CHAPTER 19

ネットワーク攻撃の回避

この章では、ネットワーク攻撃を回避する手順について説明します。内容は次のとおりです。

- 接続制限とタイムアウトの設定（p.19-2）
- IP スプーフィングの回避（p.19-4）
- フラグメント サイズの設定（p.19-4）
- 不正な接続のブロック（p.19-5）

接続制限とタイムアウトの設定

ここでは、TCP および UDP 接続の最大数を設定し、接続タイムアウトを設定し、TCP シーケンスのランダム化をディセーブルにする手順について説明します。

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、データをスクランブル化している場合だけにしてください。TCP 接続ごとに、Initial Sequence Number（ISN）を 2 つずつ使用します。1 つはクライアントが作成し、もう 1 つはサーバが作成します。FWSM は、ホスト / サーバによって生成された ISN をランダム化します。攻撃側が次の ISN を予測してセッションを乗っ取る可能性を排除するために、ISN の少なくとも一方はランダムに作成する必要があります。

（注） Network Address Translation（NAT; ネットワーク アドレス変換）設定で最大接続数と、TCP シーケンスのランダム化も設定できます。両方の方法を使用して、同じトラフィックに設定値を設定する場合、FWSM は低い方の制限を使用します。いずれかの方法を使用して TCP シーケンスのランダム化がディセーブルである場合、FWSM は TCP シーケンスのランダム化をディセーブルにします。

NAT も初期接続制限を設定します。これにより、Denial of Service（DoS; サービスの拒絶）攻撃を回避するための TCP 代行受信が開始されます。接続制限、TCP のランダム化、初期制限を設定するには、「透過ファイアウォール モードと NAT を設定しない場合の接続制限の設定」（p.7-8）および 第 12 章「NAT の設定」を参照してください。

接続制限を設定する手順は、次のとおりです。

ステップ 1　トラフィックを識別するには、**class-map** コマンドを使用してクラス マップ コマンドを追加します。詳細については、「クラス マップを使用したトラフィックの識別」（p.18-3）を参照してください。

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
```

ステップ 3　アクションを割り当てるステップ 1 のクラス マップを特定するには、次のコマンドを入力します。

```
hostname(config-pmap)# class class_map_name
```

ステップ 4　最大接続数（TCP と UDP 両方）を設定するか、または TCP シーケンスのランダム化をイネーブルあるいはディセーブルにするには、次のコマンドを入力します。

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

number は 0 ～ 65,535 です。デフォルトは 0 で、これは接続に制限がないことを意味します。

1 行すべてにこのコマンドを（任意の順序で）入力することも、各属性を別のコマンドとして入力することもできます。実行コンフィギュレーションでは、このコマンドは 1 行に統合されています。

ステップ 5　接続のタイムアウト、初期接続（ハーフオープン）、ハーフクローズ接続を設定するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# set connection timeout {[embryonic seconds]
[half-closed minutes] [tcp minutes]}
```

embryonic *seconds* は、1 ～ 255（秒）です。デフォルトは 20 秒です。この値を 0 に設定できます。これは接続が決してタイムアウトしないことを意味します。**set connection** コマンドを使用しても初期接続の最大数は設定できませんが、タイムアウトは設定できます。

half-closed *minutes* は 1 ～ 255（分）です。デフォルトは 10 分です。この値を 0 に設定できます。これは接続が決してタイムアウトしないことを意味します。

tcp *minutes* は 5 ～ 65535（分）です。デフォルトは 60 分です。この値を 0 に設定できます。これは接続が決してタイムアウトしないことを意味します。

1 行すべてにこのコマンドを（任意の順序で）入力することも、各属性を別のコマンドとして入力することもできます。実行コンフィギュレーションでは、このコマンドは 1 行に統合されています。

