Configuring a Lan-to-Lan VPN with Overlapping Subnets with Juniper NetScreen/ISG/SSG Products

Version 1.0

January 2008
Contents

Introduction ........................................................................................................................................... 3
Included Platforms and Software Versions ........................................................................................ 3
Overview ............................................................................................................................................... 3
Problem Scenario ................................................................................................................................. 3
Packet Flow Details with a MIP (figure 1) ......................................................................................... 4
Network Diagram (figure 2) ............................................................................................................. 6
Configuration Steps .......................................................................................................................... 6
Basic Steps to Configure .................................................................................................................. 7

Corporate Site Configuration Example ............................................................................................... 8
1. Configure “vpn” security zone......................................................................................................... 8
2. Configure IP addresses and bind interfaces to zones ................................................................. 8
3. Configure tunnel interface and bind interface to “vpn” zone .................................................... 8
4. Configure MIP on tunnel interface ............................................................................................. 9
5. Configure static routes for default gateway and Remote site LAN .......................................... 9
6. Configure address book entries .................................................................................................. 9
7. Configure IKE phase-1 and phase-2 proposals (optional). ....................................................... 10
8. Configure IKE gateway ............................................................................................................... 10
9. Configure VPN profile and bind tunnel interface ...................................................................... 11
10. Configure security policy from Corporate LAN to Remote LAN ........................................... 11
11. Configure MIP policy from Remote LAN to Corporate LAN .................................................. 11
12. Configure outgoing “Trust” to “Untrust” permit policy ............................................................ 12
13. Configure TCP mss .................................................................................................................. 12

Remote Site Configuration Example ................................................................................................. 13
1. Configure “vpn” security zone ....................................................................................................... 13
2. Configure IP addresses and bind interfaces to zones ................................................................. 13
3. Configure tunnel interface and bind interface to “vpn” zone .................................................... 13
4. Configure MIP on tunnel interface ............................................................................................. 14
5. Configure static routes for default gateway and Remote site LAN .......................................... 14
6. Configure address book entries .................................................................................................. 14
7. Configure IKE phase-1 and phase-2 proposals (optional). ....................................................... 15
8. Configure IKE gateway ............................................................................................................... 15
9. Configure VPN profile and bind tunnel interface ...................................................................... 15
10. Configure security policy from Corporate LAN to Remote LAN ........................................... 16
11. Configure MIP policy from Remote LAN to Corporate LAN .................................................. 16
12. Configure outgoing “Trust” to “Untrust” permit policy ............................................................ 17
13. Configure TCP mss .................................................................................................................. 17

Verifying Functionality ..................................................................................................................... 17
Confirming VPN Security Association Status .................................................................................. 17
Testing Traffic Flow Across the VPN ............................................................................................... 18
Introduction

The Juniper Networks family of purpose-built security solutions is designed to satisfy customer networking and security requirements that range from small branch office and telecommuter locations to high-speed carrier and data center environments. These products include the NetScreen, ISG and SSG Firewall/VPN product families with ScreenOS software. The purpose of this application note is to detail IPSec VPN configuration between two Juniper Networks firewall/VPN devices in a scenario where the subnets on both sides overlap.

Included Platforms and Software Versions

This document applies to ScreenOS 5.3.0 or later running on the following hardware platforms...

- All NetScreen platforms including 5GT, 5XT, HSC, 25, 50, 204, 208, 500, 5200 and 5400
- All ISG platforms including 1000 and 2000
- All SSG platforms including 5, 20, 140, 320M, 350M, 520/520M and 550/550M

Overview

The configuration of a Juniper Networks Firewall/VPN product is particularly flexible. You can create route-based and policy-based VPN tunnels. Furthermore, network address translations (NAT) can be incorporated to provide solutions for certain problematic networking scenarios. This application note will focus on one such problem scenario.

With corporate mergers, branch office consolidations, and partner collaborations being commonplace, often a company will want to create a VPN to another site with the same private addressing scheme for their IP network. Since both networks use the same IP address scheme for their internal networks, it is not possible to simply build a tunnel between the two sites with normal routing. However, if the IPSec tunnel endpoints on both sides are Juniper Networks Firewall/VPN devices, it is possible to configure a tunnel between these sites with an advanced configuration using network address translations (NAT).

Problem Scenario

First it is important to understand the basic routing dilemma. If a host is attached to a local network, say 192.168.10.0/24, and the other host on the remote end is attached to a network using the same IP address subnet, it is not possible to build a tunnel and route the traffic to the other host without some sort of address translation. This is because packets are routed based on the destination IP address. Before routing occurs, a determination must be made whether the destination IP is on the same (local) network or not. If the destination IP is on the same network, say 192.168.10.10, then the destination host is found on the local network using ARP. However, if the destination IP resides on a different network, the packet is sent to the next-hop router based on the host’s routing table.

Since both the local and remote networks share the same IP addressing scheme, the traffic would be handled locally. The traffic would never route to the next hop and thus never reach the VPN tunnel. To work around this, we can perform static NAT with a mapped IP (MIP) on the source IP and destination IP of all traffic destined for the remote network.
For this reason, a route-based approach to IPSec VPNs makes sense since it would be necessary to create a "virtual" network interface on each VPN peer by creating a tunnel interface. It is important to note that when configuring the example in this application note, both source and destination addresses are translated as the packet traverses the VPN tunnel to the end host. Thus the VPN peers at each end of the tunnel will need to contact each other using a newly created IP network. This can introduce some administrative issues with certain applications, so please be sure to keep this in mind when migrating two networks with overlapping subnets.

For the purposes of this application note we will focus on a route-based VPN configuration using MIPs on the tunnel interfaces for both peers. Additional Juniper Networks Firewall/VPN specific application notes and articles can be found on Juniper Networks’ Knowledge Base at http://kb.juniper.net. In particular, the Juniper Firewall VPN Configuration and Resolution Guide and the ScreenOS Concepts & Examples Guides are valuable reference material.

Packet Flow Details with a MIP

See Figure 1 below for a packet flow example.

Figure 1.

For this example, PC1 and FW1 are at one site while PC2 and FW2 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). A TCP port 80 session is initiated from PC1 destined for the mapped IP for PC2. Below outlines the packet flow with a MIP configured on both sites’ tunnel interfaces.

A. Packet leaves PC1 destined for 10.1.20.10 to reach the remote side host PC2. Note that devices must attempt to reach devices at the remote end of the tunnel using the IP network owned by the remote device tunnel interface. Based on the default gateway configuration of PC1, the next hop would be 192.168.10.1 which is FW1.

Packet Detail

<table>
<thead>
<tr>
<th>src IP/port</th>
<th>dst IP/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.10/1024</td>
<td>10.1.20.10/80</td>
</tr>
</tbody>
</table>

B. The packet arrives at FW1 internal interface with no change to the source or destination IP or port. The packet is routed internally to the tunnel interface on FW1.

Packet Detail

<table>
<thead>
<tr>
<th>src IP/port</th>
<th>dst IP/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.10/1024</td>
<td>10.1.20.10/80</td>
</tr>
</tbody>
</table>

C. When the packet reaches FW1 tunnel interface, a MIP setting and associated policy is found. The MIP has been defined for the entire 10.1.10.0 network range. Thus all outgoing traffic from 192.168.10.0 network destined for the tunnel interface will be source translated to a 10.1.10.0 equivalent address. The packet leaves encrypted out FW1 external interface, but inner packet now has source IP changed to 10.1.10.10 (port does not change with a
MIP). Note that even though the source IP is translated to a **10.1.10.0** address, the security policy still needs to have the original source IP in the address objects.

Packet Detail

<table>
<thead>
<tr>
<th>src IP/port</th>
<th>dst IP/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.10.10/1024</td>
<td>10.1.20.10/80</td>
</tr>
</tbody>
</table>

D. The encrypted packet is received by the *FW2* external interface and decrypted. The inner packet shows source IP as **10.1.10.10** and destination IP as **10.1.20.10**. The packet is sent to the tunnel interface on *FW2*.

Packet Detail

<table>
<thead>
<tr>
<th>src IP/port</th>
<th>dst IP/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.10.10/1024</td>
<td>10.1.20.10/80</td>
</tr>
</tbody>
</table>

E. *FW2* also has a MIP defined on the tunnel interface which covers the entire network range for 10.1.20.0 network. Thus all traffic destined for **10.1.20.0** network will be destination translated to an internal **192.168.10.0** equivalent address. The route lookup will determine that 192.168.10.0 network will be routed to *FW2* internal interface. Packet leaves *FW2* internal interface with destination IP changed to **192.168.10.10**.

Packet Detail

<table>
<thead>
<tr>
<th>src IP/port</th>
<th>dst IP/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.10.10/1024</td>
<td>192.168.10.10/80</td>
</tr>
</tbody>
</table>

F. Since *PC2* has IP address **192.168.10.10**, the packet will be received by *PC2* with the same source and destination IP and ports as in step E.

So as can be seen above, the original packet was both source and destination NAT translated by the time it reached *PC2*. Note that the NAT translations do not both occur on the same device. Rather one device performs the source address translation and the remote device performs the destination address translation. The reply from *PC2* back to *PC1* will follow similar steps only reversed as below.

G. Reply packet leaves *PC2* destined for **10.1.10.10** to reach host *PC1*. Based on the default gateway configuration of *PC2*, the next hop would be 192.168.10.1 which is *FW2*.

Packet Detail

<table>
<thead>
<tr>
<th>src IP/port</th>
<th>dst IP/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.10/80</td>
<td>10.1.10.10/1024</td>
</tr>
</tbody>
</table>

H. The packet arrives at *FW2* internal interface with no change to the source or destination IPs or ports.

Packet Detail

<table>
<thead>
<tr>
<th>src IP/port</th>
<th>dst IP/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.10/80</td>
<td>10.1.10.10/1024</td>
</tr>
</tbody>
</table>

I. Packet matches existing session in *FW2* in which a MIP was defined. Thus the traffic from **192.168.10.0** network destined for the tunnel interface will be source translated to a **10.1.20.0** equivalent address. Packet leaves encrypted out *FW2* external interface, but inner packet now has source IP changed to **10.1.20.10**.
Packet Detail

<table>
<thead>
<tr>
<th>src IP/port</th>
<th>dst IP/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.20.10/80</td>
<td>10.1.10.10/1024</td>
</tr>
</tbody>
</table>

J. Packet arrives at FW1 external interface and decrypted. The inner packet shows source IP as **10.1.20.10** and destination IP as **10.1.10.10**.

Packet Detail

<table>
<thead>
<tr>
<th>src IP/port</th>
<th>dst IP/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.20.10/80</td>
<td>10.1.10.10/1024</td>
</tr>
</tbody>
</table>

K. Packet matches existing session on FW1 in which a MIP was defined. Thus the traffic destined for **10.1.10.0** network will destination translate to an internal **192.168.10.0** equivalent address. Packet leaves FW1 internal interface with destination IP changed to **192.168.10.10**.

Packet Detail

<table>
<thead>
<tr>
<th>src IP/port</th>
<th>dst IP/port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.20.10/80</td>
<td>192.168.10.10/1024</td>
</tr>
</tbody>
</table>

L. Packet arrives at PC1 with the same source and destination IP and ports as in step K.

Network Diagram

Refer to Figure 2 below for Network Topology used for this configuration example.

Figure 2.

