ASA 5500 シリーズでの TCP 状態バイパス機能の設定

目次

概要

この資料に発信および着信 トラフィックが別途の Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス (ASA) をフローするようにする TCP 状態 バイパス 機能を設定する方法を記述されています。

前提条件

要件

この資料に説明がある設定を続行できる前にインストールされる Cisco ASA は少なくとも基礎ライセンスがなければなりません。

使用するコンポーネント

ソフトウェア バージョン 9.x を実行するこの文書に記載されている情報は Cisco ASA 5500 シリーズに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

このセクションは TCP 状態 バイパス 機能および関連サポート情報の外観を提供します。

TCP 状態 バイパス 機能概要

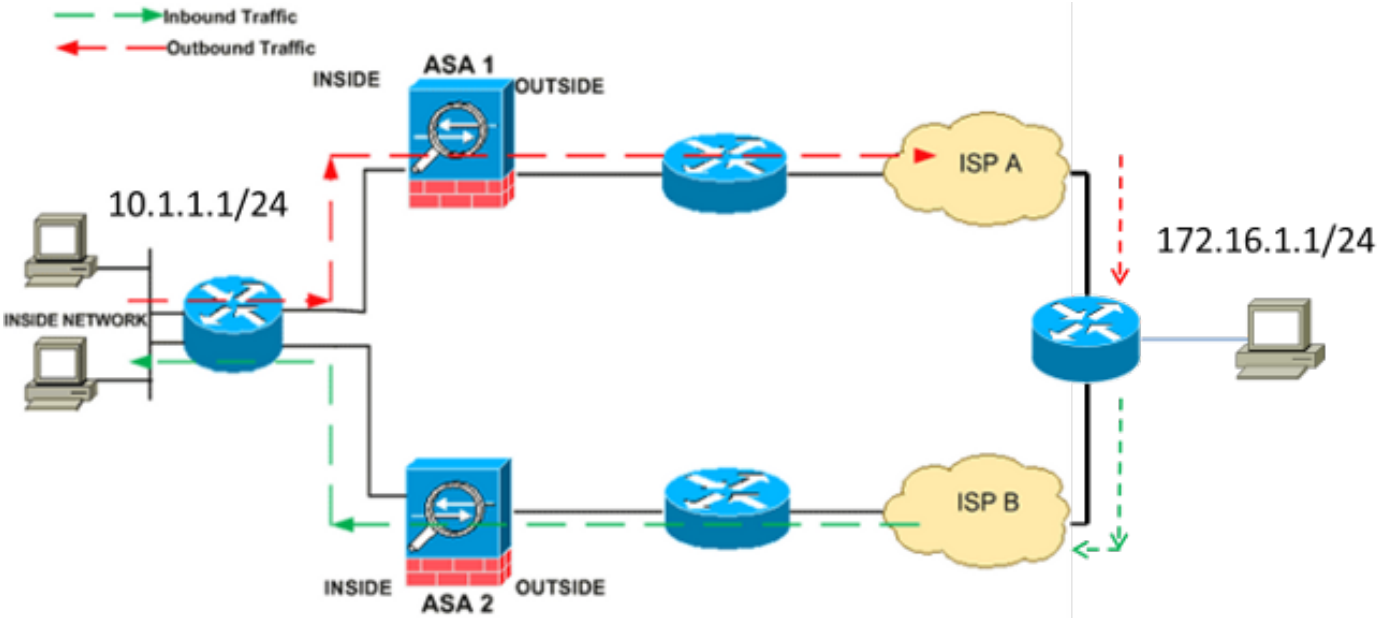
デフォルトで、ASA を通るトラフィックすべてはアダプティブ セキュリティ アルゴリズムによって割り当てられるか、または廃棄されますセキュリティポリシーに基づいて検査され。 ファイアウォール パフォーマンスを最大化するために、ASA はそれが新しい接続または確立された接続であるかどうか各パケットの状態を（たとえば、確認します）チェックしましたりおよびどちらかにそれにセッション管理 パス（新しい接続は（SYN）パケットを同期します）、高速経路（確立された接続）、またはコントロール プレーン パス（高度インスペクション）を割り当てます。

高速経路の現在の接続を一致する TCP パケットはセキュリティポリシーの各側面の再確認なしでパススルー ASA できます。 この機能によってパフォーマンスが最大化されます。 ただし、方式は高速経路で行われるチェック（（設定するために Syn パケットを使用する高速経路使用する）でセッションを TCP シーケンス番号のような）非対称的なルーティングソリューションを妨害でき、; 接続の送信および受信フローはパススルー同じ ASA なります。

