ASA 5500 シリーズでの TCP 状態バイパス機能の設定

内容

概要

このドキュメントでは、TCP 状態バイパス機能を設定する方法について説明します。この機能を使用すると、発信トラフィックと着信トラフィックが個別の Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス (ASA) を通過するようになります。

前提条件

要件

このドキュメントで説明されている設定を続行するには、Cisco ASAに少なくとも基本ライセンスがインストールされている必要があります。

使用するコンポーネント

このドキュメントの情報は、ソフトウェアバージョン9.xが稼働するCisco ASA 5500シリーズに基づくものです。

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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については、『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

このセクションでは、TCP状態バイパス機能の概要と関連するサポート情報について説明します。

TCP状態バイパス機能の概要

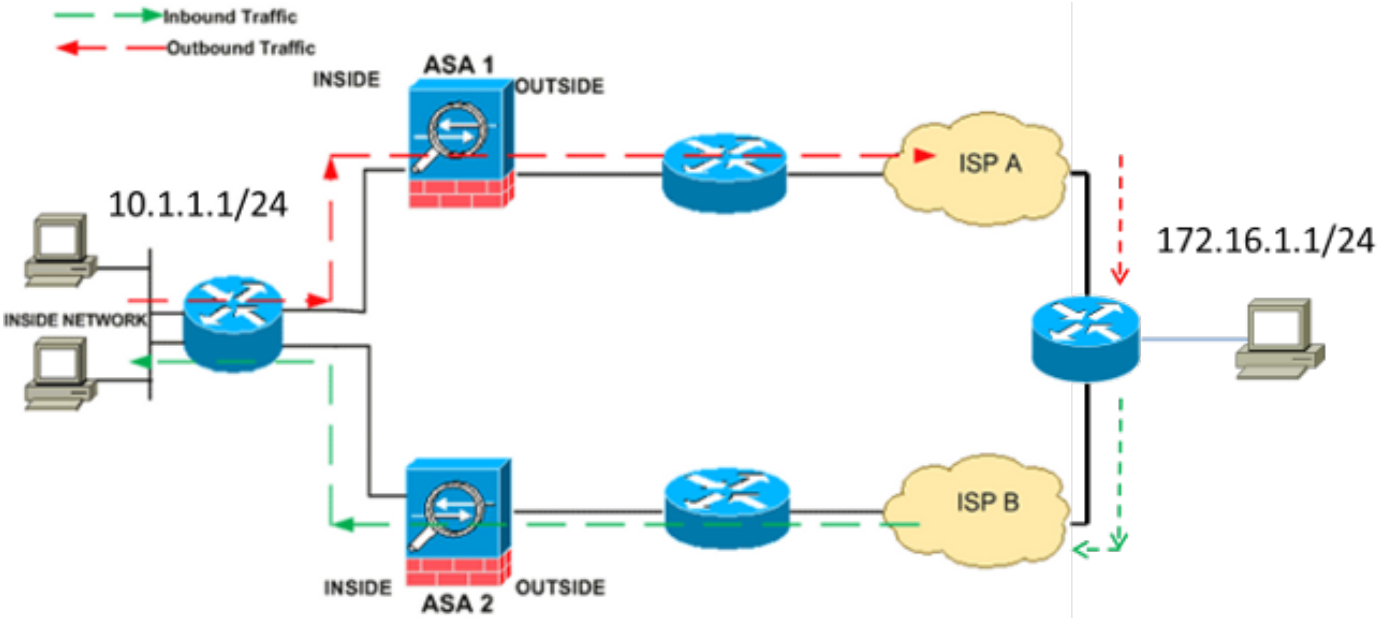
デフォルトでは、ASAを通過するすべてのトラフィックは適応型セキュリティアルゴリズム(ASA)によって検査され、セキュリティポリシーに基づいて通過または廃棄されます。ファイアウォールのパフォーマンスを最大化するため、ASAは各パケットの状態をチェックし(たとえば、新しい接続か確立された接続かをチェックし、セッション管理パス(新しい接続の同期(SYN)パケット)、高速パス（確立された接続）、コントロールプレーンパス（高度な検査）に検査)。

