CHAPTER 23

ネットワーク攻撃の防止

この章では、TCP 正規化、TCP 接続と UDP 接続の制限、およびその他の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について説明します。

この章は、次の項で構成されています。

TCP 正規化の設定

TCP 正規化機能は、検出時にセキュリティ アプライアンスが対処できる異常なパケットを識別します。セキュリティ アプライアンスは、パケットを許可、ドロップ、またはクリアできます。TCP 正規化は、攻撃からセキュリティ アプライアンスを保護するのに役立ちます。この項では、次のトピックについて取り上げます。

TCP の正規化の概要

TCP 正規化には、設定できないアクションと設定できるアクションが含まれます。通常、接続をドロップまたはクリアする設定できないアクションは、どのような場合でも不良なパケットに適用されます。設定できるアクション（「TCP ノーマライザの正規化」（P.23-2）を参照）は、ネットワークのニーズに応じたカスタマイズが必要な場合があります。

TCP 正規化に関する次のガイドラインを参考にしてください。

- ノーマライザは、SYN フラッドからの保護は行いません。セキュリティ アプライアンスには、他の方法による SYN フラッド保護機能が組み込まれています。
- ノーマライザは、セキュリティ アプライアンスがフェールオーバーのためにルーズ モードになっていない限り、SYN パケットを最初のパケットと見なします。

TCP ノーマライザの正規化

この機能はモジュラ ポリシー フレームワークを使用するため、TCP の正規化の実装は、トラフィックの特定、TCP の正規化アクションの指定、およびインターフェイスでの TCP の正規化のアクティブ化で構成されます。詳細については、第 21 章「モジュラ ポリシー フレームワークの使用」を参照してください。

TCP の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　検索する TCP 正規化基準を指定するには、次のコマンドを入力して TCP マップを作成します。

```
hostname(config)# tcp-map tcp-map-name
```

TCP マップごとに 1 つまたは複数の設定値をカスタマイズできます。

ステップ 2　（任意）次の 1 つ以上のコマンド（表 23-1 を参照）を入力して TCP マップ基準を設定します。すべての基準にデフォルト設定を使用する場合は、TCP マップにコマンドを入力する必要はありません。一部の設定をカスタマイズする場合、入力しないコマンドにはデフォルトが使用されます。デフォルト コンフィギュレーションには、次の設定が含まれます。

```
no check-retransmission
no checksum-verification
exceed-mss allow
queue-limit 0 timeout 4
reserved-bits allow
syn-data allow
synack-data drop
invalid-ack drop
seq-past-window drop
tcp-options range 6 7 clear
tcp-options range 9 255 clear
tcp-options selective-ack allow
tcp-options timestamp allow
tcp-options window-scale allow
ttl-evasion-protection
urgent-flag clear
window-variation allow-connection
```

表 23-1　tcp-map コマンド

コマンド	注意事項
check-retransmission	一貫性のない TCP 再送信を防止します。
checksum-verification	チェックサムを確認します。
exceed-mss {**allow** | **drop**}	データ長が TCP 最大セグメント サイズを超えるパケットに対するアクションを設定します。 （デフォルト）**allow** キーワードは、データ長が TCP 最大セグメント サイズを超えるパケットを許可します。 **drop** キーワードは、データ長が TCP 最大セグメント サイズを超えるパケットをドロップします。