たとえば、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。 この接続の後続パケットが *ASA 1* を通過する場合、パケットは高速経路のエントリを一致する、渡されます。 後に続くパケットが *ASA 2* に送信される場合、そこにセッション管理パスを通った SYN パケットがなかったとすると、その接続用に高速パスのエントリが存在しないので、パケットは廃棄されます。

アップストリーム ルータで、および 2 ASA 間のトラフィック交替が設定される非対称 ルーティングあれば、特定のトラフィックのための TCP 状態 バイパス 機能を設定できます。 TCP 状態 バイパス 機能はセッションが高速経路で設定される変更し、高速経路チェックをディセーブルにしますこと方法を。 この機能は、UDP 接続を取り扱うのと同様に TCP トラフィックを取り扱います。 非 SYN パケットが特定のネットワークと一致する ASA を入力し、そこに高速経路 エントリであるとき、高速経路で接続を確立するためにパケットはセッション管理 パスを通過します。 高速パス内に入ると、トラフィックは高速パス チェックをバイパスします。

次の図は、非対称ルーティングの例であり、ここでは、発信トラフィックが着信トラフィックとは異なる ASA を通過しています。



注: TCP 状態 バイパス 機能は Cisco ASA 5500 シリーズでデフォルトでディセーブルにされます。 きちんと設定されない場合さらに、TCP 状態 バイパス 設定により高頻度の接続を引き起こす場合があります。

サポート情報

このセクションは TCP 状態 バイパス 機能のためのサポート情報を記述します。

- **コンテキスト モード** âÂ Â は単一および複数のコンテキスト モードで TCP 状態 バイパス 機能サポートされます。
- **ファイアウォール モード** âÂ Â はルーティングされるで TCP 状態 バイパス 機能 透過モード サポートされ。
- **フェールオーバー** âÂ Â TCP 状態 バイパス 機能サポート フェールオーバー。

これらの機能は TCP 状態 バイパス 機能を使用するとき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** âÂ Â アプリケーション インスペクションは着信 および 発信 トラフィックが同じ ASA を通して渡す、従ってアプリケーション インスペクションは TCP 状態 バイパス 機能でサポートされません両方ことを必要とします。
- ユーザがその ASA と認証を受けなかったので他の ASA による戻りが否定されることユーザが 1 ASA と認証を受ける場合の**認証、許可、アカウンティング (AAA) 認証 された セッション** âÂ Â 、トラフィック。
- **TCP 代行受信は、最大初期接続制限、TCP シーケンス番号ランダム化** âÂ Â ASA 接続の状態のトラック、従ってこれらの機能は適用しません。
- **TCP 正規化** âÂ Â は TCP ノーマライザ無効です。
- **セキュリティ サービス モジュール (SSM) およびセキュリティ サービス カード (SSC) 機**

能性 âÂ Â IPS またはコンテンツ セキュリティ（CSC）のような SSM か SSC で、動作するあらゆるアプリケーションと TCP 状態 バイパス 機能を使用できません。

注: 変換セッションが各 ASA のために別々に設定されるので、TCP 状態 バイパス トラフィックのための ASA の両方の静的なネットワークアドレス変換（NAT）を設定するようにして下さい。 *ASA 1* のセッションのために選択されるダイナミック NAT を使用する場合、アドレスはアドレスと異なります *ASA 2.*のセッションのために選択される。

