

#### **Revision History**

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

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

#### 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.



The following document outlines the configuration of a JUNOS based Juniper gateway and the NCP VPN client.



Juniper - NCP VPN

### A. 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*.



#### RADIUS configuration





## Juniper - NCP VPN

Fa Server Manager F. Server Manager File Action View Help		
Setting - Storage Sto	ies       Actions         Imper Radius Properties       Imper Radius Properties         Overview       Conditions   Constraints Settings         Configure the settings for this network policy:       Configure the settings for this network policy:         Configure the settings for this network policy:       Configure the settings for this network policy:         Configure the settings for this network policy:       Configure the settings for this network policy:         If conditions and constraints match the connection request and the policy grants access, settings are applied.         Settings:         If ADIUS Attributes         Standard         If vendor Specific         Network Access Protection         NaP Enforcement         Extended State         Recupion         If P Filers         Concypion         If P Settings   Add Edt. Permove	te, and See
	OK Cancel	Apply

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.

#### Juniper Gateway CLI

#### 1. 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

#### 2. 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

#### 3. 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

#### 4. Address book

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

#### 5. 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"

#### 6. 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



#### Juniper - NCP VPN

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 authentication-algorithm sha1 set security ike proposal PSK-AES256-SHA1-DH2 encryption-algorithm aes-256-cbc set security ike proposal PSK-AES256-SHA1-DH2 encryption-algorithm aes-256-cbc

#### 7. 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"

#### 8. 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 <u>user@juniper.net</u> set security ike gateway dialup-ike external-interface ge-0/0/0

#### 9. 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

#### 10. 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 encryption-algorithm aes-256-cbc set security ipsec proposal ESP-AES256-SHA lifetime-seconds 28800

#### 11. 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

#### 12. 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 13. 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

#### 14. 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

15. tcp-mss to eliminate fragmentation of TCP traffic across Tunnel set security flow tcp-mss ipsec-vpn mss 1350

# 16. Save and commit configuration commit

#### NCP Client Wizard:

1. Connection Type Configuration > Profiles > Add/Import Link to Corporate Network Using IPsec: (select) > Next



### 2. Profile Name

Configuration Profile Name: Juniper Junos VPN





Juniper - NCP VPN	4
New Profile Wizard	×
Profile Name Enter the profile name of the connection	NCP
The connection may be given a descriptive na	me. Enter a name in the following field.
Profile N <u>a</u> me: Juniper Junos VPN	
	< Back Next > Cancel

#### > Next

#### 3. VPN Gateway Parameters

Gateway (Tunnel Endpoint): 10.20.10.210 Extended Authentication (XAUTH): (select)

UserID:	vpnuser1
Password:	Password12
Password (confirm):	Password12

New Profi	ìle Wizard 🛛 🛛 🗙	C
VPN ( To whi establis	Gateway Parameters ich VPN gateway should the connection be shed?	
Enter ti the VP Using f authen connec	he DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of N gateway you want to connect to. Extended Authentication (XAUTH) you can enter the user ID and password for the trication. If no authentication data are entered they will be requested when establishing the ction.	
¢	Gateway (Tunnel Endpoint): 10.20.10.210 Extended Authentication (XALITH)	
<u>8</u> 2	User ID:       Vpnuser1       Password:       Password:       Password:	
	< Back Next > Cancel	

> Next
4. Exchange Mode
Exchange Mode: aggressive mode
PFS Group: DH-Group 2





#### > Next

5. Pre-shared Key Shared Secret: Confirm Secret: Local Identity (IKE): ID:

Tunneling123 Tunneling123 Fully Qualified Username user@juniper.net

New Profil	e Wizard	×
Pre-sh Common	ared Key n Secret for Data Encryption	NCP
A share identica Enter th	d secret or pre-shared key is used to encry Ily configured on both sides (VPN client an e appropriate value for the IKE ID accordir	pt the connection. This then needs to be d VPN gateway). ng to the selected ID type.
Ŗ	Pre-shared Key	
8	Local Identity (IKE) Iype: Fully Qualified Username ID: user@juniper.net	<u> </u>
	[	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel

> Next

6. IPsec Configuration: IP Addresses

IP Address Assignment: Local IP Address





### Juniper - NCP VPN

v Profil	e Wizard		
<b>IPsec</b> Assignir	Configuration - IP Addresses g the IP address to the client		102
Specify client's l	which IP address the client is going to use P address is dynamically assigned by the \	. By selecting ''Use IKE Config Mod 'PN gateway.	e'' the
Furthern	nore, define where the DNS / WINS serve	rs (if used) can be found.	
	IP Address <u>A</u> ssignment		
	Local IP Address		•
	IP Address:		
	0.0.0		
	DNS / WINS Servers		
	DNS Server:	<u>₩</u> INS Server:	
	0.0.0	0.0.0.0	
		<back next=""></back>	Cancel

> Next > OK

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





Profile Settings Juniper J	unos VPN	X IPsec Configuration X
Basic Settings Line Management Press General Sections Advanced Prec Options the Advanced Prec Options Set Tourneting Cettificate Check	Prec Ceneral Settings	Prec Configuration     PT IECRAS     To FXASE 528 5HA0H2     TT FXASE 55 5HA0H2     TT FXASE 5128 5HA     TT FXASE 5128 5H
	Help OK	Cancel

Profile Settings Juniper Junos VPN	×	TKE Policy
Basic dangs Line Monord Proced forward Schurger Adversed Pleve Gone (Pleve Gone Adverse Assignment Set Turnshy Certricate Check	eneral Settings Gateway (Turnel Endpornt) [10:20.11.210 IPE Policy: automatic mode Pigec Policy: automatic mode Pigec Policy: automatic mode Exch. Mode: aggressive mode PS Group: DH-Group 2 (10:24 Bit) Pickoy Lifetimes Policy Editor	Nome:     Exception       Authentication:     Encoption       Pre-shared Key     AES 256 Bit       State     State       Authentication:     Pre-shared Key       Add     Pre-shared Key       Hagh:     Stata       DH Group 2 (1024 Bit)     Y
	Help OK Cancel	Help OK Cancel

Profile Settings Juniper Ju	unos VPN	_				×	IP:	ec Policy			×
Basic Settings Line Management IPsec General Settings	- IPsec Ge	meral Settin	gs Tunnel Endpoi	A):				Name:	ESP-AES256-SHA		
Advanced IPsec Options Identities	8	10.20.11.	210					Protocol	Encryption	Authentication	
Split Tunneling	Policies					_		ESP	AES 256 Bit	SHA	
Ceruicale Crieck	9	IKE Policy	autom	atic mode		4					
		IPsec Poli	cy: autom	atic mode		4					
		Exch. Moi	se: aggre	sive mode		-		Destanal	rep	-	
		rrs alou	p: jun-a	oup 2 (1024 bit)		41		<u>Flotocor</u>	and one pa		Add
				y Liretimes	Policy Editor			Enclyption Authoritication:	MES 200 Bit		Remove
								Autoentication:	Тэне	<u> </u>	
									He		Cancel
			Help	OK	Cancel					φυκ	

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

Profile Settings Juniper J	unos VPN			×
Basic Settings Line Management	IPsec Ge	neral Settings —	15 1 1 0	
IPsec General Settings Advanced IPsec Options Identities		Gateway (1 unne 10.20.10.210	el Endpointj:	
IPsec Address Assignment Split Tunneling	Policies			
Certificate Check	A	IKE Policy:	PSK-AES128-SHA-DF	12 💌
	-	IP <u>s</u> ec Policy:	ESP-AES128-SHA	•
		Exch. <u>M</u> ode:	aggressive mode	•
		PFS Group:	DH-Group 2 (1024 Bit	<b>•</b>
			Policy Lifetimes	Policy Editor
			Help OK	Cancel

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





net becare chene bamper Edition	Profile		- 🗆
onnection Configuration Log View Help tofile: Con Juniper Junos VPN	nnection: Group: Show all profiles		oup
	JUNPEC Profile Name Juniper Junos VFN Profile Settings Juniper Junos VFN Bails Settings Line Management Line Management	Communication Medium Phone Number LAN di Pase Options If Disable DPD (Dead Peer Detection)	
Statistics: Jata (Tx) in Byte: 0 Time online: ( Jata (Tx) in Byte: 0 Timeout (sec): ( Speed (KByte/s): 0,000 Encryption:	Advanced IPsec Options Identities 00:00:00 0 sec Certificate Check	Interval: 20 Se Number of getries: 8	IC.
	ctivation		

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

Basic Settings Line Management IPsec General Settings Advanced IPsec Options Identities IPsec Address Assignment	inos VPN - Split Tunneling Enter the remote IP networks the tunnel should be used for, Without entries tunneling will always be used.					
Split Turneling Certificate Check		Remote Networks	Remote IP Net Ma	sks		
		Add Edit Delete Full Local Network Enclosure Mode				
		Help	ОК	Cancel		

Profile Settings Juniper Ju Basic Settings Line Management IPsec General Settings Advanced IPsec Options Identities IPsec Address Assignment	INOS VPN - Split Tunneling Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used.					
Split Turneling Certificate Check		Remote Networks	: Remote 255.25	HP Net Mask 5.255.0	sks	
		Add Edit Delete				
		He	lp (	ок	Cancel	

Select OK and close all the windows.

Click the connection button to establish the VPN gateway connection.

## Juniper - NCP VPN





## **B.** 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;
    }
}
```

## **C. Multiple Subnets**

If multiple subnets are referenced in the same policy, the proxy-ids 0.0.0/0 are used for both local and remote!

```
Apr 20 11:13:47 matched configured proxy ids:
remote=ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
local=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.

#### Troubleshooting

The following section provides a few troubleshooting tips.

## 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 access: 0:00:24 Policy name: lnx2-telnet-lnx1 Source zone: dl2 Destination zone: 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 d12 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:



### Juniper - NCP VPN

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

#### 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.

#### 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]

#### 4. Traceoptions (IPsec)

Syntax traceoptions {

flag {

all;

next-hop-tunnel-binding;

packet-drops;

packet-processing;

security-associations;

#### }

}
Hierarchy Level
[edit security ipsec]



#### 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

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

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

Installation Guide	NCP
Juniper - NCP VPN	SECURE COMMUNICATIONS
Task	Command
Display IPsec VPN security associations for service sets.	show services ipsec-vpn ipsec security-associations
Display IPsec VPN statistics for service sets.	show services ipsec-vpn ipsec statistics
Encryption Interface	
Clear Internet Key Exchange (IKE) security associations.	clear ike security-associations
Clear IPsec security associations.	clear ipsec security-associations
Switch between primary and backup interfaces and tunnels.	request ipsec switch
Obtain a public key certificate from a certification authority.	request security certificate (signed) request security certificate (unsigned)
Generate a public and private key pair.	request security key-pair
Add a certificate provided by the Juniper Networks certificate authority.	request system certificate add
Display IKE security association information.	show ike security-associations
Display the IPsec certificate database.	show ipsec certificates
Display primary and backup interface and tunnel information.	show ipsec redundancy

Display IPsec security association information.

show ipsec security-associations Display installed certificates signed by the Juniper Networks certificate show system certificate authority.

#### 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/ipsecurity-op-cmd-table.html Published: 2010-11-08