Configuring Static and Default Routes

This chapter describes how to configure static and default routes on the ASA and includes the following sections:

- Information About Static and Default Routes, page 1-1
- Licensing Requirements for Static and Default Routes, page 1-2
- Guidelines and Limitations, page 1-2
- Configuring Static and Default Routes, page 1-2
- Monitoring a Static or Default Route, page 1-6
- Configuration Examples for Static or Default Routes, page 1-8
- Feature History for Static and Default Routes, page 1-9

Information About Static and Default Routes

To route traffic to a nonconnected host or network, you must define a static route to the host or network or, at a minimum, a default route for any networks to which the ASA is not directly connected; for example, when there is a router between a network and the ASA.

Without a static or default route defined, traffic to nonconnected hosts or networks generates the following syslog message:

%ASA-6-110001: No route to dest_address from source_address

You might want to use static routes in single context mode in the following cases:

- Your networks use a different router discovery protocol from EIGRP, RIP, or OSPF.
- Your network is small and you can easily manage static routes.
- You do not want the traffic or CPU overhead associated with routing protocols.

The simplest option is to configure a default route to send all traffic to an upstream router, relying on the router to route the traffic for you. However, in some cases the default gateway might not be able to reach the destination network, so you must also configure more specific static routes. For example, if the default gateway is outside, then the default route cannot direct traffic to any inside networks that are not directly connected to the ASA.

In transparent firewall mode, for traffic that originates on the ASA and is destined for a nondirectly connected network, you need to configure either a default route or static routes so the ASA knows out of which interface to send traffic. Traffic that originates on the ASA might include communications to a
syslog server, Websense or N2H2 server, or AAA server. If you have servers that cannot all be reached through a single default route, then you must configure static routes. Additionally, the ASA supports up to three equal cost routes on the same interface for load balancing.

**Licensing Requirements for Static and Default Routes**

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>All models</td>
<td>Base License.</td>
</tr>
</tbody>
</table>

**Guidelines and Limitations**

This section includes the guidelines and limitations for this feature.

**Context Mode Guidelines**
Supported in single and multiple context mode.

**Firewall Mode Guidelines**
Supported in routed and transparent firewall mode.

**IPv6 Guidelines**
Supports IPv6.

**Failover Guidelines**
Supports Stateful Failover of dynamic routing protocols.

**Additional Guidelines**
- IPv6 static routes are not supported in transparent mode in ASDM.
- In clustering, static route monitoring is only supported on the master unit. For information about clustering, see Chapter 1, “Configuring a Cluster of ASAs.”

**Configuring Static and Default Routes**

This section explains how to configure a static route and a static default route and includes the following topics:

- Configuring a Static Route, page 1-3
- Configuring a Default Static Route, page 1-4
- Configuring IPv6 Default and Static Routes, page 1-5
Chapter 1      Configuring Static and Default Routes

Configuring Static and Default Routes

Configuring a Static Route

Static routing algorithms are basically table mappings established by the network administrator before the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple. Because of this fact, static routing systems cannot react to network changes.

Static routes remain in the routing table even if the specified gateway becomes unavailable. If the specified gateway becomes unavailable, you need to remove the static route from the routing table manually. However, static routes are removed from the routing table if the specified interface goes down, and are reinstated when the interface comes back up.

Note

If you create a static route with an administrative distance greater than the administrative distance of the routing protocol running on the ASA, then a route to the specified destination discovered by the routing protocol takes precedence over the static route. The static route is used only if the dynamically discovered route is removed from the routing table.

You can define up to three equal cost routes to the same destination per interface. Equal-cost multi-path (ECMP) is not supported across multiple interfaces. With ECMP, the traffic is not necessarily divided evenly between the routes; traffic is distributed among the specified gateways based on an algorithm that hashes the source and destination IP addresses.

