



SECURE COMMUNICATIONS

Quick Installation Guide

high security remote access

Quick Installation Guide NCP Client with Juniper ScreenOS

As of March 2012
version 1.1

NCP Client with Juniper ScreenOS

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

Support

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

Email Addresses

helpdesk@ncp-e.com (English)
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

1. Revision History	4
2. Policy-Based VPN & Shared IKE ID with Preshared Key.....	5
3. Juniper Gateway Configuration - WebUI.....	7
4. NCP Client Wizard:	18
4.1. Connection Type.....	18
4.2. Profile Name	18
4.3. VPN Gateway Parameters.....	18
4.4. Exchange Mode	19
4.5. Pre-shared Key	19
4.6. IPsec Configuration: IP Addresses.....	19
5. NCP Client Configuration – Profile changes.....	20
6. Route-Based VPN & Multiple Proxy ID support on a Route-Based VPN	24
7. Advanced Configuration	33
8. Troubleshooting	54
8.1. Juniper Gateway Event Log	54
8.2. CLI Debugging	54

NCP Client with Juniper ScreenOS

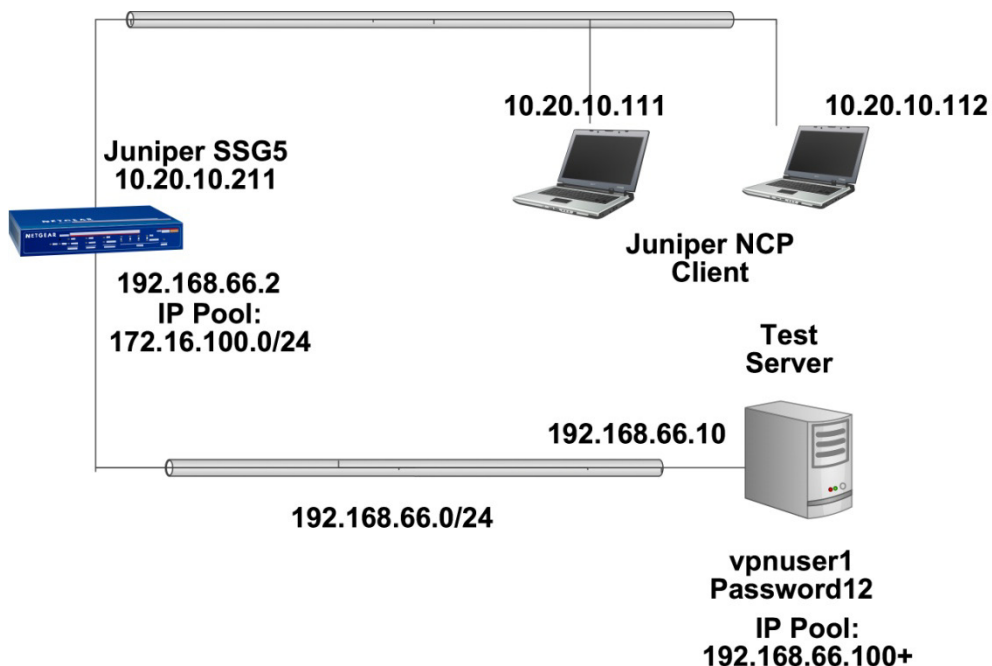
1. Revision History

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

Junos Version	NCP Client Version	Date	Changes
6.1.0r7.0	9.22 Build 63	2010-06-23	Initial document
	9.23 Build 17	2010-07-21	New NCP client version
6.3.0r4.0	9.23 Build 17	2010-08-06	New ScreenOS version
		2010-09-01	Edits and formatting
		2010-09-14	Edits and formatting
		2010-09-29	Policy and Route VPN
		2010-10-15	Update in AD config
		2010-12-20	Added Certificate config
	9.23 Build 64	2011-01-30	New NCP client version
6.3.0r7.0	9.24 Build 65	2011-05-13	New NCP client version supporting IKEv2
	9.24 Build 95	2011-09-07	Revised Multiple Logins with same IKE ID

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.



Because the SSG5 VPN pool is in the 172.16.100.0 network range we must add a persistent route in the Test Server unless the Juniper is the default gateway.

NCP Client with Juniper ScreenOS

```

Administrator: C:\Windows\system32\cmd.exe
C:\>route -p add 172.16.100.0 mask 255.255.255.0 192.168.66.2
OK!

C:\>netstat -rn
=====
Interface List
14...00 0c 29 47 a1 e3 .....Intel(R) PRO/1000 MT Network Connection #2
11...00 0c 29 47 a1 b9 .....Intel(R) PRO/1000 MT Network Connection
1...00 00 00 00 00 00 .....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
15...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.66.1     192.168.66.10    266
10.20.0.0                  255.255.0.0      On-link          10.20.13.10      266
10.20.13.10                255.255.255.255  On-link          10.20.13.10      266
10.20.255.255              255.255.255.255  On-link          10.20.13.10      266
127.0.0.0                  255.0.0.0        On-link          127.0.0.1         306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1         306
127.255.255.255            255.255.255.255  On-link          127.0.0.1         306
172.16.100.0               255.255.255.0    192.168.66.2     192.168.66.10    11
172.168.66.0               255.255.255.0    On-link          192.168.66.10    266
192.168.66.10              255.255.255.255  On-link          192.168.66.10    266
192.168.66.255             255.255.255.255  On-link          192.168.66.10    266
224.0.0.0                  240.0.0.0        On-link          127.0.0.1         306
224.0.0.0                  240.0.0.0        On-link          192.168.66.10    266
224.0.0.0                  240.0.0.0        On-link          10.20.13.10       266
255.255.255.255            255.255.255.255  On-link          127.0.0.1         306
255.255.255.255            255.255.255.255  On-link          192.168.66.10    266
255.255.255.255            255.255.255.255  On-link          10.20.13.10       266
=====
Persistent Routes:
Network Address        Netmask          Gateway Address  Metric
0.0.0.0                0.0.0.0          192.168.66.1     Default
172.16.100.0           255.255.255.0    192.168.66.2     1
=====

```

2. Policy-Based VPN & Shared IKE ID with Preshared Key

With policy-based VPN tunnels, a tunnel is treated as an object (or a building block) that together with source, destination, service, and action, comprises a policy that permits VPN traffic. (Actually, the VPN policy action is tunnel, but the action permit is implied, if unstated). In a policy-based VPN configuration, a policy specifically references a VPN tunnel by name.

With route-based VPNs – which we will show later in this document, the policy does not specifically reference a VPN tunnel. Instead, the policy references a destination address. When the security device does a route lookup to find the interface through which it must send traffic to reach that address, it finds a route through a tunnel interface, which is bound to a specific VPN tunnel. We will explain the particular benefits of route-based VPN in the relevant section below in the document.

The Shared IKE ID feature facilitates the deployment of a large number of dialup users. With this feature, the security device authenticates multiple dialup VPN users using a single Group IKE ID and preshared key. Thus, it provides IPsec protection for large remote user groups through a common VPN configuration.

This feature is similar to the Group IKE ID with preshared keys feature (not described in this document), with the following differences:

- ▶ With the Group IKE ID feature, the IKE ID can be an email address or a fully qualified domain name (FQDN). For this feature, the IKE ID must be an email address.
- ▶ Instead of using the preshared key seed value and the full user IKE ID to generate a preshared key for each user, you specify a single preshared key for all users in the group.

NCP Client with Juniper ScreenOS

- ▶ You must use XAuth (for IKEv1) or EAP (for IKEv2) to authenticate the individual users.

To set up a Shared IKE ID and preshared key on the security device:

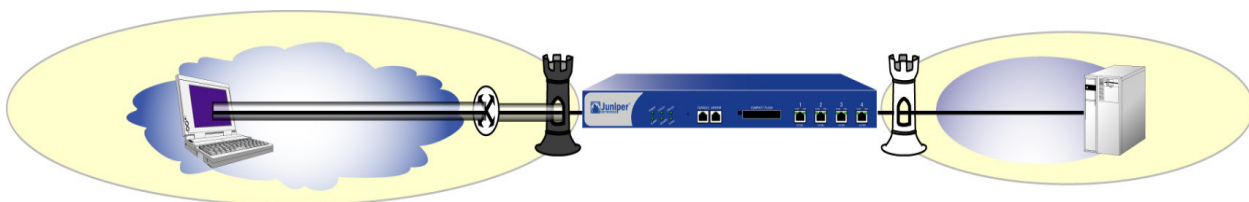
1. Create a new Group IKE ID user, and specify how many dialup users can use the Group IKE ID to log on. For this feature, use an email address as the IKE ID.
2. Assign the new Group IKE ID to a dialup user group.
3. In the dialup-to-LAN AutoKey IKE VPN configuration, create a Shared IKE ID gateway.
4. Define the XAuth users and enable XAuth on the remote IKE gateway.

On the VPN Client:

Configure a VPN tunnel to the security device using aggressive mode for Phase 1 negotiations, and enter the preshared key that you previously defined on the security device. Thereafter, the security device authenticates each remote user as follows:

- ▶ During Phase 1 negotiations, the security device first authenticates the VPN client by matching the IKE ID and preshared key that the client sends with the IKE ID and preshared key on the security device.
- ▶ If there is a match, then the security device uses XAuth to authenticate the individual user. It sends a login prompt to the user at the remote site between Phase 1 and Phase 2 IKE negotiations.
- ▶ If the remote user successfully logs on with the correct username and password, Phase 2 negotiations begin.

In this example, you create a new Group IKE ID user named "NCP Users". It accepts up to 25 Phase 1 negotiations concurrently from VPN clients with the same preshared key (Tunneling123). You name the dialup IKE user group "Office". In addition, you configure two XAuth users, test1@juniper.net and test2@juniper.net with Password "password".



3. Juniper Gateway Configuration - WebUI

Interfaces

Network > Interfaces > List > Edit (for ethernet0/3): Enter the following, and then click **OK**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 192.168.66.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > List > Edit (for ethernet0/0): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 10.20.10.211/16

IP Pool

Objects > IP Pools > Local > New:

Enter the following, and then click **OK**:

IP Pool Name: VPN Pool

Start IP: 172.16.100.100

End IP: 172.16.100.200

The screenshot shows the Juniper ScreenOS WebUI interface. At the top, a blue navigation bar contains the text "Objects > IP Pools > Edit" on the left and "ssg5-v92" with a help icon on the right. Below the navigation bar is a large light blue rectangular area representing a configuration dialog. Inside this area, there are three rows of labels and text input fields: "IP Pool Name" with the value "vpn_pool", "Start IP" with the value "172.16.100.100", and "End IP" with the value "172.16.100.200". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

NCP Client with Juniper ScreenOS

Users

Create the Shared IKE ID:

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

User Name: NCP Users

Status: Enable

IKE User: (select)

Number of Multiple Logins with Same ID: 25

Simple Identity: (select)

IKE ID Type: U-FQDN

IKE Identity: users@juniper.net

The screenshot shows the Juniper ScreenOS configuration window for 'Auth/IKE/XAuth/L2TP User'. The 'User Name' is 'NCP Users' and 'Status' is 'Enable'. Under 'IKE User', 'Simple Identity' is selected with 'IKE ID Type' set to 'U-FQDN' and 'IKE Identity' set to 'users@juniper.net'. The 'Number of Multiple Logins with Same ID' is set to 25. There are checkboxes for 'Authentication User', 'XAuth User', and 'L2TP User', all of which are currently unchecked. Password fields for 'User Password' and 'Confirm Password' are present but empty. The interface includes a sidebar with navigation options like Home, Configuration, Network, Security, Policy, and VPNs.

Create a Group:

Objects > Users > Local Groups > New: Type Office in the Group Name field, do the following, and then click OK:

Select NCP Users and use the << button to move him from the Available Members column to the Group Members column.

The screenshot shows the 'Group Name' field set to 'Office'. Below it are two columns: '<-- Group Members -->' and '<-- Available Members -->'. The 'Available Members' column contains 'NCP Users'. Between the columns are '<<' and '>>' buttons. At the bottom are 'OK' and 'Cancel' buttons.

NCP Client with Juniper ScreenOS

Create the Xauth Users:

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

User Name: test1@juniper.net

Status: Enable

XAuth User: Checked

User Password: password

Confirm Password: password

L2TP/XAuth Remote Settings

IP Pool: VPN Pool

The screenshot shows the Juniper ScreenOS configuration window for creating a new user. The breadcrumb trail is 'Objects > Users > Local > Edit'. The user name is 'test1@juniper.net' and the status is 'Enable'. Under 'Auth/IKE/XAuth/L2TP User', the 'XAuth User' checkbox is checked. The 'L2TP/XAuth Remote Settings' section shows the 'IP Pool' set to 'VPN Pool'. The 'User Password' and 'Confirm Password' fields are both set to 'password' (masked with dots). The 'Number of Multiple Logins with Same ID' is set to 1. The 'Static IP', 'Primary WINS IP', and 'Secondary WINS IP' fields are all set to '0.0.0.0'. The 'Primary DNS IP' and 'Secondary DNS IP' fields are also set to '0.0.0.0'. The 'OK' and 'Cancel' buttons are at the bottom right.

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

User Name: test2@juniper.net

Status: Enable

XAuth User: Checked

User Password: password

Confirm Password: password

L2TP/XAuth Remote Settings

IP Pool: VPN Pool

This screenshot is identical to the one above, showing the Juniper ScreenOS configuration window for creating a new user. The user name is 'test2@juniper.net'. All other settings, including the checked 'XAuth User' checkbox, the 'VPN Pool' IP pool, the 'password' for both password fields, and the various IP and DNS settings, are the same as in the first screenshot.

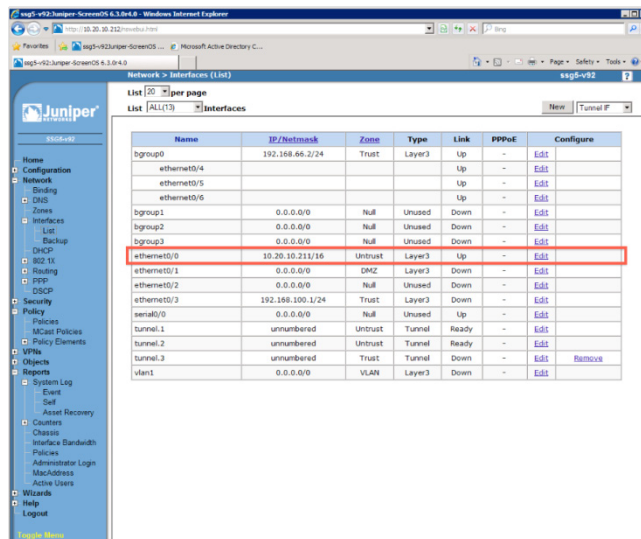
NCP Client with Juniper ScreenOS

If you don't use the Shared IKE ID functionality but configure each user individually you can combine both configuration steps (IKE User and Xauth User) for every user. Create one user as IKE User, Simple Identity (either FQDN or U-FQDN) and enable Xauth User with Password and IP Pool assigned. Then add all the users into one Group.

Gateway

The Gateway configuration needs to be bound to the correct external interface. So before you go to the Gateway configuration screen you should validate your correct Outgoing Interface, the interface that is in the Untrust Zone and where the users will connect to from the Outside.

For this go to Network > Interfaces (List) and identify the correct Interface



Name	IP/Network	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.66.2/24	Trust	Layer3	Up	-	Edit
ethernet0/4				Up	-	Edit
ethernet0/5				Up	-	Edit
ethernet0/6				Up	-	Edit
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/0	10.20.10.11/16	Untrust	Layer3	Up	-	Edit
ethernet0/1	0.0.0.0/0	DMZ	Layer3	Down	-	Edit
ethernet0/2	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/3	192.168.100.1/24	Trust	Layer3	Down	-	Edit
serial0/0	0.0.0.0/0	Null	Unused	Up	-	Edit
tunnel.1	unnumbered	Untrust	Tunnel	Ready	-	Edit
tunnel.2	unnumbered	Untrust	Tunnel	Ready	-	Edit
tunnel.3	unnumbered	Trust	Tunnel	Down	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Here the external facing Interface is the default ethernet0/0.

Now turn to the Gateway configuration.

VPNs > AutoKey > Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: VPN Gateway

Version: IKEv1

Remote Gateway: (select)

Dialup User Group: (select)

Group: Office

NCP Client with Juniper ScreenOS

Advanced

Preshared Key: Tunneling123

Outgoing Interface: ethernet0/0 (Note your own configuration may be different!)

Security Level: User Defined: Custom (select)

Phase 1 Proposal: pre-g2-aes128-sha

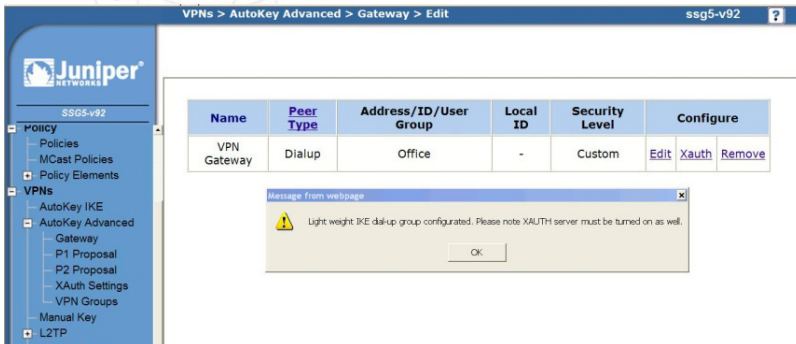
Mode (Initiator): Aggressive

Enable NAT-Traversal (recommended)

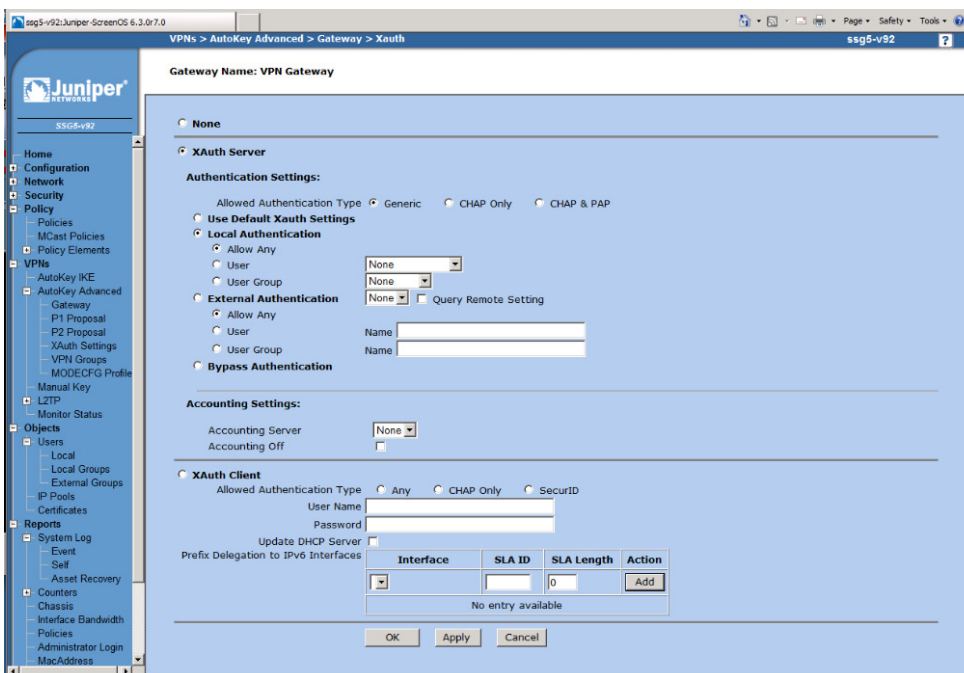
UDP Checksum (recommended)

You will get a Warning message to configure Xauth.

NCP Client with Juniper ScreenOS



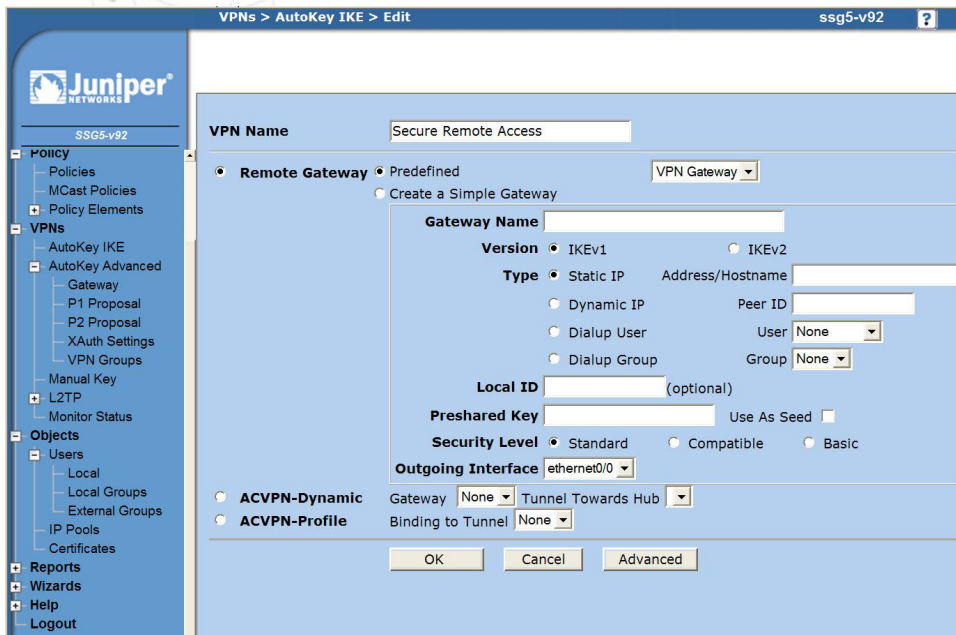
VPNs > AutoKey > Advanced > Gateway > Xauth: Enter the following, and then click **OK**:
 Xauth Server: (select)
 Local Authentication: (select)
 Allow Any



AutoKey IKE

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:
 VPN Name: Secure Remote Access
 Remote Gateway: (select)
 Predefined: VPN Gateway

NCP Client with Juniper ScreenOS



VPN Name: Secure Remote Access

☒ Remote Gateway ☐ Predefined ☐ Create a Simple Gateway

Gateway Name:

Version: ☒ IKEv1 ☐ IKEv2

Type: ☒ Static IP Address/Hostname:

☐ Dynamic IP Peer ID:

☐ Dialup User User:

☐ Dialup Group Group:

Local ID: (optional)

Preshared Key: Use As Seed: ☐

Security Level: ☒ Standard ☐ Compatible ☐ Basic

Outgoing Interface: ethernet0/0

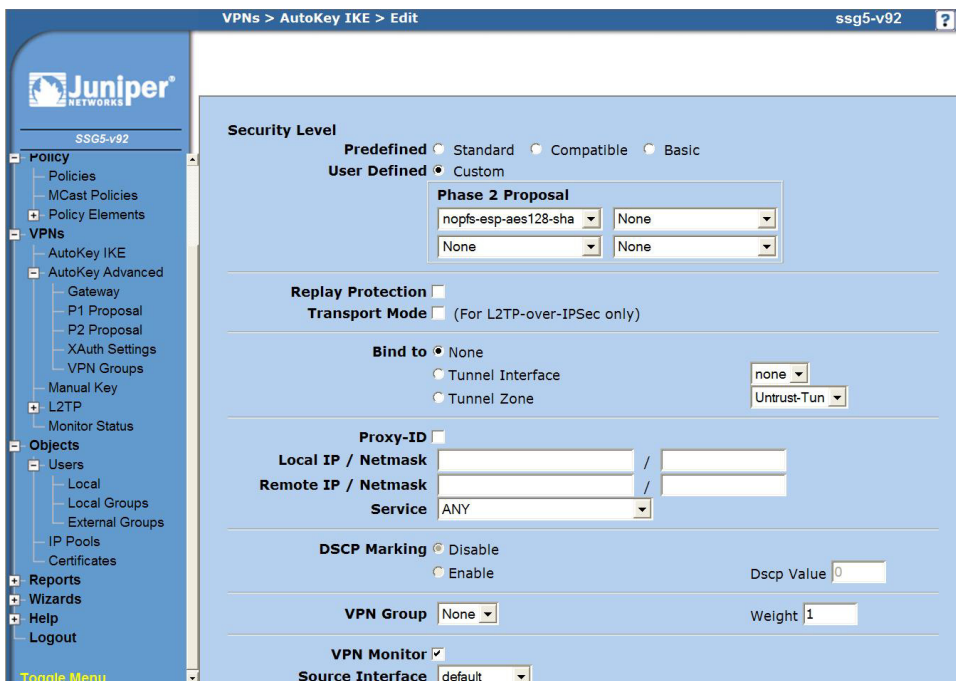
☐ ACVPN-Dynamic Gateway: Tunnel Towards Hub:

☐ ACVPN-Profile Binding to Tunnel:

OK Cancel Advanced

Advanced

Security Level: User Defined: Custom (select)
 Phase 2 Proposal: nopfs-esp-aes128-sha
 VPN Monitor: (select)



Security Level: ☒ Predefined ☐ Standard ☐ Compatible ☐ Basic

User Defined: ☒ Custom

Phase 2 Proposal:

Replay Protection: ☐

Transport Mode: ☐ (For L2TP-over-IPSec only)

Bind to: ☒ None ☐ Tunnel Interface ☐ Tunnel Zone

Proxy-ID: ☐

Local IP / Netmask: /

Remote IP / Netmask: /

Service: ANY

DSCP Marking: ☒ Disable ☐ Enable Dscp Value:

VPN Group: Weight:

VPN Monitor: ☒

Source Interface: default

NCP Client with Juniper ScreenOS

Policies

For your Policies you have the option to create either a generic Policy to any unspecified network or to specify a specific network for which the SA is created.

First we show the configuration for a generic Any network.

Policy > Policies

From: Untrust To: Trust

> New: Enter the following, and then click **OK**:

Source Address: Address Book Entry: Dial-Up VPN

Destination Address: Address Book Entry: Any

Action: Tunnel

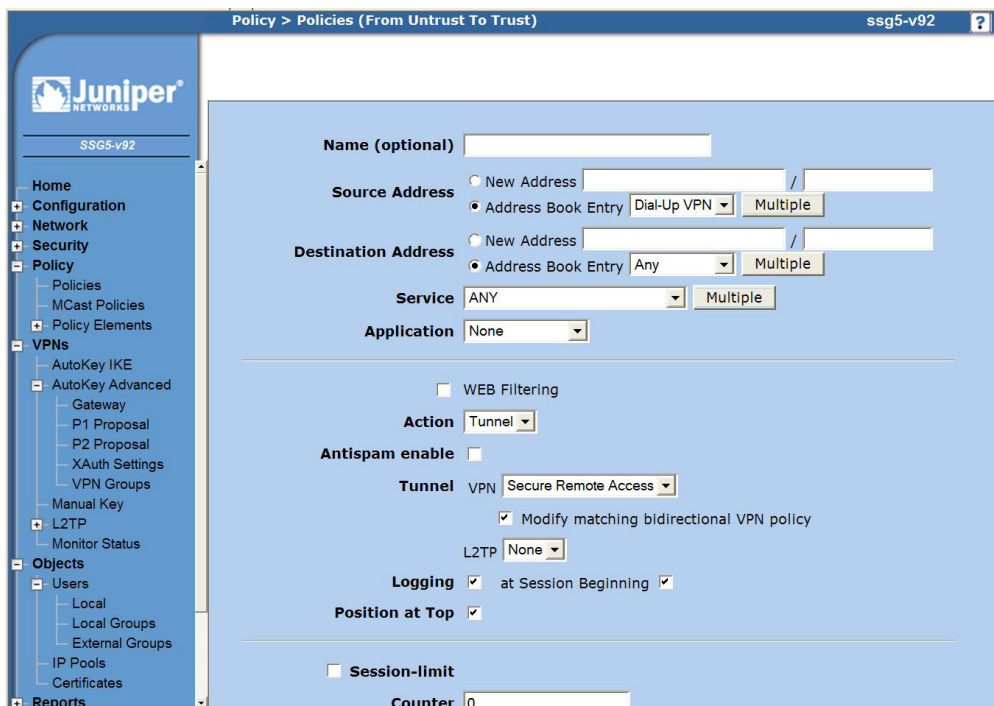
Tunnel: VPN: Secure Remote Access

Modify matching bidirectional VPN policy: (enable)

Logging: (select)

at Session Beginning: (select)

Position at Top: (select)



Policy > Policies (From Untrust To Trust) ssg5-v92

Name (optional)

Source Address
☐ New Address
☒ Address Book Entry: Dial-Up VPN

Destination Address
☐ New Address
☒ Address Book Entry: Any

Service ANY

Application None

☐ WEB Filtering

Action Tunnel

Antispam enable ☐

Tunnel VPN: Secure Remote Access

☒ Modify matching bidirectional VPN policy

L2TP None

Logging ☒ at Session Beginning ☒

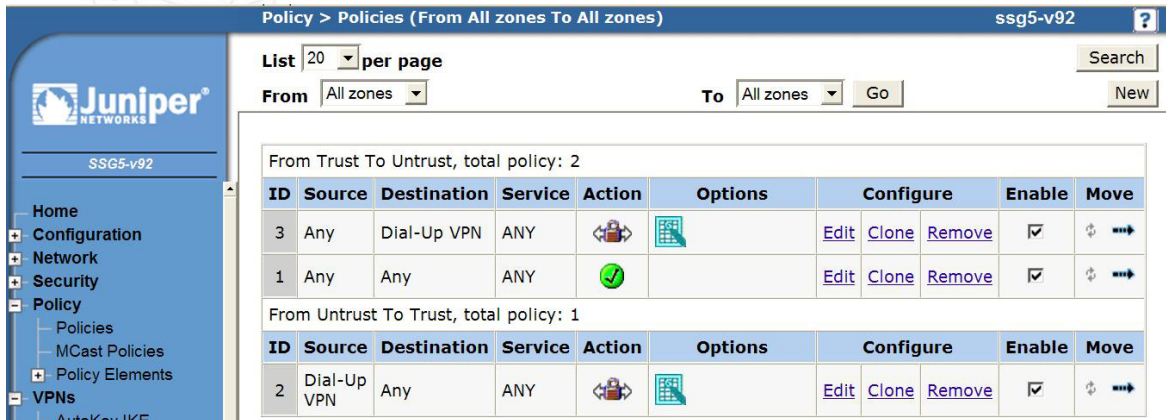
Position at Top ☒

☐ **Session-limit**

Counter 0

Watch for two policies created in the two specified zones.

NCP Client with Juniper ScreenOS



Policy > Policies (From All zones To All zones) ssg5-v92

List 20 per page

From All zones To All zones Go New

From Trust To Untrust, total policy: 2

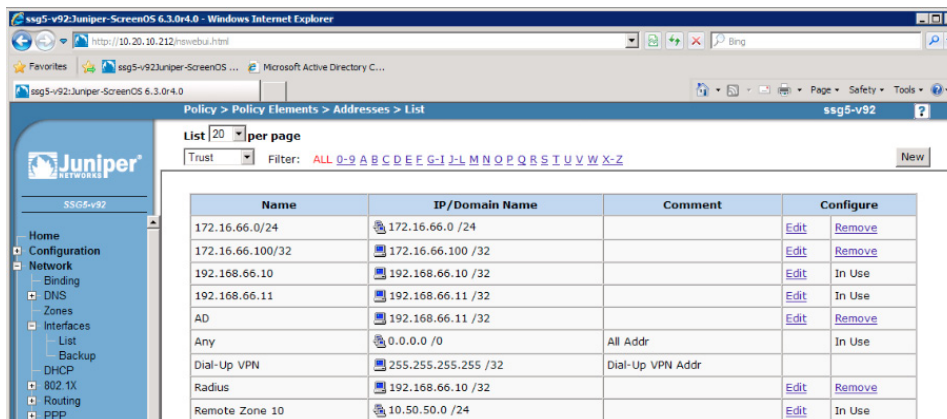
ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
3	Any	Dial-Up VPN	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	
1	Any	Any	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	

From Untrust To Trust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
2	Dial-Up VPN	Any	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	

For a specific Network Policy, which is recommended over the Any approach, you first create an entry in the Addresses List for the protected network segment(s) in the Trust Zone. Here we want to protect the network 192.168.66.0/24.

Policy > Policy Elements > Addresses > List
Select Filter Trust



ssg5-v92:Juniper-ScreenOS 6.3.0r4.0 - Windows Internet Explorer

http://10.20.10.212/nwwebui.html

Policy > Policy Elements > Addresses > List ssg5-v92

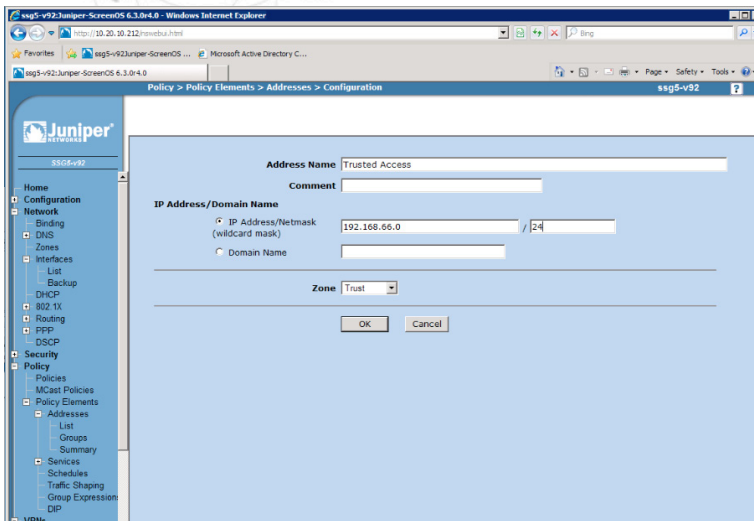
List 20 per page

Trust Filter: ALL 0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z New

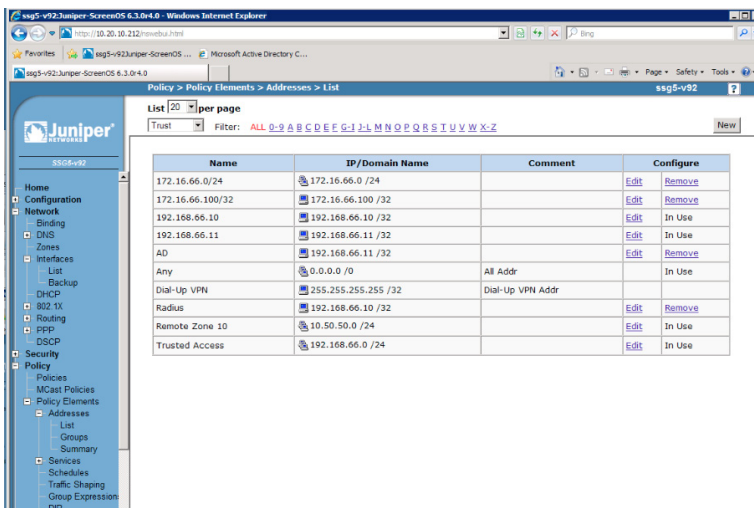
Name	IP/Domain Name	Comment	Configure
172.16.66.0/24	172.16.66.0 /24		Edit Remove
172.16.66.100/32	172.16.66.100 /32		Edit Remove
192.168.66.10	192.168.66.10 /32		Edit In Use
192.168.66.11	192.168.66.11 /32		Edit In Use
AD	192.168.66.11 /32		Edit Remove
Any	0.0.0.0 /0	All Addr	In Use
Dial-Up VPN	255.255.255.255 /32	Dial-Up VPN Addr	
Radius	192.168.66.10 /32		Edit Remove
Remote Zone 10	10.50.50.0 /24		Edit In Use

Select New
Address Name: Trusted Access
IP Address/Netmask: 192.168.66.0 / 24
Zone: Trust

NCP Client with Juniper ScreenOS



Select OK



Now we show the configuration of a Policy for a specific protected network.

Policy > Policies

From: Untrust To: Trust

> New: Enter the following, and then click **OK**:

Source Address: Address Book Entry: Dial-Up VPN

Destination Address: Address Book Entry: Trusted Access

Action: Tunnel

Tunnel: VPN: Secure Remote Access

Modify matching bidirectional VPN policy: (enable)

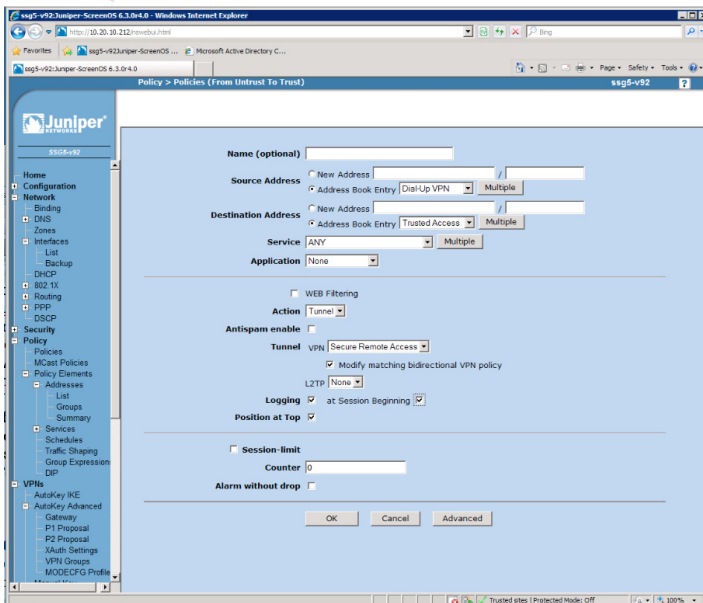
Logging: (select)

at Session Beginning: (select)

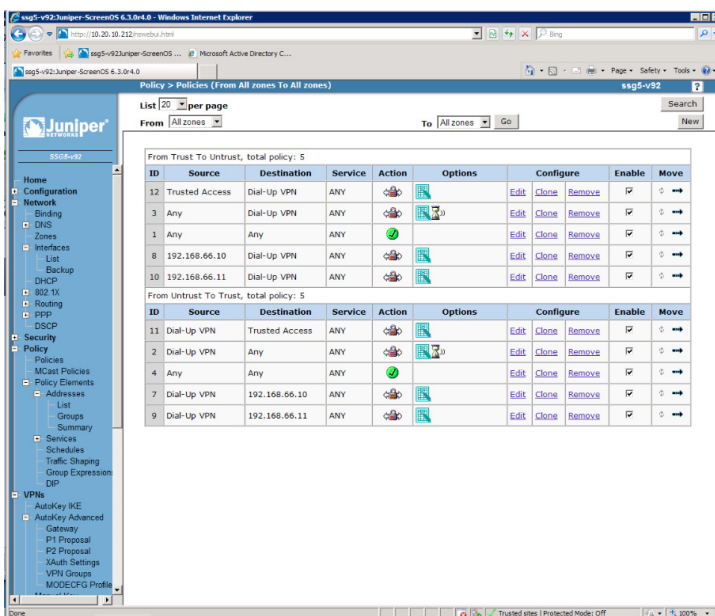
Position at Top: (select)

Quick Installation Guide

NCP Client with Juniper ScreenOS



Select OK



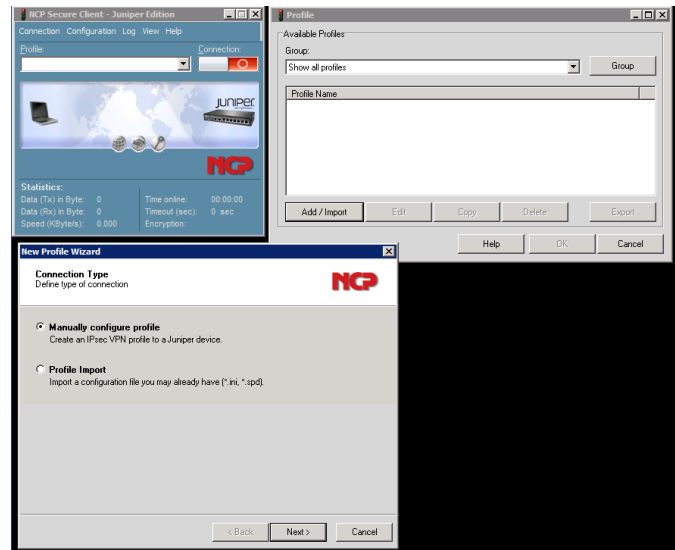
NCP Client with Juniper ScreenOS

4. NCP Client Wizard:

4.1. Connection Type

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

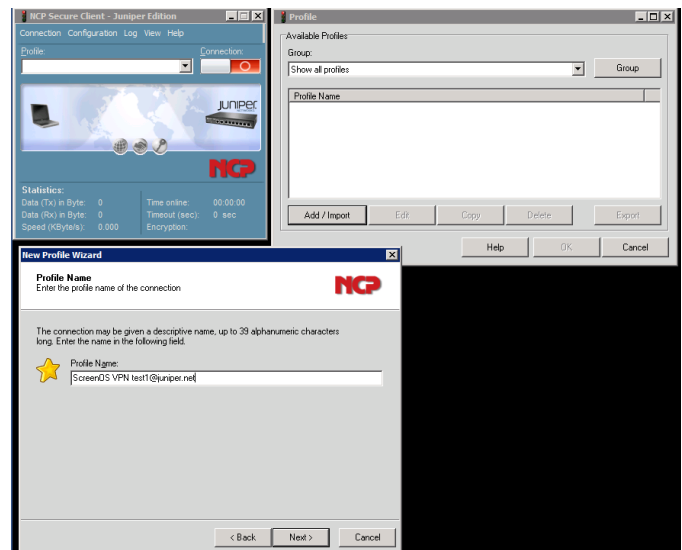
> Next



4.2. Profile Name

Configuration
Profile Name: ScreenOS VPN test1@juniper.net

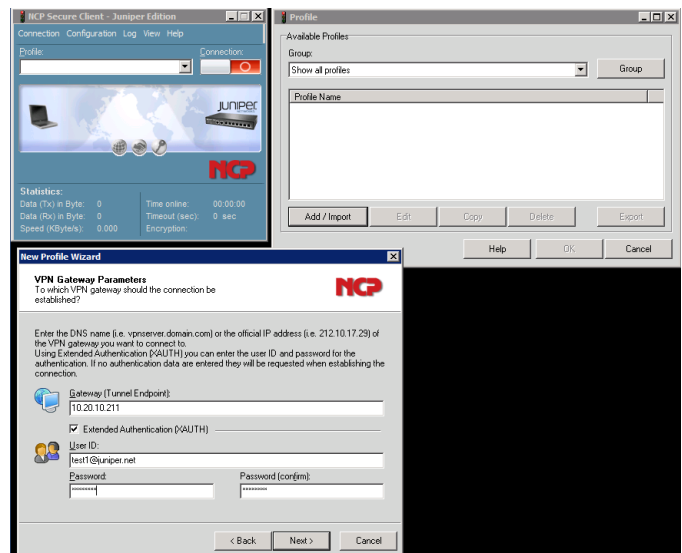
> Next



4.3. VPN Gateway Parameters

Gateway (Tunnel Endpoint): 10.20.10.210
Extended Authentication (XAUTH): (select)
UserID: test1@juniper.net
Password: password
Password (confirm): password

> Next

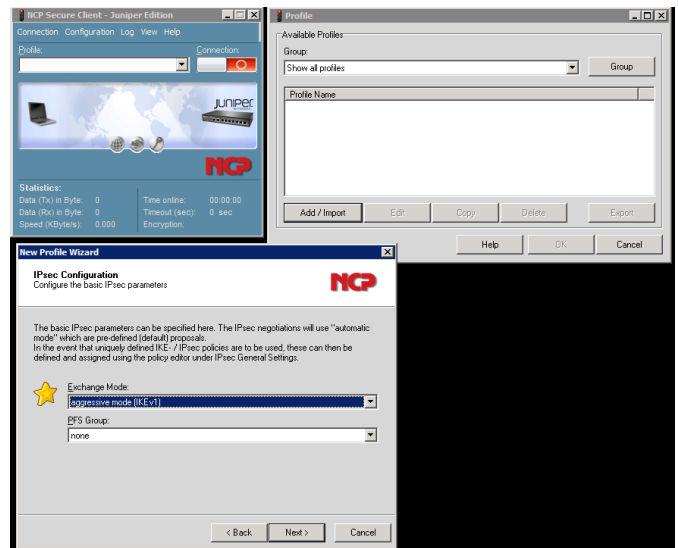


NCP Client with Juniper ScreenOS

4.4. Exchange Mode

Exchange Mode: aggressive mode
PFS Group: none

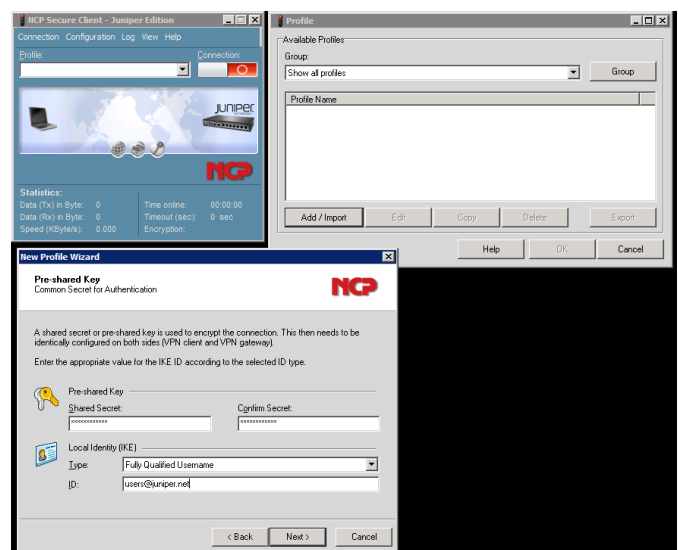
> Next



4.5. Pre-shared Key

Shared Secret: Tunneling123
Confirm Secret: Tunneling123
Local Identity (IKE): Fully Qualified Username
ID: users@juniper.net

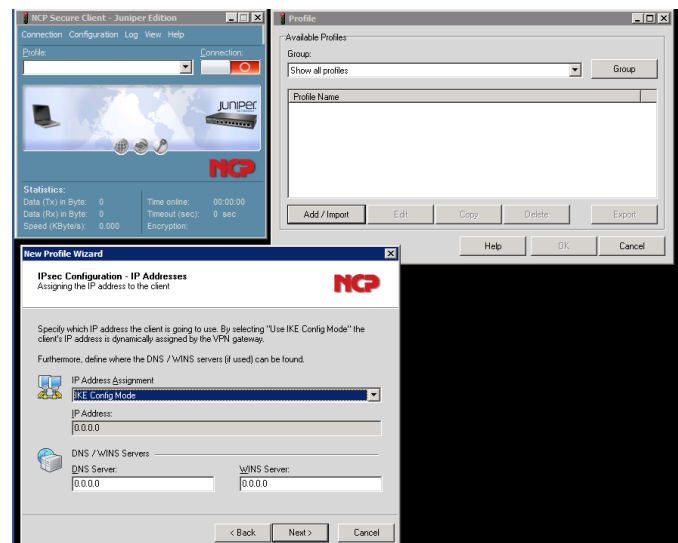
> Next



4.6. IPsec Configuration: IP Addresses

IP Address Assignment: IKE Config Mode

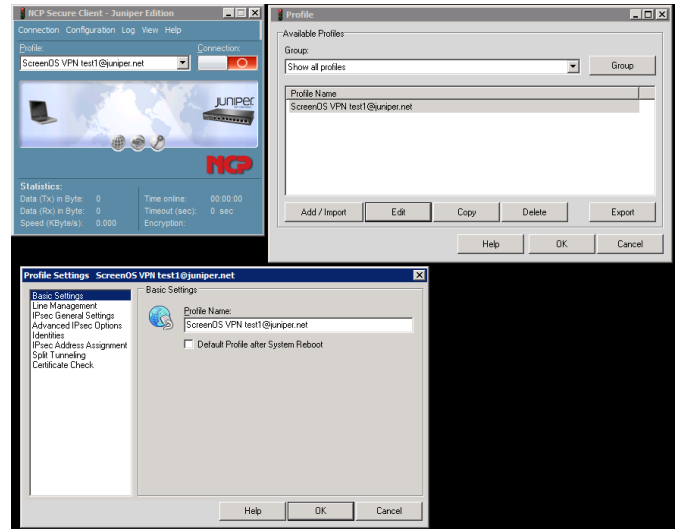
> Next > OK



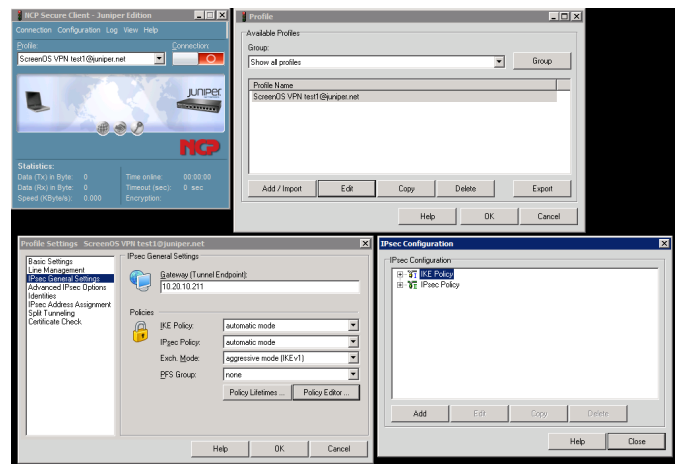
NCP Client with Juniper ScreenOS

5. NCP Client Configuration – Profile changes

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



Select IPsec General Settings:
Select Policy Editor

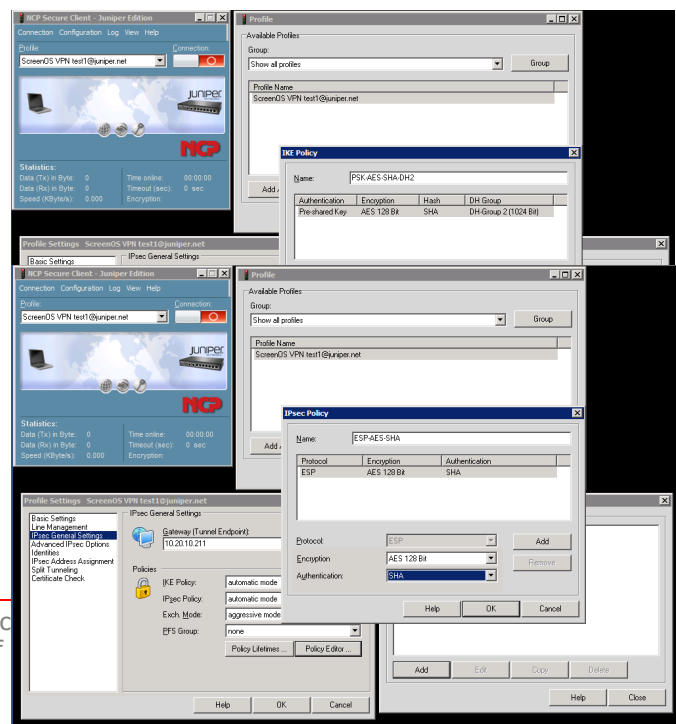


Select IKE Policy – Add

Enter the following parameters and select OK:
Name: PSK-AES-SHA-DH2

Authentication: Pre-shared Key
Encryption: AES 128 Bit
Hash: SHA
DH-Group: DH-Group 2 (1024 Bit)

Select IPsec Policy – Add



NCP Client with Juniper ScreenOS

Enter the following parameters and select OK:

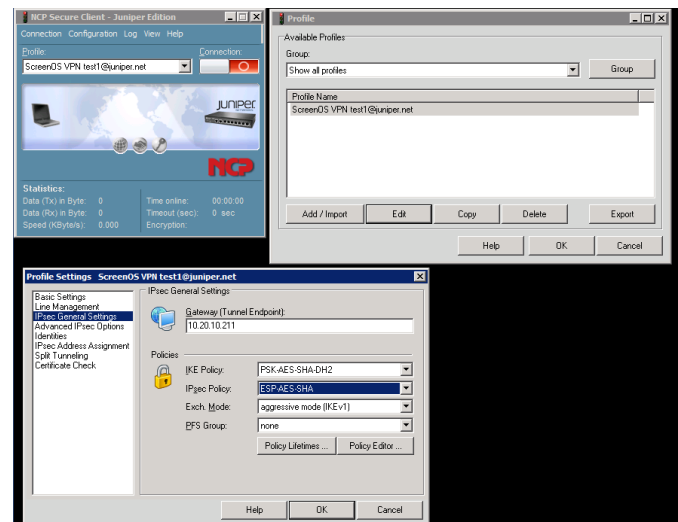
Name: ESP-AES-SHA

Encryption: AES 128 Bit

Hash: SHA

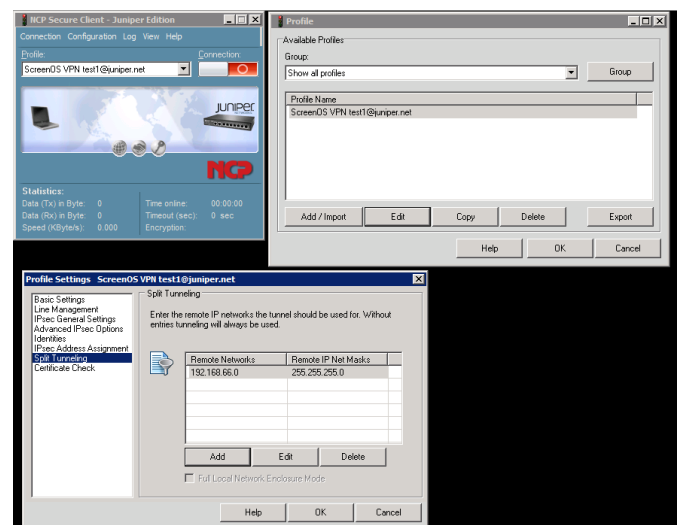
Select Close

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



The Split Tunneling parameter must be set if you configured a specific Policy on the Juniper gateway. So if you did not set the target network to Any but chose a specific network such as our Trusted Access network you must specify the matching network addresses and netmasks for all your specific policies.

Select Split Tunneling and enter the Remote Network address(es) – here 192.168.66.0/24.



Select OK and close all the windows.

Verify client network configuration via ipconfig/all and netstat -rn

Quick Installation Guide

NCP Client with Juniper ScreenOS

```
C:\Windows\system32\cmd.exe
G:\NCP>ipconfig /all

Windows IP Configuration

Host Name . . . . . : demo-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : NCP Secure Client Virtual NDIS6 Adapter
Physical Address. . . . . : 62-00-4E-43-50-49
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-8B-CB-54
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 10.20.10.111(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.20.30.3
DNS Servers . . . . . : 68.94.156.1
NetBIOS over Tcpip. . . . . : Enabled

C:\Windows\system32\cmd.exe
G:\NCP>netstat -rn

Interface List
15...02 00 4e 43 50 49 .....NCP Secure Client Virtual NDIS6 Adapter
11...00 0c 29 8b cb 54 .....Intel(R) PRO/1000 MT Network Connection
1.....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
14...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.20.30.3       10.20.10.111     266
10.20.0.0                  255.255.0.0      On-link          10.20.10.111     266
10.20.10.111               255.255.255.255  On-link          10.20.10.111     266
10.20.255.255              255.255.255.255  On-link          10.20.10.111     266
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        386
127.255.255.255           255.255.255.255  On-link          127.0.0.1        386
224.0.0.0                 240.0.0.0        On-link          127.0.0.1        386
240.0.0.0                 240.0.0.0        On-link          10.20.10.111     266
255.255.255.255           255.255.255.255  On-link          127.0.0.1        386
255.255.255.255           255.255.255.255  On-link          10.20.10.111     266

Persistent Routes:
Network Address          Netmask          Gateway Address  Metric
0.0.0.0                  0.0.0.0          10.20.30.3       Default

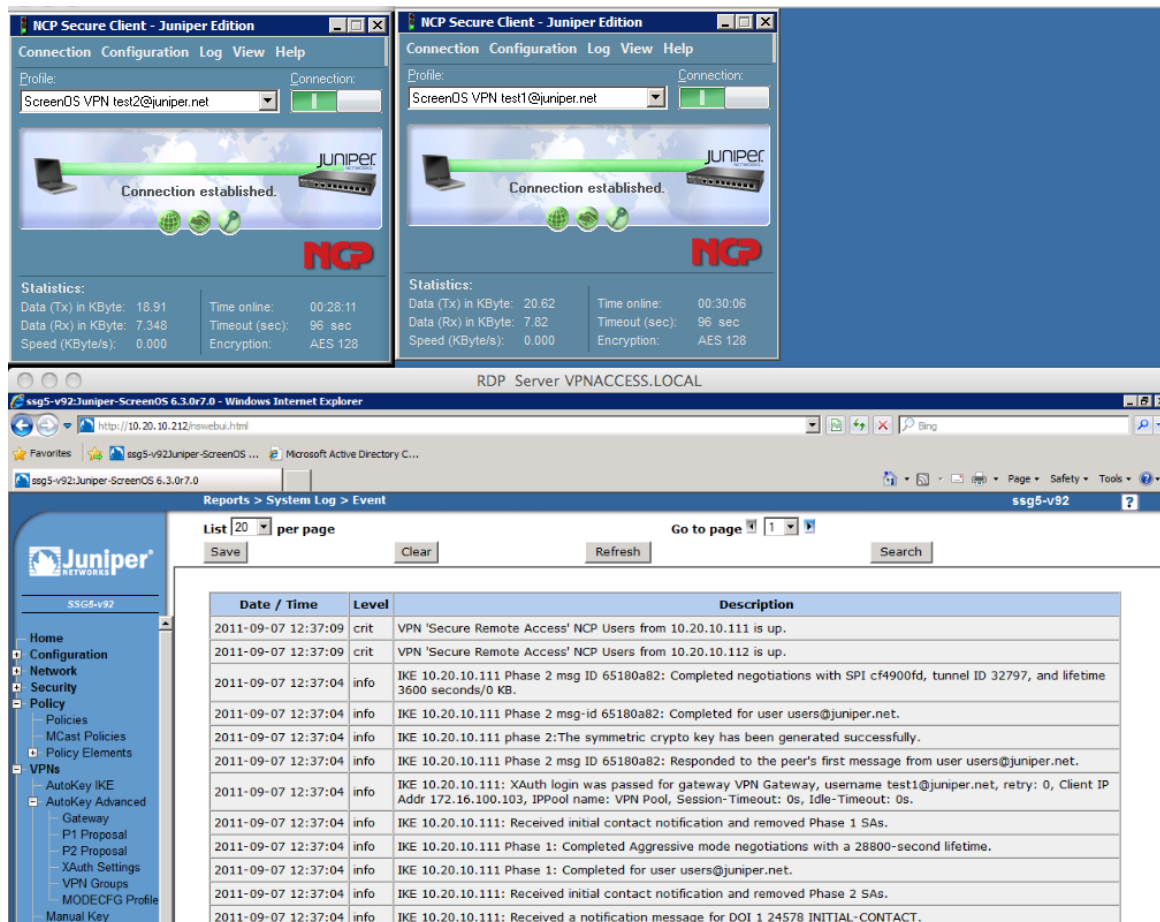
IPv6 Route Table
=====
Active Routes:
Metric Network Destination        Gateway
1 386 ::1/128                      On-link
1 386 ::ffff:0.0.0.0               On-link

Persistent Routes:
None
```

Perform the same configuration on a second client on another test computer.

Click the connection button to establish the VPN gateway connection.

Verify the Juniper gateway log.



Verify client network configuration via ipconfig/all and netstat -rn

NCP Client with Juniper ScreenOS

```

C:\Windows\system32\cmd.exe
C:\NCP>ipconfig /all

Windows IP Configuration

Host Name . . . . . : demo-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No

Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix . :
Description . . . . . : NCP Secure Client Virtual NDIS6 Adapter
Physical Address. . . . . : 02-00-4E-43-50-49
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d146:e783:1c87:7d72::15(Preferred)
IPv4 Address. . . . . : 172.16.100.100(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : Wednesday, June 23, 2010 8:57:54 AM
Lease Expires . . . . . : Tuesday, August 10, 2010 10:03:19 PM
Default Gateway . . . . . : 172.16.100.101
DHCP Server . . . . . : 172.16.100.101
DHCPv6 Iaid . . . . . : 335675470
DHCPv6 Client DUID. . . . . : 00-01-00-01-13-4D-C5-A7-00-0C-29-16-D3-D5

DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       : fec0:0:0:ffff::2%1
                       : fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-8B-CB-54
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::146:e783:1c87:7d72::15(Preferred)
IPv4 Address. . . . . : 10.20.10.111(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 68.94.156.1
DNS Servers . . . . . :
NetBIOS over Tcpip. . . . . : Enabled

C:\Windows\system32\cmd.exe
C:\NCP>netstat -rn

Interface List
15...02 00 4e 43 50 49 .....NCP Secure Client Virtual NDIS6 Adapter
11...00 0c 29 8b cb 54 .....Intel(R) PRO/1000 MT Network Connection
12...00 00 00 00 00 00 e0 .....Software Loopback Interface 1
13...00 00 00 00 00 00 e0 .....Microsoft ISATAP Adapter
14...00 00 00 00 00 00 e0 .....Teredo Tunneling Pseudo-Interface

IPv4 Route Table

Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          172.16.100.101   172.16.100.100    3
10.20.0.0                  255.255.0.0      On-link          10.20.10.111      266
10.20.10.111               255.255.255.255  On-link          10.20.10.111      266
10.20.255.255              255.255.255.255  On-link          10.20.10.111      266
127.0.0.0                  255.0.0.0        On-link          127.0.0.1          306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1          306
127.255.255.255            255.255.255.255  On-link          127.0.0.1          306
172.16.100.0               255.255.255.0    On-link          172.16.100.100    257
172.16.100.100             255.255.255.255  On-link          172.16.100.100    257
172.16.100.255             255.255.255.255  On-link          172.16.100.100    257
224.0.0.0                  240.0.0.0        On-link          10.20.10.111      266
255.255.255.255            255.255.255.255  On-link          127.0.0.1          306
255.255.255.255            255.255.255.255  On-link          10.20.10.111      266
255.255.255.255            255.255.255.255  On-link          172.16.100.100    257

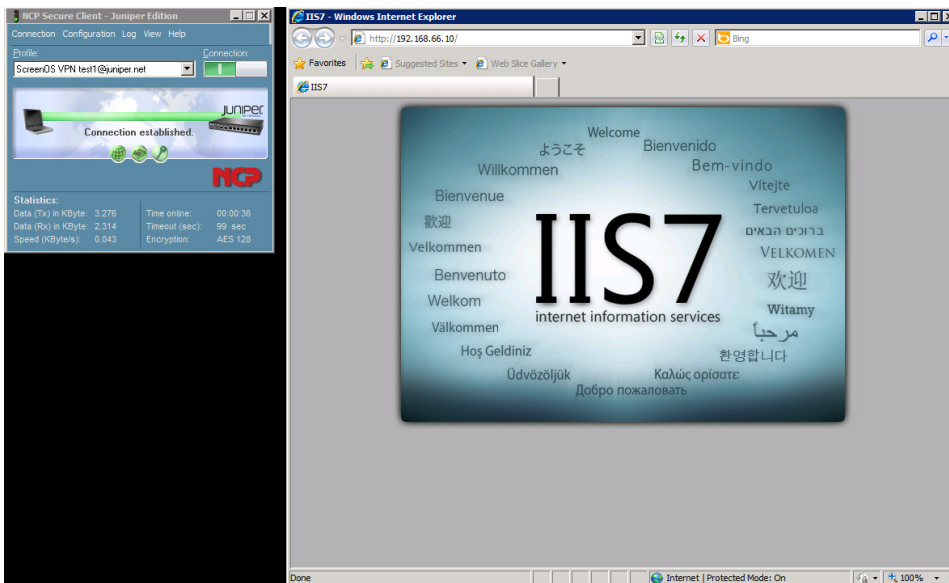
Persistent Routes:
Network Address        Netmask          Gateway Address  Metric
0.0.0.0                0.0.0.0          10.20.30.3       Default

IPv6 Route Table

Active Routes:
Metric Network Destination        Gateway
1       306 ::1/128                      On-link
15      276 fe80::146:e783:1c87:7d72::15 On-link
15      276 fe80::d146:e783:1c87:7d72::15 On-link

Persistent Routes:
None
  
```

Verify a connection to the web server.



NCP Client with Juniper ScreenOS

6. Route-Based VPN & Multiple Proxy ID support on a Route-Based VPN (Support for this feature started with ScreenOS 6.3!)

With route-based VPNs, the policy does not specifically reference a VPN tunnel. Instead, the policy references a destination address. When the security device does a route lookup to find the interface through which it must send traffic to reach that address, it finds a route through a tunnel interface, which is bound to a specific VPN tunnel.

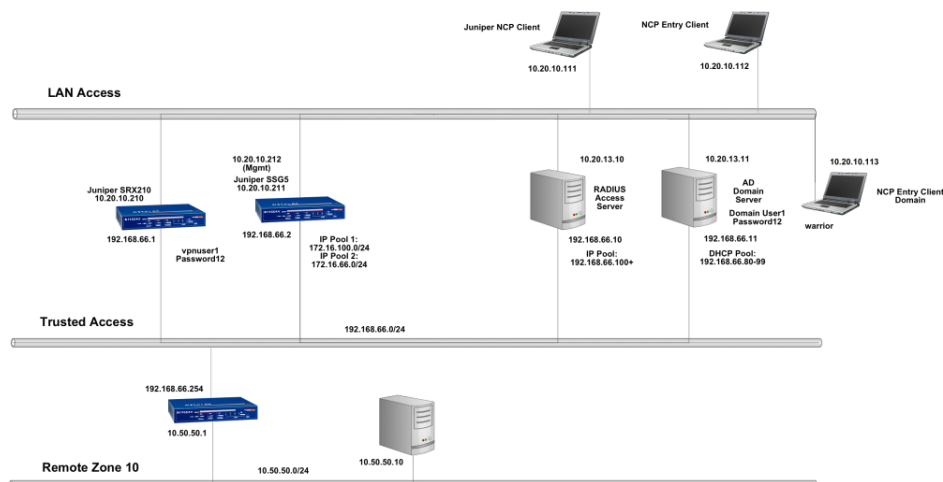
Thus, with a policy-based VPN tunnel, you can consider a tunnel as an element in the construction of a policy. With a route-based VPN tunnel, you can consider a tunnel as a means for delivering traffic, and the policy as a method for either permitting or denying the delivery of that traffic. When a tunnel does not connect large networks running dynamic routing protocols and you do not need to conserve tunnels or define various policies to filter traffic through the tunnel, a policy-based tunnel makes sense. Also, because there is no network beyond a dialup VPN client, policy-based VPN tunnels can be a good choice for dialup VPN configurations.

That said, when the dialup client supports a virtual internal IP address—which the NCP Juniper client does—there are also compelling reasons for using a route-based VPN configuration. A route-based dialup VPN tunnel offers the following benefits:

- ▶ You can bind its tunnel interface to any zone to require or not require policy enforcement.
- ▶ You can define routes to force traffic through the tunnel, unlike a policy-based VPN configuration.
- ▶ You can adjust the proxy ID to accept any IP address from the dialup VPN client by configuring the remote client's address as 255.255.255.255/32.
- ▶ You can define one or more Mapped IP (MIP) addresses on the tunnel interface.

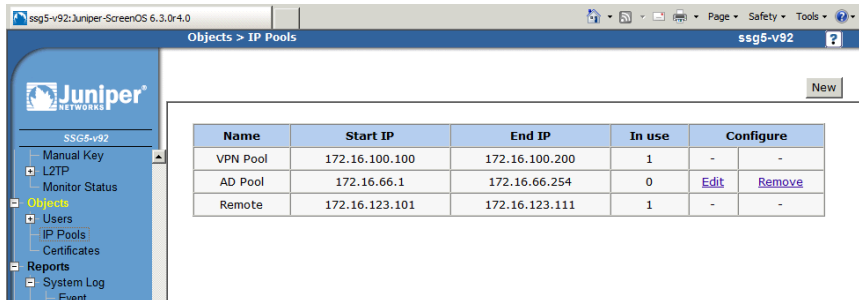
When configuring a VPN to a non-ScreenOS device, that has multiple subnets behind it, it requires defining a separate set of proxy id's to match each network that is behind the other side of the VPN. Support for multiple proxy id's is only available beginning with ScreenOS 6.3.0.

For this feature I created a new configuration as follows. Also the existing network diagram was enhanced.

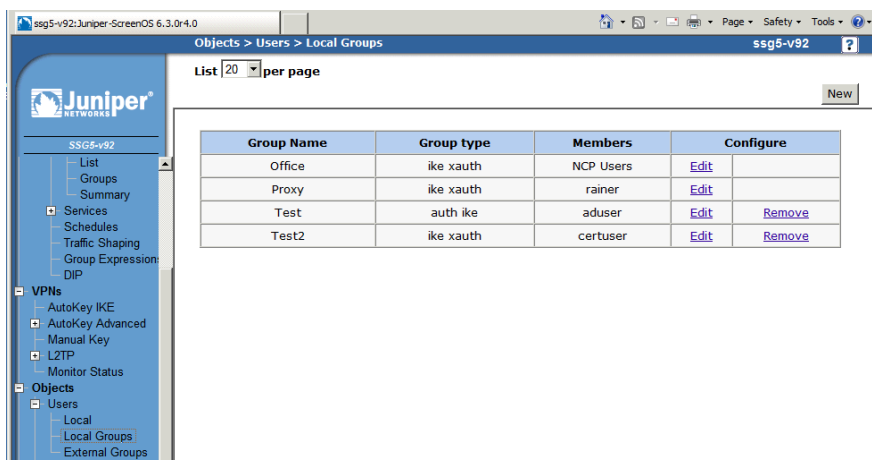
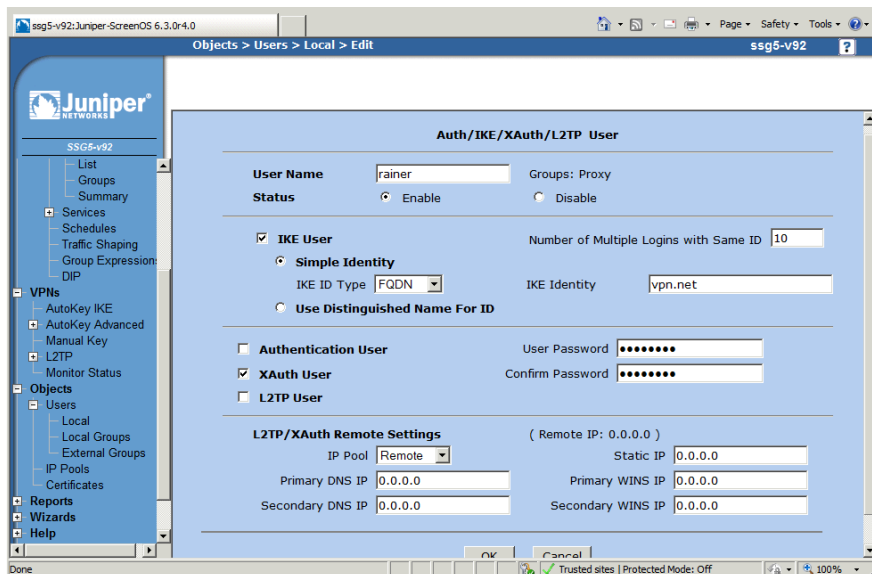


NCP Client with Juniper ScreenOS

First create a new IP Pool called "Remote"



a new IKE User and a new IKE Group "Proxy".



NCP Client with Juniper ScreenOS

Next create a new Gateway configuration "VPN Access"

The screenshot shows the Juniper ScreenOS configuration interface for a new Gateway named "VPN Access". The breadcrumb trail is "VPNs > AutoKey Advanced > Gateway > Edit". The "Version" is set to "IKEv1". Under the "Remote Gateway" section, "Static IP Address" is selected. The "IP Address/Hostname" field is empty. The "Peer ID" field is also empty. The "Dialup User" is set to "None" and the "Dialup User Group" is set to "Proxy". The "ACVPN-Dynamic" section has "Local ID" set to "[DistinguishedName]". The "ACVPN-Profile" section is empty. At the bottom are "OK", "Cancel", and "Advanced" buttons.

The screenshot shows the Juniper ScreenOS configuration interface for the "VPN Access" Gateway, showing the "IKEv2 Auth Method" section. The "Self" and "Peer" authentication methods are both set to "None". The "Preshared Key" field is empty, and the "Use As Seed" checkbox is unchecked. The "Local ID" field is empty, with "(optional)" text next to it. The "Outgoing Interface" is set to "ethernet0/0". The "Security Level" section has "Predefined" set to "Standard" and "User Defined" set to "Custom". The "Phase 1 Proposal" section has "pre-g2-aes128-sha" selected, with "None" selected for the other two options. The "Mode (Initiator)" is set to "Main (ID Protection)". The "Enable NAT-Traversal" checkbox is checked. The "UDP Checksum" checkbox is unchecked. The "Keepalive Frequency" is set to "0" seconds.

Now we need to create a new Tunnel Interface "tunnel.2". This tunnel interface is created for the trust-vr Virtual Router in the Untrust zone. The tunnel interface is Unnumbered and bound to the external (here Ethernet0/0) interface of the gateway.

Quick Installation Guide

NCP Client with Juniper ScreenOS

ssg5-v92:Juniper-ScreenOS 6.3.0-4.0

Network > Interfaces > Edit ssg5-v92

Interface: tunnel.2 (IP/Netmask: 0.0.0.0/0)

Properties: Basic Proxy ARP MIP DIP VIP IGMP NHTB Tunnel IRDP

Tunnel Interface Name: tunnel.2

Zone (VR): Untrust (trust-vr)

Fixed IP

IP Address / Netmask: 0.0.0.0 / 0

Unnumbered

Interface: ethernet0/0 (trust-vr)

Maximum Transfer Unit (MTU): Admin MTU: 0 Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy: ☐

Traffic Bandwidth

Egress: Maximum Bandwidth: 0 Kbps, Guaranteed Bandwidth: 0 Kbps

Ingress: Maximum Bandwidth: 0 Kbps

NHRP Enable: ☐

ssg5-v92:Juniper-ScreenOS 6.3.0-4.0

Network > Zones ssg5-v92

New

ID	Name	Virtual Router	Vsys	Default IF	Type	Attribute	Configure
0	Null	untrust-vr	Root	serial0/0	Null	Shared	
2	Trust	trust-vr	Root	bgroup0	Security(L3)		Edit Screen Mal-URL
1	Untrust	trust-vr	Root	ethernet0/0	Security(L3)	Shared	Edit Screen Mal-URL
4	Self	trust-vr	Root	self	Function		
10	Global	trust-vr	Root	null	Security(L3)		
6	HA	trust-vr	Root	null	Function		
5	MGT	trust-vr	Root	null	Function		Edit Screen Mal-URL
16	Untrust-Tun	trust-vr	Root	hidden.1	Tunnel		
15	V1-Null	trust-vr	Root	l2v	Security(L2)	Shared	Edit Screen Mal-URL
12	V1-Trust	trust-vr	Root	v1-trust	Security(L2)	Shared	Edit Screen Mal-URL
11	V1-Untrust	trust-vr	Root	v1-untrust	Security(L2)	Shared	Edit Screen Mal-URL
3	DMZ	trust-vr	Root	ethernet0/1	Security(L3)		Edit Screen Mal-URL
13	V1-DMZ	trust-vr	Root	v1-dmz	Security(L2)	Shared	Edit Screen Mal-URL
14	VLAN	trust-vr	Root	vlan1	Function(vlan)	Shared	Edit

ssg5-v92:Juniper-ScreenOS 6.3.0-4.0

Network > Interfaces (List) ssg5-v92

List 20 per page

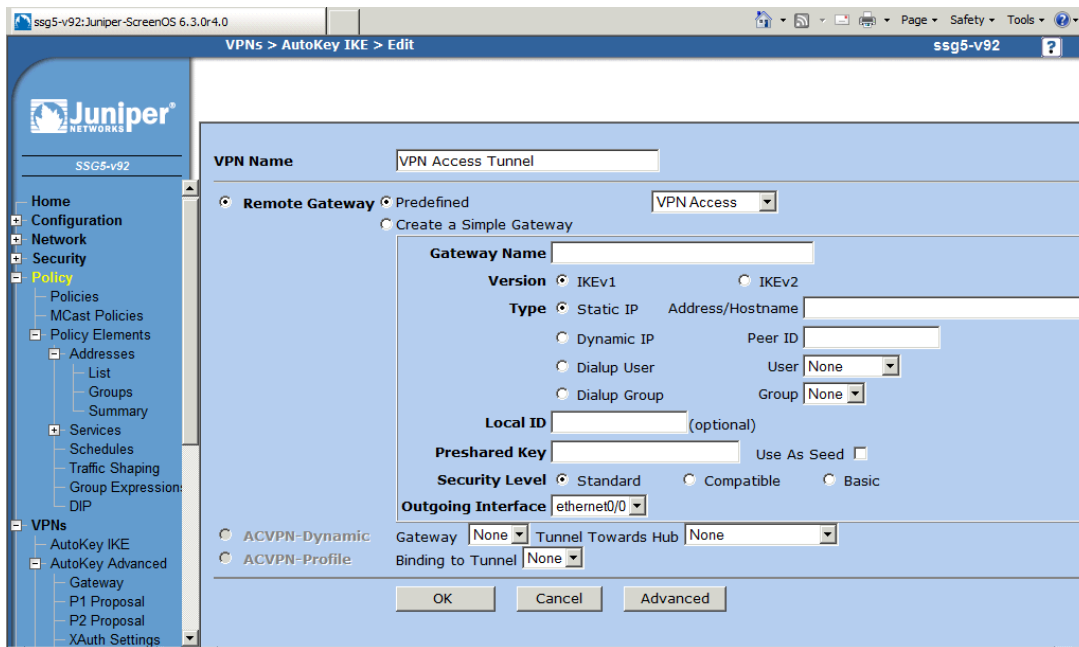
List ALL(13) Interfaces

New Tunnel IF

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.66.2/24	Trust	Layer3	Up	-	Edit
ethernet0/4				Up	-	Edit
ethernet0/5				Up	-	Edit
ethernet0/6				Up	-	Edit
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/0	10.20.10.211/16	Untrust	Layer3	Up	-	Edit
ethernet0/1	0.0.0.0/0	DMZ	Layer3	Down	-	Edit
ethernet0/2	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/3	192.168.100.1/24	Trust	Layer3	Down	-	Edit
serial0/0	0.0.0.0/0	Null	Unused	Up	-	Edit
tunnel.1	unnumbered	Untrust	Tunnel	Ready	-	Edit
tunnel.2	unnumbered	Untrust	Tunnel	Ready	-	Edit
tunnel.3	unnumbered	Trust	Tunnel	Down	-	Edit Remove
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

NCP Client with Juniper ScreenOS

Now we create a new AutoKey IKE "VPN Access Tunnel" for the gateway "VPN Access" and bind this tunnel configuration to the Tunnel Interface "tunnel.2"



Juniper Networks SSG5-v92

VPNs > AutoKey IKE > Edit

VPN Name: VPN Access Tunnel

Remote Gateway: ☒ Predefined ☐ Create a Simple Gateway

Gateway Name: VPN Access

Version: ☒ IKEv1 ☐ IKEv2

Type: ☒ Static IP ☐ Address/Hostname

Dynamic IP: ☐ Peer ID:

Dialup User: ☐ User:

Dialup Group: ☐ Group:

Local ID: (optional)

Preshared Key: Use As Seed: ☐

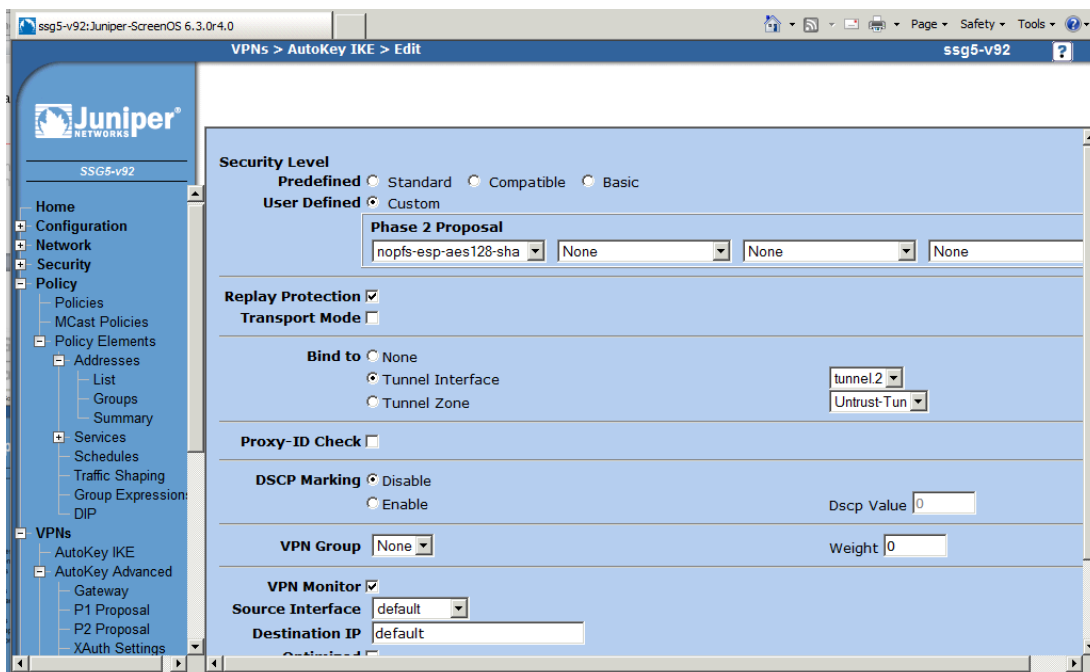
Security Level: ☒ Standard ☐ Compatible ☐ Basic

Outgoing Interface: ethernet0/0

ACVPN-Dynamic: ☐ Gateway: Tunnel Towards Hub:

ACVPN-Profile: ☐ Binding to Tunnel:

OK Cancel Advanced



Juniper Networks SSG5-v92

VPNs > AutoKey IKE > Edit

Security Level: ☒ Predefined ☐ Standard ☐ Compatible ☐ Basic

User Defined: ☒ Custom

Phase 2 Proposal:

Replay Protection: ☒

Transport Mode: ☐

Bind to: ☐ None ☒ Tunnel Interface ☐ Tunnel Zone

tunnel.2 Untrust-Tun

Proxy-ID Check: ☐

DSCP Marking: ☒ Disable ☐ Enable Dscp Value:

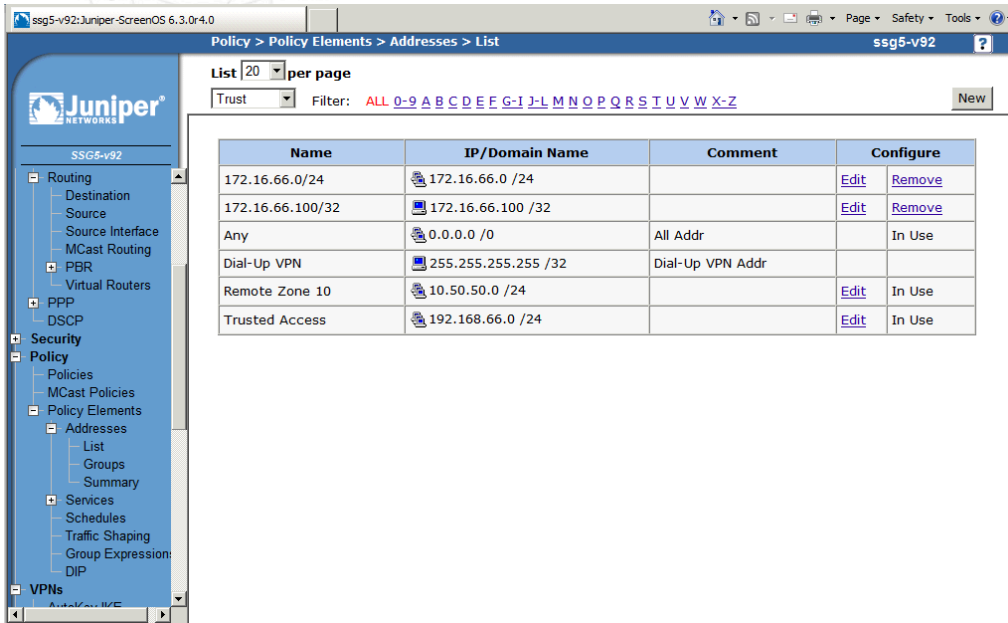
VPN Group: Weight:

VPN Monitor: ☒

Source Interface: Destination IP:

In the Policies Address List we create new Network Address entries for our networks "Trusted Access" and "Remote Zone 10" (see network diagram above).

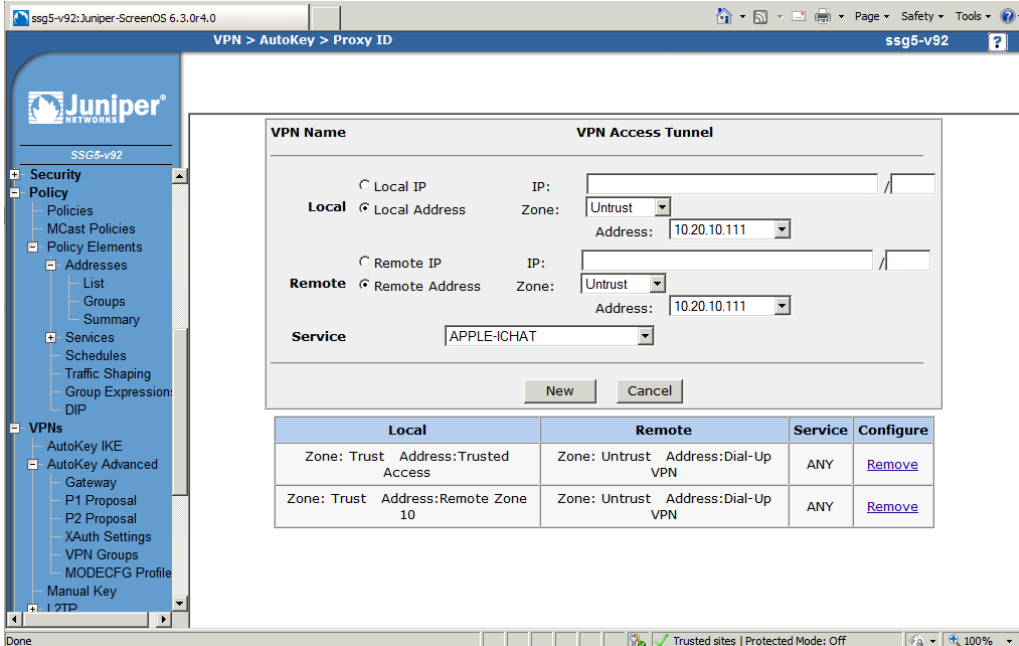
NCP Client with Juniper ScreenOS



The screenshot shows the Juniper ScreenOS configuration interface. The left sidebar displays the navigation tree with 'Policy' expanded. The main pane shows the 'List' view of addresses. A table lists several addresses with their names, IP/domain names, comments, and configuration status.

Name	IP/Domain Name	Comment	Configure
172.16.66.0/24	172.16.66.0 /24		Edit Remove
172.16.66.100/32	172.16.66.100 /32		Edit Remove
Any	0.0.0.0 /0	All Addr	In Use
Dial-Up VPN	255.255.255.255 /32	Dial-Up VPN Addr	
Remote Zone 10	10.50.50.0 /24		Edit In Use
Trusted Access	192.168.66.0 /24		Edit In Use

Now go back to AutoKey IKE and select the Proxy ID setting for the "VPN Access Tunnel" configuration. We create two Proxy ID entries, one for each VPN access network.

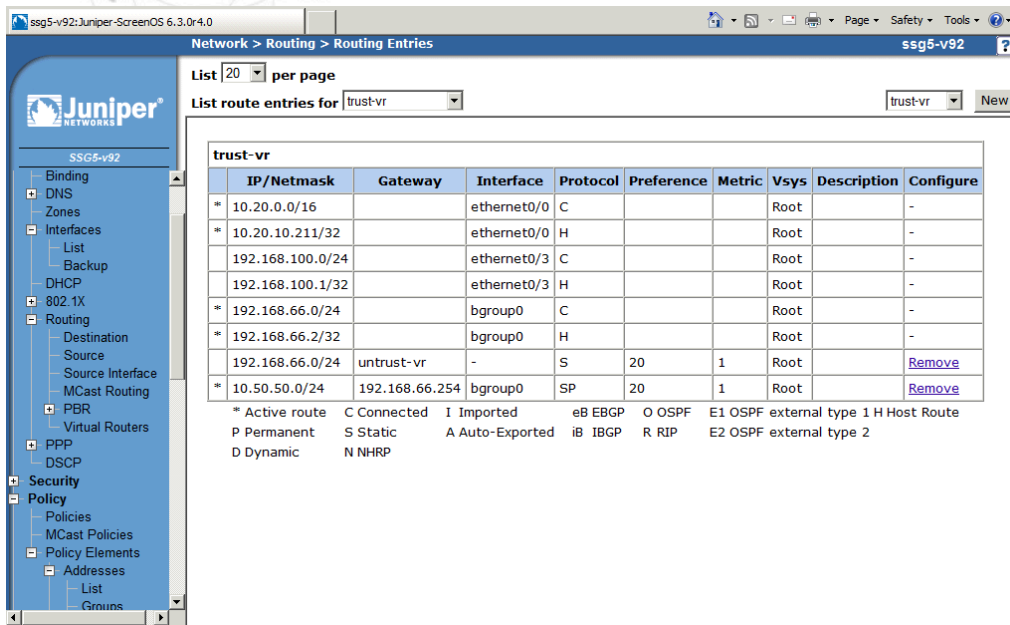


The screenshot shows the Juniper ScreenOS configuration interface for the 'VPN > AutoKey > Proxy ID' section. The 'VPN Name' is 'VPN Access Tunnel'. The configuration includes fields for Local and Remote IP/Address, Zone, and Service. Below the form is a table summarizing the configuration.

