ASA 8.2.X TCP State Bypass Feature Configuration Example

Contents

Introduction

This document describes how to configure the TCP state bypass feature. This feature allows outbound and inbound flows through separate Cisco ASA 5500 Series Adaptive Security Appliances.

Prerequisites

License Requirements

The Cisco ASA 5500 Series Adaptive Security Appliances should have at least the base license.

Components Used

The information in this document is based on Cisco Adaptive Security Appliance (ASA) with version 8.2(1) and later.

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 information on document conventions.

TCP State Bypass

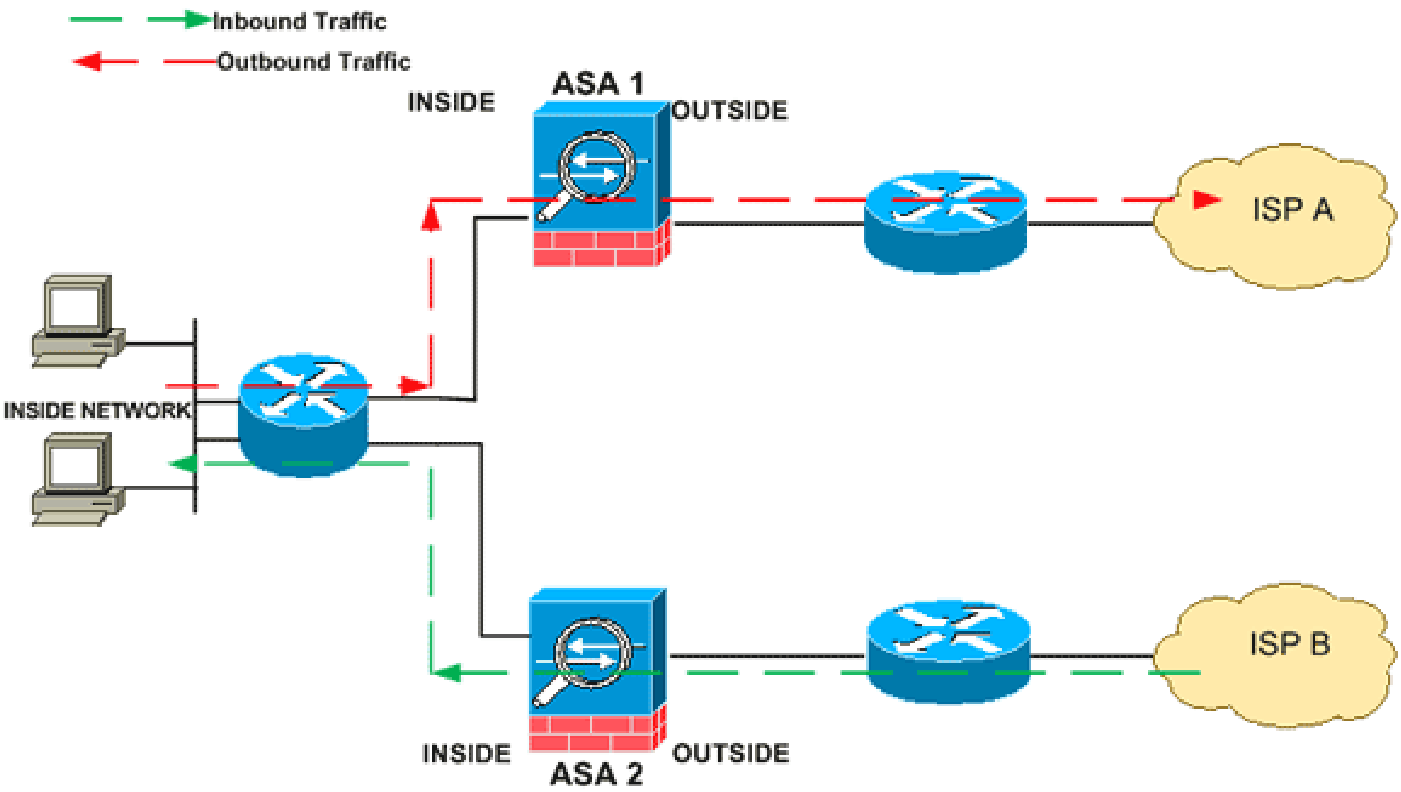
By default, all traffic that passes through the Cisco Adaptive Security Appliance (ASA) is inspected using the Adaptive Security Algorithm and is either allowed through or dropped based on the security policy. In order to maximize the firewall performance, the ASA checks the state of each packet (for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

