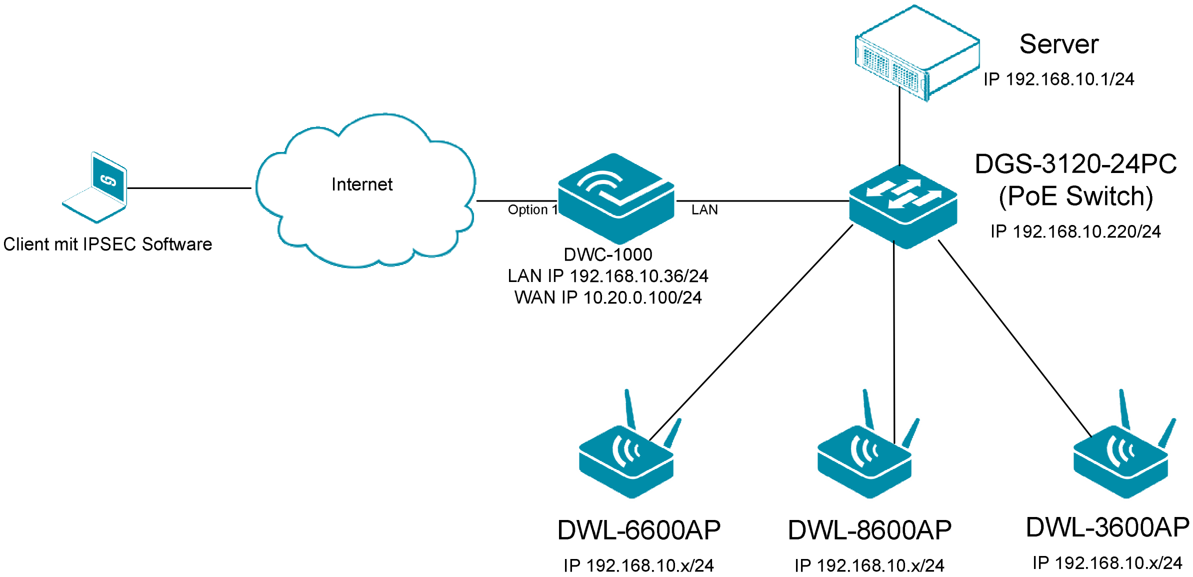
HowTo: Einrichtung einer IPSec Verbindung mit einem IPSEC VPN Client zum DWC-1000 am Beispiel der „Shrewsoft“ VPN Clientsoftware

[Voraussetzungen]

1. DWC-1000 mit Firmware Version: 4.2.0.3_B502 und höher
2. VPN Lizenz

[Szenario]

Ein Client soll sich per „Shrewsoft“ VPN Client mit IPSec auf den DWC-1000 verbinden.



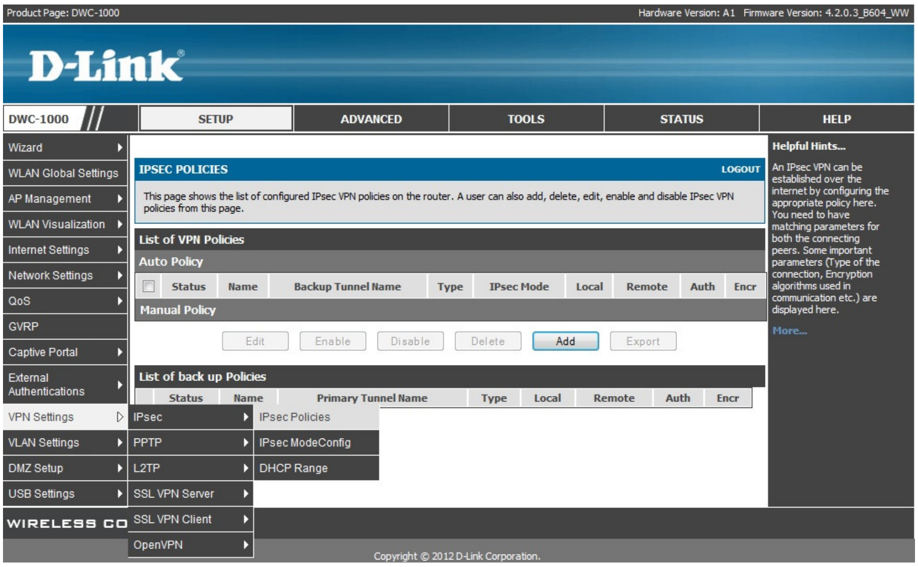
[Vorbereitung]

- ⇨ Der DWC-1000 hat im Auslieferungszustand die Standard IP 192.168.10.1/24 sowie den Benutzernamen „admin“ & Passwort „admin“
- ⇨ Bitte ändern Sie dies bei der Ersteinrichtung (Integration in Ihre bestehende Infrastruktur) des DWC-1000 in Ihrem Netzwerk, für die genaue Vorgehensweise der Einstellung der IP & des Benutzernamens schlagen Sie bitte im Handbuch (ftp://ftp.dlink.de/dwc/dwc-1000/documentation/DWC-1000_HowTo/) nach
- ⇨ Stellen Sie bitte sicher, dass Sie die aktuellste Firmware für den DWC-1000 installiert haben (ftp://ftp.dlink.de/dwc/dwc-1000/driver_software/)
- ⇨ Bitte lesen Sie vorab das Handbuch und die bereits vorhandenen Anleitungen um die grundlegende Konfiguration des DWC-1000 zu erledigen.

- ⇨ Den „Shrewsoft“ VPN Client können Sie unter folgender Adresse herunterladen https://www.shrew.net/
- ⇨ Der „Shrewsoft“ VPN Client ist eine kostenfreie Alternative zu einem NCP-Client

1.) Einrichtung der IPsec Policies
2.) Konfiguration der IPsec Mode Konfiguration
3.) Anlegen einer Benutzerdatenbank
4.) Anlegen eines IPsec Benutzers
5.) Konfiguration des Shrewsoft Client

1.) Einrichtung der IPsec Policies
Öffen Sie die Menüpunkt IPsec Policies:
(>Setup > VPN Settings > IPsec > IPsec Policies:



This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable and disable IPsec VPN policies from this page.

List of VPN Policies

Auto Policy

□	Status	Name	Backup Tunnel Name	Type	IPsec Mode	Local	Remote	Auth	Encr

Manual Policy

List of back up Policies

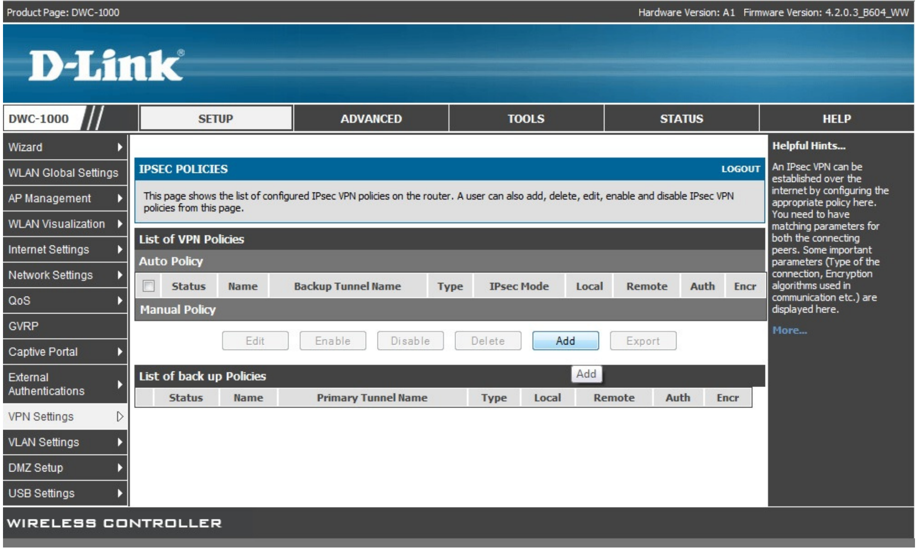
Status	Name	Primary Tunnel Name	Type	Local	Remote	Auth	Encr

Helpful Hints...

An IPsec VPN can be established over the internet by configuring the appropriate policy here. You need to have matching parameters for both the connecting peers. Some important parameters (Type of the connection, Encryption algorithms used in communication etc.) are displayed here.

Copyright © 2012 D-Link Corporation.

Erstellen Sie eine neue Policy über die Schaltfläche „Add“:



This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable and disable IPsec VPN policies from this page.

List of VPN Policies

Auto Policy

□	Status	Name	Backup Tunnel Name	Type	IPsec Mode	Local	Remote	Auth	Encr

Manual Policy

List of back up Policies

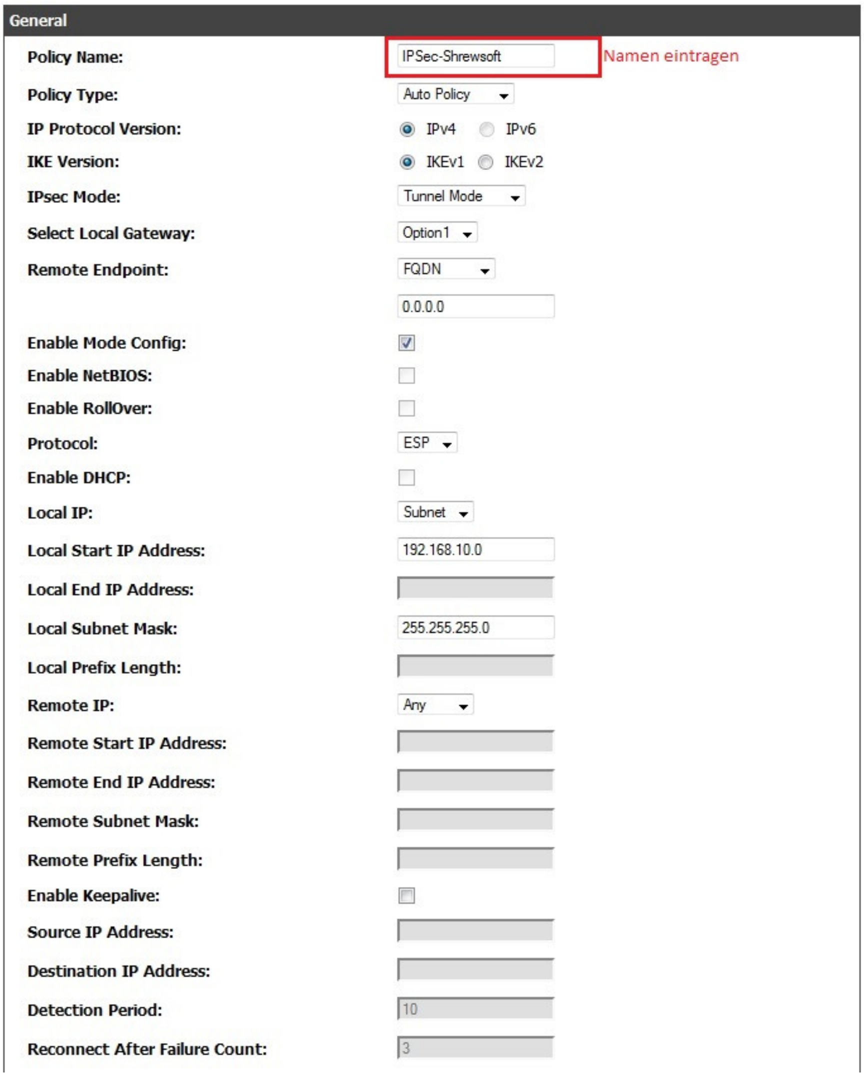
Status	Name	Primary Tunnel Name	Type	Local	Remote	Auth	Encr

Helpful Hints...

An IPsec VPN can be established over the internet by configuring the appropriate policy here. You need to have matching parameters for both the connecting peers. Some important parameters (Type of the connection, Encryption algorithms used in communication etc.) are displayed here.

Konfigurieren Sie die allgemeinen Einstellungen wie folgend:

Vergeben Sie der Policy einen Namen.
Wichtiger Hinweis: Der Policy Name kann nachträglich nicht geändert werden.

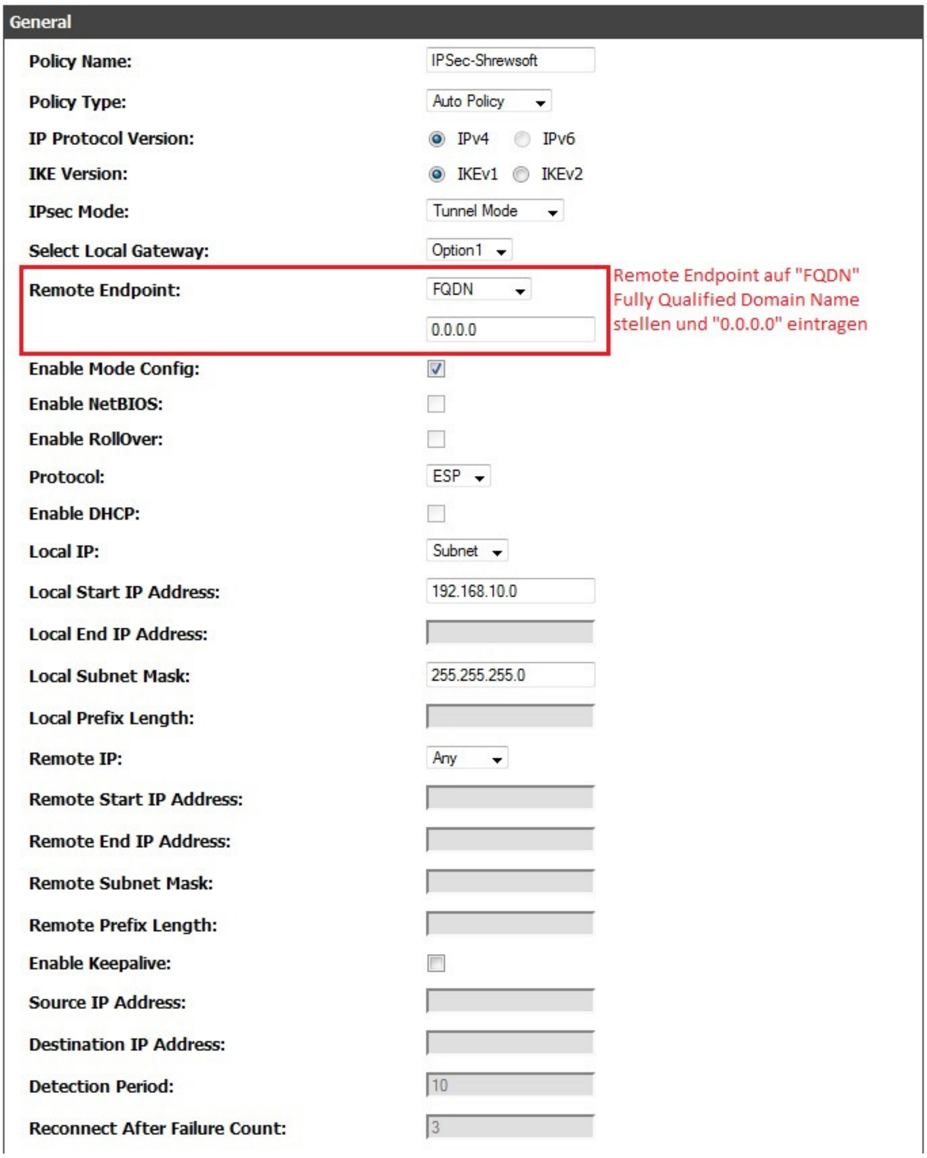


General

Policy Name:	IPSec-Shrewsoft	Namen eintragen
Policy Type:	Auto Policy	
IP Protocol Version:	● IPv4 ○ IPv6	
IKE Version:	● IKEv1 ○ IKEv2	
IPsec Mode:	Tunnel Mode	
Select Local Gateway:	Option1	
Remote Endpoint:	FQDN 0.0.0.0	
Enable Mode Config:	☑	
Enable NetBIOS:	□	
Enable RollOver:	□	
Protocol:	ESP	
Enable DHCP:	□	
Local IP:	Subnet	
Local Start IP Address:	192.168.10.0	
Local End IP Address:		
Local Subnet Mask:	255.255.255.0	
Local Prefix Length:		
Remote IP:	Any	
Remote Start IP Address:		
Remote End IP Address:		
Remote Subnet Mask:		
Remote Prefix Length:		
Enable Keepalive:	□	
Source IP Address:		
Destination IP Address:		
Detection Period:	10	
Reconnect After Failure Count:	3	

Belassen Sie den Policy Type auf: „Auto Policy“
IP Protocol Version auf: IPv4
IKE Version: IKEv1
IPsec Mode: Tunnel Mode
Select Local Gateway: Option 1

Als Remote Endpoint wählen Sie bitte „FQDN“ aus und tragen „0.0.0.0“ ein:

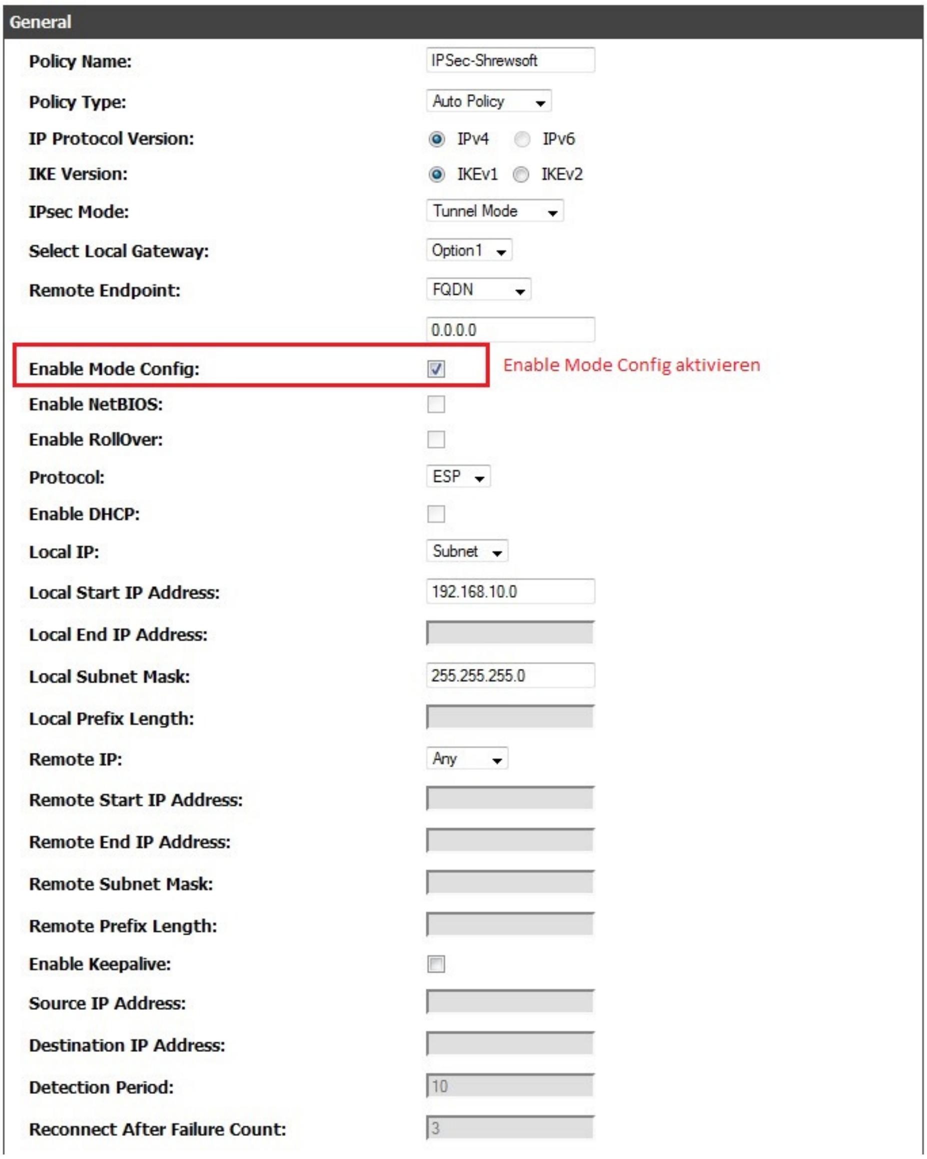


General

Policy Name:	IPSec-Shrewsoft
Policy Type:	Auto Policy
IP Protocol Version:	● IPv4 ○ IPv6
IKE Version:	● IKEv1 ○ IKEv2
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Option1
Remote Endpoint:	FQDN 0.0.0.0
Enable Mode Config:	☑
Enable NetBIOS:	□
Enable RollOver:	□
Protocol:	ESP
Enable DHCP:	□
Local IP:	Subnet
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Any
Remote Start IP Address:	
Remote End IP Address:	
Remote Subnet Mask:	
Remote Prefix Length:	
Enable Keepalive:	□
Source IP Address:	
Destination IP Address:	
Detection Period:	10
Reconnect After Failure Count:	3

Remote Endpoint auf "FQDN"
Fully Qualified Domain Name
stellen und "0.0.0.0" eintragen

Aktivieren Sie „Enable Mode Config“:

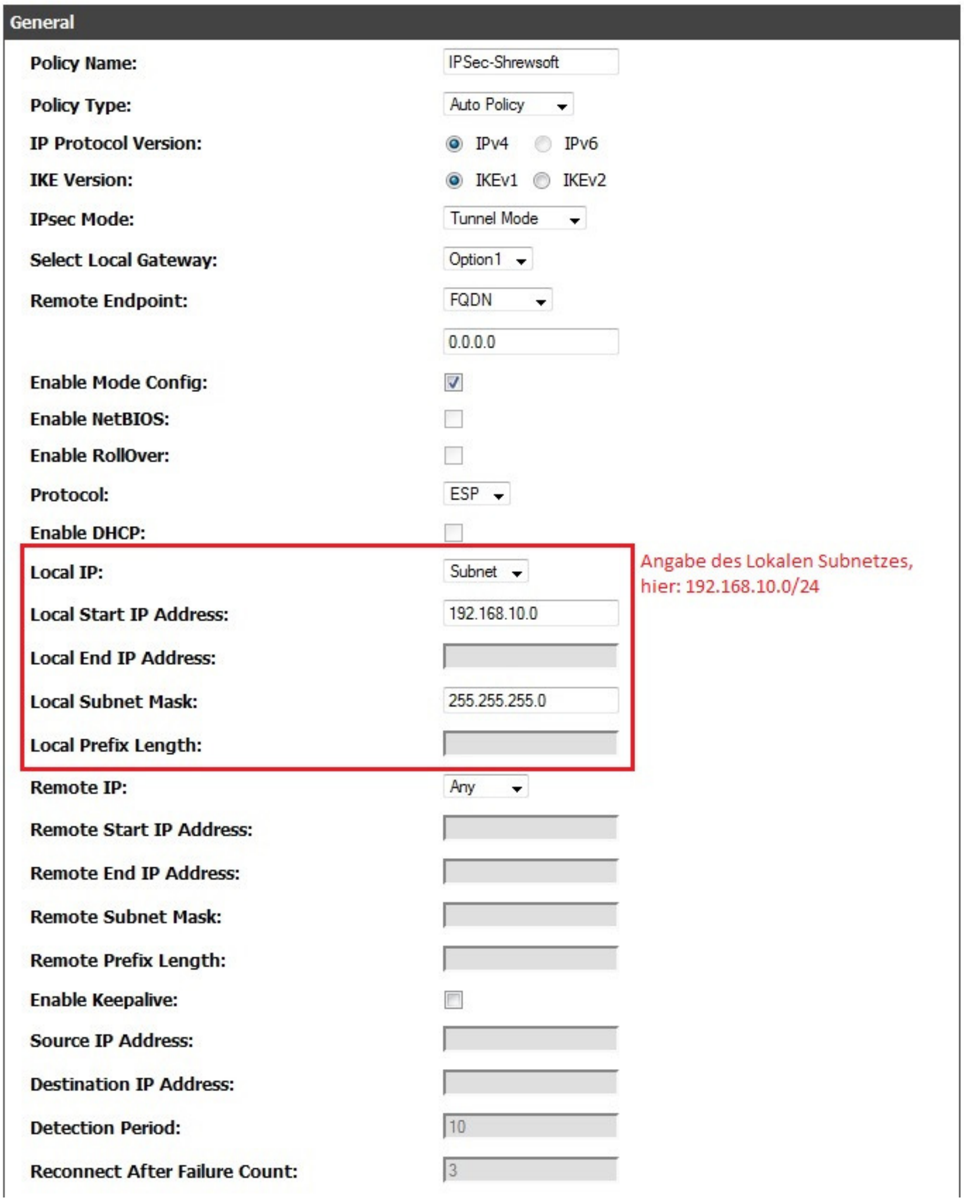


General

Policy Name:	IPSec-Shrewsoft
Policy Type:	Auto Policy
IP Protocol Version:	● IPv4 ○ IPv6
IKE Version:	● IKEv1 ○ IKEv2
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Option1
Remote Endpoint:	FQDN
	0.0.0.0
Enable Mode Config:	☑
Enable NetBIOS:	☐
Enable RollOver:	☐
Protocol:	ESP
Enable DHCP:	☐
Local IP:	Subnet
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Any
Remote Start IP Address:	
Remote End IP Address:	
Remote Subnet Mask:	
Remote Prefix Length:	
Enable Keepalive:	☐
Source IP Address:	
Destination IP Address:	
Detection Period:	10
Reconnect After Failure Count:	3

Enable Mode Config aktivieren

Wählen Sie bitte bei Local IP: „Subnet“,
tragen Sie als Local Start IP Address: „192.168.10.0“ ein,
und als Local Subnet Mask tragen Sie die „255.255.255.0“ ein.(*)



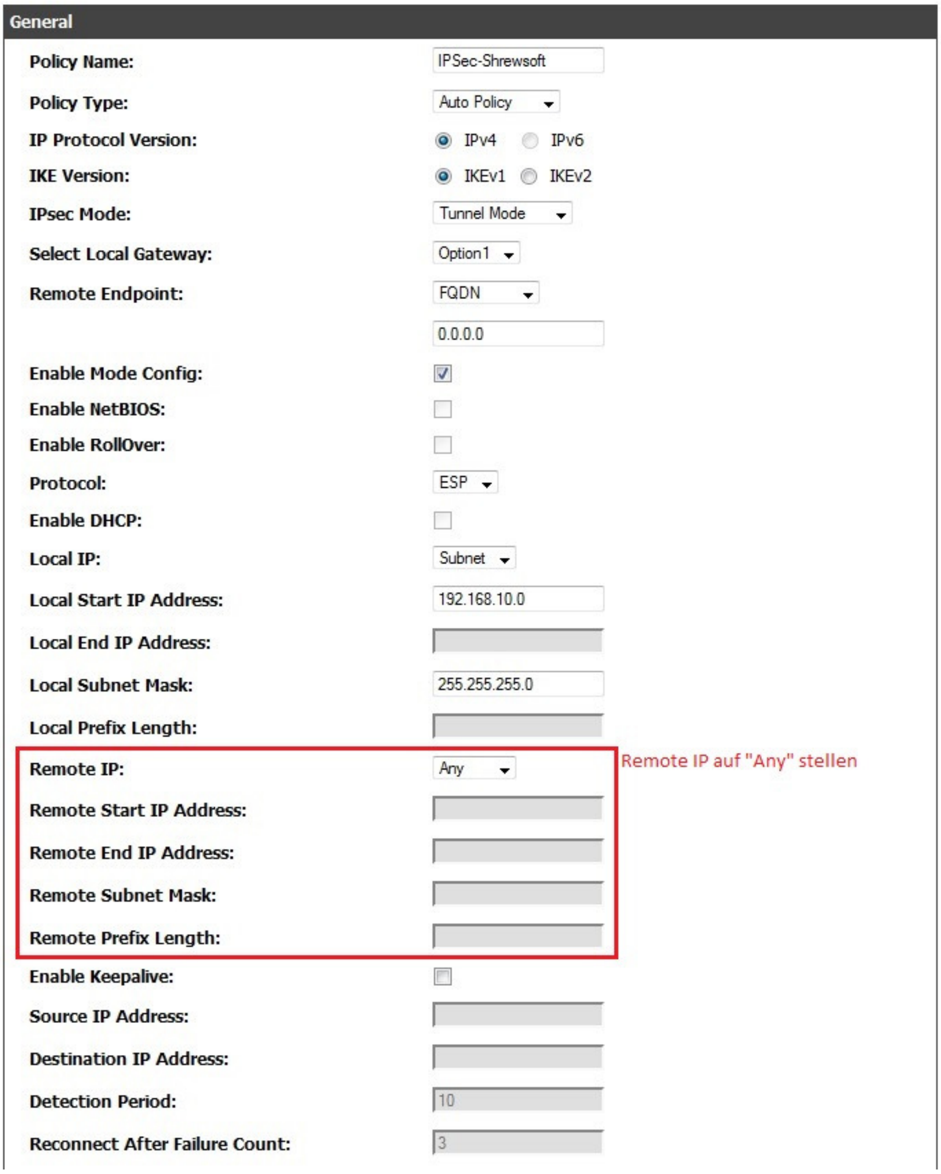
General

Policy Name:	IPSec-Shrewsoft
Policy Type:	Auto Policy
IP Protocol Version:	● IPv4 ○ IPv6
IKE Version:	● IKEv1 ○ IKEv2
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Option1
Remote Endpoint:	FQDN
	0.0.0.0
Enable Mode Config:	☑
Enable NetBIOS:	□
Enable RollOver:	□
Protocol:	ESP
Enable DHCP:	□
Local IP:	Subnet
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Any
Remote Start IP Address:	
Remote End IP Address:	
Remote Subnet Mask:	
Remote Prefix Length:	
Enable Keepalive:	□
Source IP Address:	
Destination IP Address:	
Detection Period:	10
Reconnect After Failure Count:	3

Angabe des Lokalen Subnetzes, hier: 192.168.10.0/24

(*) Sollte der DWC-1000 ein anderes lokales Subnetz verwenden, ändern Sie bitte die Local Start IP Address sowie die Local Subnet Mask entsprechend.

