CHAPTER 20

Configuring Static and Default Routes

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

Information About Static and Default Routes

To route traffic to a non-connected 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 adaptive security appliance is not directly connected; for example, when there is a router between a network and the adaptive security appliance.

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

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

Multiple context mode does not support dynamic routing,

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 adaptive security appliance.

In transparent firewall mode, for traffic that originates on the adaptive security appliance and is destined for a non-directly connected network, you need to configure either a default route or static routes so the adaptive security appliance knows out of which interface to send traffic. Traffic that originates on the

adaptive security appliance 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 adaptive security appliance supports up to three equal cost routes on the same interface for load balancing.

Licensing Requirements for Static and Default Routes

Model	License Requirement
All models	Base License.

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.

Additional Guidelines

IPv6 static routes are not supported in transparent mode in ASDM.

Configuring Static and Default Routes

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

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 adaptive security appliance, 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.

To configure a static route, see the following section:

- Add/Edit a Static Route, page 20-3

Add/Edit a Static Route

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

Command	Purpose
route *if_name dest_ip mask gateway_ip* [*distance*] **Example:** `hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 [1]`	This enables you to add a static route. The *dest_ip* and *mask* is the IP address for the destination network and the *gateway_ip* 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 adaptive security appliance and performing NAT. The *Metric/distance* 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 connect 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 routes take precedence. Connected routes always take precedence over static or dynamically discovered routes.

Configuring a Default Static Route

A default route identifies the gateway IP address to which the adaptive security appliance sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0.0.0/0 as the destination IP address. Routes that identify a specific destination take precedence over the default route.

Note In ASA software Versions 7.0 and later, if you have two default routes configured on different interfaces that have different metrics, the connection to the ASA firewall that is made from the higher metric interface fails, but connections to the ASA firewall from the lower metric interface succeed as expected.

You can define up to three equal cost default route entries per device. Defining more than one equal cost default route entry causes the traffic sent to the default route to be distributed among the specified gateways. When defining more than one default route, you must specify the same interface for each entry.

If you attempt to define more than three equal cost default routes, or if you attempt to define a default route with a different interface than a previously defined default route, you receive the following message:

```
"ERROR: Cannot add route entry, possible conflict with existing routes."
```

You can define a separate default route for tunneled traffic along with the standard default route. When you create a default route with the **tunneled** option, all traffic from a tunnel terminating on the adaptive security appliance that cannot be routed using learned or static routes, is sent to this route. For traffic emerging from a tunnel, this route overrides over any other configured or learned default routes.

Limitations on Configuring a Default Static Route

The following restrictions apply to default routes with the tunneled option:

- Do not enable unicast RPF (**ip verify reverse-path**) on the egress interface of tunneled route. Enabling Unicast RPF on the egress interface of a tunneled route causes the session to fail.
- Do not enable TCP intercept on the egress interface of the tunneled route. Doing so causes the session to fail.
- Do not use the VoIP inspection engines (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), the DNS inspect engine, or the DCE RPC inspection engine with tunneled routes. These inspection engines ignore the tunneled route.

You cannot define more than one default route with the tunneled option; ECMP for tunneled traffic is not supported.

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

Command	Purpose
route *if_name* 0.0.0.0 0.0.0.0 *gateway_ip* [distance | tunneled] **Example:** hostname(config)# route outside 0 0 192.168.2.4 tunneled	This enables you to add a static route. The *dest_ip* and *mask* is the IP address for the destination network and the *gateway_ip* 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 adaptive security appliance and performing NAT. The *distance* 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 connect 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 routes take precedence. Connected routes always take precedence over static or dynamically discovered routes.

Tip You can enter 0 0 instead of 0.0.0.0 0.0.0.0 for the destination network address and mask, for example:

```
hostname(config)# route outside 0 0 192.168.1 1
```

Configuring IPv6 Default and Static Routes

The adaptive security appliance 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

	Command	Purpose
Step 1	**ipv6 route** *if_name* **::/0** *next_hop_ipv6_addr* **Example:** hostname(config)#ipv6 route *inside* 7fff::0/32 *3FFE:1100:0:CC00::1*	This step adds a default IPv6 route. This example routes packets for network 7fff::0/32 to a networking device on the inside interface at 3FFE:1100:0:CC00::1 The address ::/0 is the IPv6 equivalent of “any.”
Step 2	**ipv6 route** *if_name destination next_hop_ipv6_addr* [*admin_distance*] **Example:** hostname(config)# ipv6 route *inside* 7fff::0/32 *3FFE:1100:0:CC00::1* [*110*]	This step adds an IPv6 static route to the IPv6 routing table. This 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.

Note The **ipv6 route** command works the same way as the **route** command, which is used to define IPv4 static routes.

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 adaptive security appliance 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. This allows you to, for example, 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 adaptive security appliance does this by associating a static route with a monitoring target that you define. It 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 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 adaptive security appliance needs to communicate with
- A persistent network object on the destination network (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 interface with route tracking.

To configure static route tracking, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**sla monitor** *sla_id* **Example:** hostname(config)# sla monitor *sla_id*	Configure 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.
Step 2	**type echo protocol ipIcmpEcho** *target_ip* **interface** *if_name* **Example:** hostname(config-sla-monitor)# type echo protocol ipIcmpEcho *target_ip* interface *if_name*	Specify 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* 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 removed the route and the backup route is used in its place.
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**] **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]	Schedule 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.
Step 4	**track** *track_id* **rtr** *sla_id* **reachability** **Example:** hostname(config)# track *track_id* rtr *sla_id* reachability	Associate a tracked static route with the SLA monitoring process. The *track_id* is a tracking number you assign with this command. The *sla_id* is the ID number of the SLA process.
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 default route obtained through DHCP or PPPOE.	
	route *if_name dest_ip mask gateway_ip* [*admin_distance*] **track** *track_id* **Example:** hostname(config)# route *if_name dest_ip mask gateway_ip* [*admin_distance*] track *track_id*	This option tracks a static route. You cannot use the **tunneled** option with the **route** command with static route tracking.

Command	Purpose
hostname(config)# interface *phy_if* hostname(config-if)# dhcp client route track *track_id* hostname(config-if)# ip address dhcp setroute hostname(config-if)# exit	This option tracks a default route obtained through DHCP, Remember that you must use the **setroute** argument with the **ip address dhcp** command to obtain the default route using DHCP.
hostname(config)# interface *phy_if* hostname(config-if)# pppoe client route track *track_id* hostname(config-if)# ip address pppoe setroute hostname(config-if)# exit	This option tracks a default route obtained through PPPoE. You must use the **setroute** argument with the **ip address pppoe** command to obtain the default route using PPPoE.

Configuration Examples for Static or Default Routes

The following example shows how to configure static routes:

Step 1 Create a static route:

```
hostname(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```

In this step, a static route is created that sends all traffic destined for 10.1.1.0/24 to the router (10.1.2.45) connected to the inside interface.

Step 2 Define three equal cost static routes that directs traffic to three different gateways on the outside interface, and adds a default route for tunneled traffic. The adaptive security appliance distributes the traffic among the specified gateways.

```
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.1
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.2
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.3
hostname(config)# route outside 0 0 192.168.2.4 tunneled
```

Unencrypted traffic received by the adaptive security appliance 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 receive by the adaptive security appliance for which there is no static or learned route is passed to the gateway with the IP address 192.168.2.4.

Feature History for Static and Default Routes

Table 20-1 lists each feature change and the platform release in which it was implemented.

Table 20-1 Feature History for Static and Default Routes

Feature Name	Platform Releases	Feature Information
Routing	7.0(1)	The **route** command was introduced. The **route** command was introduced to enter a static or default route for the specified interface.