Local	Remote	Service	Configure
Zone: Trust Address:Trusted Access	Zone: Untrust Address:Dial-Up VPN	ANY	Remove
Zone: Trust Address:Remote Zone 10	Zone: Untrust Address:Dial-Up VPN	ANY	Remove

Finally we must create a static route in the trust-vr routing domain for the remote network 10.50.50.0 with the appropriate next hop gateway. Otherwise the trust-vr router would not know how to route the packets as we can see in the troubleshooting section further below in this document.

NCP Client with Juniper ScreenOS



Network > Routing > Routing Entries

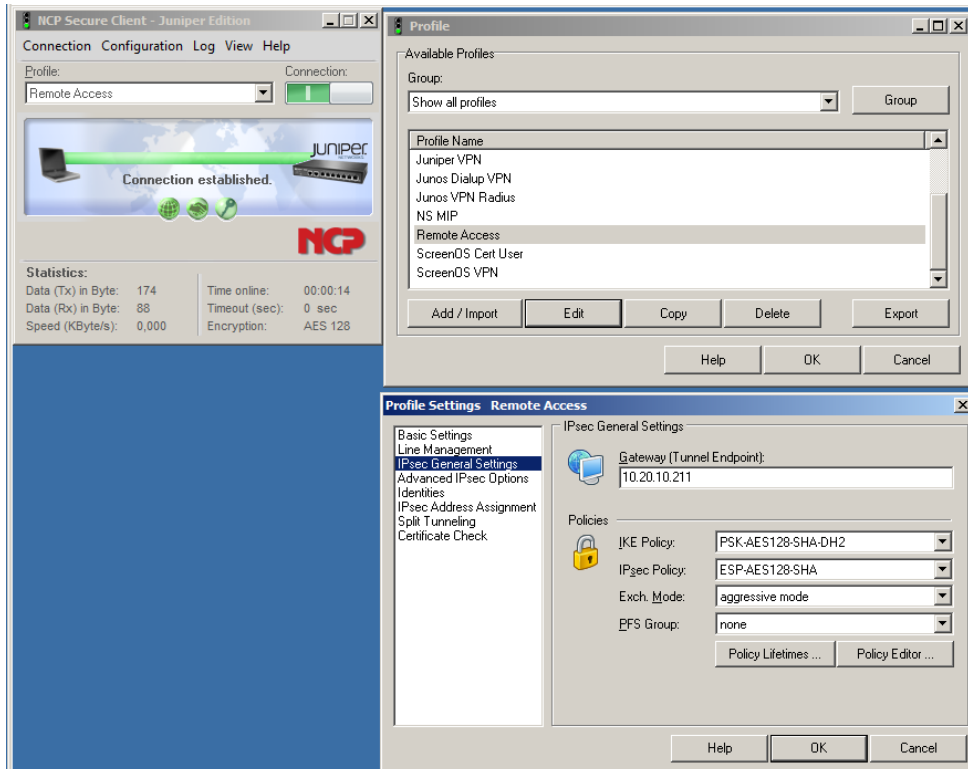
List 20 per page

List route entries for trust-vr

	IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Description	Configure
*	10.20.0.0/16		ethernet0/0	C			Root	-	-
*	10.20.10.211/32		ethernet0/0	H			Root	-	-
	192.168.100.0/24		ethernet0/3	C			Root	-	-
	192.168.100.1/32		ethernet0/3	H			Root	-	-
*	192.168.66.0/24		bgroup0	C			Root	-	-
*	192.168.66.2/32		bgroup0	H			Root	-	-
	192.168.66.0/24	untrust-vr	-	S	20	1	Root	-	Remove
*	10.50.50.0/24	192.168.66.254	bgroup0	SP	20	1	Root	-	Remove


* Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1 H Host Route
 P Permanent S Static A Auto-Exported iB IBGP R RIP E2 OSPF external type 2
 D Dynamic N NHRP

For the NCP client the configuration is identical to the previous configurations. The main configuration sections are shown here.



NCP Secure Client - Juniper Edition

Connection Configuration Log View Help

Profile: Remote Access Connection: 

Connection established.

Statistics:

Data (Tx) in Byte:	174	Time online:	00:00:14
Data (Rx) in Byte:	88	Timeout (sec):	0 sec
Speed (KByte/s):	0,000	Encryption:	AES 128

Available Profiles:

Group: Show all profiles

Profile Name:

- Juniper VPN
- Junos Dialup VPN
- Junos VPN Radius
- NS MIP
- Remote Access
- ScreenOS Cert User
- ScreenOS VPN

Add / Import Edit Copy Delete Export

Help OK Cancel

Profile Settings Remote Access

Basic Settings

- Line Management
- IPsec General Settings
- Advanced IPsec Options
- Identities
- IPsec Address Assignment
- Split Tunneling
- Certificate Check

IPsec General Settings

Gateway (Tunnel Endpoint): 10.20.10.211

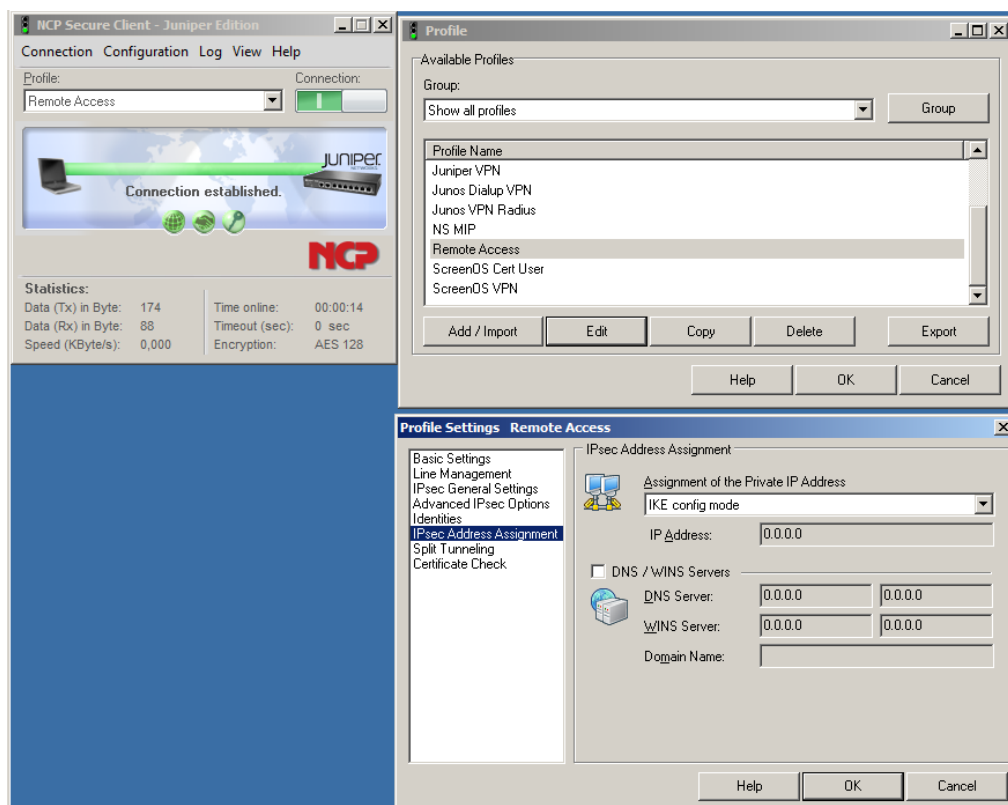
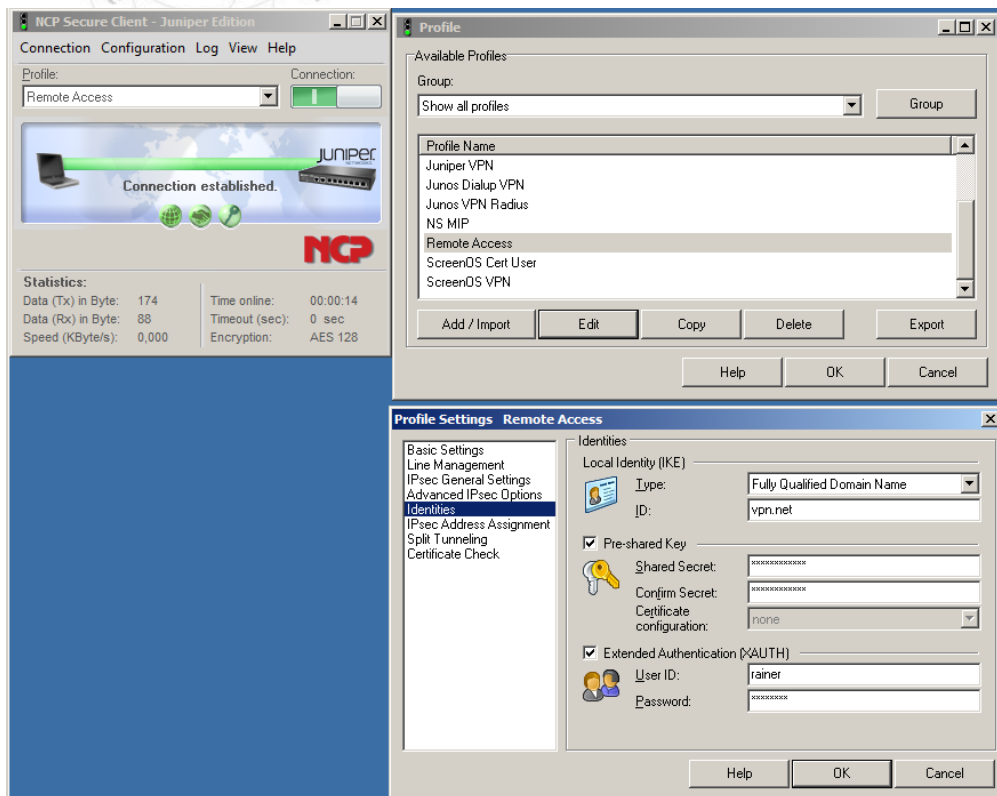
Policies

IKE Policy: PSK-AES128-SHA-DH2
 IPsec Policy: ESP-AES128-SHA
 Exch. Mode: aggressive mode
 EFS Group: none

Policy Lifetimes ... Policy Editor ...

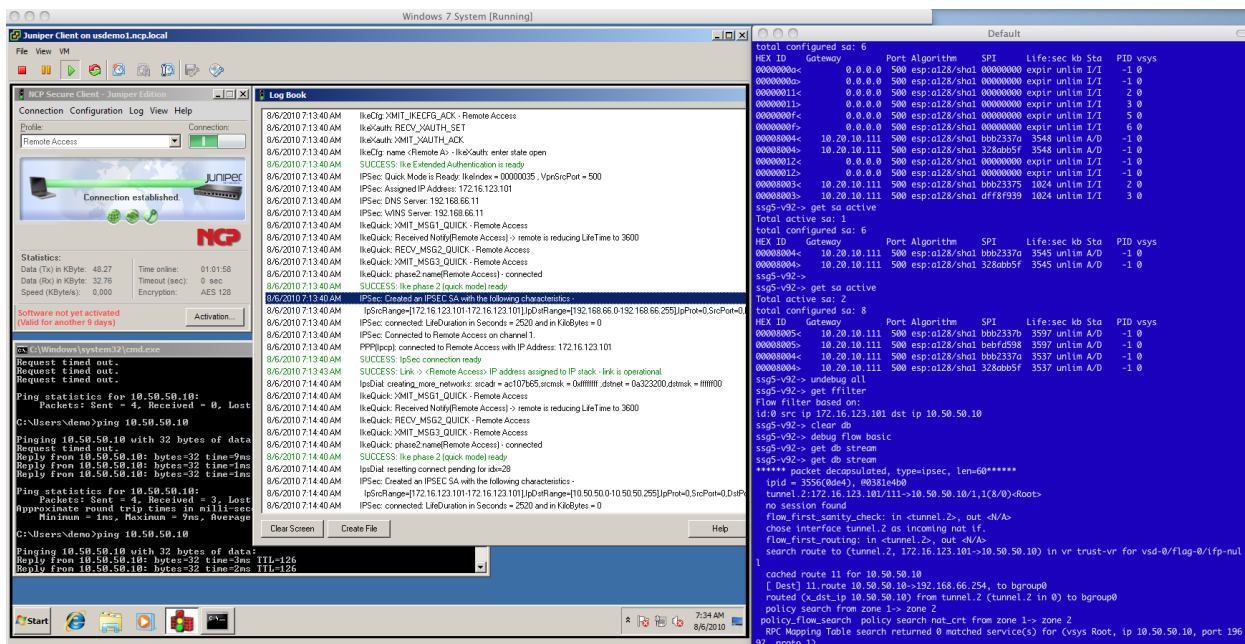
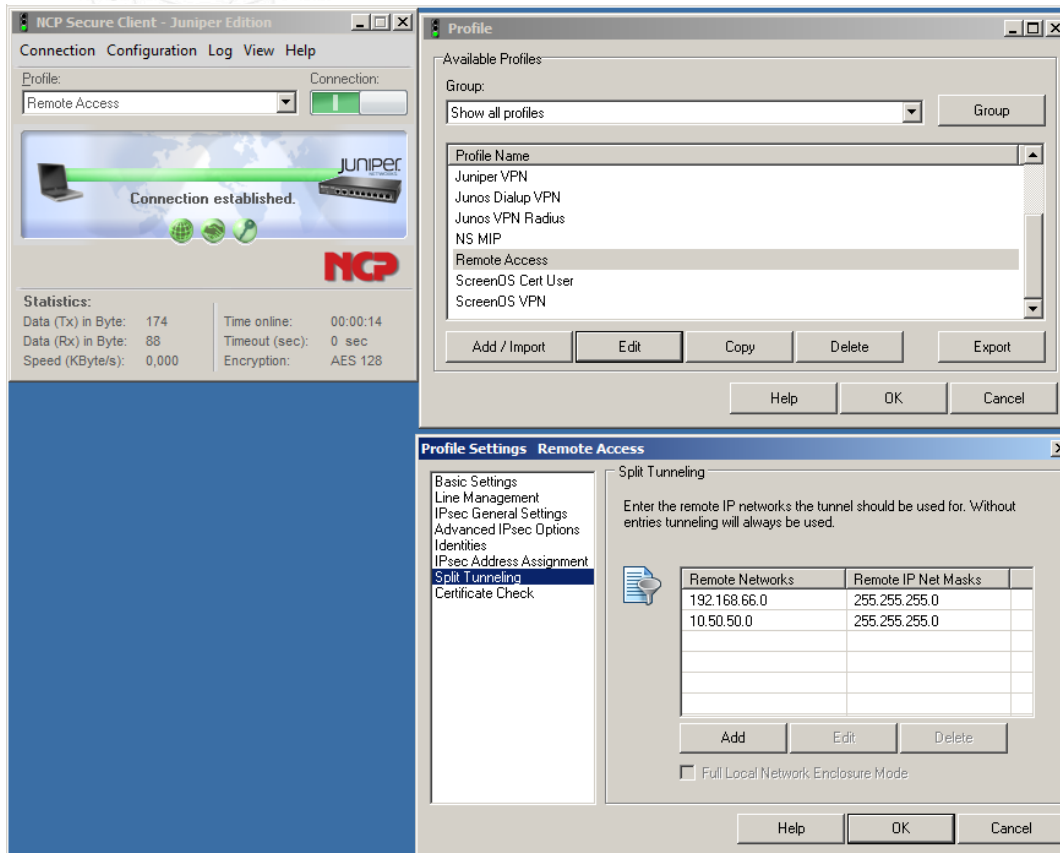
Help OK Cancel

NCP Client with Juniper ScreenOS



Quick Installation Guide

NCP Client with Juniper ScreenOS

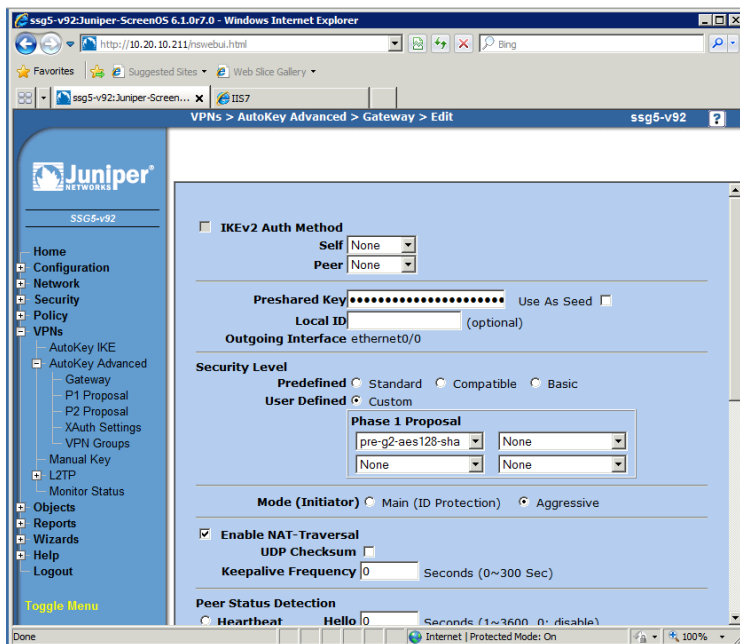


NCP Client with Juniper ScreenOS

7. Advanced Configuration

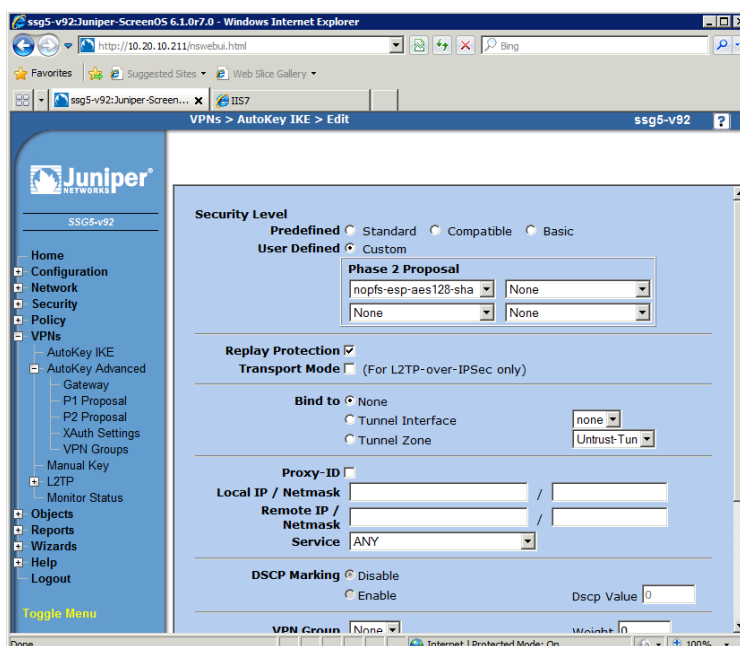
NAT-T

IPsec does not work across NAT devices. Therefore NAT Traversal is required.



Replay Protection

Replay Protection provides a safeguard against snooped connection and injected packets.



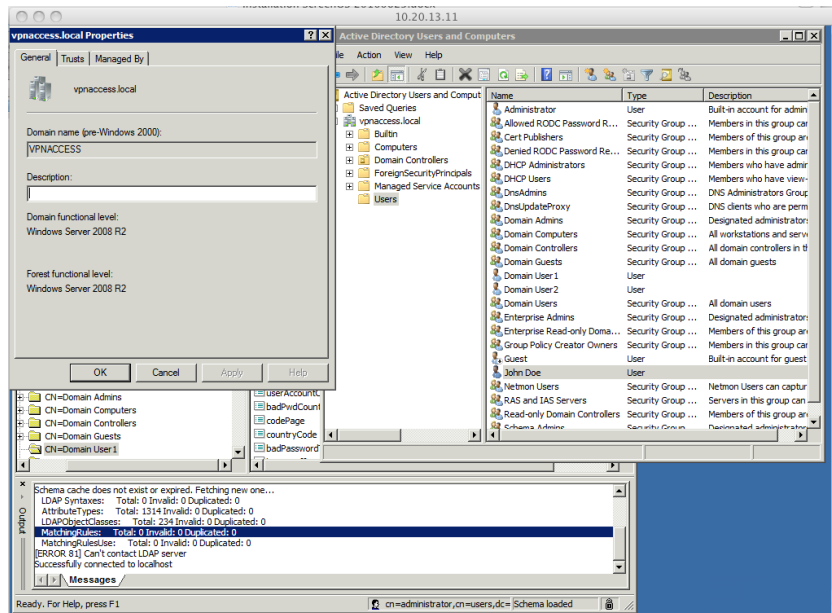
NCP Client with Juniper ScreenOS

Active Directory Authentication

In Enterprise environments authentication against user directories is standard procedure. Below I explain the configuration of extended authentication against Active Directory

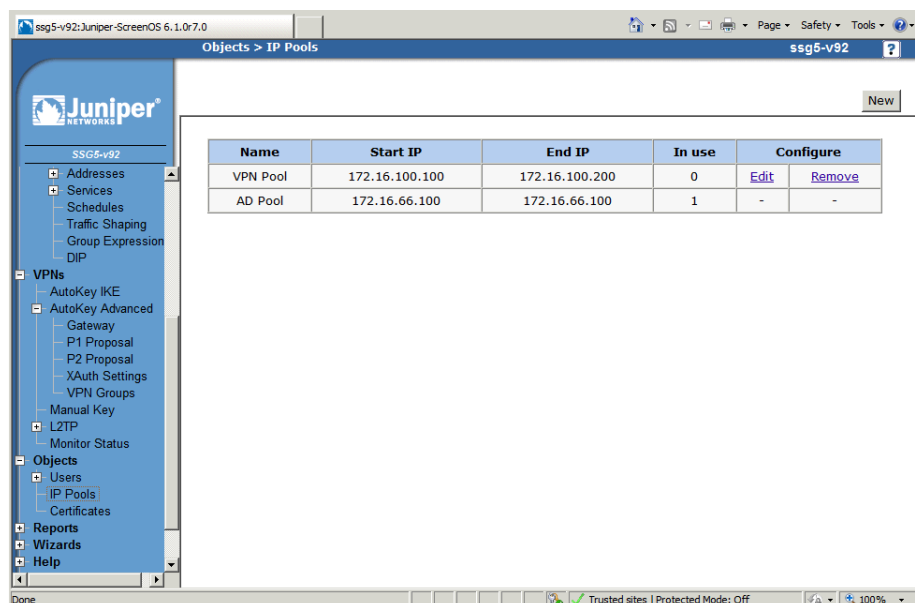
Active Directory Configuration

Here we will use a Windows Server 2008 R2 AD Domain server with the domain name vpnaccess.local and two domain users, "Domain User1" and "John Doe".



3.2 Juniper Gateway Configuration

First we setup a new IP Pool definition



NCP Client with Juniper ScreenOS

Next step is to configure the Auth Server

Configuration > Auth > Auth Servers > Edit

Name AD1

IP/Domain Name 192.168.66.11

Backup1

Backup2

Timeout 10 minutes (0 to disable)

Forced Timeout 0 minutes (0 to disable)

Account Type ☒ Auth ☒ L2TP ☐ Admin ☒ XAuth ☐ 802.1X ☐ IKEv2EAP

Username Stripping Separator Occurring 0 times

Domain Name

Failover Revert Interval seconds (0 to disable)

Source Interface none

RADIUS RADIUS Port 1645 Shared Secret

Retry times 3 Retry Timeout 3 seconds

Acct-Session-ID Length Bytes (0 for default)

Configuration > Auth > Auth Servers > Edit

RADIUS RADIUS Port 1645 Shared Secret

Retry times 3 Retry Timeout 3 seconds

Acct-Session-ID Length Bytes (0 for default)

RFC Compatibility ☐ RFC2138

Zone Verification ☐ Enabled

SecurID Client Retries 3 Client Timeout 5 seconds

Authentication Port 5500

Encryption Type ☒ DES ☐ SDI

Use Duress ☐ Yes ☒ No

LDAP LDAP Port 389 Common Name Identifier cn

Distinguished Name(dn) cn=users,dc=vpnaccess,dc=local

TACACS+ TACACS Port Shared Secret

OK Cancel

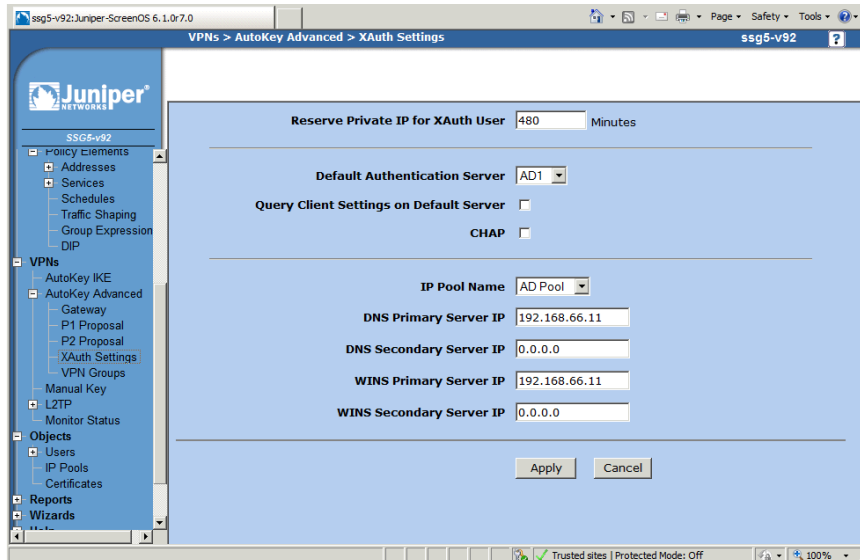
Configuration > Auth > Auth Servers

ID	Name	Server IP/Name	Type	Acct Type	Configure
0	Local	Local	Local	admin auth l2tp xauth	Edit -
1	AD1	192.168.66.11	LDAP	auth l2tp xauth	Edit -

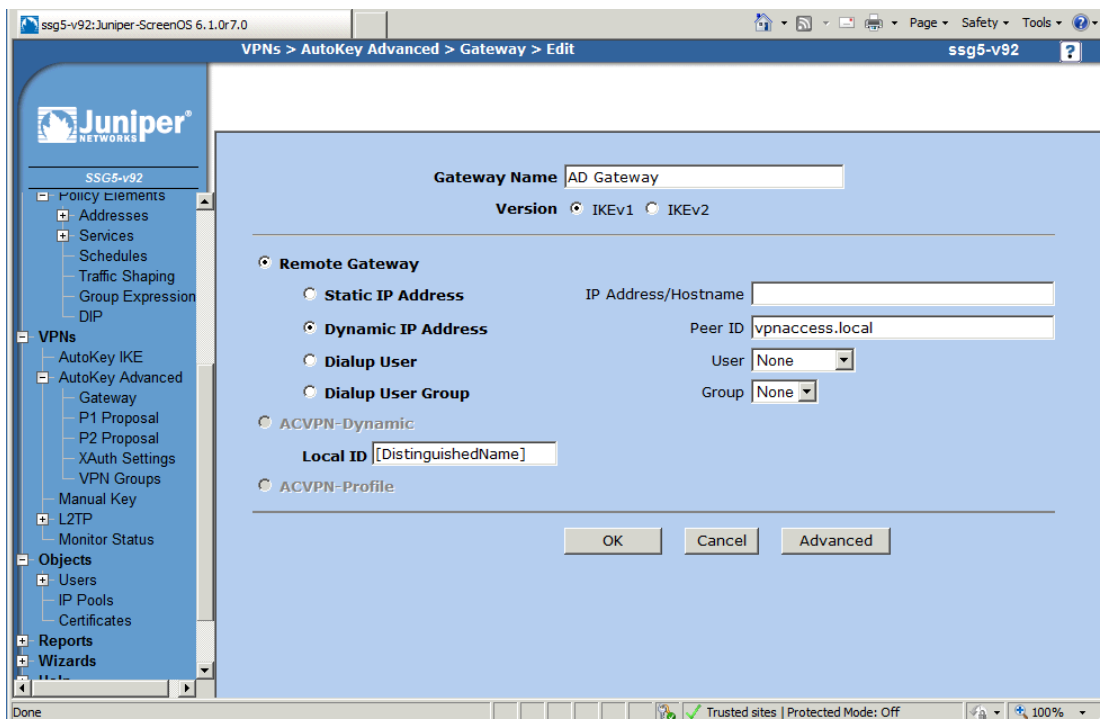
* - Auth server is in use

NCP Client with Juniper ScreenOS

Next configure the Auth Server parameters



Next create a new Gateway configuration as shown below



NCP Client with Juniper ScreenOS

ssg5-v92:Juniper-ScreenOS 6.1.0r7.0

VPNs > AutoKey Advanced > Gateway > Edit

ssg5-v92

Juniper

SSG5-v92

- Policy Elements
 - Addresses
 - Services
 - Schedules
 - Traffic Shaping
 - Group Expression
 - DIP
- VPNs
 - AutoKey IKE
 - AutoKey Advanced
 - Gateway
 - P1 Proposal
 - P2 Proposal
 - XAuth Settings
 - VPN Groups
 - Manual Key
 - L2TP
 - Monitor Status
 - Objects
 - Users
 - IP Pools
 - Certificates
 - Reports
 - Wizards
 - Help

IKEv2 Auth Method

Self: None
Peer: None

Preshared Key: [Redacted] Use As Seed: ☐

Local ID: [Redacted] (optional)

Outgoing Interface: ethernet0/0

Security Level

Predefined: ☐ Standard ☐ Compatible ☐ Basic
User Defined: ☒ Custom

Phase 1 Proposal

pre-g2-aes128-sha, None, None, None

Mode (Initiator): ☐ Main (ID Protection) ☒ Aggressive

☒ Enable NAT-Traversal

UDP Checksum: ☐

Keepalive Frequency: 5 Seconds (0~300 Sec)

Peer Status Detection

☐ Heartbeat Hello: 0 Seconds (1~3600, 0: disable)

Don't forget to go into the XAuth Gateway configuration settings

ssg5-v92:Juniper-ScreenOS 6.1.0r7.0

VPNs > AutoKey Advanced > Gateway > Xauth

ssg5-v92

Juniper

SSG5-v92

- Policy
 - Policies
 - MCast Policies
 - Policy Elements
- VPNs
 - AutoKey IKE
 - AutoKey Advanced
 - Gateway
 - P1 Proposal
 - P2 Proposal
 - XAuth Settings
 - VPN Groups
 - Manual Key
 - L2TP
 - Monitor Status
 - Objects
 - Users
 - IP Pools
 - Certificates
 - Reports
 - Wizards
 - Help
 - Logout

Gateway Name: AD Gateway

☐ None

☒ **XAuth Server**

Allowed Authentication Type: ☒ Generic ☐ CHAP Only ☐ CHAP & PAP

☐ Use Default Xauth Settings

☒ **Local Authentication**

☒ Allow Any

User: None

User Group: None

☒ **External Authentication**

☒ Allow Any

User: Name [Redacted]

User Group: Name [Redacted]

☐ Query Remote Setting

☐ **Bypass Authentication**

☒ **XAuth Client**

Allowed Authentication Type: ☐ Any ☐ CHAP Only ☐ SecurID

User Name: [Redacted]

Password: [Redacted]

Update DHCP Server: ☐

Prefix Delegation to IPv6 Interfaces: ☐

Interface	SLA ID	SLA Length	Action
[Redacted]	[Redacted]	0	Add

NCP Client with Juniper ScreenOS

And next create a VPN configuration using the configured gateway

ssg5-v92:Juniper-ScreenOS 6.1.0r7.0

VPNs > AutoKey IKE > Edit

ssg5-v92

VPN Name: AD VPN

Remote Gateway: Predefined (AD Gateway)

Create a Simple Gateway

Gateway Name:

Version: IKEv1

Type: Static IP

Address/Hostname:

Peer ID:

Dialup User:

Dialup Group:

Local ID: (optional)

Preshared Key:

Use As Seed:

Security Level: Standard

Outgoing Interface: ethernet0/0

ACVPN-Dynamic:

ACVPN-Profile:

Gateway: None

Tunnel Towards Hub: Secure MIP

Binding to Tunnel: None

OK Cancel Advanced

ssg5-v92:Juniper-ScreenOS 6.1.0r7.0

VPNs > AutoKey IKE > Edit

ssg5-v92

Security Level: Predefined

User Defined: Custom

Phase 2 Proposal: nopfs-esp-aes128-sha

Replay Protection:

Transport Mode: (For L2TP-over-IPSec only)

Bind to: None

Proxy-ID:

Local IP / Netmask: 192.168.66.0 / 24

Remote IP / Netmask: 172.16.66.100 / 32

Service: ANY

DSCP Marking: Disable

DSCP Value: 0

VPN Group: None

Weight: 0

As you see we configure Proxy-ID with the Pool Remote IP Address.

NCP Client with Juniper ScreenOS

The final step in the configuration is to create the Policy definition.

The screenshot shows the Juniper ScreenOS configuration interface for a policy. The left sidebar contains a tree view with categories like Policy, VPNs, Objects, Reports, and Wizards. The main area is titled "Policy > Policies (From Trust To Untrust)". The configuration fields include:

- Name (optional):** A text input field.
- Source Address:** Radio buttons for "New Address" and "Address Book Entry" (selected). The "Address Book Entry" dropdown shows "192.168.66.0/24" and a "Multiple" button.
- Destination Address:** Radio buttons for "New Address" and "Address Book Entry" (selected). The "Address Book Entry" dropdown shows "Any" and a "Multiple" button.
- Service:** A dropdown menu set to "ANY" with a "Multiple" button.
- Application:** A dropdown menu set to "None".
- WEB Filtering:** An unchecked checkbox.
- Action:** A dropdown menu set to "Tunnel".
- Antispam enable:** An unchecked checkbox.
- Tunnel:** A dropdown menu set to "VPN" with "AD VPN" selected.
- Modify matching bidirectional VPN policy:** A checked checkbox.
- L2TP:** A dropdown menu set to "None".
- Logging:** Two checked checkboxes: "at Session Beginning" and "at Session End".
- Session-limit:** An unchecked checkbox.

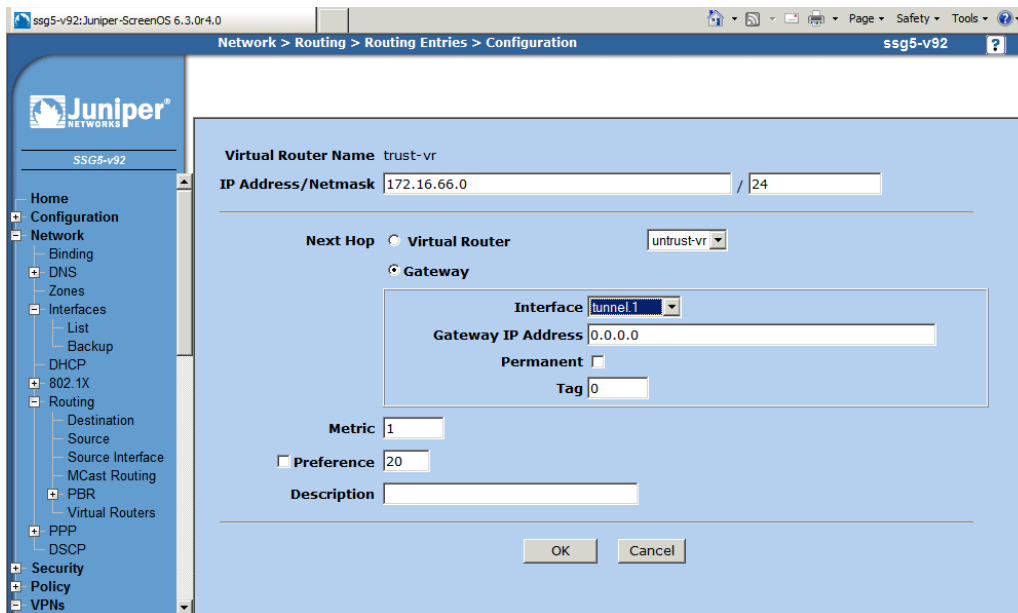
Don't forget to set the Authentication in the Advanced Policy configuration.

The screenshot shows the "Advanced Policy Settings" page in the Juniper ScreenOS configuration interface. The left sidebar is the same as the previous screenshot. The main area is titled "Advanced Policy Settings" and contains two main sections:

- NAT:** Includes checkboxes for "Source Translation" and "Destination Translation". The "Source Translation" dropdown is set to "None (Use Egress Interface IP)". The "Destination Translation" section has radio buttons for "Translate to IP" (selected) and "Translate to IP Range". The "Translate to IP" section has a "Map to Port" dropdown set to "0". The "Translate to IP Range" section has two input fields for IP ranges, both set to "0.0.0.0".
- Authentication:** A checked checkbox. It includes a section for "Auth Server" with a dropdown set to "AD1". Below this is a section for "WebAuth(Local)" with a "User Group" dropdown set to "Allow Any", a "Group Expression" dropdown set to "Allow Any", and a "User" dropdown set to "Allow Any". There is also an "External User" text input field.

NCP Client with Juniper ScreenOS

And don't forget the Routing off course, which is required. Create a Route in the trust-vr route domain for the IP Pool network with the Tunnel interface as the Gateway.



Network > Routing > Routing Entries > Configuration

Virtual Router Name: trust-vr

IP Address/Netmask: 172.16.66.0 / 24

Next Hop: ☐ Virtual Router (untrust-vr) ☒ Gateway

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

Permanent: ☐

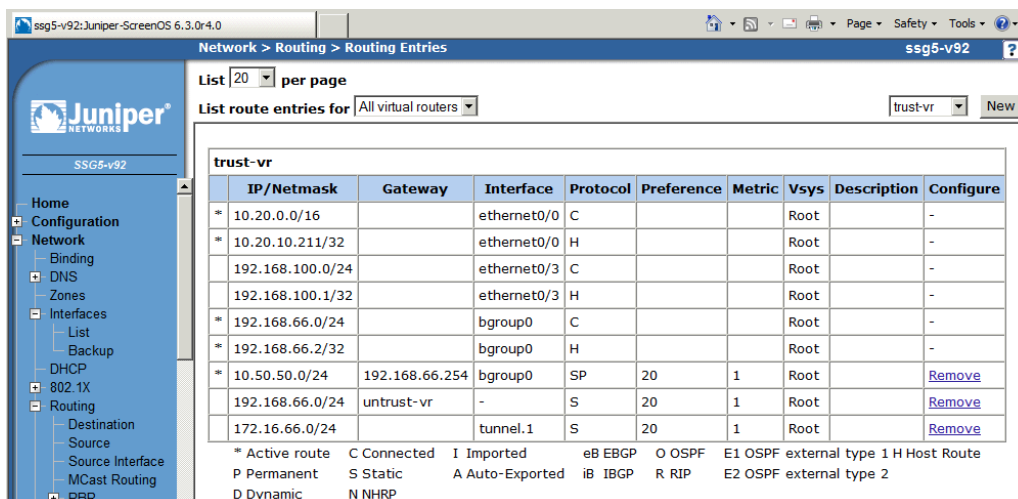
Tag: 0

Metric: 1

Preference: 20

Description:

OK Cancel



Network > Routing > Routing Entries

List: 20 per page

List route entries for: All virtual routers

trust-vr

	IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Description	Configure
*	10.20.0.0/16		ethernet0/0	C			Root		-
*	10.20.10.211/32		ethernet0/0	H			Root		-
	192.168.100.0/24		ethernet0/3	C			Root		-
	192.168.100.1/32		ethernet0/3	H			Root		-
*	192.168.66.0/24		bgroup0	C			Root		-
*	192.168.66.2/32		bgroup0	H			Root		-
*	10.50.50.0/24	192.168.66.254	bgroup0	SP	20	1	Root		Remove
	192.168.66.0/24	untrust-vr	-	S	20	1	Root		Remove
	172.16.66.0/24		tunnel.1	S	20	1	Root		Remove

* Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1 H Host Route
 P Permanent S Static A Auto-Exported iB IBGP R RIP E2 OSPF external type 2
 D Dynamic N NHRP

NCP Client with Juniper ScreenOS**NCP Client Configuration**

The NCP client configuration is identical to the steps described earlier in this document. Here I only describe the difference in the configuration.

First go into the client profile and edit Identities section. The xauth user parameters are the credentials of the Active Directory user.

The screenshot shows the 'Profile Settings AD Users' dialog box with the 'Identities' tab selected. The left sidebar lists various settings: Basic Settings, Line Management, IPsec General Settings, Advanced IPsec Options, Identities (selected), IPsec Address Assignment, Split Tunneling, and Certificate Check. The main area is titled 'Identities' and contains the following fields:

- Local Identity (IKE)**
 - Type: Fully Qualified Domain Name (dropdown)
 - ID: ypnaccess.local
- ☒ **Pre-shared Key**
 - Shared Secret: [masked]
 - Confirm Secret: [masked]
 - Certificate configuration: none (dropdown)
- ☒ **Extended Authentication (XAUTH)**
 - User ID: Domain User1
 - Password: [masked]

Buttons at the bottom: Help, OK, Cancel.

And then go to the IPsec Address Assignment.

The screenshot shows the 'Profile Settings AD Users' dialog box with the 'IPsec Address Assignment' tab selected. The left sidebar is the same as the previous screenshot. The main area is titled 'IPsec Address Assignment' and contains the following fields:

- Assignment of the Private IP Address**
 - IKE config mode (dropdown)
 - IP Address: 0.0.0.0
- ☐ **DNS / WINS Servers**
 - DNS Server: 0.0.0.0 (two input fields)
 - WINS Server: 0.0.0.0 (two input fields)
 - Domain Name: [empty]

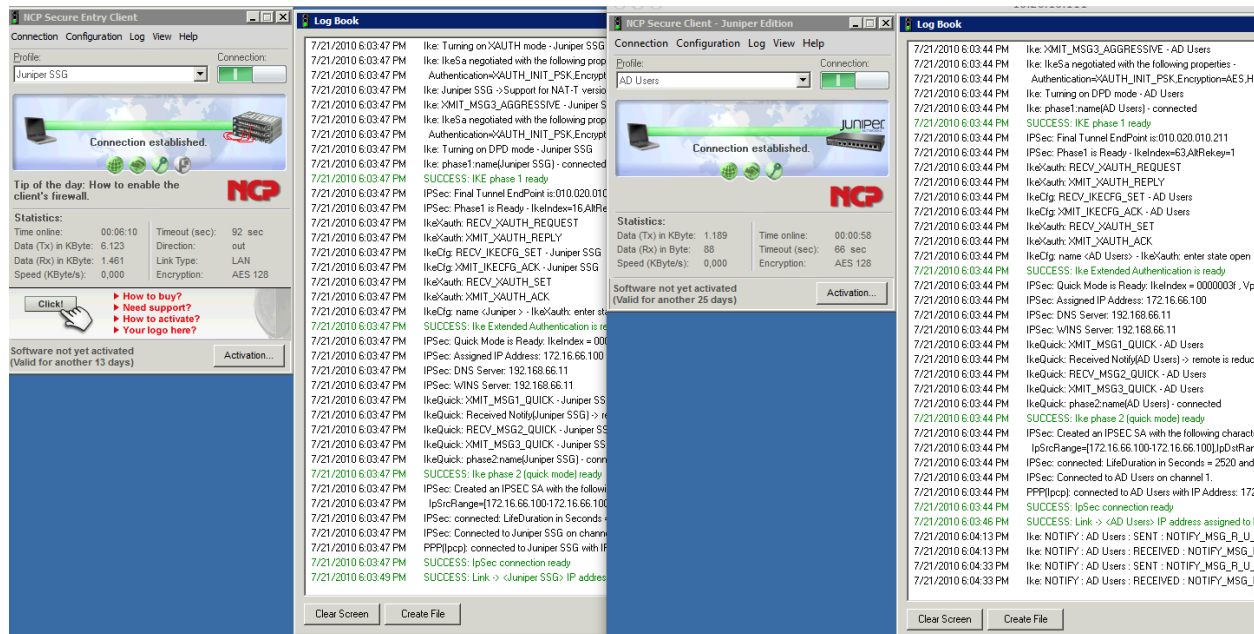
Buttons at the bottom: Help, OK, Cancel.

Quick Installation Guide

NCP Client with Juniper ScreenOS



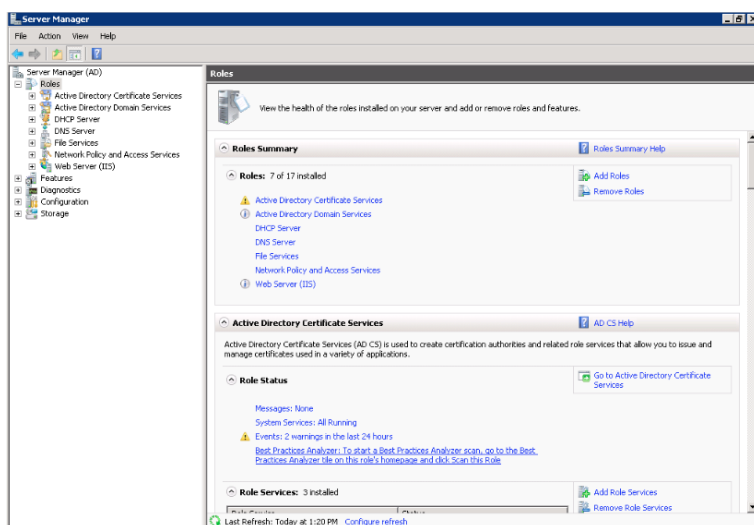
All set. Below I show the test with two separate clients connecting simultaneously.



Certificate Authentication using Active Directory Certificate CA

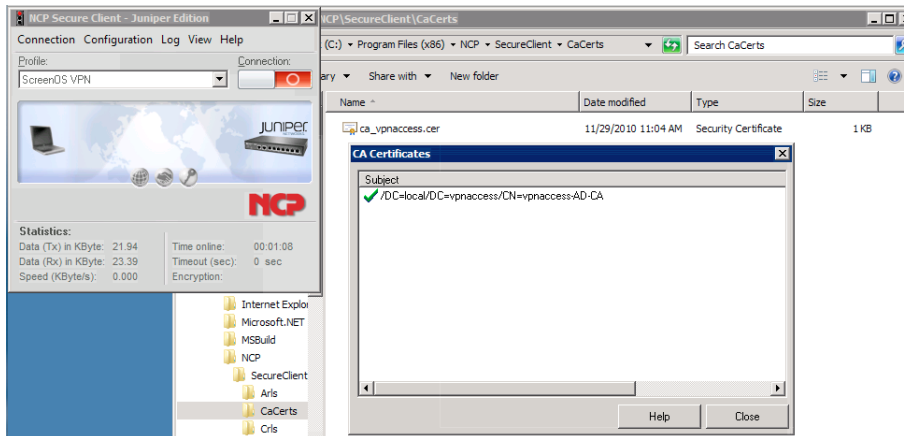
In Enterprise environments Certificates are often used as a way of authentication. In this section we describe the steps to perform a setup with Certificates using a Microsoft Active Directory Certificate CA and self-signed Certificates.

We assume Active Directory Certificate Services is up and running

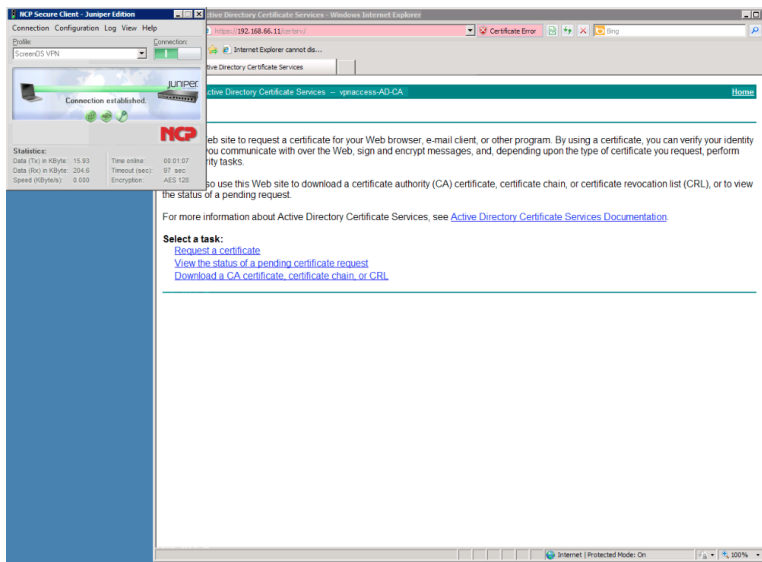


NCP Client with Juniper ScreenOS

Copy this cert into the Cacerts client folder. Verify you see it in the client under Connection – Certificates – Display CA Certificates



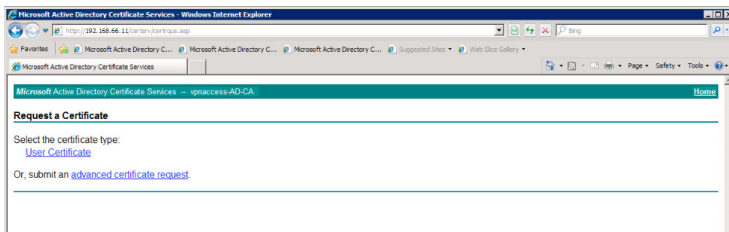
For the User Certificate, with the VPN tunnel established from the client to reach the AD/Certificate server, connect to the CA via web browser and click on "Request a certificate"



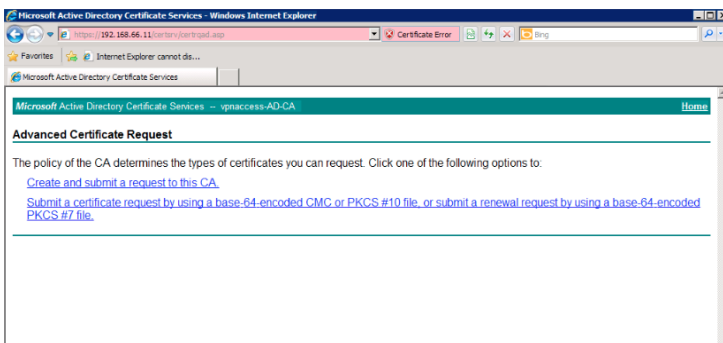
From the "Request a Certificate" screen select "submit an advanced certificate request" link. This is necessary to have the keys exportable.

NCP Client with Juniper ScreenOS

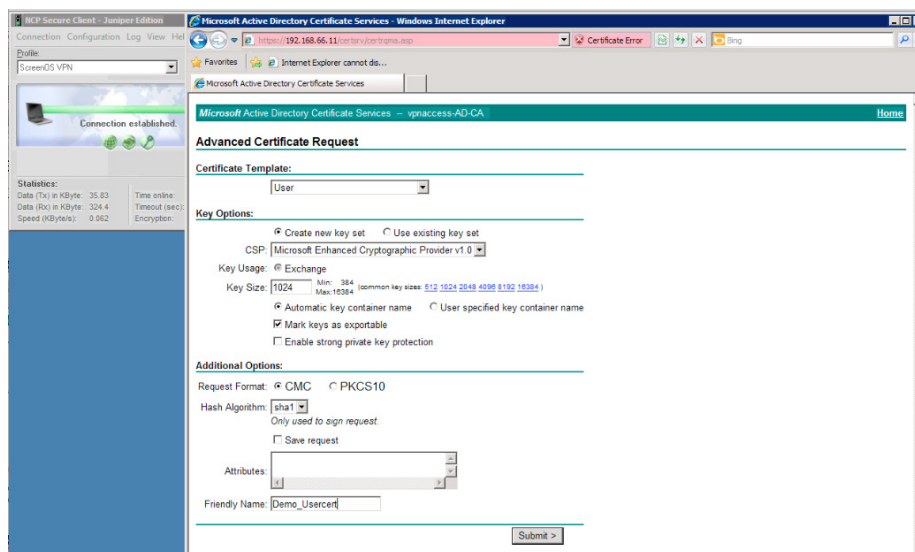
From the Microsoft TechNet: "If a certificate was issued from a Windows Server 2003 certification authority, the private key for that certificate is only exportable if the certificate request was made via the Advanced Certificate Request certification authority Web page with the Mark keys as exportable check box selected, or if the certificate is for EFS (Encrypting File System) or EFS recovery."



From the Advanced Certificate Request screen select "Create and submit a request to this CA"



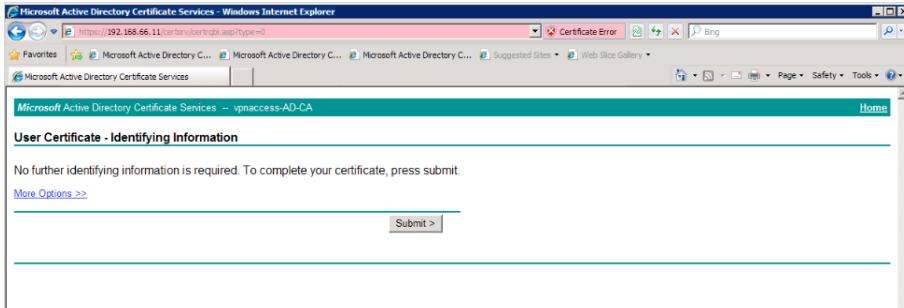
On the Advanced Certificate Request screen select Certificate Template "User" and enter a Friendly Name (eg Demo_User) and ensure that "Mark keys as exportable" is checked



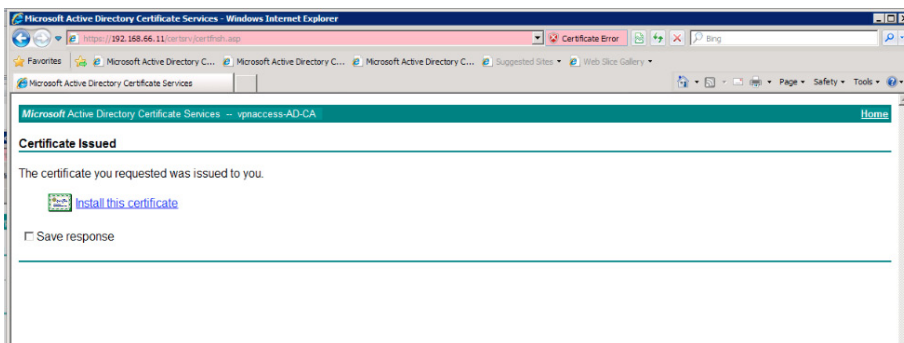
Quick Installation Guide

NCP Client with Juniper ScreenOS

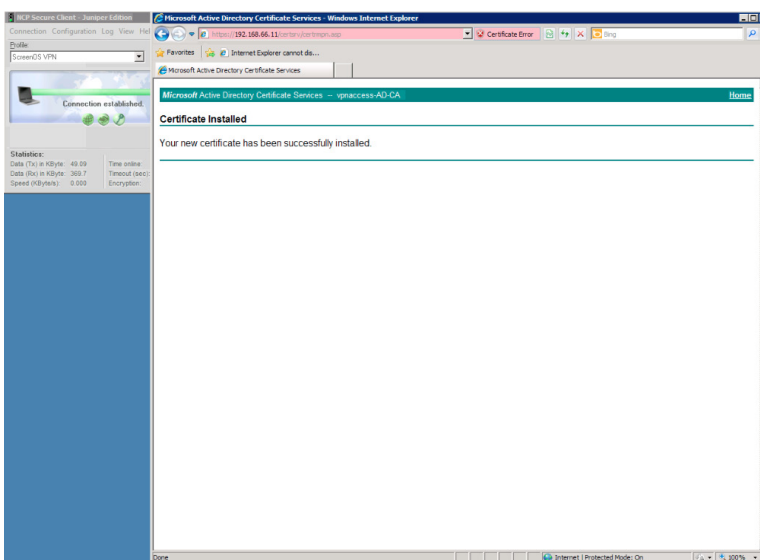
Click on Submit button



On the "Certificate Issued" screen select "Install this certificate"

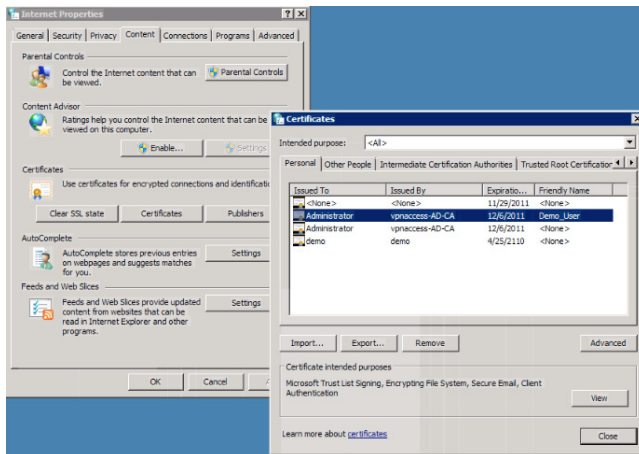


Confirm "Certificate Installed" message

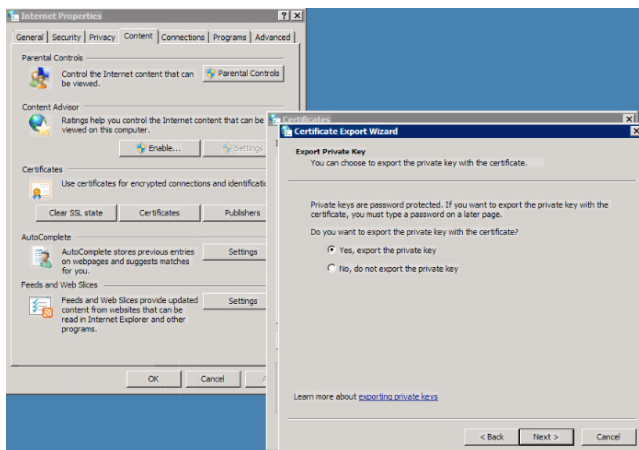


NCP Client with Juniper ScreenOS

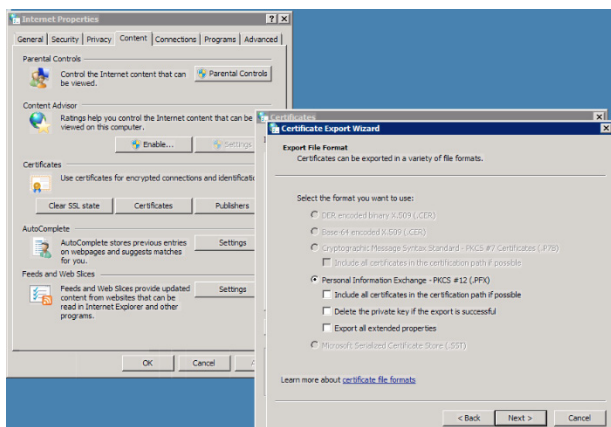
In the CA Store select the generated certificate and chose Export



In the Certificate Export Wizard select "Yes, export the private key"



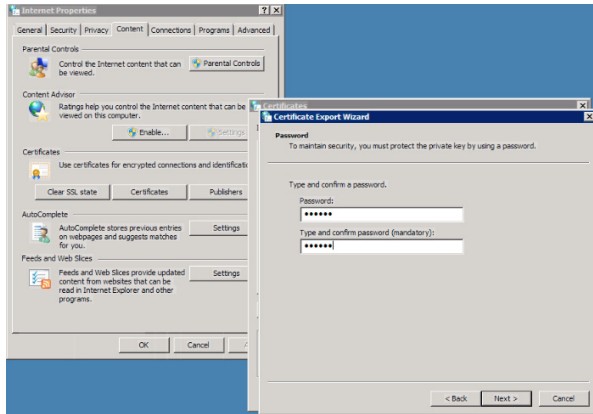
Select "Personal Information Exchange – PKCS #12"



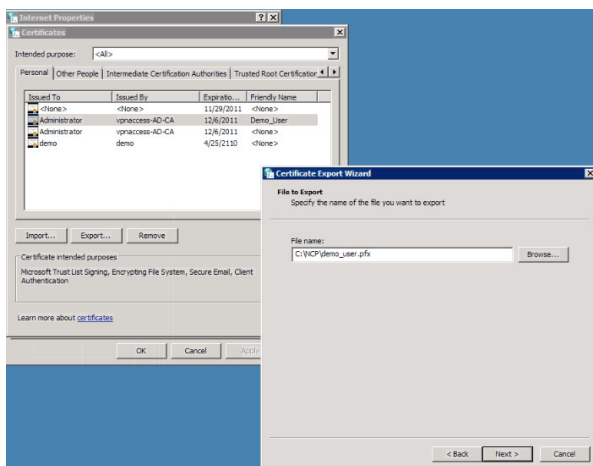
Quick Installation Guide

NCP Client with Juniper ScreenOS

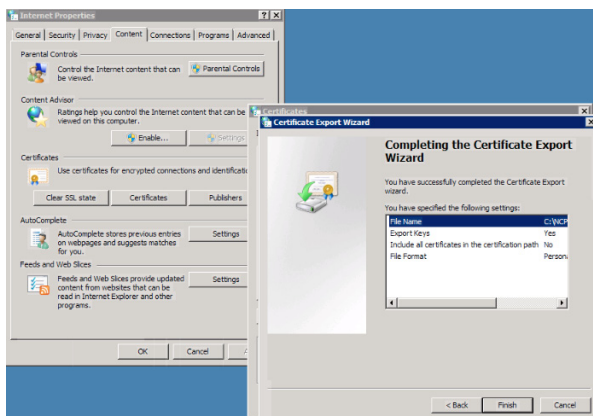
Enter the Password (eg 123456)



Complete the Client Certificate export by saving the certificate to a .pfx file

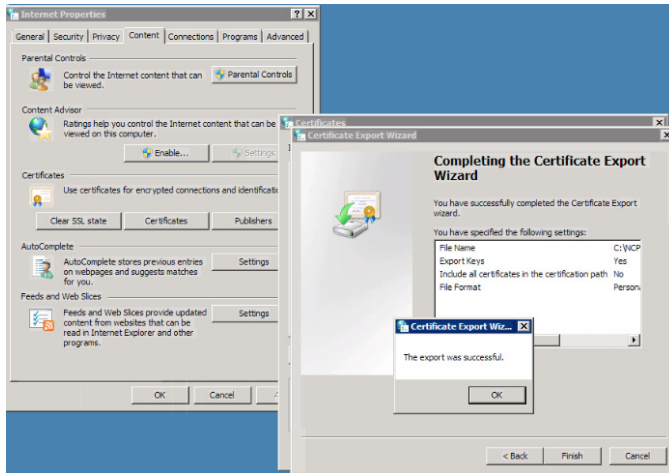


Select finish to complete the certificate export process

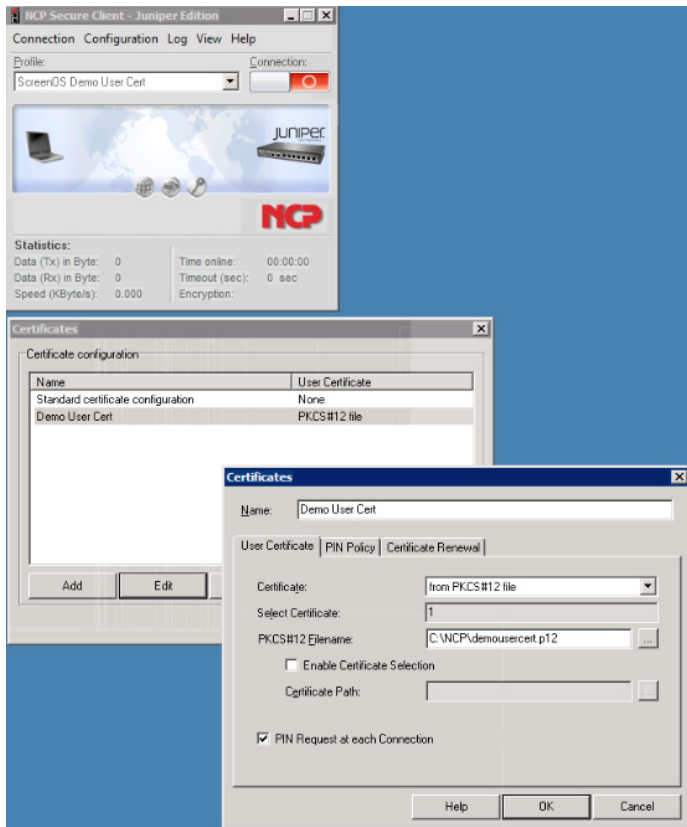


NCP Client with Juniper ScreenOS

Verify export success

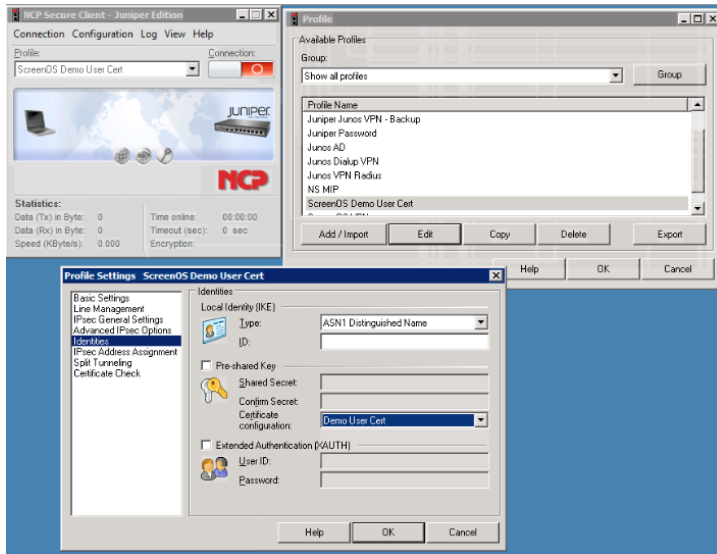


Rename the file from demo_user.pfx to demo_user.p12
Import the Certificate into the NCP client

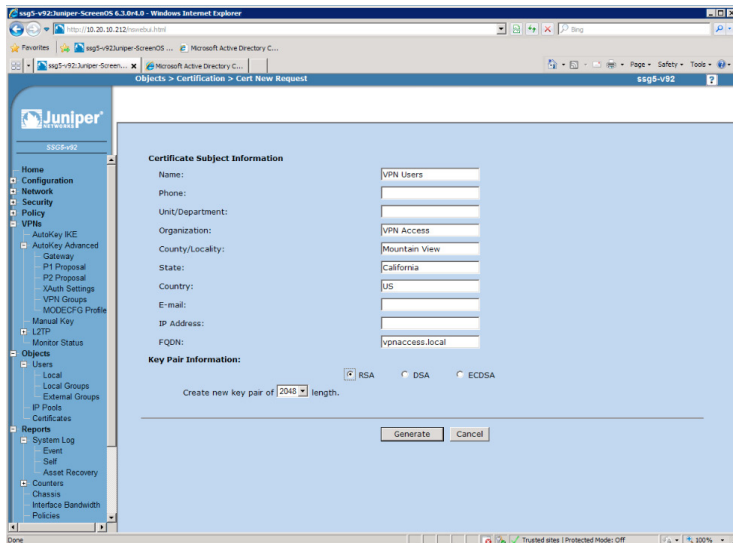


NCP Client with Juniper ScreenOS

Select certificate in the NCP Client Connection Profile

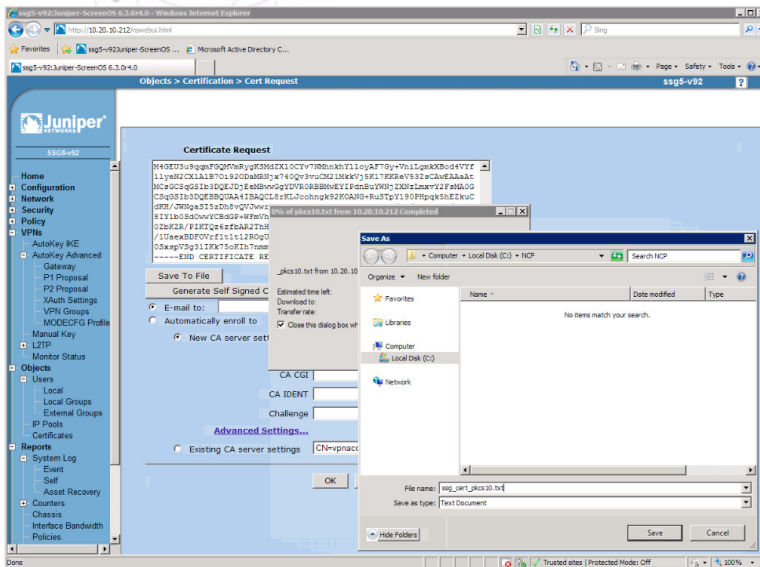


On the Juniper gateway go to Objects – Certificates and select New and enter the relevant information parameters



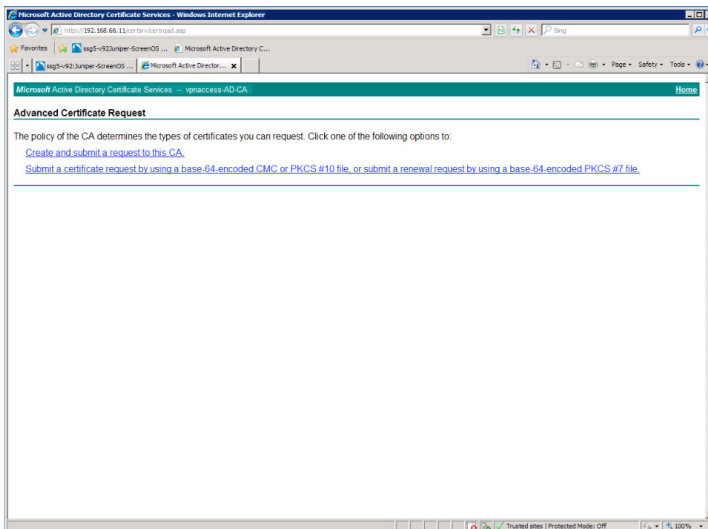
Click "Generate"
From the Cert Request window select "Save to File"

NCP Client with Juniper ScreenOS



Go back to the Cert Server Web UI and select Request a Certificate – submit an advanced certificate request

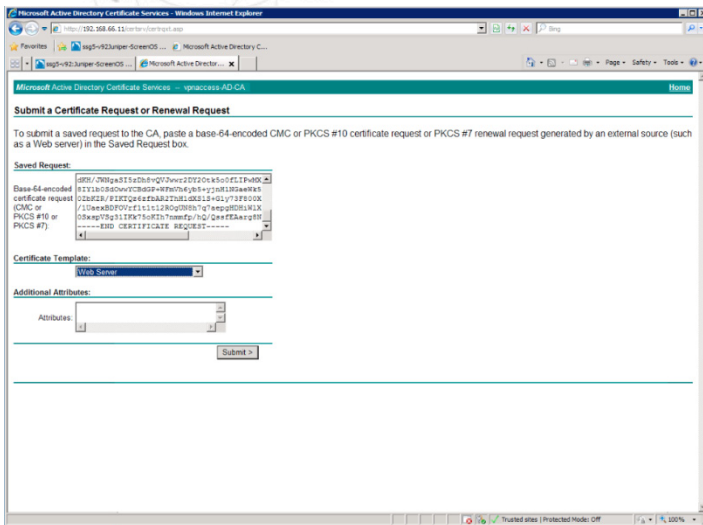
From the Advanced Certificate Request window select "Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file"



In the "Submit a Certificate Request or Renewal Request" window paste the cert request string

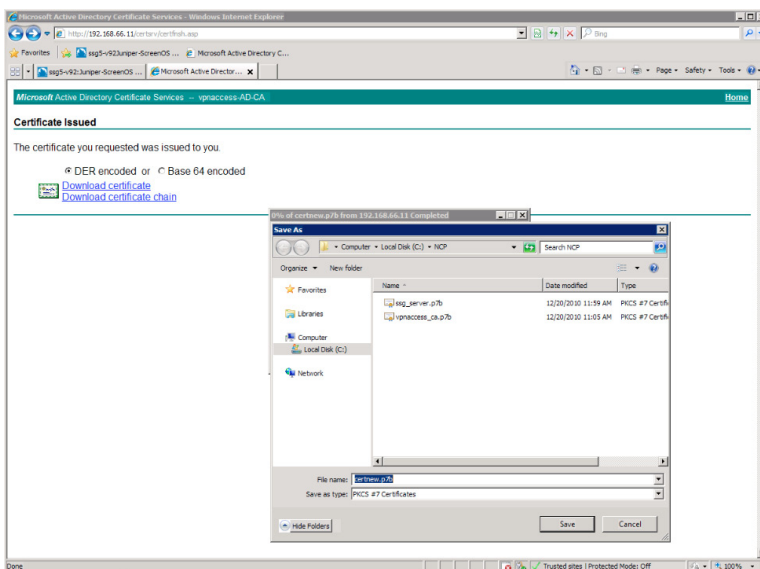
Quick Installation Guide

NCP Client with Juniper ScreenOS



Click Submit.

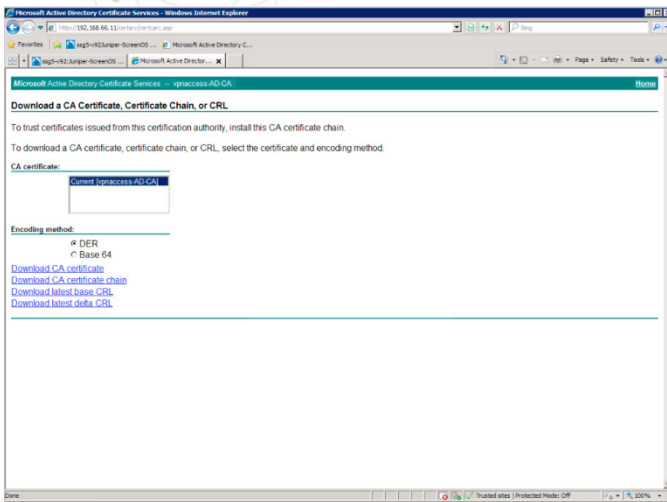
From the Certificate Issued window select "Download certificate chain". Save the file as the SSG Server Cert



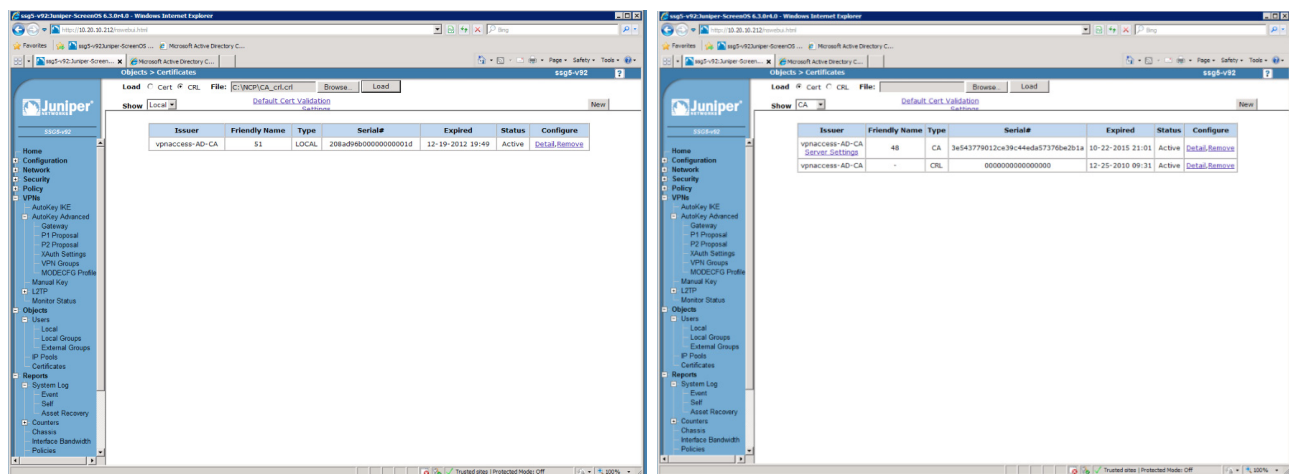
In the Juniper Gateway go back to Object – Certificates and Load the save Certificate Download Base CRL

Quick Installation Guide

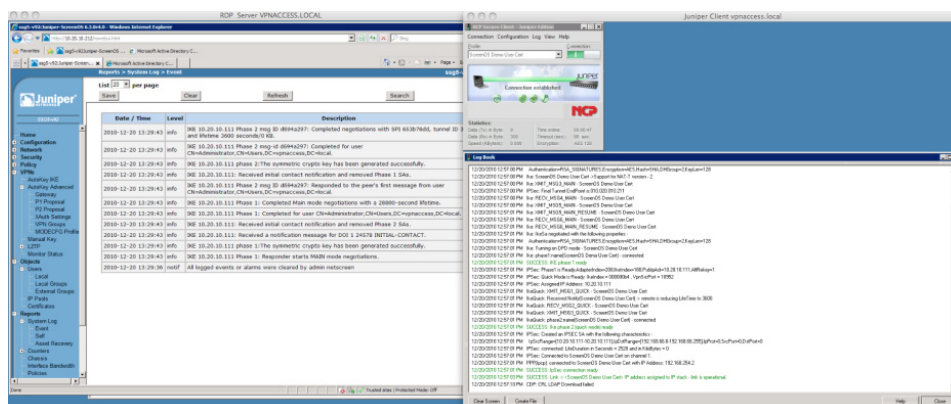
NCP Client with Juniper ScreenOS



Load CRL in Juniper Gateway. In Objects – Certificates select CRL radio button and browse to saved CRL file



Test the connection



NCP Client with Juniper ScreenOS

8. Troubleshooting

The following section provides a few troubleshooting tips.

8.1. Juniper Gateway Event Log

Look in the Event Log on the Juniper Gateway

8.2. CLI Debugging

From the CLI you can do some advanced troubleshooting.

Login to the console of the gateway

```
Rainer-Enders-MacBook-Pro:~ rainer$ ssh -l netscreen 10.20.10.212
netscreen@10.20.10.212's password:
Remote Management Console
```

Look at the sa table

```
ssg5-v92-> get sa
total configured sa: 8
HEX ID Gateway Port Algorithm SPI Life:sec kb Sta PID vsys
0000000a< 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I -1 0
0000000a> 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I -1 0
00008001< 10.20.10.111 500 esp:a128/sha1 bbb23378 2180 unlim A/D -1 0
00008001> 10.20.10.111 500 esp:a128/sha1 2af2bfe8 2180 unlim A/D -1 0
00000011< 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I 2 0
00000011> 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I 3 0
0000000f< 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I 5 0
0000000f> 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I 6 0
00008002< 10.20.10.111 500 esp:a128/sha1 bbb23379 2186 unlim A/D -1 0
00008002> 10.20.10.111 500 esp:a128/sha1 beeb3607 2186 unlim A/D -1 0
00000012< 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I -1 0
00000012> 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I -1 0
00000013< 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I -1 0
00000013> 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I -1 0
00008003< 10.20.10.111 500 esp:a128/sha1 bbb23375 2000 unlim I/I 2 0
00008003> 10.20.10.111 500 esp:a128/sha1 dff8f939 2000 unlim I/I 3 0
```

Start debugging by unsetting all previous debug configurations – if any

```
ssg5-v92-> undebug all
```

Verify filter lists – if any

```
ssg5-v92-> get ffilter
```

Clear the debug database

```
ssg5-v92-> clear db
```

NCP Client with Juniper ScreenOS

Set the filter

```
ssg5-v92-> set ffilter src-ip 10.20.10.111 dst-ip 10.50.50.10
```

```
filter added
```

Initialize debug

```
ssg5-v92-> debug flow basic
```

Get debug info

```
ssg5-v92-> get db stream
```

```
ssg5-v92-> set ffilter src-ip 172.16.123.101 dst-ip 10.50.50.10
```

```
filter added
```

```
ssg5-v92-> get db stream
```

```
***** packet decapsulated, type=ipsec, len=60*****
```

```
ipid = 3279(0ccf), @037f4cb0
```

```
tunnel.3:172.16.123.101/103->10.50.50.10/1,1(8/0)<Root>
```

```
no session found
```

```
flow_first_sanity_check: in <tunnel.3>, out <N/A>
```

```
chose interface tunnel.3 as incoming nat if.
```

```
flow_first_routing: in <tunnel.3>, out <N/A>
```

```
search route to (tunnel.3, 172.16.123.101->10.50.50.10) in vr trust-vr for vsd-0/flag-0/ifp-null
```

```
cached route 0 for 10.50.50.10
```

```
no route to (172.16.123.101->10.50.50.10) in vr trust-vr/0
```

```
packet dropped, no route
```

We see the reason for packets not being forwarded.

Root cause was missing route entry in the virtual router.

```
**** pak processing end.
```

```
***** packet decapsulated, type=ipsec, len=60*****
```

```
ipid = 3280(0cd0), @038004b0
```

```
tunnel.3:172.16.123.101/104->10.50.50.10/1,1(8/0)<Root>
```

```
no session found
```

```
flow_first_sanity_check: in <tunnel.3>, out <N/A>
```

```
chose interface tunnel.3 as incoming nat if.
```

```
flow_first_routing: in <tunnel.3>, out <N/A>
```

```
search route to (tunnel.3, 172.16.123.101->10.50.50.10) in vr trust-vr for vsd-0/flag-0/ifp-null
```

```
cached route 0 for 10.50.50.10
```

```
no route to (172.16.123.101->10.50.50.10) in vr trust-vr/0
```

```
packet dropped, no route
```

```
**** pak processing end.
```

```
ssg5-v92-> unset ffilter
```

```
filter 0 removed
```

```
ssg5-v92-> undebug all
```

```
ssg5-v92-> clear db
```

```
ssg5-v92->
```

NCP Client with Juniper ScreenOS

After route issue has been corrected.

```

ssg5-v92-> get sa
total configured sa: 6
HEX ID  Gateway      Port Algorithm  SPI    Life:sec kb Sta  PID vsys
0000000a<  0.0.0.0  500 esp:a128/sha1 00000000 expir unlim I/I  -1 0
0000000a>  0.0.0.0  500 esp:a128/sha1 00000000 expir unlim I/I  -1 0
00000011<  0.0.0.0  500 esp:a128/sha1 00000000 expir unlim I/I   2 0
00000011>  0.0.0.0  500 esp:a128/sha1 00000000 expir unlim I/I   3 0
0000000f<  0.0.0.0  500 esp:a128/sha1 00000000 expir unlim I/I   5 0
0000000f>  0.0.0.0  500 esp:a128/sha1 00000000 expir unlim I/I   6 0
00008004< 10.20.10.111 500 esp:a128/sha1 bbb2337a 3548 unlim A/D  -1 0
00008004> 10.20.10.111 500 esp:a128/sha1 328abb5f 3548 unlim A/D  -1 0
00000012<  0.0.0.0  500 esp:a128/sha1 00000000 expir unlim I/I  -1 0
00000012>  0.0.0.0  500 esp:a128/sha1 00000000 expir unlim I/I  -1 0
00008003< 10.20.10.111 500 esp:a128/sha1 bbb23375 1024 unlim I/I   2 0
00008003> 10.20.10.111 500 esp:a128/sha1 dff8f939 1024 unlim I/I   3 0
ssg5-v92-> get sa active
Total active sa: 1
total configured sa: 6
HEX ID  Gateway      Port Algorithm  SPI    Life:sec kb Sta  PID vsys
00008004< 10.20.10.111 500 esp:a128/sha1 bbb2337a 3545 unlim A/D  -1 0
00008004> 10.20.10.111 500 esp:a128/sha1 328abb5f 3545 unlim A/D  -1 0
ssg5-v92->
ssg5-v92-> get sa active
Total active sa: 2
total configured sa: 8
HEX ID  Gateway      Port Algorithm  SPI    Life:sec kb Sta  PID vsys
00008005< 10.20.10.111 500 esp:a128/sha1 bbb2337b 3597 unlim A/D  -1 0
00008005> 10.20.10.111 500 esp:a128/sha1 bebfd598 3597 unlim A/D  -1 0
00008004< 10.20.10.111 500 esp:a128/sha1 bbb2337a 3537 unlim A/D  -1 0
00008004> 10.20.10.111 500 esp:a128/sha1 328abb5f 3537 unlim A/D  -1 0
ssg5-v92-> undebg all
ssg5-v92-> get ffilter
Flow filter based on:
id:0 src ip 172.16.123.101 dst ip 10.50.50.10
ssg5-v92-> clear db
ssg5-v92-> debug flow basic
ssg5-v92-> get db stream
ssg5-v92-> get db stream
***** packet decapsulated, type=ipsec, len=60*****
  ipid = 3556(0de4), @0381e4b0
  tunnel.2:172.16.123.101/111->10.50.50.10/1,1(8/0)<Root>
  no session found
  flow_first_sanitary_check: in <tunnel.2>, out <N/A>
  chose interface tunnel.2 as incoming nat if.
  flow_first_routing: in <tunnel.2>, out <N/A>
  search route to (tunnel.2, 172.16.123.101->10.50.50.10) in vr trust-vr for vsd-
0/flag-0/ifp-null
  cached route 11 for 10.50.50.10
  [ Dest] 11.route 10.50.50.10->192.168.66.254, to bgroup0
  routed (x_dst_ip 10.50.50.10) from tunnel.2 (tunnel.2 in 0) to bgroup0
  policy search from zone 1-> zone 2
  policy_flow_search policy search nat_crt from zone 1-> zone 2

```

NCP Client with Juniper ScreenOS

```
RPC Mapping Table search returned 0 matched service(s) for (vsys Root, ip
10.50.50.10, port 19692, proto 1)
No SW RPC rule match, search HW rule
swrs_search_ip: policy matched id/idx/action = 4/3/0x1
Permitted by policy 4
No src xlate choose interface bgroup0 as outgoing phy if
no loop on ifp bgroup0.
session application type 0, name None, nas_id 0, timeout 60sec
service lookup identified service 0.
flow_first_final_check: in <tunnel.2>, out <bgroup0>
existing vector list 5-43ec5a4.
Session (id:8037) created for first pak 5
flow_first_install_session=====>
route to 192.168.66.254
cached arp entry with MAC 000c29e0653f for 192.168.66.254
arp entry found for 192.168.66.254
ifp2 bgroup0, out_ifp bgroup0, flag 00800800, tunnel ffffffff, rc 1
outgoing wing prepared, ready
flow got session.
flow session id 8037
flow_main_body_vector in ifp tunnel.2 out ifp bgroup0
flow vector index 0x5, vector addr 0x1ff2a50, orig vector 0x1ff2a50
post addr xlation: 172.16.123.101->10.50.50.10.
no more encapping needed
packet send out to 000c29e0653f through bgroup0
**** pak processing end.
***** 12818.0: <Trust/bgroup0> packet received [60]*****
ipid = 272(0110), @038f89b0
packet passed sanity check.
flow_decap_vector IPv4 process
bgroup0:10.50.50.10/1->172.16.123.101/111,1(0/0)<Root>
existing session found. sess token 3
flow got session.
flow session id 8037
flow_main_body_vector in ifp bgroup0 out ifp N/A
flow vector index 0x5, vector addr 0x1ff2a50, orig vector 0x1ff2a50
post addr xlation: 10.50.50.10->172.16.123.101.
going into tunnel 40008005.
flow_encrypt: pipeline.
chip info: PIO. Tunnel id 00008005
(vn2) doing ESP encryption and size =64
ipsec encrypt prepare engine done
ipsec encrypt set engine done
ipsec encrypt engine released
ipsec encrypt done
    put packet(3b9f958) into flush queue.
    remove packet(3b9f958) out from flush queue.

**** jump to packet:10.20.10.211->10.20.10.111
packet encapsulated, type=ipsec, len=120
ipid = 20946(51d2), @038f8984
out encryption tunnel 40008005 gw:10.20.10.111
```

NCP Client with Juniper ScreenOS

```
no more encapping needed
send out through normal path.
flow_ip_send: 51d2:10.20.10.211->10.20.10.111,50 => ethernet0/0(120) flag 0x0,
vlan 0
mac 000c298bcb54 in session
packet send out to 000c298bcb54 through ethernet0/0
**** pak processing end.
***** packet decapsulated, type=ipsec, len=60*****
ipid = 3557(0de5), @0381f4b0
tunnel.2:172.16.123.101/112->10.50.50.10/1,1(8/0)<Root>
no session found
flow_first_sanitary_check: in <tunnel.2>, out <N/A>
chose interface tunnel.2 as incoming nat if.
flow_first_routing: in <tunnel.2>, out <N/A>
search route to (tunnel.2, 172.16.123.101->10.50.50.10) in vr trust-vr for vsd-
0/flag-0/ifp-null
cached route 11 for 10.50.50.10
[ Dest] 11.route 10.50.50.10->192.168.66.254, to bgroup0
routed (x_dst_ip 10.50.50.10) from tunnel.2 (tunnel.2 in 0) to bgroup0
policy search from zone 1-> zone 2
policy_flow_search policy search nat_crt from zone 1-> zone 2
RPC Mapping Table search returned 0 matched service(s) for (vsys Root, ip
10.50.50.10, port 19691, proto 1)
No SW RPC rule match, search HW rule
swrs_search_ip: policy matched id/idx/action = 4/3/0x1
Permitted by policy 4
No src xlate choose interface bgroup0 as outgoing phy if
ssg5-v92-> unset ffilter
filter 0 removed
ssg5-v92-> undebg all
ssg5-v92-> clear db
ssg5-v92->
```

References

1. NetScreen Concepts & Examples, ScreenOS Reference Guide, Volume 5: VPNs
ScreenOS 5.1.0, P/N 093-1370-000, Rev. B
2. NetScreen Concepts & Examples, ScreenOS Reference Guide, User Authentication, Release
6.3.0, Rev. 01
3. Concepts & Examples, ScreenOS Reference Guide, Virtual Private Networks, Release 6.3.0,
Rev. 01
4. Application Note, Configuring a Dial-up VPN Using Windows XP Client with L2TP Over IPSec
(without NetScreen-Remote), Version 1.2