表 23-1　tcp-map コマンド（続き）

コマンド	注意事項
invalid-ack {**allow** | **drop**}	無効な ACK を含むパケットに対するアクションを設定します。次のような場合に無効な ACK が検出される可能性があります。 • TCP 接続が SYN-ACK-received ステータスでは、受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号と同じでない場合、その ACK は無効です。 • 受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号より大きい場合は常に、その ACK は無効です。 **allow** キーワードは、無効な ACK を含むパケットを許可します。 （デフォルト）**drop** キーワードは、無効な ACK を含むパケットをドロップします。 **（注）** 無効な ACK を含む TCP パケットは、WAAS 接続で自動的に許可されます。
queue-limit *pkt_num* [**timeout** *seconds*]	バッファに格納して TCP 接続の正しい順序に設定できる、異常なパケットの最大数を設定します。1 ～ 250 パケットです。デフォルト値の 0 は、この設定がディセーブルであり、トラフィックのタイプに応じたデフォルトのシステム キュー制限が使用されることを意味します。 • アプリケーション インスペクション（**inspect** コマンド）、IPS（**ips** コマンド）、および TCP インスペクション再送信（TCP マップ **check-retransmission** コマンド）のための接続のキュー制限は、3 パケットです。セキュリティ アプライアンスが異なるウィンドウ サイズの TCP パケットを受信した場合は、アドバタイズされた設定と一致するようにキュー制限がダイナミックに変更されます。 • 他の TCP 接続の場合は、異常なパケットはそのまま通過します。 **queue-limit** コマンドを 1 以上に設定した場合、すべての TCP トラフィックに対して許可される異常なパケットの数は、この設定と一致します。たとえば、アプリケーション インスペクション、IPS、および TCP check-retransmission のトラフィックの場合、TCP パケットからアドバタイズされたすべての設定が**キュー制限**設定を優先して、無視されます。その他の TCP トラフィックについては、異常なパケットはバッファに格納されて、そのまま通過するのではなく、正しい順序に設定されます。 **timeout** *seconds* 引数は、異常なパケットがバッファ内に留まることができる最大時間を設定します。設定できる値は 1 ～ 20 秒です。タイムアウト期間内に正しい順序に設定されて渡されなかったパケットはドロップされます。デフォルトは 4 秒です。*pkt_num* 引数を 0 に設定した場合は、どのトラフィックのタイムアウトも変更できません。**timeout** キーワードを有効にするには、制限を 1 以上に設定する必要があります。

表 23-1　tcp-map コマンド （続き）

コマンド	注意事項
reserved-bits {**allow** | **clear** | **drop**}	TCP ヘッダーの予約ビットに対するアクションを設定します。 （デフォルト）**allow** キーワードは、TCP ヘッダーの予約ビットが設定されているパケットを許可します。 **clear** キーワードは、TCP ヘッダーの予約ビットを消去して、パケットを許可します。 **drop** キーワードは、TCP ヘッダーの予約ビットが設定されているパケットをドロップします。
seq-past-window {**allow** | **drop**}	パストウィンドウ シーケンス番号を含むパケットに対するアクションを設定します。つまり、受信した TCP パケットのシーケンス番号が、TCP 受信ウィンドウの右端より大きい場合です。 **allow** キーワードは、パストウィンドウ シーケンス番号を含むパケットを許可します。このアクションは、**queue-limit** コマンドが 0（ディセーブル）に設定されている場合に限り許可されます。 （デフォルト）**drop** キーワードは、パストウィンドウ シーケンス番号を含むパケットをドロップします。
synack-data {**allow** | **drop**}	データを含む TCP SYNACK パケットに対するアクションを設定します。 **allow** キーワードは、データを含む TCP SYNACK パケットを許可します。 （デフォルト）**drop** キーワードは、データを含む TCP SYNACK パケットをドロップします。
syn-data {**allow** | **drop**}	データを含む SYN パケットに対するアクションを設定します。 （デフォルト）**allow** キーワードは、データを含む SYN パケットを許可します。 **drop** キーワードは、データを含む SYN パケットをドロップします。

