

接続設定

この章では、ASA を経由する接続用、または、ASA を宛先とする管理接続用の接続を設定する方法について説明します。

- 接続の設定 （1 ページ）
- 接続の設定 （2 ページ）
- 接続のモニタリング （25 ページ）
- 接続設定の履歴 （26 ページ）

接続の設定

接続設定とは、デバイスを通過する接続を管理するさまざまな機能のことです。

接続設定のタイプ

接続設定には次のタイプがあります。

- **さまざまなプロトコルのグローバルタイムアウト**：すべてのグローバルタイムアウトにはデフォルト値があります。接続が早期に失われる場合にのみ変更します。
- **トラフィック クラスごとの接続タイムアウト**：サービス ポリシーを使用して、特定のタイプのトラフィックのグローバルタイムアウトを上書きできます。すべてのトラフィッククラスのタイムアウトにデフォルト値があるため、それらの値を設定する必要はありません。
- **接続制限と TCP 代行受信**：デフォルトでは、ASA を経由する（または宛先とする）接続の数に制限はありません。サービスポリシールールを使用して、特定のトラフィッククラスに制限を設定します。これにより、サービス妨害（DoS）攻撃からサーバーが保護されます。特に、初期接続（TCP ハンドシェイクを完了していない接続）に制限を設定すると、SYN フラッディング攻撃から保護できます。初期接続の制限を超えると、TCP インターセプトコンポーネントがアクティブになり、接続をプロキシして攻撃を抑制します。
- **デッド接続検出（DCD）**：有効であるがアイドル状態になることが多い永続接続がある場合に、デッド接続検出を有効にします。そのような接続でアイドルタイムアウト設定を超えると、接続が閉じられることがあります。デッド接続検出では、アイドル状態であるが

有効な接続を特定し、アイドルタイマーをリセットすることで接続状態を維持します。アイドル時間を超えるたびに、DCD は接続の両側をプローブして、その接続が有効であることに両側で一致しているかどうかを確認します。**show service-policy** コマンドの出力には、DCD からのアクティビティ量を示すカウンタが含まれます。**show conn detail** コマンドを使用して、イニシエータとレスポンダに関する情報、およびそれぞれがプローブを送信した頻度を取得できます。

- **TCP シーケンスのランダム化**：それぞれの TCP 接続には 2 つの ISN（初期シーケンス番号）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 つはサーバーで生成されます。デフォルトでは、ASA 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。ランダム化により、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。ただし、TCP シーケンスのランダム化は、TCP SACK（選択的確認応答）を実質的に破棄します。クライアントが認識するシーケンス番号がサーバーが認識するものと異なるためです。必要に応じて、トラフィック クラスごとにランダム化を無効化することができます。
- **TCP 正規化**：TCP ノーマライザは、異常なパケットから保護します。一部のタイプのパケット異常をトラフィック クラスで処理する方法を設定できます。
- **TCPステートバイパス**：ネットワークで非対称ルーティングを使用するかどうかをチェックする TCP ステートをバイパスできます。
- **SCTP ステートバイパス**：Stream Control Transmission Protocol（SCTP）プロトコル検証が必要なければ、SCTP のステートフル インスペクションをバイパスできます。
- **フローのオフロード**：フローが NIC 自体で切り替えられる超高速パスにオフロードされるトラフィックを識別して選択できます。オフロードによって、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。

接続の設定

接続制限、タイムアウト、TCP 正規化、TCP シーケンスのランダム化、存続可能時間（TTL）のデクリメントには、ほとんどのネットワークに適切なデフォルト値があります。これらの接続の設定が必要となるのは、独自の要件があり、ネットワークに特定のタイプの設定がある場合、または早期のアイドル タイムアウトによる異常な接続切断が発生した場合のみです。

その他の接続関連機能は無効になっています。これらのサービスは、一般的なサービスとしてではなく、特定のトラフィック クラスにのみ設定します。これらの機能には次のものが含まれています：TCP 代行受信、TCP ステート バイパス、Dead Connection Detection（DCD; デッド接続検出）、SCTP ステート バイパス、フロー オフロード。

次の一般的な手順では、考えられるすべての接続の設定について説明します。必要に応じて実装する設定を選んでください。

始める前に

パケットがデバイスに入ると、ファイアウォールはまずアクセス制御ルールおよびNATを評価して、接続エントリを作成する必要があるかどうかを判断します。接続エントリは、ネクストホップ用のARPエントリが存在するかどうかに関係なく作成されます。このため、接続が存在しても、その接続範囲内のパケットがデバイスを通過することを意味するものではありません。アイドルタイムアウトなどの接続の設定は、不要な接続が残ってシステムリソースを占有しないようにします。

手順

ステップ1 グローバル タイムアウトの設定 （3 ページ）。これらの設定は、デバイスを通過するすべてのトラフィックに対してさまざまなプロトコルのデフォルトのアイドルタイムアウトを変更します。早期のタイムアウトによりリセットされる接続に問題がある場合は、まずグローバルタイムアウトを変更してください。

ステップ2 SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信） （6 ページ）。この手順を使用して、TCP 代行受信を設定します。

ステップ3 異常な TCP パケット処理のカスタマイズ（TCP マップ、TCP ノーマライザ） （8 ページ）（特定のトラフィック クラスについてデフォルトの TCP 正規化の動作を変更する場合）。

ステップ4 非対称ルーティングの TCP ステートチェックのバイパス（TCP ステートバイパス） （12 ページ）（このタイプのルーティング環境がある場合）。

ステップ5 TCP シーケンスのランダム化の無効化 （15 ページ）（デフォルトのランダム化が特定の接続データをスクランブルしている場合）。

ステップ6 大規模フローのオフロード （16 ページ）（コンピューティング集約型のデータセンターのパフォーマンスを改善する必要がある場合）。

ステップ7 特定のトラフィック クラスの接続の設定（すべてのサービス） （20 ページ）。これは、接続の設定用の汎用手順です。これらの設定は、サービス ポリシー ルールを使用して、特定のトラフィック クラスのグローバルのデフォルト値を上書きできます。これらのルールを使用して、TCP ノーマライザのカスタマイズ、TCP シーケンスのランダム化の変更、パケットの存続可能時間のデクリメント、およびその他のオプション機能の実装も行います。

ステップ8 TCP オプションの構成 （24 ページ）（他の標準的な TCP 動作をリセットまたは変更する必要がある場合）。

グローバル タイムアウトの設定

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グローバル アイドル タイムアウト期間を設定できます。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、リソースはフリー プールに戻されます。

グローバル タイムアウトを変更すると、サービス ポリシーによる特定のトラフィック フロー用に上書きできる新しいデフォルトのタイムアウトが設定されます。

特定のタイムアウトを設定できないプロトコル（GREなど）では、アイドルタイムアウトは2分です。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Global Timeouts]** を選択します。

ステップ 2 変更するタイムアウトのボックスをオンにして新しい値を入力することで、タイムアウトを設定します。

すべての期間は *hh*:*mm*:*ss* 形式で表示され、ほとんどの場合、最大期間は 1193:0:0 です。[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と、タイムアウトがデフォルト値に戻ります。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。

