JUNIPER NETWORKS

Network Configuration Example

Configuring VPNs with Overlapping Subnets Using J Series Routers and SRX Series Devices

Release
12.3

Published: 2012-11-14

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

Network Configuration Example Configuring VPNs with Overlapping Subnets Using J Series Routers and SRX Series Devices
Release 12.3

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

Introduction

This document provides detailed information about and a step-by-step configuration example for VPNs with overlapping subnets using J Series Services Routers and SRX Series Services Gateways. This document is intended for network design and security engineers, as well as implementation partners who support customers who require secure connectivity over public networks. This document also discusses IPsec VPN configurations between J Series or SRX Series devices in a scenario where the subnets on both sides overlap.

Business Requirements for VPNs with Overlapping Subnets

The Juniper Networks Junos operating system (Junos OS) runs on J Series Services Routers and SRX Series Services Gateways, providing not only a powerful operating system but also a rich IP services tool kit. Junos OS has enhanced security and virtual private network (VPN) capabilities using Juniper's firewall/IPsec VPN platforms that include the Juniper Networks SSG Series Secure Services Gateways.

Configuring VPNs with overlapping subnets using J Series Services Routers and SRX Series Services Gateways enables your business to establish connectivity between separate sites that have the same private addressing scheme. This might be necessary in the case of a merger of two companies that use the same private addressing scheme or in the case of branch offices being consolidated.

Related Documentation

- VPNs with Overlapping Subnets Problem Scenario on page 1
- Example: Configuring VPNs with Overlapping Subnets Using J Series Routers and SRX Series Devices on page 5

VPNs with Overlapping Subnets Problem Scenario

Overview

The configuration of a services router running Junos OS for virtual private network (VPN) support is quite flexible. You can create route-based VPN tunnels and Network Address Translation (NAT) can be incorporated to provide solutions for certain problematic networking scenarios. This topic discusses one such problem scenario.

Problem Scenario

With corporate mergers, branch office consolidations, and partner collaborations being common, often an organization must create a VPN to another network that uses the same private address subnet. Because both networks use the same internal IP addresses, it is not possible to build a tunnel between these two sites. However, if the tunnel endpoints on both sides are Juniper services routers, it is possible to configure a tunnel between these sites with an advanced configuration using NAT.

Because the range of private IP addresses is relatively small, there is a good chance that the addresses of protected networks of two VPN peers overlap. For bidirectional VPN traffic between two end entities with overlapping addresses, the security devices at both ends of the tunnel must apply Source Network Address Translation (NAT-src) and Destination Network Address Translation (NAT-dst) to the VPN traffic passing between them.

NOTE: An overlapping address space is when the IP address range in two networks are partially or completely the same.

If a host is attached to a network with the IP address 192.168.10.0/24, and the other device on the remote end is attached to a network using the same IP address subnet, it is not possible to route the traffic through the tunnel. This is because all packets are routed based on the destination IP address. Before routing occurs, determine whether the destination IP address is on the same (local) network. If the destination IP address is on the same network, for example, 10.0.0.10, the destination address is resolved using the Address Resolution Protocol (ARP). However, if the destination IP address resides on a different network, the packet is sent to the next-hop router based on the routing table of the device.

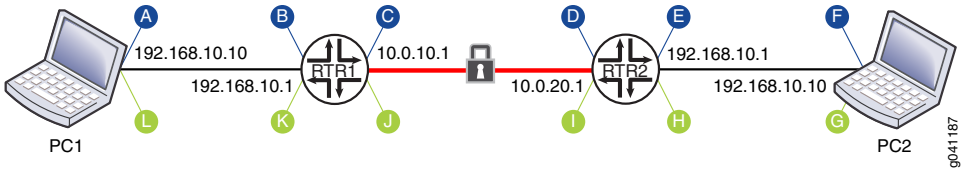
Because both the local and remote networks share the same IP addressing scheme, the packets are handled locally and not routed to the VPN tunnel. To overcome this situation, you can perform static NAT on the source IP address and destination IP address of all traffic destined for the remote network at the other end of the tunnel. For this reason, a route-based approach to IPsec VPNs is needed, because the creation of a virtual network interface on each services router is using a *secure tunnel* or the **st0** interface. Note that when configuring the scenario described in this section, source address and destination address is translated because the packet traverses the VPN tunnel to the end host. Therefore, the services routers at each end of the tunnel must contact each other using a newly created IP address network. You must be aware of this issue because it can introduce administrative problems with certain applications when migrating two networks with overlapping subnets.

This section describes how to configure route-based VPNs using source NAT and static NAT on the **st0** interface for both peers respectively. The scenario explained in this section references Figure 1 on page 2.

Source NAT and Static NAT is configured on tunnel interface at both sites respectively. Figure 1 on page 2 illustrates the packet flow.

The letters in the illustration correspond to the list of events.

Figure 1: Packet Flow Details



The following settings are assumed for the Corporate and Remote sites:

- PC1 (Computer 1) and RTR1 (Router 1) are at the Corporate site.
- PC2 (Computer 2) and RTR2 (Router 2) are at a Remote site with an IPsec VPN tunnel linking the two sites.
- Both PC1 and PC2 have IP address 192.168.10.10, and all network masks are /24 (255.255.255.0).

VPN traffic between sites with overlapping addresses requires address translation in both directions. Because the source address on outbound traffic cannot be the same as the destination address on inbound traffic, the addresses referenced in the inbound and outbound policies cannot be symmetrical.

A session is initiated to TCP port 80 from PC1 destined for PC2.

a. A packet leaves PC1 destined for 10.0.20.10 to reach the Remote site host PC2. Note that devices must attempt to reach devices at the remote end of the tunnel using the IP address network owned by the remote device tunnel interface. Based on the default gateway configuration of PC1, the next hop is 192.168.10.1, which is Router RTR1.

Source IP/Port	Destination IP/Port
192.168.10.10/1024	10.0.20.10/80

b. The packet arrives at the RTR1 internal interface with no change to the source or destination IP addresses or ports. The packet is then routed internally to the tunnel interface on RTR1.

Source IP/Port	Destination IP/Port
192.168.10.10/1024	10.0.20.10/80

c. When the packet reaches the RTR1 tunnel interface, a source NAT setting is applied. The source NAT setting is defined for the entire 10.0.10.0 network range. Therefore, all outgoing traffic from the 192.168.10.0 network destined for the tunnel interface is source-translated to a 10.0.10.0 equivalent address. The packet is encrypted when it is transmitted out of the RTR1 external interface, but the inner packet now has the source IP address changed to 10.0.10.10 (the port does not change with source NAT). Note that even though the source IP address is translated to a 10.0.10.0 address, the security policy still needs to have the original source IP address in the match objects.

