Configuring IP Addresses, Routing, and DHCP

This chapter tells how to configure IP addresses, static routes, dynamic routing, and DHCP on the Firewall Services Module (FWSM).

For routed and transparent mode, see the following sections:

For routed mode only, see the following sections:

Note Multiple security contexts do not support dynamic routing protocols, such as RIP and OSPF.

Configuring IP Addresses

This section describes how to set the IP address(es) for routed mode or for transparent mode, and includes the following topics:

Assigning IP Addresses to Interfaces for a Routed Firewall

Routed firewall mode only

To assign an IP address to a VLAN interface, enter the following command:

```
FWSM/contexta(config)# ip address interface_name ip_address mask [standby ip_address]
```

In single context mode, each interface address must be on a unique subnet. In multiple context mode, if this interface is on a shared VLAN, then the IP address must be unique, and cannot be used by another context on the shared VLAN. If the VLAN is unique, this IP address can be used by other contexts if desired.

The **standby** keyword and address is used for failover. See the "Configuring Failover" section on page 15-14 for more information.

For example, to set the IP address of the inside interface, enter the following command:

```
FWSM/contexta(config)# ip address inside 192.168.1.1 255.255.255.0
```

Setting the Management IP Address for a Transparent Firewall

Transparent firewall mode only

A transparent firewall does not participate in IP routing. The only IP configuration required for the FWSM is to set the management IP address. This address is required because the FWSM uses this address as the source address for traffic originating on the FWSM, such as system messages or communications with AAA servers. You can also use this address for remote management access.

For multiple context mode, set the management IP address within each context.

To set the management IP address, enter the following command:

```
FWSM/contexta(config)# ip address ip_address [mask] [standby ip_address]
```

This address must be on the same subnet as the upstream and downstream routers.

The **standby** keyword and address is used for failover. See the "Configuring Failover" section on page 15-14 for more information.

Configuring the Default Route

The default route identifies the router IP address to which the FWSM sends all IP packets for which it does not have a route. The FWSM might receive a default route from the dynamic routing protocol (single mode only), but we recommend setting a static default route as a backup.

For transparent firewall mode, for traffic that originates on the FWSM and is destined for a non-directly connected network, configure either a default route or static routes so the FWSM knows out of which interface to send traffic. Traffic that originates on the FWSM might include communications to a syslog server, Websense or N2H2 server, or AAA server.

The FWSM supports up to three equal cost routes on the same interface for load balancing.

Routes that identify a specific destination address take precedence over the default route.

To set a default route, enter the following command:

```
FWSM/contexta(config)# route gateway_interface 0 0 gateway_ip [metric]
```

The *metric* is the number of hops to *gateway_ip*. The default is 1 if you do not specify a metric.

For example, if the FWSM receives traffic that it does not have a route for, it sends the traffic out the outside interface to the router at 10.1.1.1:

```
FWSM/contexta(config)# route outside 0 0 10.1.1.1 1
```

Configuring Static Routes

Multiple context mode does not support dynamic routing, so you must use static routes for any networks to which the FWSM is not directly connected; for example, when there is a router between a network and the FWSM.

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

- Your networks use a different router discovery protocol from 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 (see the previous section) 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 FWSM.

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

The FWSM supports up to three equal cost routes on the same interface for load balancing.

Static routes take precedence over dynamic routes if they have the same metric (number of router hops).

To add a static route, enter the following command:

```
FWSM/contexta(config)# route gateway_interface dest_ip mask gateway_ip [metric]
```

The *metric* is the number of hops to *gateway_ip*. The default is 1 if you do not specify a metric.

The addresses you specify for the static route are the addresses that are in the packet before entering the FWSM and performing NAT.

For example, to send all traffic destined for 10.1.1.0/24 to the router (10.1.2.45) connected to the inside interface, enter the following command:

```
FWSM/contexta(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```

The following static routes are equal cost routes that direct traffic to three different routers on the outside interface. The FWSM sends 1/3 of the traffic to each router.