タイムアウトをディセーブルにするには、0 を入力します。

- [Connection]：接続スロットが解放されるまでのアイドル時間。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を閉じるまでのアイドル時間。FIN と FIN-ACK の両方が検出された場合、接続はハーフクローズ状態と見なされます。FIN のみが検出された場合は、通常の接続タイムアウトが適用されます。最小値は 30 秒です。デフォルト値は 10 分です。
- [UDP]：UDP 接続を閉じるまでのアイドル時間。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。
- [ICMP]：全般的なICMP状態が終了するまでのアイドル時間。デフォルト（および最小）は 2 秒です。
- [ICMP Error]：ASA が ICMP エコー応答パケットを受信してから ICMP 接続を削除するまでのアイドル時間で、0:0:0 から 0:1:0 の間、または ICMP timeout 値のいずれか低い方です。デフォルトは 0（ディセーブル）です。このタイムアウトが無効で、ICMP インスペクションを有効にすると、ASA では、エコー応答が受信されるとすぐにICMP接続を削除します。したがってその（すでに閉じられた）接続用に生成されたすべての ICMP エラーは破棄されます。このタイムアウトは ICMP 接続の削除を遅らせるので、重要な ICMP エラーを受信できます。
- [H.323]：H.245（TCP）および H.323（UDP）メディア接続が終了するまでのアイドル時間。デフォルト（かつ最小値）は 5 分です。H.245 と H.323 のいずれのメディア接続にも同じ接続フラグが設定されているため、H.245（TCP）接続は H.323（RTP および RTCP）メディア接続とアイドル タイムアウトを共有します。
- [H.225]：H.225 シグナリング接続を閉じるまでのアイドル時間。デフォルトは 1 時間です。すべての呼び出しがクリアされた後に接続をすぐにクローズするには、タイムアウト値を 1 秒（0:0:1）にすることを推奨します。

- [MGCP]：MGCP メディア接続が削除されるまでのアイドル時間。デフォルトは 5 分ですが、最小で 1 秒に設定できます。
- [MGCP PAT]：MGCP PAT 変換を削除するまでのアイドル時間。デフォルトは 5 分です。最小値は 30 秒です。
- [TCP Proxy Reassembly]：再構築のためバッファ内で待機しているパケットをドロップするまでのアイドル タイムアウト（0:0:10 ～ 1193:0:0）。デフォルトは、1 分（0:1:0）です。
- [Floating Connection]： 同じネットワークへの複数のルートが存在し、それぞれメトリックが異なる場合、システムは接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは 0 です（接続はタイムアウトしません）。より良いルートを使用できるようにするには、タイムアウト値を 0:0:30 ～ 1193:0:0 の間で設定します。このタイマーは、仮想トンネルインターフェイス（VTI）を介した接続には適用されません。VTI を介した接続がスタックした場合は、手動でクリアする必要があります。
- [SCTP]：Stream Control Transmission Protocol（SCTP）接続を閉じるまでのアイドル時間（0:1:0 ～ 1193:0:0）。デフォルトは 2 分（0:2:0）です。
- [Stale Routes]：古いルートをルータの情報ベースから削除する前に保持する時間。これらのルートは OSPF などの内部ゲートウェイ プロトコル用です。デフォルトは 70 秒（00:01:10）です。指定できる範囲は 00:00:10 ～ 00:01:40 です。
- [SUNRPC]：SunRPC スロットが解放されるまでのアイドル時間。この期間は 1 分以上にする必要があります。デフォルト値は 10 分です。
- [SIP]：SIP シグナリング ポート接続を閉じるまでのアイドル時間。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 ポート接続を閉じるまでのアイドル時間。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 メディア タイマーは、SIP UDP メディア パケットを使用する SIP RTP/RTCP で、UDP 非アクティブ タイムアウトの代わりに使用されます。
- [SIP Provisional Media]：SIP 暫定メディア接続のタイムアウト値（1 ～ 30 分）。デフォルトは 2 分です。
- [SIP Invite]：暫定応答のピンホールとメディア xlate を閉じるまでのアイドル時間（0:1:0 ～ 00:30:0）。デフォルトは、3 分（0:3:0）です。
- [SIP Disconnect]：CANCEL メッセージまたは BYE メッセージで 200 OK を受信しなかった場合に、SIP セッションを削除するまでのアイドル時間（0:0:1 ～ 00:10:0）。デフォルトは 2 分（0:2:0）です。
- [Authentication absolute]：認証キャッシュがタイムアウトになり、ユーザーが新しい接続を再認証する必要が生じるまでの期間。このタイマーは、AAA のルールであるカットスループロキシでのみ使用されます。この期間は、変換スロット タイムアウトよりも短い必要があります。システムは、ユーザが新しい接続を開始するまで待機します。すべての新しい

接続で認証を強制するキャッシングを無効にする前に、次の制限事項を考慮してください。

- 接続でパッシブ FTP を使用する場合は、この値を 0 に設定しないでください。
- [認証絶対タイムアウト（Authentication Absolute）] が 0 の場合、HTTPS 認証は動作しないことがあります。HTTPS 認証後に、ブラウザが複数の TCP 接続を開始して Web ページをロードすると、最初の接続は通過しますが、その後の接続では認証がトリガーされます。このため、ユーザーには、認証の成功後も常に認証ページが表示されます。これを回避するには、認証の絶対タイムアウトを 1 秒に設定します。この回避策を使用すると、認証されていないユーザーが同じ送信元 IP アドレスからアクセスすれば 1 秒間だけファイアウォールを通過できるおそれがあります。

- [Authentication inactivity]：認証キャッシュがタイムアウトになり、ユーザー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。この期間は、変換スロット値よりも短い必要があります。このタイムアウトはデフォルトで無効になっています。このタイマーは、AAA のルールであるカットスルー プロキシでのみ使用されます。
- [Translation Slot]：NAT 変換スロットが解放されるまでのアイドル時間。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。
- **PAT 変換スロット**（8.4(3) 以降、8.5(1) および 8.6(1) を除く）。PAT 変換スロットが解放されるまでのアイドル時間（0:0:30～ 0:5:0）。デフォルトは 30 秒です。前の接続がアップストリーム デバイスで引き続き開いている可能性があるため、開放された PAT ポートを使用する新しい接続を上流に位置するルータが拒否する場合、このタイムアウトを増やすことができます。
- [Connection Holddown]：接続で使用されているルートがもう存在していない、または非アクティブになったときに、システムが接続を保持する時間。このホールドダウン期間内にルートがアクティブにならない場合、接続は解放されます。接続ホールドダウンタイマーの目的は、ルートが発生してすぐにダウンする可能性がある場合に、ルートフラッピングの影響を減らすことです。ルートの収束がもっと早く発生するようにホールドダウンタイマーを減らすことができます。デフォルトは 15 秒です。指定できる範囲は 00:00:00 ～ 00:00:15 です。

ステップ 3 [Apply] をクリックします。

SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信）

攻撃者が一連の SYN パケットをホストに送信すると、SYN フラッディング サービス妨害（DoS）攻撃が発生します。これらのパケットは通常、スプーフィングされた IP アドレスから発信されます。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、正規ユーザーからの接続要求に対してサービスを提供できなくなります。

SYN フラッディング攻撃を防ぐために初期接続数を制限できます。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。

接続の初期接続しきい値を超えると、ASA はサーバーのプロキシとして動作し、その接続がターゲットホストの SYN キューに追加されないように、SYN Cookie 方式を使用してクライアント SYN 要求に対する SYN-ACK 応答を生成します。SYN クッキーは、基本的に秘密を作成するために、MSS、タイムスタンプ、およびその他の項目の数学的ハッシュから構築される SYN-ACK で返される最初のシーケンス番号です。ASA は、正しいシーケンス番号で有効な時間ウィンドウ内にクライアントから返された ACK を受信すると、クライアントが本物であることを認証し、サーバーへの接続を許可できます。プロキシを実行するコンポーネントは、TCP 代行受信と呼ばれます。

SYN フラッド攻撃からサーバーを保護するためのエンドツーエンド プロセスでは、接続制限を設定し、TCP 代行受信の統計情報をイネーブルにし、結果をモニターする必要があります。

始める前に

- 保護するサーバーの TCP SYN バックログ キューより低い初期接続制限を設定していることを確認します。これより高い初期接続制限を設定すると、有効なクライアントが、SYN 攻撃中にサーバーにアクセスできなくなります。初期接続制限に適切な値を決定するには、サーバーの容量、ネットワーク、サーバーの使用状況を入念に分析してください。
- ASA モデル上の CPU コア数によっては、同時接続および初期接続の最大数が、各コアによる接続の管理方法が原因で、設定されている数を超える場合があります。最悪の場合、ASA は最大 *n*-1 の追加接続および初期接続を許可します。ここで、*n* はコアの数です。たとえば、モデルに 4 つのコアがあり、6 つの同時接続および 4 つの初期接続を設定した場合は、各タイプで 3 つの追加接続を使用できます。ご使用のモデルのコア数を確認するには、**show cpu core** コマンドを入力します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Service Policy]** を選択します。