Source IP/Port	Destination IP/Port
10.0.10.10/1024	10.0.20.10/80

d. The encrypted packet is received by the RTR2 external interface and is decrypted. The inner packet shows the source IP address as 10.0.10.10 and the destination IP address as 10.0.20.10. The packet is sent to the tunnel interface on RTR2.

Source IP/Port	Destination IP/Port
10.0.10.10/1024	10.0.20.10/80

e. Router RTR2 has static NAT defined on the tunnel interface, which covers the entire network range for the 10.0.20.0 network. Therefore, all traffic destined for the 10.0.20.0 network is destination-translated to an internal 192.168.10.0 equivalent address. The route lookup determines that the 192.168.10.0 network is routed to the RTR2 internal interface. The packet leaves the RTR2 internal interface with the destination IP address changed to 192.168.10.10.

Source IP/Port	Destination IP/Port
10.0.10.10/1024	192.168.10.10/80

f. Since PC2 has IP address 192.168.10.10, it receives the packet with the same source and destination IP addresses and ports as in **step e**.

   As shown in the previous steps, the original packet was both source and destination NAT translated before reaching PC2. Note that the NAT translations do not occur on the same device. Instead, one device performs the source address translation, and the remote device performs the destination address translation. The reply from PC2 back to PC1 follows similar steps in a reverse format as shown in **step g**.

g. The reply packet is sent by PC2 to 10.1.10.10 to reach host PC1. Based on the default gateway configuration of PC2, the next hop is 192.168.10.1, which is RTR2.

Source IP/Port	Destination IP/Port
192.168.10.10/80	10.0.10.10/1024

h. The packet arrives at the RTR2 internal interface with no change to the source or destination IP addresses or ports.

Source IP/Port	Destination IP/Port
192.168.10.10/80	10.0.10.10/1024

i. The packet matches the existing session in RTR2 where static NAT is defined. Therefore, the traffic from the 192.168.10.0 network destined for the tunnel interface is source-translated to a 10.0.20.0 equivalent address. The packet is encrypted when

it leaves the RTR2 external interface, but the inner packet now has the source IP address changed to 10.0.20.10.

Source IP/Port	Destination IP/Port
10.0.20.10/80	10.0.10.10/1024

j. The packet arrives at the RTR1 external interface and is decrypted. The inner packet has a source IP address of 10.0.20.10 and a destination IP address of 10.0.10.10.

Source IP/Port	Destination IP/Port
10.0.20.10/80	10.0.10.10/1024

k. The packet matches the existing session on RTR1 where source NAT is defined. Thus, the traffic destined for the 10.0.10.0 network translates to an internal 192.168.10.0 equivalent address. The packet leaves the RTR1 internal interface with the destination IP address changed to 192.168.10.10.

Source IP/Port	Destination IP/Port
10.0.20.10/80	192.168.10.10/1024

l. The packet arrives at PC1 with the same source and destination IP addresses and ports as in **step k**.

Related Documentation

- Business Requirements for VPNs with Overlapping Subnets on page 1
- Example: Configuring VPNs with Overlapping Subnets Using J Series Routers and SRX Series Devices on page 5

Example: Configuring VPNs with Overlapping Subnets Using J Series Routers and SRX Series Devices

This example shows how to configure and verify VPNs with overlapping subnets.

Requirements

This example requires the following hardware and software components:

- Junos OS Release 9.5 or later
- Juniper Networks SRX Series Services Gateways or J Series Services Routers

Overview

This example shows how to configure and verify VPN with overlapping subnets.

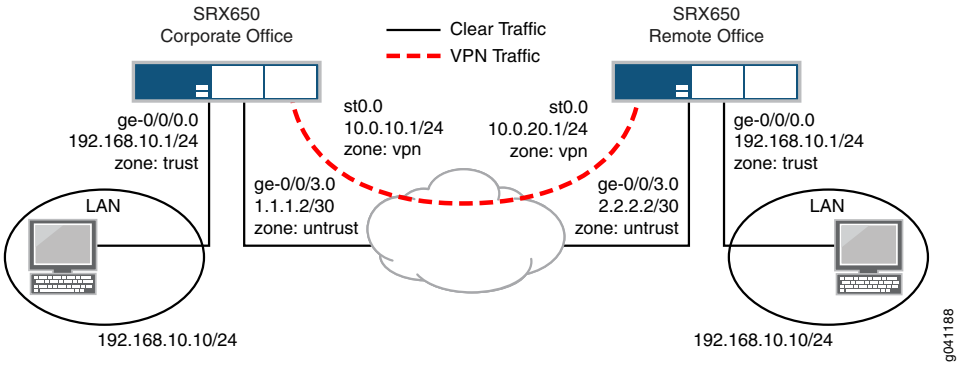
NOTE:

- Configuration and troubleshooting details of route-based virtual private networks (VPNs) and other Junos OS-specific documents are available at the Juniper Networks Knowledge Base at http://kb.juniper.net .
- For more information about VPN configuration and troubleshooting, see KB10182 (http://kb.juniper.net/KB10182) available at the Juniper Networks Knowledge Base.

Topology

Figure 2 on page 6 shows the network topology used in this configuration example.

Figure 2: Network Topology



This example requires the following:

- The internal LAN interface for both sites is **ge-0/0/0** in zone **trust** and has 192.168.10.1/24 as the private IP address.
- The Internet interface for both sites is **ge-0/0/3** in zone **untrust** and each site has a unique public IP address.
- The **st0.0** secure tunnel interface is in zone **vpn** on both sites to allow configuring unique policies specifically for tunnel (encrypted) traffic while maintaining unique policies for clear (non-encrypted) traffic.
- The address range to reach the Remote site hosts from the Corporate site is 10.0.20.0/24.
- The address range to reach Corporate site hosts from the Remote site is 10.0.10.0/24.

- All traffic between the Corporate and Remote LANs is permitted, and traffic might be initiated from either side.
- Basic non-VPN settings such as system settings, user login, and default security settings are preconfigured on both devices.

Configuration

To configure VPN with overlapping subnets involves:

Configuring the Basic Parameters on Corporate and Remote Sites

Step-by-Step Procedure

1. Configure the IP addresses for the **ge-0/0/0.0**, **ge-0/0/3.0**, and **st0.0** interfaces.
2. Configure a default route to the Internet next hop and also a static route for the remote office LAN.

