# Configure the TCP State Bypass Feature on the ASA 5500 Series

## Contents



## Introduction

This document describes how to configure the TCP state bypass feature, which allows the outbound and inbound traffic to flow through separate Cisco ASA 5500 Series Adaptive Security Appliances (ASAs).

## Prerequisites

### Requirements

The Cisco ASA must have at least the base license installed before you can proceed with the configuration that is described in this document.

### Components Used

The information in this document is based on the Cisco ASA 5500 Series that runs software Version 9.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## Background Information

This section provides an overview of the TCP state bypass feature and the related support information.

### TCP State Bypass Feature Overview

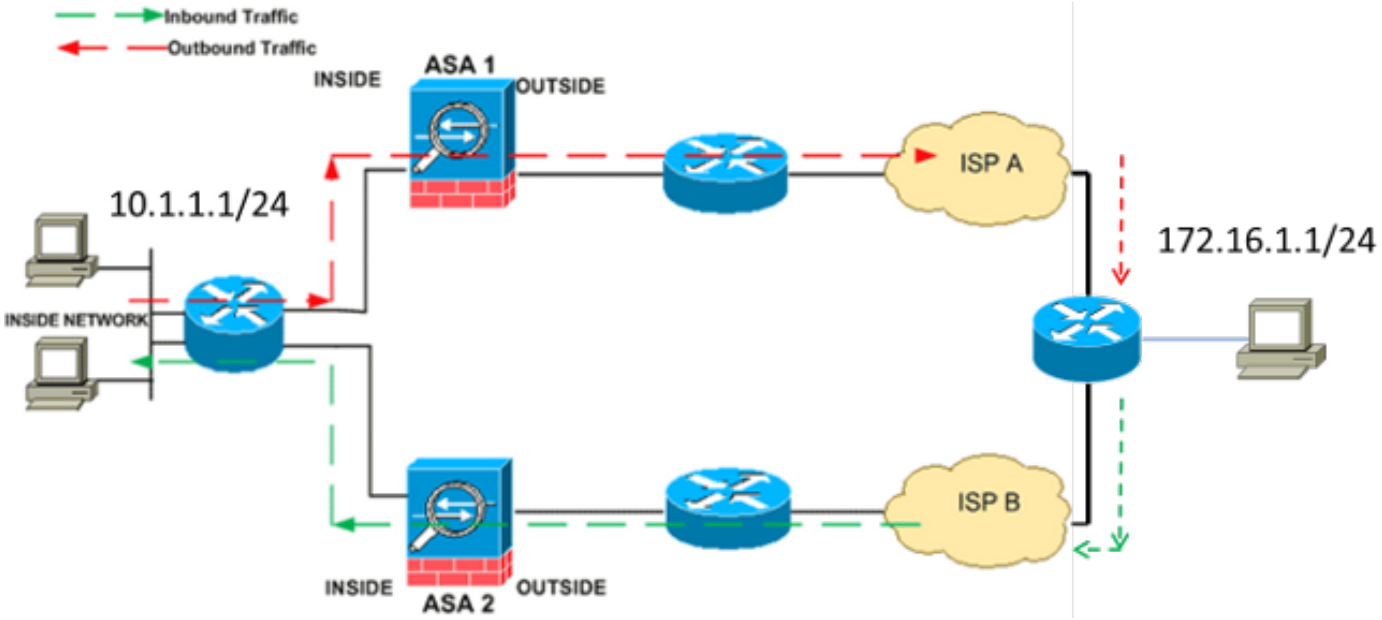
By default, all of the traffic that passes through the ASA is inspected via the Adaptive Security Algorithm and is either allowed through or dropped based on the security policy. In order to maximize the Firewall performance, the ASA checks the state of each packet (for example, it checks whether it is a new connection or an established connection) and assigns it to either the session management path (a new connection Synchronize (SYN) packet), the fast path (an established connection), or the control plane path (advanced inspection).

The TCP packets that match the current connections in the fast path can pass through the ASA without a recheck of every aspect of the security policy. This feature maximizes performance. However, the method that is used in order to establish the session in the fast path (which uses the SYN packet) and the checks that occur in the fast path (such as the TCP sequence number) can stand in the way of asymmetrical routing solutions; both the outbound and inbound flows of a connection must pass through the same ASA.

