボックスが開きます。このダイアログボックスでは、Network Object Groups パネルで定義したホストとネットワークを選択できます。
- Maximum Connections：TCP および UDP の最大接続数を設定します。
  - Maximum TCP Connections : 最大 TCP 接続数を 0 ～ 65535 の範囲で設定します。値の 0 は、接続を制限しないことを意味します。
  - Maximum UDP Connections : 最大 UDP 接続数を 0 ～ 65535 の範囲で設定します。値の 0 は、接続を制限しないことを意味します。
- Maximum Embryonic Connections : 最大初期接続数を 0 ～ 65535 の範囲で設定します。値の 0 は、接続を制限しないことを意味します。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。セキュリティ アプライアンスでは、初期接続の制限を利用して TCP 代行受信を発生させます。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。
- Randomize Sequence Number check : TCP シーケンス番号のランダム化をイネーブルにします。ランダム化をディセーブルにするには、このボックスをオフにします。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合だけにします。

モード

次の表に、この機能を使用できるモードを示します。

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

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。シグニチャとは、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るとします。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

Configuration > Properties > IP Audit > 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ることができます。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ることができます。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

次の表に、この機能を使用できるモードを示します。

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

Configuration > Properties > IP Audit > IP Audit Policy > 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、追加した後で変更することはできません。
- Policy Type：ポリシー タイプを設定します。ポリシー タイプは、追加した後で変更することはできません。
  - 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

次の表に、この機能を使用できるモードを示します。

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

Configuration > Properties > IP Audit > 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することができます。正規のトラフィックが 1 つのシグニチャに連続して一致する場合には、そのシグニチャをディセーブルにすることができます。また、アラーム数が膨大な数になるのを防ぐために、シグニチャのディセーブル化というリスクをとることもできます。

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

次の表に、この機能を使用できるモードを示します。

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 監査シグニチャ リスト

表 24-1 に、サポートされるシグニチャとシステム メッセージ番号を一覧表示します。

表 24-1　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	情報	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	情報	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	情報	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	情報	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	情報	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	情報	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	情報	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。

表 24-1　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
1100	400007	IP Fragment Attack	攻撃	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	攻撃	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。
1103	400009	IP Overlapping Fragments (Teardrop)	攻撃	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、これを悪用して DoS 状態を引き起こします。
2000	400010	ICMP Echo Reply	情報	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	情報	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	情報	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	情報	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 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	情報	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	情報	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。
2006	400016	ICMP Parameter Problem on Datagram	情報	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。

表 24-1　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
2007	400017	ICMP Timestamp Request	情報	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	情報	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	情報	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	情報	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	情報	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	情報	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	攻撃	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	攻撃	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。
2154	400025	Ping of Death Attack	攻撃	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	攻撃	SYN、FIN、ACK、または RST のど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。

表 24-1　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
3041	400027	TCP SYN+FIN flags	攻撃	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	攻撃	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	情報	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	情報	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	攻撃	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、DoS（サービス拒絶）攻撃と関連付けられています。
4051	400032	UDP Snork attack	攻撃	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	攻撃	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	情報	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	情報	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	情報	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	攻撃	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	情報	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。
6101	400039	RPC Port Unregistration	情報	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	情報	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	攻撃	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	情報	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	情報	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。

表 24-1　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
6152	400044	yppasswdd (YP password daemon) Portmap Request	情報	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	攻撃	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	攻撃	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	情報	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	情報	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	情報	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	攻撃	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。

Fragment

Configuration > Properties > Advanced > Fragment

Fragment ペインでは、セキュリティ アプライアンスの各インターフェイスにある IP フラグメント データベースの設定を行い、NFS との互換性を高めることができます。

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ときに始動します。パケットのすべてのフラグメントが指定した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。
- 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

次の表に、この機能を使用できるモードを示します。

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

Configuration > Properties > Fragment > 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 : 表示のみ。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 : 表示のみ。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 : 表示のみ。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ときに始動します。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 : 表示のみ。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：表示のみ。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：表示のみ。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：表示のみ。リアセンブリの失敗試行回数を表示します。
- Overflow：表示のみ。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