Configuration Steps

This example assumes the following (refer to figure 2 above):

- Internal LAN interface for both sites will be ethernet0/0 in zone “trust” and will have private IP 192.168.10.1/24.
- Internet interface for both sites will be ethernet0/3 in zone “untrust” and will each have a unique public IP.
- Tunnel interface tunnel.1 will be in zone “vpn” on both sites to allow for configuring unique policies specifically for tunnel (encrypted) traffic while maintaining unique policies for clear (non-encrypted) traffic.
• The address range to reach Remote side hosts from Corporate side is 10.1.20.0/24.
• The address range to reach Corporate side hosts from Remote side is 10.1.10.0/24
• All traffic between the Corporate and Remote LANs are to be permitted, and traffic may be initiated from either side.
• Basic non-VPN settings such as system settings, user login, and default security settings are already pre-configured on both devices.

**Basic Steps to Configure**

Note that both Corporate and Remote sites have similar configuration steps. Thus the below information applies to both peers.

1. Configure the “vpn” security zone. “Trust” and “Untrust” zones are predefined.
2. Configure IP addresses for interfaces ethernet0/0 and ethernet0/3. Bind the interfaces the “Trust” and “Untrust” zones respectively.
3. Create tunnel.1 interface and bind to “vpn” zone.
4. Configure MIP for the tunnel interface.
5. Configure default route to Internet next-hop and also a static route for the Remote site LAN. Optionally you can use a dynamic routing protocol such as OSPF instead but that is beyond the scope of this application note.
6. Configure address book entries for “Trust” and “vpn” zones. This will be necessary for the security policies.
7. Configure phase-1 (IKE) and phase-2 (VPN) proposals. This step is optional. You can also use one of the pre-defined p1 and p2 proposals or use one of the pre-defined security levels (i.e. basic, standard or compatible)
8. Configure IKE gateway profile referencing the phase-1 proposal from step 7.
9. Configure VPN profile referencing IKE gateway from step 8 and phase-2 proposal from step 7. Then bind interface tunnel.1 to the VPN.
10. Configure security policy to permit Corporate site LAN to Remote site LAN using the address book entries created in step 6.
11. Configure security policy to permit Remote site LAN traffic to Corporate site LAN using address book entry from step 6 with destination address as the MIP.
12. Configure outgoing “Trust” to “Untrust” permit all policy with interface source NAT for Internet traffic.
13. Configure tcp-mss for IPsec traffic to eliminate the possibility of fragmented TCP traffic. This will lessen the resource utilization on the device.
Corporate Site Configuration Example

1. Configure “vpn” security zone.

WebUI
Network > Zones > New: Enter the following, then click OK.
- Zone Name: vpn
- Virtual Router Name: trust-vr
- Zone Type: Layer 3

CLI
set zone name "vpn" vrouter "trust-vr"

2. Configure IP addresses and bind interfaces to zones.

WebUI
Network > Interfaces > Edit (for ethernet0/0): Enter the following, then click OK.
- Zone Name: Trust
- Static IP, Address/Netmask: 192.168.10.1/24
- Interface Mode: Nat

Network > Interfaces > Edit (for ethernet0/3): Enter the following, then click OK.
- Zone Name: Untrust
- Static IP, Address/Netmask: 1.1.1.2/30
- Interface Mode: Route

CLI
set interface ethernet0/0 zone "Trust"
set interface ethernet0/0 ip 192.168.10.1/24
set interface ethernet0/0 nat
set interface ethernet0/3 zone "Untrust"
set interface ethernet0/3 ip 1.1.1.2/30
set interface ethernet0/3 route

3. Configure tunnel interface and bind interface to “vpn” zone.

WebUI
Network > Interfaces > New Tunnel IF: Enter the following, then click OK.
- Tunnel Interface Name: tunnel.1
- Zone (VR): vpn (trust-vr)
- Fixed IP, Address/Netmask: 10.1.10.1/24
CLI

set interface tunnel.1 zone "vpn"
set interface tunnel.1 ip 10.1.10.1/24

4. Configure MIP on tunnel interface.

WebUI

Network > Interfaces > Edit (for tunnel.1) > MIP > New: Enter the following, then click OK.

- Mapped IP: 10.1.10.1
- Host IP: 192.168.10.1
- Netmask: 255.255.255.0
- Host Virtual Router Name: trust-vr

CLI

set interface tunnel.1 mip 10.1.10.1 host 192.168.10.1 netmask 255.255.255.0 vrouter "trust-vr"

5. Configure static routes for default gateway and Remote site LAN.

WebUI

Network > Routing > Destination > New trust-vr: Enter the following, then click OK.

- IP Address/Netmask: 0.0.0.0/0
- Next Hop: Gateway
  - Interface: ethernet0/3
  - Gateway IP Address: 1.1.1.1

Network > Routing > Destination > New trust-vr: Enter the following, then click OK.

- IP Address/Netmask: 10.1.20.0/24
- Next Hop: Gateway
  - Interface: tunnel.1

CLI

set route 0.0.0.0/0 interface ethernet0/3 gateway 1.1.1.1
set route 10.1.20.0/24 interface tunnel.1


WebUI

Objects > Addresses > List > New: Enter the following, then click OK.

- Address Name: local-net
- IP Address/Netmask: 192.168.10.0/24
- Zone: Trust
Objects > Addresses > List > New: Enter the following, then click **OK**.

Address Name: remote-net
IP Address/Netmask: 10.1.20.0/24
Zone: vpn

**CLI**

```
set address "Trust" "local-net" 192.168.10.0 255.255.255.0
set address "vpn" "remote-net" 10.1.20.0 255.255.255.0
```

7. Configure IKE phase-1 and phase-2 proposals (optional).

**WebUI**

VPNs > AutoKey Advanced > P1 Proposal > New: Enter the following, then click **OK**.

Name: ike-proposal1
Authentication Method: Preshare
DH Group: Group 2
Encryption & Data Integrity
  Encryption Algorithm: 3DES-CBC
  Hash Algorithm: SHA-1
  Lifetime: 8 Hours (default)

VPNs > AutoKey Advanced > P2 Proposal > New: Enter the following, then click **OK**.

Name: vpn-proposal1
Perfect Forward Secrecy: DH Group 2
Encapsulation
  Encryption (ESP)
    Encryption Algorithm: 3DES-CBC
    Authentication Algorithm: SHA-1
Lifetime
  In Time: 60 Min (default)

**CLI**

```
set ike p1-proposal "ike-proposal1" preshare group2 esp 3des sha-1
set ike p2-proposal "vpn-proposal1" group2 esp 3des sha-1
```

8. Configure IKE gateway.

**WebUI**

VPNs > AutoKey Advanced > Gateway > New: Enter the following, but do NOT click **OK** yet.

Gateway Name: remote-ike
Remote Gateway Type
  Static IP Address/Hostname: 2.2.2.2
Preshared Key: secretkey
Outgoing Interface: ethernet0/3
Then click Advanced. Enter the following, then click Return.

Security Level User Defined: Custom
Phase 1 Proposal: ike-proposal1
Mode (Initiator): Main (ID Protection)

Then click OK.

CLI

set ike gateway "remote-ike" address 2.2.2.2 Main outgoing-interface ethernet0/3
preshare "secretkey" proposal "ike-proposal1"

9. Configure VPN profile and bind tunnel interface.

WebUI

VPNs > AutoKey IKE > New: Enter the following, but do NOT click OK yet.

VPN Name: remote-vpn
Remote Gateway Predefined: remote-ike

Then click Advanced. Enter the following, then click Return.

Security Level User Defined: Custom
Phase 2 Proposal: vpn-proposal1
Bind to
Tunnel Interface: tunnel.1

Then click OK.

CLI

set vpn "remote-vpn" gateway "remote-ike" proposal "vpn-proposal1"
set vpn "remote-vpn" bind interface tunnel.1

10. Configure security policy from Corporate LAN to Remote LAN.

WebUI

Policies > (From: Trust, To: vpn) New: Enter the following, then click OK.