高速パスの現在の接続に一致するTCPパケットは、セキュリティポリシーのすべての側面を再確認することなく、ASAを通過できます。この機能によってパフォーマンスが最大化されます。ただし、高速パス（SYNパケットを使用する）でセッションを確立するために使用される方法と、高速パス（TCPシーケンス番号など）で発生するチェックは、非対称ルーティングソリューションの妨げになります。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ります。

たとえば、新しい接続が*ASA 1*に送信されます。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、そのパケットは高速パスのエントリと一致し、通過します。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非対称ルーティングが設定されており、トラフィックが2つのASA間で交互に送信される場合は、特定のトラフィックに対して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、高速パスでセッションが確立される方法を変更し、高速パスチェックを無効にします。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。指定されたネットワークに一致する非SYNパケットがASAに入り、高速パスエントリがない場合、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。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：Cisco ASA 5500シリーズでは、TCP状態バイパス機能はデフォルトで無効になっています。また、TCP状態バイパス設定が適切に実装されていない場合は、接続の数が多くなる可能性があります。

サポート情報

この項では、TCP状態バイパス機能のサポート情報について説明します。

- **コンテキストモード**TCP状態バイパス機能は、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**TCP状態バイパス機能は、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ています。

- **Failover** TCP state bypass機能は、フェールオーバーをサポートしています。

TCP状態バイパス機能を使用する場合、次の機能はサポートされません。

- **アプリケーション検査**「アプリケーション検査」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、TCP状態バイパス機能ではアプリケーション検査はサポートされません。

- **認証、許可、アカウンティング(AAA)認証セッション**：ユーザが1つのASAで認証を行うと、もう1つのASAを経由して返されるトラフィックが拒否されます。これは、ユーザがそのASAで認証しなかったためです。

- **TCPインターセプト、最大初期接続制限、TCPシーケンス番号のランダム化**ASAは接続の状態を追跡しないため、これらの機能は適用されません。

- **TCP正規化**TCPノーマライザが無効になっている。

- **Security Services Module(SSM)およびSecurity Services Card(SSC)機能**IPSやContent

Security(CSC)など、SSMまたはSSCで実行されるアプリケーションでは、TCP状態バイパス機能を使用できません。

注：変換セッションはASAごとに個別に確立されるため、両方のASAでTCP状態バイパストラフィック用にスタティックなネットワークアドレス変換(NAT)を設定してください。ダイナミックNATを使用する場合、*ASA 1*のセッションに対して選択されたアドレスは、ASA 2のセッションに対して選択されたアドレスとは異なります。