TCP packets that match existing connections in the fast path can pass through the adaptive security appliance without rechecking every aspect of the security policy. This feature maximizes performance. However, the method used to establish the session in the fast path (which uses the SYN packet) and the checks that occur in the fast path (such as TCP sequence number) can stand in the way of asymmetrical routing solutions: both the outbound and inbound flow 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 of this connection go through *ASA 1*, the packets will 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 upstream routers, and traffic alternates between two ASAs, then you can configure TCP state bypass for specific traffic. TCP state bypass alters the way 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 matching the specified networks enters the ASA, and there is not an fast path entry, then the packet goes through the session management path 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: TCP state bypass feature is disabled by default on the Cisco ASA 5500 Series Adaptive Security Appliances.

Support Information

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

- Context Mode—Supported in single and multiple context mode.
- Firewall Mode—Supported in routed and transparent mode.
- Failover—Supports failover.

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

- Application inspection—Application inspection requires both inbound and outbound traffic to pass through the same ASA, so application inspection is not supported with TCP state bypass.
- AAA authenticated sessions—When a user authenticates with one ASA, traffic returning via the other ASA will be denied because the user did not authenticate with that ASA.
- TCP Intercept, maximum embryonic connection limit, TCP sequence number randomization—The ASA does not keep track of the state of the connection, so these features are not applied.
- TCP normalization—The TCP normalizer is disabled.
- SSM and SSC functionality—You cannot use TCP state bypass and any application running on an SSM or SSC, such as IPS or CSC.

NAT Guidelines: Because the translation session is established separately for each ASA, be sure to configure static NAT on both ASAs for TCP state bypass traffic; if you use dynamic NAT, the address chosen for the session on *ASA 1* will differ from the address chosen for the session on *ASA 2*.

Configure

This section describes how to configure the TCP state bypass feature on the Cisco ASA 5500 Series Adaptive Security Appliance (ASA).

TCP State Bypass Feature Configuration

Complete these steps in order to configure TCP state bypass feature on the Cisco ASA 5500 Series Adaptive Security Appliance:

1. Use the **class-map class_map_name** command in order to create a *class map*. The class map is used to identify the traffic for which you want to disable stateful firewall inspection. The class map used in this example is *tcp_bypass*.
   ```
   ASA(config)#class-map tcp_bypass
   ```
2. Use the **match parameter** command in order to specify interesting traffic in the class map. When using the Modular Policy Framework, use the **match access-list** command in class-map configuration mode in order to use an access list to identify 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
   ```
   tcp_bypass is the name of the access-list used in this example. Refer to Identifying Traffic (Layer 3/4 Class Map) for more information on specifying the interesting traffic.
3. Use the **policy-map name** command in order to add a policy map or edit a policy map (which is already present) that sets the actions to take with the class map traffic specified already. When using the Modular Policy Framework, use the **policy-map** command (without the type keyword) in global configuration mode in order to assign actions to 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. Use the **class** command in policy-map configuration mode in order to assign the class map (*tcp_bypass*) already created to the policy map (*tcp_bypass_policy*) where 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
   ```
5. Use 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. 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. In order to disable the service policy, use the **no** form of this command. Use the **service-policy** command to enable a set of policies on an interface.**global** applies the policy map to all interfaces, and **interface** applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can apply only one policy map to each interface.
   ```
   ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
   ```

Here is a sample configuration for TCP state bypass:

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

ASA(config)#access-list tcp_bypass extended
```

```
permit tcp 10.1.1.0 255.255.255.224 any !--- 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 outside ASA(config-pmap-c)#static
(inside,outside) 192.168.1.224 10.1.1.0 netmask 255.255.255.224
```

Verify

The **show conn** command displays the number of active TCP and UDP connections and provides information about connections of various types. In order to display the connection state for the designated connection type, use the **show conn** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses. The output display for connections that use **TCP state bypass** includes the flag **b**.

Troubleshoot

Error message

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
```

ICMP packets were dropped by the security appliance because of security checks added by the stateful ICMP feature that are usually either ICMP echo replies without a valid echo request already passed across the security appliance or ICMP error messages not related to any TCP, UDP, or ICMP session already established in the security appliance.

ASA displays this log even if TCP state bypass is enabled because disabling this functionality (that is, checking the ICMP return entries for Type 3 in connection table) is not possible. But the TCP state bypass feature works correctly.

Use this command in order to prevent these messages from appearing:

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

Related Information

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