Redundant IPSec Tunnel Fail-over

This chapter describes the redundant IPSec tunnel fail-over feature and dead peer detection (DPD).

The following topics are discussed:

Redundant IPSec Tunnel Fail-over (IKEv1)

Overview

The Redundant IPSec Tunnel Fail-Over functionality is included with the IPSec feature license and allows the configuration of a secondary ISAKMP crypto map-based IPSec tunnel over which traffic is routed in the event that the primary ISAKMP crypto map-based tunnel cannot be used.

This feature introduces the concept of crypto (tunnel) groups when using IPSec tunnels for access to packet data networks (PDNs). A crypto group consists of two configured ISAKMP crypto maps. Each crypto map defines the IPSec policy for a tunnel. In the crypto group, one tunnel serves as the primary, the other as the secondary (redundant). Note that the method in which the system determines to encrypt user data in an IPSec tunnel remains unchanged.

Group tunnels are perpetually maintained with IPSec Dead Peer Detection (DPD) packets exchanged with the peer security gateway.

Important The peer security gateway must support RFC 3706 in order for this functionality to work properly.

When the system determines that incoming user data traffic must be routed over one of the tunnels in a group, the system automatically uses the primary tunnel until either the peer is unreachable (the IPSec DPD packets cease), or the IPSec tunnel fails to re-key. If the primary peer becomes unreachable, the system automatically begins to switch user traffic to the secondary tunnel. The system can be configured to either automatically switch user traffic back to the primary tunnel once the corresponding peer security gateway is reachable and the tunnel is configured, or require manual intervention to do so.

This functionality also supports the generation of Simple Network Management Protocol (SNMP) notifications indicating the following conditions:

- **Primary Tunnel is down.** A primary tunnel that was previously "up" is now "down" representing an error condition.
- **Primary Tunnel is up.** A primary tunnel that was previously "down" is now "up".
- **Secondary tunnel is down.** A secondary tunnel that was previously "up" is now "down" representing an error condition.
- **Secondary Tunnel is up.** A secondary tunnel that was previously "down" is now "up".
- **Fail-over successful.** The switchover of user traffic was successful. This is generated for both primary-to-secondary and secondary-to-primary switchovers.
- **Unsuccessful fail-over.** An error occurred when switching user traffic from either the primary to secondary tunnel or the secondary to primary tunnel.

Supported RFC Standard

The Redundant IPSec Tunnel Fail-over feature supports.RFC 3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, February 2004

Redundant IPSec Tunnel Fail-over Configuration

This section provides information and instructions for configuring the Redundant IPSec Tunnel Fail-over feature. These instructions assume that the system was previously configured to support subscriber data sessions either as a core service or an HA.

Important Parameters configured using this procedure must be configured in the same StarOS context.

Important StarOS supports a maximum of 32 crypto groups per context. However, configuring crypto groups to use the same loopback interface for secondary IPSec tunnels is not recommended and may compromise redundancy on the chassis.

Important This section provides the minimum instruction set for configuring crypto groups on the system. For more information on commands that configure additional parameters and options, refer *Command Line Interface Reference*.

To configure the Crypto group to support IPSec:

Step 1 Configure a crypto group by following the steps in Configuring a Crypto Group, on page 3.

Step 2 Configure one or more ISAKMP policies according to the instructions provided in the *ISAKMP Policy Configuration* chapter of this guide.

Step 3 Configure IPSec DPD settings using the instructions provided in Configuring DPD for a Crypto Group, on page 5.

Step 4 Configure an ISAKMP crypto map for the primary and secondary tunnel according to the instructions provided in the *ISAKMP Crypto Map Configuration* section of the *Crypto Maps* chapter of this guide.

Step 5 Match the existing ISAKMP crypto map to Crypto group by following the steps in Modifying a ISAKMP Crypto Map Configuration to Match a Crypto Group, on page 3.

Step 6 Verify your Crypto Group configuration by following the steps in Verifying the Crypto Group Configuration, on page 4.

