接続の設定

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。接続の設定には、次のものが含まれます。

- 最大接続数（TCP および UDP 接続、初期接続、クライアントあたりの接続）
- 接続タイムアウト
- デッド接続検出
- TCP シーケンスのランダム化
- TCP 正規化カスタマイゼーション
- TCP ステート バイパス
- グローバル タイムアウト

この章は、次の項で構成されています。

接続の設定に関する情報

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 代行受信および初期接続の制限

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。ASA 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、ASA 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。ASA 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。

（注） TCP SYN クッキー保護を使用して SYN 攻撃からサーバを保護する場合、保護するサーバの TCP SYN バックログ キューより低い初期接続制限を設定する必要があります。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 攻撃中にサーバにアクセスできなくなります。

TCP 代行受信に関する統計情報（攻撃を受けた上位 10 サーバなど）を表示する方法については、第 26 章「脅威検出の設定」を参照してください。

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、ASA 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）

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 シーケンスのランダム化

各 TCP 接続には、クライアントで生成される ISN とサーバで生成される 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。

保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

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。例：

- 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。

TCP の正規化

TCP 正規化機能は、検出時に ASA が対処できる異常なパケットを識別します。ASA 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 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 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 マップを使用した TCP ノーマライザのカスタマイズ」（P.21-6）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。ASA 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、ASA 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 ステート バイパス

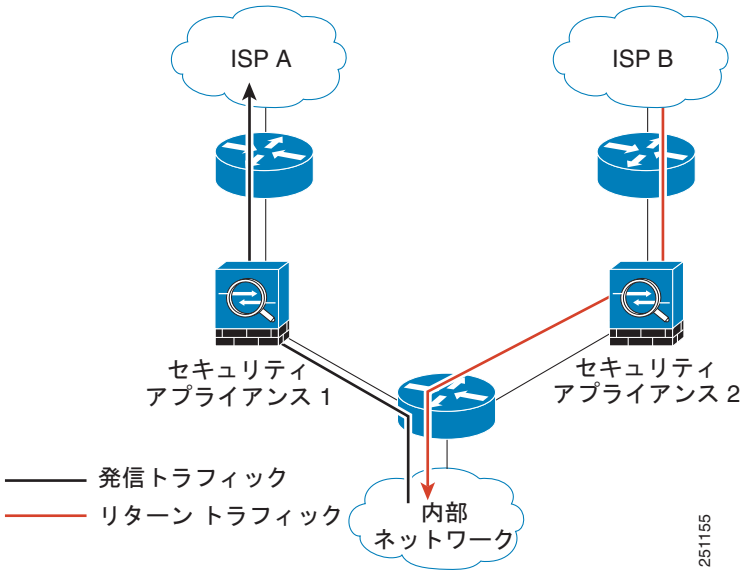
デフォルトでは、ASA を通過するトラフィックはすべて、アダプティブ セキュリティ アルゴリズムを使用して検査され、セキュリティ ポリシーに基づいて、通過を許可されるか、またはドロップされます。ASA では、各パケットの状態（新規接続であるか、または確立済み接続であるか）がチェックされ、そのパケットをセッション管理パス（新規接続の SYN パケット）、高速パス（確立済みの接続）、またはコントロール プレーン パス（高度なインスペクション）に割り当てることによって、ファイア

ウォールのパフォーマンスが最大化されます。ステートフル ファイアウォールの詳細については、一般的な操作のコンフィギュレーション ガイドの“Stateful Inspection Overview” section on page 1-20を参照してください。

高速パスの既存の接続に一致する TCP パケットは、セキュリティ ポリシーのあらゆる面の再検査を受けることなく ASA を通過できます。この機能によってパフォーマンスは最大になります。ただし、SYN パケットを使用して高速パスにセッションを確立する方法、および高速パスで行われるチェック（TCP シーケンス番号など）が、非対称ルーティング ソリューションの障害となる場合があります。これは、接続の発信フローと着信フローの両方が同じ ASA を通過する必要があるためです。

たとえば、ある新しい接続が ASA 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。この接続の後続のパケットが ASA 1 を通過する場合、パケットは高速パスのエントリと一致して、通過します。しかし、後続のパケットが ASA 2 に到着すると、SYN パケットがセッション管理パスを通過していないために、高速パスにはその接続のエントリがなく、パケットはドロップされます。図 21-1 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 21-1　非対称ルーティング