```
FWSM/contexta(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
FWSM/contexta(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.2
FWSM/contexta(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.3
```

Configuring OSPF

Single context mode only

Routed firewall mode only

This section describes how to configure Open Shortest Path First (OSPF). For an overview of OSPF, see the following topic:

- OSPF Overview, page 8-4

To enable OSPF, see the following topic:

- Enabling OSPF, page 8-5

After you enable OSPF, you can configure advanced options according to the following topics:

- Redistributing Routes Between OSPF Processes, page 8-6
- Configuring OSPF Interface Parameters, page 8-9
- Configuring OSPF Area Parameters, page 8-11
- Configuring OSPF NSSA, page 8-12
- Configuring Route Summarization Between OSPF Areas, page 8-13
- Configuring Route Summarization When Redistributing Routes into OSPF, page 8-14
- Generating a Default Route, page 8-14
- Configuring Route Calculation Timers, page 8-15
- Logging Neighbors Going Up or Down, page 8-15
- Displaying OSPF Update Packet Pacing, page 8-16
- Monitoring OSPF, page 8-16
- Restarting the OSPF Process, page 8-17

OSPF Overview

Single context mode only

Routed firewall mode only

OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. Each router in an OSPF area contains an identical link-state database, which is a list of each of the router usable interfaces and reachable neighbors.

The advantages of OSPF over RIP include the following:

- OSPF link-state database updates are sent less frequently than RIP updates, and the link-state database is updated instantly rather than gradually as stale information is timed out.
- Routing decisions are based on cost, which is an indication of the overhead required to send packets across a certain interface. The FWSM calculates the cost of an interface based on link bandwidth rather than the number of hops to the destination. The cost can be configured to specify preferred paths.

The disadvantage of shortest path first algorithms is that they require a lot of CPU cycles and memory.

The FWSM can run two processes of OSPF protocol simultaneously, on different sets of interfaces. You might want to run two processes if you have interfaces that use the same IP addresses (NAT allows these interfaces to coexist, but OSPF does not allow overlapping addresses). Or you might want to run one process on the inside, and another on the outside, and redistribute a subset of routes between the two processes. Similarly, you might need to segregate private addresses from public addresses.

Redistribution between the two OSPF processes is supported. Static and connected routes configured on OSPF-enabled interfaces on the FWSM can also be redistributed into the OSPF process. You cannot enable RIP on any of the same interfaces as the interfaces on which OSPF is enabled. Redistribution between RIP and OSPF is not supported.

The FWSM supports the following OSPF features:

- Support of intra-area, interarea, and external (type I and Type II) routes.
- Support of a virtual link.
- OSPF link-state advertisement (LSA) flooding.
- Authentication to OSPF packets (both password and MD5 authentication).
- Support for configuring the FWSM as a designated router or a designated backup router. The FWSM also can be set up as an area border router; however, the ability to configure the FWSM as an autonomous system boundary router is limited to default information only (for example, injecting a default route).
- Support for stub areas and not-so-stubby-area (NSSA).
- Area boundary router type-3 LSA filtering.
- Advertisement of static and global address translations.

Enabling OSPF

Single context mode only

Routed firewall mode only

To enable OSPF, you need to create an OSPF routing process, specify the range of IP addresses associated with the routing process, then assign area IDs associated with that range of IP addresses.

To enable OSPF, follow these steps:

Step 1 To create an OSPF routing process, enter the following command:

```
FWSM(config)# router ospf process_id
```

This command enters the router configuration mode for this OSPF process.

The *process_id* is an internally used identifier for this routing process. It can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.

Step 2 To define the IP addresses on which OSPF runs and to define the area ID for that interface, enter the following command:

```
FWSM(config-router)# network ip_address mask area area_id
```

This example shows how to enable OSPF:

```
FWSM(config)# router ospf 2
FWSM(config-router)# network 2.0.0.0 255.0.0.0 area 0
```

Redistributing Routes Between OSPF Processes

Single context mode only

Routed firewall mode only

Note Note: The maximum number of route entries for all types of routes (connected, static and dynamic) supported by FWSM is 32768, or 32K.

The FWSM can control the redistribution of routes between OSPF routing processes. The FWSM matches and changes routes according to settings in the **redistribution** command or by using a route map. See also the "Generating a Default Route" section on page 8-14 for another use for route maps.

Note The FWSM cannot redistribute routes between routing protocols. However, the FWSM can redistribute static and connected routes.

This section includes the following topics:

Adding a Route Map

Single context mode only

Routed firewall mode only

To define a route map, follow these steps:

Step 1 To create a route map entry, enter the following command:

```
FWSM(config)# route-map name {permit | deny} [sequence_number]
```

Route map entries are read in order. You can identify the order using the *sequence_number* option, or the FWSM uses the order in which you add the entries.

Step 2 Enter one or more **match** commands:

- To match any routes that have a destination network that matches a standard ACL, enter the following command:

  ```
  FWSM(config-route-map)# match ip address acl_id [acl_id] [...]
  ```

See the "Adding a Standard Access Control List" section on page 10-17 to add the standard ACL. If you specify more than one ACL, then the route can match any of the ACLs.

- To match any routes that have a specified metric, enter the following command:

```
FWSM(config-route-map)# match metric metric_value
```

The *metric_value* can be from 0 to 4294967295.

- To match any routes that have a next hop router address that matches a standard ACL, enter the following command:

```
FWSM(config-route-map)# match ip next-hop acl_id [acl_id] [...]
```

See the "Adding a Standard Access Control List" section on page 10-17 to add the standard ACL. If you specify more than one ACL, then the route can match any of the ACLs.

- To match any routes with the specified next hop interface, enter the following command:

```
FWSM(config-route-map)# match interface vlan number [vlan number]
```

If you specify more than one interface, then the route can match either interface.

- To match any routes that have been advertised by routers that match a standard ACL, enter the following command:

```
FWSM(config-route-map)# match ip route-source acl_id [acl_id] [...]
```

See the "Adding a Standard Access Control List" section on page 10-17 to add the standard ACL. If you specify more than one ACL, then the route can match any of the ACLs.

- To match the route type, enter the following command:

```
FWSM(config-route-map)# match route-type {internal | external [type-1 | type-2]}
```

Step 3 Enter one or more **set** commands.

If a route matches the **match** commands, then the following **set** commands determine the action to perform on the route before redistributing it.

- To set the metric, enter the following command:

```
FWSM(config-route-map)# set metric metric_value
```

The *metric_value* can be a value between 0 and 294967295

- To set the metric type, enter the following command:

```
FWSM(config-route-map)# set metric-type {type-1 | type-2}
```

- To set the next hop router IP address, enter the following command:

```
FWSM(config-route-map)# set ip next-hop ip_address [ip_address] [...]
```

The next hop must be an adjacent router. If you specify more than one address, if the interface associated with the first next hop address is down, then the next address is used.

The following example redistributes routes with a hop count equal to 1. The FWSM redistributes these routes as external link-state advertisements (LSAs) with a metric of 5, metric type of Type 1, and a tag equal to 1.

```
FWSM(config)# route-map 1-to-2 permit
FWSM(config-route-map)# match metric 1
FWSM(config-route-map)# set metric 5
FWSM(config-route-map)# set metric-type type-1
```

Redistributing Static, Connected, or OSPF Routes to an OSPF Process

Single context mode only

Routed firewall mode only

To redistribute static, connected, or OSPF routes from one process into another OSPF process, follow these steps:

Step 1 If you have not already done so, enter the router configuration mode for the OSPF process you want to redistribute into by entering the following command:

```
FWSM(config)# router ospf process_id
```

Step 2 To specify the routes you want to redistribute, enter the following command:

```
FWSM(config-router)# redistribute {ospf process_id | static | connect}
[match {internal | external 1 | external 2}] [metric metric-value]
[metric-type {type-1 | type-2}] [tag tag_value] [subnets] [route-map map_name]
```

The **ospf** *process_id*, **static**, and **connect** keywords specify from where you want to redistribute routes.

You can either use the options in this command to match and set route properties, or you can use a route map. The **tag** and **subnets** options do not have equivalents in the **route-map** command. If you use both a route map and options in the **redistribute** command, then they must match.

The following example redistributes routes from OSPF process 1 into OSPF process 2 by matching routes with a metric equal to 1. The FWSM redistributes these routes as external link-state advertisements (LSAs) with a metric of 5, metric type of Type 1, and a tag equal to 1.

```
FWSM(config)# route-map 1-to-2 permit
FWSM(config-route-map)# match metric 1
FWSM(config-route-map)# set metric 5
FWSM(config-route-map)# set metric-type type-1
FWSM(config-route-map)# set tag 1
FWSM(config-route-map)# router ospf 2
FWSM(config-router)# redistribute ospf 1 route-map 1-to-2
```

The following example causes the specified OSPF process routes to be redistributed into OSPF process 109. The OSPF metric is remapped to 100.

```
FWSM(config)# router ospf 109
FWSM(config-router)# redistribute ospf 108 metric 100 subnets
FWSM(config-router)# redistribute static 108 metric 100 subnets
```

In the following example, the link-state cost is specified as 5, and the metric type is set to external, indicating that it has lower priority than internal metrics.

```
FWSM(config)# router ospf 1
FWSM(config-router)# redistribute ospf 2 metric 5 metric-type external
```

Configuring OSPF Interface Parameters

Single context mode only

Routed firewall mode only

You can alter some interface-specific OSPF parameters as necessary. You are not required to alter any of these parameters, but the following interface parameters must be consistent across all routers in an attached network: **ip ospf hello-interval**, **ip ospf dead-interval**, and **ip ospf authentication-key**. Be sure that if you configure any of these parameters, the configurations for all routers on your network have compatible values.

To configure OSPF interface parameters, follow these steps:

Step 1 To enter the interface configuration mode, enter the following command:

```
FWSM(config)# interface interface_name
```

Step 2 Enter any of the following commands:

- To specify the authentication type for an interface, enter the following command:

  ```
  FWSM(config-interface)# ospf authentication [message-digest | null]
  ```

- To assign a password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password authentication, enter the following command:

  ```
  FWSM(config-interface)# ospf authentication-key key
  ```

  The *key* can be any continuous string of characters up to 8 bytes in length.

  The password created by this command is used as a key that is inserted directly into the OSPF header when the FWSM software originates routing protocol packets. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

- To explicitly specify the cost of sending a packet on an OSPF interface, enter the following command:

  ```
  FWSM(config-interface)# ospf cost cost
  ```

  The *cost* is an integer from 1 to 65535.

- To set the number of seconds that a device must wait before it declares a neighbor OSPF router down because it has not received a hello packet, enter the following command:

  ```
  FWSM(config-interface)# ospf dead-interval seconds
  ```

  The value must be the same for all nodes on the network.

- To specify the length of time between the hello packets that the FWSM sends on an OSPF interface, enter the following command:

  ```
  FWSM(config-interface)# ospf hello-interval seconds
  ```

  The value must be the same for all nodes on the network.

- To enable OSPF MD5 authentication, enter the following command:

  ```
  FWSM(config-interface)# ospf message-digest-key key_id md5 key
  ```

  Set the following values:

  - *key_id*—An identifier in the range from 1 to 255.
  - *key*—Alphanumeric password of up to 16 bytes.

  Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same key value.

  We recommend that you not keep more than one key per interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover.

- To set the priority to help determine the OSPF designated router for a network, enter the following command:

  ```
  FWSM(config-interface)# ospf priority number_value
  ```

  The *number_value* is between 0 to 255.

- To specify the number of seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to an OSPF interface, enter the following command:

  ```
  FWSM(config-interface)# ospf retransmit-interval seconds
  ```

  The *seconds* must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds. The default is 5 seconds.

- To set the estimated number of seconds required to send a link-state update packet on an OSPF interface, enter the following command:

  ```
  FWSM(config-interface)# ospf transmit-delay seconds
  ```

  The *seconds* is from 1 to 65535 seconds. The default is 1 second.

This example shows how to configure the OSPF interfaces:

```
FWSM(config)# router ospf 2
FWSM(config-router)# network 2.0.0.0 255.0.0.0 area 0
FWSM(config-router)# interface inside
FWSM(config-interface)# ospf cost 20
FWSM(config-interface)# ospf retransmit-interval 15
FWSM(config-interface)# ospf transmit-delay 10
FWSM(config-interface)# ospf priority 20
FWSM(config-interface)# ospf hello-interval 10
FWSM(config-interface)# ospf dead-interval 40
FWSM(config-interface)# ospf authentication-key cisco
FWSM(config-interface)# ospf message-digest-key 1 md5 cisco
FWSM(config-interface)# ospf authentication message-digest
```

View your configuration by entering the following command:

```
FWSM(config)# show ip ospf

Routing Process "ospf 2" with ID 20.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 5. Checksum Sum 0x 26da6
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x 209a3
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Configuring OSPF Area Parameters

Single context mode only

Routed firewall mode only

You can configure several area parameters. These area parameters (shown in the following task table) include setting authentication, defining stub areas, and assigning specific costs to the default summary route. Authentication provides password-based protection against unauthorized access to an area.

Stub areas are areas into which information on external routes is not sent. Instead, there is a default external route generated by the area border router, into the stub area for destinations outside the autonomous system. To take advantage of the OSPF stub area support, default routing must be used in the stub area. To further reduce the number of LSAs sent into a stub area, you can configure the **no-summary** keyword of the **area stub** command on the area border router to prevent it from sending summary link advertisement (LSAs type 3) into the stub area.

To specify area parameters for your network, follow these steps:

Step 1 If you have not already done so, enter the router configuration mode for the OSPF process you want to configure by entering the following command:

```
FWSM(config)# router ospf process_id
```

Step 2 Enter any of the following commands:

- To enable authentication for an OSPF area, enter the following command:

  ```
  FWSM(config-router)# area area-id authentication
  ```

- To enable MD5 authentication for an OSPF area, enter the following command:

  ```
  FWSM(config-router)# area area-id authentication message-digest
  ```

- To define an area to be a stub area, enter the following command:

  ```
  FWSM(config-router)# area area-id stub [no-summary]
  ```

- To assign a specific cost to the default summary route used for the stub area, enter the following command:

  ```
  FWSM(config-router)# area area-id default-cost cost
  ```

  The *cost* is an integer from 1 to 65535. The default is 1.

This example shows how to configure the OSPF area parameters:

```
FWSM(config)# router ospf 2
FWSM(config-router)# area 0 authentication
FWSM(config-router)# area 0 authentication message-digest
FWSM(config-router)# area 17 stub
FWSM(config-router)# area 17 default-cost 20
```

Configuring OSPF NSSA

Single context mode only

Routed firewall mode only

The OSPF implementation of a not-so-stubby-area (NSSA) is similar to an OSPF stub area. NSSA does not flood type 5 external LSAs from the core into the area, but it can import autonomous system external routes in a limited way within the area.