   Optionally, you can use a dynamic routing protocol such as OSPF, but that is beyond the scope of this document.
3. Configure a security zone and bind the interfaces to the appropriate zones.
4. Enable the necessary host-inbound services on the interfaces or the zone.

   For this example, you must enable Internet Key Exchange (IKE) service on either the **ge-0/0/3** interface or the **untrust** zone.
5. Configure address book entries for each zone.

   This is necessary for the security policies.
6. Configure the phase 1 (IKE) proposal.
7. Configure an IKE policy referencing the phase 1 proposal in step 6.
8. Configure an IKE gateway profile referencing the IKE policy in step 7.
9. Configure a phase 2 (IPsec) proposal.
10. Configure an IPsec policy referencing the phase 2 proposal in step 9.
11. Configure a VPN profile referencing the IPsec policy in step 10 and the IKE gateway in step 8.
12. Bind interface **st0.0** to the VPN.

    This makes the VPN a route-based VPN.
13. Configure source NAT settings for the **st0** interface.

14. Configure security policies to permit remote VPN traffic into the corporate LAN and vice versa.

15. Configure the TCP Maximum Segment Size (**tcp-mss**) for IPsec traffic to eliminate the possibility of fragmented TCP traffic.

    This lessens the resource utilization on the device.

Configuring the Corporate Site

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

1. Configure IP addresses for the private LAN, Internet, and **st0** interfaces.

```
[edit]
user@CORPORATE# set interfaces ge-0/0/0 unit 0 family inet address
  192.168.10.1/24
user@CORPORATE# set interfaces ge-0/0/3 unit 0 family inet address 1.1.1.2/24
user@CORPORATE# set interfaces st0 unit 0 family inet address 10.0.10.1/24
```

   Junos OS uses the concept of units for the logical component of an interface. In this example, unit 0 and family inet (IPv4) are used. It is not mandatory for **st0** interfaces on both sides to reside on the same IP address subnet, since the link is logically a point-to-point link.

2. Configure a default route and a route for the tunnel traffic.

```
[edit]
user@CORPORATE# set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1
user@CORPORATE# set routing-options static route 10.0.20.0/24 next-hop st0.0
```

   Normally, for static routes, the gateway IP address is specified as the next hop. For route-based VPNs, specify the remote peer **st0** interface IP address or just the local **st0** interface as the next hop.

3. Configure security zones, and assign interfaces to the zones.

```
[edit]
user@CORPORATE# set security zones security-zone trust interfaces ge-0/0/0.0
user@CORPORATE# set security zones security-zone untrust interfaces ge-0/0/3.0
user@CORPORATE# set security zones security-zone vpn interfaces st0.0
```

   Creating a unique zone for tunnel traffic enables you to create a set of policies specifically for VPN traffic while maintaining separation of policies for non-VPN traffic. Also, you can create *deny policies* to exclude specific hosts to access the VPN.

NOTE: If you are terminating the st0 interface in the same zone as the trusted LAN and if a policy exists to allow intra-zone traffic on that zone, no additional security policies are required.

4. Configure host-inbound services for each interface in the zones.

```
[edit]
user@CORPORATE# set security zones security-zone trust interfaces ge-0/0/0
  host-inbound-traffic system-services all
user@CORPORATE# set security zones security-zone untrust interfaces ge-0/0/3
  host-inbound-traffic system-services ike
user@CORPORATE# set security zones security-zone vpn interfaces st0.0
  host-inbound-traffic system-services all
```

Host-inbound services are for traffic destined for the Junos OS-based device. This includes but is not limited to FTP, HTTP, HTTPS, IKE, ping, rlogin, RSH, SNMP, SSH, Telnet, Trivial File Transfer Protocol (TFTP), and traceroute. This example assumes that you want to allow all such services from zone **trust**. For security reasons, only allow IKE on the Internet facing zone **untrust**, which is required for IKE negotiations to occur. Other services such as those for management, or troubleshooting, or both can also be individually enabled if required.

5. Configure address book entries for each zone.

```
[edit]
user@CORPORATE# set security zones security-zone trust address-book address
  local-net 192.168.10.0/24
user@CORPORATE# set security zones security-zone trust address-book address
  source-nat-net 10.0.10.0/24
user@CORPORATE# set security zones security-zone vpn address-book address
  remote-net 10.0.20.0/24
```

This example uses address book object names **local-net** and **remote-net** to define the Corporate to Remote LAN segments. However, in order to permit all traffic from the reverse direction, the address book object needs to reflect the source NAT address range for **st0.0**. This is because the traffic egressing out from the Remote site to reach the Corporate site has a destination address of 10.0.10.0/24, not 192.168.10.0/24.

6. Configure the IKE phase 1 proposal.

```
[edit]
user@CORPORATE# set security ike proposal p1-prop1 authentication-method
  pre-shared-keys
user@CORPORATE# set security ike proposal p1-prop1 dh-group group2
user@CORPORATE# set security ike proposal p1-prop1 authentication-algorithm
  sha1
user@CORPORATE# set security ike proposal p1-prop1 encryption-algorithm
  3des-cbc
```

This example uses a proposal that includes preshared keys, group2, triple Data Encryption Standard (3DES), and the sha1 algorithm. Define your proposal in accordance with your Corporate security policy.

7. Configure the IKE policy.

```
[edit]
user@CORPORATE# set security ike policy ike-policy1 mode main
user@CORPORATE# set security ike policy ike-policy1 proposals p1-prop1
user@CORPORATE# set security ike policy ike-policy1 pre-shared-key ascii-text
  "secretkey"
```

The IKE policy specifies main mode, which is most commonly used for site-to-site VPNs where both peers have static IP addresses. Aggressive mode is typically used when one peer is a dynamic peer. For both peers, the mode must match. In the IKE policy, both the phase 1 proposal and preshared key are defined.

8. Configure the IKE gateway (phase 1) with the peer IP address and peer ID type.

```
[edit]
user@CORPORATE# set security ike gateway remote-ike ike-policy ike-policy1
user@CORPORATE# set security ike gateway remote-ike address 2.2.2.2
user@CORPORATE# set security ike gateway remote-ike external-interface
  ge-0/0/3.0
```

A remote IKE peer can be identified by either the IP address, the FQDN/u-FQDN, or the ASN1-DN (PKI certificates). This example identifies the peer by IP address. Therefore, the gateway address must be the remote peer's public IP address. Also, it is important to specify the correct external interface. If either the peer address or external interface specified is incorrect, then the IKE gateway is not properly identified during phase 1 negotiations.

9. Configure the IPsec phase 2 proposal.

```
[edit]
user@CORPORATE# set security ipsec proposal p2-prop1 protocol esp
user@CORPORATE# set security ipsec proposal p2-prop1 authentication-algorithm
  hmac-sha1-96
user@CORPORATE# set security ipsec proposal p2-prop1 encryption-algorithm
  3des-cbc
user@CORPORATE# set security ipsec proposal p2-prop1 lifetime-seconds 3600
```

This example uses a proposal that includes Encapsulating Security Payload (ESP), 3DES encryption, the sha1 algorithm, and a lifetime of 3600 seconds (1 hour). Define your proposal in accordance with your Corporate security policy.

10. Configure the IPsec policy.

```
[edit]
user@CORPORATE# set security ipsec policy vpn-policy1 perfect-forward-secrecy
  keys group2
user@CORPORATE# set security ipsec policy vpn-policy1 proposals p2-prop1
```

The VPN policy must specify a phase 2 proposal. Perfect-forward-secrecy is optional, though recommended for increased security.

11. Configure an IPsec VPN with an IKE gateway and IPsec policy, and bind it to the **st0** interface.

```
[edit]
user@CORPORATE# set security ipsec vpn remote-vpn ike gateway remote-ike
user@CORPORATE# set security ipsec vpn remote-vpn ike ipsec-policy vpn-policy1
user@CORPORATE# set security ipsec vpn remote-vpn bind-interface st0.0
```

Binding an **st0** interface differentiates this VPN as a route-based VPN. For policy-based VPNs, you do not configure an **st0** interface. If an **st0** interface is not specified, phase 2 cannot complete negotiations if this is a route-based VPN.

12. Configure source NAT for the **st0** interface.

```
[edit]
```



```
user@CORPORATE# set security nat source rule-set nat from zone trust
user@CORPORATE# set security nat source pool pool1 address 10.0.10.10/24
user@CORPORATE# set security nat source rule-set nat from zone lan
user@CORPORATE# set security nat source rule-set nat to interface st0.0
user@CORPORATE# set security nat source rule-set nat rule 1 match source-address
  192.168.10.0/24
user@CORPORATE# set security nat source rule-set nat rule 1 then source-nat pool
  pool1
```

13. Configure security policies for tunnel traffic in both directions.

```
[edit security policies from-zone trust to-zone vpn]
user@CORPORATE# set policy remote-vpn-outgoing match source-address local-net
user@CORPORATE# set policy remote-vpn-outgoing match destination-address
  remote-net
user@CORPORATE# set policy remote-vpn-outgoing match application any
user@CORPORATE# set policy remote-vpn-outgoing then permit

[edit security policies from-zone vpn to-zone trust]
user@CORPORATE# set policy remote-vpn-incoming match source-address
  remote-net
user@CORPORATE# set policy remote-vpn-incoming match destination-address
  static-nat-net
user@CORPORATE# set policy remote-vpn-incoming match application any
user@CORPORATE# set policy remote-vpn-incoming then permit
```

A security policy permits traffic in one direction, but also allows all reply traffic without the need for a reverse direction policy. However, since traffic can be initiated from either direction, bidirectional policies are required. Also, you can create more granular policies between zone **vpn** and zone **trust** and can permit or deny traffic accordingly. Note that the policies are regular non-tunnel policies. Therefore, the policies do not specify the IPsec profile. Although the static NAT policy is bidirectional, security policies are still required to actually permit the traffic in both directions.

14. Configure a source NAT rule and a security policy for Internet traffic.

A security policy is required to permit all traffic from zone **trust** to zone **untrust**.

The device uses the specified source-nat interface, and translates the source IP address and port for outgoing traffic. This is accomplished by using the IP address of the egress interface as the source IP address and a random higher port for the source port. If required, you can create more granular policies to permit or deny certain traffic.

```
[edit security nat source rule-set nat-out]
user@CORPORATE# set from zone trust
user@CORPORATE# set to zone untrust
user@CORPORATE# set rule interface-nat match source-address 192.168.10.0/24
user@CORPORATE# set rule interface-nat match destination-address 0.0.0.0/0
user@CORPORATE# set rule interface-nat then source-nat interface

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

15. Configure **tcp-mss** to eliminate fragmentation of TCP traffic across the tunnel.

```
[edit]
user@CORPORATE# set security flow tcp-mss ipsec-vpn mss 1350
```

The **tcp-mss** parameter is negotiated as part of the TCP 3-way handshake. It limits the maximum size of a TCP segment to better fit the maximum transmission unit (MTU) limits on a network. This is especially important for VPN traffic, because the IPsec encapsulation overhead along with the IP address and frame overhead can cause the resulting ESP packet to exceed the MTU of the physical interface, causing fragmentation. Always avoid fragmentation because it increases the bandwidth and device resources. To obtain optimal performance, experiment with different **tcp-mss** values.

NOTE: For most Ethernet-based networks, we recommend having a starting value of 1350 with an MTU of 1500 or greater. You can alter the starting value if any device in the path has a lower MTU, or if there is any added overhead such as the Point-to-Point Protocol (PPP), Frame Relay, and so on.

Results For reference, the configuration of the Corporate site router is shown.

Corporate Site Configuration

```
user@CORPORATE> show configuration | no-more

## Last commit: 2011-12-14 02:57:15 PST by root
version 11.4R1;
system {
    host-name CORPORATE;
    time-zone America/Los_Angeles;
    root-authentication {
        encrypted-password "$sha1$18784$qLOsJ7qe$P/yFiwCAYw/JFS3YU4FIxIKE538Q";
## SECRET-DATA
    }
    name-server {
        4.2.2.1;
        4.2.2.2;
    }
    login {
        user admin {
            uid 2002;
            class super-user;
            authentication {
                encrypted-password "$1$Qq/O/sl7$JzYRvw.J8ljcztgFE2jrR1"; ##
SECRET-DATA
            }
        }
        user netscreen {
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "$1$KSl7udq1$Q6pSTOhBjakONxxLUsYS31"; ##
SECRET-DATA
            }
        }
```