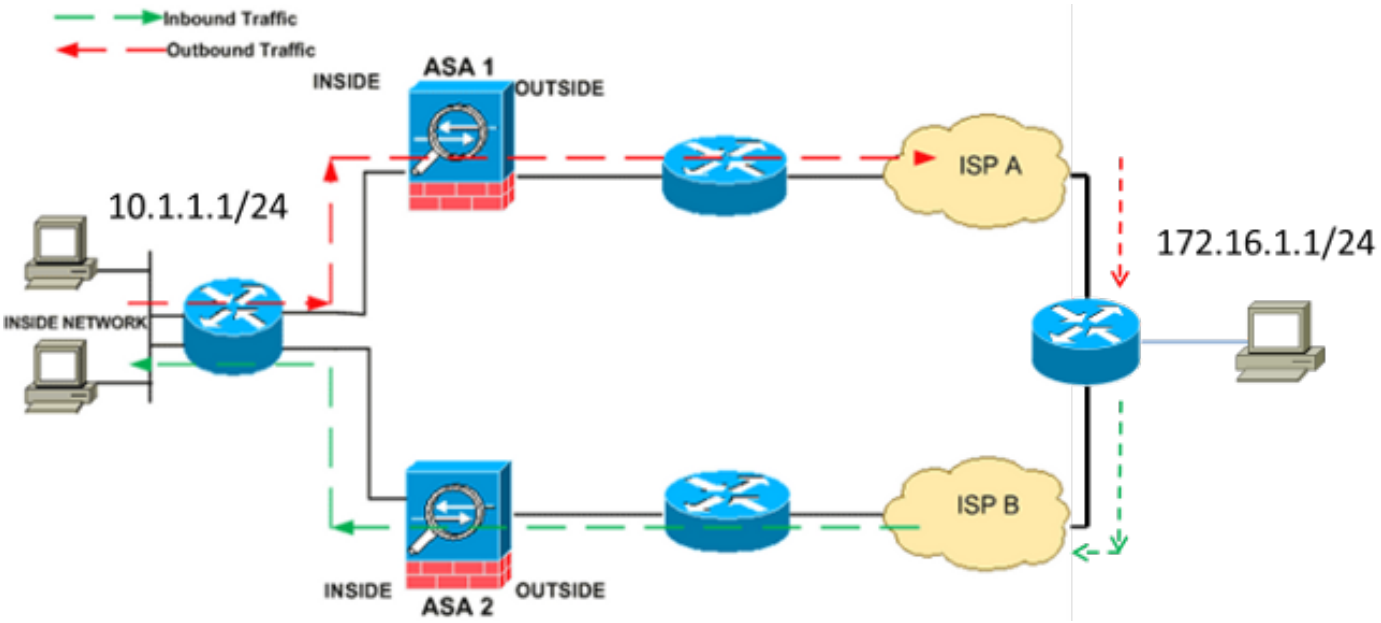
設定

このセクションでは、2つの異なるシナリオでASA 5500シリーズのTCP状態バイパス機能を設定する方法について説明します。

注：ここで使用されているコマンドの詳細については、[コマンド検索ツール（登録ユーザ専用）を使用してください。]

シナリオ 1

最初のシナリオで使用されるトポロジは次のとおりです。



注：このセクションで説明する設定を、両方のASAに適用する必要があります。

TCP状態バイパス機能を設定するには、次の手順を実行します。

1. クラスマップを作成するには、class-map class_map_nameコマンドを入力します。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無効にする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. match parameterコマンドを入力して、クラスマップ内の対象トラフィックを指定します。モジュラポリシーフレームワークを使用する場合、アクションを適用するトラフィックの識

別にアクセスリストを使用するには、クラスマップ設定モードで**match access-listコマンドを使用**します。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、この例で使用されているアクセスリストの名前です。対象のトラフィックを指定する方法の詳細については、『*CLIを使用したCisco ASA 5500シリーズコンフィギュレーションガイド8.2*』の「*トラフィックの識別（レイヤ3/4クラスマップ）*」セクションを参照してください。

3. policy-map nameコマンドを入力して、ポリシーマップを追加するか、指定したクラスマップトラフィックに対して実行するアクションを割り当てるポリシーマップ（すでに存在する）を編集します。Modular Policy Frameworkを使用する場合は、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(*type*キーワードなし)を使用して、レイヤ3/4クラスマップ(**class-map**または**class-map type management**コマンド)で識別したトラフィックにアクションを割り当てます。 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. 作成したクラスマップ(*tcp_bypass*)をポリシーマップ(*tcp_bypass_policy*)に割り当てるため、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、ポリシーマップ設定モードで*class*コマンドを入力します。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には、クラス設定モードでset connection advanced-options tcp-state-bypassコマンドを入力します。このコマンドはバージョン 8.2(1) から導入されました。 次の例に示すように、*policy-map*設定モードからクラス設定モードにアクセスできます。

```
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. service-policy policymap_name [global | interface *intf*]コマンドをグローバルコンフィギュレーションモードで使用し、すべてのインターフェイスまたは対象のインターフェイスでポリシーマップをグローバルにアクティブ化します。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。service-policyコマンド**を入力して、インターフェイス上で一連のポリシーを有効にします。globalキーワードは、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キーワード**は、ポリシーマップを1つのインターフェイスにのみ適用します。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。以下が一例です。