ステップ 2 **[Add]** > **[Add Service Policy Rule]** をクリックします。

または、保護するサーバーのルールがすでにある場合、ルールを編集します。

ステップ 3 ルールを特定のインターフェイスに適用するか、すべてのインターフェイスにグローバルに適用するかどうかを選択して、[Next] をクリックします。

ステップ 4 トラフィック分類の場合は、[Source and Destination IP Addresses (uses ACL)] を選択して、[Next] をクリックします。

ステップ 5 ACL ルールの場合は、サーバーの IP アドレスを [Destination] に入力して、サーバーのプロトコルを指定します。通常は、[Source] に **any** を使用します。終了したら、[Next] をクリックします。

たとえば、Web サーバー 10.1.1.5 および 10.1.1.6 を保護する場合は、次のように入力します。

- [Source] = any1
- [Destination] = 10.1.1.5、10.1.1.6

- [Destination Protocol] = tcp/http

ステップ 6 [Rule Actions] ページで、[Connection Settings] タブをクリックし、次のオプションを入力します。

- [初期接続（Embryonic Connections）]：ホストごとの初期 TCP 接続の最大数を 2000000 までの範囲で指定します。デフォルトは **0** で、最大初期接続数が許可されることを示します。たとえば、これを 1000 に設定できます。
- [クライアントごとの初期接続（Per Client Embryonic Connections）]：クライアントごとの同時初期 TCP 接続の最大数（2000000 まで）。クライアントごとの最大初期接続数の接続を ASA 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、ASA は接続を阻止します。たとえば、これを 50 に設定できます。
- **TCP Syn Cookie MSS**—初期接続数制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）（48 ～ 65535）。デフォルトは 1380 です。この設定は、**初期接続数**または**クライアントあたりの初期接続数**を構成する場合にのみ意味があります。

ステップ 7 [Finish] をクリックしてルールを保存し、[Apply] をクリックしてデバイスを更新します。

ステップ 8 **[Configuration]** > **[Firewall]** > **[Threat Detection]** を選択して、少なくとも [Threat Detection Statistics] グループの [TCP Intercept] 統計情報をイネーブルにします。

すべての統計情報をイネーブルにしたり、TCP 代行受信だけをイネーブルにしたりすることができます。また、モニタリング ウィンドウとレートを調整することもできます。

ステップ 9 **[Home]** > **[Firewall Dashboard]** を選択し、[Top Ten Protected Servers under SYN Attack] ダッシュボードを確認して結果をモニターします。

[Detail] ボタンをクリックすると、履歴サンプリング データが表示されます。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。

統計情報をクリアするには、[Tools] > [Command Line Interface] を使用して **clear threat-detection statistics tcp-intercept** コマンドを入力します。

異常な TCP パケット処理のカスタマイズ（TCP マップ、TCP ノーマライザ）

TCP ノーマライザは、検出されたときに ASA が処理（パケットの許可、ドロップ、またはクリアなど）できる異常なパケットを識別します。TCP 正規化は、攻撃から ASA を保護するのに役立ちます。TCP 正規化は常にイネーブルになっていますが、機能の一部の動作をカスタマイズできます。

TCP ノーマライザをカスタマイズするには、まず、TCP マップを使用して設定を定義します。次に、サービス ポリシーを使用して、選択したトラフィック クラスにマップを適用できます。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[TCP Maps]** を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] をクリックして、新しい TCP マップを追加します。マップの名前を入力します。
- マップを選択して [Edit] をクリックします。

ステップ 3 [Queue Limit] フィールドに、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 0 ～ 250 パケットの範囲で入力します。

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、および TCP check-retransmission の接続のキュー制限は 3 パケットです。ASA 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] を 1 以上に設定すると、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が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、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。

ステップ 4 [Timeout] フィールドで、異常なパケットがバッファに残存できる最大期間を 1 ～ 20 秒の間で設定します。

これらのパケットが配列されず、タイムアウト期間内に渡されなかった場合は、ドロップされます。デフォルトは 4 秒です。[Queue Limit] が 0 に設定されない場合は、すべてのトラフィックに関してタイムアウトを変更できません。[Timeout] が有効になるには、制限を 1 以上に設定する必要があります。

ステップ 5 [Reserved Bits] では、TCP ヘッダーに予約済みビットがあるパケットの処理方法（[Clear and allow]（パケットを許可する前にビットを削除する）、[Allow only]（ビットを変更しない（デフォルト））、または [Drop]（パケットを削除する））を選択します。

ステップ 6 次のいずれかのオプションを選択します。

- [Clear urgent flag] ：パケットを許可する前にパケットの URG フラグをクリアします。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。

- [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。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。
- [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ドロップします。
- [Check if transmitted data is the same as original] ：一貫性のない TCP 再送信を防止する再送信データ チェックを有効にします。
- [Drop packets which have past-window sequence]：ウィンドウ シーケンス番号を超えているパケット、つまり、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も大きい場合に、パケットをドロップします。これらのパケットを許可するには、このオプションを選択解除し、[Queue Limit] を 0（キュー制限をディセーブルにする）に設定します。
- [Drop SYN Packets with data] ：データを含む SYN パケットをドロップします。
- [Enable TTL Evasion Protection] ：接続の最大 TTL を最初のパケットで TTL によって決定させます。後続パケットの TTL は削減できますが、増やすことはできません。システムは、TTL をその接続の以前の最小 TTL にリセットします。これによって、TTL を回避した攻撃から保護します。

  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、ASA 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、ASA 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。
- [Verify TCP Checksum] ：TCP チェックサムを検証し、検証に失敗したパケットをドロップします。
- [Drop SYNACK Packets with data]：データを含む TCP SYNACK パケットをドロップします。
- [Drop packets with invalid ACK]：無効な ACK を含むパケットをドロップします。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。

（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。

ステップ 7 （任意）[TCP Options] タブをクリックして、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。

パケットを許可する前にオプションをクリアしたり、パケットに特定のタイプの単一オプションが含まれている場合にパケットを許可したり、パケットに特定のタイプのオプションが複数含まれていてもパケットを許可したりすることができます。デフォルトでは、他のすべてのオプションのクリア時に、特定のオプションがパケットごとに 1 回だけ表示される場合（それ以外の場合はパケットはドロップされます）に 5 つの名前付きオプションを許可します。また、MD5 または番号付きオプションのいずれかを含むパケットをドロップするように選択することもできます。TCP 接続をインスペクションする場合、設定に関係なく MSS オプションと選択的応答確認（SACK）オプションを除き、すべてのオプションがクリアされます。

a) [Selective Acknowledgement] 、[TCP Timestamp] 、および [Window Scale] オプションに対するアクションを選択します。

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。

b) [MSS]（最大セグメント サイズ） オプションに対するアクションを選択します。

通常の許可アクション、複数許可アクション、およびクリア アクションに加え、[Specify Maximum] を選択して、最大セグメント サイズ（68 ～ 65535）を入力できます。デフォルトの TCP MSS は、**[Configuration]** > **[Firewall]** > **[Advanced]** > **[TCP Options]** ページで定義されます。

c) **MD5 オプションを含むパケットを許可する**かどうかを選択します。

チェックボックスを選択解除すると、MD5 オプションを含むパケットはドロップされます。オプションを選択すると、通常アクション（許可、複数許可、またはクリア）を適用できます。

d) 番号の範囲別にオプションに対するアクションを選択します。

6 ～ 7、9 ～ 18、および 20 ～ 255 番のオプションはデフォルトでクリアされています。代わりにオプションを許可するか、またはオプションを含むパケットをドロップできます。さまざまなオプション範囲ごとに異なるアクションを指定できます。単に範囲の上下の数字を入力し、アクションを選択し、[Add] をクリックします。単一オプションに対するアクションを設定するには、上下の範囲に同じ数字を入力します。

