Application Note

Configuring a Dial-up VPN Using Windows XP Client with L2TP Over IPSec (without NetScreen-Remote)

Version 1.2

January 2008

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Included Platforms and Software Versions</td>
<td>3</td>
</tr>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Limitations and Caveats</td>
<td>4</td>
</tr>
<tr>
<td>Configuration Steps</td>
<td>4</td>
</tr>
<tr>
<td>Basic Steps to Configure</td>
<td>4</td>
</tr>
<tr>
<td>Windows XP Client Configuration</td>
<td>5</td>
</tr>
<tr>
<td>Requesting a Certificate Using Microsoft CA Server</td>
<td>5</td>
</tr>
<tr>
<td>Exporting and Importing Standalone Root CA Certificate</td>
<td>8</td>
</tr>
<tr>
<td>Creating Dial-Up Connection in Windows XP</td>
<td>15</td>
</tr>
<tr>
<td>Juniper Firewall/VPN Configuration</td>
<td>20</td>
</tr>
<tr>
<td>Configuring System Time and DNS</td>
<td>20</td>
</tr>
<tr>
<td>Clock and NTP Settings</td>
<td>20</td>
</tr>
<tr>
<td>DNS Settings</td>
<td>21</td>
</tr>
<tr>
<td>Generating a Certificate Request</td>
<td>21</td>
</tr>
<tr>
<td>Generating Certificate From the PKCS10 File</td>
<td>23</td>
</tr>
<tr>
<td>Installing Certificate and CRL on the Juniper Device</td>
<td>27</td>
</tr>
<tr>
<td>Configuring L2TP Defaults</td>
<td>28</td>
</tr>
<tr>
<td>Configuring IKE and L2TP User</td>
<td>29</td>
</tr>
<tr>
<td>Configuring IKE Gateway (Phase 1)</td>
<td>30</td>
</tr>
<tr>
<td>Configuring Autokey IKE VPN (Phase 2)</td>
<td>32</td>
</tr>
<tr>
<td>Configuring L2TP Tunnel</td>
<td>33</td>
</tr>
<tr>
<td>Configuring Tunnel Policy</td>
<td>33</td>
</tr>
<tr>
<td>Verifying Functionality</td>
<td>34</td>
</tr>
<tr>
<td>Confirming IPSec Security Association Status</td>
<td>34</td>
</tr>
<tr>
<td>Confirming L2TP Tunnel Status</td>
<td>35</td>
</tr>
<tr>
<td>Common Failure Reasons</td>
<td>35</td>
</tr>
</tbody>
</table>
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 L2TP over IPSec VPN configuration between a Windows PC and a Juniper Networks Firewall/VPN gateway in a dialup-VPN scenario. The PC will be using the Microsoft Windows XP native VPN client and not a third-party IPSec application such as NetScreen-Remote.

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

Before discussing configuration of a dialup VPN, it is important to understand the difference when compared with a site-to-site VPN. A site-to-site VPN consists of two VPN peer endpoints which service network(s) on both sides. PC clients do not need to run any particular VPN application and need only to point to the VPN device as the gateway to reach the remote network. This requires two devices on each end with the ability to terminate the VPN tunnel and also route traffic to the network(s) they service. In a dialup VPN, on one side there is no tunnel gateway endpoint device; the tunnel extends directly to the client itself. Thus the tunnel endpoint on the dialup peer services only that host and does not service a network. For this reason a policy-based VPN tunnel makes sense. While you can configure route-based for dialup VPN peers, this is not common and not considered ideal for this scenario.

Juniper Networks recommends using an IPSec VPN client application such as NetScreen-Remote. However, for the purposes of this application note, we will instead utilize the Microsoft Windows XP native VPN client. Note that the information here also applies to Windows 2000 clients. There are limitations when implementing L2TP over IPSec with the Windows VPN client. Be sure to review the limitations in the next section.