For example, a new connection goes to *ASA 1*. The SYN packet passes through the session management path, and an entry for the connection is added to the fast path table. If subsequent packets on this connection go through *ASA 1*, the packets match the entry in the fast path and are passed through. If subsequent packets go to *ASA 2*, where there was not a SYN packet that went through the session management path, then there is no entry in the fast path for the connection, and the packets are dropped.

If you have asymmetric routing configured on the upstream routers, and traffic alternates between two ASAs, then you can configure the TCP state bypass feature for specific traffic. The TCP state bypass feature alters the way that sessions are established in the fast path and disables the fast path checks. This feature treats TCP traffic much as it treats a UDP connection: when a non-SYN packet that matches the specified networks enters the ASA, and there is no fast path entry, then the packet goes through the session management path in order to establish the connection in the fast path. Once in the fast path, the traffic bypasses the fast path checks.

This image provides an example of asymmetric routing, where the outbound traffic goes through a different ASA than the inbound traffic:




**Note**: The TCP state bypass feature is disabled by default on the Cisco ASA 5500 Series. Additionally, the TCP state bypass configuration can cause a high number of connections if it is not properly implemented.

## Support Information

This section describes the support information for the TCP state bypass feature.

- **Context Mode** âÂÂ The TCP state bypass feature is supported in single and multiple context modes.
- **Firewall Mode** âÂÂ The TCP state bypass feature is supported in routed and transparent modes.
- **Failover** âÂÂ The TCP state bypass feature supports failover.

These features are not supported when you use the TCP state bypass feature:

- **Application inspection** âÂÂ Application inspection requires that both the inbound and outbound traffic passes through the same ASA, so application inspection is not supported with the TCP state bypass feature.
- **Authentication, Authorization, and Accounting (AAA) authenticated sessions** âÂÂ When a user authenticates with one ASA, the traffic that returns via the other ASA is denied because the user did not authenticate with that ASA.
- **TCP intercept, maximum embryonic connection limit, TCP sequence number randomization** âÂÂ The ASA does not track of the state of the connection, so these features are not applied.
- **TCP normalization** âÂÂ The TCP normalizer is disabled.

- **Security Services Module (SSM) and Security Services Card (SSC) functionality** âÂÂ You cannot use the TCP state bypass feature with any applications that run on an SSM or SSC, such as IPS or Content Security (CSC).

  **Note**: Because the translation session is established separately for each ASA, ensure that you configure static Network Address Translation (NAT) on both of the ASAs for the TCP state bypass traffic. If you use dynamic NAT, the address that is chosen for the session on *ASA 1* will differ from the address that is chosen for the session on *ASA 2*.