アップストリーム ルータに設定された非対称ルーティングがあり、トラフィックが 2 つの ASA の間で切り替わる場合は、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ディセーブルにします。この機能は、TCP トラフィックを UDP 接続と同じように処理します。指定されているネットワークに一致する非 SYN パケットが ASA に到着し、高速パスのエントリがない場合は、パケットはセッション管理パスを通過して、高速パス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。

接続設定のライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ガイドラインと制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド モードとトランスペアレント モードでサポートされます。

フェールオーバーのガイドライン

フェールオーバーはサポートされます。

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ときは、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：アプリケーション インスペクションではインバウンド トラフィックとアウトバウンド トラフィックの両方が同じ ASA を通過する必要があるので、アプリケーション インスペクションは TCP ステート バイパスではサポートされません。
- AAA 認証済みセッション：ユーザが 1 つの ASA で認証するとき、他の ASA を介して返されるトラフィックは、ユーザがその ASA で認証を受けていないので拒否されます。
- TCP 代行受信、最大初期接続制限、TCP シーケンス番号のランダム化：ASA は接続のステートを追跡しないので、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になります。
- SSM および SSC 機能：TCP ステート バイパスおよび IPS や CSC などの SSM または SSC 上で実行するアプリケーションは使用できません。

TCP ステート バイパスの NAT のガイドライン

変換セッションは ASA ごとに個別に確立されるので、TCP ステート バイパス トラフィック用に両方の ASA でスタティック NAT を設定してください。ダイナミック NAT を使用すると、ASA 1 でのセッションに選択されるアドレスが、ASA 2 でのセッションに選択されるアドレスと異なります。

最大同時接続および初期接続のガイドライン

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。

デフォルト設定

TCP ステート バイパス

TCP ステート バイパスは、デフォルトでディセーブルになっています。

接続の設定

この項は、次の内容で構成されています。

接続設定の構成のタスク フロー

ステップ 1　TCP 正規化カスタマイゼーションについては、「TCP マップを使用した TCP ノーマライザのカスタマイズ」（P.21-6）に従って TCP マップを作成します。

ステップ 2　グローバル タイムアウトを除くすべての接続設定については、第 1 章「サービス ポリシーの設定」に従ってサービス ポリシーを設定します。

ステップ 3　「接続の設定」（P.21-8）に従って接続を設定します。

ステップ 4　「グローバル タイムアウトの設定」（P.21-9）に従ってグローバル タイムアウトを設定します。

TCP マップを使用した TCP ノーマライザのカスタマイズ

TCP ノーマライザをカスタマイズするには、まず、TCP マップを使用する設定を定義します。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Objects] > [TCP Maps] ペインを選択し、[Add] をクリックします。

[Add TCP Map] ダイアログボックスが表示されます。

ステップ 2　[TCP Map Name] フィールドで、名前を入力します。

ステップ 3　[Queue Limit] フィールドで、異常なパケットの最大数を 0 ～ 250 パケットの範囲で指定します。

[Queue Limit] では、バッファリングして TCP 接続用に配列できる異常パケットの最大数を設定します。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、IPS、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、IPS、および TCP check-retransmission トラフィックの場合、[Queue Limit] 設定が優先されるため、TCP パケットからのアドバタイズされた設定はすべて無視されます。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] 領域で、[Clear and allow]、[Allow only]、または [Drop] をクリックします。

[Allow only] を指定すると、TCP ヘッダーに予約ビットのあるパケットだけが許可されます。

[Clear and allow] を指定すると、TCP ヘッダーの予約ビットをクリアしてパケットを許可します。

[Drop] を指定すると、TCP ヘッダーに予約ビットのあるパケットをドロップします。

ステップ 6　次のいずれかのオプションをオンにします。

- [Clear urgent flag]：ASA を通過する 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。この条件が検出された場合に、接続をドロップできます。
- [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]：再送信データ チェックをイネーブルにします。
- [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。このオプションを選択しない場合、[Queue Limit] を 0（ディセーブル）に設定する必要があります。
- [Drop SYN Packets with data]：データのある SYN パケットをドロップします。
- [Enable TTL Evasion Protection]：ASA の TTL 回避保護をイネーブルにします。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、このオプションをイネーブルにしないでください。
- 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、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]：チェックサム検証をイネーブルにします。
- [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 を持つ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　TCP オプションを設定するには、次のいずれかのオプションをオンにします。

- [Clear Selective Ack]：[selective-ack TCP] オプションを許可するかクリアするかを設定します。
- [Clear TCP Timestamp]：TCP タイムスタンプ オプションを許可するかクリアするかを設定します。
- [Clear Window Scale]：ウィンドウ スケール タイムスタンプ オプションを許可するかクリアするかを設定します。
- [Range]：有効な TCP オプションの範囲を設定します。正しい範囲は 6 ～ 7 と 9 ～ 255 です。下限境界値は上限境界値以下でなければなりません。範囲ごとに [Allow] または [Drop] を選択します。

ステップ 8　[OK] をクリックします。

接続の設定

接続を設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] ペインで、第 1 章「サービス ポリシーの設定」に従ってサービス ポリシーを設定します。

新しいサービス ポリシー ルールの一部として接続制限を設定できます。または、既存のサービス ポリシーを編集することもできます。

ステップ 2　[Rule Actions] ダイアログボックスで、[Connection Settings] タブをクリックします。

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。

- [TCP & UDP Connections]：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 TCP および UDP 接続の最大数を 2000000 までの範囲で指定します。どちらのプロトコルともデフォルトは 0 で、接続可能な最大許容数に設定されています。
- [Embryonic Connections]：ホストごとの初期接続の最大数を 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。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信は、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ことによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。
- [Per Client Connections]：最大 2000000 クライアントごとに、同時 TCP および UDP 接続の最大数を指定します。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。
- [Per Client Embryonic Connections]：最大 2000000 クライアントごとに同時 TCP 初期接続の最大数を指定します。クライアントあたり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、その要求の処理を TCP 代行受信機能に代行させ、接続を阻止します。

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。

- [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を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 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ように指定します。
- [Embryonic Connection Timeout]：初期接続（ハーフ オープン）接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 を入力します。デフォルトは 30 秒です。
- [Half Closed Connection Timeout]：ハーフ クローズ接続が閉じられるまで、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）と 1193:0:0 の間でアイドル タイムアウト期間を設定します。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、ASA 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。

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。

別のインライン ファイアウォールで TCP イニシャル シーケンス番号のランダム化をイネーブルにしている場合は、そのランダム化をディセーブルにできます。2 つのファイアウォールで同じ動作を実行する必要はないからです。ただし、両方のファイアウォールで ISN ランダム化をイネーブルにしたままにしてもトラフィックには影響しません。

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 アプライアンスでは、発信方向に通過する TCP SYN の ISN をランダム化します。同一セキュリティ レベルの 2 つのインターフェイス間の接続の場合、ISN は双方向の SYN でランダム化されます。

保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

ステップ 6　TCP 正規化を設定するには、[Use TCP Map] をオンにします。ドロップダウン リストから既存の 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。

[Add TCP Map] ダイアログボックスが表示されます。「TCP マップを使用した TCP ノーマライザのカスタマイズ」（P.21-6）を参照してください。

ステップ 7　[OK] をクリックします。

ステップ 8　存続可能時間を設定するには、[Decrement time to live for a connection] をオンにします。

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

ステップ 10　[OK] または [Finish] をクリックします。

グローバル タイムアウトの設定

[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインでは、ASA 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の間スロットが使用されなかった場合、リソースは空いているプールに戻されます。TCP 接続スロットは、通常の接続クローズ シーケンスの約 60 秒後に解放されます。

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 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。
- [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 状態がクローズす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（1:0:0）です。値を 0:0:0 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（0:0:1）にすることを推奨します。
- [MGCP]：MGCP メディア ポートがクローズす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（0:5:0）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（0:5:0）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。
- [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 タイムアウトを 0:0:10 ～ 1193:0:0 の範囲で設定します。デフォルトは、1 分（0:1:0）です。
- [Floating Connection]：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、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）。この機能を活用するには、0:1:0 ～ 1193:0:0 の間の新しい値にタイムアウトを変更します。
- [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。
- [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 Provisional Media]：SIP 暫定メディア接続のタイムアウト値を 0:1:0 ～ 1193:0:0 の間で変更します。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 0:3:0 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 0:2:0 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、変換スロット値よりも短い必要があります。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。

（注）　[Authentication Absolute] = 0 の場合、HTTPS 認証は動作しない場合があります。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起動されます。このため、ユーザには、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、変換スロット値よりも短い必要があります。
- [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。こ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。
- （8.4(3) 以降。8.5(1) および 8.6(1) は含まない）[PAT Translation Slot] : 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 の間）を変更します。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アップストリーム 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。

接続設定の機能履歴

表 21-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 21-1　接続設定の機能履歴

機能名	プラットフォーム リリース	機能情報
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]。
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。*

表 21-1　接続設定の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
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 タイムアウトの最小値を 30 秒に短縮	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]