CHAPTER 23

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。

Anti-Spoofing

Anti-Spoofing ペインでは、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、FWSM 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 FWSM に指示します。そのため、逆経路転送（Reverse Path Forwarding）と呼ばれます。FWSM 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 FWSM 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、FWSM 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、FWSM 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、FWSM 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、FWSM 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
•	•	•	•	—

Connection Settings（透過モードのみ）

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、FWSM 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、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。

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。FWSM 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。FWSM 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

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。ボックス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、ネットワーク オブジェクトの概要 ペイン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。FWSM 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：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
—	•	•	•	—

Fragment

Fragment ペインでは、FWSM 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：FWSM 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：ペインが開き、FWSM 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** ペインの **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

Show Fragment ペインには、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 : 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 : 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 : 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 : 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：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：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：リアセンブリの失敗試行回数を表示します。
- Overflow：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

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 ペイン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行った変更は、表示される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
•	•	•	•	—

TCP Options

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

- Force Maximum Segment Size for TCP Proxy : 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、FWSM 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、FWSM 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 Proxy : 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 ボックスで設定する値未満になる場合、FWSM 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、FWSM 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。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。FWSM 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、FWSM 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。
- Reset Inbound : アクセスリストに基づいて、インターフェイスに着信して FWSM の搬送を試み、FWSM により拒否される、すべての TCP セッションに対し、FWSM が TCP リセットを送信します。このオプションをイネーブルにしない場合は、このようなセッションのパケットがすべて FWSM によって自動的に破棄されます。

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
•	•	•	•	—

Timeouts

Timeouts ペインでは、FWSM 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）　Cisco TAC からの指示がない限り、これらの値を変更することはお勧めできません。

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。接続時間は 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てからのアイドル時間を変更します。
- 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。
- 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てから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 変換が削除されてから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。
- 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。接続時間は 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。
- Non TCP UDP：TCP/UDP 接続がクローズしてからのアイドル時間を設定します。デフォルトは 10 分です。

- 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。
- SIP Invite：PROVISIONAL 応答とメディア xlate のピンホールがクローズされてから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 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 disconnect：メディアが削除されてメディア xlates がクローズされてから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。

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
•	•	•	•	—