This application note will focus on configuring an L2TP over IPSec dialup VPN client with a policy-based VPN. This application note assumes that the user is familiar with the basic functioning of Microsoft Windows operating systems, and standard Windows items, such as buttons, menus, toolbars, windows, etc. Further, this application note assumes that the dialup client has an Internet connection, whether through a private network, DSL connection, Ethernet, wireless Ethernet, dial-up modem, or some other form of connection. 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.
Limitations and Caveats

Use of the Windows XP VPN client has certain limitations and caveats which must be taken into account. If any of the below caveats exist for your environment, then use of the Windows native client is not recommended (refer to the online VPN Resolution Guide for alternatives).

1. L2TP over IPSec VPN clients can only be identified by either IP address or ASN1-DN peer ID type. Peer ID type FQDN and u-FQDN is not supported on the Windows XP client (this is a Windows XP application limitation). So unless the Windows XP VPN client will be connecting from the same IP address every time, pre-shared key authentication method is not supported. If the client will be connecting from a dynamic IP address, you must use PKI certificates for peer identification.

2. Nat-traversal is not supported with L2TP over IPSec. This is a protocol limitation since L2TP over IPSec requires transport mode. This may pose problems if the client is behind a NAT device which doesn’t forward ESP traffic (see ‘Common Failure Reasons’ on page 35). Juniper Firewall/VPN devices do not support RFC 3947.

3. Juniper Firewall/VPN devices will create/accept only one L2TP tunnel for each L2TP Access Client (LAC)-L2TP Network Server (LNS) pair.

4. Juniper Firewall/VPN gateways can only operate as an LNS. LAC is not supported.

5. Juniper Firewall/VPN gateways support incoming connections only. Outgoing or bi-directional L2TP communications is not supported.

6. Every user must have a different IKE identity. If multiple users share the same IKE identity, the dial-in user will negotiate the new IKE tunnel, and the previous IKE tunnel will be terminated.

Configuration Steps

This example assumes the following:

- The Windows XP client will be connecting to the Juniper gateway public IP address which for the purposes of this example will be 172.19.51.197.
- The private LAN network for the Juniper gateway is 10.10.10.0/24.
- The client will be assigned an address from IP pool range 10.10.100.10-10.10.100.20.
- The Juniper Firewall/VPN gateway is already configured with other non-VPN related configuration such as interface zones, default route, etc.
- For the purposes of this application note, we will show certificate generation using a standalone Microsoft CA server. For non-Microsoft CA server implementations, contact your certificate vendor for steps to request and install your certificates.

Basic Steps to Configure

Below are the basic steps to configure the Windows XP client.

1. Request Local machine PKI certificate.
2. Export then import standalone Root CA certificate.
Below are the basic steps to configure the Juniper Firewall/VPN device.

1. Configure system clock and DNS.
2. Generate certificate request.
3. Install certificate and CRL.
4. Configure L2TP defaults.
5. Configure IKE/L2TP user.
6. Configure IKE gateway (phase 1).
7. Configure Autokey IKE VPN (phase 2).
8. Configure tunnel policy.

Windows XP Client Configuration

Requesting a Certificate Using Microsoft CA Server

1. Log into the MS CA server from your web browser. This should bring you to the CA server homepage.
   
   Example:
   http://172.19.50.129/certsrv

2. Select Request a certificate, then click Next.
3. Select **Advanced request**, then click **Next**.

4. Select **Submit a certificate request to this CA using a form**, then click **Next**.
5. Complete the form information. Be sure to include an email address which will be used as the peer ID on the Juniper Firewall/VPN device. In addition, include the following details:

   - **Intended Purpose:** IPSec Certificate
   - **Key Usage:** Both
   - **Key Size:** 1024
     (this is typical, but can be reduced to 512 bytes if fragmentation is an issue)
   - **Use local machine store:** check

   Then click **Submit**.

6. At this point, if your CA server is not set to automatically approve all certificate requests, then you or your CA admin may have to return to the Pending Certificates page and approve the certificate request you just created. For this example, we will assume that the CA server is configured to automatically approve the certificate request. Once the certificate is issued, click on link to **Install this certificate**.
You may see another Potential Scripting Violation warning message. If so, then click Yes. You should then see a screen stating that your new certificate has been successfully installed. At this point, your IPSec certificate should be installed in your machines local store.