Source Address
Address Book Entry: local-net
Destination Address
Address Book Entry: remote-net
Service: ANY
Action: Permit

CLI

set policy from "Trust" to "vpn" "local-net" "remote-net" "ANY" permit

11. Configure MIP policy from Remote LAN to Corporate LAN.
WebUI

Policies > (From: vpn, To: Trust) New: Enter the following, then click OK.

Source Address
  Address Book Entry: remote-net
Destination Address
  Address Book Entry: MIP(10.1.10.1/24)
Service: ANY
Action: Permit

CLI

set policy from "vpn" to "Trust" "remote-net" "MIP(10.1.10.1/24)" "ANY" permit

12. Configure outgoing “Trust” to “Untrust” permit policy.

WebUI

Policies > (From: Trust, To: Untrust) New: Enter the following, then click OK.

Source Address
  Address Book Entry: Any
Destination Address
  Address Book Entry: Any
Service: ANY
Action: Permit

CLI

set policy from "Trust" to "Untrust" "Any" "Any" "ANY" permit

13. Configure TCP mss.

Tcp-mss is negotiated as part of the TCP 3-way handshake. It limits the maximum size of a TCP segment to better fit the MTU limits on a network. This is especially important for VPN traffic as the IPSec encapsulation overhead along with the IP and frame overhead can cause the resulting ESP packet to exceed the MTU of the physical interface causing fragmentation. Fragmentation increases bandwidth and device resources and is always best avoided. Note the value of 1350 is a recommended starting point for most ethernet-based networks with MTU of 1500 or greater. This value may need to be altered if any device in the path has lower MTU and/or if there is any added overhead such as PPP, frame relay, etc. As a general rule you may need to experiment with different tcp-mss values to obtain optimal performance. This is configurable via CLI only.

WebUI

Not available.

CLI

set flow tcp-mss 1350
Remote Site Configuration Example

Much of the details from the Corporate Site configuration also apply to the Remote site as well. The steps are the same as previously described.

1. Configure “vpn” security zone.

   WebUI

   Network > Zones > New: Enter the following, then click OK.
   
   Zone Name: vpn
   Virtual Router Name: trust-vr
   Zone Type: Layer 3

   CLI

   set zone name "vpn" vrouter "trust-vr"

2. Configure IP addresses and bind interfaces to zones.

   WebUI

   Network > Interfaces > Edit (for ethernet0/0): Enter the following, then click OK.
   
   Zone Name: Trust
   Static IP, Address/Netmask: 192.168.10.1/24
   Interface Mode: Nat

   Network > Interfaces > Edit (for ethernet0/3): Enter the following, then click OK.
   
   Zone Name: Untrust
   Static IP, Address/Netmask: 2.2.2.2/30
   Interface Mode: Route

   CLI

   set interface ethernet0/0 zone "Trust"
   set interface ethernet0/0 ip 192.168.10.1/24
   set interface ethernet0/0 nat
   set interface ethernet0/3 zone "Untrust"
   set interface ethernet0/3 ip 2.2.2.2/30
   set interface ethernet0/3 route

3. Configure tunnel interface and bind interface to “vpn” zone.

   WebUI

   Network > Interfaces > New Tunnel IF: Enter the following, then click OK.
   
   Tunnel Interface Name: tunnel.1
   Zone (VR): vpn (trust-vr)
   Fixed IP, Address/Netmask: 10.1.20.1/24
4. Configure MIP on tunnel interface.

WebUI
Network > Interfaces > Edit (for tunnel.1) > MIP > New: Enter the following, then click OK.
- Mapped IP: 10.1.20.1
- Host IP: 192.168.10.1
- Netmask: 255.255.255.0
- Host Virtual Router Name: trust-vr

CLI
```
set interface tunnel.1 mip 10.1.20.1 host 192.168.10.1 netmask 255.255.255.0 vrouter “trust-vr”
```

5. Configure static routes for default gateway and Remote site LAN.

WebUI
Network > Routing > Destination > New trust-vr: Enter the following, then click OK.
- IP Address/Netmask: 0.0.0.0/0
- Next Hop: Gateway
  - Interface: ethernet0/3
  - Gateway IP Address: 2.2.2.1

