IPv6 Lab - Securing IS-IS

IS-IS neighbour authentication

Remove the packet filters from the previous examples

We need IS-IS and BGP to work for the remainder of the lab, so we will remove the packet filters we installed in the previous exercise. Simply go to the interfaces where you defined the “traffic-filter” commands and remove those. Also delete the “ipv6 access-list” configurations for these two traffic filters

Configuring Neighbour Security for IS-IS

Network operators consider it more and more important to turn on neighbour authentication inside their networks as attacks on infrastructure increase and operators seek to use all available tools to secure their networks.

IS-IS supports neighbour authentication. This is quite important inside discrete networks to prevent the introduction of improperly configured or unintended equipment.

Each router team will turn on authentication for IS-IS. This first step will create the key-chain to be used for the authentication.

An example configuration might be:

```
key chain asX0-key
 key 1
  key-string cisco
```

We will just use *cisco* as the key-string - clearly we do not do this on a public operational network, but instead choose something more obscure.

Note: the *key-chain* allows up to 255 keys to be set, potential a different one per interface. It is generally not recommended to set more than one per interface, as the router will try and communicate with its neighbours using all keys. If a key needs to be upgraded, common practice then is to set a second key, allowing a graceful changeover without compromising the functioning of the network. Once all the routers on the network are using the new key, the old one should be removed.

Neighbour Authentication - Part 2

Now that the key chain has been set up, the second step is to actually enable neighbour authentication for IS-IS.

An example configuration for the Core Router might be:

```
router isis asX0
 authentication mode md5 level-2
 authentication key-chain asX0-key level-2
```

Notice now that the IS-IS adjacencies do not come up unless the neighbouring router has also entered the same configuration and key. Notice also how the IS-IS adjacencies were reset soon after the configuration was entered.

Also notice that the neighbour authentication for IS-IS is independent of which protocol/topology is being used.

Check IS-IS operation

Use the various "*show isis*" commands to see the IS-IS status of the lab network now. Check the routing and the routing table. If you are missing any adjacencies, work with your neighbouring routers in your AS to work out why, and what might have gone wrong with the neighbour authentication.

Footnote: OSPF neighbour authentication

Neighbour authentication for OSPF is a little more complex than it is for IS-IS. First off, OSPFv2 only supports IPv4 adjacencies and prefixes, while OSPFv3 is used for IPv6.

We are not using OSPF in this lab, so the following is provided for your information only. Please do not configure the examples given below!

OSPFv2

If we were using OSPF for this lab, the configuration would look something like this on the core router:

```
router ospf X0
 area 0 authentication message-digest
!
interface fastethernet 0/0
 ip ospf message-digest-key 1 md5 cisco
!
interface gigabit 1/0
 ip ospf message-digest-key 1 md5 cisco
!
interface gigabit 2/0
 ip ospf message-digest-key 1 md5 cisco
```

Notice that this sets up the area to use neighbour authentication, and then applies the authentication key to each interface in turn.

OSPFv3

Neighbour authentication for OSPFv3 is no longer built in as it is for OSPFv2, but relies on the IPSEC authentication header support built into IPv6.

The configuration for the core router would look something like this:

```
ipv6 router ospf X0
 area 0 authentication ipsec spi 256 md5 0123456789ABCDEF0123456789ABCDEF
!
```

Note also that we don't need to apply any authentication per interface, as the key has been applied to the entire area. Each interface in area 0 needs to have the correct key to set up the adjacency.

Back to Agenda page

From:
https://bgp4all.com/pfs/ - **Philip Smith's Internet Development Site**

Permanent link:
https://bgp4all.com/pfs/training/apnic-ipv6-nc/5-securing-isis?rev=1521452245

Last update: **2018/03/19 09:37**