To configure a static route, see the following section:

• Adding or Editing a Static Route, page 1-3

Adding or Editing a Static Route

To add or edit a static route, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>route if_name dest_ip mask gateway_ip [distance]</td>
<td>Enables you to add a static route. The dest_ip and mask arguments indicate the IP address for the destination network and the gateway_ip argument is the address of the next-hop router. The addresses you specify for the static route are the addresses that are in the packet before entering the ASA and performing NAT. The distance argument is the administrative distance for the route. The default is 1 if you do not specify a value. Administrative distance is a parameter used to compare routes among different routing protocols. The default administrative distance for static routes is 1, giving it precedence over routes discovered by dynamic routing protocols but not directly connected routes. The default administrative distance for routes discovered by OSPF is 110. If a static route has the same administrative distance as a dynamic route, the static route takes precedence. Connected routes always take precedence over static or dynamically discovered routes.</td>
</tr>
</tbody>
</table>

Example:

hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 [1]
Examples

The following example shows static routes that are equal cost routes that direct traffic to three different gateways on the outside interface. The ASA distributes the traffic among the specified gateways.

```
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.2
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.3
```
Chapter 1 Configuring Static and Default Routes

### Configuring Static and Default Routes

**Tip**
You can enter 0 0 instead of 0.0.0.0 0.0.0.0 for the destination network address and mask, as shown in the following example:

```plaintext
hostname(config)# route outside 0 0 192.168.2.4 tunneled
```

---

**Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>route if_name 0.0.0.0 0.0.0.0 gateway_ip [distance</td>
<td>tunneled]</td>
</tr>
</tbody>
</table>

---

**Configuring IPv6 Default and Static Routes**

The ASA automatically routes IPv6 traffic between directly connected hosts if the interfaces to which the hosts are attached are enabled for IPv6 and the IPv6 ACLs allow the traffic.

To configure an IPv6 default route and static routes, perform the following steps:

**Detailed Steps**

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Adds a default IPv6 route.</td>
</tr>
<tr>
<td>ipv6 route if_name ::/0 next_hop_ipv6_addr</td>
<td>The example routes packets for network 7fff::0/32 to a networking device on the inside interface at 3FFE:1100:0:CC00::1</td>
</tr>
<tr>
<td>Example: hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1</td>
<td>The address ::/0 is the IPv6 equivalent of any.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Adds an IPv6 static route to the IPv6 routing table.</td>
</tr>
<tr>
<td>ipv6 route if_name destination next_hop_ipv6_addr [admin_distance]</td>
<td>The example routes packets for network 7fff::0/32 to a networking device on the inside interface at 3FFE:1100:0:CC00::1, and with an administrative distance of 110.</td>
</tr>
</tbody>
</table>
| Example: hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 [110] | }
Note The \texttt{ipv6 route} command works the same way as the \texttt{route} command does, which is used to define IPv4 static routes.

\section*{Monitoring a Static or Default Route}

One of the problems with static routes is that there is no inherent mechanism for determining if the route is up or down. They remain in the routing table even if the next hop gateway becomes unavailable. Static routes are only removed from the routing table if the associated interface on the ASA goes down.

The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. For example, you can define a default route to an ISP gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

The ASA implements this feature by associating a static route with a monitoring target that you define, and monitors the target using ICMP echo requests. If an echo reply is not received within a specified time period, the object is considered down and the associated route is removed from the routing table. A previously configured backup route is used in place of the removed route.

When selecting a monitoring target, you need to make sure that it can respond to ICMP echo requests. The target can be any network object that you choose, but you should consider using the following:

- The ISP gateway (for dual ISP support) address
- The next hop gateway address (if you are concerned about the availability of the gateway)
- A server on the target network, such as a AAA server, that the ASA needs to communicate with
- A persistent network object on the destination network

Note A desktop or notebook computer that may be shut down at night is not a good choice.

You can configure static route tracking for statically defined routes or default routes obtained through DHCP or PPPoE. You can only enable PPPoE clients on multiple interfaces with route tracking configured.