Exporting and Importing Standalone Root CA Certificate

Although the Local certificate has been installed, in order to use this certificate to create an L2TP over IPSec connection, you also need to ensure that the standalone Root CA’s self-signed certificate is loaded into the Trusted Root Certification Authorities certificate store. You can either manually obtain the standalone Root CA certificate from the CA admin, or you can simply export the Root CA certificate from your installed Local certificate. Then import it into the Trusted Root Certification Authorities certificate store. The below steps outline the process to export and then import the Root CA certificate.

1. From Windows XP, goto Start > Run. Then open mmc.
2. At the Console1 window, goto File > Add/Remove Snap-in...

3. At the Add/Remove Snap-in window, Click Add.

4. Select Certificates snap-in, then click Add.
5. At the Certificates snap-in window, select **Computer account**, then click **Next**.

![Select Computer](image)

6. At the Select Computer window, select **Local computer**, then click **Finish**.

![Select Computer](image)

7. Click **Close** at Add Standalone Snap-in window. Then click **OK** at the Add/Remove Snap-in window.

8. Expand Certificates (Local Computer) at the Console Root to view the certificate store. Confirm your certificate is stored by navigating to **Certificates (Local Computer) > Personal > Certificates**. You should see your IPSec certificate installed.

![Certificates](image)
9. Double-click on your VPN certificate on the right-hand pane. This will open the Certificate window. Click on the Details tab, then click on Copy To File.

10. The Certificate Export Wizard should start. Click Next.

11. Be sure that private keys are not exported. Click Next.
12. Select Cryptographic Message Syntax Standard – PKCS #7. Check the box to include all certificates in the certification path if possible. Then click Next.

13. Specify a filename and location to save the p7b file. Then click Next.

14. Click Finish to complete the export. At the export successful prompt, Click OK. This will bring you back to the Certificate window. Click OK at Certificate window.
15. At the Console1 window, navigate to **Trusted Root Certification Authorities > Certificates**. Right-click on **Certificates** and select **All Tasks > Import**.

![Certificate Import Wizard](image)

16. The Certificate Import Wizard should start. Click **Next**.

![Certificate Import Wizard](image)

17. Specify the filename and location of the previously save p7b file. Then click **Next**.
18. Select **Place all certificates in the following store**. It should show as Trusted Root Certification Authorities. Then click **Next**.

19. Click **Finish** to complete the export. At the import successful prompt, Click **OK**. This will bring you back to the Certificate window. Click **OK** at Certificate window.

20. At this point, your IPSec certificate is ready to use. To confirm this, navigate and open your Local certificate and check the **Certification Path** tab. You should not see a red “x” on the Root CA certificate.
Creating Dial-Up Connection in Windows XP

Windows XP by default will attempt to connect an L2TP connection over IPSec. To configure the machine as a VPN client follow the below steps.

1. Goto Control Panel > Network Connections. Alternatively, you can also right-click on My Network Places and then click on Properties.

2. Double-click Create a new connection.

3. This will open the New Connection Wizard. Click Next.
4. Select **Connect to the network at my workplace**. Then click **Next**.

5. Select **Virtual Private Network connection**. Then click **Next**.

6. Specify a name for the connection. Then click **Next**.
7. Enter the public IP address or domain name of your Juniper Firewall/VPN gateway device. This IP address should be reachable by the Windows PC (test with ping). Then click Next.

8. Select **My use only** or **Anyone's use** depending on how many user accounts exist on the PC and who you would like to allow access to the VPN connection. Then click Next.

9. Quit the New Connection Wizard by clicking on *Finish*. 
10. Open your new connection. Enter the L2TP User name and Password that will be used for this connection. Then click Properties.

11. In the Properties window, click on the Options tab. You may want to enable **Redial if line is dropped** if you require the connection to remain up at all times.

12. Click on Security tab. Select **Advanced (custom settings)**. Then click **Settings**.
13. In the Data encryption drop-down, select Optional encryption. Allow the following protocols: PAP, CHAP. Juniper Firewall/VPN gateways do NOT support MS-CHAP. Then click OK.

14. You may see the message below. Click Yes.

15. Click on Networking tab. In the Type of VPN drop-down, select L2TP IPSec VPN. Then click OK.

Your Windows VPN client is now ready to connect to the Juniper VPN gateway.
Juniper Firewall/VPN Configuration

Configuring System Time and DNS

Accurate system time and DNS settings are necessary when implementing PKI certificates on Juniper Firewall/VPN gateways. DNS is required to resolve IP addresses during such processes as CRL updates. The certificate valid dates depend on the correct date and time for which the certificate request was initiated. For this reason Juniper recommends configuring NTP on the Firewall/VPN gateway.

Clock and NTP Settings

For this example, we will assume PST timezone (GMT -8) and two publicly available NTP servers us.pool.ntp.org and ca.pool.ntp.org.

WebUI

Configuration > Date/Time: Enter the following, then click OK.

Set Time Zone: -8
Automatically synchronize with an Internet Time Server (NTP): check
Primary server IP/Name: us.pool.ntp.org
Backup server1 IP/Name: ca.pool.ntp.org

CLI

set clock timezone -8
set clock ntp
set ntp server "us.pool.ntp.org"
set ntp server backup1 "ca.pool.ntp.org"
DNS Settings

For this example, we will name our Juniper gateway Corporate-SSG and use domain name juniper.net. We will also use public DNS servers 4.2.2.1 and 4.2.2.2.

WebUI

Network > DNS > Host: Enter the following, then click OK.

Host Name: Corporate-SSG
Domain Name: juniper.net
Primary DNS Server: 4.2.2.1
Secondary DNS Server: 4.2.2.1

CLI

set hostname Corporate-SSG
set domain juniper.net
set dns host dns1 4.2.2.1
set dns host dns2 4.2.2.2

Generating a Certificate Request

The first step to generating a certificate request is to configure the certificate subject information. The next step is to generate the host keys. This step will automatically generate a PKCS10 format certificate request which you would then send to your Certificate Authority.

Fill out the certificate request form details. Note that if the IP address is specified then this certificate will specifically be used for that particular IP address. That means if the IP address of the Juniper device changes a new certificate will need to be generated.

The certificate subject information shown below are for example purposes only. Enter the information relevant for your location. For more details regarding PKI certificates and their use in ScreenOS, refer to the ScreenOS Concepts & Examples Guides.
WebUI

Objects > Certificates > New: Enter the following, then click Generate.

Name: Admin
Phone: 888-314-5822
Unit/Department: JTAC
Organization: Juniper Networks
County/Locality: Sunnyvale
State: CA
Country: US
FQDN: Corporate-SSG.juniper.net
Key Pair Information: RSA
Key Pair Length: 1024

CLI

set pki x509 dn name "Admin"
set pki x509 dn phone "888-314-5822"
set pki x509 dn org-unit-name "JTAC"
set pki x509 dn org-name "Juniper Networks"
set pki x509 dn local-name "Sunnyvale"
set pki x509 dn state-name "CA"
set pki x509 dn country-name "US"

exec pki rsa new-key 1024

The key generation process may take a few minutes to complete as it requires intensive computation. Once complete, a PKCS10 file will be generated which contains a hash of the above information, and will be interpreted by the CA. The PKCS10 output should resemble the below output:
Save the PKCS10 to a file and send it to your Certificate Authority admin.

**Generating Certificate From the PKCS10 File**

For our example we will use the same Microsoft CA server to generate the certificate.

1. Log into the MS CA server from your web browser. This should bring you to the CA server homepage.

   Example:
   
   http://172.19.50.129/certsrv

2. Select Request a certificate, then click Next.
3. Select **Advanced request**, then click **Next**.

4. Select **Submit a certificate request using a base64 encoded PKCS #10 file**, then click **Next**.
5. Copy and paste your PKCS10 output including the BEGIN and END lines into the request window. Then click Submit.

6. If your CA server is not set to automatically approve all certificate requests, then your CA admin will need to approve the certificate request. For this example, we will assume that the CA server is configured to automatically approve the certificate request. Once the certificate is issued, click on link to Download CA certification path (p7b file).
7. In addition to downloading the certificate path, you may also need to download the current CRL for the CA. Return to the CA homepage. Then click on Retrieve the CA certificate or certificate revocation list.

8. Click on Download latest certificate revocation list. Note the saved location of the p7b and CRL file as you will need to know this in order to upload them to your Juniper Firewall/VPN gateway.
Installing Certificate and CRL on the Juniper Device

You can install the certificate via WebUI or CLI. For WebUI, you need to know the location of the saved p7b and CRL files. For CLI, you must upload the p7b and CRL files to a TFTP server which is reachable by the Juniper gateway device. Note that with a p7b certificate path file, the Local certificate and the standalone Root CA certificate will both automatically load.

Install P7b Certificate Path File

**WebUI**
Objects > Certificates: Click Browse and locate the saved Juniper p7b file. Then click Load.

**CLI**
exec pki x509 tftp 172.19.50.129 cert-name ssgcert.p7b

Install CRL File

**WebUI**
Objects > Certificates: Select CRL and then browse for the CRL file. Then click Load.

**CLI**
exec pki x509 tftp 172.19.50.129 crl-name certrl.crl
Confirm CA certificate and CRL Files Loaded

**WebUI**

Objects > Certificates: Select CA in the Show drop-down. Confirm both CA certificate and CRL are loaded.

**CLI**

get pki x509 list ca-cert  
get pki x509 list crl

Configuring L2TP Defaults

Configuring an IP Pool

**WebUI**

Objects > IP Pools > New: Enter the following, then click OK.

- **IP Pool Name**: `L2TP_pool`
- **Start IP**: `10.10.100.10`
- **End IP**: `10.10.100.20`

**CLI**

set ippool "L2TP_pool" 10.10.100.10 10.10.100.20
Configuring L2TP defaults

**WebUI**

VPNs > L2TP > Default Settings: Enter the following, then click **OK**.

- **IP Pool Name:** `L2TP_pool`
- **PPP Authentication:** `ANY`
- **DNS Primary Server IP:** `4.2.2.1`
- **DNS Secondary Server IP:** `4.2.2.2`

**CLI**

```
set l2tp default ippool "L2TP_pool"
set l2tp default ppp-auth any
set l2tp default dns1 4.2.2.1
set l2tp default dns2 4.2.2.2
```

Configuring IKE and L2TP User

An IKE user as well as an L2TP user is required for this implementation. The users can be two separate user profiles or they can be combined into one user profile. For the purposes of this application note, we will configure one user profile which encompasses both the L2TP user and the IKE user. Thus the user name must match the user name configured for the Windows XP VPN connection which in this case is “l2tpuser”. The IKE peer ID must specify distinguished name (ASN1-DN) and the email address must be present to properly identify the user.

**WebUI**

Objects > Users > Local > New: Enter the following, then click **OK**.

- **User Name:** `l2tpuser`
- **Status:** `Enable`
- **IKE User:** `check`
- **Share Limit:** `1`
- **Use Distinguished Name For ID**
- **OU:** `JTAC`
- **Organization:** `Juniper Networks`
CLI

set user "l2tpuser" ike-id asn1-dn wildcard "OU=JTAC,O=Juniper Networks, L=Sunnyvale,ST=CA,C=US,Email=vpnuser@juniper.net" share-limit 1
set user "l2tpuser" type ike l2tp
set user "l2tpuser" password "secret"
unset user "l2tpuser" type auth
set user "l2tpuser" enable

Configuring IKE Gateway (Phase 1)

For this example the IKE gateway will be configured as a Dial-UP peer using the Windows XP Local certificate for peer identification. This means that you do not specify the IP address of the peer but rather specify dialup user. Furthermore, since the peer will be identified by a certificate generated with RSA keys, all phase 1 proposals for this gateway must begin with RSA and not Pre (pre-shared). You cannot specify both types within the same proposal set. Also be sure to specify the correct outgoing interface which should be the Internet facing interface.

Note that for L2TP over IPSec, you must also use Main mode. You should not use Aggressive mode which is commonly used for non-L2TP VPNs.
WebUI

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

Gateway Name: **WindowsVPN-gateway**
Remote Gateway Type
   Dialup User: **l2tpuser**
Outgoing Interface: **ethernet0/3**

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

Phase 1 Proposal: **rsa-g2-des-md5, rsa-g2-des-sha, rsa-g2-3des-md5, rsa-g2-3des-sha**
Mode (Initiator): **Main (ID Protection)**
Preferred Certificate
   Peer CA: **All**

At the Gateway screen, click **OK**.
CLI

set ike gateway "WindowsVPN-gateway" dialup "l2tpuser" Main outgoing-interface ethernet0/3 proposal "rsa-g2-des-md5" "rsa-g2-3des-md5" "rsa-g2-des-sha" "rsa-g2-3des-sha"
set ike gateway "WindowsVPN-gateway" cert peer-ca all

Configuring Autokey IKE VPN (Phase 2)

For L2TP over IPSec connections, you must use transport mode.

WebUI

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

VPN Name: WindowsVPN-vpn
Security Level: Compatible
Remote Gateway Predefined: WindowsVPN-gateway

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

Transport Mode: check
At the Autokey IKE screen, click **OK**.

**CLI**

```
set vpn "WindowsVPN-vpn" gateway "WindowsVPN-gateway" transport sec-level compatible
```

**Configuring L2TP Tunnel**

**WebUI**

VPNs > L2TP > Tunnel > New: Enter the following, then click **OK**.

- **Name:** WindowsVPN-l2tp
- **Use Default Settings**
- **Outgoing Interface:** `ethernet0/3`

![WebUI Configuration](image)

**CLI**

```
set l2tp "WindowsVPN-l2tp" outgoing-interface ethernet0/3
```

**Configuring Tunnel Policy**

The tunnel policy for an L2TP over IPSec connection must have action as tunnel. This is an implicit permit policy which means you cannot also specify an action of deny. Since the VPN to be specified in the policy was configured for transport mode during the Autokey IKE phase 2 configuration, then an L2TP tunnel is also required to be specified or the command will fail.

For the purposes of this application note, we will assume that address object “10.10.10.0/24” has already been configured. Address object “Dial-Up VPN” is already predefined by default on all Juniper Firewall/VPN gateways.
WebUI

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

Source Address
  Address Book Entry: Dial-Up VPN
Destination Address
  Address Book Entry: 10.10.10.0/24
Service: ANY
Action: Tunnel
  Tunnel VPN: WindowsVPN-vpn
  Tunnel L2TP: WindowsVPN-l2tp

CLI

set policy name "L2TP_policy" from "Untrust" to "Trust" "Dial-Up VPN" "10.10.10.0/24" "ANY" tunnel vpn "WindowsVPN-vpn" l2tp "WindowsVPN-l2tp"

Verifying Functionality

Confirming IPSec Security Association Status

IPSec must establish before the L2TP portion of the tunnel can connect. Thus, the first step would be to confirm IPSec VPN status. Assuming that Windows XP VPN client has successfully connected to the Juniper gateway, the security association should be in Active state, confirm the security association status with command: `get sa` (see example output below).

```
CORPORATE-> get sa
total configured sa: 1
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000000<   172.19.51.168  500 esp:3des/md5  d54c5153  3580  244M A/-   -1 0
00000000>   172.19.51.168  500 esp:3des/md5  c25820dd  3580  244M A/-   -1 0
```

The State should show as A/-. The possible states are below:
I/I  SA Inactive. VPN is currently not connected.
A/-  SA is Active, VPN monitoring is not enabled
A/D  SA is Active, VPN monitoring is enabled but failing thus DOWN
A/U  SA is Active, VPN monitoring is enabled and UP

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

Confirming L2TP Tunnel Status

L2TP should complete after IPSec phase 2 completes. To confirm L2TP tunnel status, use commands: `get l2tp all` and `get l2tp all active`.

```
CORPORATE-SSG-> get l2tp all
ID L2TP Name       User        Peer IP         Host   KpAlv Intface
--HEX--- --------------- -------------- --------------- ------ ----- -------
00000002 WindowsVPN-l2tp all-l2tp-users 0.0.0.0                   60 eth0/3
```

```
CORPORATE-SSG-> get l2tp all active
L2TP Name       Tunnel Id Peer Address    Port Peer Host    Calls State   t_info
--------------- --------- --------------- ---- ------------ ----- ------- --HEX---
WindowsVPN-l2tp (  1/  1) 172.19.51.168   1701 jtac-lab         1 establish 80008001
WindowsVPN-l2tp (  0/  0) 0.0.0.0            0                  0    idle 80000002
```

The State should show as Established. This confirms that the tunnel is up. The next step is to confirm traffic flow. Test by initiating a ping from the Windows PC to a host on the Juniper gateway private LAN (example: ping 10.10.10.1)

If the security association is not in active state or there are no established L2TP tunnels, then refer to the Juniper Firewall VPN Configuration and Resolution Guide for troubleshooting tips and methodology.

Common Failure Reasons

There are a number of reasons why L2TP over IPSec connections can fail. This is by no means an exhaustive list, but these are common issues seen in the field. For detailed troubleshooting, Juniper recommends following the Juniper Firewall VPN Configuration and Resolution Guide or search within the Juniper Networks Knowledge Base at http://kb.juniper.net.

Problem

VPN connection starts but fails immediately with Error 769: The specified destination address is not reachable.

Possible Cause

Check your Windows PC network connection. Be sure that your link is enabled and in connected state. Also be sure that you are using the correct outgoing interface for your connection. Finally, check your network settings to confirm that you have an IP address on the expected network.
Problem
VPN connection attempts, but fails with Error 678: The remote computer did not respond.

Possible Cause
This could be a network issue. Is the Juniper gateway reachable by the Windows PC? Test by attempting to ping from the PC to the public IP address of the Juniper gateway. If the request times out, then check your network connection at the Windows client side to confirm that Internet access is working and that you have configured the correct IP address for the Juniper gateway. You can also check the Juniper gateway event logs to see if any IKE phase 1 attempts are seen from your Windows client. If you do not see any then likely the IKE requests are not reaching the Juniper gateway.

Another possible reason for this error could be the existence of other IPSec VPN clients installed on the Windows PC. Check to see if any other VPN client applications are installed. These can interfere with the Windows XP VPN client as they may be contending for the same IKE resources on the PC.

Finally check to see if any PC firewalls are enabled. If so then try disabling or uninstalling any such firewalls and try the connection again.

Problem
VPN connection attempts, but fails with Error 792: The L2TP connection attempt failed because security negotiation timed out.

Possible Cause
This could indicate a mis-match in the configuration of the Windows VPN client or the Juniper gateway. Check the Juniper Firewall/VPN gateway event log to see any IKE error messages are seen. Follow troubleshooting steps as outlined previously on the Juniper online resolution guide.

This could also indicate a problem with fragmentation on the network. During the phase 1 negotiations, if you are using 1024 byte RSA keys then the resulting certificate send packet could exceed the MTU of your network interface and also the interface of any devices between the Windows PC and the Juniper gateway. The result of the overly large packet is that the packet will need to be fragmented when the packet is transmitted. Troubleshoot your network to see if any devices in the path are dropping fragments to and from the Windows PC. On the Juniper Firewall/VPN device, check your screen options to see if block frag is enabled. If so, then try disabling the block frag screen and attempt the connection again.

Problem
VPN connection reaches Verifying username and password stage, but fails with Error 691: Access was denied because the username and/or password was invalid on the domain.

Possible Cause
This is likely mis-configuration of either username or the password. On the Windows PC, be sure that the username matches the IKE/L2TP user entry configured on the Juniper gateway. Also recheck the passwords on both the Windows client and the Juniper gateway.
Problem

VPN successfully connects, but the Windows VPN client cannot reach users on the private LAN.

Possible Cause

Confirm that the tunnel policy is configured with the correct address object. Also confirm that the address object is configured for the correct network address. You may want to consult the Juniper online resolution guide for ways to troubleshoot traffic flow issues.

If the tunnel policy is correct, then check if there is a NAT device between the Windows client and the Juniper gateway. If so then that NAT device may not be able to forward ESP (IP protocol 50) packets. L2TP over IPSec protocol does not support nat-traversal since transport mode does not support it. Check your NAT device for IPSec forwarding options. You may need to consult with the vendor of your NAT device if it is a third-party device.

Note that such NAT issues may also affect the ability to complete the L2TP over IPSec connection as well. The reason for this is IPSec must establish first before the L2TP tunnel can build. All L2TP tunnel connection messages are thus encrypted in an IPSec ESP packet. If there is a NAT issue then IPSec may complete, but L2TP itself may fail.