Step 7 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring a Crypto Group

Use the following example to configure a crypto group on your system for redundant IPSec tunnel fail-over support:

```
configure
  context ctxt_name
    ikev1 keepalive dpd interval dur timeout dur num-retry retries
    crypto-group group_name
      match address acl_name [ preference ]
      match ip pool pool-name pool_name
      switchover auto [ do-not-revert ]
      end
```

Important The **match ip pool** command is not supported within a crypto group on the ASR 5500 platform.

Notes:

- *ctxt_name* is the destination context where the Crypto Group is to be configured.
- *group_name* is name of the Crypto group you want to configure for IPSec tunnel failover support.
- *acl_name* is name of the pre-configured crypto ACL. It is used for configurations not implementing the IPSec Tunnel Failover feature and match the crypto map to a previously defined crypto ACL. For more information on crypto ACL, refer to the Access Control chapter of this guide.
- *pool_name* is the name of an existing IP pool that should be matched.

Modifying a ISAKMP Crypto Map Configuration to Match a Crypto Group

Use the following example to match the crypto group with ISAKMP crypto map:

```
configure
  context ctxt_name
    crypto map map_name1 ipsec-isakmp
      match crypto-group group_name primary
      end
configure
```

```
context ctxt_name
   crypto map map_name2 ipsec-isakmp
      match crypto-group group_name seondary
      end
```

Notes:

- *ctxt_name* is the system context in which you wish to create and configure the ISAKMP crypto maps.
- *group_name* is name of the Crypto group configured in the same context for IPSec Tunnel Failover feature.
- *map_name1* is name of the preconfigured ISAKMP crypto map to match with crypto group as primary.
- *map_name2* is name of the preconfigured ISAKMP crypto map to match with crypto group as secondary.

Verifying the Crypto Group Configuration

Enter the following Exec mode command for the appropriate context to display and verify your crypto group configuration:

show crypto group [summary | name *group_name* **]**

The output of this command is a concise listing of crypto group parameter settings configured on the system.

Dead Peer Detection (DPD) Configuration

This section provides instructions for configuring the Dead Peer Detection (DPD).

Defined by RFC 3706, Dead Peer Detection (DPD) is used to simplify the messaging required to verify communication between peers and tunnel availability.

DPD is configured at the context level and is used in support of the IPSec Tunnel Failover feature (refer to the Redundant IPSec Tunnel Fail-Over section) and/or to help prevent tunnel state mismatches between an FA and HA when IPSec is used for Mobile IP applications. When used with Mobile IP applications, DPD ensures the availability of tunnels between the FA and HA. (Note that the starIPSECDynTunUp and starIPSECDynTunDown SNMP traps are triggered to indicate tunnel state for the Mobile IP scenario.)

Regardless of the application, DPD must be supported/configured on both security peers. If the system is configured with DPD but it is communicating with a peer that does not have DPD configured, IPSec tunnels still come up. However, the only indication that the remote peer does not support DPD exists in the output of the **show crypto isakmp security-associations summary** command.

Important If DPD is enabled while IPSec tunnels are up, it will not take affect until all of the tunnels are cleared.

Important DPD must be configured in the same StarOS context as other IPSec Parameters.

To configure the Crypto group to support IPSec:

Step 1 Enable dead peer detection on system in support of the IPSec Tunnel Failover feature by following the steps in Configuring DPD for a Crypto Group, on page 5.

Step 2 Verify your DPD configuration by following the steps in Verifying the DPD Configuration, on page 5

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring DPD for a Crypto Group

Use the following example to configure a crypto group on your system for redundant IPSec tunnel fail-over support:

```
configure
  context ctxt_name
    ikev1 keepalive dpd interval dur timeout dur num-retry retries
    end
```

Notes:

- *ctxt_name* is the destination context where the Crypto Group is to be configured.

Verifying the DPD Configuration

Enter the following Exec mode command for the appropriate context to display and verify your crypto group with DPD configuration:

```
show crypto group [ summary | name group_name ]
```

The output of this command is a concise listing of crypto group parameter settings configured on the system.