OSPFv3 IPSec Authentication

Table 1: Feature History

Feature	Release Information	Description
OSPFv3 IPSec Authentication	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	OSPFv3 authentication protects OSPFv3 routing payload with IPSec encryption and hashing. The solution is based on statically configured cryptographic keys that build on top of crypto map solutions. OSPFv3 is supported on service side and transport side.

OSPFv3 IPSec authentication

OSPFv3 IPSec authentication refers to a security mechanism used in IPv6 networks where Open Shortest Path First version 3 (OSPFv3) routing protocol packets are authenticated and optionally encrypted through the IP Security (IPSec) protocol. In order to ensure that OSPFv3 packets are not altered and re-sent to the device, OSPFv3 packets must be authenticated. OSPFv3 uses the IPSec secure socket API to add authentication to OSPFv3 packets. This API supports IPv6.

Since OSPFv3 does not provide built-in authentication or encryption, IPSec is employed to ensure the integrity and confidentiality of OSPFv3 routing messages exchanged between routers. This approach helps prevent unauthorized devices from modifying or injecting routing information and protects against unauthorized packet capture and replay attacks, thereby enhancing the security of routing updates in enterprise or service provider IPv6 networks. To implement OSPFv3 IPSec authentication, you must configure IPSec security associations between participating routers, specifying appropriate authentication (such as HMAC with SHA or MD5).

To configure IPsec, you configure a security policy, which is a combination of the security policy index (SPI) and the key (the key is used to create and validate the hash value). IPsec for OSPFv3 can be configured on an interface or on an OSPFv3 area. For higher security, you should configure a different policy on each interface configured with IPsec. If you configure IPsec for an OSPFv3 area, the policy is applied to all of the interfaces in that area, except for the interfaces that have IPsec configured directly. Once IPsec is configured for OSPFv3, IPsec is invisible to you.

The secure socket API is used by applications to secure traffic. The API needs to allow the application to open, listen, and close secure sockets. The binding between the application and the secure socket layer also allows the secure socket layer to inform the application of changes to the socket, such as connection open and close events. The secure socket API is able to identify the socket; that is, it can identify the local and remote addresses, masks, ports, and protocol that carry the traffic requiring security.

Each interface has a secure socket state:

- NULL: Do not create a secure socket for the interface if authentication is configured for the area.
- DOWN: IPsec has been configured for the interface (or the area that contains the interface), but OSPFv3 either has not requested IPsec to create a secure socket for this interface, or there is an error condition.
- GOING UP: OSPFv3 has requested a secure socket from IPsec and is waiting for a CRYPTO_SS_SOCKET_UP message from IPsec.
- UP: OSPFv3 has received a CRYPTO_SS_SOCKET_UP message from IPsec.
- CLOSING: The secure socket for the interface has been closed. A new socket may be opened for the interface, in which case the current secure socket makes the transition to the DOWN state. Otherwise, the interface will become UNCONFIGURED.
- UNCONFIGURED: Authentication is not configured on the interface.

OSPFv3 will not send or accept packets while in the DOWN state.

Prerequisites for OSPFv3 IPSec authentication

Configure the IP Security (IPsec) secure socket application program interface (API) on OSPFv3 to enable authentication.

Restrictions for OSPFv3 IPSec authentication

- The OSPF for IPv6 (OSPFv3) authentication with IPSec feature is not supported on the IP BASE license package. The Advanced Enterprise Services package license must be used.
- OSPFv3 encryption is not supported.
- The OSPFv3 configuration is supported only on interface-level using configuration groups. However, both interface-level and area-level configuration is supported using CLI add-on templates.

Configure OSPFv3 IPSec authentication

Once you have configured OSPFv3 and decided on your authentication, you must define the security policy on each of the devices within the group. The security policy consists of the combination of the key and the SPI. To define a security policy, you must define an SPI and a key.

You can configure an authentication or encryption policy either on an interface or for an OSPFv3 area. When you configure for an area, the security policy is applied to all of the interfaces in the area. For higher security, use a different policy on each interface.

You can configure authentication on virtual links.

- Configure authentication on an interface
- Configure authentication in an OSPFv3 area

Configure OSPFv3 IPv4 Routing Using a Configuration Group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Transport VPN feature in a Transport and Management profile for VPN 0 or VPN 512. Create and configure a Service VPN feature in a Service profile for VPNs 1 through 511, and 513 through 65530.

Step 3 Create and configure an OSPFv3 IPV4 routing feature.

a. Configure Basic Configuration.

Table 2: Basic Configuration

Field	Description
Router ID	Enter the OSPFv3 IPv4 router ID, in decimal four-part dotted notation. This is the IP address associated with the router for OSPF adjacencies.
Reference Bandwidth (Mbps)	Specify the reference bandwidth for the OSPF auto-cost calculation for the interface. Range: 1 through 4294967 Mbps Default: 100 Mbps
RFC 1583 Compatible	By default, the OSPF calculation is done per RFC 1583. Disable this option to calculate the cost of summary routes based on RFC 2328.

Field	Description
Originate	Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear: • **Always**: Enable this option to always advertise the default route in an OSPF routing domain. • **Default Metric**: Set the metric used to generate the default route. Range: 0 through 16777214 Default: 10 • **Metric Type**: Choose to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route.
SPF Calculation Delay (milliseconds)	Specify the amount of time between when the first change to a topology is received until performing the SPF calculation. Range: 1 through 600000 milliseconds (60 seconds) Default: 200 milliseconds
Initial Hold Time (milliseconds)	Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 milliseconds (60 seconds) Default: 1000 milliseconds
Maximum Hold Time (milliseconds)	Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 Default: 10000 milliseconds (60 seconds)
Distance for External Routes	Specify the OSPF route administration distance for routes learned from other domains. Range: 1 through 255 Default: 110
Distance for Inter-Area Routes	Specify the OSPF route administration distance for routes coming from one area into another. Range: 1 through 255 Default: 110
Distance for Intra-Area Routes	Specify the OSPF route administration distance for routes within an area. Range: 0 through 255 Default: 110

b. Configure Interface.

Table 3: Interface Settings

Field	Description
Add Interface	Configure the properties of an interface. Configure the area range of an interface in an OSPFv3 area.
Name	Enter the name of the interface, in the format `geslot/port` or `loopback number`.
Cost (optional)	Specify a number for the Type 3 summary LSA. OSPF uses this metric during its SPF calculation to determine the shortest path to a destination. Range: 0 through 16777214
Authentication Type (optional)	Specify the SPI and authentication key if you use IPSec SHA1 authentication type. • **no-auth**: Select no authentication. • **ipsec-sha1**: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication.
SPI (optional)	Specifies the Security Policy Index (SPI) value. Range: 256 through 4294967295
Authentication Key (optional)	Provide a value for the authentication key. When IPSEC SHA-1 authentication is used, the key must be 40 hex digits long.
Passive Interface (optional)	Specify whether to set the OSPFv3 interface to be passive. A passive interface advertises its address, but does not actively run the OSPFv3 protocol. Default: Disabled
Add Range	Configure the area range of an interface in an OSPF area.
IP Address*	Enter the IP address.
Subnet Mask*	Enter the subnet mask.
Cost	Specify a number for the Type 3 summary LSA. OSPF uses this metric during its SPF calculation to determine the shortest path to a destination. Range: 0 through 16777214
No-advertise*	Enable this option to not advertise the Type 3 summary LSAs.

c. Configure Redistribute.

d. Configure Area Parameters.

Table 4: Area

Field	Description
Add Area	

Field	Description
Area Number*	Enter the number of the OSPF area. Range: 32-bit number
Set the area type	Choose the type of OSPF area: • Stub • NSSA

What to do next

Also see Deploy a configuration group.

Configure OSPFv3 IPv6 Routing Using a Configuration Group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Transport VPN feature in a Transport and Management profile or a Service VPN feature in a Service profile.

Step 3 Create and configure a OSPFv3 IPv6 feature.

a. Configure Basic Configuration.

Table 5: Basic Settings

Field	Description
Router ID	Enter the OSPF router ID, in decimal four-part dotted notation. This value is the IP address that is associated with the router for OSPF adjacencies. Default: No Router ID is configured.
Add Redistribute	

Field	Description
Protocol	Choose the protocol from which to redistribute routes into OSPFv3, for all OSPFv3 sessions. • **Connected** • **Static** • **BGP**
Select Route Policy	Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF.

b. Configure Area Parameters.

Table 6: Area

Field	Description
Area Number*	Enter the number of the OSPFv3 area. Allowed value: Any 32-bit integer
Area Type	Choose the type of OSPFv3 area: • **Stub**: No external routes • **NSSA**: Not-so-stubby area, allows external routes • **Normal** **Note** You can't enter a value for **Area type** if you have entered 0 as a value for **Area Number**.
Interface	
Add Interface	Configure the properties of an interface in an OSPFv3 area.
Name*	Enter the name of the interface. Examples of interface names: GigabitEthernet0/0/1, GigabitEthernet0/1/2.1, GigabitEthernet0, or Loopback1.
Cost	Specify a number for the Type 3 summary link-state advertisement (LSA). OSPFv3 uses this metric during its SPF calculation to determine the shortest path to a destination. Range: 0 through 16777215
Authentication Type	Specify the SPI and authentication key if you use IPSec SHA1. • **no-auth**: Select no authentication. • **ipsec-sha1**: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication.

Field	Description
SPI	Specifies the Security Policy Index (SPI) value. Range: 256 through 4294967295
Authentication Key	Provide a value for the authentication key. When IPSEC SHA-1 authentication is used, the key must be 40 hex digits long.
Passive Interface	Specify whether to set the OSPFv3 interface to be passive. A passive interface advertises its address, but does not actively run the OSPFv3 protocol. Default: Disabled
IPv6 Range	
Add IPv6 Range	Configure the area range of an interface in an OSPFv3 area.
Network Address*	Enter the IPv6 address.
Subnet Mask*	Enter the subnet mask.
No Advertise*	Enable this option to not advertise the Type 3 summary LSAs.
Cost	Specify the cost of the OSPFv3 interface. Range: 1 through 65535

c. Configure Advanced Parameters.

Table 7: Advanced

Field	Description
Route Policy	Enter the name of a localized control policy to apply to routes coming from OSPFv3 neighbors.
Reference Bandwidth (Mbps)	Specify the reference bandwidth for the OSPFv3 autocost calculation for the interface. Range: 1 through 4294967 Mbps Default: 100 Mbps
RFC 1583 Compatible	By default, the OSPFv3 calculation is done per RFC 1583. Disable this option to calculate the cost of summary routes based on RFC 2328.

Field	Description
Originate	Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear: • **Always**: Enable this option to always advertise the default route in an OSPF routing domain. • **Default Metric**: Set the metric used to generate the default route. Range: 0 through 16777214 Default: 10 • **Metric Type**: Choose to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route.
Distance	Define the OSPFv3 route administration distance based on route type. Default: 100
Distance for External Routes	Set the OSPFv3 distance for routes learned from other domains. Range: 0 through 255 Default: 110
Distance for Inter-Area Routes	Set the distance for routes coming from one area into another. Range: 0 through 255 Default: 110
Distance for Intra-Area Routes	Set the distance for routes within an area. Range: 0 through 255 Default: 110
SPF Calculation Timers	Configure the amount of time between when OSPFv3 detects a topology and when it runs its SPF algorithm.
SPF Calculation Delay (milliseconds)	Specify the amount of time between when the first change to a topology is received until performing the SPF calculation. Range: 1 through 600000 ms (600 seconds) Default: 200 ms
Initial Hold Time (milliseconds)	Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 1000 ms
Maximum Hold Time (milliseconds)	Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 10000 ms (10 seconds)

Field	Description
Maximum Metric (Router LSA)	Configure OSPFv3 to advertise a maximum metric so that other routers do not prefer this vEdge router as an intermediate hop in their Shortest Path First (SPF) calculation. • **Immediately**: Force the maximum metric to take effect immediately, through operator intervention. • **On-startup**: Advertise the maximum metric for the specified number of seconds after the router starts up. Range: 5 through 86400 seconds Maximum metric is disabled by default.

What to do next

Also see Deploy a configuration group.

Configure OSPFv3 IPSec authentication at an interface-level using CLI

Before you begin

Follow these steps to configure OSPFv3 IPSec authentication at an interface-level using CLI.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# config-transaction
```

Step 2 In the configuration mode, configure an interface type such as, Gigabit Ethernet.

Specifies an interface type and number, and places the device in interface configuration mode.

Example:

```
Device(config)# interface GigabitEthernet3
```

Step 3 Configure OSPFv3 authentication on the interface.

Specifies the authentication type for an interface.

Example:

```
Device(config-if)# ospfv3 authentication ipsec spi 256 sha1 0 0987654321098765432109876543210987654321
```

Configure OSPFv3 IPSec authentication at an area-level using CLI

Before you begin

Follow these steps to configure OSPFv3 IPSec authentication at an area-level.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# config-transaction
```

Step 2 Enable OSPFv3 router configuration mode.

Example:

```
Device(config)# router ospfv3 <process-id>
```

Step 3 Configure OSPFv3 authentication on the interface.

Enables authentication in an OSPFv3 area.

Example:

```
Device(config-rtr)# area <area-id> authentication ipsec spi <spi> authentication-algorithm
```

```
Device(config)# router ospfv3 <process-id>
Device(config-rtr)# area <> authentication ipsec spi <> [md5/sha1] <>
interface GigabitEthernetY/Y
ospfv3 <> [ipv4/ipv6] area <>
```

Configuration examples for IPv6 OSPFv3 IPSec authentication

You can configure OSPFv3 IPSec authentication on an interface or in an area.

Note Interface-level authentication takes priority over area-level authentication

Configuring IPv6 OSPFv3 authentication on an interface

This example shows how to define authentication on Ethernet interface 0/0:

```
interface Ethernet0/0
 ospfv3 1 ipv6 area 0
 ospfv3 1 ipv6 dead-interval 40
 ospfv3 1 ipv6 hello-interval 10
 ospfv3 1 ipv6 retransmit-interval 5
 ospfv3 authentication ipsec spi 256 sha1 0 0987654321098765432109876543210987654321
```

Configuring IPv6 OSPFv3 authentication in an area

This example shows how to define authentication on OSPFv3 area 0:

```
router ospfv3 1
 router-id 10.11.11.1
 area 0 authentication ipsec spi 256 sha1 0 0987654321098765432109876543210987654321
```