ステップ 6　1 つまたは複数のインターフェイス上でポリシー マップを実行するには、次のコマンドを入力します。

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

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** はポリシーを 1 つのインターフェイスに適用します。許可されるのはグローバル ポリシー 1 つのみです。サービス ポリシーをインターフェイスに適用すると、そのインターフェイス上のグローバル ポリシーが上書きされます。各インターフェイスに対し、ポリシー マップ 1 つを適用できます。

IP スプーフィングの回避

Unicast Reverse Path Forwarding（uRPF）をインターフェイス上でイネーブルにすることができます。uRPF は、すべてのパケットの送信元 IP アドレスが、ルーティング テーブル内の正しい送信元インターフェイスと一致するかどうかを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用して正しい送信元を不明にすること）を防ぎます。

通常、パケットの送信先を決定する場合、FWSM は宛先アドレスのみを認識します。uRPF は送信元アドレスも認識するよう FWSM に指示します。そのため、この機能は Reverse Path Forwarding と呼ばれます。FWSM 経由で許可したい任意のトラフィックについては、FWSM ルーティング テーブルに送信元アドレスまで戻るルートを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。

外部トラフィックについては、たとえば、FWSM は uRPF 保護要件を満たすため、デフォルトのルートを使用できます。トラフィックが外部インターフェイスから入り、ルーティング テーブルがその送信元アドレスを知らない場合、FWSM はデフォルトのルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく指定します。

トラフィックが、ルーティング テーブルにとって既知であるが、内部インターフェイスに対応付けられているアドレスから外部インターフェイスに入る場合、FWSM はパケットを廃棄します。同様に、トラフィックが未知の送信元アドレスから内部インターフェイスに入る場合、一致するルート（デフォルトのルート）が外部インターフェイスを示すので、FWSM はパケットを廃棄します。

ユニキャスト RPF は次のように実行されます。

- Internet Control Message Protocol（ICMP）パケットにはセッションがないので、各パケットが検証されます。
- UDP および TCP にはセッションがあるので、初期パケットはリバース ルート検索を必要とします。セッション中に着信する以降のパケットは、セッションの一部として維持された既存のステートを使用して検証されます。非初期パケットは、初期パケットが使用する同一のインターフェイス上に着信するように検証されます。

uRPF 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、FWSM は、IP パケットにつき最大 24 のフラグメント、およびリアセンブリを待つ最大 200 のフラグメントを許可します。定期的にパケットをフラグメント化するアプリケーション（NFS over UDP など）がある場合、ネットワーク上でフラグメント化を行う必要があるかもしれません。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、FWSM 経由でフラグメントを許可しないことを推奨します。フラグメント化されたパケットは、DoS 攻撃としてしばしば使用されます。フラグメントを許可しないようにするには、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回避したい場合、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。

不正な接続のブロック

ホストがネットワークを攻撃しようとしていることが分かっている（たとえば、システム ログ メッセージが攻撃を表示する）場合、IP アドレスおよび他の識別パラメータに基づいて接続をブロック（または排除）できます。排除を解除するまで新しい接続は実行されません。

（注） トラフィックをモニタする IPS がある場合、IPS は自動的に接続を排除します。

接続を手動で排除する手順は、次のとおりです。

ステップ 1　必要に応じて、次のコマンドを入力して接続の詳細を表示します。

```
hostname# show conn
```

FWSM に、次のような各接続の詳細を表示します。

```
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　送信元 IP アドレスから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 アドレスのみを入力すると、以降の接続はすべて排除されます。既存の接続はアクティブのままです。

既存の接続を廃棄するには、送信元 IP アドレスからの以降の接続をブロックするのと同様に、宛先 IP アドレス、送信元ポートおよび宛先ポート、プロトコルを入力します。デフォルトでは、IP のプロトコルは 0 です。

マルチコンテキスト モードの場合、このコマンドを admin コンテキストに入力できます。他のコンテキストに割り当てられた VLAN（仮想 LAN）ID を指定することで、別のコンテキストで接続を回避できます。

ステップ 3　排除を解除するには、次のコマンドを入力します。

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