

# Quick Installation Guide

high security remote access

## Quick Installation Guide NCP Client with Juniper Junos

As of March 2012  
version 1.1

### NCP Client with Juniper Junos

## Network Communications Products engineering

### USA:

NCP engineering, Inc.  
444 Castro Street, Suite 711  
Mountain View, CA 94041  
Tel.: +1 (650) 316-6273  
Fax: +1 (650) 251-4155

### Germany:

NCP engineering GmbH  
Dombuehler Str. 2  
D-90449 Nuremberg  
Tel.: +49 (911) 9968-0  
Fax: +49 (911) 9968-299

### Internet

<http://www.ncp-e.com>

### Email

[info@ncp-e.com](mailto:info@ncp-e.com)

### Support

NCP offers support for all international users by means of Fax and Email.

### Email Addresses

[helpdesk@ncp-e.com](mailto:helpdesk@ncp-e.com) (English)  
[support@ncp-e.com](mailto:support@ncp-e.com) (German)

### Fax

+1 (650) 251-4155 (USA)  
+49 (911) 9968-458 (Europe)

When submitting a support request, please include the following information:

- ▶ exact product name
- ▶ serial number
- ▶ version number
- ▶ an accurate description of your problem
- ▶ any error message(s)

## Copyright

While considerable care has been taken in the preparation and publication of this manual, errors in content, typo-graphical or otherwise, may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP. NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or suitability of use for any particular purpose.

Furthermore, NCP reserves the right to revise this publication and to make amendments to the contents, at any time, without obligation to notify any person or entity of such revisions or changes. This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH.

All trademarks or registered trademarks appearing in this manual belong to their respective owners.

© 2012 NCP engineering GmbH, All rights reserved.

## Contents

<b>1. Revision History .....</b>	<b>4</b>
<b>2. Remote Access VPN with Xauth and Radius .....</b>	<b>5</b>
<b>3. Juniper Gateway CLI .....</b>	<b>6</b>
<b>4. NCP Client Wizard: .....</b>	<b>9</b>
4.1. Connection Type.....	9
4.2. Profile Name .....	9
4.3. VPN Gateway Parameters .....	9
4.4. Exchange Mode .....	10
4.5. Pre-shared Key .....	10
4.6. IPsec Configuration: IP Addresses .....	10
<b>5. Remote Access VPN with Xauth and Active Directory .....</b>	<b>13</b>
<b>6. Multiple Subnets.....</b>	<b>14</b>
<b>7. Troubleshooting .....</b>	<b>14</b>
7.1. Verifying Firewall User Authentication.....	14
7.2. Traceoptions (Flow) .....	15
7.3. Traceoptions (IKE).....	16
7.4. Traceoptions (IPsec) .....	16
7.5. Traceoptions General .....	16
<b>8. Table 1: IPsec Services Operational Mode Commands .....</b>	<b>17</b>

NCP Client with Juniper Junos

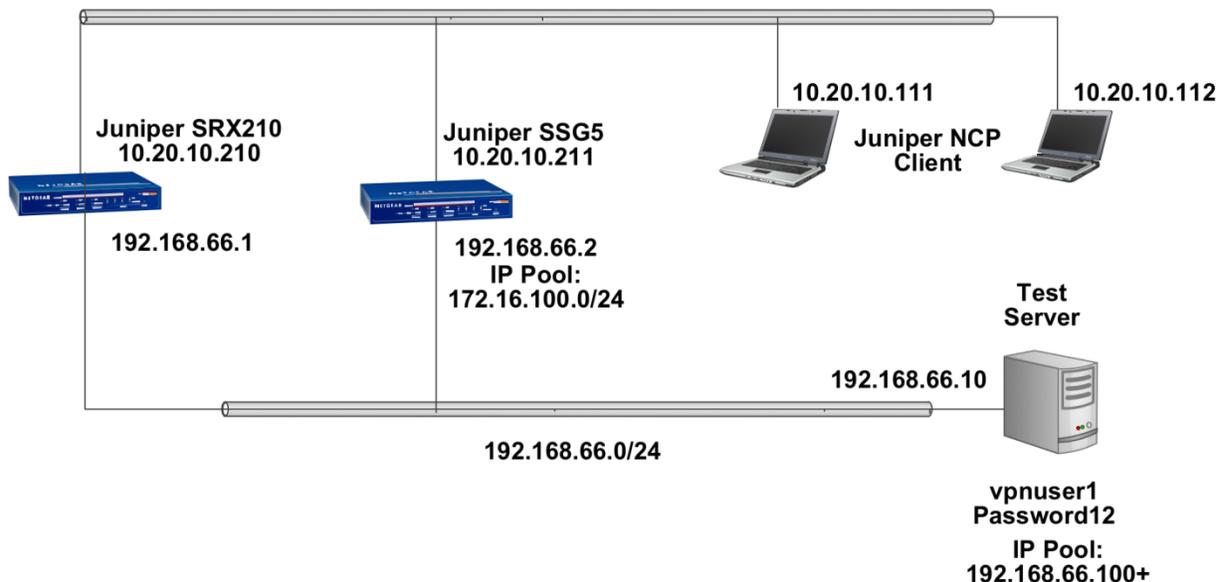
## 1. Revision History

This document outlines the configuration of a Junos based Juniper VPN gateway and the NCP VPN client.

Junos Version	NCP Client Version	Date
10.0R3.10	9.22 Build 63	2010-06-23
10.1R1.8		2010-08-18
		2010-09-08
		2010-10-20
10.4R1.9	9.23 Build 64	2011-01-14
11.1R2.3	9.24 Build 65	2011-05-13

## Network Diagram

The following simple network is used for testing. The Test Server runs on Windows Server 2008 R2 Enterprise. It runs a Web Server (IIS 7) as well as Network Policy and Access Service, which provides for RADIUS authentication.

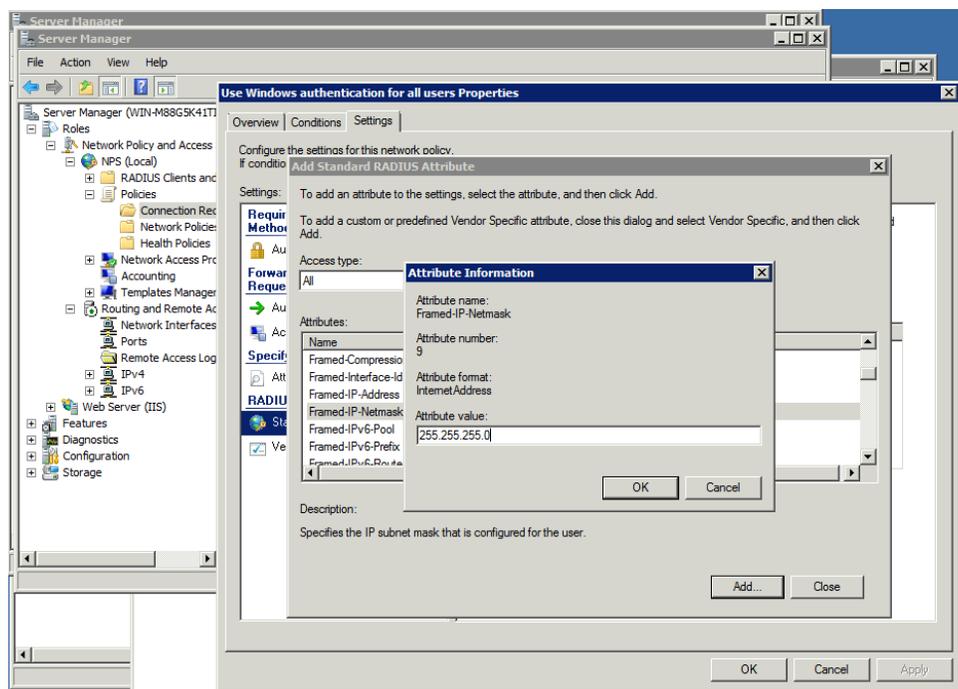
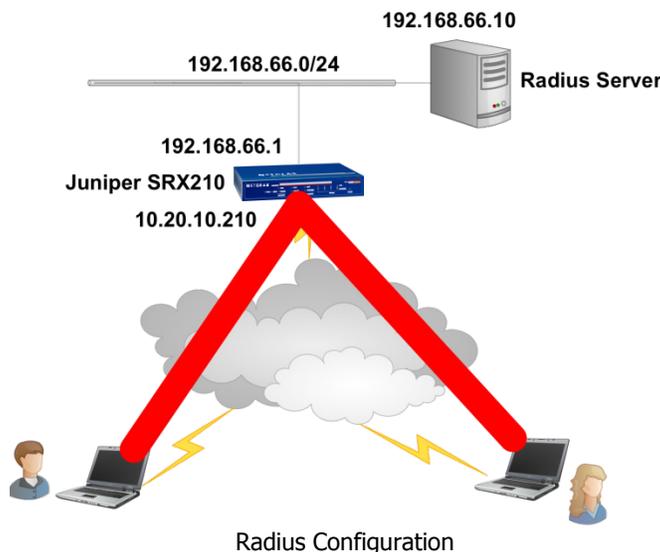


NCP Client with Juniper Junos

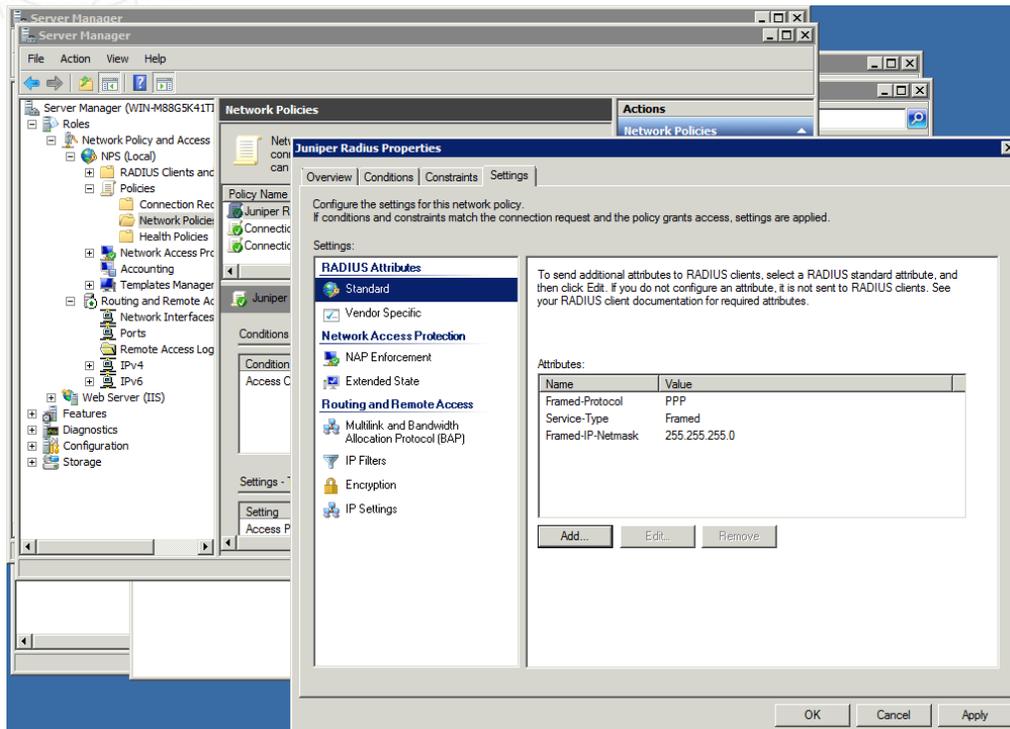
## 2. Remote Access VPN with Xauth and Radius

In this example, the following configuration applies:

- ▶ Internal LAN interface fe-0/0/7
- ▶ Internal LAN interface ge-0/0/0 in zone you create a new group IKE ID user named "NCP Users". You configure it to accept up to 10 Phase 1 negotiations concurrently from VPN clients with preshared keys containing an IKE ID ending with the string juniper.net. The seed value for the preshared key is Tunneling123. You name the dialup IKE user group Office.



## NCP Client with Juniper Junos



In order for the IP address to be passed to the client it is important to define the Framed-IP-Netmask RADIUS attribute as shown here.

### 3. Juniper Gateway CLI Interfaces

```
set interfaces ge-0/0/0 unit 0 family inet address 10.20.10.210/16
set interfaces fe-0/0/7 unit 0 family inet address 192.168.66.1/24
```

#### Security Zones

```
set security zones security-zone trust interfaces fe-0/0/7.0
set security zones security-zone untrust interfaces ge-0/0/0.0
```

#### Host-inbound Services

```
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ssh
set security zones security-zone untrust host-inbound-traffic system-services ping
```

#### Address book

```
set security zones security-zone trust address-book address local-net 192.168.66.0/24
```

### NCP Client with Juniper Junos

#### Access Profiles

```
set access profile xauth-users authentication-order radius
set access profile xauth-users session-options client-idle-timeout 180
set access profile xauth-users radius-server 192.168.66.10 port 1812
set access profile xauth-users radius-server 192.168.66.10 secret "secret"
```

#### IKE Proposals

```
set security ike proposal PSK-AES128-SHA1-DH2 authentication-method pre-shared-keys
set security ike proposal PSK-AES128-SHA1-DH2 dh-group group2
set security ike proposal PSK-AES128-SHA1-DH2 authentication-algorithm sha1
set security ike proposal PSK-AES128-SHA1-DH2 encryption-algorithm aes-128-cbc
set security ike proposal PSK-AES128-SHA1-DH2 lifetime-seconds 28800
set security ike proposal PSK-AES256-SHA1-DH2 authentication-method pre-shared-keys
set security ike proposal PSK-AES256-SHA1-DH2 dh-group group2
set security ike proposal PSK-AES256-SHA1-DH2 authentication-algorithm sha1
set security ike proposal PSK-AES256-SHA1-DH2 encryption-algorithm aes-256-cbc
set security ike proposal PSK-AES256-SHA1-DH2 lifetime-seconds 28800
```

#### IKE Policies

```
set security ike policy dialup-ike-policy mode aggressive
set security ike policy dialup-ike-policy proposals PSK-AES128-SHA1-DH2
set security ike policy dialup-ike-policy pre-shared-key ascii-text "Tunneling123"
```

#### IKE Gateway (Phase 1) with dynamic peer as U-FQDN

```
set security ike gateway dialup-ike ike-policy dialup-ike-policy
set security ike gateway dialup-ike dynamic user-at-hostname user@juniper.net
set security ike gateway dialup-ike external-interface ge-0/0/0
```

#### Shared IKE User Limit and Xauth

```
set security ike gateway dialup-ike dynamic connections-limit 10
set security ike gateway dialup-ike dynamic ike-user-type shared-ike-id
set security ike gateway dialup-ike xauth access-profile xauth-users
```

#### IPsec Proposals

```
set security ipsec proposal ESP-AES128-SHA protocol esp
set security ipsec proposal ESP-AES128-SHA authentication-algorithm hmac-sha1-96
set security ipsec proposal ESP-AES128-SHA encryption-algorithm aes-128-cbc
set security ipsec proposal ESP-AES128-SHA lifetime-seconds 28800
set security ipsec proposal ESP-AES256-SHA protocol esp
set security ipsec proposal ESP-AES256-SHA authentication-algorithm hmac-sha1-96
set security ipsec proposal ESP-AES256-SHA encryption-algorithm aes-256-cbc
set security ipsec proposal ESP-AES256-SHA lifetime-seconds 28800
```

### NCP Client with Juniper Junos

#### IPsec Policies

```
set security ipsec policy dialup-ipsec-policy perfect-forward-secrecy keys group2
set security ipsec policy dialup-ipsec-policy proposals ESP-AES128-SHA
```

#### IPsec VPN with IKE Gateway and IPsec Policy

```
set security ipsec vpn dialup-vpn ike gateway dialup-ike
set security ipsec vpn dialup-vpn ike ipsec-policy dialup-ipsec-policy
set security ipsec vpn dialup-vpn establish-tunnels on-traffic
```

#### IPsec VPN Security Policy for incoming Tunnel Traffic

```
edit security policies from-zone untrust to-zone trust
    ## [edit security policies from-zone untrust to-zone trust]
set policy dialup-unt-tr match source-address any
set policy dialup-unt-tr match destination-address local-net
set policy dialup-unt-tr match application any
set policy dialup-unt-tr then permit tunnel ipsec-vpn dialup-vpn
exit
```

#### Security Policy for Internet Traffic

```
edit security policies from-zone trust to-zone untrust
    ## [edit security policies from-zone trust to-zone untrust]
set policy any-permit match source-address any
set policy any-permit match destination-address any
set policy any-permit match application any
set policy any-permit then permit source-nat interface
exit
```

#### TCP-MSS to eliminate fragmentation of TCP traffic across Tunnel

```
set security flow tcp-mss ipsec-vpn mss 1350
```

#### Save and commit configuration

```
commit
```

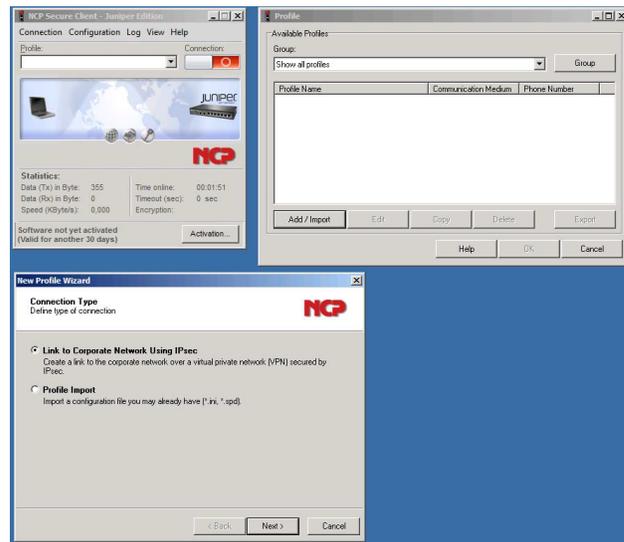
NCP Client with Juniper Junos

### 4. NCP Client Wizard:

#### 4.1. Connection Type

Configuration > Profiles > Add/Import  
 Link to Corporate Network Using IPsec: (select)

> Next



#### 4.2. Profile Name

Configuration  
 Profile Name: Juniper Junos VPN

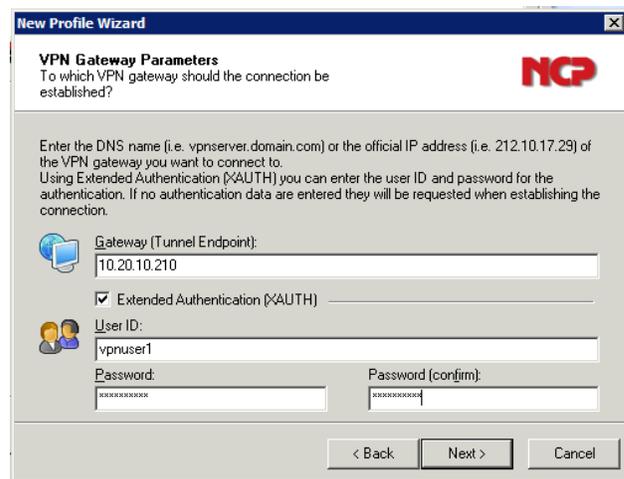
> Next



#### 4.3. VPN Gateway Parameters

Gateway (Tunnel Endpoint): 10.20.10.210  
 Extended Authentication (XAUTH): (select)  
 UserID: vpnuser1  
 Password: Password12  
 Password (confirm): Password12

> Next

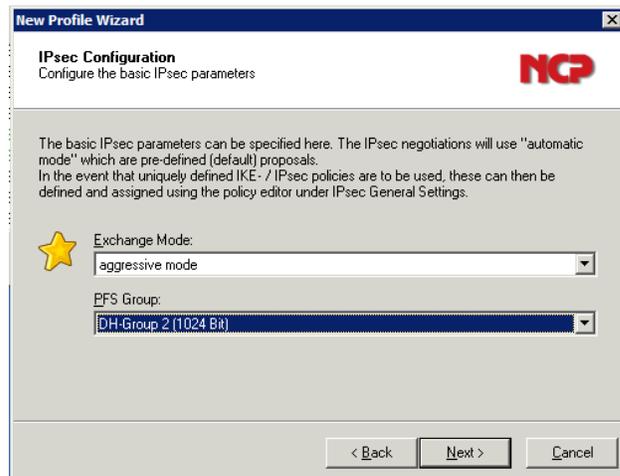


NCP Client with Juniper Junos

### 4.4. Exchange Mode

Exchange Mode: aggressive mode  
 PFS Group: DH-Group 2

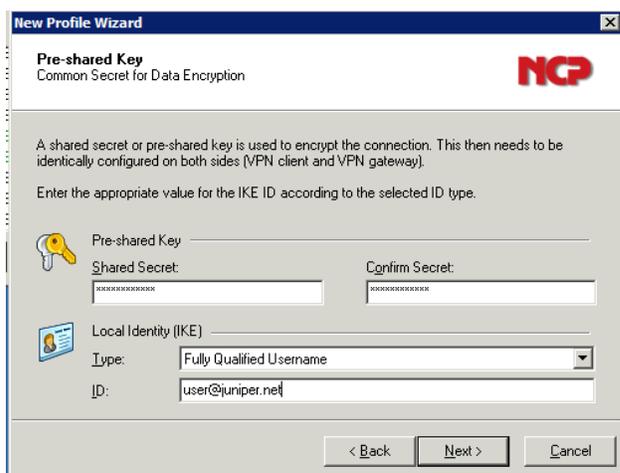
> Next



### 4.5. Pre-shared Key

Shared Secret: Tunneling123  
 Confirm Secret: Tunneling123  
 Local Identity (IKE): Fully Qualified Username  
 ID: [user@juniper.net](mailto:user@juniper.net)

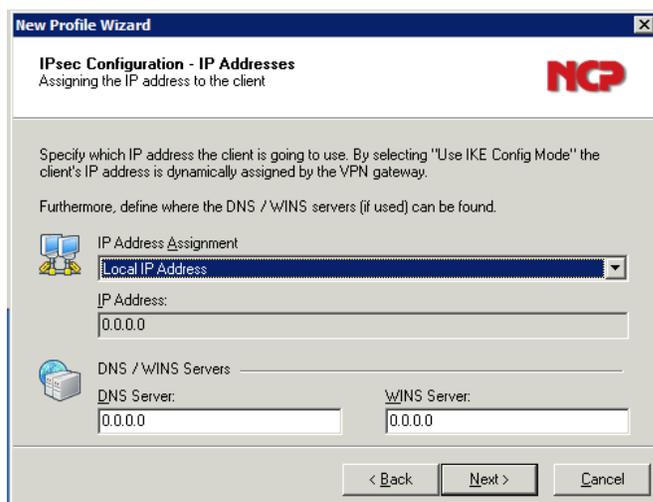
> Next



### 4.6. IPsec Configuration: IP Addresses

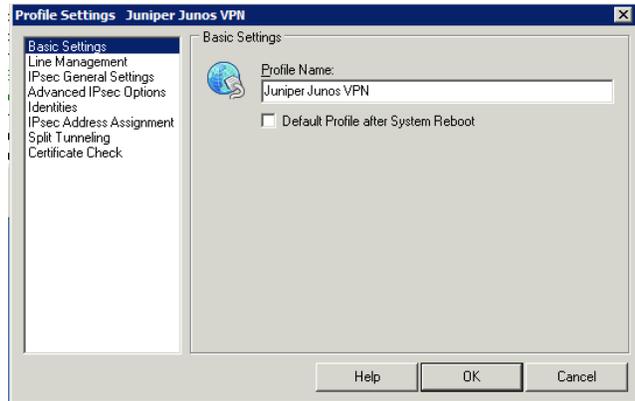
IP Address Assignment: Local IP Address

> Next > OK

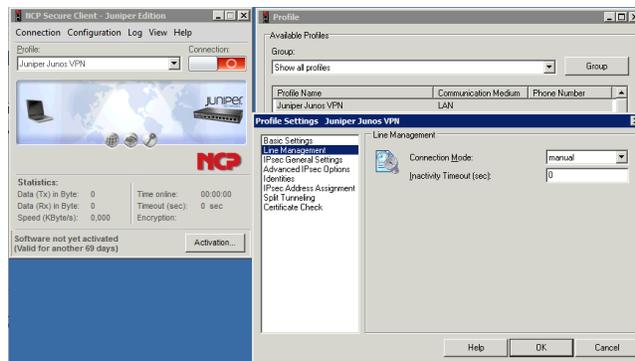


NCP Client with Juniper Junos

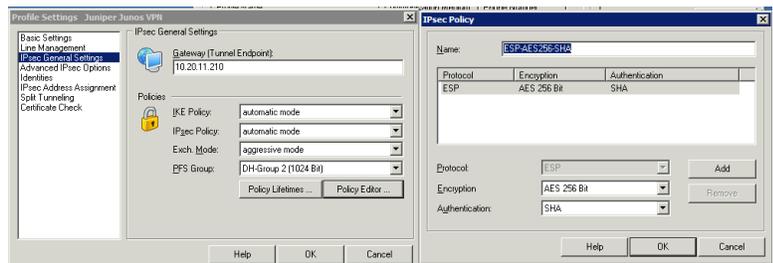
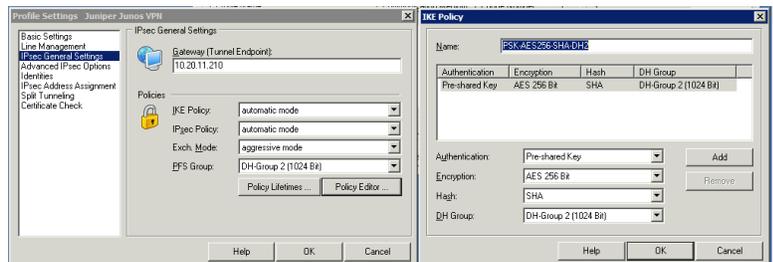
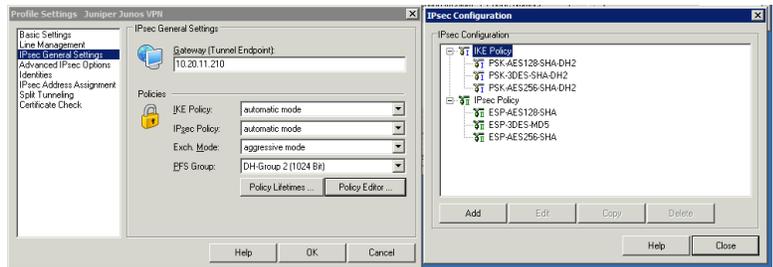
Edit the Profile to specify specific Profile > Juniper Junos VPN > Edit



Line Management:  
Inactivity Timeout: set to 0

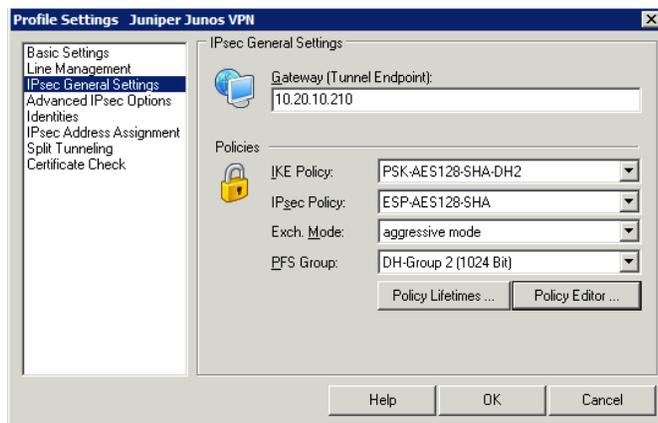


IPsec General Settings:  
Policy Editor  
Edit and/or Add the appropriate policies as needed

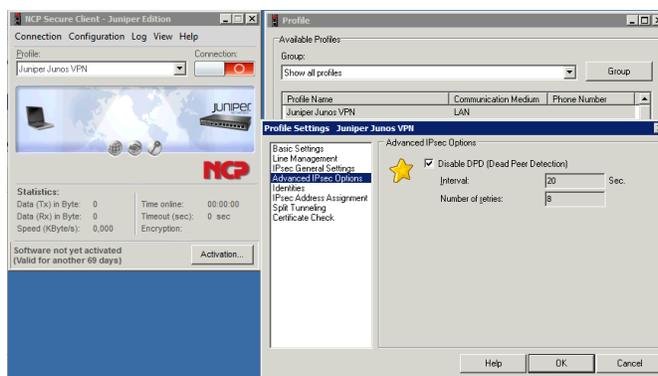


## NCP Client with Juniper Junos

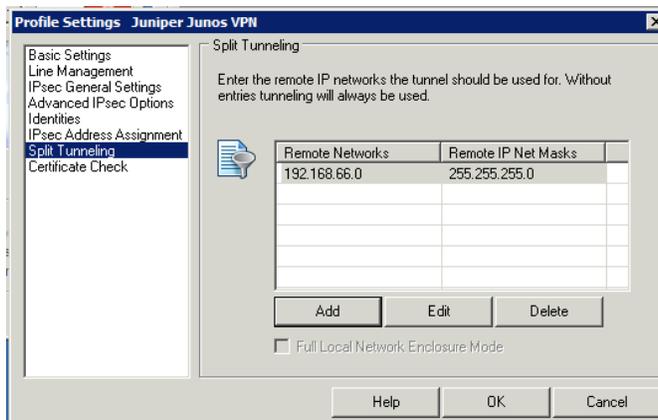
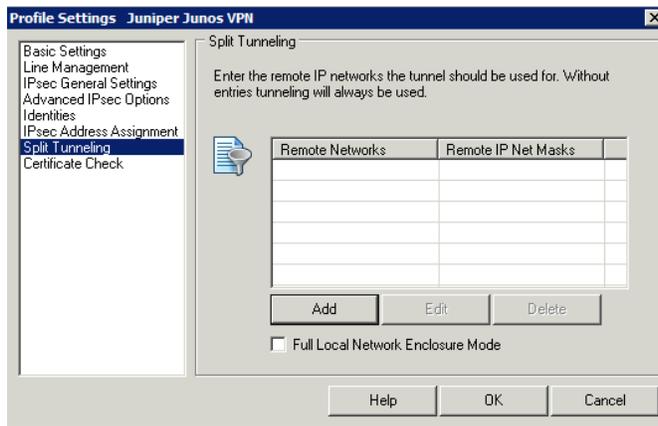
Select the configured policies from the IKE Policy and IPsec Policy drop-down menu



Advanced IPsec Options:  
Disable DPD (Dead Peer Detection)  
Enable this option by marking the checkbox

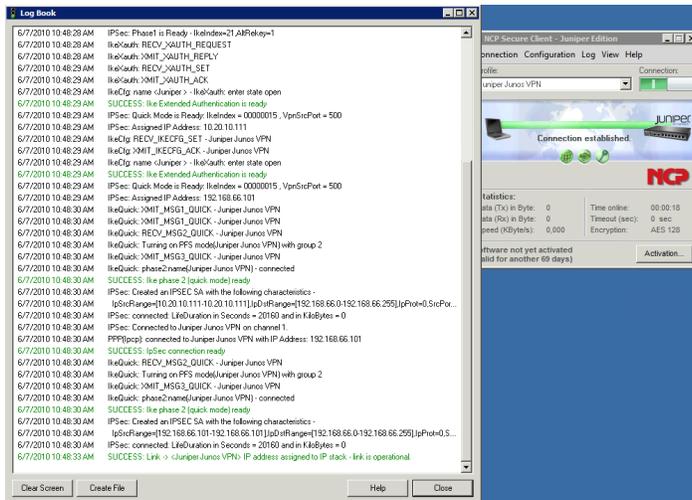


Split Tunneling:  
In Remote Networks  
enter the VPN network address: 192.168.66.0 / 255.255.255.0



## NCP Client with Juniper Junos

Select OK and close all the windows.  
Click the connection button to establish the VPN gateway connection.



## 5. Remote Access VPN with Xauth and Active Directory

The following configuration is used for Active Directory configuration.

On the Juniper SRX gateway you need to configure the LDAP Server and options:

```
access {
  profile xauth-users {
    authentication-order ldap;
  }
  ldap-options {
    base-distinguished-name cn=users,dc=vpnaccess,dc=local;
    search {
      search-filter sAMAccountName=;
      admin-search {
        distinguished-name cn=Administrator,cn=Users,dc=vpnaccess,dc=local;
        password "$9$VebgaZGi.fzDiORSeXxDikqmTz369tu"; ## SECRET-DATA
      }
    }
  }
  ldap-server {
    192.168.66.11;
  }
}
```

## 6. Multiple Subnets

If multiple subnets are referenced in the same policy, the proxy-ids 0.0.0.0/0 are used for both local and remote!

```
Apr 20 11:13:47 matched configured proxy ids: re-
mote=ipv4_subnet(any:0,[0..7]=0.0.0.0/0) lo-
cal=ipv4_subnet(any:0,[0..7]=0.0.0.0/0) in vpn: INSTANCE-vpn ncp_0002_0005_0000.
```

You will need to create multiple policies for this situation. Also you will need to configure as many VPN entries under ipsec and refer to the same gateway, as the same VPN cannot be used in multiple security policies.

Wrong:

```
policy tr-utr-ncp { match { source-address [ LAN-ONE LAN-TWO LAN-THREE ];
                                ## Cannot have multiple subnets
                        destination-address any; application any; } then { permit { tunnel { ipsec-vpn vpn-ncp; }
} } }
```

## 7. Troubleshooting

The following section provides a few troubleshooting tips.

### 7.1. Verifying Firewall User Authentication

The following section provides information on how to display the firewall authentication user history.

To provide higher level of debug information, traceoptions can be used in the firewall authentication:

```
firewall-authentication {
traceoptions {
flag {
all <detail | extensive | terse>;
authentication <detail | extensive | terse>;
proxy <detail | extensive | terse>;
```

Use the show security firewall-authentication CLI command to display information on authenticated firewall users. For more information, see the *JUNOS Software CLI Reference*.

```
user@host# show security firewall-authentication history
History of firewall authentication data: Authentications: 2 Id Source Ip Date
Time Duration Status User 1 99.99.99.1 2007-10-12 21:24:02 0:00:24 Failed troy 2
99.99.99.1 2007-10-12 21:24:48 0:00:22 Success voyager user@host> show security
firewall-authentication history identifier 1 Username: troy Source IP: 99.99.99.1
Authentication state: Failed Authentication method: Pass-through using Telnet
Access start date: 2007-10-12 Access start time: 21:24:02 Duration of user ac-
cess: 0:00:24 Policy name: lnx2-telnet-lnx1 Source zone: dl2 Destination zone:
```

### NCP Client with Juniper Junos

```
dl1 Access profile: wonder Bytes sent by this user: 0 Bytes received by this
user: 2660 Client-groups: Sunnyvale Bangalore user@host> show security firewall-
authentication users Firewall authentication data: Total users in table: 1 Id
Source Ip Src zone Dst zone Profile Age Status User 3 99.99.99.1 dl2 dl1
wonder 1 Failed TechPubs user@host> show security firewall-authentication
users identifier 3 Username: TechPubs Source IP: 99.99.99.1 Authentication state:
Failed Authentication method: Pass-through using Telnet Age: 1 Access time
remaining: 9 Source zone: dl2 Destination zone: dl1 Policy name: lnx2-telnet-lnx1
Access profile: wonder Interface Name: ge-0/0/1.0 Bytes sent by this user: 0
Bytes received by this user: 1521
```

#### What it Means

The output displays information about firewall users authenticating to the network.

Verify the following information:

- ▶ Number of firewall users who successfully authenticated and firewall users who failed to log in.
- ▶ Details on each firewall user trying to authenticate.

## 7.2. Traceoptions (Flow)

#### Syntax

```
traceoptions {
    file filename <files number > <match regular-expression > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag ;
}
```

#### Hierarchy Level

[edit security flow]

#### Release Information

Statement introduced in Release 8.5 of JUNOS software.

#### Description

Configure flow tracing options.

This statement is supported on J-series and SRX-series devices.

## 7.3. Traceoptions (IKE)

### Syntax

```
traceoptions {  
    file filename {  
        <files number >;  
        <match regular-expression >;  
        <size maximum-file-size >;  
        <world-readable | no-world-readable>;  
    }  
    flag flag ;  
}
```

### Hierarchy Level

[edit security ike]

## 7.4. Traceoptions (IPsec)

### Syntax

```
traceoptions {  
    flag {  
        all;  
        next-hop-tunnel-binding;  
        packet-drops;  
        packet-processing;  
        security-associations;  
    }  
}
```

### Hierarchy Level

[edit security ipsec]

## 7.5. Traceoptions General

set system processes general-authentication-service traceoptions flag all

i.e. for authd /var/log/authd

set security firewall-authentication traceoptions flag all i.e. for fwauthd /var/log/fwauthd

## 8. Table 1: IPsec Services Operational Mode Commands

Task	Command
<b>Adaptive Services Interface</b>	
Delete certificate authority (CA) digital certificates from the router.	<a href="#">clear security pki ca-certificate</a>
Delete manually generated local digital certificate requests from the router.	<a href="#">clear security pki certificate-request</a>
Delete all CRLs from the router.	<a href="#">clear security pki crl</a>
Delete local digital certificates, certificate requests, and the corresponding public/private key pairs from the router.	<a href="#">clear security pki local-certificate</a>
Delete local and remote certificates from the IPsec configuration memory cache.	<a href="#">clear services ipsec-vpn certificates</a>
Clear IPsec statistics.	<a href="#">clear services ipsec-vpn ipsec statistics</a>
Clear either Internet Key Exchange (IKE) or IPsec VPN security associations.	<a href="#">clear services ipsec-vpn ike security-associations</a> <a href="#">clear services ipsec-vpn ipsec security-associations</a>
Request a digital certificate from a CA online by using the Simple Certificate Enrollment Protocol (SCEP).	<a href="#">request security pki ca-certificate enroll</a>
Manually load a CA digital certificate from a specified location.	<a href="#">request security pki ca-certificate load</a>
Manually install a CRL on the router.	<a href="#">request security pki crl load</a>
Manually generate a local digital certificate request in the Public-Key Cryptography Standards #10 (PKCS-10) format.	<a href="#">request security pki generate-certificate-request</a>
Generate a Public Key Infrastructure (PKI) public and private key pair for a local digital certificate.	<a href="#">request security pki generate-key-pair</a>
Request a CA to enroll and install a local digital certificate online by using the SCEP.	<a href="#">request security pki local-certificate enroll</a>
Manually load a local digital certificate from a specified location.	<a href="#">request security pki local-certificate load</a>
Switch between the primary and backup IPsec VPN tunnels.	<a href="#">request services ipsec-vpn ipsec switch tunnel</a>
Display information about certificate authority (CA) digital certificates installed in the router.	<a href="#">show security pki ca-certificate</a>
Display information about manually generated local digital certificate requests that are stored in the router.	<a href="#">show security pki certificate-request</a>
Display information about the local digital certificates and the corresponding public keys installed in the router.	<a href="#">show security pki local-certificate</a>
Display local and remote certificates installed in the IPsec configuration memory cache that are used for the IKE negotiation.	<a href="#">show services ipsec-vpn certificates</a>
Display IKE VPN security associations for service sets.	<a href="#">show services ipsec-vpn ike security-associations</a>
Display IPsec VPN security associations for service sets.	<a href="#">show services ipsec-vpn ipsec security-associations</a>
Display IPsec VPN statistics for service sets.	<a href="#">show services ipsec-vpn ipsec statistics</a>
<b>Encryption Interface</b>	
Clear Internet Key Exchange (IKE) security associations.	<a href="#">clear ike security-associations</a>
Clear IPsec security associations.	<a href="#">clear ipsec security-associations</a>
Switch between primary and backup interfaces and tunnels.	<a href="#">request ipsec switch</a>
Obtain a public key certificate from a certification authority.	<a href="#">request security certificate (signed)</a> <a href="#">request security certificate (unsigned)</a>
Generate a public and private key pair.	<a href="#">request security key-pair</a>
Add a certificate provided by the Juniper Networks certificate authority.	<a href="#">request system certificate add</a>

### NCP Client with Juniper Junos

Display IKE security association information.	<a href="#">show ike security-associations</a>
Display the IPsec certificate database.	<a href="#">show ipsec certificates</a>
Display primary and backup interface and tunnel information.	<a href="#">show ipsec redundancy</a>
Display IPsec security association information.	<a href="#">show ipsec security-associations</a>
Display installed certificates signed by the Juniper Networks certificate authority.	<a href="#">show system certificate</a>

### References

1. JUNOS Enhanced Services, Remote Access VPN with XAuth, Configuration and Troubleshooting Version 1.4, Richard Kim, Technical Support Engineer, Advanced JTAC
2. Configuring Dynamic VPN, Version 1.2, November 2009
3. JUNOS® Software CLI Reference
4. IP Security Operational Mode Commands, [http://www.juniper.net/techpubs/en\\_US/junos10.4/topics/reference/general/ip-security-op-cmd-table.html](http://www.juniper.net/techpubs/en_US/junos10.4/topics/reference/general/ip-security-op-cmd-table.html)

Published: 2010-11-08