```
    }
    services {
        ssh;
        telnet;
        web-management {
            http {
                interface [ ge-0/0/0.0 ge-0/0/3.0 ];
            }
        }
        dhcp {
            router {
                192.168.1.4;
            }
            pool 192.168.1.0/24 {
                address-range low 192.168.1.5 high 192.168.1.100;
            }
        }
    }
syslog {
        user * {
            any emergency;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
    }
    max-configuration-rollbacks 20;
    license {
        autoupdate {
            url https://www.juniper.net/key_retrieval;
        }
    }
    processes {
        wireless-lan-service {
            traceoptions {
                file wland;
                flag all;
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 192.168.10.1/24;
            }
        }
    }
    ge-0/0/3 {
        unit 0 {
            family inet {
                address 1.1.1.2/24;
            }
        }
    }
    st0 {
```

```
        unit 0 {
            family inet {
                address 10.0.10.1/24;
            }
        }
    }
}
routing-options {
    static {
        inactive: route 0.0.0.0/0 next-hop 10.100.37.1;
        route 2.2.2.0/30 next-hop 1.1.1.1;
        route 10.0.20.0/24 next-hop st0.0;
    }
}
security {
    ike {
        traceoptions {
            file iked;
            flag all;
            level 15;
        }
        proposal ike_prop {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 36500;
        }
        policy ike_pol {
            proposals ike_prop;
            pre-shared-key ascii-text "$9$G3jqf3nCO1h9AOIhcMWNdbs2a5T3"; ##
SECRET-DATA
        }
        gateway ike_gate {
            ike-policy ike_pol;
            address 2.2.2.2;
            external-interface ge-0/0/2.0;
        }
    }
    ipsec {
        proposal ipsec_prop {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 7200;
        }
        policy ipsec_pol {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec_prop;
        }
        vpn rb_vpn {
            bind-interface st0.0;
            ike {
                gateway ike_gate;
                ipsec-policy ipsec_pol;
            }
            establish-tunnels immediately;
        }
    }
```

```
    alg {
        sip retain-hold-resource;
    }
    utm {
        custom-objects {
            url-pattern {
                urllist3 {
                    value [ http://www.juniper.net http://xyz.com ];
                }
                urllist4 {
                    value http://www.abc.com;
                }
                urllist5 {
                    value [ http://www.juniper.net 1.2.3.4 ];
                }
                urllist6 {
                    value [ http://www.acmegizmo.com 1.2.3.4 ];
                }
            }
            custom-url-category {
                custurl3 {
                    value urllist3;
                }
                custurl4 {
                    value urllist4;
                }
                custurl5 {
                    value urllist5;
                }
                custurl6 {
                    value urllist6;
                }
            }
        }
        feature-profile {
            web-filtering {
                url-whitelist custurl4;
                url-blacklist custurl4;
                type juniper-local;
                juniper-local {
                    profile localprofile1 {
                        default permit;
                        custom-block-message "Access to this site is not
permitted.";
                        fallback-settings {
                            default block;
                            too-many-requests block;
                        }
                    }
                }
            }
            content-filtering {
                profile contentfilter1;
            }
        }
        utm-policy utmp5 {
            content-filtering {
                http-profile contentfilter1;
            }
            web-filtering {
                http-profile localprofile1;
```

```
        }
    }
}
flow {
    traceoptions {
        file my-nat-trace;
        flag basic-datapath;
        flag all;
        packet-filter client-traffic {
            source-prefix 192.168.0.1/32;
        }
    }
}
screen {
    ids-option untrust-screen {
        icmp {
            ping-death;
        }
        ip {
            source-route-option;
            tear-drop;
        }
        tcp {
            syn-flood {
                alarm-threshold 1024;
                attack-threshold 200;
                source-threshold 1024;
                destination-threshold 2048;
                queue-size 2000; ## Warning: 'queue-size' is deprecated
                timeout 20;
            }
            land;
        }
    }
}
nat {
    source {
        pool pool1 {
            address {
                10.0.10.10/24;
            }
        }
        rule-set nat {
            from zone trust;
            to zone vpn;
            rule 1 {
                match {
                    source-address 192.168.10.0/24;
                }
                then {
                    source-nat {
                        pool {
                            pool1;
                        }
                    }
                }
            }
        }
    }
}
policies {
```

```
            from-zone trust to-zone vpn {
                policy remote-vpn-outgoing {
                    match {
                        source-address local_net;
                        destination-address remote_net;
                        application any;
                    }
                    then {
                        permit;
                    }
                }
            }
        }
        zones {
            security-zone untrust {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                }
                interfaces {
                    ge-0/0/3.0;
                }
            }
            security-zone trust {
                address-book {
                    address local_net 192.168.10.0/24;
                    address nat_net 10.0.10.0/24;
                }
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                }
                interfaces {
                    ge-0/0/1.0;
                }
            }
            security-zone vpn {
                address-book {
                    address remote_net 10.0.20.0/24;
                }
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                }
                interfaces {
                    st0.0;
                }
            }
        }
    }
    wlan {
        access-point silver {
            mac-address 00:12:cf:c7:5d:c0;
            access-point-options {
                country {
                    US;
                }
            }
```

```
    }
}
vlans {
    vlan-trust {
        vlan-id 3;
    }
}
```

Configuring the Remote Site

Step-by-Step Procedure

Most of the Corporate site configuration applies to the Remote site as well. Therefore, the same information is not repeated in this example unless some specific details for the Remote site need to be pointed out. To begin, enter configuration mode using either the **configure** or **edit** command.

1. Configure IP addresses for the private LAN, Internet, and **st0** interfaces.

   ```
   [edit]
   user@REMOTE# set interfaces ge-0/0/0 unit 0 family inet address 192.168.10.1/24
   user@REMOTE# set interfaces ge-0/0/3 unit 0 family inet address 2.2.2.2/24
   user@REMOTE# set interfaces st0 unit 0 family inet address 10.0.20.1/24
   ```

   See "Configuring the Corporate Site" on page 8 for details.

2. Configure a default route and a route for the tunnel traffic.

   ```
   [edit]
   user@REMOTE# set routing-options static route 0.0.0.0/0 next-hop 2.2.2.1
   user@REMOTE# set routing-options static route 10.0.10.0/24 next-hop st0.0
   ```

   See "Configuring the Corporate Site" on page 8 for details.

3. Configure security zones, and assign interfaces to the zones.

   ```
   [edit]
   user@REMOTE# set security zones security-zone trust interfaces ge-0/0/0.0
   user@REMOTE# set security zones security-zone untrust interfaces ge-0/0/3.0
   user@REMOTE# set security zones security-zone vpn interfaces st0.0
   ```

   See "Configuring the Corporate Site" on page 8 for details.

4. Configure host-inbound services for each interface in the zones.

   ```
   [edit]
   user@REMOTE# set security zones security-zone trust interfaces ge-0/0/0
     host-inbound-traffic system-services all
   user@REMOTE# set security zones security-zone untrust interfaces ge-0/0/3
     host-inbound-traffic system-services ike
   user@REMOTE# set security zones security-zone vpn interfaces st0.0
     host-inbound-traffic system-services all
   ```

   See "Configuring the Corporate Site" on page 8 for details.

5. Configure address book entries for each zone.

   ```
   [edit]
   user@REMOTE# set security zones security-zone trust address-book address
     local-net 192.168.10.0/24
   user@REMOTE# set security zones security-zone trust address-book address
     static-nat-net 10.0.20.0/24
   ```

```
user@REMOTE# set security zones security-zone vpn address-book address corp-net
  10.0.10.0/24
```

See "Configuring the Corporate Site" on page 8 for details. However, for the Remote site, the static NAT network is 10.0.20.0/24.

6. Configure the IKE phase 1 proposal.

