Configuring BFD Authentication for OSPF

Beginning with JUNOS Release 9.6, you can configure authentication for BFD sessions running over OSPFv2. Routing instances are also supported. Only three steps are needed to configure authentication on a BFD session:

1. Specify the BFD authentication algorithm for the OSPFv2 protocol.
2. Associate the authentication keychain with the OSPFv2 protocol.
3. Configure the related security authentication keychain.

The following sections provide instructions for configuring and viewing BFD authentication on OSPF:

Configuring BFD Authentication Parameters

To configure BFD authentication:

1. Specify the algorithm (keyed-md5, keyed-sha-1, meticulous-keyed-md5, meticulous-keyed-sha-1, or simple-password) to use for BFD authentication on an OSPF route or routing instance.

   ```
   [edit]
   user@host# set protocols ospf interface if2-ospf bfd-liveness-detection
      authentication algorithm keyed-sha-1
   ```

NOTE: Nonstop active routing (NSR) is not supported with meticulous-keyed-md5 and meticulous-keyed-sha-1 authentication algorithms. BFD sessions using these algorithms may go down after a switchover.

2. Specify the keychain to be used to associate BFD sessions on the specified OSPF route or routing instance with the unique security authentication keychain attributes. This should match the keychain name configured at the [edit security authentication key-chains] hierarchy level.

   ```
   [edit]
   user@host# set protocols ospf interface if2-ospf bfd-liveness-detection
      authentication keychain bfd-ospf
   ```

NOTE: The algorithm and keychain must be configured on both ends of the BFD session, and they must match. Any mismatch in configuration prevents the BFD session from being created.

3. Specify the unique security authentication information for BFD sessions:

- The matching *key-chain-name* as specified in step 2.
- At least one *key*, a unique integer between 0 and 63. Creating multiple keys allows multiple clients to use the BFD session.
- The *secret-data* used to allow access to the session.
- The time at which the authentication key becomes active, *yyyy-mm-dd.hh:mm:ss*.

```
[edit security]
user@host# authentication-key-chains key-chain bfd-ospf key 53 secret
   $9$ggaJDmPQ6/tJgF/AtREVsyPsnCtUHm start-time 2009-06-14.10:00:00
```

4. (Optional) Specify loose authentication checking if you are transitioning from nonauthenticated sessions to authenticated sessions.

```
[edit]
user@host> set protocols ospf interface if2-ospf bfd-liveness-detection
   authentication loose-check
```

5. (Optional) View your configuration using the show bfd session detail or show bfd session extensive command.
6. Repeat these steps to configure the other end of the BFD session.

NOTE: BFD authentication is only supported in the domestic image and is not available in the export image.

Viewing Authentication Information for BFD Sessions

You can view the existing BFD authentication configuration using the show bfd session detail and show bfd session extensive commands.

The following example shows BFD authentication configured for the if2-ospf BGP group. It specifies the keyed SHA-1 authentication algorithm and a keychain name of bfd-ospf. The authentication keychain is configured with two keys. Key 1 contains the secret data "9ggaJDmPQ6/tJgF/AtREVsyPsnCtUHm" and a start time of June 1, 2009, at 9:46:02 AM PST. Key 2 contains the secret data "9a5jiKW9I.reP38ny.TszF2/9" and a start time of June 1, 2009, at 3:29:20 PM PST.

```
[edit protocols ospf]
interface if2–ospf {
   bfd-liveness-detection {
      authentication {
         algorithm keyed-sha-1;
         key-chain bfd-ospf;
      }
   }
}
[edit security]
authentication key-chains {
```

```
    key-chain bfd-ospf {
      key 1 {
        secret "$9$ggaJDmPQ6/tJgF/AtREVsyPsnCtUHm";
        start-time "2009-6-1.09:46:02 -0700";
      }
      key 2 {
        secret "$9$a5jiKW9I.reP38ny.TszF2/9";
        start-time "2009-6-1.15:29:20 -0700";
      }
    }
  }
```

If you commit these updates to your configuration, you would see output similar to the following. In the output for the show bfd sessions detail command, Authenticate is displayed to indicate that BFD authentication is configured. For more information about the configuration, use the show bfd sessions extensive command. The output for this command provides the keychain name, the authentication algorithm and mode for each client in the session, and the overall BFD authentication configuration status, keychain name, and authentication algorithm and mode.

show bfd sessions detail

```
user@host# show bfd session detail

                                                  Detect   Transmit
Address                 State     Interface       Time     Interval  Multiplier
10.9.1.33               Up        so-7/1/0.0       0.600     0.200      3
  Client OSPF, TX interval 0.200, RX interval 0.200, multiplier 3, Authenticate
  Session up time 3d 00:34
  Local diagnostic None, remote diagnostic None
  Remote state Up, version 1
  Replicated

1 sessions, 1 clients
Cumulative transmit rate 10.0 pps, cumulative receive rate 10.0 pps
```

show bfd sessions extensive

```
user@host# show bfd session extensive
                                                  Detect   Transmit
Address                 State     Interface       Time     Interval  Multiplier
10.9.1.33               Up        so-7/1/0.0       0.600     0.200      3
  Client OSPF, TX interval 0.200, RX interval 0.200, multiplier 3, Authenticate

       keychain bfd-ospf, algo keyed-md5, mode loose

  Session up time 3d 00:34
  Local diagnostic None, remote diagnostic None
  Remote state Up, version 1
  Replicated
  Min async interval 0.200, min slow interval 1.000
  Adaptive async tx interval 0.200, rx interval 0.200
  Local min tx interval 0.200, min rx interval 0.200, multiplier 3
  Remote min tx interval 0.100, min rx interval 0.100, multiplier 3
  Threshold transmission interval 0.000, Threshold for detection time 0.000
  Local discriminator 11, remote discriminator 80
  Echo mode disabled/inactive
 Authentication enabled/active, keychain bfd-ospf, algo keyed-sha-1, mode strict

1 sessions, 1 clients
Cumulative transmit rate 10.0 pps, cumulative receive rate 10.0 pps
```

Related Topics

- Overview of BFD Authentication for OSPF
- bfd-liveness-detection statement
- authentication-key-chains statement in the *JUNOS System Basics Configuration Guide*
- show bfd session command in the *JUNOS Routing Protocols and Policies Command Reference*
- Configuring BFD for OSPF

Published: 2010-04-14