Network > Routing > Destination > New trust-vr: Enter the following, then click OK.
- IP Address/Netmask: 10.1.10.0/24
- Next Hop: Gateway
  - Interface: tunnel.1

CLI
```
set route 0.0.0.0/0 interface ethernet0/3 gateway 2.2.2.1
set route 10.1.10.0/24 interface tunnel.1
```


WebUI
Objects > Addresses > List > New: Enter the following, then click OK.
- Address Name: local-net
- IP Address/Netmask: 192.168.10.0/24
- Zone: Trust
Objects > Addresses > List > New: Enter the following, then click **OK**.

- **Address Name:** corporate-net
- **IP Address/Netmask:** 10.1.10.0/24
- **Zone:** vpn

**CLI**

```
set address "Trust" "local-net" 192.168.10.0 255.255.255.0
set address "vpn" "corporate-net" 10.1.10.0 255.255.255.0
```

7. **Configure IKE phase-1 and phase-2 proposals (optional).**

**WebUI**

VPNs > AutoKey Advanced > P1 Proposal > New: Enter the following, then click **OK**.

- **Name:** ike-proposal1
- **Authentication Method:** Preshare
- **DH Group:** Group 2
- **Encryption & Data Integrity**
  - **Encryption Algorithm:** 3DES-CBC
  - **Hash Algorithm:** SHA-1
  - **Lifetime:** 8 Hours (default)

VPNs > AutoKey Advanced > P2 Proposal > New: Enter the following, then click **OK**.

- **Name:** vpn-proposal1
- **Perfect Forward Secrecy:** DH Group 2
- **Encryption (ESP)**
  - **Encryption Algorithm:** 3DES-CBC
  - **Authentication Algorithm:** SHA-1
- **Lifetime**
  - **In Time:** 60 Min (default)

**CLI**

```
set ike p1-proposal "ike-proposal1" preshare group2 esp 3des sha-1
set ike p2-proposal "vpn-proposal1" group2 esp 3des sha-1
```

8. **Configure IKE gateway.**

**WebUI**

VPNs > AutoKey Advanced > Gateway > New: Enter the following, but do **NOT** click **OK** yet.

- **Gateway Name:** corporate-ike
- **Remote Gateway Type**
  - **Static IP Address/Hostname:** 1.1.1.2
- **Preshared Key:** secretkey
- **Outgoing Interface:** ethernet0/3
Then click **Advanced**. Enter the following, then click **Return**.

**Security Level User Defined:** **Custom**  
**Phase 1 Proposal:** **ike-proposal1**  
**Mode (Initiator):** **Main (ID Protection)**

Then click **OK**.

**CLI**

```
set ike gateway "corporate-ike" address 1.1.1.2 Main outgoing-interface ethernet0/3 preshare "secretkey" proposal "ike-proposal1"
```

9. **Configure VPN profile and bind tunnel interface.**

**WebUI**

VPNs > AutoKey IKE > New: Enter the following, but do NOT click **OK** yet.  

**VPN Name:** **corporate-vpn**  
**Remote Gateway Predefined:** **corporate-ike**

Then click **Advanced**. Enter the following, then click **Return**.

**Security Level User Defined:** **Custom**  
**Phase 2 Proposal:** **vpn-proposal1**  
**Bind to**  
**Tunnel Interface:** **tunnel.1**

Then click **OK**.

**CLI**

```
set vpn "corporate-vpn" gateway "remote-ike" proposal "vpn-proposal1"  
set vpn "corporate-vpn" bind interface tunnel.1
```

10. **Configure security policy from Corporate LAN to Remote LAN.**

**WebUI**

Policies > (From: **Trust**, To: **vpn**) New: Enter the following, then click **OK**.  

**Source Address**  
**Address Book Entry:** **local-net**  
**Destination Address**  
**Address Book Entry:** **corporate-net**  
**Service:** **ANY**  
**Action:** **Permit**

**CLI**

```
set policy from "Trust" to "vpn" "local-net" "corporate-net" "ANY" permit
```

11. **Configure MIP policy from Remote LAN to Corporate LAN.**
WebUI

Policies > (From: vpn, To: Trust) New: Enter the following, then click OK.

Source Address
  Address Book Entry: corporate-net
Destination Address
  Address Book Entry: MIP(10.1.20.1/24)
Service: ANY
Action: Permit

CLI

set policy from "vpn" to "Trust" "corporate-net" "MIP(10.1.20.1/24)" "ANY" permit

12. Configure outgoing “Trust” to “Untrust” permit policy.

WebUI

Policies > (From: Trust, To: Untrust) New: Enter the following, then click OK.

Source Address
  Address Book Entry: Any
Destination Address
  Address Book Entry: Any
Service: ANY
Action: Permit

CLI

set policy from "Trust" to "Untrust" "Any" "Any" "ANY" permit

13. Configure TCP mss.

WebUI

Not available.

CLI

set flow tcp-mss 1350

Verifying Functionality

Confirming VPN Security Association Status

The first step would be to confirm VPN status. Assuming that traffic is already flowing through the VPN and the tunnel should be in UP state, confirm the security association status with command: get sa (see example output below).
CORPORATE-> get sa
total configured sa: 1

<table>
<thead>
<tr>
<th>HEX ID</th>
<th>Gateway</th>
<th>Port Algorithm</th>
<th>SPI</th>
<th>Life:sec</th>
<th>kb</th>
<th>Sta</th>
<th>PID</th>
<th>vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000001&lt;</td>
<td>2.2.2.2</td>
<td>500 esp:3des/sha1 c2elf0e4</td>
<td>3296</td>
<td>unlim</td>
<td>A/-</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000001&gt;</td>
<td>2.2.2.2</td>
<td>500 esp:3des/sha1 74099e47</td>
<td>3296</td>
<td>unlim</td>
<td>A/-</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

We can see that the remote peer is 2.2.2.2. The State shows A/-. The possible states are below:

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/I</td>
<td>SA Inactive. VPN is currently not connected.</td>
</tr>
<tr>
<td>A/-</td>
<td>SA is Active, VPN monitoring is not enabled</td>
</tr>
<tr>
<td>A/D</td>
<td>SA is Active, VPN monitoring is enabled but failing thus DOWN</td>
</tr>
<tr>
<td>A/U</td>
<td>SA is Active, VPN monitoring is enabled and UP</td>
</tr>
</tbody>
</table>

For additional troubleshooting assistance for IKE and IPSec, refer to the Juniper Firewall VPN Configuration and Resolution Guide.

**Testing Traffic Flow Across the VPN**

Once you have confirmed status of the security association, then the next step is to test traffic flow across the VPN. One way to test traffic flow is through pings. We can ping from local host PC to remote host PC. We can also initiate pings from the Juniper Firewall/VPN device itself. Below is an example of ping testing from the Corporate site Firewall/VPN device to the Remote side PC host.

CORPORATE-> ping 10.1.20.10 from ethernet0/0

Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 10.1.20.10, timeout is 1 seconds from ethernet0/0
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=20/23/30 ms

Recall that to reach the Remote site network, the destination address must be the remote host mapped IP address. Note also that when initiating pings from the Firewall/VPN device the source interface needs to be specified in order to be sure that route lookup will be correct and the appropriate zones can be referenced in policy lookup. In this case ethernet0/0 resides in the same security zone as the Corporate host PC. Therefore interface ethernet0/0 will need to be specified in pings so that the policy lookup can be from zone “trust” to zone “vpn”.

Likewise, to confirm bi-directional operation, we can initiate a ping from the Remote site peer to the Corporate network host PC. If successful, then that confirms that the routing and policies are correct to allow the traffic in both directions. If either side is not successful, then refer to the Juniper Firewall VPN Configuration and Resolution Guide.