Securepoint Security Systems

Version 2007nx Release 3



•O• SECUREPOINT

Contents

1	Con	figuration of the appliance	4
	1.1	Setting up network objects	4
	1.2	Creating firewall rules	7
	1.3	Setting up certificates	9
	1.4	IPSec configuration1	4
	1.4.	1 Configuration with the assistant1	4
	1.4.	2 Configuration using the layer view1	7
2	Con	figuration of the VPN client 'The GreenBow' under Windows2	4

VPN with IPSec and roadwarrior (GreenBow VPN client))

A VPN connects one or several computers or networks by using a different network, e. g. the internet, as a means of transport. For instance, this could be the computer of a member of staff at their home or in a subsidiary which is linked to the network at the headquarter through the internet.

For the user, the VPN looks like a normal network connection to the destination computer. The actual way of transmission is not perceived. The VPN provides the user with a virtual IPconnection which is tunneled by an actual one. The data packages transmitted via this connection are encoded at the client and decoded by the Securepoint servers - and the other way around.

Target: Setting up a VPN with IPSec between the Securepoint appliance and a roadwarrior (VPN-Client).



fig. 1 VPN layer

1 Configuration of the appliance

1.1 Setting up network objects

The first step is to create a number of network objects. In this example the roadwarriors were set up as individual objects and moved into the group "Grp-roadwarrior". They may also be bundled in a subnet (192.168.31.0/24). This is useful when all roadwarriors always have the same privileges. In that case an exact identification as described in section (A) would not be necessary. A configuration as in section (B) would be sufficient.

4 computers and 3 computer groups are created:

Computer group	Computer	Meaning
Grp-external-interface	external-interface	The external firewall interface.
Grp-internal-net	internal-net	The internal net
Grp-roadwarrior	Roadwarrior01	The roadwarriors (VPN clients).
	Roadwarrior02	

Proceed as follows:

> Over *Firewall* select the tab *Network-objects*. Click on the button *Computer*.

Two possibilities are presented to you here. If you have a permanent IP-address, continue with A (permanent IP-address). In the case of dynamic IP-addresses continue with B (dynamic IP-addresses).

Section A permanent IP-address

The IP is inserted, therefore the bitcount 32 has to be (= Host). The zone is firewallexternal. A symbol has to be selected in the group Grp-external-interface.

ᅌ Securepoint 2007n	x R3 Build 38 - [Firewal	11]					_ 2 🛛
🖕 Configuration Firewall	Applications VPN Network	k Extras Windows Info					_ 8 ×
Save Rule update	irewall Applications VPN	Network Authenticatio	n Report Life	Beload N	etwork Tools		
🎢 🛒 🧖 🕅	Rules Static N	IAT Hide NAT QoS Se	vices Network objects				
firewall.foo.loca	Computer	Group Modify Delete	Filter value	Reset View			
	Computer in c	omputer group Avai	lable computer:				
	🗄 🜍 internet	Na	me	IP address/Login	Mask	Sector	Static NAT
			any	0.0.0	U	external	
	Add computer		X	Add com	outer group Name o	p f group	
				Ext	Grp-ext	ernal-interface	
	Name	external-interface		A			
	IP address	223.23.13.1					
	Mask	Host 🔽					
	Sector	firewall-external 🛛 🗸					
	Static NAT		-	010 08		V3 V3 V3 V3	N
	Group	Grp-external-interface	-				2
				a *			
		OK Cancel		📦 📦	800	0 🛎 💼 🔂 🗸	U
				8	4		
					OK	Cance	
a Firewall					<u></u>		
R3b2 (5409) Connected t	o: firewall.foo.local	admin Run	ning Config: wizard				

fig. 2 external interface with permanent IP-address

Section B dynamic IP-address

If a permanent IP does not exist, but a dynamic DNS service (dyn-DNS) is used, the interface has to be set up with the IP 0.0.0.0 and the mask 0.



fig. 3 external interface with dynamio IP-address

Now set up the internal net and the roadwarriors in the way shown. The first roadwarrior here receives the IP 192.168.31.1. The second roadwarrior receives the IP 192.168.31.2.