To configure static route tracking, perform the following steps:
### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** sla monitor sla_id                | Configures the tracked object monitoring parameters by defining the monitoring process.  
If you are configuring a new monitoring process, you enter sla monitor configuration mode.  
If you are changing the monitoring parameters for an unscheduled monitoring process that already has a type defined, you automatically enter sla protocol configuration mode. |
| Example: hostname(config)# sla monitor sla_id |                                                                        |
| **Step 2** type echo protocol ipIcmpEcho target_ip interface if_name    | Specifies the monitoring protocol. If you are changing the monitoring parameters for an unscheduled monitoring process that already has a type defined, you automatically enter sla protocol configuration mode and cannot change this setting. The target_ip argument is the IP address of the network object whose availability the tracking process monitors. While this object is available, the tracking process route is installed in the routing table. When this object becomes unavailable, the tracking process removes the route and the backup route is used in its place. |
| Example: hostname(config-sla-monitor)# type echo protocol ipIcmpEcho target_ip interface if_name | |
| **Step 3** sla monitor schedule sla_id [life {forever | seconds}] [start-time {hh:mm [:ss] | month day | day month} | pending | now | after hh:mm:ss} [ageout seconds] [recurring] | Schedules the monitoring process. Typically, you will use the sla monitor schedule sla_id life forever start-time now command for the monitoring schedule, and allow the monitoring configuration to determine how often the testing occurs. However, you can schedule this monitoring process to begin in the future and to only occur at specified times. |
| Example: hostname(config)# sla monitor schedule sla_id [life {forever | seconds}] [start-time {hh:mm [:ss] | month day | day month} | pending | now | after hh:mm:ss} [ageout seconds] [recurring] | |
| **Step 4** track track_id rtr sla_id reachability | Associates a tracked static route with the SLA monitoring process.  
The track_id argument is a tracking number you assign with this command. The sla_id argument is the ID number of the SLA process. |
| Example: hostname(config)# track track_id rtr sla_id reachability | |
| **Step 5** Do one of the following to define the static route to be installed in the routing table while the tracked object is reachable. These options allow you to track a static route or a default route obtained through DHCP or PPPOE. | Tracks a static route.  
You cannot use the tunneled option with the route command in static route tracking. |
| route if_name dest_ip mask gateway_ip [admin_distance] track track_id | |
### Configuration Examples for Static or Default Routes

The following example shows how to create a static route that sends all traffic destined for 10.1.1.0/24 to the router 10.1.2.45, which is connected to the inside interface, defines three equal cost static routes that direct traffic to three different gateways on the outside interface, and adds a default route for tunneled traffic. The ASA then distributes the traffic among the specified gateways:

```plaintext
hostname(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
hostname(config)# route outside 10.10.0.0 255.255.255.0 192.168.2.1
hostname(config)# route outside 10.10.0.0 255.255.255.0 192.168.2.2
hostname(config)# route outside 10.10.0.0 255.255.255.0 192.168.2.3
hostname(config)# route outside 0 0 192.168.2.4 tunneled
```

Unencrypted traffic received by the ASA for which there is no static or learned route is distributed among the gateways with the IP addresses 192.168.2.1, 192.168.2.2, and 192.168.2.3. Encrypted traffic received by the ASA for which there is no static or learned route is passed to the gateway with the IP address 192.168.2.4.

The following example creates a static route that sends all traffic destined for 10.1.1.0/24 to the router (10.1.2.45) connected to the inside interface:

```plaintext
hostname(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```
Feature History for Static and Default Routes

Table 1-1 lists each feature change and the platform release in which it was implemented.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing</td>
<td>7.0(1)</td>
<td>Static and default routing were introduced. We introduced the <code>route</code> command.</td>
</tr>
<tr>
<td>Clustering</td>
<td>9.0(1)</td>
<td>Supports static route monitoring on the master unit only.</td>
</tr>
</tbody>
</table>