表 23-1　tcp-map コマンド （続き）

コマンド	注意事項
tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**} または **tcp-options range** *lower upper* {**allow** | **clear** | **drop**}	selective-ack、timestamp、window-scale などの TCP オプションを含むパケットに対するアクションを設定します。 （デフォルト）**allow** キーワードは、指定したオプションを含むパケットを許可します。 （**range** の場合のデフォルト）**clear** キーワードは、オプションを消去して、パケットを許可します。 **drop** キーワードは、指定したオプションを含むパケットをドロップします。 **selective-ack** キーワードは、SACK オプションに対するアクションを設定します。 **timestamp** キーワードは、タイムスタンプ オプションに対するアクションを設定します。タイムスタンプ オプションを消去すると、PAWS と RTT がディセーブルになります。 **widow-scale** キーワードは、ウィンドウ スケール メカニズム オプションに対するアクションを設定します。 **range** キーワードは、オプションの範囲を指定します。*lower* 引数は、範囲の下限を設定します。6、7、または 9 ～ 255 です。 *upper* 引数は、範囲の上限を設定します。6、7、または 9 ～ 255 です。
ttl-evasion-protection	TTL 回避保護をディセーブルにします。セキュリティ ポリシーを回避しようとする攻撃を防ぐ場合は、このコマンドを入力しないでください。 たとえば、攻撃者は TTL を非常に短くしてポリシーを通過するパケットを送信できます。TTL がゼロになると、セキュリティ アプライアンスとエンドポイントの間のルータはパケットをドロップします。この時点で、攻撃者は TTL を長くした悪意のあるパケットを送信できます。このパケットは、セキュリティ アプライアンスにとって再送信のように見えるため、通過します。一方、エンドポイント ホストにとっては、このパケットが攻撃者によって受信された最初のパケットになります。この場合、攻撃者はセキュリティによる攻撃の防止を受けず、攻撃に成功します。

表 23-1　tcp-map コマンド（続き）

コマンド	注意事項
urgent-flag {**allow** | **clear**}	URG フラグを含むパケットに対するアクションを設定します。URG フラグは、ストリーム中の他のデータよりもプライオリティの高い情報がこのパケットに含まれていることを示すために使用します。TCP RFC では、URG フラグの正確な解釈が明確にされていません。そのため、エンド システムは緊急オフセットをさまざまな方法で処理しており、これが攻撃に対する脆弱性になることがあります。 **allow** キーワードは、URG フラグを含むパケットを許可します。 （デフォルト）**clear** キーワードは、URG フラグを消去してパケットを許可します。
window-variation {**allow** | **drop**}	予想外のウィンドウ サイズの変更が発生した接続に対するアクションを設定します。ウィンドウ サイズ メカニズムによって、TCP は大きなウィンドウをアドバタイズでき、続いて、過剰な量のデータを受け入れずに、はるかに小さなウィンドウをアドバタイズできます。TCP 仕様により、「ウィンドウの縮小」は極力避けることが推奨されています。この条件が検出された場合に、接続をドロップできます。 （デフォルト）**allow** キーワードは、ウィンドウが変化した接続を許可します。 **drop** キーワードは、ウィンドウが変化した接続をドロップします。

ステップ 3　トラフィックを特定するには、**class-map** コマンドを使用してクラス マップを追加します。詳細については、「通過トラフィック用のレイヤ 3/4 クラス マップの作成」（P.21-5）を参照してください。

たとえば、次のコマンドを使用してすべてのトラフィックを照合できます。

```
hostname(config)# class-map TCPNORM
hostname(config-cmap)# match any
```

特定のトラフィックを照合する場合は、次のようにアクセス リストを照合できます。

```
hostname(config)# access list TCPNORM extended permit ip any 10.1.1.1 255.255.255.255
hostname(config)# class-map TCP_norm_class
hostname(config-cmap)# match access-list TCPNORM
```

ステップ 4　クラス マップ トラフィックで行うアクションを設定するポリシー マップを追加または編集するには、次のコマンドを入力します。

```
hostname(config)# policy-map name
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name はステップ 1 で追加したクラス マップです。

次に例を示します。

```
hostname(config)# policy-map TCP_norm_policy
hostname(config-pmap)# class TCP_norm_class
hostname(config-pmap-c)#
```

ステップ 5　次のコマンドを入力して、TCP マップをクラス マップに適用します。

```
hostname(config-pmap-c)# set connection advanced-options tcp-map-name
```

ステップ 6　1 つ以上のインターフェイスでポリシー マップをアクティブにするには、次のコマンドを入力します。

```
hostname(config)# service-policy policymap_name {global | interface interface_name}
```

ここで、**global** はポリシー マップをすべてのインターフェイスに適用し、**interface** は 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、インスペクションのグローバル ポリシーがあり、TCP 正規化のインターフェイス ポリシーがある場合、インターフェイスに対してインスペクションと TCP 正規化の両方が適用されます。ただし、インスペクションのグローバル ポリシーがあり、インスペクションのインターフェイス ポリシーもある場合、そのインターフェイスにはインターフェイス ポリシーのインスペクションのみが適用されます。

たとえば、既知の FTP データ ポートと Telnet ポートの間の TCP ポート範囲に送信されるすべてのトラフィックで緊急フラグと緊急オフセット パケットを許可するには、次のコマンドを入力します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet
hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap
hostname(config-pmap-c)# service-policy pmap global
```

接続の制限値とタイムアウトの設定

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。セキュリティ アプライアンスを通過する接続、またはセキュリティ アプライアンスへの管理接続に対して制限値を設定できます。この項では、次のトピックについて取り上げます。

- 「接続制限値の概要」（P.23-7）
- 「接続の制限値とタイムアウトのイネーブル化」（P.23-9）

（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.23-8）
- 「クライアントレス SSL 互換での管理パケットの TCP 代行受信のディセーブル化」（P.23-8）
- 「デッド接続検出（DCD）の概要」（P.23-8）
- 「TCP シーケンスランダム化概要」（P.23-8）

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 互換での管理パケットの 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 代行受信をイネーブルにすると、3 ウェイ TCP 接続確立のハンドシェイク パケットが代行受信されるため、セキュリティ アプライアンスではクライアントレス SSL 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 では、クライアントレス SSL 接続で selective-ack や他の TCP オプションを提供するために、3 ウェイ ハンドシェイク パケットを処理する機能が必要になります。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（DCD）の概要

DCD では、デッド接続を検出して、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、そのデッド接続を期限切れにすることができます。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 タイムアウトは現在時刻に更新され、それに応じてアイドル タイムアウトが再スケジュールされます。

DCD をイネーブルにすると、TCP ノーマライザでのアイドルタイムアウト処理の動作が変更されます。DCD プローブにより、**show conn** コマンドで表示される接続でのアイドル タイムアウトがリセットされます。タイムアウト コマンドで設定したタイムアウト値を超過していても、DCD プローブのために存続している接続を判別するため、**show service-policy** コマンドには、DCD からのアクティビティ数を示すカウンタが含まれています。

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。

保護対象のホストの ISN をランダム化することにより、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。

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。

接続の制限値とタイムアウトのイネーブル化

接続制限とタイムアウトを設定する手順は、次のとおりです。

ステップ 1　トラフィックを特定するには、**class-map** コマンドを使用してクラス マップを追加します。詳細については、「通過トラフィック用のレイヤ 3/4 クラス マップの作成」（P.21-5）を参照してください。

たとえば、次のコマンドを使用してすべてのトラフィックを照合できます。

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
```

特定のトラフィックを照合する場合は、次のようにアクセス リストを照合できます。

```
hostname(config)# access list CONNS extended permit ip any 10.1.1.1 255.255.255.255
hostname(config)# class-map CONNS
hostname(config-cmap)# match access-list CONNS
```

ステップ 2　クラス マップ トラフィックで行うアクションを設定するポリシー マップを追加または編集するには、次のコマンドを入力します。

```
hostname(config)# policy-map name
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name はステップ 1 で追加したクラス マップです。

次に例を示します。

```
hostname(config)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)#
```

ステップ 3　最大接続制限値、または TCP シーケンスのランダム化をイネーブルにするかどうかを設定するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# set connection {[conn-max n] [embryonic-conn-max n]
[per-client-embryonic-max n] [per-client-max n] [random-sequence-number {enable |
disable}]}
```

ここで、**conn-max** *n* 引数には、許可される同時 TCP 接続または同時 UDP 接続、あるいはその両方の最大数を 0 ～ 65535 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。

TCP または UDP の同時接続を許可するように 2 つのサーバが設定されている場合、接続制限数は、設定されている各サーバに別々に適用されます。

embryonic-conn-max *n* 引数には、許可される同時初期接続の最大数を 0 ～ 65535 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。

per-client-embryonic-max *n* 引数には、クライアントごとに許可される同時初期接続の最大数を 0 ～ 65535 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。

per-client-max *n* 引数には、クライアントごとに許可される同時接続の最大数を 0 ～ 65535 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。

random-sequence-number {**enable** | **disable**} キーワードで、TCP シーケンス番号のランダム化をイネーブルまたはディセーブルにします。詳細については、「TCP シーケンスランダム化概要」（P.23-8）を参照してください。

このコマンドを 1 行ですべて入力することも（順序は任意）、各属性を別々のコマンドとして入力することもできます。セキュリティ アプライアンスは、コマンドを実行コンフィギュレーション内で 1 行に結合します。

ステップ 4　接続タイムアウトを設定するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# set connection timeout {[embryonic hh:mm:ss] {tcp hh:mm:ss
[reset]] [half-closed hh:mm:ss] [dcd hh:mm:ss [max_retries]]}
```