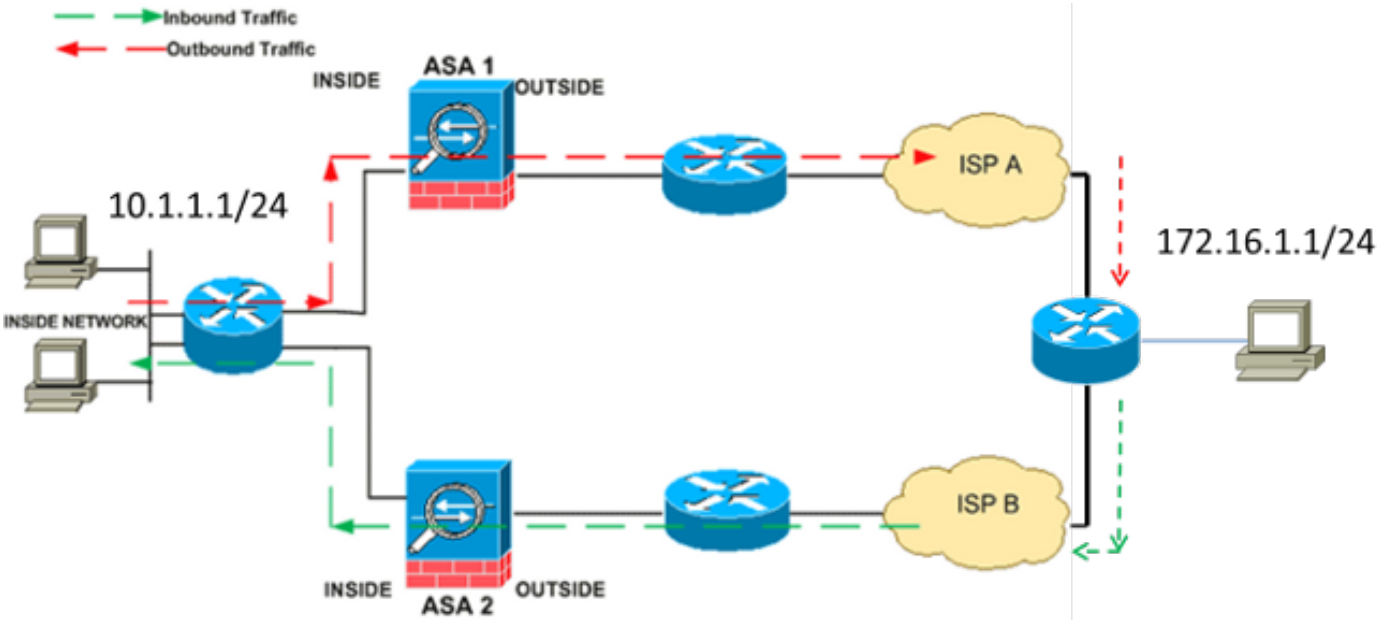
# Configure

This section describes how to configure the TCP state bypass feature on the ASA 5500 Series in two different scenarios.

**Note**: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands that are used in this section.

## Scenario 1

This is the topology that is used for the first scenario:




**Note**: You must apply the configuration that is described in this section to both of the ASAs.

Complete these steps in order to configure the TCP state bypass feature:

1. Enter the **class-map class_map_name** command in order to create a *class map*. The class map is used in order to identify the traffic for which you want to disable stateful Firewall inspection.**Note**: The class map that is used in this example is **tcp_bypass**.`ASA(config)#class-map tcp_bypass`
2. Enter the **match parameter** command in order to specify the traffic of interest within the

class map. When you use the Modular Policy Framework, use the **match access-list** command in *class-map configuration* mode in order to use an access list for identification of the traffic to which you want to apply actions. Here is an example of this configuration:

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

**Note**: The **tcp_bypass** is the name of the access-list that is used in this example. Refer to the Identifying Traffic (Layer 3/4 Class Map) section of the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2* for more information about how to specify the traffic of interest.

3. Enter the **policy-map name** command in order to add a policy map or edit a policy map (that is already present) that assigns the actions to be taken in regards to the specified class map traffic. When you use the Modular Policy Framework, use the **policy-map** command (without the *type* keyword) in *global configuration* mode in order to assign actions to the traffic that you identified with a Layer 3/4 class map (the **class-map** or **class-map type management** command). In this example, the policy map is **tcp_bypass_policy**:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```
4. Enter the **class** command in *policy-map configuration* mode in order to assign the created class map (*tcp_bypass*) to the policy map (*tcp_bypass_policy*) so that you can assign the actions to the class map traffic. In this example, the class map is **tcp_bypass**:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```
5. Enter the **set connection advanced-options tcp-state-bypass** command in *class configuration* mode in order to enable the TCP state bypass feature. This command was introduced in Version 8.2(1). The *class configuration* mode is accessible from the *policy-map configuration* mode, as shown in this example:
   ```
   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. Enter the **service-policy policymap_name [ global | interface *intf* ]** command in *global configuration* mode in order to activate a policy map globally on all of the interfaces or on a targeted interface. In order to disable the service policy, use the **no** form of this command. Enter the **service-policy** command in order to enable a set of policies on an interface. The **global** keyword applies the policy map to all of the interfaces, and the **interface** keyword applies the policy map to only one interface. Only one global policy is allowed. In order to override the global policy on an interface, you can apply a service policy to that interface. You can apply only one policy map to each interface. Here is an example:
   ```
   ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
   ```

Here is an example configuration for the TCP state bypass feature on *ASA1*:

```
!--- 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
```

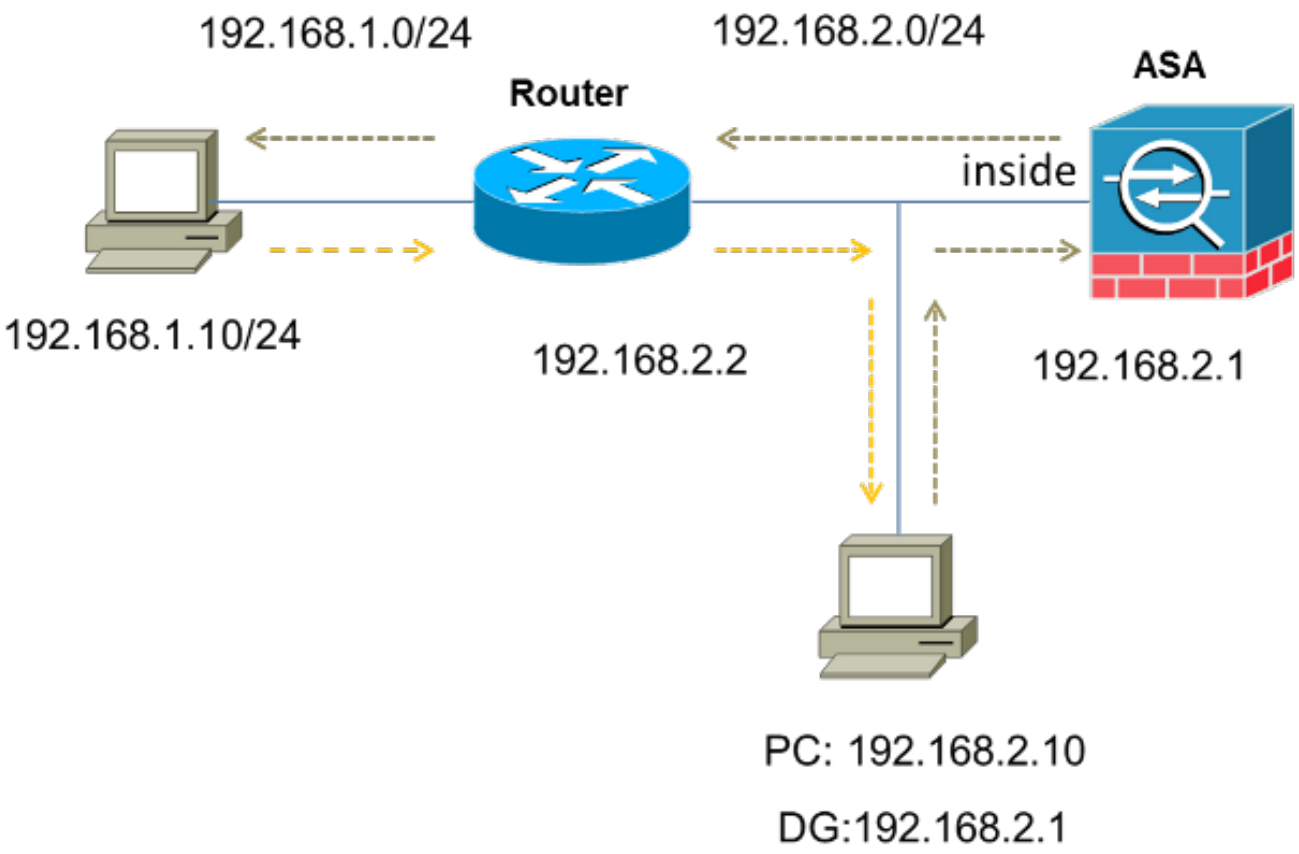
Here is an example configuration for the TCP state bypass feature on *ASA2*:

```
!--- 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
```

## Scenario 2

This section describes how to configure the TCP state bypass feature on the ASA for scenarios that use asymmetric routing, where the traffic enters and leaves the ASA from same interface (*u-turning*).

Here is the topology that is used in this scenario:




Complete these steps in order to configure the TCP state bypass feature:

1. Create an *access-list* in order to match the traffic that should bypass the TCP inspection:
   `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. Enter the **class-map class_map_name** command in order to create a *class map*. The class map is used in order to identify the traffic for which you want to disable stateful Firewall inspection.**Note**: The class map that is used in this example is **tcp_bypass**.`ASA(config)#class-map tcp_bypass`
3. Enter the **match parameter** command in order to specify the traffic of interest in the class map. When you use the Modular Policy Framework, use the **match access-list** command in *class-map configuration* mode in order to use an access list for identification of the traffic to which you want to apply actions. Here is an example of this configuration:
   `ASA(config)#class-map tcp_bypass`
   `ASA(config-cmap)#match access-list tcp_bypass` **Note**: The **tcp_bypass** is the name of the access-list that is used in this example. Refer to Identifying Traffic (Layer 3/4 Class Map) section of the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2* for more information about how to specify the traffic of interest.
4. Enter the **policy-map name** command in order to add a policy map or edit a policy map (that is already present) that sets the actions to be taken in regards to the specified class map traffic. When you use the Modular Policy Framework, use the **policy-map** command (without

the *type* keyword) in *global configuration* mode in order to assign the actions to the traffic that you identified with a Layer 3/4 class map (the **class-map** or **class-map type management** command). In this example, the policy map is **tcp_bypass_policy**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```

5. Enter the **class** command in *policy-map configuration* mode in order to assign the created class map (*tcp_bypass*) to the policy map (*tcp_bypass_policy*) so that you can assign actions to the class map traffic. In this example, the class map is **tcp_bypass**:

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

6. Enter the **set connection advanced-options tcp-state-bypass** command in *class configuration* mode in order to enable the TCP state bypass feature. This command was introduced in Version 8.2(1). The *class configuration* mode is accessible from the *policy-map configuration* mode, as shown in this example:

```
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. Enter the **service-policy policymap_name [ global | interface *intf* ]** command in *global configuration* mode in order to activate a policy map globally on all of the interfaces or on a targeted interface. In order to disable the service policy, use the **no** form of this command. Enter the **service-policy** command in order to enable a set of policies on an interface. The **global** keyword applies the policy map to all of the interfaces, and the **interface** keyword applies the policy to only one interface. Only one global policy is allowed. In order to override the global policy on an interface, you can apply a service policy to that interface. You can apply only one policy map to each interface. Here is an example:

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

8. Permit the same security level for the traffic on the ASA:

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

Here is an example configuration for the TCP state bypass feature on the ASA:

```
!--- 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
```

# Verify

Enter the **show conn** command in order to view the number of active TCP and UDP connections and information about the connections of various types. In order to display the connection state for the designated connection type, enter the **show conn** command in *privileged EXEC* mode.

> **Note**: This command supports IPv4 and IPv6 addresses. The output that is displayed for the connections that use the TCP state bypass feature includes the flag **b**.

Here is an example output:

```
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
```

# Troubleshoot

There is no specific troubleshooting information for this feature. Refer to these documents for general connectivity troubleshooting information:

- ASA Packet Captures with CLI and ASDM Configuration Example
- ASA 8.2: Packet Flow through Cisco ASA Firewall

> **Note**: The TCP state bypass connections are not replicated to the standby unit in a failover pair.

## Error Messages

The ASA displays this error message even after the TCP state bypass feature is enabled:

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

The Internet Control Message Protocol (ICMP) packets are dropped by the ASA because of the security checks that are added by the stateful ICMP feature. These are usually either ICMP *echo* replies without a valid *echo request* already passed across the ASA, or ICMP error messages that are not related to any TCP, UDP, or ICMP session currently established in the ASA.

The ASA displays this log even if the TCP state bypass feature is enabled because the disablement of this functionality (that is, checks of the ICMP *return* entries for Type 3 in the connection table) is not possible. However, the TCP state bypass feature works correctly.

Enter this command in order to prevent the appearance of these messages:

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

## Related Information

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Requests for Comments (RFCs)
- Technical Support & Documentation - Cisco Systems