Add network	
Name	internal-net
IP address	10.1.2.0
Mask	24
Sector	internal 🗸 🗸
Group	Grp-internal-net
	OK Cancel

fig. 4 internal net

Add computer	
Name	roadwarrior02
IP address	192.168.31.2
Mask	Host 🔽
Sector	vpn-ipsec 🔽
Group	Grp-roadwarrior 💌
(OK Cancel

fig. 6 roadwarrior02

The result is shown in fig. 7.

Computer Group Modify	Delete.	Reset View	•		
omputer in computer group	Available computer:				
∎ 🕥 internet	Name	IP address/Login	Mask	Sector	Static NAT
🗄 🖷 Grp-external-interface	 any 	0.0.0.0	0	external	
🛛 🗛 Grp-internal-net	🐖 external-interface	223.23.13.1	Host	firewall-external	
🗠 🚳 Grp-roadwarrior	🛃 internal-net	10.1.2.0	24	internal	
	🔎 roadwarrior01	192.168.31.1	Host	vpn-ipsec	
	🔎 roadwarrior02	192.168.31.2	Host	vpn-ipsec	

fig. 7 result of setting up network objects

Add computer	
Name	roadwarrior01
IP address	192.168.31.1
Mask	Host 🗸
Sector	vpn-ipsec 🗸
Group	Grp-roadwarrion
	OK Cancel

fig. 5 roadwarrior01

1.2 Creating firewall rules

Proceed as follows:

Over Firewall select the tab Rules and create the firewall-rules as shown in the images.

Only two rules are needed. The first rule enables the external computers to create an IPSecconnection to the external interface of the appliance.

襘 Securepoint 2007nx R3	Build 38 - [Firewall]	- - X
🎃 Configuration Firewall App	olications VPN Network Extras Windows Info	_ 8 ×
Save - Carlos Firewal	Applications VPN Network Authentication Report Life Reload	
1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Rules Static NAT Hide NAT QoS Services Network objects	
firewall foo. local	🍓 New rule 📃 🗖 🔀	
	Rules Time schedule Remark	
	From computer group To computer group Service group Action	Time QoS
	OK Cancel	×
🔏 VPN connecti à Firewall		
R3b2 (5409) Connected to: fir	rewall.foo.local admin Running Config: wizard	

fig. 8 firewall rule internet

The second rule enables the roadwarrior to fully access the internal network.

🖕 New rule	🖕 New rule 📃 🗖 🔀							
Rules Time schedule Remark]							
From computer group	To computer group	Service group	Action					
🚚 Grp-external-interface	Grp-external-interface	administration any	ACCEPT 💌					
Grp-roadwarrior	Cirp-roadwarrior	default-internet dns ipsec mail netbios	Activated					
roadwarrior01	internal-net	ntp openvpn any	QoS					
	M							
			OK Cancel					

fig. 9 firewall rule roadwarrior

> In order to complete this step perform a rule update to activate the rules.

ѝ Securepoint 2007nx R3 Build	38 - [[Firewall]							
🖕 Configuration Firewall Application	s VPN	Network Extras Windows	info						_ @ X
Save Rule update	e plications	VPN Network Av	thentication	Life Reload	Network] Tools			
firewall.foo.local	Rules	Static NAT Hide NAT Qc	S Services Network obje	ects	Sea	arch			
	ID	From computer group	To computer group	Service group	Action	Activated	Log Time	QoS	^
	17	 internet 	🖷 Grp-external-interface	ipsec	Gocept	0			
	18	る Grp-roadwarrior	🛵 Grp-internal-net	any	Gccept	0			
	<								>
VFN connecti a Firewall									
R3b2 (5409) Connected to: firewall.fr	oo.local	admin	Running Config: wizard						

fig. 10 firewall rule update

1.3 Setting up certificates

Proceed as follows:

> Over VPN select the tab Certificates.



fig. 11 VPN tab certificates

First the certification authority (CA) has to be established with which the server certificate and the client certificates for the roadwarriors are signed. Therefore, the first step is to create a root certificate.

- > Click on the icon New and select Root certificate.
- > Insert the data in the way shown in the following image.

server certificate client certificate				
1024 V 1/ 1/2000 V 5/29/2018 V	12:00:00 AM 🛟 11:59:59 PM 🛟			
myCA GERMANY	v			
NDS				
Securepoint				
Support support@securepoint.de				
	2			
	client certificate			

fig. 12 creating a root certificate

When you click on OK the dialog is shown again to setting up a client or server certificate.

After a CA has been created, server- and client-certificates may be generated. One server is needed as well as one client-certificate for each roadwarrior. These certificates only have to differ in their names.

- Select User / server certificate.
- Insert the data as shown in the following image. The most fields are already set with the data from the root certificate.

Certificates 🛛 🔀						
Creating ce User / se Root cer OpenVPI OpenVPI OpenVPI	rtificate for firewall.foo.local erver certificate tificate N server certificate N client certificate					
Key length Earliest validity date Latest validity date Designation Land State City Organisation Organisation unit Email CA	1024 ▼ 1/ 1/2000 12:00:00 AM 5/29/2011 11:59:59 PM fw.foo.local GERMANY ▼ NDS Lueneburg Securepoint support@securepoint.de ▼ me					
O IP O Host nan O Email						
	OK Cancel					

fig. 13 creating server certificate

Afterwards, client-certificates are needed.

- > Select User / server-certificate.
- > Insert the data as shown in the following image.

Certificates		Certificates	×
Creating certil User / serv Root certific OpenVPN s OpenVPN s	ficate for firewall.foo.local er certificate cate server certificate client certificate	Creating certif User / servi Root certific OpenVPN s OpenVPN c	icate for firewall.foo.local er cettificate sate erver cettificate slient cettificate
Key length Earliest validity date Latest validity date Designation Land State City Organisation Organisation unit Email CA Alternative X509v3 name Q IP Q Host name Q Email	1024 1/ 1/2000 5/29/2011 11:59:59 PM roadwarrior01 GERMANY NDS Lueneburg Securepoint Support support@securepoint.de myCA	Key length Earliest validity date Latest validity date Designation Land State City Organisation Organisation unit Email CA Alternative X509v3 name O IP O Host name O Email	1024 ▼ 1/ 1/2000 12:00:00 AM 5/29/2011 11:53:59 PM roadwarrior02 GERMANY MDS Lueneburg Securepoint Support support@securepoint.de ▼ myCA ▼
	OK Cancel		OK Cancel

fig. 14 roadwarrior01 certificate

- fig. 15 roadwarrior02 certificate
- > Click Cancel on the new dialog to finish the certificate creation.

After creating the client-certificate, now export the certificates for usage on a roadwarrior.

> Click on the icon *Export* and select the data type that you want.

Depending on the destination system, you have to choose whether the certificates are to be saved in the standard format (.pem) or in the Personal Information Exchange Syntax (.p12). PKCS#12-files are given a password.

> In the following step the certificate can be stored locally.

😫 Securepoint 2007nx R3 Build 38 - [VPN connections]			
늘 Configuration Firewall Applications VPN Network Extras Window	rs Info		
Save Rule update Firewall Applications VPN Network A	withentication Report	Reload Network Tools	
Martificates 🛛 🕅 🕅 🕅 🕅			
Firewall foo.local	Addify Delete Import CRL Export CR	L Delete CRL	
E CAS	Certificate road Name of issuer myC	warrior01 A	
Cetts Revoked	Country DE State NDS City Luen Organisation Secu Organisation unit Supp Email address supp	eburg repoint ort ort@securepoint.de	
Export X	Valid from Satu Valid until Suno	rday, 1. January 2000, 00:00:00 Jay, 29. May 2011, 23:59:59	
Standard	ID	Name	Validity Type
• pkcs #12	♀ firewall.foo.local_3 ♀ firewall.foo.local_4	fw.foo.local roadwarrior01	OK Cert OK Cert
Password unsecure	♀ firewall.foo.local_5	roadwarrior02	OK Cert
OK Cancel			
	<		
a Firewall 🔏 VPN connections			
R3b2 (5409) Connected to: firewall.foo.local admin	Running config: ipsec		

fig. 16 export certificate

1.4 IPSec configuration

This configuration can be conducted in two different methods. Either through a assistant guided configuration or a manual configuration based on a drawing layer.

1.4.1 Configuration with the assistant

Proceed as follows:

- > Click the icon VPN and select the tab VPN connections.
- > Click the icon *New*. The *IPSec Wizard* appears.
- Select *Roadwarrior* and click *Next*.

2 Securepoint 2007nx R3 Build 38 - [VPN connections]	×
Configuration Firewall Applications VPN Network Extras Windows Info 📃 🖻	\times
Image: Save Filework Image: Save Image:	
I PN connections Certificates	
Firewall foo.local	
📄 🖬 IPSec Wizard	~
Creating a new IPsec connection	
Which kind of connection do you want to create?	
Site to Site (Connecting two Firewalls)	
Connecting a Notebook with the Firewally	
	~
Thewaii VPN connections Next Cancel	_
December 2010 Connected of Incrementoring	

fig. 17 IPSec Wizard - step 1

Select Native IPSec and click Next.

🍁 IPSec Wizard								
reating a new IPsec connection Roadwarrior								
Is it a native IPsec connection (for example with the Greenbow VPN client) or a L2TP connection (for example, with Microsoft L2TP client)?								
 Native IPsec ► L2TP 								
Back Next	Cancel							

fig. 18 IPSec Wizad - step2

- Enter a name for the connection.
- Select Certificate as authentication method and select the roadwarrior01 certificate out of the dropdown list.

🎃 IPSec Wizard								
Creating a new IPsec connection Roadwarrior								
please specify the name and IP addre Which class of authentication do you	ess of the Roadwarrior. want to use?							
Name of the connect Preshared Key Certificate	ior roadwarrior1							
	Back	Cancel						

fig. 19 IPSec Wizard - step 3

- > Enter the local net that the roadwarrior is entitled to access.
- > Allocate a permanent tunnel IP-address.
- > Complete the configuration by clicking the *Finish* button.

🍘 IPSec Wizard								
Creating a new IPsec connection Roadwarrior								
Which subnet may the user access	and what is his IP address in the tunnel?							
Local Net / Mask	10.1.2.0							
Tunnel IP address	192.168.31.1							
	Back	iish Cancel						

fig. 20 IPSec Wizard - step 4

- > The result of the configuration is shown in fig. 21.
- Repeat the procedure for the second roadwarrior.
- > At last you have to update the connections. Click onto the icon Update.

🎃 Securepoint 2007nx R3 Build	d 38 - [VPN connections]	
🙀 Configuration Firewall Application	ns VPN Network Extras Windows Info	a ×
Save Rule update Firewall Ap	Image: Point and the second	
🗃 🚮 🚜 🛜 🛛 🚺	VPN connections Certificates	
firewall.foo.local	New Fint Image: Connect Image: Connect all Imag	
	frewall.foo.local>roadwarrior1 Phase 1 Phase 2 Delete Load Initiate Stop	
		_
		_
		_
		_
		-
		-
		-
		-
		-
		-
		-
	\PSec/	<u> </u>
Erewall Strews		
R 3h2 (5409) Connected to: firewall f	foo.local admin Running.config: ipsec	

fig. 21 result of the configuration - updating the connection

1.4.2 Configuration using the layer view

Proceed as follows:

- > Over VPN select the tab VPN connections.
- > Change to the VPN layer view by clicking onto the icon *View*.
- By using the mouse move the existing firewall-object from the left window onto the VPN viewport.

🎃 Securepo	oint 2007n	c R3 Bu	rild 38 - [VPN connect	tions]								_ @ 🛛
🖕 Configurat	tion Firewall	Applica	tions VPN	Network Ext	ras Windo	ws Info							_ & ×
Save Ru	ile update	irewall	Applications	VPN	Network	Authentication	Report	Life		eload Ne	twork Tools		
1 1 2	2 🔀		VPN co	onnections Cr	ertificates								
firew	vall.foo.local			y 🛄 w View	Print	✓ Text	Connect	O Update	Iist	Connect a	all New laye	Delete layer	
				•/									
à Firewall	1. Sec. 1. Sec	/PN conr	nections										
R3b2 (5409)	Connected to	o: firewa	all.foo.local		admin	Runnin	na confia: ip:	sec					

fig. 22 Draging the firewall symbol onto the VPN layer

- > Now create a new roadwarrior object in the left window.
- > Click on the notebook icon in the toolbar of the left window.
- In the dialog Roadwarrior add the roadwarrior is set up with IP (0.0.0.0), because it may vary all the time!



fig. 23 creating object roadwarrior1

Now move the freshly created roadwarrior object from the left window onto the VPN viewport.



fig. 24 Draging roadwarrior object onto the VPN layer

> Now click on the icon *Connect* and on the roadwarrior object.

A flag appears on the roadwarrior object with the information *Please click on destination object*.

Click on the firewall object.

VPN connections	Certificates						
New Vie	ew Print	Text Connect	⊘ Update	ist Connect all	New layer	Delete layer	
		_					
Please click	on destination obj						
		roadwarrior		C	firewall.foo.loc	al	
\IPSec/							

fig. 25 connecting objects

Now a new dialog opens automatically: IPSec connection - accept

You may now choose between two ways to proceed:

Procedure A

If a roadwarrior is to be identified exactly, it is recommended to enter the certificate reference. The configured connection will then be assigned to exactly one roadwarrior.

Procedure B

This describes how to set up a configuration for several roadwarriors with a valid certificate.

Procedure A

- In the dialog *IPSec connection accept, General* select the authentication method CERT and the ID-type SUBJECT. In a default case further settings can simply be adopted.
- In the tab *firewall.foo.local* select the server certificate and confirm your entries with OK.

1	PSec cor	nnection - ac	cept		×
	General	firewall.foo.local	roadwarrior1	Subnet	
	Denon Metho	nination d	firewall.foo.l C to F	ocal>roadwarrior1	
	Auth. r	neth.	CERT		~
	ID type	•	SUBJECT		×
	Key life	•	8		~
	IKE life	•	1		~
	PFS		yes		~
	Keying	tries	1		~
	IKE (P	hase 1)	3des-sha		~
	ESP (F	Phase 2)	3des-sha1		~
	DH Gr	oup	1024		~
	Only p encryp	ermit this tion			
			OK	Car	ncel

fig. 26 IPSec connection - tab General

IPSec connection - acc	cept	×
General firewall.foo.local	roadwarrior1 Subnet	
Local gateway	defaultroute	
Route over		
Local gateway ID	×	
Local key		
Local certificate	fw.foo.local 🗸 🗸	
Remote host/gatew.	any	
DynDns Name		
Remote host/gatew. ID	pport/CN=fw.foo.local/email4d 🗸	-
Remote key		1
Start automatically	yes 🗸	
	_	
Dead peer Detection		
	OK Cancel	

fig. 27 IPSec connection - tab firewall.foo.local

After clicking *OK* the tab *Subnet* is displayed. You have to configure the subnet which regulates the routing between the roadwarrior and the internal net. The subnet for a roadwarrior consists of one single IP (bitcount 32).

- > Click on the icon New. The dialog IPSec subnet appears.
- > Enter the subnets and click OK.

