Example: Configuring a Route-Based Site-to-Site VPN using J-Web

Last updated: 7/2013

This configuration example shows how to configure a route-based IPsec VPN to allow data to be securely transferred between a branch office and the corporate office using J-Web.

This example includes:

- **Topology**
- **Configuration steps for Corporate SRX**
- **Verifying the IKE Phase 1 Status**
- **Verifying the IPsec Phase 2 Status**
- **Reviewing Statistics and Errors for an IPsec Security Association**
- **Troubleshooting**

For this same example using the CLI, refer to [http://www.juniper.net/techpubs/en_US/junos12.1x44/topics/example/ipsec-route-based-vpn-configuring.html](http://www.juniper.net/techpubs/en_US/junos12.1x44/topics/example/ipsec-route-based-vpn-configuring.html).

The hierarchical steps and screen outputs in this document are based on the Junos 12.1X44 release.
Configuration steps for Corporate (Sunnyvale) SRX

A. Configure LAN/WAN interface, static route, security zone, and address book information:

NOTE: This section contains the prerequisite steps for the VPN configuration. If your LAN/WAN interfaces, static route, security zone, and local address book are already configured, then jump to the Section B to configure the VPN related configuration.

1. Configure LAN interface on Trust side.
   1. Select Configure>Interfaces>Ports
   2. Select ge-0/0/0 in the left pane
   3. Click Add>logical interface.
   4. In the Add Interface box,
      a. Add the following attributes:
         Unit: 0
      b. Select IPv4 Address box>Enable address configuration
         Click Add. Provide the address attributes:
         IPv4 Address: 10.10.10.1
         Subnet: 24
   5. Click OK

2. Configure WAN interface on Untrust side (Internet side).
   1. Select Configure>Interfaces>Ports
   2. Select ge-0/0/3 in the left pane
   3. Click Add>logical interface.
   4. In the Add Interface box,
      a. Add the following attributes:
         Unit: 0
      b. Select IPv4 Address box>Enable address configuration
         Click Add. Provide the address attributes:
         IPv4 Address: 1.1.1.2
         Subnet: 30
   5. Click OK

3. Configure static route (default route).
   1. Select Routing>Static Routing
   2. Click Add
   3. In the Add Static Route box,
      a. Select IPv4
      b. Add the following attributes:
         IP address: 0.0.0.0
         Subnet mask: 0.0.0.0/0
      c. Under next-hop
         Click Add
         IP Address: 1.1.1.1
      d. Click OK
   4. Click OK
4. Configure the **untrust** security zone.
   1. Select **Security>Zones/Screens**
   2. Click **Add**
   3. In the **Add Zone** box,
      a. Under **Main** TAB, provide the following details.
         Zone name: untrust
         Zone type : security

4. Assign an interface to the security zone.
   a. In the **Add Zone** box,
      Under **Interfaces in this zone** section:
      Select the interface **ge-0/0/3.0** from the **Available** list.
   b. After selecting interface, you click the right arrow key to move the interface to the selected column.

5. Configure the **trust** security zone.
   1. Select **Security>Zones/Screens**
   2. Click **Add**
   3. In the **Add Zone** box,
      a. Under **Main** TAB, provide the following details.
         Zone name: trust
         Zone type : security

4. Assign an interface to the **trust** security zone.
   a. In the **Add Zone** box,
      Under **Interfaces in this zone** section:
      Select the interface **ge-0/0/0.0** from the **Available** pool.
   b. After selecting interface, you click the right arrow key to move the interface to the selected column.

5. Specify allowed system services for the trust security zone
   a. In the **Add Zone** box,
      Under **Host Inbound traffic –Zone** tab,
      Select the services all from the pool of Available services.
      Select the protocol all from the pool of Available protocols.
      Click **OK**

6. Configure an address book entry for the Sunnyvale network and attach a zone to it.
   1. Select **Configure>Security>Address Book**
   2. Click **Add**
   3. In the **Add Address Book** box,
      a. Add the following attributes:
         Address Book Name: book1
      b. Click **Address** TAB and provide the following attributes:
         Address Name : Sunnyvale
         Address type : IP address
         Value : 10.10.10.0/24
      c. Under **Attach zone** section,
         Select trust from the pool of Available zones.
      d. Click **OK**
B. Configure **VPN related** interface, static route, security zone, and address book information:

1. Specify ‘ike’ to be allowed under interface `ge-0/0/3.0` under security zone ‘untrust’.
   1. In the **Add Zone** box,
      a. Select **Security> Zones/Screens**
      b. Select security zone ‘untrust’ and click ‘Edit’
      c. Under **Host Inbound traffic – Zone** tab,
         Select the services `ike` from the pool of Available services.
      d. Click **OK**

   **Important:** *Step 1 is mandatory because if ‘IKE’ is not enabled on the external interface, then the SRX will not accept inbound ike packets. The IKE packets will be dropped, and IKE negotiations will not proceed further.*

2. Configure the tunnel (st0) interface.
   1. Select **Configure> Interfaces> Ports**
   2. Select `st0` in the left pane
   3. Click **Add> logical interface.**
   4. In the **Add Interface** box,
      a. Add the following attributes:
         Unit: 0
         b. Check **IPv4 Address** box> **Enable address configuration**
            Click **Add**. Provide the address attributes:
            IPv4 Address: 10.11.10
            Subnet: 24
   5. Click **OK**

3. Configure a route for tunnel traffic by specifying the remote destination network and the next-hop as the st0 interface.
   1. Select **Routing> Static Routing**
   2. Click **Add**
   3. In the **Add Static Route** box,
      a. Select IPv4
      b. Add the following attributes:
         IP address: **192.168.168.0**
         Subnet mask: **24**
      c. under next-hop
         Click **Add**
         Interface: st0.0
      d. Click **OK**
   4. Click **OK**
4. Configure a security zone named **vpn-chicago**.
   1. Select **Security>Zones/Screens**
   2. Click **Add**
   3. In the **Add Zone** box,
      a. Under **Main** TAB, provide the following details.
         Zone name: vpn-chicago
         Zone type: security

5. Assign the tunnel interface to the security zone (vpn-chicago in this example).
   1. In the **Add Zone** box,
      a. Under **Interfaces in this zone** section:
         Select the interface **st0.0** from the **Available** list.
      b. After selecting interface must click the right arrow key to move interface to selected column

6. Configure address book entry for the remote network and attach a zone to it.
   1. Select **Configure>Security>Address Book**
   2. Click **Add**
   3. In the **Add Address Book** box,
      a. Add the following attributes:
         Address Book Name: book2
      b. Click **Address** TAB and provide the following attributes:
         Address Name: Chicago
         Address type: IP address
         Value: **192.168.168.0/24**
      c. Under **Attach zone** section,
         Select **vpn-chicago** from the pool of **Available** zones.
      d. Click **OK**

**C. Configure IKE:**

The IKE Phase 1 proposal, IKE policy, and IKE gateway are created in this section.

Select **IPSec VPN>Auto Tunnel>Phase 1**

1. Create the IKE Phase 1 proposal.
   a. Under **Proposal** TAB, click **Add**.
      Provide the following attributes:
      name: **ike-phase1-proposal**
      authentication-method: **pre-shared-keys**
      dh-group: **group2**
      authentication-algorithm: **sha1**
      encryption-algorithm: **aes-128-cbc**
   b. Click **OK**
2. Create an IKE policy for main mode. Also specify the *ike-phase1-proposal* (created above) and preshared key auth method.

   a. Under **Policy** TAB, click **Add**.

   b. Under **IKE Policy** TAB
      
      Provide the following attributes:
      
      * name: *ike-phase1-policy*
      * mode: *main*

      Specify a reference to the IKE proposal:

      Under **proposal** section, select **User Defined**.
      Select **ike-phase1-proposal** from the list of **Available** proposals.

      After selecting ike-phase1-proposal, you must click the right arrow key to move interface to selected column.

   c. Click **OK**

   d. Define the IKE Phase 1 policy authentication method.

      Under **IKE Policy options** TAB
      Select **pre-shared-key**.
      Select **Ascii text** and enter in password that will be used by both VPN endpoints for the **preshared key**.

   e. Click **OK**

3. Create an IKE Phase 1 gateway. Specify the IKE policy (phase 1), external (outgoing interface), and the peer IP address/FQDN:

   a. Under **Gateway** TAB, click **Add**.

      Provide the following attributes:

      * name: *gw-chicago*
      * policy: *ike-phase1-policy*
      * external-interface: ge-0/0/3.0*
      * Address/FQDN: 2.2.2.2*

      **Note:** The address/FQDN should be the remote peer’s public IP address. It is important also to specify the correct external interface. If either the peer address or external interface is incorrect, then the IKE gateway is not identified during phase 1 negotiation.
**D. Configure IPsec:**

The IPsec Phase 2 proposal, IPsec policy, and IPsec VPN are created in this section.

Select **IPSec VPN**>**Auto Tunnel**> **Phase 2**

1. Create the IPsec Phase 2 proposal.
   a. Under **Proposal** TAB, click **Add**.
      Provide the following attributes:
      - **name**: `ipsec-phase2-proposal`
      - **protocol**: `esp`
      - **authentication-algorithm**: `hmac-sha1-96`
      - **encryption-algorithm**: `aes-128-cbc`

2. Create an IPSec policy and specify the IPsec Phase 2 proposal created above, along with perfect-forward-secrecy (PFS).
   a. Under **IPSec Policy** TAB, click **Add**.
      Provide the following attributes:
      - **name**: `ipsec-phase2-policy`
      - **perfect-forward-secrecy**: `group2`

      Specify a reference to the IPSec proposal:

      Under **proposal** section, select **User Defined**.
      Select **ike-phase2-proposal** from the list of **Available** proposals.

      After selecting ike-phase2-proposal, you must click the right arrow key to move interface to selected column.

3. Create the IPSec VPN specifying the Remote gateway, IPsec policy, and tunnel interface.
   a. Under **Auto Key VPN** TAB, click **Add**.
      Provide the following attributes:
      - **name**: `ike-vpn-chicago`
      - **Remote Gateway**: `gw-chicago`
      - **Ipsec Policy**: from the drop-down list select `ipsec-phase2-policy`
      - **Bind to tunnel interface**: from the drop-down list select `st0.0`

   b. Click **OK**
E. Configure Security Policies:

The security policies are configured for tunnel traffic in both directions in this section.

*Note: The security policies include zone information configured in the previous steps.*

Select Security>Policy>Apply Policy

1. Create the security policy to permit traffic from the trust zone to the vpn-chicago zone.
   a. Click ‘Add’
   b. Under ‘Add Policy’ Window, provide the following details:
      - policy name: vpn-tr-chi
   c. Under policy context,
      - From zone: from the drop-down list select ‘trust’
      - To zone: from the drop-down list select ‘vpn-chicago’
   d. Under Source Address,
      - Select ‘Sunnyvale’ from the list of available Address-book entries.
   e. Under Destination Address,
      - Select ‘chicago’ from the list of available Address-book entries.
   f. Under Applications,
      - Select ‘any’ from the list of available Applications/Sets entries.
   g. Under Policy Action, select ‘permit’ from the drop down list.

2. Create the security policy to permit traffic from the vpn-chicago zone to the trust zone.
   a. Click ‘Add’
   b. Under ‘Add Policy’ Window, provide the following details:
      - policy name: vpn-chi-tr
   c. Under policy context,
      - From zone: from the drop-down list select ‘vpn-chicago’
      - To zone: from the drop-down list select ‘trust’
   d. Under Source Address,
      - Select ‘chicago’ from the list of available Address-book entries.
   e. Under Destination Address,
      - Select ‘Sunnyvale’ from the list of available Address-book entries.
   f. Under Applications,
      - Select ‘any’ from the list of available Applications/Sets entries.
   g. Under Policy Action, select ‘permit’ from the drop down list.

Configuration steps for Branch (Chicago) SRX

To configure the Chicago SRX, follow the configuration steps for the Sunnyvale SRX, replacing the parameters from the topology.
Verifying the IKE Phase 1 Status

For CLI:
From operational mode, enter the show security IPSec security-associations command.
user@host> show security ike security-associations
Index Remote Address State Initiator cookie Responder cookie Mode
4708557 2.2.2.2 UP d77t81e85fe7e7e3 8bbae363d59cc85f Main

For J-Web:
The steps and tips to check the IKE Phase 1 status are below. (The steps to check the IPsec Phase 2 status are in the section that follows this.)

1. Click ‘Monitor’ TAB
2. Select IPSec VPN>Phase 1
   On the right hand side pane you will see the active IKE associations.

This screen lists all the active IKE Phase 1 SAs. Each SA contains the following information:
- Index—This value is unique for each IKE SA, which you can use the CLI command, ‘show security ike security-associations <index> detail’, to get more information about the SA.
- Remote Address—Verify that the remote IP address is correct.
- State
  - UP—The Phase 1 SA has been established.
  - DOWN—There was a problem establishing the Phase 1 SA.
- Mode—Verify that the correct mode is being used.
Things to check:

1. In the ‘show security ike security-associations’ command output, notice that the remote address is 2.2.2.2 and the state is UP.

   If the State shows DOWN or if there are no IKE security associations present, 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) or mismatched preshared keys or phase 1 proposals (all must match on both peers). An incorrect external interface is another common mis-configuration. This interface must be the correct interface that receives the IKE packets.

2. If the configurations have been checked, then check the kmd log for any errors or use the traceoptions option.

   Note: KMD Logs can be downloaded via J-Web for viewing by going to Maintain Tab->Files->Click on Log Files. Locate KMD line and click on Download.

For information about traceoptions, see Troubleshooting.

Verifying the IPsec Phase 2 Status

For CLI:
From operational mode, enter the show security ipsec security-associations command.
user@host> show security ipsec security-associations

total configured sa: 2

<table>
<thead>
<tr>
<th>ID</th>
<th>Gateway</th>
<th>Port</th>
<th>Algorithm</th>
<th>SPI</th>
<th>Life:sec/kb</th>
<th>Mon vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;131073 2.2.2</td>
<td>500</td>
<td>ESP:aes-128/sha1</td>
<td>c20d30b2</td>
<td>3363/ unlim</td>
<td>- 0</td>
<td></td>
</tr>
<tr>
<td>&gt;131073 2.2.2</td>
<td>500</td>
<td>ESP:aes-128/sha1</td>
<td>dbb8bef1</td>
<td>3363/ unlim</td>
<td>- 0</td>
<td></td>
</tr>
</tbody>
</table>

For J-Web:
The steps and tips to check the IPsec Phase 2 status are below.

1. Click ‘Monitor’ TAB
2. Select IPSec VPN>Phase 2
   On the right hand side pane , click ‘IPSec SA’ TAB.
This screen contains the following information:

- The ID number is 751261. Use this value with the CLI command ‘show security ipsec security-associations <index>’ to get more information about this particular SA.
- There is one IPsec SA pair using port 500, which indicates that no NAT-traversal is implemented. (NAT-traversal uses port 4500 or another random high-number port.)
- The SPIs, lifetime (in seconds), and usage limits (or lifesize in KB) are shown for both directions. The 2921/ unlim value indicates that the Phase 2 lifetime expires in 2921 seconds, and that no lifesize has been specified, which indicates that it is unlimited. Phase 2 lifetime can differ from Phase 1 lifetime, as Phase 2 is not dependent on Phase 1 after the VPN is up.

Things to check:

1. If no IPsec SA is listed, confirm that the phase 2 proposals, including the proxy ID settings, are correct for both peers.
   
   Note that for route-based VPNs, the default local proxy ID is 0.0.0.0/0, the remote proxy ID is 0.0.0.0/0, and the service is any. This can cause issues if you have multiple route-based VPNs from the same peer IP. In this case, you need to specify unique proxy IDs for each IPsec SA. Also, for some third-party vendors, you may need to configure the proxy ID to match.

2. Another common reason for phase 2 failing to complete is the failure to specify ST interface binding.
3. If IPsec cannot complete, check the messages log, and look for any logs with the keyword **KMD**. This should typically show whether or not the SA came up or not.

**Example:**

Apr 19 11:47:54  rng **kmd[1319]**: IKE Phase-2: Completed negotiations, connection established with tunnel-ID:131073 and lifetime 2992 seconds/0 KB - Local gateway: 172.22.135.251, Remote gateway: 24.6.221.146, Local Proxy ID: ipv4_subnet(any:0,[0..7]=0.0.0.0/0), Remote Proxy ID: ipv4_subnet(any:0,[0..7]=0.0.0.0/0), Protocol: ESP, Auth algo: sha1, Encryption algo: 3des-cbc, Direction: inbound, SPI: 93eb6df3, AUX-SPI: 0, Type: dynamic

**Note:** Message Logs can be downloaded via J-Web for viewing by going to maintain Tab->Files->Click on Log Files. Locate MESSAGES line and click on Download.

If the tunnel still fails to come UP, jump to the **Troubleshooting** section.
Reviewing Statistics and Errors for an IPsec Security Association

1. Click ‘Monitor’ TAB
2. Select IPSec VPN>Phase 2
   On the right hand side pane, click ‘Statistics’ TAB.

If you see packet loss issues across a VPN, you can adjust the refresh interval and then monitor the statistics to confirm that the encrypted and decrypted packet counters are incrementing. You should also check whether the other error counters are incrementing.

Troubleshooting

For step-by-step troubleshooting, refer to:
KB10100 - Resolution Guide - How to Troubleshoot a VPN Tunnel that won't come up on a SRX Series device

For help with configuring traceoptions for debugging and trimming output, refer to:
http://kb.juniper.net/KB16108