```
[edit]
user@REMOTE# set security ike proposal p1-prop1 authentication-method
  pre-shared-keys
user@REMOTE# set security ike proposal p1-prop1 dh-group group2
user@REMOTE# set security ike proposal p1-prop1 authentication-algorithm sha1
user@REMOTE# set security ike proposal p1-prop1 encryption-algorithm 3des-cbc
```

NOTE: The proposal must match the peer side exactly or phase 1 fails.

7. Configure the IKE policy.

```
[edit]
user@REMOTE# set security ike policy ike-policy1 mode main
user@REMOTE# set security ike policy ike-policy1 proposals p1-prop1
user@REMOTE# set security ike policy ike-policy1 pre-shared-key ascii-text secretkey
```

NOTE: Ensure that the preshared key matches exactly with the peer side.

8. Configure the IKE gateway (phase 1) with the peer IP address and peer ID type.

```
[edit]
user@REMOTE# set security ike gateway corp-ike ike-policy ike-policy1
user@REMOTE# set security ike gateway corp-ike address 1.1.1.2
user@REMOTE# set security ike gateway corp-ike external-interface ge-0/0/3.0
```

Since both peers have static IP addresses, you can use the IP address as the peer ID type. If one peer has a dynamic IP address, then the IKE peer needs to be identified by either the domain name (FQDN), email address (u-FQDN), or distinguished name (ASN1-DN).

9. Configure an IPsec phase 2 proposal.

```
[edit]
user@REMOTE# set security ipsec proposal p2-prop1 protocol esp
user@REMOTE# set security ipsec proposal p2-prop1 authentication-algorithm
  hmac-sha1-96
user@REMOTE# set security ipsec proposal p2-prop1 encryption-algorithm 3des-cbc
user@REMOTE# set security ipsec proposal p2-prop1 lifetime-seconds 3600
```

NOTE: The proposal must match the peer side exactly or phase 2 fails.

10. Configure an IPsec policy.

```
[edit]
user@REMOTE# set security ipsec policy vpn-policy1 perfect-forward-secrecy keys
  group2
user@REMOTE# set security ipsec policy vpn-policy1 proposals p2-prop1
```

If the remote peer is configured for perfect-forward-secrecy, it must be configured in this step.

11. Configure an IPsec VPN with an IKE gateway and IPsec policy, and bind it to the **st0** interface.

```
[edit]
user@REMOTE# set security ipsec vpn corp-vpn ike gateway corp-ike
user@REMOTE# set security ipsec vpn corp-vpn ike ipsec-policy vpn-policy1
user@REMOTE# set security ipsec vpn corp-vpn bind-interface st0.0
user@REMOTE# set security ipsec vpn corp-vpn establish-tunnels immediately
```

See "Configuring the Corporate Site" on page 8 for details.

12. Configure static NAT for the **st0** interface.

```
[edit]
user@REMOTE# set security nat source rule-set nat from zone trust
user@REMOTE# set security nat source pool pool1 address 10.0.20.10/24
user@REMOTE# set security nat source rule-set nat from zone lan
user@REMOTE# set security nat source rule-set nat to interface st0.0
user@REMOTE# set security nat source rule-set nat rule 1 match source-address
  192.168.10.10/24
user@REMOTE# set security nat source rule-set nat rule 1 then source-nat pool pool1
```

Similar to Corporate site settings, map the entire 10.0.20.10/24 subnet with the remote LAN 192.168.10.10/24 subnet. This is again a one-to-one mapping for each host on the subnet to the other. You do not need to perform any port translations in this instance.

13. Configure security policies for tunnel traffic in both directions.

```
[edit security policies from-zone trust to-zone vpn]
user@REMOTE# set policy corp-vpn-outgoing match source-address local-net
user@REMOTE# set policy corp-vpn-outgoing match destination-address corp-net
user@REMOTE# set policy corp-vpn-outgoing match application any
user@REMOTE# set policy corp-vpn-outgoing then permit

[edit security policies from-zone vpn to-zone trust]
user@REMOTE# set policy corp-vpn-incoming match source-address corp-net
user@REMOTE# set policy corp-vpn-incoming match destination-address
  static-nat-net
user@REMOTE# set policy corp-vpn-incoming match application any
user@REMOTE# set policy corp-vpn-incoming then permit
```

See "Configuring the Corporate Site" on page 8 for details.

14. Configure a source NAT rule and a security policy for Internet traffic.

```
[edit security nat source rule-set nat-out]
user@REMOTE# set from zone trust
user@REMOTE# set to zone untrust
user@REMOTE# set rule interface-nat match source-address 192.168.10.10/24
```

```
user@REMOTE# set rule interface-nat match destination-address 0.0.0.0/0
user@REMOTE# set rule interface-nat then source-nat interface

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

See "Configuring the Corporate Site" on page 8 for details.

15. Configure the **tcp-mss** parameter to eliminate fragmentation of TCP traffic across the tunnel.

```
[edit]
user@REMOTE# set security flow tcp-mss ipsec-vpn mss 1350
```

See "Configuring the Corporate Site" on page 8 for details.

For reference, the configuration of the Remote site router is shown.