ここで、**embryonic** *hh*:*mm*:*ss* キーワードには、TCP 初期（ハーフオープン）接続が閉じられるまでのタイムアウトを 0:0:5 ～ 1193:00:00 の範囲で設定します。デフォルトは 0:0:30 です。この値を 0 に設置することもでき、この場合は接続がタイムアウトしないことを意味します。

tcp *hh*:*mm*:*ss* キーワードには、タイムアウトを 0:5:0 ～ 1193:00:00 の範囲で設定します。デフォルトは 1:0:0 です。この値を 0 に設置することもでき、この場合は接続がタイムアウトしないことを意味します。**reset** キーワードを指定すると、接続のタイムアウト時にリセット パケットが TCP エンドポイントに送信されます。

half-closed *hh*:*mm*:*ss* アイドル タイムアウトを 0:5:0 から 1193:0:0 の範囲で設定します。デフォルトは 0:10:0 です。ハーフクローズの接続は DCD の影響を受けません。また、セキュリティ アプライアンスは、ハーフクローズ接続を切断するときにリセット パケットを送信しません。

dcd キーワードは、DCD をイネーブルにします。DCD では、デッド接続を検出して、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、そのデッド接続を期限切れにすることができます。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。TCP 接続がタイムアウトすると、セキュリティ アプライアンスは、エンドホストに DCD プローブを送信して接続の有効性を判断します。最大再試行回数を超えてもエンドホストの一方が応答しない場合、セキュリティ アプライアンスはその接続を解放します。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、セキュリティ アプライアンスはアクティビティ タイムアウトを現在時刻に更新し、それに応じてアイドル タイムアウトを再スケジュールします。*retry-interval* には、DCD プローブに応答がない場合に別のプローブを送信するまで待機する時間を、*hh*:*mm*:*ss* 形式で、0:0:1 から 24:0:0 の範囲で設定します。デフォルトは 0:0:15 です。*max-retries* には、接続が無活動状態であると宣言するまでに失敗する DCD の連続再試行回数を設定します。最小値は 1、最大値は 255 です。デフォルトは 5 です。

このコマンドを 1 行ですべて入力することも（順序は任意）、各属性を別々のコマンドとして入力することもできます。コマンドは実行コンフィギュレーションで 1 行に結合されます。

ステップ 5　1 つ以上のインターフェイスでポリシー マップをアクティブにするには、次のコマンドを入力します。

```
hostname(config)# service-policy policymap_name {global | interface interface_name}
```

ここで、**global** はポリシー マップをすべてのインターフェイスに適用し、**interface** は 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、グローバル ポリシーでは検査を行うように設定されており、インターフェイス ポリシーでは TCP 正規化が指定されている場合は、検査と TCP 正規化の両方がインターフェイスに適用されます。ただし、インスペクションのグローバル ポリシーがあり、インスペクションのインターフェイス ポリシーもある場合、そのインターフェイスにはインターフェイス ポリシーのインスペクションのみが適用されます。

次の例では、すべてのトラフィックに対して接続の制限値とタイムアウトを設定しています。

```
hostname(config)# class-map CONNS
```

```
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection conn-max 1000 embryonic-conn-max 3000
hostname(config-pmap-c)# set connection timeout tcp 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

複数のパラメータを使用して **set connection** コマンドを入力するか、各パラメータを別々のコマンドとして入力できます。セキュリティ アプライアンスは、コマンドを実行コンフィギュレーション内で 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力するとします。

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map コマンドの出力には、2 つのコマンドの結果が単一の結合コマンドとして表示されます。