IPSec connection - accept									
General firewall.foo	General firewall.foo.local roadwarrior1 Subnet								
New Delete	:		- I	_					
firewall.foo.local	Mask	roadwarrior1	Mask 🖉						
			_						
			_						
U		1							
		OK	Cancel						

Connection	firewall.fo	oo.local>roadwarrior1
irewall.foo.local		
Su	bnet	10.1.2.0
Ma	ask	24
oadwarrior1 —	iubnet	192.168.31.1

fig. 29 enter subnets

fig. 28 IPSec connection - tab Subnet

- After the configuration you have to update the connections by click on the icon Update (fig. 34).
- In the following step check the status of the services under *Applications* in the tab *Status of services*. For the VPN connection the SERVICE_IPSEC is required (see fig. 35).
- Now copy the certificates that have been created in the section certificates (see 1.3) onto the destination systems.

Procedure B

If "CERT" is chosen as the ID-type, all roadwarriors with a valid certificate can use this connection (if the subnet-configuration is compatible).

- > Select the ID type CERT on the tab General.
- > On the tab *firewall.foo.local* select the server certificate.

Sec connection - acc	ept	×	IPSec connection - acc	cept
General firewall.foo.local	roadwarrior1 Subnet		General firewall.foo.local	roadwarrior1 Subnet
Denomination	firewall.foo.local>roadwarrior	1	Local gateway	defaultroute 🗸
Method	C to F		Route over	
Auth. meth.	CERT	~	Local gateway ID	· · · · · · · · · · · · · · · · · · ·
ID type	CERT	~	Local key	
Key life	8	~	Local certificate	fw.foo.local
IKE life	1	~	Remote host/gatew.	any
PFS	yes	~	DynDns Name	
Keyingtries	1	~	Remote host/gatew. ID	·
IKE (Phase 1)	3des-sha	~	Remote key	
ESP (Phase 2)	3des-sha1	~	Start automatically	yes 🗸
DH Group	1024	*		
Only permit this encryption			Dead peer Detection	
	ОК С.	ancel		OK Cancel

The advantage of this configuration is that all roadwarrior-IPs can be configured in one single window.

After clicking *OK* the tab *Subnet* is displayed. You have to configure the subnet which regulates the routing between the roadwarrior and the internal net. The subnet for a roadwarrior consists of one single IP (bitcount 32).

- > Click on the icon New. The dialog IPSec subnet appears.
- > Enter the subnets and click OK.

IP:	Sec connection	- accep	t		×
ſ	General firewall.foo	o.local roa	idwarrior1 Subn	et	_
	New Delete				
f	firewall.foo.local	Mask	roadwarrior1	Mask	<u>^</u>
L		1			
			ОК	Cancel	

Connection	firewall.fo	po.local>roadwarrior1
irewall.foo.loc	al	
Subnet Mask		10.1.2.0
		24
oadwarrior1 —	Subnet	192.168.31.1

fig. 33 enter subnets

fig. 32 tab Subnet - click icon New

After the configuration you have to update the connections by click on the icon Update.

🖕 Securepoint 2007nx R3 Build 38 - [VPN connections]	
🖕 Configuration Firewall Applications VPN Network Extras Windows Info	- 8 ×
Save Applications Applicati	
Image: Second	
Toadwarrior1 New View Print Text Connect Update List Connect al New Tayer Delete Tayer roadwarrior1 INEW View Print Text Connect Update List Connect al New Tayer Delete Tayer Text Connect al Interval Text Text Connect al Interval Text Text Text Connect al Interval Text Text Text Text Text Text Text Text	
S VPN connecti	
R3b2 (5409) Connected to: firewall.foo.local admin Running Config: ipsec	

fig. 34 update the connections

In the following step check the status of the services under Applications in the tab Status of services. For the VPN connection the SERVICE_IPSEC is required.

╈ Securepoint 2007nx R3 Build 38 - [Applications]				- 7 🛛
🍟 Configuration Firewall Applications VPN Network Extras	Windows Info			_ 8 ×
Save - Gale update Firewall Replications VPN	work Authentication Report	Life Reload	Network Tools	
🗃 🚮 🔏 💫 🔢 HTTP Proxy Spam Filter	SMTP Gateway POP3 Proxy Vol	P Proxy VNC Proxy ID)S Status of services	
firewall.foo.local Name of service	Condition	Cluster		
service_ope	NSSH 🕝	£ 3		
SERVICE_SEN	DMAIL 🧑	Ō		
SERVICE_DNS		<u> </u>		
SERVICE_POP	3_PROXY			
SERVICE_HTT	P_PROXY 🥝			
SERVICE_VOIF	PROXY 🛛 🙆			
SERVICE_VNC	_PROXY 🛛 🔯			
🍓 SERVICE_DYN	DNS 🛛 🔯			
SERVICE_NTP				
SERVICE_IDS		£3		
SERVICE_L2TF	· 😢			
SERVICE_PPTI	₽ 🚺 🚺			
SERVICE_SPU	VA 🤣			
SERVICE_WEE	ISERVER 🛛 😣			
SERVICE DHC	PD 😰			
SERVICE_IPSE	с 🥪			
SERVICE_OPE	NVPN 🥝			
			Acc	ept values
🚜 VPN connecti 🚳 Applications				
R3b2 (5409) Connected to: firewall.foo.local a	dmin Running Config: ipsec			

fig. 35 checking status of SERVICE_IPSEC

Now copy the certificates that have been created in the section certificates (see 1.3) onto the destination systems.

2 Configuration of the VPN client 'The GreenBow' under Windows

Proceed as follows:

- > Install the GreenBow VPN client on an assigned computer and start the client.
- With GreenBow a new phase 1 is set up by clicking on *Configuration* with the right mouse-button.
- In Phase 1 the IP of the Securepoint Security Appliance as well as the wanted encoding have to be entered first.

🔄 TheGreenBow VPN Client				
File VPN Configuration View	Tools ?			
THEGREENBOW	IDSon VDN Client			
🔑 Console	Phase 1 (Authentication)			
Parameters	Name Securpoint/PN			
😂 Connections	Interface Any			
	Remote Gateway 223.23.13.1 Preshared Key			
	Save & Apply			
VPN ready	Tunnel: 🥑			

fig. 36 create new phase 1

Then the certificate is imported.

> Click on the button *Certificates import*.

The dialog Certificate import opens.

> The p12 file can be imported via *Import*.

After the import you see a string.

- The string under User Certificate has to be marked and copied. This string is needed under P1 Advanced.
- Save your entries with OK.

Certificates Import
6DP
Root Certificate /C=DE/ST=NDS/L=Lueneburg/0=Securepoint/0U=Support/CN
User Certificate upport/CN=roadwarrior01/emailAddress=support@securepoint.de
🗌 User Private Key
Choose below the Certificate location and type:
Certificate from a PKCS#12 file
Import Certificates from a PKCS12 file Import
Ok Cancel

fig. 37 Import dialog - copy the string under User Certificate

> Click on the button *P1 Advanced*.

The dialog Phase 1 Advanced opens.

Phase1 Advanced	i -	
		and a
		639
Advanced featur	86	
📃 Config Mod	e Redund.0	GW
🗌 Aggressive	Mode NA1	T-T Automatic
X-Auth		
🥅 X-Auth Pop	up Lo	ogin 🗌
🔲 Hybrid Mod	e Passw	vord
Local and Remo	ite ID	
	Choose the type of ID:	Set the value for the ID:
Local ID	DER ASN1 DN	 t/CN=roadwarrior01/em
Remote ID	· ·	•
	, -	
		Ok Cancel

fig. 38 Phase 1 - entering copied string

- Here, the type: "DER ANS1 DN" is to be selected as the local ID. The copied string is inserted as the *ID*. Afterwards, a new Phase 2 can be set up.
- Save your entries with OK.

In Phase 2 the network configuration is conducted. The local address is the IP which the roadwarrior receives in the VPN tunnel. The address with which the roadwarrior want to connect is the subnet as has already been entered during firewall configuration.

- > With the right mouse-button click on the created Phase 1 in the left window.
- Create a Phase 2.
- > Insert the information according to the following image.



fig. 39 setting up phase 2

> The tunnel can be opened after a concluding click on Save & Apply.