```
ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
```

*ASA*1のTCP状態バイパス機能の設定例を次に示します。

```
!--- 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設定例を次に示します。

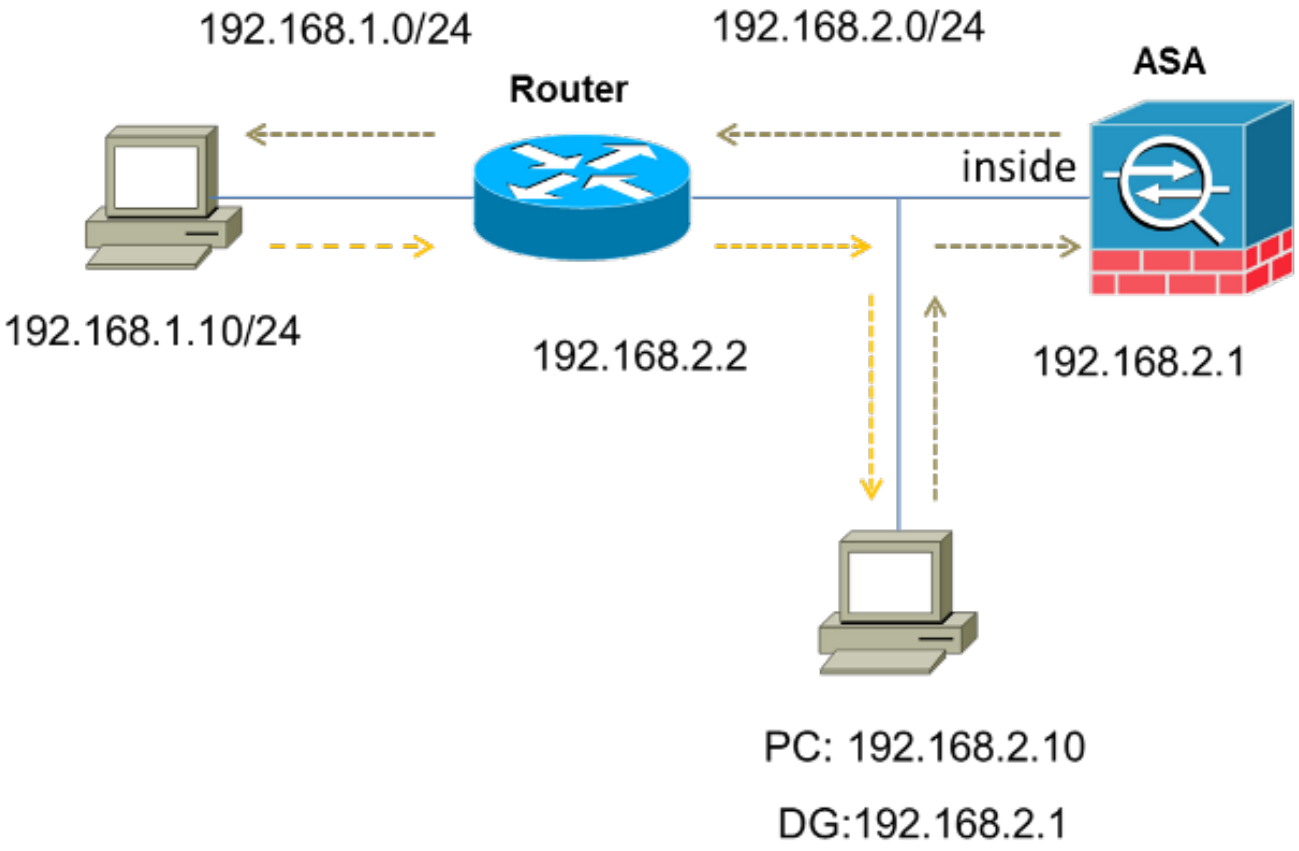
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

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

このセクションでは、非対称ルーティングを使用するシナリオでASAのTCP状態バイパス機能を設定する方法について説明します。このシナリオでは、トラフィックが同じインターフェイスからASAに出入りする(*u*ターン)場合です。

