IP/GRE Termination

In This Chapter

This section describes advanced IP/GRE termination configurations.

Topics in this section include:

- Applicability on page 1470
- Summary on page 1471
- Overview on page 1472
- Configuration on page 1475
- Conclusion on page 1497

Applicability

This note is applicable only to 7750 SR-7 and SR-12 systems and was tested on release 9.0R8. IP/GRE tunnel termination requires an MS-ISA equipped on IOM2-20g or IOM3-XP. IP/GRE is not supported in a 7450 ESS (even with mixed mode) or 7710 SR chassis. Also it is not supported by the MS-ISA-E (the non-encrypted version of the MS-ISA).

Note: The following syntax changes were introduced in release 10.0R8 with the support for IP-in-IP tunneling:

1. The definition for a GRE tunnel before 10.0R8 was:

```
interface "int-gre-tunnel" tunnel create
    sap tunnel-1.private:1 create
        gre-tunnel "gre-tunnel-1" to 10.0.0.2 create
```

From 10.0R8 onward, the **gre-tunnel** parameter has been replaced by the **ip-tunnel** parameter together with a sub-parameter **gre-header** to identify this to be a GRE tunnel. In addition, the **to** *ip-address* parameter has been deprecated and replaced with the sub-parameter **dest-ip**.

The above configuration becomes:

```
interface "int-gre-tunnel" tunnel create
   sap tunnel-1.private:1 create
       ip-tunnel "gre-tunnel-1" create
           dest-ip 10.0.0.2
           gre-header
```

2. The **show gre tunnel** command has been replaced by the **show ip tunnel** command.

Summary

The 7x50 previously only supported GRE SDP tunnels which use pseudowire encapsulation. Starting with SR-OS 8.0R5, the 7750 SR-7 and SR-12 support tunneling IPv4 packets in an IPv4 GRE tunnel. A common use case is remote access to a VPRN over a public IP network because IP/GRE tunneling allows encapsulated packets to follow a path based on the outer IP header which is useful when the inner IP packet cannot or should not be forwarded natively over this path.

This section provides configuration and troubleshooting commands for IP/GRE termination.

Overview

Generic Routing Encapsulation (GRE) allows packets of one protocol, the payload protocol, to be encapsulated by packets of another protocol called the delivery protocol. A GRE packet has an Outer Delivery Header, GRE Header and Payload Packet (Figure 230).

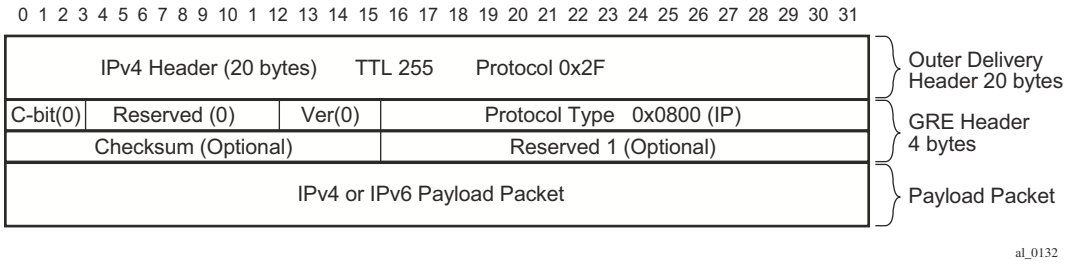

Figure 230: GRE Packet Format

The following information discusses the outer delivery and GRE header for outgoing traffic.

- Outer Delivery header
  - → The source address in the IPv4 delivery header is the configured source address.
  - → The destination address in the IPv4 delivery header is the configured remote-ip (or backup-remote-ip) address.
  - → The IP protocol value in the IPv4 delivery header is 0x02F or 47 (GRE).
  - → The DSCP in the IPv4 Outer Delivery header is:
    - – Set to the value configured for the tunnel.
    - – Otherwise, the DSCP value from the Payload Packet is copied into the Outer Delivery header.
  - → The TTL in the IPv4 Outer Delivery header is set to 255.
- GRE Header
  - → The Checksum (C) bit in the GRE header is set to 0 (no checksum present).
  - → The version in the GRE header is 0.
  - → The protocol type in the GRE header is 0x0800 for IPv4.

The following information discusses the outer delivery and GRE header for incoming traffic:

- Outer Delivery header
  - → If the packet is a fragment (More Fragments=1, non-zero fragment offset), it is dropped.
  - → If the Checksum (C) bit in the GRE header is set then the included checksum is validated; if the checksum is incorrect, the packet is discarded.
  - → If the version in the GRE header is not 0 the packet is discarded.
  - → If the source/destination address pair in the IPv4 delivery header is any other combination the packet is dropped.
- GRE Header
  - → If the Checksum (C) bit in the GRE header is set then the included checksum is validated; if the checksum is incorrect the packet is discarded.
  - → If the version in the GRE header is not 0 the packet is discarded.

7750 SR-12/SR-7 Implementation

Encapsulation, de-encapsulation and other datapath operations related to IP/GRE are handled by the isa-tunnel MDA.

Note that for GRE tunnels configured as SDPs (which are not covered by this section), no isa-tunnel MDA is required.

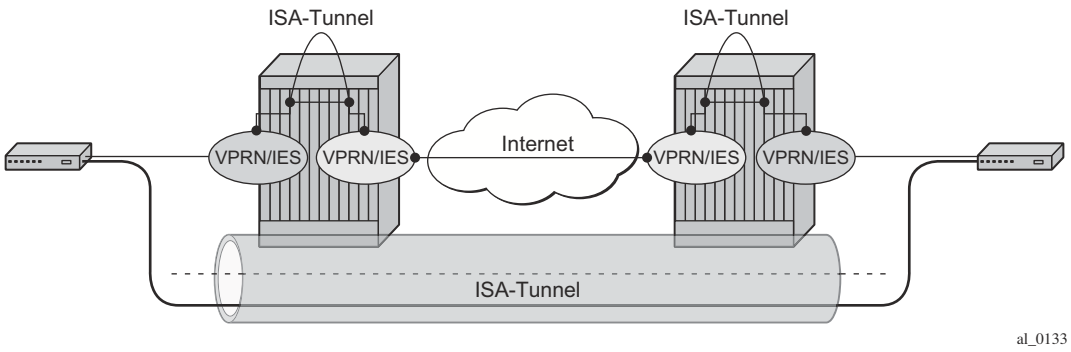

Figure 231: 7x50 Implementation

From SR-OS 8.0R5, the 7750 SR-7 and SR-12 supports the IP/GRE tunnels with static routes and BGP only. IPv6, BFD, OSPF, IS-IS, RIP and multicast are not supported.

From SR-OS 9.0R1, IP/GRE tunnels have been enhanced by adding the support of OSPFv2 and BFD on private tunnel interfaces (used with static routes, OSPFv2 or BGP) and GRE protection by tunneling into an IPSec tunnel.

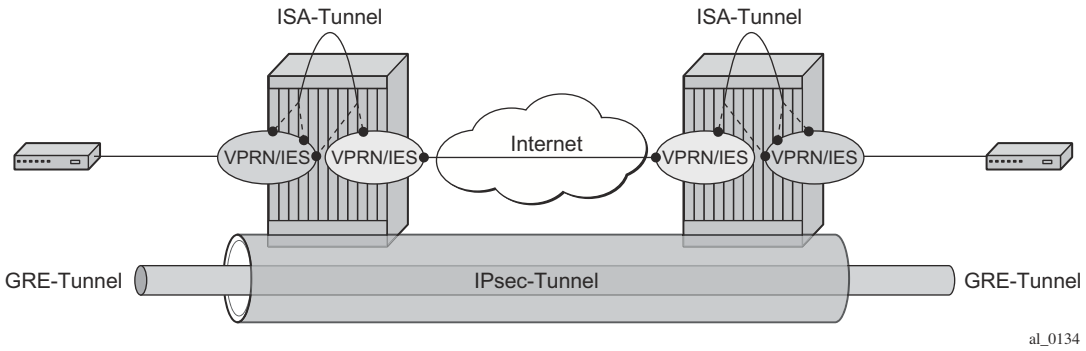

Figure 232: IP/GRE over IPSec Tunnel

Configuration

Tunnel ISA MDA

From SR-OS 8.0 R5, the isa-tunnel MDA supports IP/GRE and IPSec tunnels.

```
*A:PE-1#configure card 1 mda 1 mda-type "isa-tunnel"
```

To check the MDA configuration:

```
*A:PE-1# show mda
===============================================================
MDA Summary
===============================================================
Slot  Mda   Provisioned   Equipped   Admin    Operational
            Mda-type      Mda-type   State    State
---------------------------------------------------------------
snip-
 1     2     isa-tunnel      isa-ms     up       up
```

Tunnel Groups and Tunnel Group Restrictions

The first step of the GRE tunnel configuration is to configure a tunnel-group.

```
*A:PE-1# configure isa tunnel-group ?
  - tunnel-group <tunnel-group-id> [create]
  - no tunnel-group <tunnel-group-id>

 <tunnel-group-id>    : [1..16]
 <create>             : keyword - mandatory while creating an entry.
```

Chassis-mode B or higher is required.

```
*A:PE-11# configure isa tunnel-group 1 create
MINOR: IPSECGRPMGR #1008 Chassis mode B or higher is required
```

A tunnel group can have one tunnel-ISA designated primary and optionally one tunnel-ISA designated backup. When a GRE tunnel is created it is assigned to the primary tunnel-ISA in its tunnel group. If the primary tunnel-ISA fails, the backup tunnel-ISA (if not already claimed by another tunnel-group) takes over for the failed card.

```
*A:PE-1>config>isa>tunnel-grp#
 [no] backup          - Configure ISA-Tunnel-Group backup ISA
 [no] description     - Configure the ISA group description
 [no] primary         - Configure ISA-Tunnel-Group primary ISA
 [no] shutdown        - Administratively enable/disable an ISA-Tunnel-Group
```

```
A:PE-1>config>isa# info
----------------------------------------------
        tunnel-group 1 create
            primary 1/2
            backup 2/1
            no shutdown
        exit
----------------------------------------------
```

The failed tunnels are re-established using a cold-standby on the backup tunnel-ISA (cold standby means the backup tunnel-ISA has no state or configuration information about the tunnels prior to the failure).

A tunnel-ISA cannot be primary for more than one tunnel group.

```
*A:PE-1>config>isa>tunnel-grp# primary 1/2
MINOR: IPSECGRPMGR #1003 The specified MDA is primary in another Tunnel Group
```

A tunnel-ISA cannot be primary in one tunnel group and backup in another tunnel group.

```
*A:PE-1>config>isa>tunnel-grp# backup 1/2
MINOR: IPSECGRPMGR #1003 The specified MDA is primary in another Tunnel Group
```

To check the isa tunnel-group:

```
*A:PE-1# show isa tunnel-group
===============================================================
ISA Tunnel Groups
===============================================================
Tunnel    PrimaryIsa   BackupIsa   ActiveIsa  Admin   Oper
GroupId                                       State   State
---------------------------------------------------------------
1         1/2          2/1         1/2        Up      Up
```

To check the number of the GRE tunnels:

```
*A:PE-1# show gre tunnel count
-----------------------------
GRE Tunnels: 1
```

To check all gre-tunnels:

```
*A:PE-1# show gre tunnel
===============================================================================
GRE Tunnels
===============================================================================
TunnelName                      LocalAddress     SvcId       Admn
 SapId                           RemoteAddress    DlvrySvcId  Oper
  To                              Bkup RemAddr     DSCP        Oper Rem Addr
-------------------------------------------------------------------------------
gre-tunnel-1                    192.168.1.1      1           Up
```

```
 tunnel-1.private:1               192.168.0.1      2           Up
  10.0.0.2                                          None        192.168.0.1
protected-gre-tunnel             192.168.4.1      3           Up
 tunnel-1.private:5               192.168.3.1      3           Up
  10.0.0.5                                          None        192.168.3.1
-------------------------------------------------------------------------------
GRE Tunnels: 2
===============================================================================
```

To check the detailed tunnel information:

```
*A:PE-1# show gre tunnel "gre-tunnel-1"
===============================================================================
GRE Tunnel Configuration Detail
===============================================================================
Service Id       : 1                    Sap Id           : tunnel-1.private:1
Tunnel Name      : gre-tunnel-1
Description      : None
Target Address   : 10.0.0.2             Delivery Service : 2
Admin State      : Up                   Oper State       : Up
Source Address   : 192.168.1.1          Oper Remote Addr : 192.168.0.1
Remote Address   : 192.168.0.1          Backup Address   :
DSCP             : None
Oper Flags       : None

===============================================================================
GRE Tunnel Statistics: gre-tunnel-1
===============================================================================
Errors Rx        : 0                    Errors Tx        : 0
Pkts Rx          : 7                    Pkts Tx          : 7
Bytes Rx         : 532                  Bytes Tx         : 364
Key Ignored Rx   : 0                    Too Big Tx       : 0
Seq Ignored Rx   : 0
Vers Unsup. Rx   : 0
Invalid Chksum Rx: 0
Loops Rx         : 0
```

Interfaces

The interface toward the Internet (or WAN):

- Can be a network interface or VPRN/IES interface.
- Provide IP reachability.

The tunnel public interface:

- Can be an IES or VPRN interface.
- Represents the public side of the tunnel-ISA.

The delivery VPRN/IES service (the service connected to the Internet) must have at least one IP interface associated with a public tunnel SAP in order to receive and process GRE encapsulated packets.

The public tunnel SAP type has the format **tunnel-***id*.**private**|**public**:*tag* (where the *id* corresponds to the tunnel group) as shown in the following example.

```
*A:PE-1>config>service>ies>if# sap ?

  tunnel-id      - tunnel-<id>.<private|public>:<tag>

*A:PE-1>config>service>ies# info
----------------------------------------------
           interface "int-tunnel-public" create
                address 192.168.1.2/30
                tos-marking-state untrusted
                sap tunnel-1.public:1 create
                exit
            exit
            no shutdown
```

Mask /32 is not supported on the public tunnel.

```
*A:PE-1>config>service>ies# interface "tunnel-public" sap tunnel-1.public:1 create
INFO: PIP #1288 Cannot bind when there are /32 or /128 addresses configured
```

The tunnel private interface:

- Can be an IES or VPRN interface.
- Represents the private side of the tunnel-ISA.

The private tunnel SAP has the format **tunnel-***id*.**private**|**public**:*tag* (where the *id* corresponds to the tunnel-group) as shown in the following CLI example where an unprotected GRE tunnel is configured under the SAP.

```
*A:PE-1>config>service>vprn>if# sap ?

  tunnel-id      - tunnel-<id>.<private|public>:<tag>



*A:PE-1>config>service>vprn# info
----------------------------------------------------------------
 ---snip--
            interface "int-gre-tunnel" tunnel create
                address 10.0.0.1/30
                ip-mtu 1476
                bfd 100 receive 100 multiplier 3
                sap tunnel-1.private:1 create
                    gre-tunnel "gre-tunnel-1" to 10.0.0.2 create
---snip---
```

It is not mandatory to have the same tag (internal dot1q) in private and public GRE tunnels.

```
sap tunnel-1.private:1 <=> sap tunnel-1.public:2
```

Unprotected GRE Tunnel Configuration

To associate an unprotected GRE tunnel with a private tunnel SAP the **gre-tunnel** command is configured under the SAP context.

```
*A:PE-1>config>service>vprn# info
----------------------------------------------------------------
---snip--
            interface "gre-tunnel" tunnel create
                address 10.0.0.1/30
                ip-mtu 1476
                sap tunnel-1.private:1
                    gre-tunnel "gre-tunnel" to 10.0.0.2
---snip---
```

The **to** keyword followed by the private IP address of the remote tunnel endpoint is mandatory.

If this remote IP address is not within the subnet of the local private endpoint then the tunnel will not come up.

Under the **gre-tunnel** command, configure the following parameters:

- The source address of the GRE tunnel. This is the source IPv4 address of GRE encapsulated packets sent by the delivery service. It must be an address in the subnet of the associated public tunnel SAP interface.
- The remote IP address. If this address is reachable in the delivery service (there is a route) then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service.
- The backup remote IP address. If the remote IP address of the tunnel is not reachable then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service.
- The delivery service. This is the identifier or name of the IES or VPRN service where GRE encapsulated packets are injected and terminated. The delivery service can be the same service where the private tunnel SAP interface resides.
- The DSCP marking in the outer IP header of GRE encapsulated packets. If this is not configured then the default copies the DSCP from the inner IP header to the outer IP header.

```
*A:PE-1>config>service>vprn# info
----------------------------------------------------------------
---snip--
            interface "gre-tunnel" tunnel create
                address 10.0.0.1/30
                ip-mtu 1476
                bfd 100 receive 100 multiplier 3
                sap tunnel-1.private:1 create
```

```
gre-tunnel "gre-tunnel-1" to 10.0.0.2 create
    source 192.168.1.1
    remote-ip 192.168.0.1
    delivery-service 2
    dscp af22
    no shutdown
exit
```

- A private tunnel SAP can have only one GRE tunnel (per SAP).

```
*A:PE-1>config>service>vprn>if>sap# gre-tunnel "gre-tunnel-2" to 10.0.0.2 create
MINOR: SVCMGR #5120 Only one GRE tunnel allowed per SAP
```

IP/GRE Tunneling via Static Route

A static route can reference the GRE tunnel directly (by next-hop IP address) or the GRE tunnel can be the resolved next-hop for an indirect static route (Figure 233).

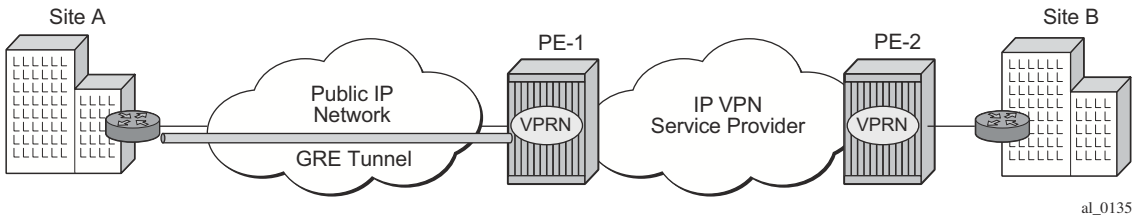

Figure 233: GRE for Remote Access to a VPRN Service

The details of both ends on the GRE tunnel, at site A and PE-1, are shown in Figure 234.

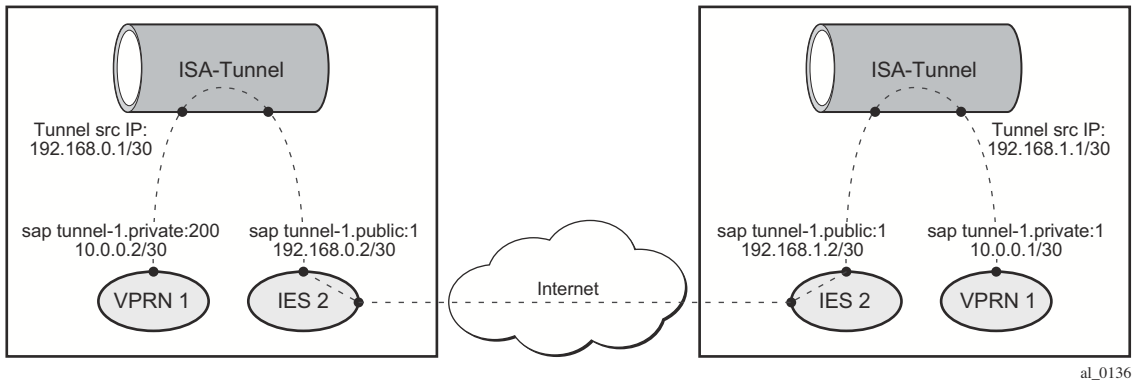

Figure 234: IP/GRE Tunneling via Static Route

The following shows the configuration of PE-1.

```
A:PE-1# configure service vprn 1
A:PE-1>config>service>vprn# info
----------------------------------------------
            route-distinguisher 64496:1
            vrf-target target:64496:1
            interface "int-gre-tunnel" tunnel create
                address 10.0.0.1/30
                ip-mtu 1476
```

```
            sap tunnel-1.private:1 create
                gre-tunnel "gre-tunnel-1" to 10.0.0.2 create
                    source 192.168.1.1
                    remote-ip 192.168.0.1
                    delivery-service 2
                    no shutdown
                exit
            exit
        exit
        static-route 172.16.1.1/32 next-hop 10.0.0.2
```

To check the static route status:

```
*A:PE-1# show router 1 static-route
===============================================================================
Static Route Table (Service: 1)  Family: IPv4
===============================================================================
Prefix                                    Tag         Met    Pref Type Act
   Next Hop                                Interface
-------------------------------------------------------------------------------
172.16.1.1/32                             0           1      5    NH   Y
   10.0.0.2                                int-gre-tunnel
-------------------------------------------------------------------------------
No. of Static Routes: 1
```

IP/GRE Tunneling via BGP Peering

In this section, the configuration has BGP running inside the GRE tunnel (the only supported routing protocol in SR-OS 8.0R5).

```
*A:PE-1>config>service>vprn# info
----------------------------------------------
            router-id 192.0.2.2
            autonomous-system 64496
            route-distinguisher 64496:1
            vrf-target target:64496:1
            interface "int-gre-tunnel" tunnel create
                address 10.0.0.1/30
                ip-mtu 1476
                sap tunnel-1.private:1 create
                    gre-tunnel "gre-tunnel-1" to 10.0.0.2 create
                        source 192.168.1.1
                        remote-ip 192.168.0.1
                        delivery-service 2
                        no shutdown
                    exit
                exit
            static-route 172.16.1.1/32 next-hop 10.0.0.2
            bgp
                local-as 64496
                router-id 192.0.2.2
                group "group-1"
                    type internal
                    local-as 64496
                    local-address 172.32.1.1
                    neighbor 172.16.1.1
                    exit
                exit
                no shutdown
            exit
```

It is mandatory to configure the autonomous-system under the VPRN otherwise the BGP neighboring will not be established.

To check the BGP status:

```
*A:PE-1# show router 1 bgp neighbor
===============================================================================
BGP Neighbor
===============================================================================
Peer  : 172.16.1.1
Group : group-1
-------------------------------------------------------------------------------
Peer AS              : 64496           Peer Port           : 179
Peer Address         : 172.16.1.1
Local AS             : 64496           Local Port          : 49554
Local Address        : 172.32.1.1
Peer Type            : Internal
State                : Established     Last State          : Active
---snip---
```

IP/GRE Tunneling via OSPFv2 Peering

From SR-OS 9.0R1, OSPFv2 can be run on IES and VPRN IP interfaces associated with private GRE tunnel SAPs.

All OSPF features are supported including area 0 and non-area 0 support, virtual links, authentication, BFD, configurable protocol timers.

```
*A:PE-1>config>service>vprn# info
----------------------------------------------
            router-id 192.0.2.2
            route-distinguisher 64496:1
            vrf-target target:64496:1
            interface "int-gre-tunnel" tunnel create
                address 10.0.0.1/30
                ip-mtu 1476
                bfd 100 receive 100 multiplier 3
                sap tunnel-1.private:1 create
                    gre-tunnel "gre-tunnel-1" to 10.0.0.2 create
                        source 192.168.1.1
                        remote-ip 192.168.0.1
                        delivery-service 2
                        no shutdown
                    exit
                exit
            exit
            ospf
                area 0.0.0.0
                    interface "int-gre-tunnel"
                    exit
                    interface "int-CE-1"
                        interface-type point-to-point
                    exit
                exit
            exit
            no shutdown
```

To check the OSPF status:

```
*A:PE-1# show router 1 ospf neighbor
===============================================================================
OSPF Neighbors
===============================================================================
Interface-Name                   Rtr Id          State      Pri  RetxQ   TTL
   Area-Id
-------------------------------------------------------------------------------
int-gre-tunnel                   192.0.2.1       Full       1    0       30
   0.0.0.0
-------------------------------------------------------------------------------
No. of Neighbors: 1
===============================================================================
```

To check the OSPF routes:

```
*A:PE-1# show router 1 route-table protocol ospf
===============================================================================
Route Table (Service: 1)
===============================================================================
Dest Prefix[Flags]                              Type    Proto    Age         Pref
      Next Hop[Interface Name]                                     Metric
-------------------------------------------------------------------------------
172.16.1.1/32                                   Remote  OSPF     00h04m58s   10
       10.0.0.2                                                        10
-------------------------------------------------------------------------------
```

IP/GRE Tunneling Protection using IPSec Tunnel Mode

To provide protection against the potential threats (such as spoofing) the GRE packets can be encrypted and authenticated using IPSec.

In SR-OS 9.0R1 GRE packets receive IPSec protection by forwarding them, after encapsulation by one tunnel-ISA, into an IPSec tunnel supported by another (or the same) tunnel-ISA.

Note that when configuring GRE protection by an IPSec tunnel:

- A GRE tunnel and its protecting IPSec tunnel may belong to the same or different tunnel-groups (the same tunnel-group is assumed in the example below).
- A GRE tunnel and its protecting IPSec tunnel may be assigned to the same tunnel-ISA (if they belong to the same tunnel-group) or different tunnel-ISAs.
- A single IPSec tunnel can protect one or more GRE tunnels in addition to other IP traffic that meets the IPSec security policy.
- The private IPSec tunnel SAP interface and public GRE tunnel SAP interface are always part of the same VPRN. The private GRE tunnel SAP interface can be part of this same VPRN or a different VPRN.

In the following example the GRE tunnel and its protecting IPSec tunnel belong to the same tunnel group.

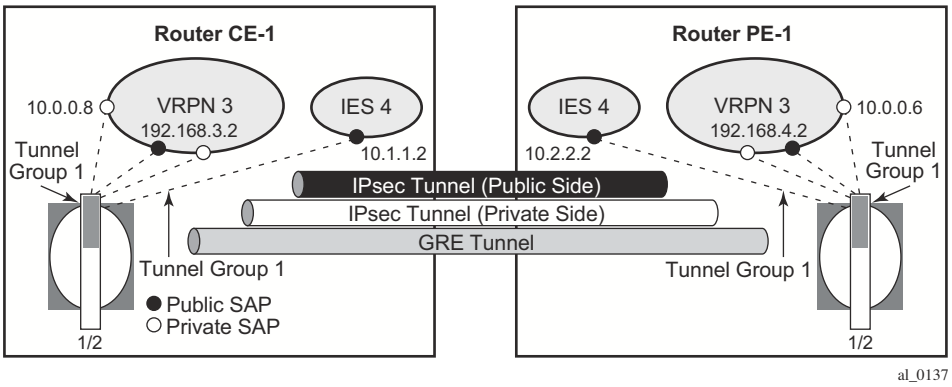

Figure 235: Example GRE over IPSec Tunnel

IPSec Configuration

An ike-policy and ipsec-transform must be configured as shown below.

```
*A:PE-1>config>ipsec# info
----------------------------------------------
        ike-policy 1 create
            dh-group 5
        exit
        ipsec-transform 1 create
            esp-encryption-algorithm aes256
        exit
----------------------------------------------
```

The public/private side of the GRE tunnel and the private side of the IPSec tunnel are in the same VPRN, as shown in the following configuration example.

```
*A:PE-1# configure service vprn 3
*A:PE-1>config>service>vprn# info
----------------------------------------------
            ipsec
                security-policy 1 create
                    entry 1 create
                        local-ip 192.168.4.0/24
                        remote-ip 192.168.3.0/24
                    exit
                exit
            exit
            route-distinguisher 64496:3
            vrf-target target:64496:3
            interface "int-private-ipsec-1" tunnel create
                sap tunnel-1.private:3 create
                    ipsec-tunnel "ipsec-tunnel-for-gre-tunnel" create
                        security-policy 1
                       local-gateway-address 10.2.2.1 peer 10.1.1.1 delivery-service 4
                        dynamic-keying
                            ike-policy 1
                            pre-shared-key "ALU"
                            transform 1
                        exit
                        no shutdown
                    exit
                exit
            exit
            interface "int-public-gre-1" create
                address 192.168.4.2/24
                sap tunnel-1.public:4 create
                exit
            exit
            interface "int-private-gre-1" tunnel create
                address 10.0.0.6/30
                sap tunnel-1.private:5 create
                    gre-tunnel "protected-gre-tunnel" to 10.0.0.5 create
                        source 192.168.4.1
                        remote-ip 192.168.3.1
                        delivery-service 3
```

```
                    no shutdown
                exit
            exit
        exit
        static-route 192.168.3.0/24 ipsec-tunnel "ipsec-tunnel-for-gre-tunnel"
        no shutdown
```

The following displays a configuration example of the public side of the IPSec tunnel:

```
*A:PE-1>config>service>ies# info
----------------------------------------------
        interface "public-ipsec-1" create
            address 10.2.2.2/24
            tos-marking-state untrusted
            sap tunnel-1.public:3 create
            exit
        exit
```

To check the GRE tunnel:

```
*A:PE-1# show gre tunnel
===============================================================================
GRE Tunnels
===============================================================================
TunnelName                      LocalAddress     SvcId       Admn
 SapId                           RemoteAddress    DlvrySvcId  Oper
  To                              Bkup RemAddr     DSCP        Oper Rem Addr
-------------------------------------------------------------------------------
protected-gre-tunnel            192.168.4.1      3           Up
 tunnel-1.private:5              192.168.3.1      3           Up
  10.0.0.5                                        None        192.168.3.1
-------------------------------------------------------------------------------
```

To check the GRE tunnel info:

```
*A:PE-1# show gre tunnel "gre-tunnel-1"
===============================================================================
GRE Tunnel Configuration Detail
===============================================================================
Service Id       : 1                    Sap Id           : tunnel-1.private:1
Tunnel Name      : gre-tunnel-1
Description      : None
Target Address   : 10.0.0.2             Delivery Service : 2
Admin State      : Up                   Oper State       : Up
Source Address   : 192.168.1.1          Oper Remote Addr : 192.168.0.1
Remote Address   : 192.168.0.1          Backup Address   :
DSCP             : None
Oper Flags       : None

===============================================================================
GRE Tunnel Statistics: gre-tunnel-1
===============================================================================
Errors Rx        : 0                    Errors Tx        : 0
Pkts Rx          : 9164                 Pkts Tx          : 14176
Bytes Rx         : 703812               Bytes Tx         : 750429
```

```
Key Ignored Rx   : 0                    Too Big Tx       : 0
Seq Ignored Rx   : 0
Vers Unsup. Rx   : 0
Invalid Chksum Rx: 0
Loops Rx         : 0
```

By default the IPSec tunnel is down if it is not used by any traffic.

```
*A:PE-1# show ipsec tunnel
===============================================================================
IPsec Tunnels
===============================================================================
TunnelName                       LocalAddress      SvcId        Admn   Keying
  SapId                            RemoteAddress     DlvrySvcId   Oper   Sec
                                                                         Plcy
-------------------------------------------------------------------------------
ipsec-tunnel-for-gre-tunnel      10.2.2.1          3            Up     Dynamic
  tunnel-1.private:3               10.1.1.1          4              Down   1
-------------------------------------------------------------------------------
```

Once it is used by any traffic the status will be changed to be up.

```
*A:PE-1# ping router 3 10.0.0.5
PING 10.0.0.5 56 data bytes
64 bytes from 10.0.0.5: icmp_seq=1 ttl=64 time=4.64ms.
64 bytes from 10.0.0.5: icmp_seq=2 ttl=64 time=4.54ms.
64 bytes from 10.0.0.5: icmp_seq=3 ttl=64 time=4.42ms.
64 bytes from 10.0.0.5: icmp_seq=4 ttl=64 time=5.01ms.
64 bytes from 10.0.0.5: icmp_seq=5 ttl=64 time=4.40ms.
```

To check the IPSec tunnel:

```
*A:PE-1# show ipsec tunnel
===============================================================================
IPsec Tunnels
===============================================================================
TunnelName                       LocalAddress      SvcId        Admn   Keying
  SapId                            RemoteAddress     DlvrySvcId   Oper   Sec
                                                                         Plcy
-------------------------------------------------------------------------------
ipsec-tunnel-for-gre-tunnel      10.2.2.1          3            Up     Dynamic
  tunnel-1.private:3               10.1.1.1          4              Up     1
-------------------------------------------------------------------------------
IPsec Tunnels: 1
===============================================================================
```

BFD Support on Private Tunnel Interfaces

The SR-OS 9.0R1 introduces support for BFD on IP interfaces associated with private GRE tunnel SAPs. The BFD state of the interface can be used by static routes, OSPFv2 and/or BGP configured on the interface. It is not used to trigger a switch over to the backup remote IP address of the GRE tunnel.

The following displays a static-route example:

```
*A:PE-1>config>service>vprn# info
----------------------------------------------
            router-id 192.0.2.2
            route-distinguisher 64496:1
            vrf-target target:64496:1
            interface "int-gre-tunnel" tunnel create
                address 10.0.0.1/30
                ip-mtu 1476
                bfd 100 receive 100 multiplier 3
                sap tunnel-1.private:1 create
                    gre-tunnel "gre-tunnel-1" to 10.0.0.2 create
                        source 192.168.1.1
                        remote-ip 192.168.0.1
                        delivery-service 2
                        no shutdown
                    exit
                exit
            exit
            static-route 172.16.1.1/32 next-hop 10.0.0.2 bfd-enable
```

To check the BFD session:

```
*A:PE-1# show router 1 bfd session
===============================================================================
BFD Session
===============================================================================
Interface                     State                Tx Intvl  Rx Intvl  Multipl
  Remote Address              Protocols            Tx Pkts   Rx Pkts   Type
-------------------------------------------------------------------------------
gre-tunnel                    Up (3)               100       100       3
   10.0.0.2                   static               N/A       N/A       cpm-np
-------------------------------------------------------------------------------
No. of BFD sessions: 1
===============================================================================
```

The following displays an OSPF example:

```
*A:PE-1>config>service>vprn# info
----------------------------------------------
            router-id 192.0.2.2
            route-distinguisher 64496:1
            vrf-target target:64496:1
            interface "int-gre-tunnel" tunnel create
                address 10.0.0.1/30
                ip-mtu 1476
                bfd 100 receive 100 multiplier 3
                sap tunnel-1.private:1 create
                    gre-tunnel "gre-tunnel-1" to 10.0.0.2 create
                        source 192.168.1.1
                        remote-ip 192.168.0.1
                        delivery-service 2
                        no shutdown
                    exit
                exit
            exit
            ospf
                area 0.0.0.0
                    interface "int-gre-tunnel"
                        bfd-enable
                    exit
---snip--
```

To check the BFD session:

```
*A:PE-1# show router 1 bfd session
===============================================================================
BFD Session
===============================================================================
Interface                     State                Tx Intvl  Rx Intvl  Multipl
  Remote Address              Protocols            Tx Pkts   Rx Pkts   Type
-------------------------------------------------------------------------------
int-gre-tunnel                Up (3)               100       100       3
   10.0.0.2                   ospf2                N/A       N/A       cpm-np
-------------------------------------------------------------------------------
```

The following displays a BGP example:

```
*A:PE-1>config>service>vprn# info
----------------------------------------------
            router-id 192.0.2.2
            autonomous-system 64496
            route-distinguisher 64496:1
            vrf-target target:64496:1
            interface "int-gre-tunnel" tunnel create
                address 10.0.0.1/30
                ip-mtu 1476
                bfd 100 receive 100 multiplier 3
                sap tunnel-1.private:1 create
                    gre-tunnel "gre-tunnel-1" to 10.0.0.2 create
                        source 192.168.1.1
                        remote-ip 192.168.0.1
```

```
                delivery-service 2
                no shutdown
            exit
        exit
    exit
    static-route 172.16.1.1/32 next-hop 10.0.0.2
    bgp
        local-as 64496
        router-id 192.0.2.2
        group "group-1"
            type internal
            local-as 64496
            local-address 172.32.1.1
            neighbor 172.16.1.1
                bfd-enable
            exit
        exit
        no shutdown
    exit
```

To check the BFD session:

```
*A:PE-1# show router 1 bfd session
===============================================================================
BFD Session
===============================================================================
Interface                     State                Tx Intvl  Rx Intvl  Multipl
  Remote Address              Protocols            Tx Pkts   Rx Pkts   Type
-------------------------------------------------------------------------------
int-CE-1                      Up (3)               100       100       3
   172.16.1.1                 bgp                  N/A       N/A       cpm-np
-------------------------------------------------------------------------------
No. of BFD sessions: 1
===============================================================================
```

IP/GRE Termination – Advanced Topics

DSCP Value of Outer Delivery Header

- Default behavior — The DSCP value from the Payload header is copied into the outer GRE header. This is a one to one copy and no QoS classifications are required. It is performed when no DSCP value is configured under the private gre-tunnel.
- Non Default behavior — DSCP is configured under the private SAP (example below using af41).

```
interface "gre-tunnel" tunnel create
    address 10.0.0.1/30
    sap tunnel-1.private:200 create
       gre-tunnel "gre-tunnel" to 10.0.0.2
          source 192.168.11.2
          remote-ip 192.168.10.2
          delivery-service 21
          dscp af41
```

The log filter output: TOS=88 (DSCP=af41) in the public network.

```
Maximum entries configured : 1000
Number of entries logged   : 2
2010/12/13 18:26:15  Ip Filter: 10:10  Desc:
SAP: 1/1/1  Direction: Egress  Action: Forward
Src MAC: 1c-2c-01-01-00-01  Dst MAC: 1c-2d-01-01-00-01  EtherType: 0800
Src IP: 192.168.11.2 Dst IP: 192.168.10.2 Flags: 0  TOS: 88  TTL: 254
```

IP-MTU

It is possible to configure the IP MTU of a private tunnel SAP interface. This sets the maximum IP packet size payload (including IP header) that can be sent into the tunnel (it applies to the packet size before the tunnel encapsulation is added).

```
vprn 1 customer 1 create
            router-id 172.17.1.1
            autonomous-system 650000
            route-distinguisher 65000:1
            interface "gre-tunnel" tunnel
                address 10.0.0.1/30
                ip-mtu 1476
                sap tunnel-1.private:201
```

When an IPv4 packet needs to be forwarded to the tunnel and is larger than IP MTU bytes:

- If the DF bit is clear, the payload packet is IP fragmented to the MTU size prior to tunnel encapsulation.
- If the DF bit is set, the payload packet is discarded.

The IP-MTU range supported is from 512 to 9000 bytes.

To display information about the tunnel operational MTU.

```
*A:PE-1# show router 1 interface  "gre-tunnel" detail  | match MTU
IP Oper MTU      : 1476                 ICMP Mask Reply   : True
```

Statistics and Accounting

Collect-stats can be configured under public and private SAPs.

For Public SAPs:

```
*A:PE-1>config>service>ies>if# sap tunnel-1.public:2 collect-stats
```

For Private SAPs:

```
*A:PE-1>config>service>vprn>if# sap tunnel-1.private:2 collect-stats
```

Filtering, Policing and QoS

An ip-filter and QoS policy can be applied to the ingress and egress traffic of the private and public SAPS.

Public SAPs:

```
*A:PE-1>config>service>vprn>if# info
----------------------------------------------
---snip---
                sap tunnel-1.private:1 create
                    ingress
                        qos 10
                        filter ip 1
                    exit
                    egress
                        qos 10
                        filter ip 1
                    exit
```

Private SAPs:

```
*A:PE-1>config>service>ies>if# info
----------------------------------------------
                address 192.168.1.2/30
                tos-marking-state untrusted
                sap tunnel-1.public:1 create
                    ingress
                        qos 10
                        filter ip 1
                    exit
                    egress
                        qos 10
                        filter ip 1
                    exit
```

Mirroring

The public and private SAPs can be mirrored.

```
*A:PE-1# show debug
debug
    mirror-source 99
        sap tunnel-1.private:3 egress ingress
        sap tunnel-1.public:1 egress ingress
        no shutdown
    exit
exit
```

Conclusion

This section provides configuration and show commands for IP/GRE termination.