Network Configuration Example

Configuring Branch SRX Series for MPLS over IPsec (1500-byte MTU)

Published: 2014-12-17

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network Configuration Example Configuring Branch SRX Series for MPLS over IPsec (1500-byte MTU)

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

CHAPTER 1

Simplified MPLS Through IPsec over 1500-byte Media

About This Network Configuration Example

This network configuration example provides an overview of simplified MPLS over IPsec over 1500-byte media. It also contains a sample use case showing how to provide simplified configuration for VPLS or Layer 3 VPN services with GRE through IPsec tunneling, over 1500-byte media (Internet).

This document complements the configuration guidance provided in Example: Configuring Selective Packet Services and further explains the MPLS through IPsec over 1500byte media fragmentation and reassembly use case scenario.

Use Case for MPLS Through IPsec over 1500-byte Media

Use selective packet services in a single routing instance (the default one) without utilizing lt interfaces. You can perform IPsec encapsulated packet fragmentation on the outgoing physical interface of the sending device and reassembly on the receiving device before the IPsec decryption.

Related Documentation

- Simplified MPLS Through IPsec over 1500-byte Media Overview on page 7
- Example: Configuring MPLS over GRE with IPsec Fragmentation and Reassembly on page 8

Simplified MPLS Through IPsec over 1500-byte Media Overview

When you transmit a virtual private LAN service (VPLS) frame over a Layer 3 IP network, you need to encapsulate the MPLS packet into generic routing encapsulation (GRE) and then transmit the frame across the IP network. However, when you transmit VPLS over GRE over 1500-byte media such as the Internet, the VPLS frame is corrupted at the receiving end. Hence, it is not possible to send a 1500-byte Ethernet frame across a VPLS service running over the Internet. The Ethernet frame beyond 1448 bytes (24byte GRE + 20byte IP + 2*4byte MPLS) is blocked. Hence, the VPN traffic forwarded over 1500-byte media must be fragmented.

Juniper Networks® Branch SRX Series Services Gateways provide a solution for IPsec encapsulated packet fragmentation and reassembly.

Related Documentation

- Example: Configuring MPLS over GRE with IPsec Fragmentation and Reassembly on page 8

Example: Configuring MPLS over GRE with IPsec Fragmentation and Reassembly

The virtual private network (VPN) traffic forwarded over 1500-byte media is blocked because of the protocol encapsulation overhead (Layer 2, MPLS, GRE and IPsec, and GRE or IPsec).

This document provide a solution to fragment an IPsec encapsulated packet and reassemble the fragmented packets.

This example shows how to configure selective packet services using a single routing instance (the default one) without utilizing the lt interface.

You can perform IPsec encapsulated packet fragmentation on the outgoing physical interface of the sending device and reassembly on the receiving device before IPsec decryption.

NOTE: **The reassembly of fragmented packets uses a lot of device resources, and the performance of the device will be slower than the nonfragmented traffic.**

The topic includes the following sections:

Requirements

This example uses the following hardware and software components:

- Branch SRX Series Services Gateways
- Junos OS Release 11.4 or later

Overview and Topology

This example includes the following configurations:

- Configure interfaces for the appropriate protocol encapsulation with a required maximum transmission unit (MTU) value.
- Apply firewall filter on the ge-0/0/10.10 interface to set the packet mode. Configure the outgoing interface ge-0/0/14.0 with an appropriate MTU value.
- Set the largest MTU value to GRE and IPsec logical interfaces to avoid IPsec fragmentation at logical interfaces. GRE encapsulated traffic is tunneled inside IPsec.
- Add the MPLS family to the GRE interface gr-0/0/0 and apply a firewall filter to enable packet mode. Create firewall filters to configure interfaces to work with packet mode.

- Perform basic IPsec tunnel configuration on the device with the **df-bit clear** option added in IPsec VPN configuration to allow fragmentation of oversized IPsec packets on the outgoing interface ge-0/0/14.0.
- Configure all noncustomer- facing interfaces such as ge-0/0/14.0, gr-0/0/0.0, lo0.0, and st0.0 in a single security zone.
- Configure a policy to permit all (intrazone) traffic.
- Configure OSPF for lo0.0 address distribution, and LDP for label distribution. Then you configure IBGP with the inet-vpn and l2vpn families.
- Configure two routing instances, one for Layer 3 VPN and other for VPLS application.

Figure 1 on page 9 shows the topology used in this example.

Figure 1: IPsec Tunnel over the GRE Tunnel

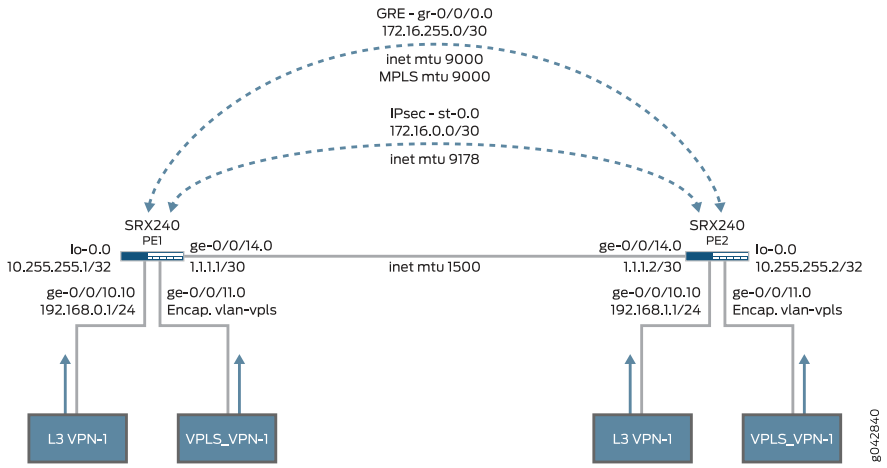

Table 1 on page 10 provides a summary of the parameters used in this topology.

Table 1: Components of the Topology

Components	Description
PE1 and PE2	PE1 AND PE2 SRX Series Firewalls: • IP address for PE1: 10.255.255.1/32 • IP address for PE2: 10.255.255.2/32 ge-0/0/10.10: • IP address: 192.168.0.1/24 • Customer-facing L3VPN interface • **input packet-mode-inet**: inet family in packet mode
	ge-0/0/11.0: • Customer-facing VPLS interface • **vlan-vpls**: VPLS encapsulation
	ge-0/0/14.0: • Outgoing interface • IP address: 1.1.1.1/30 • **mtu 1514**: Outgoing interface MTU
	gr-0/0/0: • Core interface connecting to MPLS • IP address: 172.16.255.1/30 • **input packet-mode**: MPLS family in packet mode
	lo0: • Logical Interface • IP address: 10.255.255.1/32
	st0.0: • Tunnel interface • IP address: 172.16.0.1/30
	• **df-bit clear** — This option clears the do not fragment (DF) bit in the outgoing packet header • **L3VPN**— Routing instance for Layer3 VPN application • **VPLS_VPN-1**— Routing instance for VPLS application

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/10.10 description "LAN Side"
set interfaces ge-0/0/10.10 vlan-tagging
set interfaces ge-0/0/10.10 mtu 9192
set interfaces ge-0/0/10.10 unit 10 description L3VPN-1
set interfaces ge-0/0/10.10 unit 10 vlan-id 10
set interfaces ge-0/0/10.10 unit 10 family inet filter input packet-mode-inet
set interfaces ge-0/0/10.10 unit 10 family inet address 192.168.0.1/24
set interfaces ge-0/0/11 description "LAN Side"
set interfaces ge-0/0/11 flexible-vlan-tagging
set interfaces ge-0/0/11 mtu 1522
set interfaces ge-0/0/11 encapsulation vlan-vpls
set interfaces ge-0/0/11 unit 0 description VPLS_VPN-1
set interfaces ge-0/0/11 unit 0 encapsulation vlan-vpls
set interfaces ge-0/0/11 unit 0 vlan-id 512
set interfaces ge-0/0/14 description Internet
set interfaces ge-0/0/14 mtu 1514
set interfaces ge-0/0/14 unit 0 family inet address 1.1.1.1/30
set interfaces gr-0/0/0 unit 0 description "MPLS core facing interface"
set interfaces gr-0/0/0 unit 0 tunnel source 172.16.0.1
set interfaces gr-0/0/0 unit 0 tunnel destination 172.16.0.2
set interfaces gr-0/0/0 unit 0 family inet mtu 9000
set interfaces gr-0/0/0 unit 0 family inet address 172.16.255.1/30
set interfaces gr-0/0/0 unit 0 family mpls mtu 9000
set interfaces gr-0/0/0 unit 0 family mpls filter input packet-mode
set interfaces lo0 unit 0 family inet address 10.255.255.1/32
set interfaces st0 unit 0 family inet mtu 9178 address 172.16.0.1/30
set firewall family inet filter packet-mode-inet term all-traffic then packet-mode
set firewall family inet filter packet-mode-inet term all-traffic then accept
set firewall family mpls filter packet-mode term all-traffic then packet-mode
set firewall family mpls filter packet-mode term all-traffic then accept
set security ike policy standard mode main
set security ike policy standard proposal-set standard
set security ike policy standard pre-shared-key ascii-text "$9$GOjkPFnCBIc5QIcylLXUjH"
set security ike gateway srx240-2 ike-policy standard
set security ike gateway srx240-2 address 1.1.1.2
set security ike gateway srx240-2 external-interface ge-0/0/14.0
set security ipsec policy standard proposal-set standard
set security ipsec vpn ipsec-vpn-1 bind-interface st0.0
set security ipsec vpn ipsec-vpn-1 df-bit clear
set security ipsec vpn ipsec-vpn-1 ike gateway srx240-2
set security ipsec vpn ipsec-vpn-1 ike ipsec-policy standard
set security ipsec vpn ipsec-vpn-1 establish-tunnels immediately
set security policies from-zone Internet to-zone Internet policy Internet match source-address
any
set security policies from-zone Internet to-zone Internet policy Internet match destination-address
any
set security policies from-zone Internet to-zone Internet policy Internet match application any
set security policies from-zone Internet to-zone Internet policy Internet then permit
set security zones security-zone Internet host-inbound-traffic system-services all
set security zones security-zone Internet host-inbound-traffic protocols all
set security zones security-zone Internet interfaces ge-0/0/14.0
```

```
set security zones security-zone Internet interfaces gr-0/0/0.0
set security zones security-zone Internet interfaces lo0.0
set security zones security-zone Internet interfaces st0.0
set protocols mpls interface gr-0/0/0.0
set protocols bgp tcp-mss 1200
set protocols bgp group IBGP type internal
set protocols bgp group IBGP local-address 10.255.255.1
set protocols bgp group IBGP local-as 65100
set protocols bgp group IBGP neighbor 10.255.255.2
set protocols bgp group IBGP neighbor 10.255.255.2 family inet any
set protocols bgp group IBGP neighbor 10.255.255.2 family inet-vpn any
set protocols bgp group IBGP neighbor 10.255.255.2 family l2vpn signaling
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface gr-0/0/0.0
set protocols ldp interface gr-0/0/0.0
set protocols ldp interface lo0.0
set routing-instances L3VPN-1 instance-type vrf
set routing-instances L3VPN-1 interface ge-0/0/10.10
set routing-instances L3VPN-1 route-distinguisher 10.255.255.1:1000
set routing-instances L3VPN-1 vrf-target target:65100:1000
set routing-instances L3VPN-1 vrf-target import target:65100:1000
set routing-instances L3VPN-1 vrf-target export target:65100:1000
set routing-instances L3VPN-1 vrf-table-label
set routing-instances L3VPN-1 routing-options auto-export
set routing-instances VPLS_VPN-1 instance-type vpls
set routing-instances VPLS_VPN-1 interface ge-0/0/11.0
set routing-instances VPLS_VPN-1 route-distinguisher 10.255.255.1:1001
set routing-instances VPLS_VPN-1 vrf-target target:65100:1001
set routing-instances VPLS_VPN-1 protocols vpls no-tunnel-services
set routing-instances VPLS_VPN-1 protocols vpls site 1 site-identifier 1
set routing-instances VPLS_VPN-1 protocols vpls site 1 interface ge-0/0/11.0
set routing-instances VPLS_VPN-1 protocols vpls mac-tlv-receive
set routing-instances VPLS_VPN-1 protocols vpls mac-tlv-send
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To fragment the MPLS frame and reassemble the packet:

1. Configure the physical Interfaces.

```
[edit interfaces]
user@host# set ge-0/0/10.10 description "LAN Side"
user@host# set ge-0/0/10.10 vlan-tagging
user@host# set ge-0/0/10.10 mtu 9192
user@host# set ge-0/0/10.10 unit 10 description L3VPN-1
user@host# set ge-0/0/10.10 unit 10 vlan-id 10
user@host# set ge-0/0/10.10 unit 10 family inet filter input packet-mode-inet
user@host# set ge-0/0/10.10 unit 10 family inet address 192.168.0.1/24

user@host# set ge-0/0/11 description "LAN Side"
user@host# set ge-0/0/11 flexible-vlan-tagging
user@host# set ge-0/0/11 mtu 1522
user@host# set ge-0/0/11 encapsulation vlan-vpls
user@host# set ge-0/0/11 unit 0 description VPLS_VPN-1
user@host# set ge-0/0/11 unit 0 encapsulation vlan-vpls
user@host# set ge-0/0/11 unit 0 vlan-id 512

user@host# set ge-0/0/14 description Internet
user@host# set ge-0/0/14 mtu 1514
user@host# set ge-0/0/14 unit 0 family inet address 1.1.1.1/30
```

2. Configure the logical Interfaces.

```
[edit interfaces]
user@host# set gr-0/0/0 unit 0 description "MPLS core facing interface"
user@host# set gr-0/0/0 unit 0 tunnel source 172.16.0.1
user@host# set gr-0/0/0 unit 0 tunnel destination 172.16.0.2
user@host# set gr-0/0/0 unit 0 family inet mtu 9000
user@host# set gr-0/0/0 unit 0 family inet address 172.16.255.1/30
user@host# set gr-0/0/0 unit 0 family mpls mtu 9000
user@host# set gr-0/0/0 unit 0 family mpls filter input packet-mode

user@host# set lo0 unit 0 family inet address 10.255.255.1/32
user@host# set st0 unit 0 family inet mtu 9178 address 172.16.0.1/30
```

3. Configure the firewall filters that are used to configure interfaces to work with packet mode.

```
[edit firewall]
user@host# set family inet filter packet-mode-inet term all-traffic then packet-mode
user@host# set family inet filter packet-mode-inet term all-traffic then accept
user@host# set family mpls filter packet-mode term all-traffic then packet-mode
user@host# set family mpls filter packet-mode term all-traffic then accept
```

4. Configure the IKE and IPsec policies.

```
[edit security]
user@host# set ike policy standard mode main
user@host# set ike policy standard proposal-set standard
```

```
user@host# set ike policy standard pre-shared-key ascii-text
  "$9$GOjkPFnCBIc5QIcylLXUjH"
user@host# set ike gateway srx240-2 ike-policy standard
user@host# set ike gateway srx240-2 address 1.1.1.2
user@host# set ike gateway srx240-2 external-interface ge-0/0/14.0

user@host# set ipsec policy standard proposal-set standard
user@host# set ipsec vpn ipsec-vpn-1 bind-interface st0.0
user@host# set ipsec vpn ipsec-vpn-1 df-bit clear
user@host# set ipsec vpn ipsec-vpn-1 ike gateway srx240-2
user@host# set ipsec vpn ipsec-vpn-1 ike ipsec-policy standard
user@host# set ipsec vpn ipsec-vpn-1 establish-tunnels immediately
```

5. Configure all noncustomer-facing interfaces in a single security zone and a policy to permit all (intrazone) traffic.

```
[edit security policies from-zone Internet to-zone Internet]
user@host# set policy Internet match source-address any
user@host# set policy Internet match destination-address any
user@host# set policy Internet match application any
user@host# set policy Internet then permit

[edit security zones security-zone Internet]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all

user@host# set interfaces ge-0/0/14.0
user@host# set interfaces gr-0/0/0.0
user@host# set interfaces lo0.0
user@host# set interfaces st0.0
```

6. Configure the OSPF protocol for lo0.0 address distribution, and configure IBGP with the inet-vpn and l2vpn families.

```
[edit protocols]
user@host# set mpls interface gr-0/0/0.0

user@host# set bgp tcp-mss 1200
user@host# set bgp group IBGP type internal
user@host# set bgp group IBGP local-address 10.255.255.1
user@host# set bgp group IBGP local-as 65100
user@host# set bgp group IBGP neighbor 10.255.255.2
user@host# set bgp group IBGP neighbor 10.255.255.2 family inet any
user@host# set bgp group IBGP neighbor 10.255.255.2 family inet-vpn any
user@host# set bgp group IBGP neighbor 10.255.255.2 family l2vpn signaling

user@host# set ospf traffic-engineering
user@host# set ospf area 0.0.0.0 interface lo0.0
user@host# set ospf area 0.0.0.0 interface lo0.0 passive
user@host# set ospf area 0.0.0.0 interface gr-0/0/0.0

user@host# set ldp interface gr-0/0/0.0
user@host# set ldp interface lo0.0
```

7. Configure two routing instances, one for Layer 3 VPN and the other for the VPLS application.

```
[edit routing-instances]
user@host# set L3VPN-1 instance-type vrf
user@host# set L3VPN-1 route-distinguisher 10.255.255.1:1000
user@host# set L3VPN-1 interface ge-0/0/10.10
user@host# set L3VPN-1 vrf-target target:65100:1000
user@host# set L3VPN-1 vrf-target import target:65100:1000
user@host# set L3VPN-1 vrf-target export target:65100:1000
user@host# set L3VPN-1 vrf-table-label
user@host# set L3VPN-1 routing-options auto-export

user@host# set VPLS_VPN-1 instance-type vpls
user@host# set VPLS_VPN-1 interface ge-0/0/11.0
user@host# set VPLS_VPN-1 route-distinguisher 10.255.255.1:1001
user@host# set VPLS_VPN-1 vrf-target target:65100:1001
user@host# set VPLS_VPN-1 protocols vpls no-tunnel-services
user@host# set VPLS_VPN-1 protocols vpls site 1 site-identifier 1
user@host# set VPLS_VPN-1 protocols vpls site 1 interface ge-0/0/11.0
user@host# set VPLS_VPN-1 protocols vpls mac-tlv-receive
user@host# set VPLS_VPN-1 protocols vpls mac-tlv-send
```

Results Display the results of the configuration:

```
user@host> show configuration
interfaces {
  ge-0/0/10.10 {
    description "LAN Side";
    vlan-tagging;
    mtu 9192;
    unit 10 {
      description L3VPN-1;
      vlan-id 10;
      family inet {
        filter {
          input packet-mode-inet;
        }
        address 192.168.0.1/24;
      }
    }
  }
  ge-0/0/11 {
    description "LAN Side";
    flexible-vlan-tagging;
    mtu 1522;
    encapsulation vlan-vpls;
    unit 0 {
      description VPLS_VPN-1;
      encapsulation vlan-vpls;
      vlan-id 512;
    }
  }
  ge-0/0/14 {
    description Internet;
    mtu 1514;
    unit 0 {
      family inet {
        address 1.1.1.1/30;
      }
    }
  }
  gr-0/0/0 {
    unit 0 {
      description "MPLS core facing interface";
      tunnel {
        source 172.16.0.1;
        destination 172.16.0.2;
      }
      family inet {
        mtu 9000;
        address 172.16.255.1/30;
      }
      family mpls {
        mtu 9000;
        filter {
          input packet-mode;
        }
      }
```



```
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.255.255.1/32;
            }
        }
    }
    st0 {
        unit 0 {
            family inet {
                mtu 9178;
                address 172.16.0.1/30;
            }
        }
    }
}
firewall {
    family inet {
        filter packet-mode-inet {
            term all-traffic {
                then {
                    packet-mode;
                    accept;
                }
            }
        }
    }
    family mpls {
        filter packet-mode {
            term all-traffic {
                then {
                    packet-mode;
                    accept;
                }
            }
        }
    }
}
security {
    ike {
        policy standard {
            mode main;
            proposal-set standard;
            pre-shared-key ascii-text "$9$GOjkPFnCBIc5QIcylLXUjH";
        }
        gateway srx240-2 {
            ike-policy standard;
            address 1.1.1.2;
            external-interface ge-0/0/14.0;
        }
    }
    ipsec {
        policy standard {
            proposal-set standard;
```

```
            }
            vpn ipsec-vpn-1 {
                bind-interface st0.0;
                df-bit clear;
                ike {
                    gateway srx240-2;
                    ipsec-policy standard;
                }
                establish-tunnels immediately;
            }
        }
        policies {
            from-zone Internet to-zone Internet {
                policy Internet {
                    match {
                        source-address any;
                        destination-address any;
                        application any;
                    }
                    then {
                        permit;
                    }
                }
            }
        }
        zones {
            security-zone Internet {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
                interfaces {
                    ge-0/0/14.0;
                    gr-0/0/0.0;
                    lo0.0;
                    st0.0;
                }
            }
        }
    }
    protocols {
        mpls {
            interface gr-0/0/0.0;
        }
        bgp {
            tcp-mss 1200;
            group IBGP {
                type internal;
                local-address 10.255.255.1;
                local-as 65100;
                neighbor 10.255.255.2 {
                    family inet {
```

```
                any;
            }
            family inet-vpn {
                any;
            }
            family l2vpn {
                signaling;
            }
        }
    }
}
ospf {
    traffic-engineering;
    area 0.0.0.0 {
        interface lo0.0 {
            passive;
        }
        interface gr-0/0/0.0;
    }
}
ldp {
    interface gr-0/0/0.0;
    interface lo0.0;
}
}
routing-instances {
L3VPN-1 {
    instance-type vrf;
    interface ge-0/0/10.10;
    route-distinguisher 10.255.255.1:1000
    vrf-target {
        target:65100:1000;
        import target:65100:1000;
        export target:65100:1000;
    }
    vrf-table-label;
    routing-options {
        auto-export;
    }
}
VPLS_VPN-1 {
    instance-type vpls;
    interface ge-0/0/11.0;
    route-distinguisher 10.255.255.1:1001;
    vrf-target target:65100:1001;
    protocols {
        vpls {
            no-tunnel-services;
            site 1 {
                site-identifier 1;
                interface ge-0/0/11.0;
            }
            mac-tlv-receive;
            mac-tlv-send;
        }
    }
```

```
    }
}
```

Verification

Confirm that the configuration is working properly.

- Verifying That the Physical and Logical Interfaces Are Up on page 21
- Verifying the Fragmented IP Packet on the Outgoing Interface on page 22

Verifying That the Physical and Logical Interfaces Are Up

Purpose Verify that the physical and logical interfaces are up on the device.

Action From operational mode on the SRX Series Services Gateway, enter the **show interfaces terse** command.

```
user@host> show interfaces terse
 Interface               Admin Link Proto    Local                 Remote
ge-0/0/0                 up    up
ge-0/0/0.0               up    up   inet     1.1.1.1/30
                                            192.168.184.109/25
gr-0/0/0                 up    up
gr-0/0/0.0               up    up   inet     172.16.255.1/30
                                    mpls
ip-0/0/0                 up    up
lsq-0/0/0                up    up
lt-0/0/0                 up    up
ge-0/0/9                 up    down
ge-0/0/10                up    down
ge-0/0/10.10             up    down inet     192.168.0.1/24
ge-0/0/10.32767          up    down
ge-0/0/11                up    down
ge-0/0/11.0              up    down vpls
ge-0/0/11.32767          up    down
ge-0/0/12                up    down
ge-0/0/13                up    down
ge-0/0/14                up    down
ge-0/0/14.0              up    down inet
ge-0/0/15                up    down
fxp2                     up    up
fxp2.0                   up    up   tnp      0x1
gre                      up    up
ipip                     up    up
lo0                      up    up
lo0.0                    up    up   inet     10.255.184.109      --> 0/0
                                            10.255.255.1        --> 0/0
                                            127.0.0.1           --> 0/0
                                    inet6
st0                      up    up
st0.0                    up    up   inet     172.16.0.1/30
tap                      up    up
vlan                     up    up


<some output removed for brevity>
```

Meaning The output of the **show interfaces terse** command shows that all physical and logical interfaces used in this configuration are up and active.

Verifying the Fragmented IP Packet on the Outgoing Interface

Purpose Verify that the IP packet of 1500 bytes is created and sent to the outgoing interface ge-0/0/14.0.

Action From operational mode on the SRX Series Services Gateway, enter the **show interfaces ge-0/0/14.0 extensive**

```
user@host> show interfaces ge-0/0/14.0 extensive
Logical interface ge-0/0/14.0 (Index 79) (SNMP ifIndex 564) (Generation 144)
    Flags: Device-Down SNMP-Traps Encapsulation: ENET2
    Traffic statistics:
     Input  bytes  :                   0
     Output bytes  :                   0
     Input  packets:                   0
     Output packets:                   0
    Local statistics:
     Input  bytes  :                   0
     Output bytes  :                   0
     Input  packets:                   0
     Output packets:                   0
    Transit statistics:
     Input  bytes  :                   0                    0 bps
     Output bytes  :                   0                    0 bps
     Input  packets:                   0                    0 pps
     Output packets:                   0                    0 pps
    Security: Zone: Internet
    Allowed host-inbound traffic : bootp bfd bgp dns dvmrp igmp ldp msdp nhrp
ospf pgm pim rip router-discovery rsvp sap vrrp dhcp finger ftp tftp ident-reset
 http https ike netconf ping reverse-telnet
    reverse-ssh rlogin rpm rsh snmp snmp-trap ssh telnet traceroute xnm-clear-text
 xnm-ssl lsping ntp sip
    Flow Statistics :
    Flow Input statistics :
      Self packets :                    0
      ICMP packets :                    0
      VPN packets :                     0
      Multicast packets :               0
      Bytes permitted by policy :       0
      Connections established :         0
    Flow Output statistics:
      Multicast packets :               0
      Bytes permitted by policy :       0
    Flow error statistics (Packets dropped due to):
      Address spoofing:                 0
      Authentication failed:            0
      Incoming NAT errors:              0
      Invalid zone received packet:     0
      Multiple user authentications:    0
      Multiple incoming NAT:            0
      No parent for a gate:             0
      No one interested in self packets: 0
      No minor session:                 0
      No more sessions:                 0
      No NAT gate:                      0
      No route present:                 0
      No SA for incoming SPI:           0
      No tunnel found:                  0
      No session for a gate:            0
```



```
    No zone or NULL zone binding       0
    Policy denied:                     0
    Security association not active:   64
    TCP sequence number out of window: 0
    Syn-attack protection:             0
    User authentication errors:        0
  Protocol inet, MTU: 1500, Generation: 158, Route table: 0
    Flags: Sendbcast-pkt-to-re
    Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
      Destination: 1.1.1.0/30, Local: 1.1.1.1, Broadcast: 1.1.1.3, Generation:
154
```

Meaning The output of the **show interfaces ge-0/0/14.0 extensive** command shows that the fragmented IP packet of 1500 bytes is sent to outgoing interface ge-0/0/14.

Related Documentation

- Simplified MPLS Through IPsec over 1500-byte Media Overview on page 7
- Example: Configuring MPLS over GRE with IPsec Fragmentation and Reassembly on page 8