このシナリオで使用されるトポロジを次に示します。



TCP状態バイパス機能を設定するには、次の手順を実行します。

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照合するために、アクセスリストを作成します。

   ```
   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には、class-map class_map_nameコマンドを入力します。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無効にするトラフィックを識

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. match parameterコマンド**を入力**して、クラスマップに関連するトラフィックを指定します。モジュラポリシーフレームワークを使用する場合は、クラスマップ設定モードで**match access-listコマンドを使用**し、アクションを適用するトラフィックの識別にアクセスリストを使用します。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、この例で使用されているアクセスリストの名前です。対象のトラフィックを指定する方法の詳細については、*『CLIを使用したCisco ASA 5500シリーズコンフィギュレーションガイド8.2』の「トラフィックの識別（レイヤ3/4クラスマップ）」*セクションを参照してください。

4. policy-map nameコマンドを入力して、ポリシーマップを追加するか、指定したクラスマップトラフィックに対して実行するアクションを設定するポリシーマップ（すでに存在する）を編集します。Modular Policy Frameworkを使用する場合は、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(*type*キーワードなし)を使用して、レイヤ3/4クラスマップ(**class-mapまたはclass-map type managementコマンド)で識別したトラフィックにアクションを割り当りります。** 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. 作成したクラスマップ(*tcp_bypass*)をポリシーマップ(*tcp_bypass_policy*)に割り当てるため、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、ポリシーマップ設定モードで*class*コマンドを入力します。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**にするには、クラス設定モードで**set connection advanced-options tcp-state-bypassコマンドを入力します。このコマンドはバージョン 8.2(1) から導入されました。 *クラス設定モード*は、次の例に示すように、*ポリシーマップ設定*モードからアクセスできます。

```
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. service-policy policymap_name [global | interface *intf*]**コマンドを使用して**います。このコマンドは、*グローバルコンフィギュレーションモード*で、すべてのインターフェイスまたは対象のインターフェイスでポリシーマップをグローバルにアクティブ化します。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。service-policyコマンド**を入力して、インターフェイス上で一連のポリシーを有効にします。globalキーワードは、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キーワード**は、ポリシーを1つのインターフェイスにのみ適用します。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。以下が一例です。

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

8. ASA上のトラフィックに対して同じセキュリティレベルを許可します。

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

ASAのTCP状態バイパス機能の設定例を次に示します。

```
!--- 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

Enter the show conn コマンドを発行して、アクティブなTCPおよびUDP接続の数と、さまざまなタイプの接続に関する情報を表示します。指定された接続タイプの接続状態を表示するには、show conn 特権EXECモードでコマンドを発行します。

> **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に対して表示される出力には、フラグ**bが含まれます**。

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
```

トラブルシュート

この機能に関する特定のトラブルシューティング情報はありません。一般的な接続のトラブルシューティング情報については、次のドキュメントを参照してください。

- CLI および ASDM を使用した ASA パケット 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：TCP状態バイパス接続は、フェールオーバーペアのスタンバイユニットには複製されません。

エラー メッセージ

TCP状態バイパス機能を有効にしても、ASAは次のエラーメッセージを表示します。

%PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface interface_name to dest_address:no matching session

Internet Control Message Protocol（ICMP；インターネット制御メッセージプロトコル）パケットは、ステートフルICMP機能によって追加されたセキュリティチェックのために、ASAによってドロップされます。通常は、有効なエコー要求がASAに渡されていない*ICMPエコー応答*か、ASAで現在確立されているTCP、UDP、またはICMPセッションに関連しないICMPエラーメッセージのどちらかです。

ASAは、この機能を無効にできない（つまり、接続テーブルのタイプ3のICMPリターンエントリをチェックする）ため、TCP状態バイパス機能が有効になっている場合でも、このログを表示します。ただし、TCP状態バイパス機能は正常に動作します。

これらのメッセージが表示されないようにするには、次のコマンドを入力します。

```
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 (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems