CONTENTS

OSPFv3 Encryption and Authentication

« OSPFv3 BFD (/workbook/view/service-provider-v4/task/ospfv3-bfd-MjgzNQ%3D%3D) | Single-Level IS-IS (/workbook/view/service-provider-v4/task/single-level-is-is-MjgzNw%3D%3D) »

Last updated: April 23, 2016

> **Note:**
> This task assumes that you have already completed the OSPFv3 (http://labs.ine.com/workbook/view/service-provider-v4/task/ospfv3-MjgzMg%3D%3D) task. Refer to the **Base IPv6 Diagram** in order to complete this task.

Task

- Configure OSPFv3 IPsec ESP Encryption and Authentication between XR1 and XR2 using the following parameters:
  - Use Security Parameter Index (SPI) 1920
  - Use ESP with AES 256-bit Encryption and SHA1 Authentication
  - For the AES encryption key use 0x0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef
  - For the SHA authentication key 0x0123456789012345678901234567890123456789

Configuration **Click to *collapse***

> **Note:**
> OSPFv3 IPsec ESP Encryption and Authentication is not supported in regular IOS until software release 12.4(9)T

```
XR1:
router ospfv3 1
 area 0
  interface GigabitEthernet0/0/0/0.1920
   encryption ipsec spi 1920 esp aes 256
0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef authentication
sha1 01234567890123456789012345678901234567890123456789
  !
 !
!


XR2:
router ospfv3 1
 area 0
  interface GigabitEthernet0/0/0/0.1920
   encryption ipsec spi 1920 esp aes 256
0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef authentication
sha1 01234567890123456789012345678901234567890123456789
  !
 !
!
```

Verification

XR1 and XR2 are running ESP encryption and authentication for OSPFv3 on the link connecting them, and they are OSPFv3 adjacent.

```
RP/0/0/CPU0:XR1#show ospfv3 interface GigabitEthernet0/0/0/0.1920
Thu Apr 23 18:47:36.318 UTC

GigabitEthernet0/0/0/0.1920 is up, line protocol is up, ipsec is up
  Link Local address fe80::250:56ff:fe9e:59fe, Interface ID 9
  Area 0, Process ID 1, Instance ID 0, Router ID 19.19.19.19
  Network Type BROADCAST, Cost: 1
   ESP Encryption AES-256, Authentication SHA1, SPI 1920
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 20.20.20.20, local address fe80::250:56ff:fe9e:27ac
  Backup Designated router (ID) 19.19.19.19, local address fe80::250:56ff:fe9e:59fe
  Flush timer for old DR LSA due in 00:00:33
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 0/4/1, flood queue length 0
  Next 0(0)/0(0)/0(0)
  Last flood scan length is 1, maximum is 20
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 20.20.20.20  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Reference count is 5


RP/0/0/CPU0:XR2#show ospfv3 interface GigabitEthernet0/0/0/0.1920
Thu Apr 23 18:47:57.987 UTC

GigabitEthernet0/0/0/0.1920 is up, line protocol is up, ipsec is up
  Link Local address fe80::250:56ff:fe9e:27ac, Interface ID 7
  Area 0, Process ID 1, Instance ID 0, Router ID 20.20.20.20
  Network Type BROADCAST, Cost: 1
   ESP Encryption AES-256, Authentication SHA1, SPI 1920
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 20.20.20.20, local address fe80::250:56ff:fe9e:27ac
  Backup Designated router (ID) 19.19.19.19, local address fe80::250:56ff:fe9e:59fe
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 0/2/1, flood queue length 0
  Next 0(0)/0(0)/0(0)
  Last flood scan length is 1, maximum is 14
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 19.19.19.19  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
  Reference count is 37


RP/0/0/CPU0:XR1#show ospfv3 neighbor
Thu Apr 23 18:56:49.190 UTC

Neighbors for OSPFv3 1


Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
```

```
20.20.20.20     1     FULL/DR         00:00:39    7              GigabitEthernet0/0/0/0.1920
    Neighbor is up for 00:11:38
5.5.5.5         1     FULL/  -        00:00:33    13             GigabitEthernet0/0/0/0.519
    Neighbor is up for 00:11:39
6.6.6.6         1     FULL/DR         00:00:36    14             GigabitEthernet0/0/0/0.619
    Neighbor is up for 00:11:39


Total neighbor count: 3


RP/0/0/CPU0:XR2#show ospfv3 neighbor
Thu Apr 23 18:56:26.292 UTC


Neighbors for OSPFv3 1


Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
19.19.19.19     1     FULL/BDR        00:00:38    9              GigabitEthernet0/0/0/0.1920
    Neighbor is up for 00:11:15


Total neighbor count: 1
```

Notice that one hop IPSec tunnels have been created between XR1 and XR2. The IPSec tunnel is encrypting the OSPFv3 traffic. The transform set is using AES 256 bit with SHA1 for hashing. The SA type is shown as manual, as all the keys were entered manually (no ISAKAMP stage).

```
RP/0/0/CPU0:XR1#show crypto ipsec sa
Thu Apr 23 18:58:30.933 UTC


SA id:          2
Node id:        0/0/CPU0
SA Type:        MANUAL
SA State:       UP
Ref Count:      1
outbound esp sas:
         spi: 0x780(1920)
         transform: esp-256-aes esp-sha-hmac
        in use settings = Transport
        no sa timing
        sa DPD disabled
        sa anti-replay (HW accel): Disable, window 0
inbound esp sas:
         spi: 0x780(1920)
         transform: esp-256-aes esp-sha-hmac
        in use settings = Transport
        no sa timing
        sa DPD disabled
        sa anti-replay (HW accel): Disable, window 0
```

« OSPFv3 BFD (/workbook/view/service-provider-v4/task/ospfv3-bfd-MjgzNQ%3D%3D) | Single-Level IS-IS (/workbook/view/service-provider-v4/task/single-level-is-is-MjgzNw%3D%3D) »