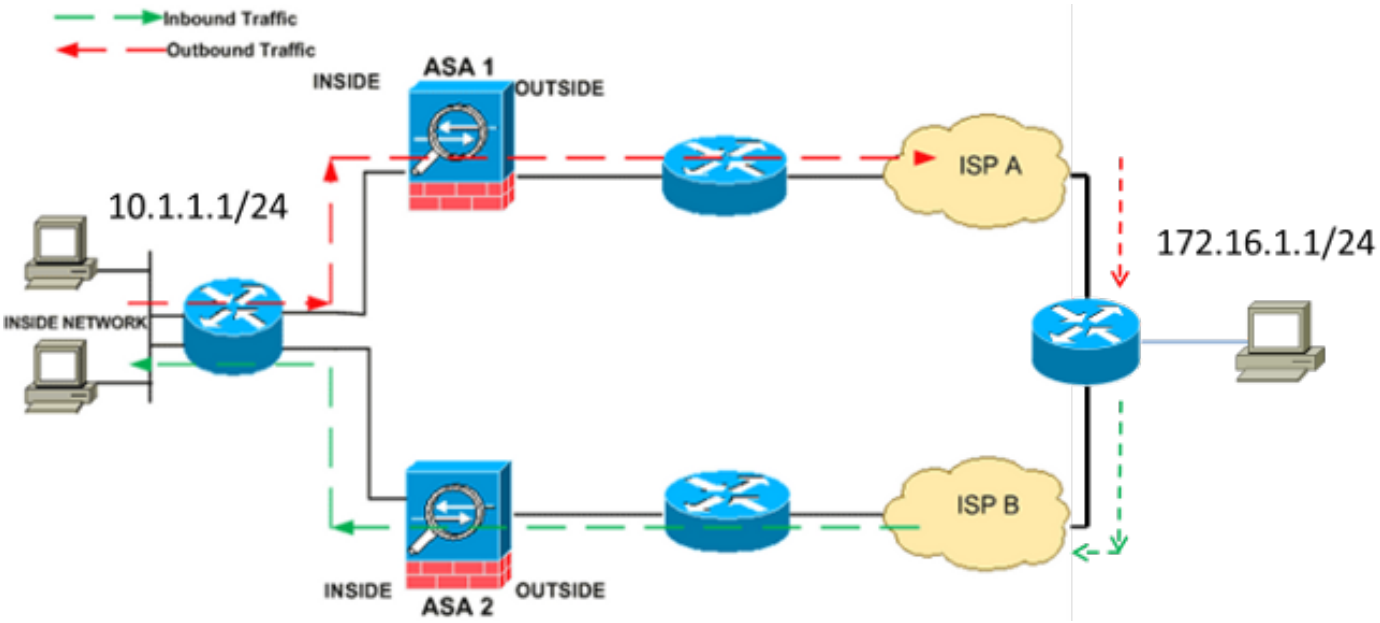
設定

このセクションは 2 つの異なるシナリオの ASA 5500 シリーズの TCP 状態 バイパス 機能を設定する方法を記述します。

注: このセクションで使用するコマンドに関する詳細を得るために Command Lookup Tool を（登録ユーザ専用）使用して下さい。

シナリオ 1

これは最初のシナリオのために使用するトポロジーです:



注: ASA の両方へのこのセクションに説明がある設定を適用して下さい。

TCP 状態 バイパス 機能を設定するためにこれらのステップを完了して下さい:

1. クラスマップを作成するために class-map class_map_name コマンドを入力して下さい。クラスマップはステートフル ファイアウォール インスペクションをディセーブルにしたいと思うトラフィックを識別するために使用されます。**注:** この例で使用するクラスマップは **tcp_bypass** です。`ASA(config)#class-map tcp_bypass`
2. クラスマップ内の対象のトラフィックを規定 するために一致パラメータ コマンドを入力して下さい。 モジュラ 政策の枠組を使用するとき、クラスマップコンフィギュレーション モ

ードで **access-list コマンドを**アクションを適用したいと思うトラフィックの識別のためにアクセス リストを使用するために**一致するのに**使用して下さい。 次にこの設定の例を示します。

```
ASA(config)#class-map tcp_bypass
ASA(config-cmap)#match access-list tcp_bypass
```

注: tcp_bypass はこの例で使用する access-list の名前です。 *CLI を使用して Cisco ASA 5500 シリーズ コンフィギュレーション ガイド*の識別トラフィック（レイヤ 3/4 クラスマップ）セクションを、興味のトラフィックを規定 する方法に関する詳細については *8.2* 参照して下さい。