NSSA imports type 7 autonomous system external routes within an NSSA area by redistribution. These type 7 LSAs are translated into type 5 LSAs by NSSA area border routers, which are flooded throughout the whole routing domain. Summarization and filtering are supported during the translation.

You can simplify administration if you are an Internet service provider (ISP) or a network administrator that must connect a central site using OSPF to a remote site that is using a different routing protocol using NSSA.

Before the implementation of NSSA, the connection between the corporate site border router and the remote router could not be run as an OSPF stub area because routes for the remote site could not be redistributed into the stub area, and two routing protocols needed to be maintained. A simple protocol such as RIP was usually run and handled the redistribution. With NSSA, you can extend OSPF to cover the remote connection by defining the area between the corporate router and the remote router as an NSSA.

To specify area parameters for your network as needed to configure OSPF NSSA, follow these steps:

Step 1 If you have not already done so, enter the router configuration mode for the OSPF process you want to configure by entering the following command:

```
FWSM(config)# router ospf process_id
```

Step 2 Enter any of the following commands:

- To define an NSSA area, enter the following command:

  ```
  FWSM(config-router)# area area-id nssa [no-redistribution]
  [default-information-originate]
  ```

- To summarize groups of addresses, enter the following command:

```
FWSM(config-router)# summary address ip_address mask [not advertise] [tag tag]
```

This command helps reduce the size of the routing table. Using this command for OSPF causes an OSPF autonomous system boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address.

OSPF does not support **summary-address 0.0.0.0 0.0.0.0**.

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement:

```
FWSM(config-router)# summary-address 10.1.1.0 255.255.0.0
```

Before you use this feature, consider these guidelines:

- You can set a type 7 default route that can be used to reach external destinations. When configured, the router generates a type 7 default into the NSSA or the NSSA area boundary router.
- Every router within the same area must agree that the area is NSSA; otherwise, the routers will not be able to communicate.

Configuring Route Summarization Between OSPF Areas

Single context mode only

Routed firewall mode only

Route summarization is the consolidation of advertised addresses. This feature causes a single summary route to be advertised to other areas by an area boundary router. In OSPF, an area boundary router advertises networks in one area into another area. If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the area boundary router to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

To define an address range for route summarization, follow these steps:

Step 1 If you have not already done so, enter the router configuration mode for the OSPF process you want to configure by entering the following command:

```
FWSM(config)# router ospf process_id
```

Step 2 To set the address range, enter the following command:

```
FWSM(config-router)# area area-id range ip-address mask [advertise | not-advertise]
```

This example shows how to configure route summarization between OSPF areas:

```
FWSM(config)# router ospf 1
FWSM(config-router)# area 17 range 12.1.0.0 255.255.0.0
```

Configuring Route Summarization When Redistributing Routes into OSPF

Single context mode only

Routed firewall mode only

When routes from other protocols are redistributed into OSPF, each route is advertised individually in an external LSA. However, you can configure the FWSM to advertise a single route for all the redistributed routes that are covered by a specified network address and mask. This configuration decreases the size of the OSPF link-state database.

To configure the software advertisement on one summary route for all redistributed routes covered by a network address and mask, follow these steps:

Step 1 If you have not already done so, enter the router configuration mode for the OSPF process you want to configure by entering the following command:

```
FWSM(config)# router ospf process_id
```

Step 2 To set the summary address, enter the following command:

```
FWSM(config-router)# summary-address ip_address mask [not advertise] [tag tag]
```

OSPF does not support **summary-address 0.0.0.0 0.0.0.0**.

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement:

```
FWSM(config)# router ospf 1
FWSM(config-router)# summary-address 10.1.0.0 255.255.0.0
```

Generating a Default Route

Single context mode only

Routed firewall mode only

You can force an autonomous system boundary router to generate a default route into an OSPF routing domain. Whenever you specifically configure redistribution of routes into an OSPF routing domain, the router automatically becomes an autonomous system boundary router. However, an autonomous system boundary router does not by default generate a default route into the OSPF routing domain.

To generate a default route, follow these steps:

Step 1 If you have not already done so, enter the router configuration mode for the OSPF process you want to configure by entering the following command:

```
FWSM(config)# router ospf process_id
```

Step 2 To force the autonomous system boundary router to generate a default route, enter the following command:

```
FWSM(config-router)# default-information originate [always] [metric metric-value]
[metric-type {1 | 2}] [route-map map-name]
```

This example shows how to generate a default route:

```
FWSM(config)# router ospf 2
FWSM(config-router)# default-information originate always
```

Configuring Route Calculation Timers

Single context mode only

Routed firewall mode only

You can configure the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation. You also can configure the hold time between two consecutive SPF calculations.

To configure route calculation timers, follow these steps:

Step 1 If you have not already done so, enter the router configuration mode for the OSPF process you want to configure by entering the following command:

```
FWSM(config)# router ospf process_id
```

Step 2 To configure the route calculation time, enter the following command:

```
FWSM(config-router)# timers spf spf-delay spf-holdtime
```

The *spf-delay* is the delay time (in seconds) between when OSPF receives a topology change and when it starts an SPF calculation. It can be an integer from 0 to 65535. The default time is 5 seconds. A value of 0 means that there is no delay; that is, the SPF calculation is started immediately.

The *spf-holdtime* is the minimum time (in seconds) between two consecutive SPF calculations. It can be an integer from 0 to 65535. The default time is 10 seconds. A value of 0 means that there is no delay; that is, two SPF calculations can be done, one immediately after the other.

This example shows how to configure route calculation timers:

```
FWSM(config)# router ospf 1
FWSM(config-router)# timers spf 10 120
```

Logging Neighbors Going Up or Down

Single context mode only

Routed firewall mode only

By default, the system sends a system message when an OSPF neighbor goes up or down.

Configure this command if you want to know about OSPF neighbors going up or down without turning on the **debug ip ospf adjacency** command. The **log-adj-changes router** configuration command provides a higher level view of the peer relationship with less output. Configure **log-adj-changes detail** if you want to see messages for each state change.

To log neighbors going up or down, follow these steps:

Step 1 If you have not already done so, enter the router configuration mode for the OSPF process you want to configure by entering the following command:

```
FWSM(config)# router ospf process_id
```

Step 2 To configure logging fir neighbors going up or down, enter the following command:

```
FWSM(config-router)# log-adj-changes [detail]
```

This example shows how to log neighbors:

```
FWSM(config)# router ospf 1
FWSM(config-router)# log-adj-changes detail
```

Displaying OSPF Update Packet Pacing

Single context mode only

Routed firewall mode only

OSPF update packets are automatically paced so they are not sent less than 33 milliseconds apart. Without pacing, some update packets could get lost in situations where the link is slow, a neighbor could not receive the updates quickly enough, or the router could run out of buffer space. For example, without pacing packets might be dropped if either of the following topologies exist:

- A fast router is connected to a slower router over a point-to-point link.
- During flooding, several neighbors send updates to a single router at the same time.

Pacing is also used between resends to increase efficiency and minimize lost retransmissions. You also can display the LSAs waiting to be sent out an interface. The benefit of the pacing is that OSPF update and retransmission packets are sent more efficiently.

There are no configuration tasks for this feature; it occurs automatically.

To observe OSPF packet pacing by displaying a list of LSAs waiting to be flooded over a specified interface, enter the following command:

```
FWSM# show ip ospf flood-list vlan number
```

Monitoring OSPF

Single context mode only

Routed firewall mode only

You can display specific statistics such as the contents of IP routing tables, caches, and databases. You can use the information provided to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path that your device packets are taking through the network.

To display various routing statistics, perform one of these tasks, as needed:

- To display general information about OSPF routing processes, enter the following command:

  ```
  FWSM# show ip ospf [process-id]
  ```

- To display the internal OSPF routing table entries to the area border router and autonomous system border router, enter the following command:

  ```
  FWSM# show ip ospf border-routers
  ```

- To display lists of information related to the OSPF database for a specific router, enter the following command:

  ```
  FWSM# show ip ospf [process-id [area-id]] database
  ```

- To display a list of LSAs waiting to be flooded over an interface (to observe OSPF packet pacing), enter the following command:

  ```
  FWSM# show ip ospf flood-list interface interface-type
  ```

- To display OSPF-related interface information, enter the following command:

  ```
  FWSM# show ip ospf interface [interface-type interface-number]
  ```

- To display OSPF neighbor information on a per-interface basis, enter the following command:

  ```
  FWSM# show ip ospf neighbor [interface-name] [neighbor-id] detail
  ```

- To display a list of all LSAs requested by a router, enter the following command:

  ```
  FWSM# show ip ospf request-list [neighbor] [interface] [interface-neighbor]
  ```

- To display a list of all LSAs waiting to be resent, enter the following command:

  ```
  FWSM# show ip ospf retransmission-list [neighbor] [interface] [interface-neighbor]
  ```

- To display a list of all summary address redistribution information configured under an OSPF process, enter the following command:

  ```
  FWSM# show ip ospf [process-id] summary-address
  ```

- To display OSPF-related virtual links information, enter the following command:

  ```
  FWSM# show ip ospf virtual-links
  ```

Restarting the OSPF Process

To restart an OSPF process, clear redistribution, or counters, enter the following command:

```
FWSM(config)# clear ip ospf pid {process | redistribution | counters
[neighbor [neighbor-interface] [neighbor-id]]}
```

Configuring RIP

Single context mode only

Routed firewall mode only

This section describes how to configure Route Information Protocol (RIP), and includes:

RIP Overview

Single context mode only

Routed firewall mode only

Devices that support RIP send routing-update messages at regular intervals and when the network topology changes. These RIP packets contain information about the networks that the devices can reach, as well as the number of routers or gateways that a packet must travel through to reach the destination address. RIP generates more traffic than OSPF, but is easier to configure initially.

RIP has advantages over static routes because the initial configuration is simple, and you do not need to update the configuration when the topology changes. The disadvantage to RIP is that there is more network and processing overhead than static routing.

The FWSM uses a limited version of RIP; it does not send out RIP updates that identify the networks that the FWSM can reach. However, you can enable one or both of the following methods:

- Passive RIP—The FWSM listens for RIP updates but does not send any updates about its networks out of the interface.

  Passive RIP allows the FWSM to learn about networks to which it is not directly connected.

- Default Route Updates—Instead of sending normal RIP updates that describe all the networks reachable through the FWSM, the FWSM sends a default route to participating devices that identifies the FWSM as the default gateway.

  You can use the default route option with passive RIP, or alone. You might use the default route option alone if you use static routes on the FWSM, but do not want to configure static routes on downstream routers. Typically, you would not enable the default route option on the outside interface, because the FWSM is not typically the default gateway for the upstream router.

Enabling RIP

Single context mode only

Routed firewall mode only

To enable RIP on an interface, enter the following command:

```
FWSM(config)# rip interface_name {default | passive} [version {1 | 2
[authentication {text | md5} key key_id]}]
```

You can both types of RIP on an interface by entering the command two times, one for each method.

If you want to use both modes, then enter the **rip** command two times with different modes for a given interface. For example, enter the following commands:

```
FWSM(config)# rip inside default version 2 authentication md5 scorpius 1
FWSM(config)# rip inside passive version 2 authentication md5 scorpius 1
```

If you want to enable passive RIP on all interfaces, but only enable default routes on the inside interface, enter the following commands:

```
FWSM(config)# rip inside default version 2 authentication md5 scorpius 1
FWSM(config)# rip inside passive version 2 authentication md5 scorpius 1
FWSM(config)# rip outside passive version 2 authentication md5 scorpius 1
```

Note Before testing your configuration, flush the ARP caches on any routers connected to the FWSM. For Cisco routers, use the **clear arp** command to flush the ARP cache.

Configuring the DHCP Server

This section describes how to use the Dynamic Host Configuration Protocol (DHCP) server provided by the FWSM. It includes the following topics:

Enabling the DHCP Server

The FWSM can act as a DHCP server. DHCP is a protocol that supplies network settings to hosts including the host IP address, the default gateway, and a DNS server.

Note The FWSM DHCP server does not support BOOTP requests.

Note For multiple context mode, you cannot enable the DHCP server or DHCP relay on an interface that is used by more than one context (a shared VLAN).

The DHCP server can be enabled on any interface. Clients must be directly connected to the FWSM and cannot send requests through another relay agent or a router.

To enable the DHCP server on a given FWSM interface, follow these steps:

Step 1 To create a DHCP address pool, enter the following command:

```
FWSM/contexta(config)# dhcpd address ip_address-ip_address interface_name
```

The FWSM assigns a client one of the addresses from this pool to use for a given length of time. These addresses are the local untranslated addresses for the directly connected network.

The address pool must be on the same subnet as the FWSM interface.

Step 2 (Optional) To specify the IP address(es) of the DNS server(s) the client will use, enter the following command:

```
FWSM/contexta(config)# dhcpd dns dns1 [dns2]
```

You can specify up to two DNS servers.

Step 3 (Optional) To specify the IP address(es) of the WINS server(s) the client will use, enter the following command:

```
FWSM/contexta(config)# dhcpd wins wins1 [wins2]
```

You can specify up to two WINS servers.

Step 4 (Optional) To change the lease length to be granted to the client, enter the following command:

```
FWSM/contexta(config)# dhcpd lease lease_length
```

This lease equals the amount of time (in seconds) the client can use its allocated IP address before the lease expires. Enter a value between 0 to 1,048,575. The default value is 3600 seconds.