Remote Site Configuration

```
user@REMOTE> show configuration | no-more

## Last commit: 2011-12-13 23:06:50 GMT-8 by root
version 11.4R1;
system {
    host-name REMOTE;
    time-zone GMT-8;
    root-authentication {
        encrypted-password "$sha1$19062$9aSvd7DT$y4rgkDG4H5cgR381bbDnBgv8nihZ";
## SECRET-DATA
    }
    name-server {
        4.2.2.1;
        4.2.2.2;
    }
    login {
        user admin {
            uid 2005;
            class super-user;
            authentication {
                encrypted-password "$1$iltZokFW$OO8iKKAdREqgfPmuhP5KX0"; ##
SECRET-DATA
            }
        }
        user netscreen {
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "$1$5z3lCZd2$KaPzg8oAoFrK26742QXp9/"; ##
SECRET-DATA
            }
        }
    }
    services {
        ftp;
        ssh;
        telnet;
        web-management {
            http {
                interface [ vlan.0 ge-0/0/0.0 ];
```

```
            }
            https {
                system-generated-certificate;
                interface vlan.0;
            }
        }
    }
    syslog {
        archive size 100k files 3;
        user * {
            any emergency;
        }
        file messages {
            any critical;
            authorization info;
        }
        file interactive-commands {
            interactive-commands error;
        }
    }
    max-configurations-on-flash 5;
    max-configuration-rollbacks 20;
    license {
        autoupdate {
            url https://www.juniper.net/key_retrieval;
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.100.37.220/24;
            }
        }
    }
    fe-0/0/2 {
        unit 0 {
            family inet {
                address 192.168.10.1/24;
            }
        }
    }
    ge-0/0/3 {
        unit 0 {
            family inet {
                address 2.2.2.2/24;
            }
        }
    }
    st0 {
        unit 0 {
            family inet {
                address 10.0.20.1/24;
            }
        }
    }
}
routing-options {
    static {
        inactive: route 0.0.0.0/0 next-hop [ 10.100.37.1 1.1.1.1 ];
```

```
        route 1.1.1.0/30 next-hop 2.2.2.1;
        route 10.0.10.0/24 next-hop st0.0;
    }
}
protocols {
    ospf {
        export test;
    }
}
policy-options {
    policy-statement test {
        term 1 {
            from protocol direct;
        }
    }
}
security {
    ike {
        traceoptions {
            file iked;
            flag all;
        }
        proposal ike_prop {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 36500;
        }
        policy ike_pol {
            proposals ike_prop;
            pre-shared-key ascii-text "$9$9uzTtORrlMx-wvWxdwsZGk.P5QnEhr"; ##
SECRET-DATA
        }
        gateway ike_gate {
            ike-policy ike_pol;
            address 1.1.1.2;
            external-interface fe-0/0/3.0;
        }
    }
    ipsec {
        traceoptions {
            flag all;
        }
        proposal ipsec_prop {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 7200;
        }
        policy ipsec_pol {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec_prop;
        }
        vpn rb_vpn {
            bind-interface st0.0;
            ike {
                gateway ike_gate;
                ipsec-policy ipsec_pol;
```

```
        }
        establish-tunnels immediately;
    }
}
alg {
    h323;
}
forwarding-options {
    family {
        inet6 {
            mode flow-based;
        }
    }
}
flow {
    tcp-mss {
        ipsec-vpn {
            mss 1350;
        }
    }
}
screen {
    ids-option untrust-screen {
        icmp {
            ping-death;
        }
        ip {
            source-route-option;
            tear-drop;
        }
        tcp {
            syn-flood {
                alarm-threshold 1024;
                attack-threshold 200;
                source-threshold 1024;
                destination-threshold 2048;
                timeout 20;
            }
            land;
        }
    }
}
nat {
    static {
        rule-set nat {
            from zone vpn;
            rule 1 {
                match {
                    destination-address 10.0.20.10/24;
                }
                then {
                    static-nat prefix 192.168.10.10/24;
                }
            }
        }
    }
}
policies {
    from-zone vpn to-zone trust {
        policy corp-vpn-incoming {
            match {
```

```
                    source-address remote_net;
                    destination-address local_net;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
    }
    zones {
        security-zone untrust {
            host-inbound-traffic {
                system-services {
                    all;
                }
            }
            interfaces {
                ge-0/0/0.0;
            }
        }
        security-zone trust {
            address-book {
                address local_net 192.168.10.10/24;
                address nat_net 10.0.20.0/24;
            }
            host-inbound-traffic {
                system-services {
                    all;
                }
            }
            interfaces {
                ge-0/0/3.0;
            }
        }
        security-zone vpn {
            address-book {
                address remote_net 10.0.10.0/24;
            }
            host-inbound-traffic {
                system-services {
                    all;
                }
            }
            interfaces {
                st0.0;
            }
        }
    }
}
routing-instances {
    cust-e {
        instance-type virtual-router;
        routing-options {
            static {
                route 1.1.1.0/29 next-hop 10.0.2.6;
                route 192.168.9.0/24 discard;
            }
            autonomous-system 65200;
        }
        protocols {
```

```
            inactive: bgp {
                group provider-ebgp {
                    type external;
                    multihop {
                        ttl 2;
                    }
                    export cust-e-export;
                    peer-as 65000;
                    neighbor 1.1.1.1;
                }
            }
        }
    }
}
services {
    unified-access-control {
        infranet-controller infranet-controller-2 {
            address 10.64.106.29;
            port 11123;
            interface ge-0/0/3.0;
            password "$9$6TOx/pBIRSeMXhS4ZjqQzhSrlK8"; ## SECRET-DATA
        }
    }
}
```

Verification

Confirm that the configuration is working properly.

Verifying the VPN Connection — Confirm IKE (Phase 1) Status

Purpose Confirm the VPN connection by checking the status of IKE phase 1 security associations.

Action Use the following command from the Corporate site's services router:

```
user@CORPORATE> show security ike security-associations

Index  Remote Address   State  Initiator cookie   Responder cookie   Mode
3    2.2.2.2      UP   744a594d957dd513   1e1307db82f58387   Main
```

The output shows that the remote peer is **2.2.2.2**, and the state shown is **UP**. If the state shown is **DOWN** or if there are no IKE security associations shown, then there is a problem with phase 1 establishment. Confirm that the remote IP address, IKE policy, and external interfaces are all correct. Common errors include incorrect IKE policy parameters such as wrong mode type (aggressive or main), pre-shared key, or phase 1 proposals (all parameters must match on both peers). An incorrect external interface is another common misconfiguration. This interface must be the interface that receives the IKE packets. If configurations are checked and are set correctly, then check the **kmd log** for any errors.

Note the index number in the output. The index number generated is 3 in this example. This value is unique for each IKE security association and allows you to get more details from that particular security association (SA) as shown here:

```
user@CORPORATE> show security ike security-associations index 3 detail

IKE peer 2.2.2.2, Index 3,
Role: Responder, State: UP
Initiator cookie: 744a594d957dd513, Responder cookie: 1e1307db82f58387
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 1.1.1.2:500, Remote: 2.2.2.2:500
Lifetime: Expires in 28570 seconds
Algorithms:
Authentication     : sha1
Encryption       : 3des-cbc
Pseudo random function: hmac-sha1
Traffic statistics:
Input bytes    : 852
Output bytes   : 940
Input packets :   5
Output packets:   5
Flags: Caller notification sent
IPSec security associations: 1 created, 0 deleted
Phase 2 negotiations in progress: 0
```

The **detail** option provides more information, including the role (initiator or responder). This is useful to know because troubleshooting is always best done on the peer that has the responder role. Also shown are details regarding the authentication and encryption algorithms used, the phase 1 lifetime, and traffic statistics. Traffic statistics can be used to verify that traffic is flowing properly in both directions. Finally, note the number of IPsec security associations created or in progress. This can help to determine the existence of any completed phase 2 negotiations.

Verifying the VPN Connection — Confirm IPsec (Phase 2) Status

Purpose Confirm that IPsec (phase 2) is connected.

Action Once IKE phase 1 is confirmed, run the **show security ipsec security-associations** command to view IPsec (phase 2) SAs.

```
user@CORPORATE> show security ipsec security-associations

total configured sa: 2
ID    Gateway  Port  Algorithm    SPI     Life:sec/kb  Mon  vsys
<16385  2.2.2.2  500   ESP:3des/sha1  6eeeaf54  3121/ unlim  -    0
>16385  2.2.2.2  500   ESP:3des/sha1  2e07fe78  3121/ unlim  -    0
```

In this output, there is one IPsec SA pair, and the port used is **500**, which means there is no NAT traversal (nat-traversal would show port 4500 or random high port). Also, you can see the security parameter index (**SPI**) used for both directions, as well as the lifetime (in seconds) and usage limits or lifesize (in kilobytes). **3121/ unlim** means that the phase 2 lifetime is set to expire in 3121 seconds, and because no lifesize is specified, it displays as **unlim**. Phase 2 lifetime can differ from phase 1 lifetime, since phase 2 is not dependent on phase 1 once the VPN is up. The **Mon** column refers to VPN monitoring status. When

VPN monitoring is enabled, this shows **U** (up) or **D** (down). A hyphen (**-**) means that VPN monitoring is not enabled for this SA. Note that **vsys** always shows **0**.

Note that the **ID** number is **16385** in the output. This is the index value and is unique for each IPsec SA. You can view more details for a particular security association as shown here:

```
user@CORPORATE> show security ipsec security-associations index 16385 detail

Virtual-system: Root
Local Gateway: 1.1.1.2, Remote Gateway: 2.2.2.2
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  DF-bit: clear

  Direction: inbound, SPI: 1861136212, AUX-SPI: 0
  Hard lifetime: Expires in 3113 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2523 seconds
  Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
  Anti-replay service: enabled, Replay window size: 32

  Direction: outbound, SPI: 772275832, AUX-SPI: 0
  Hard lifetime: Expires in 3113 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2523 seconds
  Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
  Anti-replay service: enabled, Replay window size: 32
```

In this output, local identity and remote identity elements are displayed. These elements comprise the proxy ID for this SA. Proxy ID mismatch is a very common reason for phase 2 failing to complete. If no IPsec SA is listed, then confirm the phase 2 proposals and check that the proxy ID settings are correct for both peers. Note that for route-based VPNs, the default proxy ID is *local=0.0.0.0/0, remote=0.0.0.0/0, service=any*. This can cause issues if you have multiple route-based VPNs from the same peer IP, in which case, you must specify unique proxy IDs for each IPsec SA. Also for some third-party vendors, you might need to manually enter the proxy ID to match. Another common reason for phase 2 failing to complete can be not specifying secure tunnel (ST) interface binding. If IPsec cannot complete, check the **kmd log**.

Verifying Statistics and Errors for an IPsec SA

Purpose Verify ESP and authentication header counters, and check for any errors with a particular IPsec security association.

Action

```
user@CORPORATE> show security ipsec statistics index 16385

ESP Statistics:
  Encrypted bytes: 920
  Decrypted bytes: 6208
  Encrypted packets: 5
  Decrypted packets: 87
AH Statistics:
  Input bytes: 0
```

```
  Output bytes: 0
  Input packets: 0
  Output packets: 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

You normally do not want to see error values other than zero. However, if you are experiencing packet loss issues across a VPN, then one approach is to run the command multiple times and confirm that the encrypted and decrypted packet counters are incrementing. Also, determine whether any of the error counters increment while you are experiencing the issue. It might also be necessary to enable security flow traceoptions to determine and troubleshoot ESP packets that are experiencing errors.

Verifying Traffic Flow Across the VPN

Purpose Test traffic flow across the VPN after phase 1 and phase 2 have completed successfully. You can test traffic flow by using the **ping** command. You can ping from the local host PC to the remote host PC. You can also initiate pings from the Junos OS-based device.

Action Use the **ping** command to test connectivity from the Corporate site Junos OS-based device to the Remote site PC host.

```
user@CORPORATE> ping 10.0.20.10 interface ge-0/0/0.0 count 5

PING 10.0.20.10 (10.0.20.10): 56 data bytes
64 bytes from 192.168.10.1: icmp_seq=0 ttl=65 time=3.552 ms
64 bytes from 192.168.10.1: icmp_seq=1 ttl=65 time=2.683 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=65 time=2.666 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=65 time=2.667 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=65 time=3.109 ms

--- 10.0.20.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.666/2.935/3.552/0.352 ms
```

To reach the Remote site network, the destination address must be the remote peer static NAT address. Note that pings are initiated from the Junos OS-based device, that the source interface or source address must be specified to ensure that correct route lookup takes place, and that the appropriate zones are referenced in policy lookup.

In this example, **ge-0/0/0.0** resides in the same security zone as the Corporate host PC. Therefore, interface **ge-0/0/0.0** or the IP address of the interface must be specified in pings, so that the policy lookup can be from zone **trust** to zone **vpn**.

If pings fail, this could indicate an issue with routing, policy, end host, or perhaps with the encryption/decryption of the ESP packets. One way to check is to view IPsec statistics to see if any errors have been reported. Also, you can confirm end host connectivity by pinging from a host on the same subnet as the end host. If it is reachable by other hosts, the end host is probably not the reason for the issue. For routing and policy issues, enable security flow traceoptions.

Related Documentation

- Business Requirements for VPNs with Overlapping Subnets on page 1
- VPNs with Overlapping Subnets Problem Scenario on page 1