3. ポリシーマップを追加するか、または（policy-map name コマンドを編集するために既にあっている）ポリシーマップ入力して下さい特定のクラス マップ トラフィックに関して奪取されるべきアクションを割り当てる。 モジュラ 政策の枠組を使用するとき、レイヤ 3/4 クラスマップと識別したトラフィックにアクションを割り当てるために*グローバル コンフィギュレーション モード*で **policy-map コマンドを**（*Type キーワード*なしで）使用して下さい（**class-map** か **class-map タイプ管理コマンド**）。 次の例では、ポリシー マップは *tcp_bypass_policy* です。
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```
4. クラスマップ トラフィックにアクションを割り当てることができるようにポリシーマップ（*tcp_bypass_policy*）に作成されたクラスマップ（*tcp_bypass*）を割り当てるために*ポリシーマップコンフィギュレーション* モードで class コマンドを入力して下さい。 この例では、クラスマップは **tcp_bypass** です:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```
5. TCP 状態 バイパス 機能を有効に するために*クラスコンフィギュレーションモード*で一定接続詳細オプション TCP 状態バイパス コマンドを入力して下さい。 このコマンドはバージョン 8.2(1) から導入されました。 *クラスコンフィギュレーションモード*はこの例に示すように*ポリシーマップコンフィギュレーション* モードからアクセス可能、です:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
   ```
6. サービス ポリシー policymap_name を入力して下さい[グローバル な | インターフェイスすべてまたはターゲット インターフェイスのポリシーマップをグローバルにアクティブにするために*グローバル コンフィギュレーション モード*の *intf*]コマンドをインターフェイスさせて下さい。 サービス ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。 一組のインターフェイスのポリシーを有効に するために **service-policy コマンドを**入力して下さい。 **Global キーワードは**インターフェイスすべてにポリシーマップを加え、**インターフェイス** キーワードは 1 つのインターフェイスだけにポリシーマップを加えます。 許可されるグローバル ポリシーは 1 つだけです。 インターフェイスでグローバル ポリシーを上書きするには、サービス ポリシーをインターフェイスに適用します。 各インターフェイスに適用できるポリシー マップは 1 つだけです。 次に例を示します。
   ```
   ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
   ```

ASA1 の TCP 状態 バイパス 機能のための設定例はここにあります:

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA1(config)#access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.
```

```
ASA1(config)#class-map tcp_bypass
ASA1(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA1(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.

ASA1(config-cmap)#policy-map tcp_bypass_policy
ASA1(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA1(config-pmap-c)#set connection advanced-options tcp-state-bypass

!--- Use the service-policy policymap_name [ global | interface intf ]
!--- command in global configuration mode in order to activate a policy map
!--- globally on all interfaces or on a targeted interface.

ASA1(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA1(config)#object network obj-10.1.1.0
ASA1(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

ASA2 の TCP 状態 バイパス 機能のための設定例はここにあります:

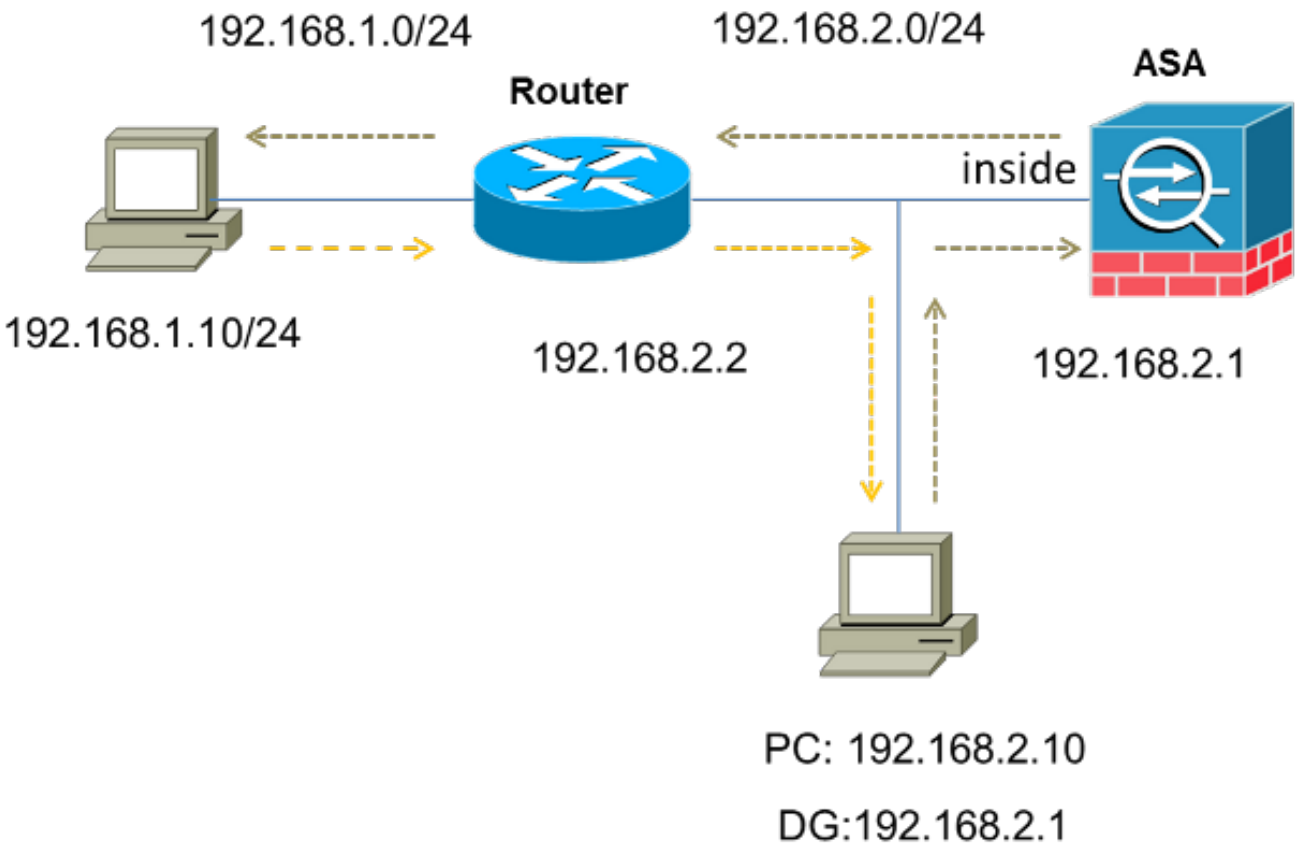
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA2(config)#access-list tcp_bypass extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA2(config)#class-map tcp_bypass
ASA2(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA2(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.

ASA2(config-cmap)#policy-map tcp_bypass_policy
ASA2(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA2(config-pmap-c)#set connection advanced-options tcp-state-bypass

!--- Use the service-policy policymap_name [ global | interface intf ]
!--- command in global configuration mode in order to activate a policy map
!--- globally on all interfaces or on a targeted interface.

ASA2(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA2(config)#object network obj-10.1.1.0
```

```
ASA2(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

シナリオ2

このセクションはトラフィックが同じインターフェイス (u *回転*) からの ASA を入力し、出て行く、非対称 ルーティングを使用するシナリオのための ASA の TCP 状態 バイパス 機能を設定する方法を記述します。

このシナリオで使用するトポロジーはここにあります:



TCP 状態 バイパス 機能を設定するためにこれらのステップを完了して下さい:

1. TCP インスペクションをバイパスする必要があるトラフィックを一致するために *access-list* を作成して下さい:
   ```
   ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
   192.168.1.0 255.255.255.0
   ```
2. クラスマップを作成するために class-map class_map_name コマンドを入力して下さい。クラスマップはステートフル ファイアウォール インスペクションをディセーブルにしたいと思うトラフィックを識別するために使用されます。**注:** この例で使用するクラスマップは **tcp_bypass** です。`ASA(config)#class-map tcp_bypass`
3. クラスマップの対象のトラフィックを規定 するために一致パラメータ コマンドを入力して下さい。 モジュラ 政策の枠組を使用するとき、クラスマップコンフィギュレーション モードで **access-list コマンドを**アクションを適用したいと思うトラフィックの識別のためにアクセス リストを使用するために**一致するのに**使用して下さい。 次にこの設定の例を示します。
   ```
   ASA(config)#class-map tcp_bypass
   ```