設定した範囲を削除する場合は、その範囲を選択し、[削除（Delete）] をクリックします。

ステップ 8 [OK] および [Apply] をクリックします。

サービス ポリシーで TCP マップを使用できるようになります。マップがトラフィックに影響するのは、サービス ポリシーを通して適用された場合だけです。

ステップ 9 サービス ポリシーを使用して、TCP マップをトラフィック クラスに適用します。

a) [Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。
b) ルールを追加または編集します。ルールをグローバルに適用したり、インターフェイスに適用したりすることができます。たとえば、すべてのトラフィックに対して異常なパケットの処理をカスタマイズするには、すべてのトラフィックに一致するグローバル ルールを作成します。[Rule Actions] ページに進みます。
c) [Connection Settings] タブをクリックします。
d) [Use TCP Map] を選択し、作成したマップを選択します。
e) [Finish] または [OK] をクリックしてから、[Apply] をクリックします。

非対称ルーティングの TCP ステートチェックのバイパス（TCP ステートバイパス）

TCP ステートバイパスを使用すると、トラフィックは ASA デバイスでステートフル検査チェックをバイパスできます。

実装の注意事項

ネットワークで非対称ルーティング環境を設定し、特定の接続の発信フローと着信フローが 2 つの異なる ASA デバイスを通過できる場合は、影響を受けるトラフィックに TCP ステートバイパスを実装する必要があります。

ただし、TCP ステートバイパスによってネットワークのセキュリティが弱体化するため、非常に詳細に限定された通信クラスでバイパスを適用する必要があります。

非対称ルーティングの問題

非対称ルーティングの問題は、接続のリターントラフィックがアウトバウンドトラフィックとは異なるファイアウォールを通過する場合に発生します。この場合、パケットが高速パステーブルの既存の接続エントリと一致しないため、パケットがドロップされます。

トラフィック検査と高速パス動作

デフォルトでは、ASA はアダプティブ セキュリティ アルゴリズムを使用してすべてのトラフィックを検査します。ASA は、セキュリティポリシーに基づいてトラフィックを許可またはドロップします。ASA は、各パケットの状態（新しい接続か確立済みの接続か）を確認することにより、ファイアウォールのパフォーマンスを最大化します。新しい接続の SYN パケットをセッション管理パスに割り当てます。確立済みの接続を高速パスに割り当てます。高度な検査が必要なパケットをコントロールプレーンパスに割り当てます。

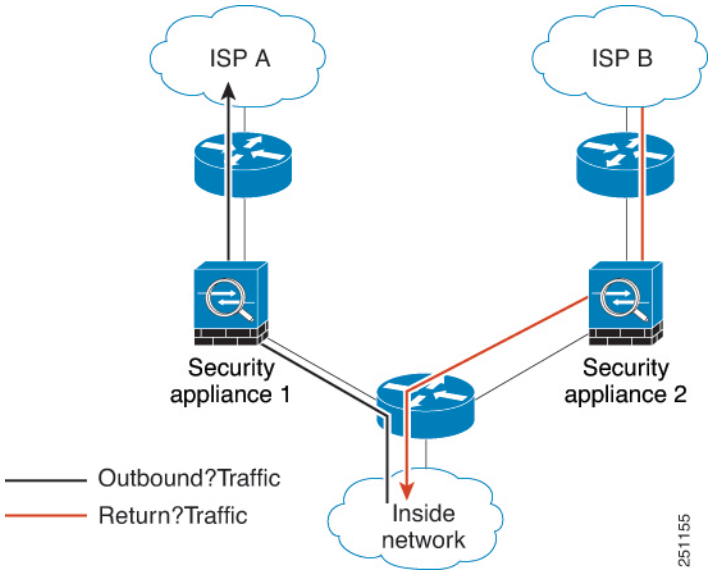
ASA は、既存の接続に一致する TCP パケットが、セキュリティポリシーのあらゆる側面を再チェックせずに高速パス経由で通過することを許可します。この機能により、パフォーマンスが向上します。ただし、高速パスの確立方式は、非対称ルーティングソリューションの妨げになる可能性があります。この方式では SYN パケットが使用され、TCP シーケンス番号の検証

などのチェックが実行されます。接続のアウトバウンドフローとインバウンドフローの両方が同じ ASA デバイスを通過する必要があります。

非対称ルーティングのシナリオ

たとえば、ある新しい接続がセキュリティ アプライアンス 1 に到達するとします。SYN パケットはセッション管理パスを通過し、接続のエントリが高速パステーブルに追加されます。この接続の後続パケットがセキュリティ アプライアンス 1 を通過した場合、高速パス内のエントリに一致するのでこのパケットは送信されます。しかし、後続のパケットがセキュリティアプライアンス 2 に送信され、そこで SYN パケットがセッション管理パスを通過していない場合、高速パスにはその接続のエントリが存在しないため、セキュリティアプライアンス 2 はパケットをドロップします。次の図は、非対称ルーティングの例を示したもので、アウトバウンド トラフィックはインバウンド トラフィックとは異なる ASA を通過しています。

図 *1* : 非対称ルーティング



アップストリームルータに非対称ルーティングが設定されていて、2 つの ASA デバイス間でトラフィックが交互に流れる場合は、特定のトラフィックに対して TCP ステートバイパスを設定できます。TCP ステート バイパスは、高速パスでのセッションの確立方法を変更し、高速パスのインスペクションを無効化します。この機能では、TCP トラフィックが UDP 接続と同様に処理されます。指定されたネットワークに一致する非 SYN パケットが ASA デバイスに入り、高速パスエントリが存在しない場合、そのパケットはセッション管理パスを通過して高速パスでの接続を確立します。いったん高速パスに入ると、トラフィックは高速パスのインスペクションをバイパスします。

TCP ステートバイパスのガイドラインと制限事項

TCP ステートバイパスでサポートされない機能

TCP ステートバイパスを使用する場合、次の機能はサポートされません。

- アプリケーションインスペクション：インスペクションでは、着信トラフィックと発信トラフィックの両方が同じ ASA を通過する必要があるため、インスペクションは TCP ステート バイパス トラフィックに適用されません。
- AAA 認証セッション：ユーザーがある ASA で認証される場合、他の ASA 経由で戻るトラフィックは、その ASA でユーザーが認証されていないため、拒否されます。
- TCP 代行受信、最大初期接続制限、TCP シーケンス番号ランダム化：ASAでは接続の状態が追跡されないため、これらの機能は適用されません。
- TCP 正規化：TCP ノーマライザはディセーブルです。
- サービス モジュール機能：TCP ステート バイパスと、ASA FirePOWER などの任意のタイプのサービス モジュール上で実行されるアプリケーションを使用することはできません。

TCP ステートバイパスの NAT ガイドライン

変換セッションはデバイスごとに個別に確立されるため、TCP ステート バイパス トラフィック用に両方のデバイスでスタティック NAT を設定する必要があります。ダイナミック NAT を使用すると、デバイス 1 でのセッションに選択されるアドレスは、デバイス 2 でのセッションに選択されるアドレスとは異なります。

TCP ステート バイパスの設定

非対称ルーティング環境で TCP ステートチェックをバイパスするには、影響を受けるホストまたはネットワークのみに適用するトラフィッククラスを注意深く定義してから、サービスポリシーを使用してトラフィッククラスで TCP ステートバイパスを有効にします。バイパスによってネットワークのセキュリティが低下するため、そのアプリケーションをできるだけ制限します。

始める前に

特定の接続に 2 分間トラフィックがない場合、接続はタイムアウトします。このデフォルトは TCP ステート バイパス トラフィック クラスの [アイドル接続タイムアウト（Idle Connection Timeout）] を変更するとオーバーライドできます通常の TCP 接続は、デフォルトで 60 分後にタイムアウトします。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Service Policy]** を選択します。

ステップ 2 **[Add]** > **[Add Service Policy Rule]** をクリックします。

または、ホストのルールがすでにある場合、ルールを編集します。

ステップ 3 ルールを特定のインターフェイスに適用するか、すべてのインターフェイスにグローバルに適用するかどうかを選択して、[Next] をクリックします。

ステップ 4 トラフィック分類の場合は、[Source and Destination IP Addresses (uses ACL)] を選択して、[Next] をクリックします。

ステップ 5 ACL ルールの場合は、[Source] と [Destination] にルートの両端のホストの IP アドレスを入力して、プロトコルを TCP として指定します。終了したら、[Next] をクリックします。

10.1.1.1 ～ 10.2.2.2 の間で TCP ステート チェックをバイパスする場合は、次のように入力します。

- [Source] = 10.1.1.1
- [Destination] = 10.2.2.2
- [Destination Protocol] = tcp

ステップ 6 [Rule Actions] ページで、[Connection Settings] タブをクリックし、[TCP State Bypass] を選択します。

ステップ 7 [Finish] をクリックしてルールを保存し、[Apply] をクリックしてデバイスを更新します。

TCP シーケンスのランダム化の無効化

各 TCP 接続には、クライアントで生成される ISN とサーバーで生成される ISN の 2 つの ISN があります。ASA 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。ただし、TCP シーケンスのランダム化は、TCP SACK（選択的確認応答）を実質的に破棄します。クライアントが認識するシーケンス番号がサーバーが認識するものと異なるためです。

たとえば、データがスクランブルされるため、必要に応じて TCP 初期シーケンス番号ランダム化を無効化することができます。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。
- ASA 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。
- ASA 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。
- ISA 3000 のハードウェア バイパスを有効にします。ISA 3000 がデータ パスの一部でなくなると、TCP 接続はドロップされます。

（注） クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Service Policy]** を選択します。

ステップ 2 **[Add]** > **[Add Service Policy Rule]** をクリックします。

または、ターゲットのトラフィックのルールがすでにある場合、ルールを編集します。

ステップ 3 ルールを特定のインターフェイスに適用するか、すべてのインターフェイスにグローバルに適用するかどうかを選択して、[Next] をクリックします。

ステップ 4 トラフィック分類の場合は、トラフィック一致のタイプを識別します。クラスマップは、TCP トラフィック用にします。TCP ポート一致を行う特定のホストを識別したり（ACL を使用して）、任意のトラフィックと照合したりすることができます。[Next] をクリックし、ACL でホストを設定するか、ポートを定義して、[Next] を再度クリックします。

たとえば、10.2.2.2 に送信するすべての TCP トラフィックに対して TCP シーケンス番号ランダム化をディセーブルにする場合は、次のように入力します。

- [Source] = any1
- [Destination] = 10.2.2.2
- [Destination Protocol] = tcp

ステップ 5 [Rule Actions] ページで、[Connection Settings] タブをクリックし、[Randomize Sequence Number] をオフにします。

ステップ 6 [Finish] をクリックしてルールを保存し、[Apply] をクリックしてデバイスを更新します。

大規模フローのオフロード

データセンターのサポートされているデバイス上で Cisco ASA を展開する場合は、超高速パスにオフロードするトラフィックを識別して、トラフィックが NIC 自身でスイッチングされるようにできます。オフロードによって、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。

- ハイパフォーマンス コンピューティング（HPC）調査サイト。ここでは、ASA はストレージと高コンピューティング ステーション間で展開されます。1 つの調査サイトが NFS 経由の FTP ファイル転送またはファイル同期を使用してバックアップを行うと、大量のデータ トラフィックが ASA 上のすべてのコンテキストに影響を与えます。NFS を介する FTP

ファイル転送およびファイル同期のオフロードによって、他のトラフィックへの影響が軽減されます。

- 主にコンプライアンス目的で使用される High Frequency Trading（HFT）。ここでは、ASA はワークステーションと Exchange 間で展開されます。セキュリティは通常は問題にはなりませんが、遅延は大きな問題です。

オフロードされる前に、ASA は接続の確立時にアクセス ルールやインスペクションなどの通常のセキュリティ処理を最初に適用します。ASA のセッションも切断されます。ただし、一旦接続が確立されると、オフロードされる資格があれば、さらなる処理が ASA ではなく NIC で行われます。

オフロードされたフローは、基本的な TCP フラグとオプションのチェック、設定した場合にはチェックサムの確認などの、制限されたステートフル インスペクションを受信し続けます。システムは必要に応じてさらなる処理のためにファイアウォール システムへのパケットを選択的に増やすことができます。

オフロードが可能なフローを識別するには、フロー オフロード サービスを適用するサービス ポリシー ルールを作成します。一致するフローはその後、次の条件を満たす場合にオフロードされます。

- IPv4 アドレスのみ。
- TCP、UDP、GRE のみ。
- 標準または 802.1Q タグ付きイーサネット フレームのみ。
- （トランスペアレント モードのみ。）インターフェイスを 2 つだけ含むブリッジ グループのマルチキャスト フロー。

オフロードされたフローのリバース フローもオフロードされます。

フローオフロードの実装に関する制限事項

デバイスの制限事項

この機能は、以下のデバイスでサポートされています。

- Firepower 4100/9300

オフロードできないフロー

次のフロータイプをオフロードしようとしないでください。

- IPv6 アドレッシングなど、IPv4 アドレッシングを使用しないフロー。
- TCP、UDP、GRE 以外のプロトコルに対するフロー。

（注） PPTP GRE 接続はオフロードできません。

- インスペクションが必要なフロー。FTP など場合によっては、コントロール チャネルはオフロードできませんがセカンダリ データ チャネルはオフロードできます。
- ASA FirePOWER など別のモジュールを通過するフロー。
- デバイスで終端する IPsec および TLS/DTLS VPN 接続。

（注） Secure Firewall 3100 および Secure Firewall 4200 のプラットフォームは、この制限の例外です。これらのプラットフォームでは、そのデバイスで終端する IPsec VPN 接続および DTLS VPN 接続のフローオフロードがサポートされています。この機能およびその実装の詳細については、Secure Firewall 3100 および Secure Firewall 4200 のプラットフォーム特有のリリースノートを参照してください。

- ルーテッド モードのマルチキャスト フロー。
- 3 つ以上のインターフェイスがあるブリッジ グループに対するトランスペアレント モードのマルチキャスト フロー。
- TCP インターセプト フロー。
- TCP ステートバイパスフロー。同じトラフィックにフローオフロードと TCP ステートバイパスを設定することはできません。
- AAA カットスループロキシフロー。
- Vpath、VXLAN 関連のフロー。
- セキュリティ グループでタグ付けされたフロー。
- クラスターで非対称フローが発生した場合に備えて、別のクラスターノードから転送されるリバースフロー。
- クラスタ内の一元化されたフロー（フローのオーナーが制御ユニットでない場合）。

その他の制限事項

フローオフロードを導入する場合は、次の運用上の制約事項を考慮してください。

- フローオフロードとデッド接続検出（DCD）は互換性がありません。オフロードできる接続に DCD を設定しないでください。
- フローオフロード条件に一致する複数のフローがキューイングされて、ハードウェア上の同じ場所に同時にオフロードされる場合、最初のフローのみがオフロードされます。他のフローは通常どおりに処理されます。これをコリジョン（衝突）といいます。この状況の統計を表示するには、CLI で **show flow-offload flow** コマンドを使用します。

- オフロードされたフローはFXOSインターフェイスを通過しますが、それらのフローの統計は論理デバイスインターフェイスには表示されません。したがって、論理デバイスインターフェイスのカウンタとパケットレートには、オフロードされたフローは反映されません。

オフロードを無効にする条件

フローがオフロードされた後、フロー内のパケットは次の条件を満たす場合にファイアウォール オペレーティング システムに返され、さらに処理されます。

- タイムスタンプ以外の TCP オプションが含まれている。
- フラグメント化されている。
- これらは等コスト マルチパス（ECMP）ルーティングの対象であり、入力パケットは 1 つのインターフェイスから別のインターフェイスに移動する。
- ルーティングテーブルへの変更がフローに適用されます。新しいルートを決定するためにパケットがデバイスに返されます。

フロー オフロードの設定

フロー オフロードを設定するには、サービスをイネーブルにしてから、オフロードする対象トラフィックを識別するサービス ポリシーを作成する必要があります。最初にサービスを有効にするときは、再起動する必要があります。

手順

ステップ 1 フロー オフロード サービスをイネーブルにします。

最初にサービスを有効にするときは、再起動する必要があります。

リロードが必要な場合、ヒットレスなモード変更を行うには、クラスタまたはフェールオーバーペアに関して特に考慮すべき事柄があります。

- クラスタリング：最初に制御ノードでコマンドを入力しますが、制御ノードをすぐにリブートしないでください。代わりに、まずクラスタの各ノードをリブートしてから、制御ノードに戻ってリブートします。次に、制御ノード上でオフロードサービスポリシーを設定します。
- フェールオーバー：最初にアクティブユニット上でコマンドを入力しますが、アクティブユニットをすぐにリブートしないでください。代わりに、スタンバイ ユニットをリブートしてから、アクティブ ユニットをリブートします。次に、アクティブ ユニット上でオフロード サービス ポリシーを設定します。

a) **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Offload Engine]** を選択します。
b) **[オフロードエンジンの有効化（Enable Offload Engine）]** をオンにします。
c) [Apply] をクリックします。

d) [Save] をクリックし、変更内容をスタートアップ コンフィギュレーションに保存します。
e) **[ツール（Tools）]** > **[システムリロード（System Reload）]** を選択して、デバイスをリブートします。

ステップ 2 オフロードする対象のトラフィックを識別するサービス ポリシー ルールを作成します。

a) **[Configuration]** > **[Firewall]** > **[Service Policy]** を選択します。
b) **[Add]** > **[Add Service Policy Rule]** をクリックします。

   または、ホストのルールがすでにある場合、ルールを編集します。

c) ルールを特定のインターフェイスに適用するか、すべてのインターフェイスにグローバルに適用するかどうかを選択して、[Next] をクリックします。
d) トラフィック分類の場合は、アクセス リスト（**[Source and Destination IP Addresses (uses ACL)]**）またはポート（**[TCP or UDP or SCTP Destination Port]**）による照合が最も一般的なオプションです。オプションを選択して [Next] をクリックします。
e) ACL またはポートの条件を入力します。終了したら、[Next] をクリックします。

   たとえば、10.1.1.0/255.255.255.224 サブネット上のすべての TCP トラフィックをオフロードの対象とする場合は、次のように入力します。

   - [Source] = 10.1.1.0/255.255.255.224（または 10.1.1.0/27）
   - [Destination] = any
   - [Destination Protocol] = tcp

f) [Rule Actions] ページで、[Connection Settings] タブをクリックし、[Flow Offload] を選択します。
g) [Finish] をクリックしてルールを保存し、[Apply] をクリックしてデバイスを更新します。

特定のトラフィック クラスの接続の設定（すべてのサービス）

サービス ポリシーを使用して、特定のトラフィック クラスに対してさまざまな接続の設定を行うことができます。サービス ポリシーを使用して、次の内容を実行します。

- DoS 攻撃と SYN フラッディング攻撃から保護するのに使用される接続制限と接続タイムアウトをカスタマイズします。
- アイドル状態でも有効な接続を維持するように、Dead Connection Detection（DCD; デッド接続検出）を実装します。
- TCP シーケンス番号ランダム化が不要な場合、それをディセーブルにします。
- TCP ノーマライザが異常な TCP パケットから保護する方法をカスタマイズします。
- 非対称ルーティングの対象であるトラフィックに対して TCP ステートバイパスを導入します。バイパス トラフィックはインスペクションの対象になりません。

- SCTP ステートフル インスペクションをオフにするには、Stream Control Transmission Protocol（SCTP）ステート バイパスを実装します。
- サポート対象のハードウェア プラットフォームのパフォーマンスを向上させるには、フロー オフロードを実装します。
- ASA がトレース ルート出力に表示されるように、パケットの存続可能時間（TTL）をデクリメントします。

（注） パケット存続時間（TTL）をデクリメントすると、TTL が 1 のパケットはドロップされますが、接続に TTL がより大きいパケットを含むと想定されるセッションでは、接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL = 1 で送信されるため、トランスペアレントモードの ASA デバイスでは、パケット存続時間をデクリメントすると予期しない結果が発生する可能性があります。ASA がルーテッドモードで動作している場合は、パケット存続時間の設定をデクリメントしても OSPF のプロセスに影響を与えません。

同時に使用できない TCP ステート バイパスと TCP ノーマライザのカスタマイズを除き、特定のトラフィック クラスに対してこれらの設定の任意の組み合わせを設定できます。

ヒント この手順は、ASA を通過するトラフィックのサービス ポリシーを示します。管理（to the box）トラフィックに対して接続の最大数と初期接続の最大数を設定することもできます。

始める前に

TCP ノーマライザをカスタマイズする場合は、続行する前に必要な TCP マップを作成してください。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Service Policy]** を選択して、ルールを開きます。

- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。ウィザードの [Rules] ページまで進みます。
- 接続の設定を変更するルールがある場合は、それを選択して [Edit] をクリックします。

ステップ 2 [Rule Actions] ウィザード ページまたはタブで、[Connection Settings] タブを選択します。

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。

デフォルトでは、接続制限はありません。制限を実装すると、システムはそれらの追跡を開始する必要があります。これにより、CPUとメモリの使用率が増加し、特にクラスタでは高負荷がかかったシステムに動作上の問題が発生する可能性があります。

- [Maximum TCP & UDP Connections][Maximum TCP, UDP and SCTP Connections] ：（TCP、UDP、SCTP）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最大数（2000000まで）。デフォルトは0で、最大可能接続数が許可されることを示します。TCP接続の場合、これは確立された接続のみに適用されます。
- [Embryonic Connections] ：ホストごとの初期 TCP 接続の最大数を 2000000 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。デフォルトは **0** で、最大初期接続数が許可されることを示します。0 以外の制限を設定することで、TCP 代行受信を有効にします。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。また、クライアントごとのオプションを設定して、SYN フラッディングから保護します。
- [Per Client Connections]： （TCP、UDP、SCTP）クライアントごとの同時接続の最大数を指定します（最大 2000000）。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、ASAは、その接続を拒否してパケットをドロップします。TCP接続の場合、これには確立済み接続、ハーフオープン接続、ハーフクローズ接続が含まれています。
- [Per Client Embryonic Connections]：クライアントごとの同時 TCP 初期接続の最大数を 2000000 までの範囲で指定します。クライアントごとの最大初期接続数の接続をASA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、ASA は接続を阻止します。
- **TCP Syn Cookie MSS**—初期接続数制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）（48 ～ 65535）。デフォルトは 1380 です。この設定は、**初期接続数**または**クライアントあたりの初期接続数**を構成する場合にのみ意味があります。

ステップ 4 接続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。

- [Embryonic Connection Timeout] ：初期（ハーフオープン）TCP 接続スロットが解放されるまでのアイドル時間。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を閉じるまでのアイドル タイムアウト期間（0:5:0（9.1(1) 以前の場合）または 0:0:30（9.1(2) 以降の場合）～ 1193:0:0）。デフォルト値は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、ASAは、ハーフクローズ接続を切断するときにリセットを送信しません。
- [Idle Connection Timeout] ：（TCP だけでなく、あらゆるプロトコルの）接続スロットが解放されるまでのアイドル時間。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] ：ASA 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かどうか。
- [Dead Connection Detection (DCD)]：Dead Connection Detection（DCD; デッド接続検出）をイネーブルにするかどうか。アイドル接続の期限が切れる前に、ASA はエンド ホストにプローブを送信して接続が有効であるかどうかを判断します。両方のホストが応答した場合は、接続が維持されます。それ以外の場合は、接続が解放されます。最大試行回数（デフォルトは 5 で、範囲は 1 ～ 255）と、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期間である試行間隔（デフォルトは 0:0:15 で、範囲は 0:0:1 ～ 24:0:0）を設定します。トランスペアレント ファイアウォール モードで動作している場合、エンドポイントにスタティック ルートを設定する必要があります。オフロードも行われる接続には DCD を設定できないため、DCD とフローオフロードのトラフィック クラスが重複しないようにしてください。発信側と受信側で送信された DCD プローブの個数を追跡するには、**show conn detail** コマンドを使用します。

  クラスタまたは高可用性構成で動作しているシステムでは、間隔を 1 分（0:1:0）未満に設定しないことを推奨します。接続をシステム間で移動する必要がある場合、必要な変更には 30 秒以上かかり、変更が行われる前に接続が削除される場合があります。

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。

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。

ステップ 6 TCP ノーマライザの動作をカスタマイズするには、[Use TCP Map] をオンにし、ドロップダウンリストあら既存の 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。

ステップ 7 クラスに一致するパケット存続可能時間（TTL）をデクリメントするには、[Decrement time to live for a connection] をオンにします。

TTL のデクリメントは、ASA がトレース ルートにホップの 1 つとして表示されるために必要です。また、[Configuration] > [Device Management] > [Management Access] > [ICMP] で ICMP 到達不能メッセージのレート制限を増やす必要もあります。

ステップ 8 TCP ステート バイパスをイネーブルにするには、[TCP State Bypass] をオンにします。

ステップ 9 SCTP ステート バイパスをイネーブルにするには、[SCTP State Bypass] をオンにします。

SCTP ステートフル インスペクションをオフにするには、SCTP ステート バイパスを実装します。詳細については、SCTP ステートフル インスペクションを参照してください。

ステップ 10 （Firepower 4100/9300 シャーシ の ASA、FXOS 1.1.3 以降のみ。）フロー オフロードを有効にするには、[Flow Offload] をオンにします。

フローが NIC 自体で切り替えられる超高速パスにオフロードされる適切なトラフィック。オフロード サービスを有効にする必要もあります。**[Configuration]** > **[Firewall]** > **[Advanced]** > **[Offload Engine]** を選択します。

ステップ 11 [OK] または [Finish] をクリックします。

TCP オプションの構成

各種オプションを構成して、TCP 動作のいくつかの側面を制御できます。これらの設定のデフォルト値は、ほとんどのネットワークに適しています。

手順

ステップ 1 **[構成（Configuration）] > [ファイアウォール（Firewall）] > [詳細（Advanced）] > [TCPオプション（TCP Options）]** の順に選択します。

ステップ 2 インターフェイスごとの TCP リセット動作を構成します。

a) 変更するインターフェイスを選択し、[編集（Edit）] をクリックします。

b) 使用するオプションを選択します。

- **拒否されたインバウンド TCP パケットのリセット応答を送信します。**ASA の通過を試み、アクセスリストまたは AAA 設定に基づいて ASA によって拒否されたすべての着信 TCP セッションに TCP リセットを送信します。ASA は、アクセスリストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。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かった場合、ASA は拒否されたパケットを何も通知せずに廃棄します。

c) [OK] をクリックします。

ステップ 3 その他の TCP オプションを構成します。

- **拒否された外部 TCP パケットのリセット応答を送信します。**最もセキュリティレベルの低いインターフェイスで終端し、アクセスリストまたは AAA 設定に基づいて ASA によって拒否された TCP パケットのリセットを送信します。ASA は、アクセスリストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。このオプションをイネーブルにしなかった場合、ASA は拒否された接続パケットを何も通知せずに廃棄します。

  インターフェイス PAT では、このオプションを使用することを推奨します。このオプションを使用すると、外部 SMTP または FTP サーバーからの IDENT を ASA で終端できます。これらの接続をアクティブにリセットすることによって、30 秒のタイムアウト遅延を回避できます。

- **TCP 接続の最大セグメント サイズを強制的に X バイトにします。**最大 TCP セグメントサイズをバイト単位で設定します（48 ～任意の最大値）。デフォルト値は 1380 バイトです。この機能をディセーブルにするには、bytes を 0 に設定します。

- **TCP 接続の最小セグメントサイズを強制的に X バイトにします。**最大セグメントサイズを上書きし、bytes 未満にならないようにします（48 ～ 65535 バイト）。この機能は、デフォルトでディセーブルです（0 に設定）。
- **TCP の終了後、少なくとも 15 秒間、TCP 接続を TIME_WAIT 状態に強制的に維持します。**最終的な通常の TCP クローズダウンシーケンスのあと、各 TCP 接続が 15 秒以上短縮 TIME_WAIT 状態で維持されるよう強制します。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。
- **TCP 最大未処理セグメント数**。TCP 未処理セグメントの最大数を 6 ～ 24 に設定します。デフォルト値は 6 です。SIP 電話機が Call Manager に接続していないことを確認したら、未処理の TCP セグメントの最大数を増やすことができます。

ステップ 4 [Apply] をクリックします。

接続のモニタリング

次のページを使用して、接続をモニターします。

- **[Home]** > **[Firewall Dashboard]** で、[Top Ten Protected Servers under SYN Attack] ダッシュボードを確認して TCP 代行受信をモニターします。[Detail] ボタンをクリックすると、履歴サンプリングデータが表示されます。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。
- **[Monitoring]** > **[Properties]** > **[Connections]** で、現在の接続を表示します。
- **[Monitoring]** > **[Properties]** > **[Connection Graphs]** で、パフォーマンスをモニターします。

さらに、**[Tools]** > **[Command Line Interface]** を使用して次のコマンドを入力できます。

- **show conn** [**detail**]

  接続情報を表示します。詳細情報は、フラグを使用して特別な接続の特性を示します。たとえば、「b」フラグは、TCPステート バイパスの対象であるトラフィックを示します。

  detail キーワードを使用すると、デッド接続検出（DCD）プローブの情報が表示されます。この情報は、発信側と応答側で接続がプローブされた頻度を示します。たとえば、DCD 対応接続の接続詳細は次のようになります。

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show flow-offload**{**info** [**detail**] | **cpu** | **flow** [**count** | **detail**] | **statistics**}

全般的なステータス情報、オフロードの CPU 使用率、オフロードされたフローの数と詳細、オフロードされたフロー統計情報を含む、フローのオフロードに関する情報を示します。

- **show service-policy**

  Dead Connection Detection（DCD; デッド接続検出）の統計情報を含むサービス ポリシーの統計情報を表示します。

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  攻撃を受けて保護された上位 10 サーバーを表示します。**all** キーワードは、トレースされているすべてのサーバーの履歴データを表示します。**detail** キーワードは、履歴サンプリング データを表示します。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。

（注） Cisco ASA 設定では、初期接続（3 ウェイ ハンドシェイク プロセスがまだ完了していない接続要求）はすぐに閉じられ、アクティブデバイスとスタンバイデバイス間で同期されません。この設計により、HA システムの効率とセキュリティが確保されます。このため、両方の Cisco ASA で接続数に違いが生じる可能性がありますが、これは予想されることです。

接続設定の履歴

機能名	プラットフォームリリース	説明
TCP ステート バイパス	8.2(1)	この機能が導入されました。**set connection advanced-options tcp-state-bypass** コマンドが導入されました。
すべてのプロトコルの接続タイムアウト	8.2(2)	アイドル タイムアウトは、TCP だけでなく、すべてのプロトコルに適用するように変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policies] > [Rule Actions] > [Connection Settings]。

機能名	プラットフォームリリース	説明
バックアップ スタティック ルートを使用する接続のタイムアウト	8.2(5)/8.4(2)	同じネットワークへの複数のスタティック ルートが存在しており、それぞれメトリックが異なる場合は、ASA は接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは0です（接続はタイムアウトしません）。この機能を使用するには、タイムアウトを新しい値に変更します。 次の画面が変更されました。[Configuration] > [Firewall] > [Advanced] > [Global Timeouts]。
PAT xlate に対する設定可能なタイムアウト	8.4(3)	PAT xlate がタイムアウトし（デフォルトでは 30 秒後）、ASA が新しい変換用にポートを再使用すると、一部のアップストリーム ルータは、前の接続がアップストリーム デバイスで依然として開いている可能性があるため、この新しい接続を拒否する場合があります。PAT xlate のタイムアウトを、30 秒～ 5 分の範囲内の値に設定できるようになりました。 次の画面が変更されました。[Configuration] > [Firewall] > [Advanced] > [Global Timeouts]。 この機能は、*8.5(1)* または *8.6(1)* では使用できません。
サービス ポリシー ルールの最大接続数の引き上げ	9.0(1)	サービス ポリシー ルールの最大接続数が 65535 から 2000000 に引き上げられました。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules] > [Connection Settings]。
ハーフ クローズ タイムアウト最小値を 30 秒に削減	9.1(2)	グローバルタイムアウトおよび接続タイムアウトの両方のハーフ クローズド タイムアウトの最小値は、より優れた DoS 保護を提供するために 5 分から 30 秒に短縮されました。 次の画面が変更されました。 [Configuration] > [Firewall] > [Service Policy Rules] > [Connection Settings]、 [Configuration] > [Firewall] > [Advanced] > [Global Timeouts]

機能名	プラットフォームリリース	説明
ルートの収束に対する接続ホールドダウン タイムアウト。	9.4(3) 9.6(2)	接続で使用されているルートがもう存在していない、または非アクティブになったときに、システムが接続を保持する時間を設定できるようになりました。このホールドダウン期間内にルートがアクティブにならない場合、接続は解放されます。ルートの収束がさらに迅速に行われるようにホールドダウンタイマーを短縮することができます。ただし、ほとんどのネットワークでは、ルートのフラッピングを防止するためにデフォルトの 15 秒が適切です。 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Global Timeouts]** の画面が変更されました。
SCTP アイドル タイムアウトおよび SCTP ステート バイパス	9.5(2)	SCTP 接続のアイドル タイムアウトを設定できます。また、SCTP ステート バイパスを有効にして、トラフィックのクラスで SCTP ステートフル インスペクションをオフにできます。 次の画面が変更されました：**[Configuration]** > **[Firewall]** > **[Advanced]** > **[Global Timeouts]**、**[Configuration]** > **[Firewall]** > **[Service Policy Rules]** ウィザード、[Connection Settings] タブ。
Firepower 9300 上の ASA のフロー オフロード。	9.5(2.1)	ASA からオフロードされ、（Firepower 9300 上の）NIC に直接切り替えられる必要があるフローを特定できます。これにより、データセンターのより大きなデータ フローのパフォーマンスが向上します。 この機能には、FXOS 1.1.3 が必要です。 次の画面が追加または変更されました：**[Configuration]** > **[Firewall]** > **[Advanced]** > **[Offload Engine]**、**[Configuration]** > **[Firewall]** > **[Service Policy Rules]** の下でルールを追加または編集する場合の **[Rule Actions]** > **[Connection Settings]** タブ。
Firepower 4100 シリーズ 上の ASA のフロー オフロードのサポート。	9.6(1)	ASA からオフロードされ、Firepower 4100 シリーズ の NIC で直接切り替える必要があるフローを特定できます。 この機能では、FXOS 1.1.4 が必要です。 この機能には、新規のコマンドまたは ASDM 画面はありません。

機能名	プラットフォームリリース	説明
トランスペアレント モードでのマルチキャスト接続のフローオフロードのサポート。	9.6(2)	トランスペアレント モードの Firepower 4100 および 9300 シリーズ デバイスで、NIC に直接切り替えられるマルチキャスト接続をオフロードできるようになりました。マルチキャスト オフロードは、インターフェイスを 2 つだけ含むブリッジ グループに使用できます。 この機能には、新規のコマンドまたは ASDM 画面はありません。
TCP オプション処理の変更。	9.6(2)	TCP マップを設定する際にパケットの TCP ヘッダー内の TCP MSS および MD5 オプションに対するアクションを指定できるようになりました。さらに、MSS、タイムスタンプ、ウィンドウ サイズ、および選択的確認応答オプションのデフォルトの処理が変更されました。以前は、これらのオプションは、ヘッダーに特定のタイプのオプションが 2 つ以上ある場合でも許可されていました。現在は、パケットに特定のタイプのオプションが 2 つ以上含まれている場合、そのパケットはデフォルトでドロップされます。たとえば、以前は 2 つのタイムスタンプ オプションがあるパケットは許可されていましたが、現在はドロップされます。 MD5、MSS、選択的確認応答、タイムスタンプ、およびウィンドウ サイズに対し、同じタイプの複数のオプションを有効にするための TCP マップを設定できます。MD5 オプションの場合、以前のデフォルトではオプションがクリアされたのに対し、現在のデフォルトでは許可されます。また、MD5 オプションを含むパケットをドロップすることもできます。MSS オプションの場合は、TCP マップで最大セグメント サイズを設定できます（トラフィック クラスごとに）。他のすべての TCP オプションのデフォルトに変更はありません。これらはクリアされます。 次の画面が変更されました：**[Configuration]** > **[Firewall]** > **[Objects]** > **[TCP Maps]**[Add/Edit] ダイアログボックス
内部ゲートウェイ プロトコルの古いルートのタイムアウト	9.7(1)	OSPF などの内部ゲートウェイ プロトコルの古いルートを削除するためのタイムアウトを設定できるようになりました。 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Global Timeouts]** の画面が変更されました。

機能名	プラットフォームリリース	説明
ICMP エラーのグローバル タイムアウト	9.8(1)	ASA が ICMP エコー応答パケットを受信してから ICMP 接続を削除するまでのアイドル時間を設定できるようになりました。このタイムアウトが無効（デフォルト）で、ICMP インスペクションが有効に設定されている場合、ASA はエコー応答を受信するとすぐに ICMP 接続を削除します。したがって、終了しているその接続に対して生成されたすべての ICMP エラーは破棄されます。このタイムアウトは ICMP 接続の削除を遅らせるので、重要な ICMP エラーを受信することが可能になります。 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Global Timeouts]** の画面が変更されました。
TCP ステート バイパスのデフォルトのアイドル タイムアウト	9.10(1)	TCP ステート バイパス接続のデフォルトのアイドル タイムアウトは 1 時間ではなく、2 分になりました。
デッド接続検出（DCD）の発信側および応答側の情報、およびクラスタ内の DCD のサポート。	9.13(1)	デッド接続検出（DCD）を有効にした場合は、**show conn detail** コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。**show conn** の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。 新規/変更された画面：なし。
初期接続の最大セグメントサイズ（MSS）を設定します。	9.16(1)	サービスポリシーを設定して、初期接続制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）を設定できます。これは、最大初期接続数も設定するサービスポリシーの場合に意味があります。 追加または変更された画面：[Add/Edit Service Policy] ウィザードの [Connection Settings]
SIP Call Init のアイドル グローバル タイムアウトの設定	9.16(x)	Call_Init コール状態の SIP セッションが（最初の招待メッセージの受信後）削除されるまでのアイドル時間（つまり応答を受信しなかった場合）を、0:0:1 ～ 1193:0:0 の範囲で設定できます。デフォルト値は 32 秒（0:00:32）です。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。