次の表に、この機能を使用できるモードを示します。

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

Configuration > Properties > Fragment > 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設定します。
- 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ときに始動します。パケットのすべてのフラグメントが指定した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。
- 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

次の表に、この機能を使用できるモードを示します。

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

Configuration > Properties > Anti-Spoofing

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）をイネーブルにすることができます。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。
- Enable：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

次の表に、この機能を使用できるモードを示します。

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 Options

Configuration > Properties > TCP Options

TCP Options ウィンドウでは、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 領域 : 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 カラム : インターフェイス名を示します。
  - Inbound Reset カラム : 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 アプライアンスの搬送を試み、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る、すべての着信 TCP セッションの 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。このオプションをイネーブルにしない場合は、拒否されたパケットがセキュリティ アプライアンスによって自動的に破棄されます。
  - Outbound Reset カラム : 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 アプライアンスの搬送を試み、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る、すべての発信 TCP セッションの 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。このオプションをイネーブルにしない場合は、拒否されたパケットがセキュリティ アプライアンスによって自動的に破棄されます。
  - Edit ボタン : 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。
- Send Reset Reply for Denied Outside TCP Packets チェックボックス : 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る、TCP パケットのリセットをイネーブルにします。このオプションをイネーブルにしない場合は、拒否されたパケットがセキュリティ アプライアンスによって自動的に破棄されます。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 チェックボックスおよびフィールド : 48 から最大数の間で、最大 TCP セグメント サイズをバイト単位で設定します。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することができます。ホストとサーバの両方は、接続を最初に確立するときに最大セグメント 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 チェックボックスおよびフィールド : 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 サイズを無効化します。この機能はデフォルトでディセーブルになっています（0 に設定）。ホストとサーバの両方は、最初に接続を確立するときに最大セグメント 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 フィールドで設定する値未満になる場合、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 チェックボックス：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。この機能は、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の場合に使用できます。セキュリティ アプライアンスのデフォルト動作では、シャットダウン シーケンスが追跡され、2 つの FIN、および最後の FIN セグメントの ACK の後に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率を維持することができます。ただし同時クローズでは、トランザクションの両エンドがクロージング シーケンスを開始します。これは、一方のエンドがクローズすると、もう一方のエンドは確認応答してからそれ自体のクロージング シーケンスを開始する、標準クローズ シーケンス（RFC 793 を参照）の場合とは対照的です。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。CLOSING 状態になっているソケットが数多く存在すると、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、このような動作が生じてメインフレーム サーバのパフォーマンスを低下させることで知られています。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

次の表に、この機能を使用できるモードを示します。

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

Configuration > Properties > TCP Options > 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 チェックボックス：セキュリティ アプライアンスの搬送を試み、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る、すべての着信 TCP セッションの 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。このオプションをイネーブルにしない場合は、拒否されたパケットがセキュリティ アプライアンスによって自動的に破棄されます。

  ID 要求（IDENT）接続をリセットする必要がある場合には、着信トラフィックのリセットを明示的に送信できます。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 が着信 IDENT プロセスを停止するため、IDENT がタイムアウトになるのを待つ必要がなくなります。IDENT のタイムアウトを待機すると、外部ホストは IDNET がタイムアウトになるまで SYN の再送信を続けるため、トラフィックの速度が低下す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改善される場合があります。

- Send Reset Reply for Denied Outbound TCP Packets チェックボックス：セキュリティ アプライアンスの搬送を試み、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る、すべての発信 TCP セッションの 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。このオプションをイネーブルにしない場合は、拒否されたパケットがセキュリティ アプライアンスによって自動的に破棄されます。このオプションはデフォルトでイネーブルになっています。たとえば、発信リセットをディセーブルにして、トラフィック ストーム中の CPU の負荷を軽減させることができます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—

Timeouts

Configuration > Properties > Timeouts

Timeouts ウィンドウでは、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中にスロットが使用されなかった場合は、リソースがフリー 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 と入力します。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 状態がクローズされ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 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 ポートがクローズされ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（00:00:05）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、Translation Slot の値より短くする必要があります。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、Translation Slot の値より短くする必要があります。
- 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

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—