```
ASA(config-cmap)#match access-list tcp_bypass
```
注: tcp_bypass はこの例で使用する access-list の名前です。 *Cisco ASA 5500 シリーズ コンフィギュレーション ガイド*の[トラフィック（レイヤ 3/4 クラスマップ）セクションを *CLI を使用して*識別することを]、興味のトラフィックを規定 する方法に関する詳細については *8.2* 参照して下さい。

4. ポリシーマップを追加するために **policy-map name コマンドを**入力すれば（既にあっている）そのポリシーマップ編集することは特定のクラス マップ トラフィックに関して奪取 されるべきアクションを設定 します。 モジュラ 政策の枠組を使用するとき、レイヤ 3/4 クラスマップと識別したトラフィックにアクションを割り当てるために*グローバル コンフィギュレーション モード*で **policy-map コマンドを**（*Type キーワード*なしで）使用して下さい（**class-map** か **class-map タイプ管理コマンド**）。 次の例では、ポリシー マップは *tcp_bypass_policy* です。
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```
5. クラスマップ トラフィックにアクションを割り当てることができるようにポリシーマップ（*tcp_bypass_policy*）に作成されたクラスマップ（*tcp_bypass*）を割り当てるために*ポリシーマップコンフィギュレーション* モードで **class コマンドを**入力して下さい。 この例では、クラスマップは **tcp_bypass** です:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```
6. TCP 状態 バイパス 機能を有効に するために*クラスコンフィギュレーションモード*で**一定接続詳細オプション TCP 状態バイパス** コマンドを入力して下さい。 このコマンドはバージョン 8.2(1) から導入されました。 *クラスコンフィギュレーションモード*はこの例に示すように*ポリシーマップコンフィギュレーション* モードからアクセス可能、です:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
   ```
7. **サービス ポリシー policymap_name を**入力して下さい[**グローバル な |** インターフェイスすべてまたはターゲット インターフェイスのポリシーマップをグローバルにアクティブにするために*グローバル コンフィギュレーション モード*の ***intf***]コマンドを**インターフェイスさせて下さい**。 サービス ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。 一組のインターフェイスのポリシーを有効に するために **service-policy コマンドを**入力して下さい。 **Global キーワードは**インターフェイスすべてにポリシーマップを加え、**インターフェイス** キーワードは 1 つのインターフェイスだけにポリシーを適用します。 許可されるグローバル ポリシーは 1 つだけです。 インターフェイスでグローバル ポリシーを上書きするには、サービス ポリシーをインターフェイスに適用します。 各インターフェイスに適用できるポリシー マップは 1 つだけです。 次に例を示します。
   ```
   ASA(config-pmap-c)#service-policy tcp_bypass_policy inside
   ```
8. 割り当て ASA のトラフィックの同じセキュリティレベル:
   ```
   ASA(config)#same-security-traffic permit intra-interface
   ```

