How to configure IPsec Authentication for OSPFv3

This series of technical tips are created to provide step by step guidelines for everyday tasks. Most ‘How To Guides’ are written with the assumption that the user (you) can get connected to the device in question and that in most cases the device is up and operational. You just need to perform a certain task that would be considered complex without the assistance of an experienced guide (me).

In this guide I describe how to configure IPsec authentication for OSPFv3.

Background

Attackers can send forged protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which can degrade the functionality of the router. To prevent such attacks, we must ensure that routers form routing protocol peering or neighboring relationships only with trusted peers. One way to do this is by authenticating routing protocol messages. JUNOS supports HMAC-MDS authentication for BGP, IS-IS, OSPF, RIP, and RSVP protocols. HMAC-MDS authentication uses a secret key combined with the data being protected to compute a hash. When the protocols send messages, the computed hash is transmitted with the data. The receiver uses the matching key to validate the message hash.

JUNOS supports the IPsec security suite for both IPv4 and IPv6. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. JUNOS also supports IKE, which defines mechanisms for key generation and exchange, and manages SAs.

IPv6 has, using the Authentication extension header, a standard authentication procedure using IPsec security associations (SA). Because of this, OSPFv3 has no need for its own authentication of OSPFv3 packets; it just uses IPv6 authentication.

From the Juniper “Routing Protocols Configuration Guide”:

OSPF version 3 (OSPFv3) provides a method for protecting and securing the OSPF traffic through the router. OSPFv3 uses the IP Authentication Header (AH) and the IP Encapsulating Security Payload (ESP) to authenticate routing information.

Use ESP with NULL encryption to provide authentication to the OSPFv3 protocol headers only. Use AH to provide authentication to the OSPFv3 protocol headers, portions of the IPv6 header, and portions of the extension headers. Use ESP with non-NULL encryption for full confidentiality.
OSPFv3 authentication uses static keyed IP security protocol (IPsec) security associations (SAs) similar to BGP IPsec. Tunnel mode SAs and dynamic IPsec SAs using Internet Key Exchange (IKE) authentication are not supported. Dynamic keyed IPsec SAs run on the Routing Engine and do not require a services PIC.

OSPFv3 authentication is a two-step process: Configure authentication on the interface referencing the IPsec security association name; and creating the IPsec SA.

**Procedure**

Step 1: You specify the IPsec authentication name by including the `name` option at the `[edit protocols ospf3 area area-id interface interface-name ipsec-sa name]` hierarchy. You configure the actual IPsec authentication separately.

```plaintext
protocols {
    ospf3 {
        area 0.0.0.0 {
            interface ge-0/1/0.0 {
                interface-type p2p;
                ipsec-sa sa-proteus;
            }
            interface ge-0/2/0.0 {
                interface-type p2p;
                ipsec-sa sa-proteus;
            }
            interface ge-0/0/3.0 {
                interface-type p2p;
                ipsec-sa sa-proteus;
            }
        }
    }
}
```

Step 2: Configure the IPsec SA at the `[edit security ipsec]` hierarchy using the `set security-association name` command. Only manual keyed (aka static) IPsec SAs are supported. Specify the mode as transport; the direction should be bidirectional; the protocol either ah or esp; and the `spi-value` is an arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet) with a range: 256 through 16639.

Both hmac-md5-96 (128-bit digest) and hmac-sha1-96 (160-bit digest) authentication is supported. The key is either an ASCII text or hexadecimal string. For hmac-md5-96, the key must be 16 ASCII characters;
for hmac-sha1-96, the key must be 20 ASCII characters. The hexadecimal key for hmac-md5-96 must be 32 hexadecimal characters; for hmac-sha1-96, 40 hexadecimal characters.

```
security {
    ipsec {
        security-association sa-proteus {
            mode transport;
            manual {
                direction bidirectional {
                    protocol ah;
                    spi 7127;
                    authentication {
                        algorithm hmac-md5-96;
                        key ascii-text "$9$e2CM7VYgojHmDiu1ESMWUjH.5Fm/CAu13nyK8X-dHq.FFuO1"; ## SECRET-DATA
                    }
                }
            }
        }
    }
}
```

**Conclusion**

These procedures are meant to walk an administrator through a process that might seem very complex and error prone. Hopefully these steps will break that task apart and simplify the operation. If you find a better way of doing this task, please send an e-mail to john@proteus.net and share your results.