Step 5 (Optional) To configure the domain name the client uses, enter the following command:

```
FWSM/contexta(config)# dhcpd domain domain_name
```

Step 6 To enable the DHCP daemon within the FWSM to listen for DHCP client requests on the enabled interface, enter the following command:

```
FWSM/contexta(config)# dhcpd enable interface_name
```

For example, to assign the range 10.0.1.101 to 10.0.1.110 to hosts connected to the inside interface, enter the following commands:

```
FWSM/contexta(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
FWSM/contexta(config)# dhcpd dns 209.165.201.2 209.165.202.129
FWSM/contexta(config)# dhcpd wins 209.165.201.5
FWSM/contexta(config)# dhcpd lease 3000
FWSM/contexta(config)# dhcpd domain example.com
FWSM/contexta(config)# dhcpd enable inside
```

Using Cisco IP Phones with a DHCP Server

Enterprises with small branch offices that implement a Cisco IP Telephony Voice over IP (VoIP) solution typically implement Cisco CallManager at a central office to control Cisco IP Phones at small branch offices. This implementation allows centralized call processing, reduces the equipment required, and eliminates the administration of additional Cisco CallManager and other servers at branch offices.

Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, if it does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.

- DHCP option 150 provides the IP addresses of a list of TFTP servers
- DHCP option 66 gives the IP address or the host name of a single TFTP server.

Cisco IP Phones might also include DHCP option 3 in their requests, which lists the IP addresses of default routers.

Cisco IP Phones might include both option 150 and 66 in a single request. In this case, the FWSM DHCP server provides values for both options in the response if they are configured on the FWSM.

You can configure the FWSM to send information for most options listed in RFC 2132. The following table shows the syntax for any option number, as well as the syntax for commonly-used options 66,150, and 3:

- To provide information for DHCP requests that include an option number as specified in RFC-2132, enter the following command:

  ```
  FWSM/contexta(config)# dhcpd option number string
  ```

- To provide the IP address or name of a TFTP server for option 66, enter the following command:

  ```
  FWSM/contexta(config)# dhcpd option 66 ascii server_name
  ```

- To provide the IP address or names of one or two TFTP servers for option 150, enter the following command:

  ```
  FWSM/contexta(config)# dhcpd option 150 ip server_ip1 [server_ip2]
  ```

  The *server_ip1* is the IP address or name of the primary TFTP server while *server_ip2* is the IP address or name of the secondary TFTP server. A maximum of two TFTP servers can be identified using option 150.

- To provide a list of router IP addresses for option 3, enter the following command:

  ```
  FWSM/contexta(config)# dhcpd option 3 ip router_ip1 [router_ip2] [...]
  ```

Configuring DHCP Relay

Routed firewall mode only

A DHCP relay agent allows the FWSM to forward DHCP requests from clients to a router connected to a different interface.

The following restrictions apply to the use of the DHCP relay agent:

- The relay agent cannot be enabled if the DHCP server feature is also enabled.
- Clients must be directly connected to the FWSM and cannot send requests through another relay agent or a router.
- For multiple context mode, you cannot enable DHCP relay on an interface that is used by more than one context (a shared VLAN), not can the DHCP server reside on a shared VLAN.

Note DHCP relay services are not available in transparent firewall mode. However, you can allow DHCP packets through the FWSM; DHCP relay is unnecessary. To allow DHCP requests and replies through the FWSM in transparent mode, you need to configure two ACLs, one that allows DCHP requests from the inside interface to the outside, and one that allows the replies from the server in the other direction.

To enable DHCP relay, follow these steps:

Step 1 To set the IP address of a DHCP server on a different interface from the DHCP client, enter the following command:

```
FWSM/contexta(config)# dhcprelay server ip_address interface_name
```

You can use this command up to four times to identify up to four servers. The *interface_name* cannot be a shared VLAN.

Step 2 To enable DHCP relay on the interface connected to the clients, enter the following command:

```
FWSM/contexta(config)# dhcprelay enable interface_name
```

The *interface_name* cannot be a shared VLAN.

Step 3 (Optional) To set the number of seconds allowed for relay address negotiation, enter the following command:

```
FWSM/contexta(config)# dhcprelay timeout seconds
```

Step 4 (Optional) To change the first default router address in the packet sent from the DHCP server to the address of the FWSM interface, enter the following command:

```
FWSM/contexta(config)# dhcprelay setroute interface_name
```

This action allows the client to set its default route to point to the FWSM even if the DHCP server specifies a different router.

If there is no default router option in the packet, the FWSM adds one containing the interface address.

The following example enables the FWSM to forward DHCP requests from clients connected to the inside interface to a DHCP server on the outside interface:

```
FWSM/contexta(config)# dhcprelay server 201.168.200.4 outside
FWSM/contexta(config)# dhcprelay enable inside
FWSM/contexta(config)# dhcprelay setroute inside
```