ASA の TCP 状態 バイパス 機能のための設定例はここにあります:

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to bypass inspection to improve the performance.

ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
192.168.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA(config)#class-map tcp_bypass
ASA(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA(config-cmap)#match access-list tcp_bypass
```

```
!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.

ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass

!--- Use the service-policy policymap_name [ global | interface intf ]
!--- command in global configuration mode in order to activate a policy map
!--- globally on all interfaces or on a targeted interface.

ASA(config-pmap-c)#service-policy tcp_bypass_policy inside

!--- Permit same security level traffic on the ASA to support U-turning

ASA(config)#same-security-traffic permit intra-interface
```

確認

アクティブ TCP の数をおよびさまざまな型の接続についての UDP 接続および情報表示するために show conn コマンドを入力して下さい。 指定接続タイプのための接続状態を表示するために、*特権EXECモード*で show conn コマンドを入力して下さい。

> **注:** このコマンドは IPv4 と IPv6 のアドレスをサポートします。 TCP 状態 バイパス 機能を使用する接続のために表示する出力はフラグ **b.が**含まれています。

次に出力例を示します。

```
ASA(config)show conn
1 in use, 3 most used
TCP tcp 10.1.1.1:49525 tcp 172.16.1.1:21, idle 0:01:10, bytes 230, flags b
```

トラブルシューティング

この機能のための特定のトラブルシューティング情報がありません。 一般の接続 トラブルシューティング情報に関してはこれらの文書を参照して下さい:

- **CLI および ASDM を使用したパケットのキャプチャの設定例**
- ASA 8.2： Cisco ASA ファイアウォールを介するパケット フロー

  注: フェールオーバー ペアのスタンバイユニットへの TCP 状態 バイパス接続は複製されません。

エラー メッセージ

ASA は TCP 状態 バイパス 機能が有効に なった後でさえもこのエラーメッセージを表示する:

%PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface interface_name to dest_address:no matching session
インターネット制御メッセージ プロトコル （ICMP）パケットはステートフル ICMP 機能によって追加される保安検査が理由で ASA によって廃棄されます。 これらは通常既に ASA を渡って渡される有効な*エコー要求*なしに現在 ASA で設定されるあらゆる TCP、UDP、または ICMP セッションと関連していない ICMPエコー応答または ICMPエラーメッセージです。

ASA はこの機能性の無力が（すなわち、接続テーブルの型 3 を ICMP *戻り*エントリのチェックします）可能性のあるではないので TCP 状態 バイパス 機能が有効に なってもこのログを表示する。 ただし、TCP 状態 バイパス 機能は正しく動作します。

これらのメッセージの外観を防ぐためにこのコマンドを入力して下さい:

```
hostname(config)#no logging message 313004
```

関連情報

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems