

Quick Installation Guide NCP Client with Juniper ScreenOS

As of March 2012 version 1.1

te access SP **Quick Insta**

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 support@ncp-e.com

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

(USA) (Europe)

(English)

(German)

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.



NCP Client with Juniper ScreenOS

Contents

1.	Re	evision History	4
2.	Po	blicy-Based VPN & Shared IKE ID with Preshared Key	5
3.	Ju	Iniper Gateway Configuration - WebUI	7
4.	N	CP Client Wizard:	
4	l.1.	Connection Type	18
4	ł.2.	Profile Name	18
4	ł.3.	VPN Gateway Parameters	18
4	ł.4.	Exchange Mode	19
4	ł.5.	Pre-shared Key	19
4	ł.6.	IPsec Configuration: IP Addresses	19
5.	N	CP Client Configuration – Profile changes	20
6.	Ro	oute-Based VPN & Multiple Proxy ID support on a Route-Based VPN	24
7.	Ac	lvanced Configuration	
8.	Tr	oubleshooting	54
8	3.1.	Juniper Gateway Event Log	54
8	3.2.	CLI Debugging	



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.



Administrator: C:\Win	dows\system32\cmd.ex	e		
C:∖>route -p add 1	.72.16.100.0 mask	255.255.255.0 192	.168.66.2	^
OK!				
C:∖>netstat -rn				
Interface List				
1400 0c 29 47	a1 c3Intel	(R) PRO/1000 MT N	etwork Connection	#2
1100 0C 29 47	al byIntel	ave Loophack Inte	etwork Connection	
1200 00 00 00	00 00 00 e0 Micro	soft ISATAP Adapt	er	
1300 00 00 00	00 00 00 e0 Tered	o Tunneling Pseud	o-Interface	
1500 00 00 00	00 00 00 e0 Micro	soft ISATAP Adapt	er #2	
IPv4 Route Table				
Active Routes:				
Network Destinatio	n Netmask	Gateway	Interface	Metric
10.0.0.0	0.0.0.0	192.168.66.1	192.168.66.10	266
10.20.0.0	255.255.0.0		10.20.13.10	200
10.20.13.10	200.200.200.200 0FF 0FF 0FF 0FF		10.20.13.10	200
10.20.200.200	200.200.200.200		10.20.10.10	200
127.0.0.0	222.0.0.0 200 200 200 200	On-link	127.0.0.1	200
100 000 000 000	200.200.200.200.200 9EE 9EE 9EE 9EE	On-link	127.0.0.1	206
179 16 100 0	2JJ-2JJ-2JJ-2JJ	100 100 00 0	100 100 00 10	11
102 100 66 0	200.200.200.00 900 900 900 0	0p-lipk	102 100 00 10	266
102 100 00 0	200.200.200.00 966 966 966 966		102 100 00 10	200
102 100 00 10	200.200.200.200.200 9EE 9EE 9EE 9EE	On-link	102 100 00 10	200
224 0 0 0	233-233-233-233	On-link	127 0 0 1	200
221.0.0.0	240.0.0.0	On-link	100 100 00 10	266
221.0.0.0	240.0.0.0	On-link	10 20 12 10	200
	210.0.0.0 210.0.0.0	On-link	100.20.13.10	200
200.200.200.200	200.200.200.200.200 9EE 9EE 9EE 9EE	On-link	102 160 66 10	266
255-255-255-255 255 255 255 255	200-200-200-200 200-200-200-200	On link	10 20 12 10	200
233.233.233.233	233.233.233.233		10.20.13.10	200
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.



> 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".





ssg5-v92

?

NCP Client with Juniper ScreenOS

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

Objects > IP Pools > Edit

IP Pool Name	vpn_pool
Start IP	172.16.100.100
End IP	172.16.100.200
	OK Cancel



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: <u>users@juniper.net</u>

ssg5-v92:Juniper-ScreenOS 6.3.0r7.0				👌 • 🖸 × 🗔 🖷 •	Page • Safety • T	ools + 🔞 +
Obj	ects > Users > Local > Edit				ssg5-v92	?
🔁 Juniper'						
SSG5-v92		Α.	uth/IKE/XAuth/L2TP User			
Home	User Name	NCP Users				
Network	Status	Enable	C Disable			
Security Policy						
- Policies	IKE User Eimple Ident	lite	Number of Multiple Logi	ns with Same ID 25		
Policy Elements	IKE I	D Type U-FQDN	IKE Identity	users@juniper.net	_	
VPNs AutoKey IKE	🔍 Use Distingu	ished Name For ID				
E AutoKey Advanced						
– P1 Proposal	Authentication Use	r	User Password			
- P2 Proposal - XAuth Settings	XAuth User		Confirm Password			
- VPN Groups	L2TP User					
MODECFG Profile			OK Cancel			
L2TP Monitor Status			Curcer			
- Objects						

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.

Group Name	Office		
< Group Members> NCP Users	<< >>	< Available Members> NCP Users	
	ОК С	ancel	



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

ssg5-v92:Juniper-ScreenOS 6.3	.0r7.0	🦄 + 🖸 - 🗆 👘 + Page + Safety + Tools + 🔞 +
Muniper [.]	Objects > Users > Local > Edit	ssg5-v92 ?
\$\$G5+v92		uth/IKE/XAuth/L2TP User
Home • Configuration • Network	User Name test1@juniper.net Status C Enable	C Disable
Security Policy Policies MCast Policies Policy Elements	IKE User Simple Identity Supple Identity	Number of Multiple Logins with Same ID 1
VPNs AutoKey IKE AutoKey Advanced Gateway	Use Distinguished Name For ID	User Password
P1 Proposal P2 Proposal XAuth Settings VPN Groups	L2TP User	(Remote IP: 0.0.0.)
MODECFG Profile Manual Key L2TP Monitor Status	Primary DNS IP 00.0.0	Static IP 0.0.0.0 Primary WINS IP 0.0.0.0
Objects Users Local Local Groups External Groups	Secondary Dies IP 0.0.0.0	OK Cancel

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

ssg5-v92:Juniper-ScreenOS 6.3.0r7.0			🋐 🕶 🗔 👻 🖃 👼 👻 Page 🗸 Safety 🕶 Tools 🕶 😧
ob Juniper	jects > Users > Local > Edit		ssg5-v92 ?
S5G5-v92		Auth/1	KE/XAuth/L2TP User
- Home Configuration Network	User Name Status	test2@juniper.net	C Disable
Security Policy Policies MCast Policies Policy Elements	 IKE User Simple Ident Use Distingu 	ity ished Name For ID	Number of Multiple Logins with Same ID 1
VPNs AutoKey IKE Gateway P1 Proposal P2 Proposal	Authentication User XAuth User L2TP User	r	User Password Confirm Password
XAuth Settings VPN Groups MonceCFG Profile Manual Key LIZTP Monitor Status Objects	L2TP/XAuth Remot Primary Secondary	e Settings IP Pool VPN Pool DNS IP 0.0.0.0 DNS IP 0.0.0.0	(Remote IP: 0.0.0) Static IP (0.0.0.0 Primary WINS ID (0.0.0.0 Secondary WINS IP (0.0.0
Local Local Local Groups External Groups		_	OK Cancel



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.

🗩 🕑 🗢 🎦 http://10.20.10.2	12,hewebui html			•	9 ** ×	P Bing		1
Favorites 🍦 🎦 ssg5-v92Ju	niper-ScreenOS 🙋 Microsoft Active Di	ectory C						
ssg5-v92:Juniper-ScreenOS 6.3.0	9:4.0				5	• 🖸 • 🖻	🖶 • Page • Safety •	Tools -
	Network > Interfaces (List)						ssg5-v92	?
	List 20 • per page							
The luniner	List ALL(13) Interfa	ces					New Tunnel	F *
a Januari her								
\$\$G5-192	Name	IP/Netmask	Zone	Туре	Link	PPPoE	Configure	
	bgroup0	192.168.66.2/24	Trust	Layer3	Up		Edit	
Configuration	ethernet0/4				Up	-	Edit	
etwork	ethernet0/5		1		Up	-	Edit	
Binding	ethernet0/6				Up	-	Edit	
Zones	bgroup1	0.0.0/0	Null	Unused	Down		Edit	_
Interfaces	bgroup2	0.0.0/0	Null	Unused	Down	-	Edit	
Backup	bgroup3	0.0.0/0	Null	Unused	Down	-	Edit	
DHCP	ethemet0/0	10.20.10.211/16	Untrust	Laver3	Up	-	Edit	
Buz 1x	ethernet0/1	0.0.0/0	DMZ	Laver3	Down		Edit	-
PPP	ethemet0/2	0.0.0/0	Null	Unused	Down	-	Edit	
- DSCP	ethernet0/3	192,168,100,1/24	Trust	Laver3	Down		Edit	_
Policy	secial0/0	0.0.0/0	Null	Unused	Un		Edit	
- Policies	tunnel.1	unnumbered	Untrust	Tunnel	Ready		Edit	
Policy Elements	tunnel.2	unnumbered	Untrust	Tunnel	Ready	-	Edit	
PNs	tunnel.3	unnumbered	Trust	Tunnel	Down		Edit Remove	_
Reports	vlant	0.0.0/0	VLAN	Laver3	Down		Edit	
System Log		0.0.014/0	Tott	cayers			Austra	
Event								
Asset Recovery								
Counters								
Chassis								
Interface Bandwidth								
Policies								
Administrator Login								
MacAddress								
Active Users								
Wizards								
Help								
opout								

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

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



V / W

1					
	VPNs > AutoKey Advanced > Gateway	> Edit		ssg5-v92	?
SSG5-v92	Gateway Nam	e VPN Gateway			
- Policies - MCast Policies	Versio	n • IKEv1 O IKEv2			
Policy Elements	Remote Gateway				
VPNs AutoKey IKE	Static IP Address	IP Address/Hostname			
 AutoKey Advanced Gateway 	O Dynamic IP Address	Peer ID			
- P1 Proposal	O Dialup User	User	None 💌		
 P2 Proposal XAuth Settings 	Dialup User Group	Group	Office -		
	ACVPN-Dynamic Local ID [DistinguishedName] ACVPN Profile	1			
- Objects	ACVPN-Pione				
Users Users Local Local Groups External Groups Certificates Wizards Help Logout		OK Can	el Advanced		

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.



	VPNs > AutoK	ey Advanced	> Gateway > Edit				ssg5	-v92
SSG5-v92	Name	Peer Type	Address/ID/User Group	Local ID	Security Level		Config	jure
- Policies - MCast Policies	VPN Gateway	Dialup	Office		Custom	Edit	Xauth	Remove
Policy Elements VPNs AutoKey IKE AutoKey Advanced Gateway P1 Proposal P2 Proposal Xauth Settings VPN Groups Manual Key L2TP		Message from we	bbase gint IKE dakup group configurated. Pk	ease note XAUTH	server must be turne	d on as we	X.	

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

Local Authentication: (select) Allow Any

ssg5-v92:Juniper-ScreenOS 6.3.0r3	7.0 🛅 + 🔂 - 🖂 👘 - Page - Safety - Tools - 🕯
	VPNs > AutoKey Advanced > Gateway > Xauth ssg5-v92 ?
Juniper"	Gateway Name: VPN Gateway
SSG5-v92	○ None
Home	© XAuth Server
Configuration	
Network	Authentication Settings:
Security	Allowed Authentication Type @ Generic _ CHAR Only _ CHAR & RAR
Policy	
Policies MCast Palisies	© Local Authentication
Policy Elements	C Allow Any
- VPNs	C User None •
AutoKey IKE	
 AutoKey Advanced 	
Gateway	External Authentication None 1 Query Remote Setting
P1 Proposal	Allow Any
- P2 Proposal	C User Name
XAuth Settings	C User Group Name
MODECFG Profile	C Bypass Authentication
Manual Key	
L2IP	Accounting Settings:
- Monitor Status	
- Users	Accounting Server
Local	Accounting Off
- Local Groups	C Markle Official
External Groups	Adventeent
- IP Pools	Allowed Audiendosadon Type C Any C Char Only C Security
Certificates	User Name
- Reports	Password
- System Log	Update DHCP Server
- Self	Prehz Delegation to IPv6 Interfaces Interface SLA ID SLA Length Action
Asset Recovery	
Counters	
- Chassis	No entry available
Interface Bandwidth	
Policies	OK Apply Cancel
Administrator Login	
<	

AutoKey IKE

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



	1 1 7 2							
VI	PNs > AutoKey IKE > E	dit					ssg5-v92	?
The luminor								
SSG5-v92	N Name	Secure Remote Access						
Policies MCast Policies	Remote Gateway ®	Predefined Create a Simple Gatewa	ау	J	VPN Gatev	/ay 💌		
Policy Elements VPNs		Gateway Name						
AutoKey IKE		Version	• IKE	Ev1		C IKEv2		
 AutoKey Advanced Gateway 		Туре	• Sta	atic IP	Address/	Hostname		
P1 Proposal			O Dy	namic IP		Peer ID		
- P2 Proposal			O Dia	alup User		User	None 👻	
VPN Groups			O Dia	alup Group	5	Group	None -	
Manual Key		Local ID			(optiona	D.		
L2TP Monitor Status		Preshared Key			X-F-0-	Use As Se	ed 🔲	
- Objects		Security Level	• Sta	andard	C Com	natible	C Basic	
Users		Outgoing Interface	ethern	et0/0 👻	com	Jacobie	Buble	
Local Groups	ACVPN-Dynamic	Gateway None - Tur	nel To	wards Hul	•			
- IP Pools	ACVPN-Profile	Binding to Tunnel Non	e 🔻					
Certificates		OK Car	cel	Adva	nced			
+ Reports								
- Help								
Logout								

Advanced

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

	VPNs > AutoKey IKE > Edit		ssg5-v92 🔽
The luninor			
SSG5-v92 Policies	Security Level Predefined User Defined	C Standard C Compatible C E Custom	lasic
Policy Elements		Phase 2 Proposal	
- VPNs		hopis-esp-aes 128-sna 💽 None	
- AutoKey IKE		None None	
 AutoKey Advanced Gateway P1 Proposal P2 Proposal 	Replay Protection Transport Mode	(For L2TP-over-IPSec only)	
- XAuth Settings	Bind to	None	
- VPN Groups	bille to	C Tunnel Interface	none 💌
— Manual Key			Untrust-Tun 👻
L2TP		Funder Zone	,
- Objects	Proxy-ID		
- Users	Local IP / Netmask	1	
- Local	Remote IP / Netmask	/	
- Local Groups	Service	ANY	
- IP Pools			
Certificates	DSCP Marking	© Disable	-
Reports		Enable	Dscp Value 0
+ Wizards	VPN Group	None -	Weight 1
Logout		,	
	VPN Monitor		
Toggle Menu 📃	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) s	sg5-v92 ?
D Juniner [®]		
A ANETWORKS		4
	-	
SSG5-v92	Name (optional)	
Marine -		
Home	Source Address	
+ Configuration	Address Book Entry Dial-Up VPN Multiple	
+ Network	C New Address /	
+ Security	Destination Address	
Policy		
- Policies	Service ANY Multiple	
	Application None	
	WEB Filtering	
- P1 Proposal	Action Tunnel -	
- P2 Proposal		
- XAuth Settings	Antispam enable	
- VPN Groups	Tunnel VIII Secure Remote Access	
– Manual Key		
+ L2TP	Modify matching bidirectional VPN policy	
Monitor Status		
- Objects		
E-Users	Logging 🗹 at Session Beginning 🗹	
- Local	Position at Ton	
- Local Groups		
External Groups		
- IP Pools	Session-limit	
Certificates		
+ Reports	Counter 0	

Watch for two policies created in the two specified zones.



	Poli	cy > Poli	cies (From All	zones To	All zone	s)				ssg5-v92	
	List	20 – p	er page								Searc
Juniper"	Fro	m All zor	ies 💌			To All zones	•	Go			Ne
SSG5-v92	Fro	m Trust T	⁻ o Untrust, tota	I policy: 2	2						
	ID	Source	Destination	Service	Action	Options		Config	jure	Enable	Move
Configuration	3	Any	Dial-Up VPN	ANY	¢ 8 ¢	6	<u>Edit</u>	<u>Clone</u>	Remove	2	\$
etwork ecurity	1	Any	Any	ANY	Ø		Edit	<u>Clone</u>	Remove	2	\$
Policios	Fro	m Untrus	t To Trust, tota	I policy: :							
MCast Policies	ID	Source	Destination	Service	Action	Options		Config	jure	Enable	Move
Policy Elements PNs	2	Dial-Up	Any	ANY		E	Edit	Clone	Remove	v	¢

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				_ 🗆 ×
G) = http://10.20.10.212	2/nswebui.html		💌 🗟 😽 🗙 🔎 Bing		ρ.
👷 Favorites 🛛 🙀 🎦 ssg5-v923unij	per-ScreenOS 🙋 Microsoft Active Director	y C			
ssg5-v92:Juniper-ScreenOS 6.3.0r4	4.0		🟠 • 🖾 · 🖻	🖶 • Page • Safety •	Tools • 🔞 •
	Policy > Policy Elements > Addre	esses > List		ssg5-v92	?
	List 20 v per page				
M Juniper	Trust Filter: ALL 0-9	<u>A B C D E F G-I J-L M N O P Q R S T U V W</u>	<u>X-Z</u>		New
A NETWORKS					
SSG5-v92	Name	IP/Domain Name	Comment	Configure	
- Home	172.16.66.0/24	172.16.66.0 /24		Edit Remove	
Configuration	172.16.66.100/32	. 172.16.66.100 /32		Edit Remove	
 Network Binding 	192.168.66.10	1 92.168.66.10 /32		Edit In Use	
. DNS	192.168.66.11	1 92.168.66.11 /32		Edit In Use	
- Zones	AD	. 192.168.66.11 /32		Edit Remove	
- List	Any	₫0.0.0.0 /0	All Addr	In Use	
- Backup - DHCP	Dial-Up VPN		Dial-Up VPN Addr		
• 802.1X	Radius	1 92.168.66.10 /32		Edit Remove	
+ PPP	Remote Zone 10	a 10.50.50.0 /24		Edit In Use	

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



Standard Screen Screen OS	5.3.0r4.0 - Windows Internet Explorer		
😋 🕞 🗢 🎦 http://10.20.10.	212/nswebui.html	🔽 🗟 🖘 🗙 🔎 Bing	P -
👷 Favorites 🏼 🍰 ssg5-v923	uniper-ScreenOS 🙋 Microsoft Active Directory C		
ssg5-v92:Juniper-ScreenOS 6.3	0r4.0	🚺 * 🔂 - 🖃 🖶 * Pa	ge 🔹 Safety 🔹 Tools 🔹 😥 🔹
	Policy > Policy Elements > Addresses > Con	nfiguration	ssg5-v92 ?
The luminor			
A Sumper			
SSG5+y92	Address Name	Trusted Access	
Home	Comment		
Configuration	IP Address/Domain Name		
 Network Binding 	ID Address/Natmask		
 DNS 	(wildcard mask)	192.168.66.0 / 24	
Zones	C Domain Name		
 Interfaces 		· · · · · · · · · · · · · · · · · · ·	
Backup			
- DHCP	Zone	Trust 💽	
• 802.1X			
Routing PPP		OK Cancel	
DSCP			
Security			
Policies			
MCast Policies			
Policy Elements			
- Addresses			
Groups			
Summary			
Schedules			
Traffic Shaping			
Group Expression:			
- VPNs			

Select OK

🖉 ssg5-v92:Juniper-Screen(os 6.3.0	r4.0 - Windows Internet Explorer				_ 0
🕒 🕞 🗢 🎦 http://10.20.1	10.212/	nswebui.html		💌 🗟 🐓 🗙 🔎 Bing		٩
👷 Pavorites 🛛 🍰 ssg5-v/	92.Junipe	er-ScreenOS 😢 Microsoft Active Directory	c			
ston5-v92: Juniner-ScreenOS (5.3.0(4)			A • N • =	- Per	ze • Safety • Tools • 😱
		Policy > Policy Elements > Addre	sses > List			ssa5-v92 ?
	-					•
		List 20 per page				
Juniper		Trust Filter: ALL 0-9 A	BCDEFG-IJ-LMNOPQRSTUVW	<u>X-Z</u>		New
A ARTWORKS						
SSG5-v92		Name	IP/Domain Name	Comment		Configure
Home	-	172.16.66.0/24	A 172.16.66.0 /24		Edit	Remove
Configuration		172.16.66.100/32	3 172.16.66.100 /32		Edit	Remove
- Network Binding		192.168.66.10	192.168.66.10 /32		Edit	In Use
DNS		192.168.66.11	192.168.66.11 /32		Edit	In Use
Zones		AD	192.168.66.11 /32		Edit	Remove
List		Any	0.0.0.0 /0	All Addr		In Use
- Backup		Dial-Up VPN		Dial-Up VPN Addr		
 802.1X 		Radius	1 92.168.66.10 /32		Edit	Remove
Routing PPP		Remote Zone 10	10.50.50.0 /24		Edit	In Use
L DSCP		Trusted Access	192.168.66.0 /24		Edit	In Use
Security Delice						
Policies						
- MCast Policies						
 Policy Elements 						
- Addresses						
Groups						
Summary	_					
 Services 						
- Schedules						
Traffic Shaping						
Group Expression						

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)



NCP Client with Juniper ScreenOS

Ssg5-v92:Juniper-ScreenOS 6.3.0r4.0 - Windows Internet Explorer	
Co - Martine //10.20.10.212/newebui.html	• 🛛 + 🗙 🖓 Bing 🛛 🔎 •
🔶 Pavorites 🔄 📩 ssg5-v92Juniper-ScreenOS 🖉 Microsoft Active Directory C	
	D . D . Then a Dama Cafety a Tank a Da
Palicy > Palicies (From United To T	
Policy > Policies (Prolitionarius) for	usi) sajovoz <mark>?</mark>
(N) luniner	
Name (option	
- Home Source Addr	C New Address /
Configuration	Address Book Entry Dial-Up VPN Multiple
- Network Binding	C New Address
DNS Destination Addr	ess C address Dark Colors Touted Access T Multiple
Zones	Address Book Entry Hosted Access
Interfaces Serv	ANY Multiple
Backup Applicat	tion None 💌
DHCP	
■ 802.1X	WEB Eitering
Routing DOD	- Web Pittering
DSCP	tion Tunnel
Security Antispam ena	ible 🗖
Policy Tur	Inel VPN Secure Remote Access -
MCast Policies	
Policy Elements	Modify matching bidirectional VPN policy
Addresses	L2TP None -
List	ing 🔽 at Session Beginning 🔽
Summary Position at	Top 🔽
Services	
Schedules	mit
Group Expression	
DIP	iter 0
VPNs Alarm without d	rop 🗖
Autokey IKE	
Gateway	OK Cancel Advanced
P1 Proposal	
P2 Proposal Voute Settings	
VPN Groups	
MODECFG Profile	
	👔 🎲 🗸 Trusted sites Protected Mode: Off

Select OK

Ssg5-v92:Juniper-Screen05 6	3.0r4.0 - V	Vindows Internet Expl	rer									_	
G C + Attp://10.20.10.2	12/hswebui J	html				_ ⊇	** ×	P Bing					۰ م
👷 Favorites 🛛 🙀 🏠 ssg5-v92Ju	niper-Screen	nOS 🩋 Microsoft Act	ive Directory C										
ssg5-v92:Juniper-ScreenOS 6.3.0	r4.0						Č	• 5	· 🖻 🖶 •	Page • Saf	ety •	Tools •	
	Policy	y > Policies (From	All zones To All zone	:5)						ssg5-v	92		2
	List	20 💌 per page									5	Search	
N luniner'	From	All zones 💌				To All zones •	Go					Nev	v
2 NETWORKS												_	_
	Fro	m Trust To Untrust	, total policy: 5										
	ID	Source	Destination	Service	Action	Options		Config	jure	Enable	Мо	ve	
Configuration	12	Trusted Access	Dial-Up VPN	ANY	42	III.	Edit	Clone	Remove	F	φ		
Binding	з	Any	Dial-Up VPN	ANY	48	III Zo	Edit	Clone	Remove	R	¢		
Zones	1	Any	Any	ANY	Ø		Edit	<u>Clone</u>	Remove	9	Φ		
List	8	192.168.66.10	Dial-Up VPN	ANY	42 0		Edit	Clone	Remove	9	Φ		
- Backup - DHCP	10	192.168.66.11	Dial-Up VPN	ANY	42		Edit	Clone	Remove	9	0	+	
 802.1X Reution 	Fro	m Untrust To Trust	, total policy: 5										
PPP	ID	Source	Destination	Service	Action	Options		Config	jure	Enable	Мо	ve	
- DSCP - Security	11	Dial-Up VPN	Trusted Access	ANY	42		Edit	Clone	Remove	9	\$		
 Policy Policies 	2	Dial-Up VPN	Any	ANY	4	<u>R R</u> »	Edit	Clone	Remove	5	φ		
MCast Policies	4	Any	Any	ANY	9		Edit	<u>Clone</u>	Remove	F	٥		
Addresses	7	Dial-Up VPN	192.168.66.10	ANY	48 0		Edit	<u>Clone</u>	Remove	F	\$		
Groups	9	Dial-Up VPN	192.168.66.11	ANY	48 0	E	Edit	Clone	Remove	9	\$		
Senices Schedules Schedules Traffic Shaping Oraup Expression: DiP VPIs Autokey IKE Autokey Kem Autokey Advanced Gateway P1 Proposal P2 Proposal P2 Proposal VAuth Settings VPD Groups MODECFG Profile													
Done							rusted sit	es Protec	ted Mode: Off	4	a • 13	100%	



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







- 🗆 ×

▼ Group

Cancel

Help

NCP Client with Juniper ScreenOS

4.4. Exchange Mode

Exchange Mode: PFS Group:

aggressive mode none

> Next



Available

JUNIPER

A shared secret or pre-shared key is used to encrypt the connection. This then needs to be identically configured on both sides (VFN client and VFN gateway). Enter the appropriate value for the IKE ID according to the selected ID two

Fully Qualified Usemane

users@juniper.net

Confirm Se

Pre-shared Key Common Secret for Authentication

Pre-shared Ker R Shared Secret:

Local Identity (IKE)

Type:

ĮD:

Group: Show all profil

Profile Name

Add / Import

NCP

•

X

4.5. Pre-shared Key

Shared Secret: Confirm Secret: Local Identity (IKE): ID:

Tunneling123 Tunneling123 Fully Qualified Username users@juniper.net

> Next

4.6. IPsec Configuration: IP Addresses

IP Address Assignment: IKE Config Mode

> Next > OK





5. NCP Client Configuration – Profile changes

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



Select IPsec General Settings: Select Policy Editor

NCP Secure Client - Junip	er Edition 📃 🔳 🗙	Profile		_ _ ×
Connection Configuration Log	View Help	Available Profiles		
Profile:	Connection	Group:		
ScreenOS VPN text1@juniper.r	iet 🗾 🔼	Show all profiles	Group	
		Profile Name		
	JUNIPER	ScreenUS VPN test1@juniper.net		
	and the second second			
	0 0			
	NCO			
Statistics:				
Data (Tx) in Byte: 0				
Data (Rx) in Byte: 0 Speed (KByte/s): 0 000	Timeout (sec): 0 sec Encryption	Add / Import Edit	Copy Delete Expor	t
			Heb OK Can	cel I
				cer
Profile Settings Screen05	VPN test1@juniper.net	×	IPsec Configuration	×
Profile Settings ScreenOS Basic Settings	VPN test1@juniper.net IPsec General Settings	×	IPsec Configuration	×
Profile Settings Screen05 Basic Settings Line Management IPsec General Settings	IPsec General Settings	point):	IPsec Configuration IPsec Configuration IPsec Configuration IP 3T IKE Policy	×
Profile Settings Screen05 Basic Settings Line Management IPsec General Settings Advanced IPsec Options Identifies	VPN test1@juniper.net IPsec General Settings Gateway (Tunnel Endp 10.20.10.211	point):	IPsec Configuration IPsec Configuration 문급 IKE Policy 문 같은 IPsec Policy	×
Profile Settings Screen05 Basic Settings Line Management IPsec General Settings Advanced IPsec Options Idemities IPsec Address Assignment Solt Tureating	VPN test1@juniper.net Psec General Settings	point:	These Configuration Proce Configuration IP of IKE Poleg IP of IKE Poleg IP of IRec Poleg	×
Profile Settings Screen05 Basic Settings Line Management Proce General Sectings Advanced IPsec Diplons Identilies IPsec Address Assignment Split Turneling Certificate Check	VPII test10juniper.net Psec General Settings Gateway (Turnel End) 10.20.10.211 Policies ME Policy:	point):	IPsec Configuration "IPsec Configuration ⊕: 37 IKE Polog ⊞: 37 IPsec Polog	×
Profile Settings Screen05 Baic Settings Line Management Heas General Settings Advanced Prece Datas Identities IPace Address Assignment Spkt Turneling Cettilicate Check	VPR text10juniper.net IPsec General Setting: Gateway (Tunnel End) 10.20.10.211 Policies IKE Policy: a IPsec Policy: a	vlomatic mode v	I Phee Configuration - IPree Configuration 는 국립 VE Retor 표 객실 IPree Policy	×
Profile Settings Screen03 Baic Settings Line Management Heas General Settings Identities IPace Address Assignment Split Turneling Cethlicate Check	VPH test1@juniper.net IPec General Setings Galeway (Turnel End 10.20.10.211 Pokcies JKE Pokcy: a IPgec Pokcy: a Exch. Mode: a		IPsec Configuration IP True Configuration IP True Readon IP True Readon IP True Readon IP True Readon	×
Profile Settings Second Baic Settings Line Mengement References Second References Second Pace Address Assignment Self Turneling Cettlicate Check	VPH text3 Opunger.net IPsec General Settings IPsec General Settings IPsec General Settings ISE Policy: IPsec Policy: Exch. Mode: PS Group: PS Group: ISE Policy: ISE Policy:	vicrostic mode v ucrostic mode v ggerestive mode (IKEV1) v	These Configuration Rhese Configuration 대 작품 (Place Policy) 대 작품 (Place Policy)	×
Profile Settings Second Baic Settings Line Management Pade General Settings Identifies Set Turnering Cettificate Check	VPH text3 Opunger.net IPsec General Settings IPsec General Settings Internet Settings	vicrosic mode v ucrosic mode v ucrosic mode v ggessive mode (IC2v1) v ore v Policy Literios Policy Literios	Prec Configuration Prec Configuration Prec Configuration 中のでの時代の 日本 日本 日本 Prec Parks 日本 Prec Parks 日本 Prec Configuration	×
Politi Settings ScreenDP Basic Settings Ter Managada Advanced Plese Option Advanced Plese Option Identities Place Address Assignment Spil Turnitig Centicum Overk	VPII Lest 10 geneparatet IP-see General Setings file aleway (Turnel End 10.20.10.211 Policies IP-gen Policy IP-gen Policy Besch Mode B*S Group	adomatic mode adomatic mode adomatic mode adomatic mode adomatic mode adomatic mode adomatic mode adomatic mode adomatic mode adomatic mode adomatic mode adomatic mode adomatic mode ad	[Phet Configuration Phet Configuration 는 것 [Phet Parks] 요. 맛 [Phet Parky	X
Profile Settings Concerds Ease Safety In the Management Protocomment Protocomment Protocomment Set Turneling Casticate Data	VPU Letd U gungerand IPec Germal Settings Galeway (Turnel End 10.21.10.21) Pokos IFE Pokoy IFE Pokoy Exch. Mode BS Group I	voint) utenatie mode v utenatie mode v utenatie mode v utenatie mode v v gerestier mode ((EV1) v Policy Lifetimes – Policy Editor –	Preconguistion IPreconguistion IPreconguistion	Deter
Profile Settings Concerds Basic Advision Basic Advisor Professional Press Dytons Identification Basic Advisor Split Turneling Centicate Check	VPT Let 19 junper net Prec General Setings functional Setings george galeway (Turnel End 10.20.10.211 Policis JE Policy Inger Policy Des General Each Mode	Z udrović mode – 2 udrović mode – 2 udrović mode – 2 udrović mode – 2 Paky Letner – Paky Edvr. –	Preconguistion Add Eff Copy	Direce

Select IKE Policy – Add

Enter the following parameters and select OK:Name: PSK-AES-SHA-DH2Authentication:Pre-shared KeyEncryption:AES 128 BitHash:SHADH-Group:DH-Group 2 (1024 Bit)

Select IPsec Policy – Add

© NCP engineering • info@ncp-e.com • www.ncp-e.c Page 20 of





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 Spit 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.

		1 minut	
NCP Secure Client - Junipe			Profile
Connection Configuration Log	view nep		Available Profiles
Frohie:	a 18	Lonnection	Group:
Screenus VPN rest (@juniper.n	et _		Show all profiles Group
			Profile Name
		JUNIPEC	ScreenDS VPN test1@juniper.net
- A		and the second s	
	00	- Education	
U V		NCO	
Statistics: Data (Tx) in Byte: 0		e: 00:00:00	
Data (Rx) in Byte: 0		ec): 0 sec	Add / Import Edit Copy Delete Export
Speed (KByte/s): 0.000		N	
			Help DK Cancel
Profile Settings ScreenOS	VPN test1	@juniper.net	×
Basic Settings	Split Tunn	ieing	
IPsec General Settings	Enter the	remote IP networks the prefind will always be us	tunnel should be used for. Without
Advanced IPsec Uptions Identities	011100 10		1994.
IPsec Address Assignment Solt Turneling		Remote Naturatio	Demote IP Net Marke
Certificate Check	3	192.168.66.0	255.255.255.0
		Add	Edit Delote
		Add	Edit Delete
		Add Full Local Network B	Edt Delete
		Add Ful Local Network 6	Edit Delete

Select OK and close all the windows.

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



🚾 C:\Windows\system32\cmd.exe	C:\Windows\system32\cmd.exe	
C:\NCP> C:\NCP}ipconfig ∕all	C:\NCP>netstat -rn Interface List	
Vindows IP Configuration	1502 00 4e 43 50 49NCP Secure Client Ortical NDISS Hdapter 1100 0c 29 8b cb 54Intel(R) PRO/1000 MT Network Connection Software Loophack Interface 1	
Host Name : demo-PC Primary Dns Suffix : Node Type : Hybrid IP Routing Enabled : No WINS Proxy Enabled : No	1200 00 00 00 00 00 00 00 00 00 00 00 0	
Ethernet adapter Local Area Connection 2:	Active Routes: Network Destination Netmask Gateway Interface Metr 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	ic
Hedia State	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	66 66 86 86 86 86 86 86 86 86 86 86 86 8
Connection-specific DNS Suffix .: Description: Intel(R) PRO/1000 MT Network Connection Physical Address: 90-8C-29-8B-CB-54 DHCF Enabled: No Autoconfiguration Enabled: Yes	Persistent Routes: Network Address Netrask Gateway Address Metric 6.8.6.0 3.6.6.0 18.20.30.3 Default	==
IPv4 Address. : 10.20.10.111(Preferred) Subnet Mask : 255.255.0.0 Default Gateway : 10.20.30.3 DNS Servers : 60.94.156.1 NetBIOS over Tepip. : EnAled	Active Routes: If Petrik Mercych Bestination Gateway If James Grading Gateway 1 3306 ff00:://8 Persistent Routes:	

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:\Windows\system32\cmd.exe
C:\NCP>ipconfig /all	C:\NCP>netstat -rn
Windows IP Configuration	Interface List 1582 00 4e 43 50 49NCP Secure Client Virtual NDIS6 Adapter 11 00 6e 29 0b 54
Host Name	11.00 00 27 09 05 91
Ethernet adapter Local Area Connection 2:	IPv4 Route Table
Connection-specific DNS Suffix : Description	Action Netnask Gateway Interface Metric 0:0.0.0 0:0.0.0 172.16.100.100 23 10:0.0.10 0:0.0.0 172.16.100.100 23 10:0.0.10 0:0.0.0 0:0.0.0 172.16.100.100 23 10:0.20.25.255.255.255.255.255.255.255.255 0.0.110.10.111 266 26 26.10.111 266 10:20.255.255.255.255.255.255.255 0.0.110.10.111 266 26 27.10.111 266 10:20.257.257.265.255.255.255 0.0.110.10.111 266 26 27.10.0.1 266 127.215.100.0 255.255.255.255 0.0.110.111 266 27.10.0.1 306 127.216.100.0 255.255.255.0 0.0.110.111 266 257 257 172.16.100.0 255.255.255.0 0.0.110.111 27.100.100 257 257 172.16.100.0 255.255.255 0.0.110.111 127.100.100 257 172.16.100.100.255 255.255.255 0.0.110.111 127.100.100 257 127.16.100.100.255 255.255.255
DNS Servers	Persistent Routes: Network Address Netmask Gateway Address Metric 0.0.0.0 0.0.0.0 10.20.30.3 Default
NetBlus over Icpip Enabled	IPv6 Route Table
Ethernet adapter Local Area Connection: Connection-specific DNS Suffix .: Description Intel(B) PRO/1000 HT Network Connection Physical Address Ho Physical Address Ho Nutro Emailed Ho Auto Emailed	Active Reutes: Gitway If Hetric Network Destination Gitway 15 276 fe88::/64 0 0 1 206 ff88::/6 0 1.016 15 276 ff88::/8 0 0 1.016 0 1 0 0.010 1.016 1 0 0.010 0 1.016 0 1.016 0 1.016 0 1.016 0 1.016 0 1.016 0 1.016 0 1.016 0 1.016 0 1.016 0 1.016 0 1.016 0 1.016 0 1.01
NetBIOS over Icpip Enabled	C:\NCP>_

Verify a connection to the web server.

NCP Secure Client - Juniper Edition	🖉 1157 - Windows Internet Explorer	- 🗆 🗵
Connection Configuration Log View Help	🕞 🕞 🖉 http://192.168.66.10/	P -
Profile: Connection	As Fauntites the All Summerted Stars - All Web Size Collegy -	
ScreenOS VPN test1@juniper.net	Contraction of the subgrasted sites . Contract date in the same date is a contract of the sa	
Connection extablished.	₩ Welkommen Bienvenue W Welkommen Benvenuto Welkom Wakommen Hoş Geldiniz Hoş Geldiniz Mage Kakûç opiarate Adopo nowanobate	
	Done	🔍 100% 🔹 🎵



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 255.255.255/32.
- > 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"

ssg5-v92: Juniper-ScreenOS 6.3.0	0r4.0	1	<u>م</u>	• 🗅 • 🖃 🖶	• Page •	Safety • Tools •	• 🔞 •
Objects > IP Pools \$595-v92							
						Ner	w
	Name	Start IP	End IP	In use	Co	onfigure	
Manual Key	VPN Pool	172.16.100.100	172.16.100.200	1	-	-	
Monitor Status	AD Pool	172.16.66.1	172.16.66.254	0	Edit	<u>Remove</u>	
Objects	Remote	172.16.123.101	172.16.123.111	1	-	-	
Users IP Pools Certificates Reports System Log Event							

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

ssg5-v92: Juniper-ScreenOS 6.3.0r4.0		🏠 🔹 🔂 👻 🖃 🖶 🔹 Page 🔹 Safety 🔹 Tools 🔹 🔞	
Objects > Us	ers > Local > Edit	ssg5-v92 ?	
SSG5-492	Aut	th/IKE/XAuth/L2TP User	-
List Us	er Name rainer	Groups: Proxy	l
Summary Sta	atus 📀 Enable	C Disable	l
Services Schodulas Control Co	IKE User ^c Simple Identity IKE ID Type FODN v ^c Use Distinguished Name I	Number of Multiple Logins with Same ID 10 IKE Identity vpn.net	
L2TP Manitas Status	uthentication User		l
Objects Users L2	Auth User 2TP User		
Local Groups L2	TP/XAuth Remote Settings	(Remote IP: 0.0.0.0)	
- External Groups	IP Pool Remote 💌	Static IP 0.0.0.0	
Certificates	Primary DNS IP 0.0.0.0	Primary WINS IP 0.0.0.0	
Reports S Wizards	econdary DNS IP 0.0.0.0	Secondary WINS IP 0.0.0.0	
• Help			-1
Done		OK Concel	1

ssg5-v92:Juniper-ScreenOS 6.3.0r4.	0		👌 • 🗟 •	🗈 🌐 👻 Page	e ▼ Safety ▼ To	iols + 🔞 +
	Objects > Users > Local Group	5			ssg5-v92	?
Juniper [®]	List 20 💌 per page					New
SSG5-v92	Group Name	Group type	Members	Co	onfigure	
Groups	Office Proxy	ike xauth ike xauth	NCP Users rainer	Edit Edit		_
Services	Test	auth ike	aduser	Edit	Remove	
- Schedules	Test2	ike xauth	certuser	Edit	Remove	
Group Expression DIP AutoKey IKE AutoKey KKE AutoKey Advanced Manual Key LZTP Monitor Status Objects Users Local Local External Groups DIP						



NCP Client with Juniper ScreenOS

Next create a new Gateway configuration "VPN Access"

	4.0 🏠 🕈 🖾 👘 🔻 Page 🕶 Safety 🕶 Tools 🛪 🔞 🖛
	VPNs > AutoKey Advanced > Gateway > Edit ssg5-v92 ?
Juniper	
SSG5-v92	Gateway Name VPN Access
Homo	Version 📀 IKEv1 😳 IKEv2
+ Configuration	
+ Network	• Remote Gateway
Security	C Chakie TD Address / Upstrams
- Policies	
- MCast Policies	O Dynamic IP Address Peer ID
Policy Elements	O Dialup User User None 💌
 Addresses 	Dialup User Group Group Group Group
- Groups	C ACVPN-Dynamic
Summary	
+ Services	Local ID [LoisunguishedName]
- Traffic Shaping	C ACVPN-Profile
- Group Expression	
	OK Cancel Advanced
- AutoKev IKE	
- AutoKey Advanced	
- Gateway	
- P1 Proposal	
_	
ssg5-v92:Juniper-ScreenOS 6.3.0r4	4.0 👌 🕆 🔂 🗸 🖃 🖶 🖓 Age + Safety + Tools + 🔞 +
ssg5-v92:Juniper-ScreenOS 6.3.0r4	4.0 In the second seco
ssg5-v92:Juniper-ScreenOS 6.3.0r4	4.0 👘 • Rage • Safety • Tools • @ • VPNs > AutoKey Advanced > Gateway > Edit ssg5-v92 ?
ssg5-v92:Juniper-ScreenOS 6.3.0r4	4.0 👘 ▼ 🖻 🖷 ▼ Page ▼ Safety ▼ Tools ▼ 🖗 ▼ VPNs > AutoKey Advanced > Gateway > Edit ssg5-v92 了
ssg5-v92:Juniper-ScreenOS 6.3.0r4	4.0 to key Advanced > Gateway > Edit ssg5-v92 ?
ssg5-v92:Juniper-ScreenOS 6.3.0r4	4.0 In Page + Safety + Tools + () + VPNs > AutoKey Advanced > Gateway > Edit SSg5-V92 ?
ssg5-v92:Juniper-ScreenOS 6.3.0r4	4.0 In Page + Safety + Tools + O+ VPNs > AutoKey Advanced > Gateway > Edit Ssg5-V92 ?
sg5-v92:Juniper-ScreenOS 6.3.0r4	4.0 In Page + Safety + Tools + O + VPNs > AutoKey Advanced > Gateway > Edit Ssg5-V92 ? IKEv2 Auth Method Self None *
sg5-v92:Juniper-ScreenOS 6.3.0r4	4.0 Image - Safety - Tools - @+ VPNs > AutoKey Advanced > Gateway > Edit S5g5-v92 2 IKEv2 Auth Method Self None ▼ Peer None ▼
ssg5-v92:Junper-ScreenOS 6.3.0r4	4.0 Image: Safety - Tools - @+ VPNs > AutoKey Advanced > Gateway > Edit Ssg5-v92 ? IKEv2 Auth Method Self None ▼ Peer None ▼ Preshared Key
ssg5-v92:Junper-ScreenOS 6.3.0r4	4.0 Image: Safety - Tools - Original - Tools -
Seg5-v92:Juniper-ScreenOS 6.3.0r4	4.0 Image: Page: Safety - Tools · @ + VPNs > AutoKey Advanced > Gateway > Edit Ssg5-v92 ? IKEv2 Auth Method Self None ▼ Peer None ▼ Preshared Key •••••••••••••••••••••••••••••••••••
Seg5-v92:Junper-ScreenOS 6.3.0r4	4.0 Image: Page + Safety + Tools + @+ VPNs > AutoKey Advanced > Gateway > Edit Ssg5-v92 ? IKEv2 Auth Method Self None ▼ Peer None ▼ Preshared Key •••••••••••••••••••••••••••••••••••
sg5-v92:Junper-ScreenOS 6.3.0r4 SSG5-v92 Home Configuration Network Security Policies Policy Policies Policy Elements Addresses	4.0 Image: Page: Safety + Tools + Image: VPNs > AutoKey Advanced > Gateway > Edit VPNs > AutoKey Advanced > Gateway > Edit Ssg5-v92 IMEv2 Auth Method Self None ▼ Peer None ▼ Peer None ▼ Preshared Key••••••••••••••••••••••••••••••••••••
sg5-v92:Juniper-ScreenOS 6.3.0r4 Signature ScreenOS 6.3.0r4 Signature ScreenOS 6.3.0r4 Security Policy Policy Policies MCast Policies Policy Elements Addresses List Groups	4.0 Image: Safety + Tools + Image: Safety + Ima
Seg5-v92:Juniper-ScreenOS 6.3.0r4	4.0 Image: Safety = Tools + Ima
Seg5-v92:Junper-ScreenOS 6.3.0r4	4.0 Image: Page: Safety - Tools - Image: Page: Pa
seg5-v92:Junper-ScreenOS 6.3.0r4 Seg5-v92 Home Configuration Network Security Policies MCast Policies Addresses List Groups Summary Services Schedules Taffic Sharing	4.0 Image: Safety + Tools + Image: Safety + Tools + Image: Safety + Tools + Image: Page: Safety + Image: Page: Safety + Image: Page:
seg5-v92:Junper-ScreenOS 6.3.0r4 Seg5-v92 Home Configuration Network Security Policy Policy Policy Policy Elements Addresses List Groups Summary Services Schedules Traffic Shaping Group Expression;	4.0 Image: Page: Safety - Tools - Image: Page: Pa
seg5-v92:Junper-ScreenOS 6.3.0r4 Security Policy Security Sec	4.0 Image: Page: Safety + Tools + Image: VPNs > AutoKey Advanced > Gateway > Edit VPNs > AutoKey Advanced > Gateway > Edit ssg5-v92 Image: Interface interface Image:
sey5-v92:Juniper-ScreenOS 6.3.0r4 SSC5-v92 Home Configuration Network Security Policies Policy Policies Oricipe Elements Addresses List Groups Summary Services Schedules Traffic Shaping Group Expression: DIP VNs AutoKey INFE	4.0 Image: Safety + Tools + Q+ VPNs > AutoKey Advanced > Gateway > Edit \$\$sg5-v92 Image: Intervention of the second s
sg5-v92:Junper-ScreenOS 6.3.0r4 Sco5-v92 Home Configuration Network Security Policy Policy Policies Addresses List Groups Summary Services Schedules Traffic Shaping Group Expression: DIP VPNs AutoKey IKE AutoKey Advanced	4.0 Image: Safety + Tools + Ø+ VPNs > AutoKey Advanced > Gateway > Edit \$
seg5-v92: Juniper-ScreenOS 6.3.0r4 ScreenOS 6.3.0r4 ScreenOS 6.3.0r4 Home Configuration Network Security Policy Policies MCast Policies Policy Elements Policy Elements Policy Elements Addresses List Groups Summary Services Schedules Traffic Shaping Group Expression: DIP VPNs AutoKey IKE AutoKey IKE AutoKey IKE	4.0 Image: Safety - Tools - Ima
seg5-v92:Junper-ScreenOS 6.3.0r4 Seg5-v92: Home Configuration Network Policy Policies MCast Policies Policy Elements Addresses List Groups Summary Services Schedules Trafic Shaping Group Expression: DIP VPNs AutoKey IKE AutoKey KK AutoKey Advanced Gateway P1 Proposal P2 P2 Proposal P2	4.0 Image: Safety = Tools • Image: Safety = Tools • Image: VPNs > AutoKey Advanced > Gateway > Edit VPNs > AutoKey Advanced > Gateway > Edit Ssg5-v92 Image: Im

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.



NCP Client with Juniper ScreenOS

ssg5-v92: Juniper-ScreenOS 6.3.0r4.0			🚹 • 🔝 - 🖃 e	🌧 🔹 Page 🔹 Safety 👻 Tools 👻 🔞 👻
Netwo	ork > Interfaces > Edit			ssg5-v92 🛜
Inter	face: tunnel.2 (IP/Netmask	: 0.0.0.0/0)		Back To Interface List
Prope	erties: Basic Proxy ARP M	TTP DTP VTP TGMP N	IHTB Tunnel IRDP	
	Turnel Interfere News	human 2		-
SSG5-v92	runnel Interface Name	tunnel.z		
- Home	Zone (VR)	Untrust (trust-vr)		
Configuration				
Network C F	ixed IP			
+ DNS	IP Address / Netmask			
Zones				
Interfaces	Innumbered			
- List	Interface	ethernet0/0 (trust-vr) 💌		
- DHCP		,		
Routing Ma	ximum Transfer Unit(MTU)	Admin MTU 0 Byt	es (Operating MTU: 150	0; Default MTU: 1500)
Destination				
- Source Interface	DNS Proxy			
MCast Routing				
	Teeffie Deuduidth			
Virtual Routers	Tranic Bandwidth	Egress Maximum B	andwidth ju Kbps	•
DSCP		Guaranteed E	Bandwidth 0 Kbps	3
+ Security		Ingress Maximum P	andwidth 0 Khos	
Policy		Maximum B	Kups	
Policies MCast Policies		_		
	NHRP Enable			<u>•</u>

	ssg5-v92: Juniper-ScreenOS	6.3.	0r4.0					ć	• • •		• Page • Safety • To	ools + 🔞 +
ſ			Ne	work > Zones							ssg5-v92	?
1												New
	SSG5-v92		I	D Name	Virtual Router	Vsys	Default IF	Туре	Attribute		Configure	
	Homo) Null	untrust-vr	Root	serial0/0	Null	Shared			
Ľ	Configuration		. :	2 Trust	trust-vr	Root	bgroup0	Security(L3)		Edit	Screen, Mai-URL	
R	Network			l Untrust	trust-vr	Root	ethernet0/0	Security(L3)	Shared	Edit	Screen, Mal-URL	
I	Binding DNS			l Self	trust-vr	Root	self	Function				-
I	Zones		1	0 Global	trust-vr	Root	null	Security(L3)				-
I	 Interfaces List 			і НА	trust-vr	Root	null	Function				<u> </u>
ł	Backup			6 MGT	trust-vr	Root	null	Function		Edit	Screen, Mal-URL	<u> </u>
	- DHCP	۲	1	6 Untrust-Tun	trust-vr	Root	hidden.1	Tunnel				-
1	E Routing		1	5 V1-Null	trust-vr	Root	l2v	Security(L2)	Shared	Edit	Screen, Mal-URL	-
I	- Destination		1	2 V1-Trust	trust-vr	Root	v1-trust	Security(L2)	Shared	Edit	Screen, Mai-URL	
J	- Source Interface		1	1 V1-Untrust	trust-vr	Root	v1-untrust	Security(L2)	Shared	Edit	Screen, Mal-URL	
1	- MCast Routing			DMZ	trust-vr	Root	ethernet0/1	Security(L3)		Edit	Screen, Mal-URL	
I	Virtual Routers		1	3 V1-DMZ	trust-vr	Root	v1-dmz	Security(L2)	Shared	Edit	Screen, Mal-URL	
I	PPP		1	4 VLAN	trust-vr	Root	vlan1	Function(vlan)	Shared	Edit		
	DSCP Security Policy Policies MCast Policies	•					-	*				

ssg5-v92: Juniper-ScreenOS 6.3.0	Ir4.0				6 · 🔊	- 🗆 🖶	• Page •	Safety • Tool
	Network > Interfaces (Lis	it)					s	sg5-v92
	List 20 vper page List ALL(13) Inter	faces					New	Tunnel IF
	Name	IP/Netmask	Zone	Туре	Link	PPPoE	Co	onfigure
Home	bgroup0	192.168.66.2/24	Trust	Layer3	Up	-	Edit	
Configuration	ethernet0/4				Up	-	Edit	
Network	ethernet0/5				Up	-	Edit	
DNS	ethernet0/6				Up	-	Edit	
Zones	bgroup1	0.0.0/0	Null	Unused	Down	-	Edit	
List	bgroup2	0.0.0/0	Null	Unused	Down	-	Edit	
Backup	bgroup3	0.0.0/0	Null	Unused	Down	-	Edit	
- DHCP	ethernet0/0	10.20.10.211/16	Untrust	Layer3	Up	-	Edit	
- Routing	ethernet0/1	0.0.0/0	DMZ	Layer3	Down	-	Edit	
- Destination	ethernet0/2	0.0.0/0	Null	Unused	Down	-	Edit	
- Source Interface	ethernet0/3	192.168.100.1/24	Trust	Layer3	Down	-	Edit	
- MCast Routing	serial0/0	0.0.0/0	Null	Unused	Up	-	Edit	
Virtual Routers	tunnel.1	unnumbered	Untrust	Tunnel	Ready	-	Edit	
PPP	tunnel.2	unnumbered	Untrust	Tunnel	Ready	-	Edit	
- Security	tunnel.3	unnumbered	Trust	Tunnel	Down	-	Edit	Remove
Policy	vlan1	0.0.0/0	VLAN	Laver3	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"

ssg5-v92:Juniper-ScreenOS 6.3	.0r4.0	🏠 🔹 🔂 👻 🖃 👘 🔹 Page 🔹 Safety 🔹 Tools 🔹 🔞 🔹
	VPNs > AutoKey IKE	E > Edit ssg5-v92 ?
		<u> </u>
(
Juniper		
NETWORKS		
	VPN Name	VPN Access Tunnel
5565-V92		
- Home	Remote Gatewa	VPN Access
Configuration		C Create a Simple Gateway
Network		
 Security 		Gateway Name
Policy		Version 💿 IKEv1 🔍 IKEv2
- Policies		Type 🤄 Static IP Address/Hostname
- Policy Elements		
- Addresses		O Dynamic IP Peer ID
List		🔿 Dialup User 🛛 User None 💌
- Groups		C Dialup Group Group None 🔽
Summary		
Services		(optional)
- Schedules		Preshared Key Use As Seed
Group Expression		Security Level Standard Compatible Sasic
DIP		
- VPNs		
- AutoKey IKE	ACVPN-Dynamic	Gateway None Tunnel Towards Hub None
- AutoKey Advanced	ACVPN-Profile	Binding to Tunnel None 🚬
- Gateway		
- P1 Proposal		OK Cancel Advanced
- P2 Proposal		
Auth Settings		(
	2 0:4 0	💧 y 🖸 y 🔤 🖨 y Pane y Safety y Tools y 🙆
ssg5-v92: Juniper-ScreenOS 6.	3.0r4.0	h v 🖸 v 🖂 🚓 v Page v Safety v Tools v 🔞
ssg5-v92:Juniper-ScreenOS 6.	3.0r4.0 VPNs > AutoKey IK	te > Edit ssg5-v92 ?
ssg5-v92: Juniper-ScreenOS 6.	3.0r4.0 VPNs > AutoKey IK	te > Edit ssg5-v92 ?
ssg5-v92:Juniper-ScreenOS 6.	3.0r4.0 VPNs > AutoKey IK	te > Edit Page + Safety + Tools + @ Ssg5-v92 ?
ssg5-v92:Juniper-ScreenOS 6.	3.0r4.0 VPNs > AutoKey IK	te > Edit ssg5-v92 ?
ssg5-v92:Juniper-ScreenOS 6.	3.0r4.0 VPNs > AutoKey IK	te > Edit ssg5-v92 ?
SSG5-v92:Juniper-ScreenOS 6.1	3.0r4.0 VPNs > AutoKey IK Security Level	te > Edit ssg5-v92 ?
SSG5-v92:Juniper-ScreenOS 6.1	3.0r4.0 VPNs > AutoKey IK Security Level Predefined	CE > Edit Safety - Tools - @ CE > Edit Ssg5-v92 2 CE Standard C Compatible C Basic
SIG5-v92:Juniper-ScreenOS 6.1	3.074.0 VPNs > AutoKey IK Security Level Predefined User Defined	CE > Edit • Page • Safety • Tools • @ CE > Edit • ssg5-v92 ? • Standard • Compatible • Basic • Custom
SSG5-v92:Junper-ScreenOS 6.	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined	CE > Edit • Page • Safety • Tools • @ CE > Edit • • • • • • • • • • • • • • • • • • •
Ssg5-v92:Juniper-ScreenOS 6.1	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined	C > Edit • Page • Safety • Tools • @ CE > Edit • ssg5-v92 ? C Standard C Compatible C Basic • Custom Phase 2 Proposal nopfs-esp-aes128-sha V None V None
Ssg5-v92:Junper-ScreenOS 6.	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined	Image: Safety - Tools - Image: Safety -
Seg5-v92:Juniper-ScreenOS 6.	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined Replay Protection	Image: Standard Compatible Basic Image: Custom Custom Phase 2 Proposal Impfs-esp-aes128-sha Image: None Image: None
SSG5-v92:Juniper-ScreenOS 6.1	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined Replay Protection Transport Mode	Ce > Edit • Page • Safety • Tools • @ Ce > Edit • ssg5-v92 ? Ce > Standard • Compatible • Basic • Custom Phase 2 Proposal Inopfs-esp-aes128-sha • None • None V
Seg5-v92:Junper-ScreenOS 6.1	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined Replay Protection Transport Mode	CE > Edit • Page • Safety • Tools • @ CE > Edit • ssg5-v92 ? CE > Standard • Compatible • Basic • Custom Phase 2 Proposal nopfs-esp-aes128-sha • None • None V
Seg5-v92:Junper-ScreenOS 6.1	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined Replay Protection Transport Mode Bind to	CE > Edit Ssafety - Tools - @ CE > Edit Ssg5-v92 ? CE > Standard C Compatible C Basic C Custom Phase 2 Proposal nopfs-esp-aes128-sha V None None None None None
Seg5-v92:Juniper-ScreenOS 6.	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined Replay Protection Transport Mode Bind to	Image: Solution of the sector of the sect
Seg5-v92:Juniper-ScreenOS 6.	3.074.0 VPNs > AutoKey IK Security Level Predefined User Defined Replay Protection Transport Mode Bind to	Image: Second
Sigs-v92:Juniper-ScreenOS 6.	3.074.0 VPNs > AutoKey IK Security Level Predefined User Defined Replay Protection Transport Mode Bind to	Standard Compatible Phase 2 Proposal nopfs-esp-aes128-sha None None None Image: Standard Compatible Standard None Image: Standard Compatible Standard Compatible Standard Compatible Pase None Image: Standard Compatible
Seg5-v92:Juniper-ScreenOS 6.	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined Replay Protection Transport Mode Bind to Proxy-ID Check	Standard Compatible Basic Custom Custom Phase 2 Proposal nopfs-esp-aes128-sha None None None Tunnel Interface Untrust Tun
Seg5-v92:Junper-ScreenOS 6.1	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined Replay Protection Transport Mode Bind to Proxy-ID Check	Image: Standard Compatible C Basic Image: Standard Compatible C Basic Image: Custom Custom Phase 2 Proposal Image: None Image: None Image: None Image: None Image: None Image: Custom Image: None Image: None Image: Custo
Seg5-v92: Juniper-ScreenOS 6. Signature Signature Configuration Configuration Security Policies MCast Policies Policy Elements Addresses List Groups Summary Services Schedules Traffic Shaping Group Expression	3.074.0 VPNs > AutoKey IK Security Level Predefined User Defined User Defined Replay Protection Transport Mode Bind to Proxy-ID Check DSCP Marking	Image: Solution of the second sec
Seg5-v92:Juniper-ScreenOS 6.	3.074.0 VPNs > AutoKey IK Security Level Predefined User Defined User Defined Bind to Proxy-ID Check DSCP Marking	Standard Compatible Standard Compatible Standard Compatible Standard Compatible Standard Compatible Standard Compatible Phase 2 Proposal nopfs-esp-aes128-sha None None None None Image: Standard Compatible Standard None None Image: Standard Compatible None None Image: Standard Compatible Image: Standard Compatib
Seg5-v92:Junper-ScreenOS 6.	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined Replay Protection Transport Mode Bind to Proxy-ID Check DSCP Marking	Standard Compatible Compatible Basic Custom Custom Phase 2 Proposal nopfs-esp-aes128-shar None Disable Enable
Seg5-v92:Junper-ScreenOS 6.3 Screener	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined Replay Protection Transport Mode Bind to Proxy-ID Check DSCP Marking VPN Group	C > Edit Standard Compatible Custom Phase 2 Proposal nopfs-esp-aes128-sha None None None Tunnel Interface Tunnel Zone Disable Enable Dscp Value None Weight
Seg5-v92: Juniper-ScreenOS 6. SG5-v92 Home Configuration Network Security Policies MCast Policies Policy Elements Addresses List Groups Summary Services Schedules Traffic Shaping Group Expression: DIP VPNs AutoKey IKE AutoKey IKE AutoKey Advanced	3.0r4.0 VPNs > AutoKey IK Security Level Predefined User Defined User Defined Bind to Proxy-ID Check DSCP Marking VPN Group	C > Edit ssg5-v92 C > Edit ssg5-v92 C Standard Compatible Phase 2 Proposal nopfs-esp-aes128-sha None None None Tunnel Interface Tunnel Z O Disable Enable Dscp Value None Veight
Seg5-v92: Juniper-ScreenOS 6. Signature Configuration Configuration Security Policy Policies Policy Elements Addresses List Groups Summary Services Schedules Traffic Shaping Group Expression DIP VPNs AutoKey IKE AutoKey Advanced Gateway	3.074.0 VPNs > AutoKey IK Security Level Predefined User Defined User Defined Bind to Proxy-ID Check DSCP Marking VPN Group VPN Monitor	C > Edit ssg5-v92 C Standard Compatible Custom Phase 2 Proposal nopfs-esp-aes128-sha None None None C None Tunnel Interface Tunnel Zone C Disable E Enable Disable E Enable None Weight
Seg5-v92:Junper-ScreenOS 6.1	3.074.0 VPNs > AutoKey IK Security Level Predefined User Defined User Defined Bind to Proxy-ID Check DSCP Marking VPN Group VPN Monitor Source Interface	C > Edit ssg5-v92 C Standard Compatible C Standard Compatible C Custom Phase 2 Proposal nopfs-esp-aes128-shar None None None C None C Tunnel Interface Tunnel Zone C Disable C Enable D Dscp Value O None Weight
Seg5-v92:Junper-ScreenOS 6.	3.074.0 VPNs > AutoKey IK Security Level Predefined User Defined User Defined Bind to Proxy-ID Check DSCP Marking VPN Group VPN Monitor Source Interface Destination IP	Standard Compatible Costandard Compatible Custom Phase 2 Proposal nopfs-esp-aes128-sha None None None V default

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 · / ·

1.	1				
ssg5-v92: Juniper-ScreenOS 6.3.	0r4.0		🏠 • 🔝 - 🖃 e	🚽 🔹 Page 🔹 Safety 🕶 1	Fools + 🔞 +
	Policy > Policy Elements >	Addresses > List		ssg5-v92	?
	List 20 💌 per page				
Juniper	Trust 💌 Filter: ALL	0-9 A B C D E F G-I J-L M N O P Q I	<u>R S T U V W X-Z</u>		New
NETWORKS					
SSG5-v92	Name	IP/Domain Name	Comment	Configure	
Routing	172.16.66.0/24	a 172.16.66.0 /24		Edit Remove	
- Destination - Source	172.16.66.100/32			Edit Remove	
- Source Interface	Any	a.0.0.0 /0	All Addr	In Use	
	Dial-Up VPN		Dial-Up VPN Addr		
Virtual Routers	Remote Zone 10	10.50.50.0 /24		Edit In Use	
DSCP	Trusted Access	a 192.168.66.0 /24		Edit In Use	
+ Security					
- Policies					
 MCast Policies Policy Elements 					
Addresses					
- List					
- Groups					
Services					
 Schedules 					
- Traffic Shaping					
- Group Expression:					
- VPNs					

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.

ssg5-v92:Juniper-ScreenOS 6.3.0r4.0		👌 • 🔊 -	- 🖶 • F	Page 🔹 Safety 🔹 Tools 🔹 🔞 🗸
VPN > A	lutoKey > Proxy ID			ssg5-v92 🛛 ?
Juniper				
SSG5.v92	VPN Name	VPN Access Tunnel		
Security Policy Policy Policy Policy Policy Policy Elements Addresses List Groups Summary Services Schedules Traffic Shaping	C Local IP II Local & Local Address Zor C Remote IP IP Remote & Remote Address Zon Service Address	P: Untrust v Address: 10.20.10.111 v e: Untrust v Address: 10.20.10.111 v e: Untrust v Address: 10.20.10.111 v]	
Group Expression:		New Cancel		
- VPNs	Local	Remote	Service	Configure
AutoKey IKE AutoKey Advanced Gateway	Zone: Trust Address:Trusted Access	Zone: Untrust Address:Dial-Up VPN	ANY	<u>Remove</u>
– P1 Proposal – P2 Proposal	Zone: Trust Address:Remote Zone 10	Zone: Untrust Address:Dial-Up VPN	ANY	<u>Remove</u>
Auth Settings VPN Groups MoDECFG Profile Manual Key T=1 2TP ✓				
Done		Trusted sites Protecte	d Mode: Off	🖓 🔹 🔍 100% 👻

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.



1.6.1			1 1 1									
ssg5-v92:Juniper-ScreenOS 6.3	3.0r4.0						ł	• • 🔊	- 🖃 🤤	💼 🔻 Page 🕶 Sa	fety 🔹 Tools 🔹	• (?)
	Net	wo	ork > Routing > Ro	uting Entries							ssg5-v92	?
	List	t 2	20 🔻 per page									
	1.164		uto ontrios for t	ust-vr						tru	st-vr	New
										1.00		
	Шг											1
SSG5-v92		tru	ist-vr		1							
Binding	<u> </u>		IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Description	Configure	
– Zones		*	10.20.0.0/16		ethernet0/0	С			Root		-	
Interfaces		*	10.20.10.211/32		ethernet0/0	н			Root		-	
- List Backup		Ì	192.168.100.0/24		ethernet0/3	с			Root		-	
- DHCP		Ī	192.168.100.1/32		ethernet0/3	н			Root		-	
802.1X Routing		*	192.168.66.0/24		bgroup0	с			Root		-	
- Destination		*	192.168.66.2/32		bgroup0	н			Root		-	
- Source	l f	-¦	192.168.66.0/24	untrust-vr	-	s	20	1	Root		Remove	
- Source Interface - MCast Routing		*	10.50.50.0/24	192.168.66.254	bgroup0	SP	20	1	Root		<u>Remove</u>	
. ■- PBR	1 -		* Active route C	Connected I I	mported	eB EBGP	O OSPF	E1 OSPF	extern	al type 1 H Ho	st Route	1
Virtual Routers			P Permanent S	Static A A	uto-Exported	iB IBGP	R RIP	E2 OSPF	extern	al type 2		
			D Dynamic N	NHRP								
- Security												
Policy												
- Policies MCast Policies												
Policy Elements												
- Addresses												
- List	1											
Groups												

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

NCP Secure Client - Juniper Edition	Profile
Connection Configuration Log View Help Profile: Connection: Remote Access	Available Profiles Group: Show all profiles Profile Name Juniper VPN Junos Dialup VPN Junos VPN Radius NS MIP Remote Access
Statistics: Time online: 00:00:14 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	ScreenUS Lett User ScreenUS VPN Add / Import Edit Copy Delete Export
	Profile Settings Remote Access X Basic Settings IPsec General Settings IPsec General Settings Line Management IPsec General Settings Gateway (Turnel Endpoint): Idvanced IPsec Options Idvanced IPsec Options Idvanced IPsec Options Idvanced IPsec Options IV IV IV IPsec Address Assignment Split Turneling IV IV Policies IV IV IV IV IV IV IV IV IV IV IV IV IV IV IV IV IV IV IV IV IV IV IV
	Help OK Cancel



IN LA	~ >	
NCP Secure Client - Juniper Edition	×	ProfileX
Connection Configuration Log View H	elp	Available Profiles
Prohie:	Lonnection:	Group:
		Show all profiles Group
		Profile Name
	Juniper.	Juniper VPN
Connection established.		Junos Dialup VPN
		NS MIP
	NCP	Remote Access
Statistics:		ScreenDS Cert User
Data (Tx) in Byte: 174 Time online:	00:00:14	
Data (Rx) in Byte: 88 Timeout (see Speed (KByte/s): 0.000 Encryption:	c): 0 sec AFS 128	Add / Import Edit Copy Delete Export
	ALO 120	
		Help OK Cancel
	l.	Desfile Cattings - Demote Access
		Line Management Local Identity (IKE)
		IPsec General Settings Type: Fully Qualified Domain Name
		Identities Upp. net
		Split Tunneling Pre-shared Key
		Certificate Check Shared Secret:
		Confirm Secret: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
		Certificate
		Extended Authentication (XAUTH)
		Baseword: XXXXXXX
		Help OK Cancel
NCP Secure Client - Juniner Edition		
Connection Configuration Log View h	-lein	Profile
Profile:	Connection:	Available Profiles
Remote Access		Group:
_		Show all prohies
	IL IOIDOC	Profile Name
	JUI IIPEI.	Juniper VPN
Connection established		Junos Dialup VPN
		NS MIP
	NCO	Remote Access
Chattalian		ScreenOS Cert User
Data (Tx) in Byte: 174 Time online	00:00:14	
Data (Rx) in Byte: 88 Timeout (se	c): 0 sec	Add / Import Edit Copy Delete Export
Speed (KByte/s): 0,000 Encryption:	AES 128	
		Help OK Cancel
		Profile Sattings - Damate Access
		Prome Sectings Remote Access
		Basic Settings
		IPsec General Settings Assignment of the Private IP Address
		Identities
		IPsec Address Assignment IP Address: 0.0.0.0 Split Tunneling
		Certificate Check

IP <u>A</u>ddress: DNS / WINS Servers DNS Server:

WINS Server: Do<u>m</u>ain Name: 0.0.0.0

0.0.0.0

Help

0.0.0.0

0.0.0.0

Cancel

ΟK



NCP Secure Client - Juniper Edition	Profile
Connection Configuration Log View Help	Available Profiles
Profile: Connection:	Group:
Remote Access	Show all profiles Group
	D-O-News
JUNIPEr.	Juniper VPN
Connection established.	Junos Dialup VPN
B & A	Junos VPN Radius
	NS MIP Bemote Access
	ScreenOS Cert User
Statistics:	ScreenOS VPN
Data (1X) in Byte: 174 Time online: 00:00:14 Data (Rx) in Byte: 88 Timeout (sec): 0 sec	Add Unext Edit Com Databa Errort
Speed (KByte/s): 0,000 Encryption: AES 128	
	Help OK Cancel
	Profile Settings Remote Access
	Profile Settings Remote Access
	Profile Settings Remote Access Basic Settings Line Management IPsec General Settings Enter the remote IP networks the tunnel should be used for. Without
	Basic Settings Split Tunneling Ine Management Split Tunneling IPsec General Settings Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used.
	Profile Settings Remote Access Basic Settings Line Management IPsec General Settings Advanced IPsec Options Identities UPsec Address Assignment IPsec Address Assignment
	Profile Settings Remote Access Basic Settings Split Tunneling Line Management Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. Identities IPsec Options Identities Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Address Assignment Split Tunneling Split Tunneling Remote Networks Remote Networks Remote IP Net Masks 192 159 65 0 255 055 055 0
	Profile Settings Remote Access Basic Settings Split Tunneling Line Management Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Central Settings Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Address Assignment Split Tunneling Split Tunneling Remote Networks Certificate Check 192.168.66.0 255.255.255.0 195.050.0
	Profile Settings Remote Access Basic Settings Split Tunneling Line Management Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. Identities Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Caddress Assignment Split Tunneling Split Tunneling Remote Networks Certificate Check Percent Set 255.255.0 10.50.50.0 255.255.255.0
	Profile Settings Remote Access Basic Settings Split Tunneling Line Management Prese Central Settings Advanced IPsec Options Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Address Assignment Split Tunneling Split Tunneling Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Address Assignment Split Tunneling Certificate Check Remote Networks ID 2168.66.0 255.255.05 ID 50.50.0 255.255.255.0
	Profile Settings Remote Access Basic Settings Split Tunneling Line Management Presc Options IPsec Options Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Address Assignment Split Tunneling Split Tunneling Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Address Assignment Split Tunneling Certificate Check Permote Networks ID 50.50.0 255.255.255.0 ID 50.50.0 255.255.255.0
	Profile Settings Remote Access Basic Settings Split Tunneling Line Management Prese Options IPsec Options Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Address Assignment Split Tunneling Split Tunneling Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Address Assignment Split Tunneling Certificate Check Percent Networks Remote Networks Remote IP Net Masks 192:168.66.0 255.255.05 10.50.50.0 255.255.255.0 10.50.50.0 255.255.255.0
	Profile Settings Split Tunneling Basic Settings Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Central Settings Advanced IPsec Options Identities IPsec Address Assignment Split Tunneling Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. IPsec Address Assignment Split Tunneling Certificate Check Remote Networks Remote Networks Remote IP Net Masks 192:168.66.0 255.255.255.0 10.50.50.0 255.255.255.0 Add Edit Add Edit
	Profile Settings Split Tunneling Basic Settings Enter the remote IP networks the tunnel should be used for, Without entries tunneling will always be used. IPsec General Settings Enter the remote IP networks the tunnel should be used for, Without entries tunneling will always be used. Split Tunneling Enter the remote IP networks the tunnel should be used for, Without entries tunneling will always be used. Split Tunneling Enter the remote IP networks Certificate Check Remote Networks Add Edit Delete Full Local Network Enclosure Mode
	Profile Settings Split Tunneling Basic Settings Split Tunneling Line Management Psec General Settings Advanced IPsec Ditions Identities Identities Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used. Prese General Settings Advanced IPsec Ditions Identities Immediate Settings Prese General Settings Prese General Settings Advanced IPsec Ditions Identities tunneling will always be used. IPsec Address Assignment Split Tunneling Detrificate Check Premote Networks Remote Networks Remote IP Net Masks 192 168 66.0 255.255.255.0 10 50.50.0 255.255.255.0 Add Edit Delete Full Local Network Enclosure Mode





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.

Ssg5-v92:Juniper-ScreenOS	6.1.0r7.0 - Windows Internet Explorer	_ 🗆 🗙
	211/nswebui.html	₽ •
🚖 Favorites 🛛 🚖 🙋 Suggester	d Sites 🔻 🙋 Web Slice Gallery 🝷	
👷 🔹 🔊 ssg5-v92: Juniper-Scree	en X 🔏 IIS7	
	VPNs > AutoKey IKE > Edit ssg5-v92	?
	Security Level	-
SSG5-v92	Predefined C Standard C Compatible C Basic	
- Home	User Defined 🕤 Custom	
Configuration	Phase 2 Proposal	
Network	nopfs-esp-aes128-sha 💌 None 💌	
Security	None None	
+ Policy - VPNs		
- AutoKey IKE	Replay Protection 🔽	
AutoKey Advanced	Transport Mode (For L2TP-over-IPSec only)	
- Gateway	Dind to C North	_
– P1 Proposal	Bind to • None	
- XAuth Settings	C Tunnel Interface	
- VPN Groups		
Manual Key	Proxy-ID	
L2TP Monitor Status	Local IP / Netmask /	
Objects	Remote IP /	_
Reports	Netmask / / /	
Wizards		
	DSCP Marking @ Disable	
	C Enable Dscp Value 0	
Toggle Menu		
Dana	VPN Crown None V Woight 0	•
Done	j j j j j j j j protected Mode: On j ∲ j ▼ j 🔍 1	10% ¥ ///



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

ssg5-v92: Juniper-ScreenOS 6.1.0r7.	o		合	- 🔊 - 🖃 🖷	🛛 🕶 Page 🕶	Safety - Tools	- (
	Objects > IP Poo	ls				ssg5-v92	?
						N	lew
NETWORKS							
SSG5-v92	Name	Start IP	End IP	In use	Co	onfigure	
Addresses	VPN Pool	172.16.100.100	172.16.100.200	0	Edit	Remove	
Services Schedules	AD Pool	172.16.66.100	172.16.66.100	1	-	-	
- Traffic Shaping			-				
Group Expression							
- VPNs							
- AutoKey IKE							
AutoKey Advanced							
– P1 Proposal							
- P2 Proposal							
- XAuth Settings							
- VPN Groups							
Manual Key							
Monitor Status							
Objects							
Users							
IP Pools							
Reports							
- Wizards							
- Help 🚽							
ne			🐪 🗸 Trusted sites	Protected Mode:	Off	🖓 👻 🔍 100	%



Next step is to configure the Auth Server

ssg5-v92:Juniper-ScreenOS 6.1.0r7.0	🚹 🔹 🗔 👻 🖃 🖷 👻 Page × Safety × Tools × 🔞 •
Configuation > Au	th > Auth Servers > Edit \$\$55-v92 💡
Juniper [.]	_
SSG5.v92 Name	AD1
IP/Domain Name	192.168.66.11
Home Gonfiguration Backup1	
Date/Time Backup2	
Admin Timeout	10 minutes (0 to disable)
- Auth WebAuth Enrord Timoout	
- Firewall	Minutes (u to disable)
Infranet Auth	Stripping Separator
Report Settings Settings Settings	Densis Name
Security Reliev	
- Policies Failover	Revert Interval 0 seconds (0 to disable)
MCast Policies Source Interface Policy Elements	none
Addresses	
Schedules	KADIUS Port 1645 Shared Secret
Traffic Shaping Group Expression	Retry times 3 Retry Timeout 3 seconds
DIP	Acct-Session-ID Length Bytes (0 for default)
ssg5-v92:Juniper-ScreenOS 6.1.0r7.0	🖓 • 🕤 - 🗆 👼 • Page • Safety • Tools • 🚷
Configuation > Au	th > Auth Servers > Edit \$\$55-V92 ?
	Retry times 3 Retry Timeout 3 cocords
SSG5-v92	Acet Costies TD Looph To Looph To Looph To Looph To Looph
Home	Bytes (U for default)
Date/Time	Zone Verification Escaled
Update Admin	Zone vennoadon I EndDied
- Auth	Client Batrice Development of Francisco I

E	Auth WebAuth Firewall		C SecurID	Client Retries Authentication Port	3 Client Timeout 5 seconds
	Infranet Auth Report Settings letwork			Encryption Type Use Duress	© DES C SDI C Yes © No
	Policy Policies MCast Policies Policy Elements		C LDAP	LDAP Port Distinguished Name(dn)	389 Common Name Identifier Cn cn=users,dc=vpnaccess,dc=local Cn Cn
	Addresses Services Schedules Traffic Shaping		C TACACS+	TACACS Port	Shared Secret
•	Group Expression	•	1	OK Cancel	

Trusted sites | Protected Mode: Off





Next configure the Auth Server parameters

VPNs > AutoKey Advanced > XAuth Settings ssg5-v92	
Reserve Private IP for XAuth User 480 Minutes	
SSG5-v92	
Addresses Default Authentication Server AD1	
Schedules Query Client Settings on Default Server	
Group Expression CHAP	
UPNs	
AutoKey IKE IP Pool Name AD Pool 💌	
Otal way DNS Primary Server IP 192.168.66.11	
P2 Proposal DNS Secondary Server IP 0.0.0.0	
VPN Groups WINS Primary Server IP 192.168.66.11	
U2TP WINS Secondary Server IP 0.0.0.0	
Objects	
Users	
Apply Cancel	
Certificates	
Wiards	
Trusted sites Protected Mode: Off	•

Next create a new Gateway configuration as shown below

ssg5-v92: Juniper-ScreenOS 6.1.0r7	.0		🟠 • 🔝 - 🖃 🖶 • Pag	je 🔹 Safety 👻 Tools 👻 🔞 🗸
	VPNs > AutoKey Advanced > Gateway	/ > Edit		ssg5-v92 ?
SSG5-v92 POIICY Elements Addresses Schedules Traffic Shaping Group Expression DIP VPNs AutoKey IKE AutoKey IKE A	VPNs > AutoKey Advanced > Gateway Gateway Na Ver © Remote Gateway © Static IP Address © Dynamic IP Address © Dialup User © Dialup User Group © ACVPN-Dynamic Local ID [DistinguishedName] © ACVPN-Profile	 > Edit ame AD Gateway sion • IKEv1 • IKEv2 IP Address/Hostname Peer ID User Group 	Vpnaccess.local None Advanced	ssg5-v92
Users IP Pools Certificates Wizards Done		Viruster	sites Protected Mode: Off	√ ≜ ▼ 3€ 100% ▼



NCP Client with Juniper ScreenOS

	177		
ssg5-v92: Juniper-ScreenOS 6. 1.0r7.0		拱 🔹 Page 🔹 Safety 👻 Too	ols • 🔞 •
l l	/PNs > AutoKey Advanced > Gateway > Edit	ssg5-v92	?
SSG-92 SSG-92 SSG-92 POIRCY Elements Addresses Schedules Traffic Shaping Group Expression DIP VPNs AutoKey Advanced Gateway P1 Proposal Xath Settings VPN Groups Manual Key L2TP Monitor Status	PNs > AutoKey Advanced > Gateway > Edit IKEv2 Auth Method Self Peer None Preshared Key Local ID Outgoing Interface ethernet0/0 Security Level Predefined C Standard C Compatible C Basic User Defined C Standard C None None None Mode (Initiator) C	ssg5-v92	
Objects Users IP Pools Certificates	✓ Enable NAT-Traversal UDP Checksum □ Keepalive Frequency 5 Seconds (0~300 Sec)		_
+ Wizards	Peer Status Detection O 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 👌 🔹 🖻 🚽 Page + Safety + Tools + 🔞 +
	VPNs > AutoKey Advanced > Gateway > Xauth ssg5-v92 ?
	Gateway Name: AD Gateway
	O None
- Policy	• XAuth Server
- MCast Policies	Allowed Authentication Type 🖲 Generic 🔗 CHAP Only 🔗 CHAP & PAP
Policy Elements	C Use Default Xauth Settings
- VPNs	C Local Authentication
- AutoKey IKE	C Allow Any
- AutoKey Advanced	C User None 💌
- Galeway - P1 Proposal	C User Group None 🔽
- P2 Proposal	External Authentication AD1 Z Guery Remote Setting
- XAuth Settings	C Allow Any
VPN Groups	C User Name
— Manual Key	User Group Name
Monitor Status	
- Objects	C XAuth Client
- IP Pools	Allowed Authentication Type C Any C CHAP Only C SecurID
Certificates	User Name
. ■ Reports	Password
🛨 Wizards	
+ Help	Prefix Delegation to IPv6 Interfaces Interfaces SLA ID SLA Length Action
Logout	Interface SLA ID SLA Length Action
Toggle Menu 🔻	
Done	💦 🗸 Trusted sites Protected Mode: Off



NCP Client with Juniper ScreenOS

ssa5-v92: Juniper-ScreenOS 6.1	.077.0 🐴 + 🔊 - 🖃 🚔 + Page + Safety + Tools + 🔞)-
	VPNs > AutoKey IKE > Edit ssg5-v92 ?	
Juniper		
SSG5-v92	VPN Name AD VPN	
Addresses	Remote Gateway Predefined AD Gateway	
- Schedules	C Create a Simple Gateway	
- Traffic Shaping	Gateway Name	
- Group Expression	Version KEv1 KEv2	
	Type • Static IP Address/Hostname	_
- VPNs		
AutoKey Advanced	O Dynamic IP Peer ID	
Gateway	O Dialup User User None 🔽	
– P1 Proposal	O Dialup Group Group None 🔽	
P2 Proposal	Local ID (optional)	
VPN Groups	Drocharod Koy	
- Manual Key	Use As Seed 1	
I L2TP	Security Level 🕐 Standard 🔗 Compatible 🔗 Basic	
Monitor Status	Outgoing Interface ethernet0/0 🔽	
- Objects	ACVPN-Dynamic Gateway None Tunnel Towards Hub Secure MIP	
- IP Pools	C ACVPN-Profile Binding to Tunnel None	
Certificates		_
Reports	OK Cancel Advanced	
+ Wizards		
Done	💦 🗸 Trusted sites Protected Mode: Off	11.
ssg5-v92: Juniper-ScreenOS 6. 1	LO7.0 🎳 + 💽 - 🖃 🖷 + Page + Safety + Tools + 🕡) -
ssg5-v92;Juniper-ScreenOS 6. 1	Lor7.0 👌 ་ 🗟 ་ 🖻 🚔 ་ Page ፣ Safety ፣ Tools ፣ 🕼 VPNs > AutoKey IKE > Edit ssg5-v92 ?)-
ssg5-v92:Juniper-ScreenOS 6. 5	Lor7.0 In Page + Safety + Tools + (i) VPNs > AutoKey IKE > Edit Ssg5-v92)-
ssg5-v92:Juniper-ScreenOS 6.	LO7.0 In Page + Safety + Tools + (in VPNs > AutoKey IKE > Edit Ssg5-v92 ?)-
Support Streen States Streen States Streen States Streen States Streen States Streen States Streen S	LOT7.0 International Internati	9-
ssg5-v92:Juniper-ScreenOS 6. 3	LOT7.0 International Internati	•
ssg5-v92:Juniper-ScreenOS 6. J	LOT7.0 In the second se	
ssg5-v92:Juniper-ScreenOS 6. 3	LO7.0 In Page + Safety + Tools + () VPNs > AutoKey IKE > Edit Ssg5-v92 ? Security Level Predefined O Standard O Compatible O Basic User Defined O Standard	
SSG5-v92:Juniper-ScreenOS 6.1	Lor7.0 In Page - Safety - Tools - (VPNs > AutoKey IKE > Edit Ssg5-v92 ? Security Level Predefined C Standard C Compatible C Basic User Defined C Custom	•
ssg5-v92:Juniper-ScreenOS 6.	Lor2.0 In Page + Safety + Tools + (in the second se	•
Sig5-v92:Juniper-ScreenOS 6.1	Lor.0 Intervention in the intervention intervention in the intervention interventintervention intervention intervention intervention intervention	•
Sig5-v92:Juniper-ScreenOS 6.1	Lor.0 Intervention in the intervention intervention in the intervention intervent	•
SIG5-v92:Juniper-ScreenOS 6.1	Lor.0 Page - Safety - Tools - (VPNs > Autokey IKE > Edit Ssg5-v92 ? Security Level Predefined C Standard C Compatible Basic User Defined C Custom Phase 2 Proposal nopfs-esp-aes128-sha None None None None	•
Sig5-v92:Juniper-ScreenOS 6.1	Lor.0 Page + Safety + Tools + VPNs > AutoKey IKE > Edit ssg5-v92 ? Security Level Predefined C Standard C Compatible Basic User Defined C Custom Phase 2 Proposal nopfs-esp-aes128-sha None Replay Protection Replay Protection	•
Sig5-v92:Juniper-ScreenOS 6.1	Lor.0 Page + Safety + Tools + VPNs > AutoKey IKE > Edit ssg5-v92 ? Security Level Predefined C Standard C Compatible Basic User Defined C Custom Phase 2 Proposal nopfs-esp-aes128-sha None Replay Protection Replay Protection (For L2TP-over-IPSec only)	
Sig5-v92:Juniper-ScreenOS 6.1	Lor.0 VPNs > AutoKey IKE > Edit ssg5-v92 ? Security Level Predefined C Standard C Compatible Basic User Defined C Custom Phase 2 Proposal nopfs-esp-aes128-sha None Non	•
Seg5-v92:Juniper-ScreenOS 6. 1 Sig5-v92 Sig5-v92 Sig5-v92 Services Serv	Lor.0 Page - Safety - Tools - (VPNs > Autokey IKE > Edit ssg5-v92 ? Security Level Predefined C Standard C Compatible C Basic User Defined C Custom Phase 2 Proposal nopfs-esp-aes128-sha None None None Replay Protection C Transport Mode (For L2TP-over-IPSec only) Bind to C None C Tunnel Interface	•
Sig5-v92:Juniper-ScreenOS 6.1	Lor.0 Introduction Interface Interfa	•
Sig5-v92:Juniper-ScreenOS 6.1	Lor.0 Page + Safety + Tools • VPNs > AutoKey IKE > Edit ssg5-v92 ? Security Level Predefined © Standard © Compatible © Basic User Defined © Custom Phase 2 Proposal nopfs-esp-aes128-sha ▼ None ▼ None ▼ None ▼ None ▼ None ▼ Transport Mode □ (For L2TP-over-IPSec only) Bind to © None © Tunnel Interface © Tunnel Interface © Tunnel Zone ♥ Untust Tun ▼	×
Seg5-v92:Juniper-ScreenOS 6.1	Lor.0 VPNs > AutoKey IKE > Edit ssg5-v92 Security Level Predefined Standard Compatible Basic User Defined Custom Phase 2 Proposal nopfs-esp-aes128-sha None None None None None None Proxy-ID ↓ Proxy-ID ↓ None Proxy-ID ↓ None Phase 2 Proposal None Phase 2 Proposal Phase 2 Proposal None Phase 2 Proposal None Proxy-ID ↓ Proxy-ID ↓ None Phase 2 Proposal None Proxy-ID ↓ Proxy-ID ↓ Prox	
Sig5-v92:Juniper-ScreenOS 6.1	Lor.0 VPNs > Autokey IKE > Edit ssg5-v92 Security Level Predefined © Standard © Compatible © Basic User Defined © Custom Phase 2 Proposal nopfs-esp-aes128-sha ▼ None None None None None None None None	
Seg5-v92:Juniper-ScreenOS 6.1	Lor.0 VPNs > AutoKey IKE > Edit Ssg5-v92 VPNs > AutoKey IKE > Edit Ssg5-v92 Security Level Predefined C Standard C Compatible Basic User Defined C Custom Phase 2 Proposal nopfs-esp-aes128-sha None None None None None None Phase 2 Proposal None Phase Phase 2 Proposal None Phase 2 Proposal None Phase Phase Phase 2 Proposal None Phase	
Seg5-v92:Juniper-ScreenOS 6.1	Lor.0 VPNs > AutoKey IKE > Edit Ssg5-v92 Security Level Predefined C Standard C Compatible Basic User Defined C Custom Phase 2 Proposal nopfs-esp-aes128-sha None None None None None None None None	
ssg5-v92:Juniper-ScreenOS 6.1 Sig5-v92 Sig5-v92 Addresses Addresses Services Schulzes Group Expression DIP VPNS AutoKey IKE AutoKey Kanced - Gateway - P1 Proposal - 22 Proposal - Xuth Settings - VPN Groups Manual Key L L2TP Monitor Status Objects U Sers - Users	Lor.0 VPNs > Autokey IKE > Edit ssg5-v92 ? Security Level Predefined C Standard C Compatible C Basic User Defined C Custom Phase 2 Proposal nopfs-esp-aes128-sha None None None None None None Phase 2 (For L2TP-over-IPSec only) Bind to C None C Tunnel Interface C Tunnel Interface C Tunnel Interface C Tunnel Zone None Proxy-ID V Local IP / Netmask 192.168.66.0 / 24 Remote IP / Netmask 172.16.66.100 / 32 Service ANY	•
Sig5-v92:Juniper-ScreenOS 6.1	Lor.0 VPNs > Autokey IKE > Edit ssg5-v92 ? Security Level Predefined © Standard © Compatible © Basic User Defined © Custom Phase 2 Proposal nopfs-esp-aes128-sha None N	
Seg5-v92:Juniper-ScreenOS 6.1	Lor.7.0 VPNs > AutoKey IKE > Edit Security Level Predefined C Standard C Compatible Basic User Defined C Custom Phase 2 Proposal nopfs-esp-aes128-sha None None None None None None Proxy-ID Froxy-ID Proxy-ID Doce I IP / Netmask 192.168.66.0 Y DSCP Marking C Disable C Enable Dscp Value 0	
Seg5-v92:Juniper-ScreenOS 6.1	Lor.7.0 Image: Page + Safety + Tools + Image: Security Level Security Level Predefined © Standard © Compatible © Basic User Defined © Custom Phase 2 Proposal Image: Protection © None None None None None Replay Protection © None Transport Mode © (For L2TP-over-IPSec only) Bind to © None Untrust-Tun ♥ Proxy-ID ♥ Local IP / Netmask 192.168.66.0 / 24 Remote IP / Netmask 192.166.6100 / 32 32 DSCP Marking © Disable Enable Dscp Value © 10	
Sig5-v92:Juniper-ScreenOS 6.1	Lor2.0 VPNs > AutoKey IKE > Edit ssg5-v92 ? Security Level Predefined © Standard © Compatible © Basic User Defined © Custom Phase 2 Proposal nopfs-esp-aes128-sha None	

And next create a VPN configuration using the configured gateway

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



NCP Client with Juniper ScreenOS

ssg5-v92: Juniper-ScreenOS 6. 1.0r7.0		🏠 🔹 🗟 👻 🚍 📥 🔹 Page 🔹 Safety 👻 Tools 🔹 🔞 🔹
Policy > Polici	es (From Trust To L	Intrust) ssg5-v92 ?
Juniper		
		<u>▲</u>
SSG5-v92	Name (optional)	
Policy		
- Policies	Source Address	C New Address / //
MCast Policies		Address Book Entry 192.168.66.0/24 Multiple
+ Policy Elements		C New Address
AutoKey IKE Des	tination Address	
AutoKey Advanced		
- Gateway	Service	ANY Multiple
– P1 Proposal	Application	Nene
- P2 Proposal	Аррисации	
VPN Groups		
– Manual Key		WEB Filtering
L2TP	Action	Tunnel
Monitor Status		_
Objects	Antispam enable	
+ Users	Tunnel	VPN AD VPN
Certificates		Modify matching hidirectional VPN policy
Reports		
+ Wizards		L2TP None V
+ Help	Logging	🔽 at Session Beginning 🔽
Logout		
Tangle Hann		
	Session-limit	Trusted sites Destacted Medey Off

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

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

ssg5-v92:Juniper-ScreenOS 6.1.0r7.0	🛐 🕶 🔂 👻 🖃 💼 🍷 Page 🔹 Safety 👻 Tools 👻 🔞 👻
Policy > Policies	(From Trust To Untrust) ssg5-v92 ?
SSG5-v92	Advanced Policy Settings
Policy	
 Policies MCast Policies Policy Elements VPNs AutoKey IKE AutoKey Advanced Gateway P1 Proposal P2 Proposal 	■ Source Translation (DIP on) None (Use Egress Interface IP) ■ ■ Destination Translation ■ Translate to IP 0.0.0.0 ■ Map to Port 0 ■ Translate to IP Range 0.0.0.0 = 0.0.0.0
Xuth Settings VPN Groups Manual Key L2TP Monitor Status Objects	C Auth Server Group C Allow Any ▼ Group C Allow Any ▼ Expression C Allow Any ▼
Users IP Pools Certificates Reports Wizards Help Logout	n V WebAuth(Local)
Toggle Menu	C Toferant Author D Francisco C D Francisco Harris Author
Edit	C Infraner-uith Redirect C Redirect unauthenticated traffic Note that the second se



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.

ssg5-v92:Juniper-ScreenOS 6.3.0r4.0	🚹 👻 🖻 👻 🚍 👘 👻 Page 👻 Safety 👻 Tools 👻 🔞 👻
Network > Ro	ting > Routing Entries > Configuration ssg5-v92 ?
SSG5-v92 Virtual Route	er Name trust-vr
- Home - IP Address/M	etmask 1/2.16.66.0 / 24
+ Configuration	
- Network	ext Hop 🛇 Virtual Router untrust vr 🔻
- Binding	
DNS	Gateway
Zones	
- interfaces	
Backup	Gateway IP Address 0.0.00
	Permanent 🗖
. 802.1X	Tag 0
Routing	
- Destination	Metric 1
Source Interface	
MCast Routing	rerence 20
E PBR Des	cription
Virtual Routers	
	OK Cancel
+ Policy	
- VPNs	

	ssg5-v92: Juniper-ScreenOS 6.3	3.0r	4.0					6	• 🔊 -	-		y 🕶 Tools 🖲	• 🔞 •		
Γ		N	letv	vork > Routing > Ro	outing Entries						55	g5-v92	?		
				List 20 v per page											
I												<u> </u>			
			trust-vr												
	Homo			IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Description	Configu	ıre		
÷	Configuration	L	*	10.20.0.0/16		ethernet0/0	С			Root		-			
F	Network Binding	L	*	10.20.10.211/32		ethernet0/0	н			Root		-			
		L	Γ	192.168.100.0/24		ethernet0/3	С			Root		-			
	Zones	L	Г	192.168.100.1/32		ethernet0/3	н			Root		-			
	Interfaces	L	*	192.168.66.0/24		bgroup0	с			Root		-			
	Backup		*	192.168.66.2/32		bgroup0	н			Root		-			
	- DHCP		*	10.50.50.0/24	192.168.66.254	bgroup0	SP	20	1	Root		Remove	1		
	- Routing			192.168.66.0/24	untrust-vr	-	S	20	1	Root		Remove			
	- Destination		Γ	172.16.66.0/24		tunnel.1	S	20	1	Root		Remove			
	Source Source Interface MCast Routing			* Active route C P Permanent S D Dynamic N	Connected I I Static A A NHRP	mported uto-Exported	eb Ebgf ib Ibgp	O OSPF R RIP	E1 OSPF E2 OSPF	extern extern	al type 1 H Ho al type 2	st Route			



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.

Profile Settings AD Users							×
Basic Settings Line Management IPsec General Settings Advanced IPsec Options Identities IPsec Address Assignment Split Tunneling Certificate Check	Identities Local Id	entity (IKE) <u>I</u> ype: <u>I</u> D: shared Key <u>S</u> hared Se Confirm Se Confirm Se Confirm Se Configurati nded Authe <u>U</u> ser ID: <u>P</u> assword:	ecret: ecret: on: ntication (X	Fully Qu vpnacce xxxxxxxxxx none AUTH) Domain	alified Doma ess.local	ain Name	
			Help	, [OK		Cancel

And then go to the IPsec Address Assignment.

Profile Settings AD Users							×
Basic Settings Line Management IPsec General Settings Advanced IPsec Options Identities IPsec Address Assignment Split Tunneling Certificate Check	□ IPsec Ad	dress Assign Assignmen IKE confi IP <u>A</u> ddres / WINS Serv <u>W</u> INS Serv Do <u>m</u> ain N	nment — g mode ss: ervers — ver: ver: ame:	ivate IP / 0.0.0.0 0.0.0.0 0.0.0.0	\ddress	0.0.0.	
			Hel	P	OK		Cancel



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

Connection Configuration Log View Help Profile Connection Configuration Log View Help Profile Connection established Connection establish	NCP Secure Entry Client	l og Book	NCD Secure Client Juniper Edition	A Loo book
Polde: Connection P/21/2016 63347PM Like: Lise: Lise: Sangebiated with the following people: Jurger: SSG Image: SSG	Connection Configuration Log View Help			LOG BOOK
1721/2016 0347 PM NSUC255 like phase 2 (quick mode) eady 1721/2016 0347 PM SUC255 like phase 2 (quick mode) eady 1721/2016 0347 PM NSG2, 2UICX - Junger SS 1721/2016 0347 PM NSG2, 2UICX - SUICA - SUICA 1721/2016 0347 PM NSG2, 2UICX - SUICA - SUICA 1721/2016 0347 PM NSG2, 2UICX - SUICA - SUICA 1721/2016 0347 PM NSG2, 2UICX - SUICA - SUICA - SUICA 1721/2016 0347 PM NSG2, 2UICX - SUICA - SUIC	IVCP-Secure Entry Client Image: Secure Entry Client Connection Configuration Log View Help Connection: Juniper SSG Image: Connection: Juniper SSG Image: Connection: Connection: established. Image: Connection: Tip of the day: How to enable the client's firewall. Image: Connection: Statistics: Image: Connection: Tip of the day: How to enable the client's firewall. Image: Connection: Data (Fick) RKSyte: 1.43: Image: Connection: Data (Fick) RKSyte: 1.43: Link Type: LAN Exception: AES 128 Client's Your logo here? Software notyet activated (valid for another 13 days) Activation	Log Book 721/2010 6.03.47 PM Ike: Turning on XAUTH mode -Juniper SSG 721/2010 8.03.47 PM 1ke: Ike3 angediated with the following prop 721/2010 8.03.47 PM Ike: Ike3 angediated with the following prop 721/2010 8.03.47 PM 721/2010 8.03.47 PM IkeI Michail angediated with the following prop 721/2010 8.03.47 PM IkeI Michail angediated with the following prop 721/2010 8.03.47 PM 721/2010 8.03.47 PM IkeI Michail angediated with the following prop 721/2010 8.03.47 PM IkeI Michail angediated with the following prop 721/2010 8.03.47 PM 721/2010 8.03.47 PM IkeI Michail angediated with the following prop 721/2010 8.03.47 PM Ike IkeSa negotiated with the following prop 721/2010 8.03.47 PM 721/2010 8.03.47 PM IkeBare1 name(Jungediated With the following prop 721/2010 8.03.47 PM IkeBare1 name(Jungediated With the following prop 721/2010 8.03.47 PM 721/2010 8.03.47 PM IkeBare1 name(Jungediated With EGU) IkeBare1 name(Jungediated With IkeGPA IkeIndewised 16.44 PM 721/2010 8.03.47 PM IkeBare1 REV_VAUTH_REDUST IkeBare1 REV_VAUTH_REDUST 721/2010 8.03.47 PM IkeBare1 REV_VAUTH_REDUST IkeBare1 PM 721/2010 8.03.47 PM IkeBare1 NMIT_KECPG_BARE1 - Numper SSG 721/2010 8.03.47 PM IkeBare1 NMITH_REDUST IkeBare1 NMITH_REDUST 721/2010 8.03.47 PM IkeBare1 NMITH_RED	INCP Secure Client - Juniper Edition Connection Configuration Log View Help Erofie: Cornection: AD Users Image: Cornection: Connection established: Image: Cornection: Connection established: Image: Cornection: Data (FX) in KSyte: 1189 Data (FX) in KSyte: Time online: Data (FX) in KSyte: Encryption: AE Speed (KByteis): 0,000 Software not yet activated Activation	Log Book 7/21/2010 6:03:44 PM Ike: XMIT_MSG3_AGGRESSIVE - AD Users 7/21/2010 6:03:44 PM Ike: IkeSa negotaled with the following properties - 7/21/2010 6:03:44 PM 7/21/2010 6:03:44 PM Ike: IkeSa negotaled with the following properties - 7/21/2010 6:03:44 PM 7/21/2010 6:03:44 PM Ike: IkeSa negotaled with the following conserved set in the set in the set in the following properties - 7/21/2010 6:03:44 PM 7/21/2010 6:03:44 PM Ike: Turning on DPD mode - AD Users 7/21/2010 6:03:44 PM SetExe: Final Turnet EndPwint is (1010/2010/21) 7/21/2010 6:03:44 PM IkeSa: Final Turnet EndPwint is (1010/2010/21) 7/21/2010 6:03:44 PM IkeSa: Final Turnet EndPwint is (1010/2010/21) 7/21/2010 6:03:44 PM IkeSa: Final Turnet EndPwint is (1010/2010/21) 7/21/2010 6:03:44 PM IkeSa: Final Turnet EndPwint is (1010/2010/21) 7/21/2010 6:03:44 PM IkeSa: Final Turnet EndPwint is (1010/2010/21) 7/21/2010 6:03:44 PM IkeSa: SetExet EndB Addwint Addwint is related open 7/21/2010 6:03:44 PM IkeSa: SetExet EndB Addwinet is related open 7/21/2010 6:03:44 PM IkeSa: SetExet EndB Addwinet is related is related in Park 7/21/2010 6:03:44 PM IkeSa: SetExet EndB Addwinet is related in Park 7/21/2010 6:03:44 PM
		Clear Screen Create File		Clear Screen Create File

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

Server Manager		_ 6			
File Action View Help					
(= =) 🖄 📅 🖬					
Server Manager (AD) Active Directory Certificate Services Active Directory Certificate Services DHCP Server DHCP Server	Roles Were the health of the roles installed on your server and add or remove roles and filled on your server and add or remove roles and filled on your server.	eatures.			
a) ⊕ Dho Sarries a) ⊕ Fo Sarries a) ⊕ Fo Sarries a) ⊕ Fo Sarries a) ⊕ Hotwark hole; and Access Sarries a) ⊕ Hotwark b ⊕ Department b ⊕	Roles Summary	Roles Summary Help			
	Reles: 7 of 17 installe Active Directory Certificate Services Hord: Percency Continues Services Directory Contain Services Directory Directory Tel Services Tel Services Web Server (IIS)	Add Roles			
	Active Directory Certificate Services	AD CS Help			
	Active Directory Certificate Services (AD CS) is used to create certification authorities and re manage certificates used in a variety of applications.	lated role services that allow you to issue and			
		Go to Active Directory Certificate Services			
	Messages: None				
	System Services: All Running				
	Best Practices Analyzer 10 sets as 2 m 600°S Best Practices Analyzer 10 sets a Best Practices Analyzer scan, so to the Best Practices Analyzer ble on this role's homepade and click. Scan this Role				
	Role Services: 3 installed	Add Role Services			
	Automatica Automatic	Remove Role Services			



Create a new Windows Server CA

Export the CA cert using "CertUtil -ca.cert ca_rootcert.cer" via CLI

	Administrator: C:\Windows\system32\cmd.exe	_ 🗆 🗙
ľ	2 Dir(s) 7,539,367,936 bytes free	-
F	C:\Temp>certutil -ca.cert ca_vpnaccess.cer CA cert[0]: 3 Valid CA cert[0]:	
L	BEGIN CERTIFICATE HIIDE2CCALUAGUIBAGIQPIQPIQPEG45xE72aUzdr4rGjANBgkghkiG9v0BAQUFADBM HRUDEXYKCZIniZPULGQBCRFFbG3jVUwxCIAKBgnJKiaUz1zZAEZFg12cG5hY2NI e JwcGADUBANUBANTD3ZJaheFY2Uzz wi RKC1DATAE FW6wHChwi i uMDUH5ha Pu6x	
<	NTEUMI I UHTA AMBZANEUNETTÄ TBAG ILLÄ AIVA I SÄÄRSTRUGEN SANNAD EZHBE COGNS JONT Biskon Kakka Cauber 1920 zur se per Villy Gan Liban AHda nu kvilly Käyska Liban Elukiniki (181 jan Biskon Kakka Cauber 1920 zur se per Villy Gan Liban AHda nu kvilly Käyska Liban Per Lukiniki (181 jan Biskon Kakaka VIII Säärste Käyska Käyska VIII Sõgika Käyska VIIII Sõgika VIIII Sõgika VIIII Sõgika VIIII Sõgika	
	EXN9Xdx,q13EnuxqEbu.CCGGUirs.CxrrVM41bbf12FIEleUNX6VWHFXq2bEndE1k* 80noqr17ccKR-QEAUV1yv9qq1HLKESUzwE74+12757EHjdbvKVWHFXq2bEndE1k* Mucdq8UL233DJJD[Shi7]J1Hcj2JjHLKESUzwE74+51757EHjdbv7HjjmrfGRu7kcHWG	
	5 gree source (ap + ray 1 myn polar / k / x x r as ne g + m A dyn 5 whith a C = b k d k d v x 4 m y 1 myn polar / k / x x 7 r as ne g + m A dyn 5 whith a C = b k d k d v x 4 m y 1 m y	
	6 Le bez ¥BaCSI ceNE 04 9 u i 43 / aksi SU 9 pi 11N 30 Lun Jul Cou 5 A 20 Gani + 9 Lud 199 E Jul (1872 Art u st. 100 A 4 u ú / A U la ne de ner y Libe Hin E Juo Jul (3 1 Sanh 6 y LL L2 Y Sy NH Y S i r, i lud s 3 NSC D2 BU neo Ju + tQ Koo i q + Mine i lu + ZI Du A 1 Q 1 80 Z C 7 2 U L c Z 6 × S in C X Z E 1 U L ne ji Nit u + r 0 Gao 4 y Z Z I / J or i há / t s 1 ne ji + Z Z Du A 1 Q 1 80 Z C 7 2 U L c Z 6 × S in C X Z E 1 U L	
r	END CÈRTIFICATÈ CertUtil: -ca.cert connand completed successfully.	
	C:\Temp>_	

or via a web browser download the CA Cert



Chose "Download CA certificate chain" link and save the file. Import this cert into the Juniper gateway (Objects – Certificates)

Contraction Common C	7.0-1.0 100-	dever Totomat Fuelsees								
swgs-v92.Jumper-screenos 6	C3.074.0 - Win	dows Internet Explorer								
G C + http://10.20.10.2	12/nswebui.htm					🖬 😁 🗙 (27 Bin				<u>р</u> .
🙀 Favorites 🛛 🍰 ssg5-v92Ju	niper-ScreenOS	📖 🙋 Microsoft Active Dir	rectory C							
👷 🔹 🖾 ssq5-v92:Juniper-Screen		rosoft Active Directory C				🏠 • 🖾		- Page - Safety	- Tools -	0.
	Objects	s > Certificates	1					ssq5-v92	2	
		6 C		_						_
(Load	Cert C CRL FI	lie:		Browse Load					
(N) luniner	Show	CA -	Defaul	t Cert	Validation				New	
NETWORKS					Seronde					_
		Issuer	Friendly Name	Type	Serial#	Expired	Status	Configure		
		uppaccore AD-CA						-		
- Home		Server Settings	48	CA	3e543779012ce39c44eda57376be2b1a	10-22-2015 21:01	Active	Detail, Remove		
Configuration										
Network Socurity										
+ Policy										
- VPNs										
AutoKey IKE										
 AutoKey Advanced 										
- Gateway										
P1 Proposal										
XAuth Settings										
VPN Groups										
MODECFG Profile										
- Manual Key										
 L2TP 										
Monitor Status										
- Ulgars										
Local										
Local Groups										
External Groups										
- IP Pools										
Certificates										
Sustam Log										
Event										
Self										
Asset Recovery										
Counters										
Chassis										
Intenace Bandwidth										
Done						Trusted sites Prote	cted Mode:	Off 🕼	. 100%	• 4



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"

NCP Secure Client - Junig	per Edition		tive Directory Certificate Services - Wi	idows Internet Explorer			_ 🗆 ×
Connection Configuration	Log View He	lp	https://192.168.66.11/certarv/		💌 😺 Certificate Error	🖻 🖘 🗙 🔽 Bing	ρ.
Profile:		Connection	👍 🥫 Internet Explorer cannot ds				
Suddrus VPN	-		tive Directory Certificate Services	1			
Connection	n established.	JUNPER	ctive Directory Certificate Services -	pnaccess-AD-CA			Home
Statistics: Data (Tb) in KByte: 15.93 Data (Rb) in KByte: 204.6 Speed (KBytels) 0.000	Time online: Timeout (sec) Encryption:	NCP 97 sec AES 128 the status For more	eb site to request a certificate for ou communicate with over the W itly tasks. so use this Web site to download of a pending request. information about Active Director	ryour Web browser, e-mail cli eb, sign and encrypt message a certificate authority (CA) ce / Certificate Services, see <u>Act</u>	ent, or other progra es, and, depending intificate, certificate	Im. By using a certificate, you ca upon the type of certificate you i chain, or certificate revocation I ficate Services Documentation.	n verify your identity request, perform ist (CRL), or to view
		Select a t Reque View th Downk	task: st a certificate he status of a pending certificate r pad a CA certificate, certificate ch	equest ain, or CRL			
						Character Destructed Market On	
						ansement (Protected Mode: On	194 • 1 • 100% • 2

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."

Microsoft Active Directory Certificate Services - Windows Internet Explorer		
🔆 🕑 💌 🔊 http://192.168.66.11/certary/centrqua.aap	💌 🗟 🐓 🗙 🔎 Bing	- م
🖕 Favorites 🛛 🙀 🙋 Microsoft Active Directory C 🙋 Microsoft Active Directory C 🤌 Microsoft Active Directory C 🖉 Suggested S	Sites 🔹 🙋 Web Slice Gallery 🔹	
Hicrosoft Active Directory Certificate Services	🖓 • 🔂 - 🖃 🖷 • Page •	Safety + Tools • 🔞 •
Microsoft Active Directory Certificate Senices vpnaccess-AD-CA		Home
Request a Certificate		
Select the certificate type: User Certificate		
Or, submit an advanced certificate request.		