```
set connection conn-max 600 embryonic-conn-max 50
```

IP スプーフィングの防止

この項では、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）をイネーブルにします。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。

Unicast RPF をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# ip verify reverse-path interface interface_name
```

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。フラグメントの禁止を設定するには、次のコマンドを入力します。

```
hostname(config)# fragment chain 1 [interface_name]
```

特定のインターフェイスでフラグメント化を禁止する場合は、インターフェイス名を入力します。デフォルトでは、このコマンドはすべてのインターフェイスに適用されます。

不要な接続のブロック

あるホストがネットワークを攻撃しようとしていることがわかった場合（たとえば、システム ログ メッセージで攻撃が示された場合）、送信元 IP アドレスおよびその他の識別パラメータに基づいて、接続をブロック（排除）できます。排除を無効するまで、新しい接続は作成できません。

（注） トラフィックをモニタする IPS（AIP SSM など）がある場合は、IPS で自動的に接続を排除できます。

接続を手動で排除するには、次の手順を実行します。

ステップ 1　必要に応じて、次のコマンドを入力し、接続に関する情報を表示します。

```
hostname# show conn
```

セキュリティ アプライアンスは、各接続に関する情報を次のように表示します。

```
TCP out 64.101.68.161:4300 in 10.86.194.60:23 idle 0:00:00 bytes 1297 flags UIO
```

ステップ 2　この送信元 IP アドレスからの接続を排除するには、次のコマンドを入力します。

```
hostname(config)# shun src_ip [dst_ip src_port dest_port [protocol]] [vlan vlan_id]
```

送信元 IP アドレスだけを入力した場合、以後のすべての接続が排除されます。既存の接続はアクティブのままです。

送信元 IP アドレスからの以後の接続をブロックするだけでなく、既存の接続もドロップするには、宛先 IP アドレス、送信元と宛先のポート、およびプロトコルを入力します。デフォルトでは、プロトコルは IP を表す 0 です。

マルチ コンテキスト モードでは、このコマンドは管理コンテキストで入力できます。また、他のコンテキストのインターフェイスに割り当てられている VLAN ID を指定することで、他のコンテキストの接続を排除できます。

ステップ 3　排除を無効するには、次のコマンドを入力します。

```
hostname(config)# no shun src_ip [vlan vlan_id]
```

基本 IPS をサポートする IP 監査の設定

IP 監査機能は、セキュリティ アプライアンスを使用しないAIP SSMに基本 IPS サポートを提供します。署名の基本リストをサポートし、署名と一致するトラフィックに対して 1 つ以上のアクションを実行するようにセキュリティ アプライアンスを設定できます。

IP 監査をイネーブルにするには、次の手順を実行します。

ステップ 1　情報シグニチャに対する IP 監査ポリシーを定義するには、次のコマンドを入力します。

```
hostname(config)# ip audit name name info [action [alarm] [drop] [reset]]
```

ここで、**alarm** はパケットが署名と一致したことを示すシステム メッセージを生成し、**drop** はパケットをドロップし、**reset** はパケットをドロップして接続を閉じます。アクションを定義しない場合、デフォルト アクションはアラームの生成です。

ステップ 2　攻撃シグニチャに対する IP 監査ポリシーを定義するには、次のコマンドを入力します。

```
hostname(config)# ip audit name name attack [action [alarm] [drop] [reset]]
```

ここで、**alarm** はパケットが署名と一致したことを示すシステム メッセージを生成し、**drop** はパケットをドロップし、**reset** はパケットをドロップして接続を閉じます。アクションを定義しない場合、デフォルト アクションはアラームの生成です。

ステップ 3　ポリシーをインターフェイスに割り当てるには、次のコマンドを入力します。

```
ip audit interface interface_name policy_name
```

ステップ 4　署名をディセーブルにする方法および署名の詳細については、『*Cisco Security Appliance Command Reference*』の **ip audit signature** コマンドを参照してください。