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

🧭 Microsoft Active Directory Certificate Services - Windows Internet Explorer	_ 🗆 ×
🚱 🕞 💌 🖉 https://192.168.66.11/certary/certrams.asp 📃 😵 Certificate Error 🛛 😣 😽 🗙 🔽 Bing	ρ-
🖕 Favorites 🙀 😰 Internet Explorer cannot ds	
Microsoft Active Directory Certificate Services	
	*
Microsoft Active Directory Certificate Services - vpnaccess-AD-CA	Home
Advanced Certificate Request	
Certificate Template:	
User	
Key Options:	
Create new key set	
CSP: Microsoft Enhanced Cryptographic Provider v1.0 •	
Key Usage: @ Exchange	
Key Size: 1024 Min: 384 (common key sizes: 512 1024 2048 4096 8192 18384)	
Automatic key container name User specified key container name	
F Mark keys as exportable	
Enable strong private key protection	
Additional Options:	
Request Format: @ CMC C PKCS10	
Hash Algorithm: sha1 💌	
Only used to sign request.	
☐ Save request	
Attributes:	
x >	
Friendly Name: Demo_Usercent	
C.Amita	
Submt >	
	Whoreadd Addive Directory Certificate Services Windows Internet Explaner



Click on Submit button



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



Confirm "Certificate Installed" message

NCP Secure Client - Juniper Editio	Microsoft Active Directory Certificate Services - Windows I	nternet Explorer	
Connection Configuration Log Vie	w Hel	💌 😨 Certificate Error	🖻 🐈 🗙 🔽 Bing 🛛 👂 •
Profile	the Envertee and A Internet Evolution connet de		
Screen(DS VPN			
	C Microsoft Active Directory Certificate Services		
	Microsoft Active Directory Cartificate Services unnacc	ass-AD-CA	Home
Connection establis	shed.		IN INC.
# @ A	Certificate Installed		
	Your new certificate has been successfully installe	ed.	
Statistics: Data (Tx) in KByte: 49.09 Time or	oine		
Data (Roc) in KByte: 369.7 Timeou	ut (sec):		
Speed (KByte/s): 0.000 Encryp	stion:		
	Deep		Televent Destanted Marks Co.
	pure		amener (noterres note: on 5 4 + 4 100% +



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"





Enter the Password (eg 123456)

ral Security Privacy Content Connections	Programs Advanced	
ental Controls		
Control the Internet content that can be viewed.	Parental Controls	
ntent Advisor		
Ratings help you control the Internet con	ent that can be 👫 Certificate	x
viewed on this computer.	👘 Certific	ite Export Wizard
Poshie	Settors 1	
	Passwoi	e sintain earurity, you must contact the criviate key by using a necessory
tificates	101	annan security, you must protect the private key by using a passivoru.
Use certificates for encrypted connection	and identificatio	
8		
Clear SSL state Certificates	Publishers	and confirm a password.
		assword:
oComplete		
AutoComplete stores previous entries	Settings	
A on webpages and suggests matches —		ype and confirm password (mandatory):
for you.		•••••
ds and Web Slices		
Feeds and Web Sices provide updated content from websites that can be read in Internet Explorer and other programs.	Settings	
OK CI	incel /	
	· · · · · · · · · · · · · · · · · · ·	
		< Back Next > Cancel

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

		Y.	×			
Certificates			×	I		
_						
tended purpose: <	Al>		<u> </u>			
Personal Other People	Intermediate Certification	Authorities Trusted Ro	ot Certification + +			
Issued To	Issued By	Expiratio Friend	ly Name			
<none></none>	<none></none>	11/29/2011 <non< td=""><td>e></td><td></td><td></td><td></td></non<>	e>			
Administrator	vpnaccess-AD-CA	12/6/2011 Demo	User			
Administrator	vpnaccess-AD-CA	12/6/2011 <non< td=""><td>e></td><td></td><td></td><td></td></non<>	e>			
demo	demo	4/25/2110 <non< td=""><td>e></td><td></td><td></td><td></td></non<>	e>			
			· · · ·			
			Castificate Connet	Minned		
			certificate export	wizaru		
			File to Export			
			Specify the name	e of the file you want	to export	
,						
Import Expor	t Remove		Ele name:			
Import Expor	t Remove		File name:	ser of		Brourse
Import Expor	t Remove		File name: C:\WCP\demo_i	user.pfx		Browse
Import Expor Certificate intended purp Microsoft Trust List Signi	t Remove	Secure Email, Client	File name: C:WCP\demo_	user.pfx		Browse
Import Expor Certificate intended purp Hicrosoft Trust List Signi Authentication	t Remove	Secure Email, Client	File name: C:WCP\demo_	user.pfx		Browse
Import Expor Certificate intended purp Microsoft Trust List Sign Authentication	t Remove	Secure Email, Client	File name: C:WCP\demo_	.ser.pfx		Browse
Import Expor Certificate intended pury Microsoft Trust List Signi Authentication	t Remove	Secure Email, Client	File name: C:\VCP\demo_i	user.pfx		Browse
Import Expor Certificate intended pur Microsoft Trust List Signi Authentication	t Remove	Secure Email, Client	File name: C:\WCP\demo_i	user.pfx		Browse
Import Expor Certificate intended purp Vicrosoft Trust List Signi Authentication	t Remove	Secure Email, Client	File name: C:WCP\demo_	iser.pfx		Browse
Import Expor Certificate intended pury Norosoft Trust List Sign Authentication	t Remove	Secure Email, Client	File name: C:WCP\demo_i	.ser.pfx		Browse
Import Expor Certificate intended pury Microsoft Trust List Signi Authentication	t Remove	Secure Email, Client	File name: C:WCP\demo_d	user.pfx		Browse
Import Expor Certificate intended pury Norosoft Trust List Signi Authentication	t Remove	Secure Email, Client	File name: C:\VCP\demo_	.ser.pfx		Browse
Import Expor Certificate intended pury Microsoft Trust List Sipri Ruthentication	t Remove	Secure Email, Clent	File name: C:VNCP\demo_	user.pfx		Bronse
Import Exper Certificate intended pury Norosoft Trust List Sign Submittcation	t <u>Remove</u> boses ng, Encrypting File System, <u>btes</u> <u>CK</u> C	Secure Email, Client	Fle name:	iser pfx		Browse
Import Expor Certificate intended pury Worosoft Trust List Sign Withentcation	t Remove	Secure Email, Client	Flé name:	user pfs		Browse
Import Export Certificate intended pury Viccooft Trust List Signi Authentication	t Remove over a conset over	Secure Email, Client	Ple name:	user pfx		Browse
Import Expor Certificate intended pur, Versooft Trust List Signi Authentication earn more about <u>certific</u>	t Remove	Secure Email, Client	File name:	user.pfs		Browse
Import Export Certificate intended pury function through the second surfament caston	t Remove	Secure Email, Client	Ple name:	.ser.pfx		Browse
Inport Expor Certificate intended pury Moreoff Trust Lius Signi Auffentication	t Remove	Secure Enail, Client	File name:	user.pfx		Douse

Select finish to complete the certificate export process





Verify export success



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

NCP Secure Client - Juniper Edition			
Connection Configuration Log View	Help		
Profile:	Connection:		
ScreenDS Demo User Cert			
	Juniper		
Statistics: Data (Tx) in Byte: 0 Time onli Data (Px) in Byte: 0 Timeout	ncp ne: 00:00:00		
Speed (KByte/s): 0.000 Encryptic	on:		
Certificates		×	
Certificate configuration			
Name	User Certificate		
Standard certificate configuration	None		
Demo User Cert	PKLS#12 he		
	Certificates		×
	Name: Demo User Cert		
	User Certificate PIN Policy C	ertificate Renewal	
Add E dit	Certificate:	from PKCS#12 file	•
	Select Certificate:	1	
	PKCS#12 Eilename:	C:\NCP\demouserceit.p12	
	🔲 Enable Certificate S	Selection	
	Certilicate Path:		
	PIN Request at each Co	nnection	
		Help OK.	Cancel



Select certificate in the NCP Client Connection Profile

NCP Secure Client - Juniper Edition	Profile	_ 🗆 ×
Connection Configuration Log View Help	Available Profiles	
Profile: Connection:	Group:	
ScreenOS Demo User Cert	Show all profiles	▼ Group
	[<u></u>	
JUNIPER	Juniper Junos VPN - Backup	
	Juniper Password	11
	Junos AD	
NCO	Junos VPN Radius	
IICP	NS MIP	
Statistics: Data (Tx) in External On Time online: 00:00:00	ScreenUS Demo User Cert	
Data (Rx) in Byte: 0 Timeout (sec): 0 sec	Add / Import Edit Copy Delete	Export
Speed (KByte/s): 0.000 Encryption:		
Profile Settings ScreenOS Demo User Cert	Help	OK. Cancel
Rasis Callings		
Line Management Local Identity (IKE)		
Advanced IPsec Options	ASN1 Distinguished Name	
D: IPsec Address Assignment		
Spit Tunneing Pre-shared Key Certificate Check		
Shared Ser	net	
Confirm Se	cret	
configuratio	n: Demo User Cert	
Extended Auther	tication (XAUTH)	
👧 🛄 ser ID:		
Password:		
	Help DK Cancel	

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

Ssg5-v92:Juniper-ScreenOS 6.3.0r	1.0 - Windows Internet Explorer		- 0 ×
C C + http://10.20.10.212/ro	nebul.html	💌 🗟 😽 🗙 🔎 Bing	P •
🔆 Favorites 🛛 🌼 🎦 ssg5-v92Juniper-	ScreenOS 😰 Microsoft Active Directory C		
🔠 🔹 🎦 ssg5-v92:Juniper-Screen 🗙	Hicrosoft Active Directory C	han - 🔂 - 🖄 👘 - Page - Safety - To	ols • 🔞 •
	Objects > Certification > Cert New Request	ssg5-v92	2
Juniper			
	Certificate Subject Information		
Home	Name:	VPN Users	
Network	Phone:		
Security Policy	Unit/Department:		
VPNs	Organization:	VPN Access	
AutoKey IKE AutoKey Advanced	Country and the	Macanhain Marco	
Gateway	County/Locality:	mountain view	
P1 Proposal P2 Proposal	State:	California	
- XAuth Settings	Country:	US	
MODECFG Profile	E-mail:		
Manual Key	IP Address:		
Monitor Status	FQDN:	vpnaccess.local	
Objects Users	Key Pair Information:		
Local Local Groups External Groups IP Pools Certificates	RSA Create new key pair of 2048 v length.	C DSA C ECDSA	
Reports		Generate Cancel	
System Log Vent Self Asset Recovery Counters Chassis Interface Bandwidth Policies			
Done		👘 🍾 🗸 Trusted sites Protected Mode: Off	100% • //.

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



7' / **1**

		1.1				
ssg5-v92:Juniper-ScreenOS 6.3.0r	r4.0 - Windows Internet Explorer					_ 🗆 ×
					(A De out	
👷 Favorites 🛛 😪 🏠 ssg5-v92Juniper	-ScreenOS 🐔 Microsoft Active Director	ry C				
ssg5-v92:Juniper-ScreenOS 6.3.0r4.0					🐴 • 🖾 - 🗆 🛞 • Page • Sa	ifety + Tools + 😧 -
	Objects > Certification > Cert R	equest			ssg5-v	92 ?
Juniper'	Costificate Request	:				
Home Storey Home Active Configuration Network Security Policy VPIN Autokey KE Autokey Advanced - Gateway	Certificate Request H43TU3 begin T00/ms by 5506 11 yehr CK1A18T03 20 Damba CS40515 3DQE:D010A4 11AQC CS405153DQE:D010A4 11AQC CS405453132Db 2007 CS4054545 CS4054545 CS4054545 CS405454 CS	2X10CYY7N9hnkhY11 2X70QW3YuCM21MkkV xGgYDVR0RBBNwEY1Pd DirKLJochngk92ROAN 0%oofpkcs10.bd from 10	oyAF7Gy+VniLgmKXBo j5K17KKReV532sCAwb nBuYWNj2XNzLmxVY2E G+RuSTpY190PHpqK51 N20.10.212 Completed Save As	IAAAA IAAAA IAAAA IEZkuc Litt X uter + Local Disk (C:) + NCP	• 🕼 Search IIC?	×
P1 Proposal P2 Proposal Xouth Settings VPN Groups WODECFG Profile Manual Koroups LIZTP Montor Status Objects Users Local Local Local Costlicates Poolog Poolog RPools Report Report	Save To File Generate Self Signed C C E-mail to: Automatically enroll to C New CA server sett Advanced Se C Existing CA server 3	_peak bet from (b, d, i)) Estimated time (eff. Transfer risk: ▼ Close the datag box wh CA CGI CA IDENT Challenge Ettings	Organize New folde Fevorites Fevori	Tane -	Dett modified	III • 0
System Log Event Self Asset Recovery Counters Chassis Interface Bandwidth Policies	1	ОК	File name: Save as type: Te	g_cert_ploss0.txt	Save	× × Cancel
Done				Trus	ted sites Protected Node: Off	A • ■ 100% • //

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



NCP Client with Juniper ScreenOS

Microsoft Active Directory Certificate Services - Windows Internet Explorer		_0
🔊 🗢 🖉 http://192.168.66.11/certary/certrq:t.asp	🗾 🖻 😽 🗙 🔎 ling	9
Pavorites 🙀 🎦 ssg5-v92Juniper-ScreenOS 🙋 Microsoft Active Directory C		
🔹 🜇 ssg5-v92: tunper-ScreenOS 🖉 Microsoft Active Director 🗙	han - 🖾 - 🖄 - Page - Sa	ifety - Tools - 😯
Microsoft Active Directory Certificate Services - vonaccess-AD-CA		Home
submit a Certificate Request or Renewal Request		
o submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certif s a Web server) in the Saved Request box.	icate request or PKCS #7 renewal request generated by an external	source (such
aved Request:		
B8X-0486451120147010000000000000000000000000000000		
ertificate Template:		
Web Server		
dditional Attributes:		
Attributes:		
Submt >		
	The stand sizes Destanded blocks Off	C

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



Icrosoft Active Directory Certificate Services - Windows Internet Explorer		-0
() • (c) Http://192.168.66.11/certarv/certoarc.asp	🔳 🖶 😽 🗙 🖓 Bing	P -
avorites 🙀 🎦 ssg5-vH2Juniper-GoreenOS 🙋 Microsoft Active Directory C		
* Ssg5-/92:Junper-ScreenOS C Marcosoft Active Director 🗴	🤷 • 🔯 - 🖄 👘 • Page	• Safety • Tools • 😥 •
icrosoft Active Directory Certificate Senices - vpnaccess-AD-CA		Home
ownload a CA Certificate, Certificate Chain, or CRL		
trust certificates issued from this certification authority, install this CA certificate chain.		
download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.		
certificate:		
Ourrent (vpnaccess AD CA)		
coding method:		
e DER C Bara 64		
wnload CA certificate		
wnload CA certificate chain		
whibad latest delta CRL		

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

🖉 ssg5-v92:Juniper-Screen05 6.3.0r4.0 - Windows Internet Explorer		🚰 ssg5-v92:Juniper-Screen05 6.3.0r4.0 - Windows Internet Explorer	
G 🕢 🗢 🞦 http://10.20.20.212/rewebui.html	E 🕂 X 🖓 ling 🖉 🖉	🚱 💿 💌 http://10.20.30.212/newebui.html	B 4 × P ing P
👷 Feverites 🛛 🙀 🎦 sig5-v923unper-ScreenOS 🙋 Microsoft Active Directory C		👷 Favorites 🛛 🙀 🌇 ssp5-v923.niper-ScreenOS 🙋 Microsoft Active Directory C	
😥 🔹 🌇 sog5-v92:Juniper-Screen 🗙 🍎 Microsoft Active Directory C	🏠 + 🖸 - 🖃 🛞 + Page + Safety + Tools + 😥 +	😥 🔹 🌇 sag5-v92: Juniper Goreen 🗙 🍎 Morosoft Active Directory C	🦓 + 🔂 - 🔤 🛞 - Page - Safety + Toole - 😥 -
Objects > Certificates	ssg5-v92 ?	Objects > Certificates	ssg5-v92 ?
Load C cert @ CRL File: C:\NCP\CA_crl.crl Browse	Load	Load @ Cert C CRL File: B	irowse Load
Show Local Show Local Strong	New	Show CA	New
S & GATWORK F		E garmene F	
SSO5-492 Issuer Friendly Name Type	Serial# Expired Status Configure	SSO5-102 Issuer Friendly Name Type	Serial# Expired Status Configure
Home vpnaccess-AD-CA S1 LOCAL 208adS	660000000001d 12-19-2012 19:49 Active Detail, Remove	Home Vpnaccess-AD-CA 48 CA 3e5437	79012ce39c44eda57376be2b1a 10-22-2015 21:01 Active Detail.Remove
Configuration Network		Configuration vpnaccess-AD-CA CRL CRL	00000000000000 12-25-2010 09:31 Active Detail.Remove
E Security		Security	
VPNs		VPNs	
AutoKey IKE		AutoKey IKE	
Gateway		Gateway	
P1 Proposal P2 Proposal		P1 Proposal P2 Proposal	
- XAuth Settings		XAuth Settings	
VPN Groups MODECEG Profile		VPN Groups MODECEG Profile	
Manual Key		Manual Key	
L2TP Monitor Status		Monitor Status	
 Objects 		Objects	
Users		Local	
- Local Groups		Local Groups	
External Groups		IP Pools	
Certificates		Centificates	
Reports System co		 System Log 	
Event		Event	
Self Asset Recovery		Asset Recovery	
Counters		Counters	
Interface Bandwidth		Interface Bandwidth	
Policies -		Policies	
2	The state of the s		Trusted sizes Destanted Made: Off

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	-10
00008001> 10.20.10.111 500 esp:a128/sha1 2af2bfe8 2180 unlim A/D -	10
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	-10
00008002> 10.20.10.111 500 esp:a128/sha1 beeb3607 2186 unlim A/D	-10
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->
```



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 000000a< 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I -1 0 000000a> 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I -10 00000011< 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I 2000000011> 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I 30 000000f< 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I 50 000000f> 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I 60 00008004< 10.20.10.111 500 esp:a128/sha1 bbb2337a 3548 unlim A/D -10 00008004> 10.20.10.111 500 esp:a128/sha1 328abb5f 3548 unlim A/D -10 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I -1 0 00000012< 00000012> 0.0.0.0 500 esp:a128/sha1 00000000 expir unlim I/I -10 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 -10 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-> undebug 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_sanity_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 = 4/3/0x1Permitted 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 sanity 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 = 4/3/0x1Permitted by policy 4 No src xlate choose interface bgroup0 as outgoing phy if ssg5-v92-> unset ffilter filter 0 removed ssg5-v92-> undebug 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