Als Remote IP wählen Sie bitte „Any“:

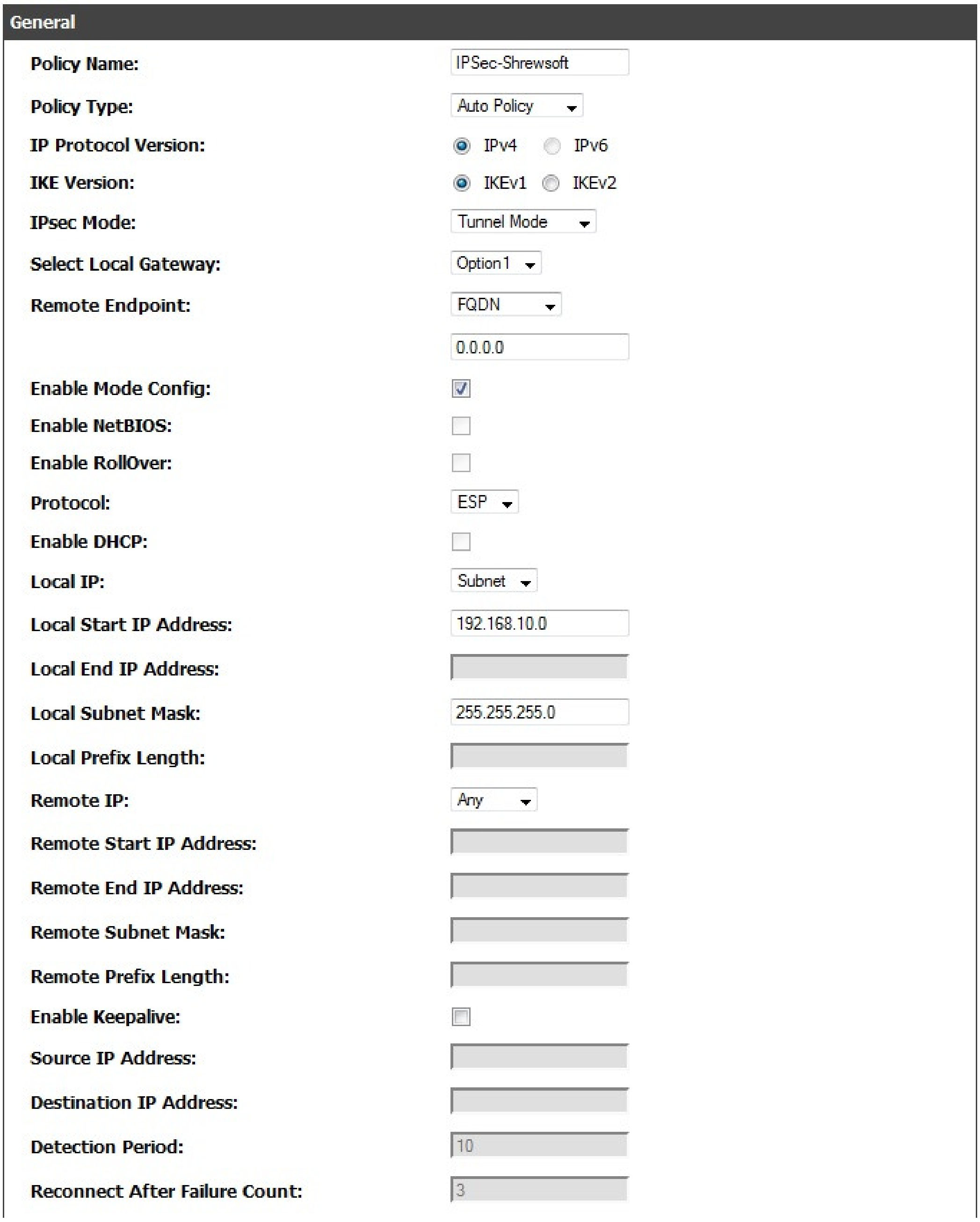


General

Policy Name:	IPSec-Shrewsoft
Policy Type:	Auto Policy
IP Protocol Version:	● IPv4 ○ IPv6
IKE Version:	● IKEv1 ○ IKEv2
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Option1
Remote Endpoint:	FQDN
	0.0.0.0
Enable Mode Config:	☑
Enable NetBIOS:	□
Enable RollOver:	□
Protocol:	ESP
Enable DHCP:	□
Local IP:	Subnet
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Any
Remote Start IP Address:	
Remote End IP Address:	
Remote Subnet Mask:	
Remote Prefix Length:	
Enable Keepalive:	□
Source IP Address:	
Destination IP Address:	
Detection Period:	10
Reconnect After Failure Count:	3

Remote IP auf "Any" stellen

Übersicht der allgemeinen Einstellungen:

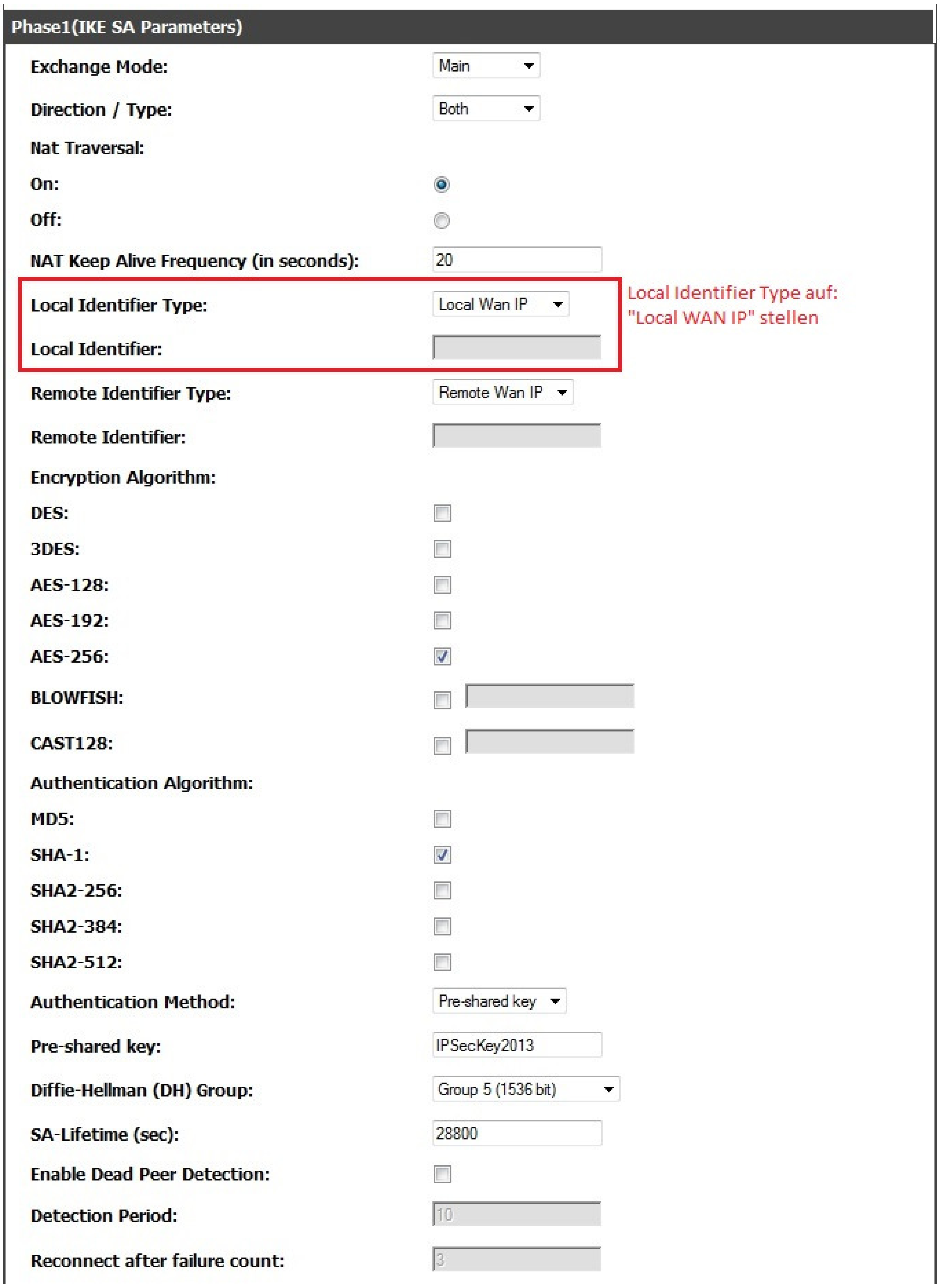


General

Policy Name:	IPSec-Shrewsoft
Policy Type:	Auto Policy
IP Protocol Version:	● IPv4 ○ IPv6
IKE Version:	● IKEv1 ○ IKEv2
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Option1
Remote Endpoint:	FQDN
	0.0.0.0
Enable Mode Config:	☑
Enable NetBIOS:	□
Enable RollOver:	□
Protocol:	ESP
Enable DHCP:	□
Local IP:	Subnet
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Any
Remote Start IP Address:	
Remote End IP Address:	
Remote Subnet Mask:	
Remote Prefix Length:	
Enable Keepalive:	□
Source IP Address:	
Destination IP Address:	
Detection Period:	10
Reconnect After Failure Count:	3

Konfiguration der Phase1:

Wählen Sie als Local Identifier Type: „Local Wan IP“ aus.



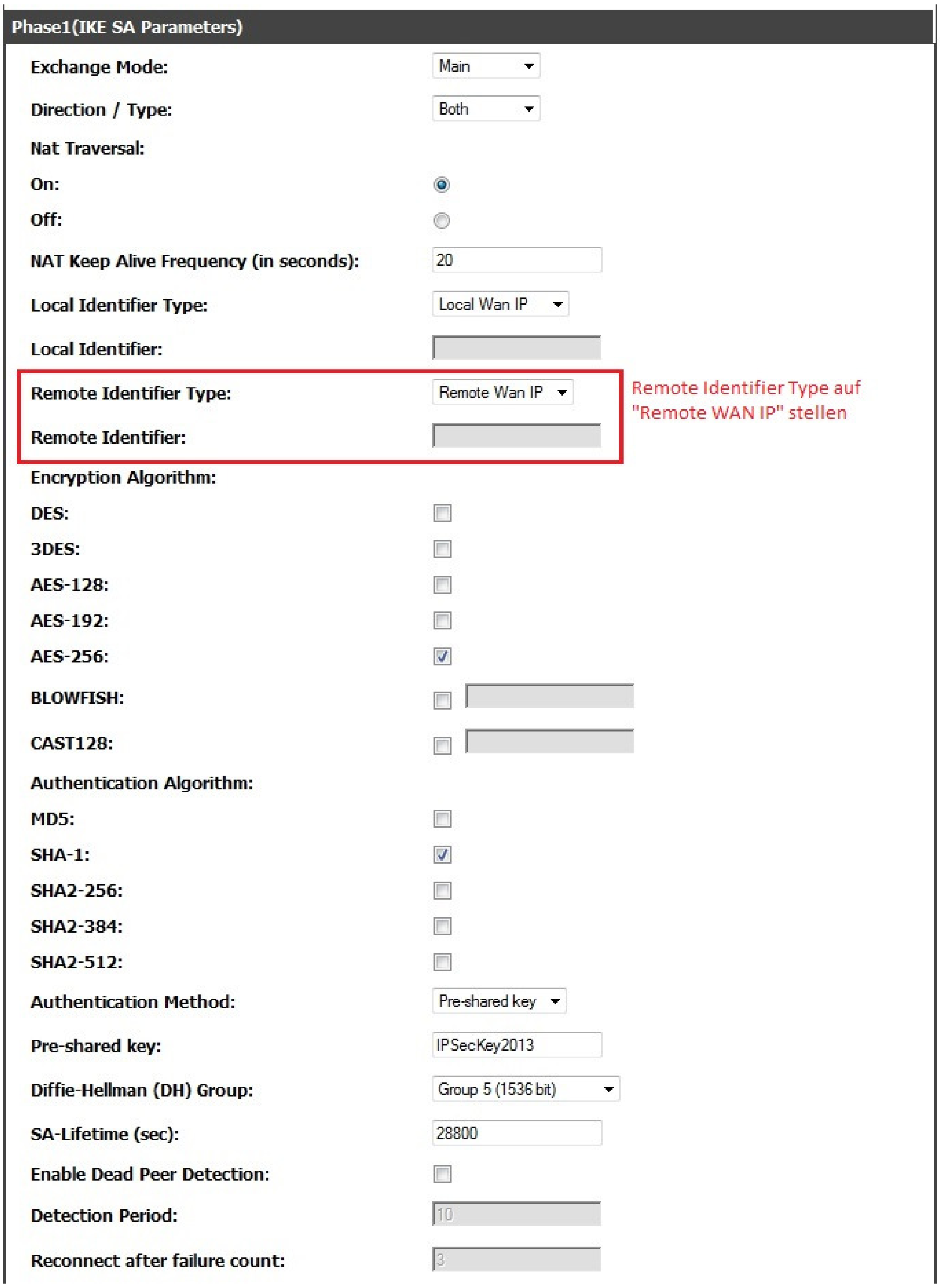
Phase1(IKE SA Parameters)

Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	●
Off:	○
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	
Encryption Algorithm:	
DES:	□
3DES:	□
AES-128:	□
AES-192:	□
AES-256:	☑
BLOWFISH:	□
CAST128:	□
Authentication Algorithm:	
MD5:	□
SHA-1:	☑
SHA2-256:	□
SHA2-384:	□
SHA2-512:	□
Authentication Method:	Pre-shared key
Pre-shared key:	IPSecKey2013
Diffie-Hellman (DH) Group:	Group 5 (1536 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	□
Detection Period:	10
Reconnect after failure count:	3

Local Identifier Type auf:
"Local WAN IP" stellen

Belassen Sie die voreingestellten Optionen für:
Exchange Mode: „Main“
Direction/Type: „Both“
NAT Traversal „On“
NAT Keep Alive „20“

Bei Remote Identifier Type wählen Sie „Remote Wan IP“:

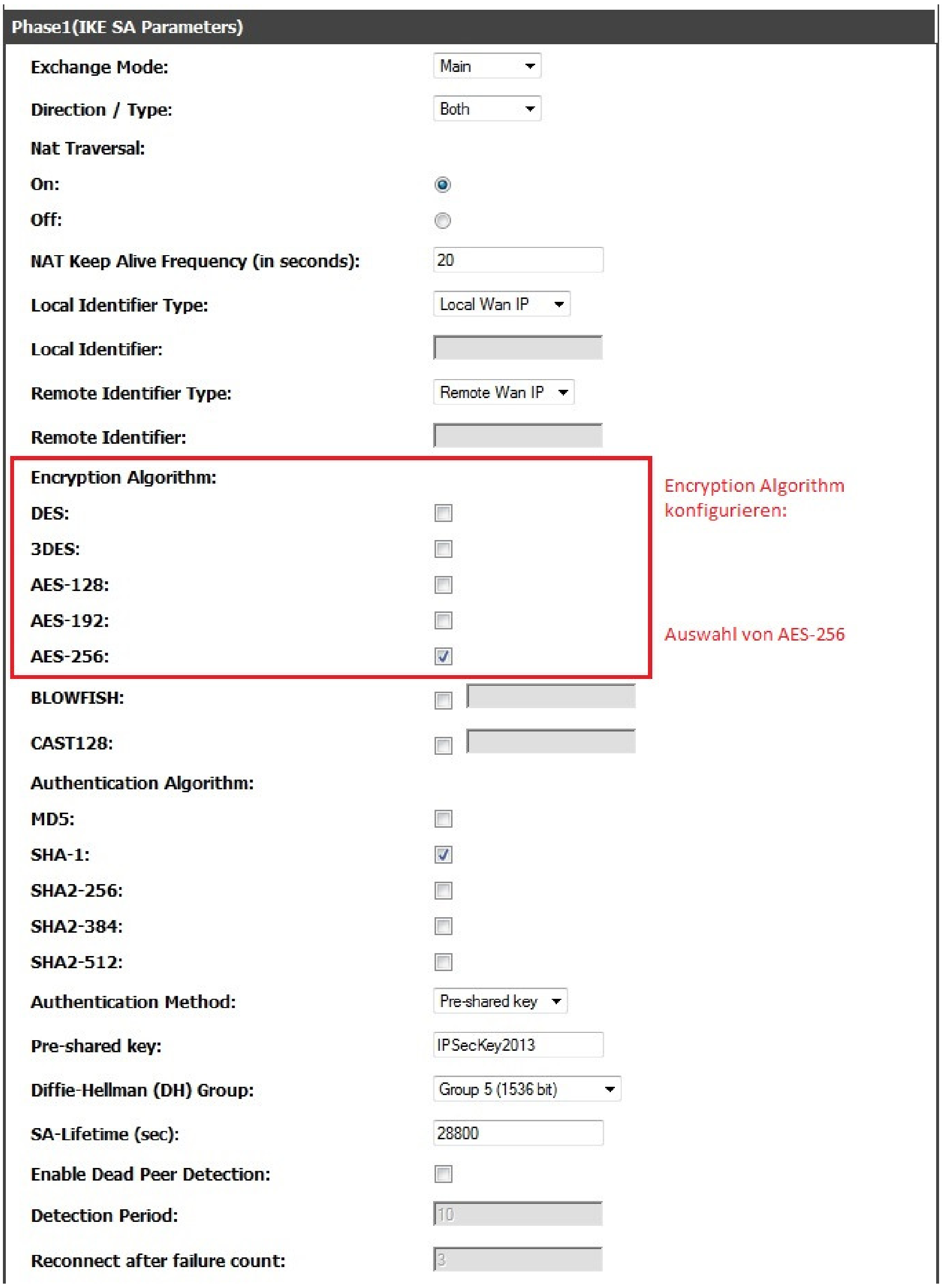


Phase1(IKE SA Parameters)

Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	●
Off:	○
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	
Encryption Algorithm:	
DES:	□
3DES:	□
AES-128:	□
AES-192:	□
AES-256:	☑
BLOWFISH:	□
CAST128:	□
Authentication Algorithm:	
MD5:	□
SHA-1:	☑
SHA2-256:	□
SHA2-384:	□
SHA2-512:	□
Authentication Method:	Pre-shared key
Pre-shared key:	IPSecKey2013
Diffie-Hellman (DH) Group:	Group 5 (1536 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	□
Detection Period:	10
Reconnect after failure count:	3

Remote Identifier Type auf "Remote WAN IP" stellen

Als Encryption Algorithm wählen Sie bitte AES-256 aus:



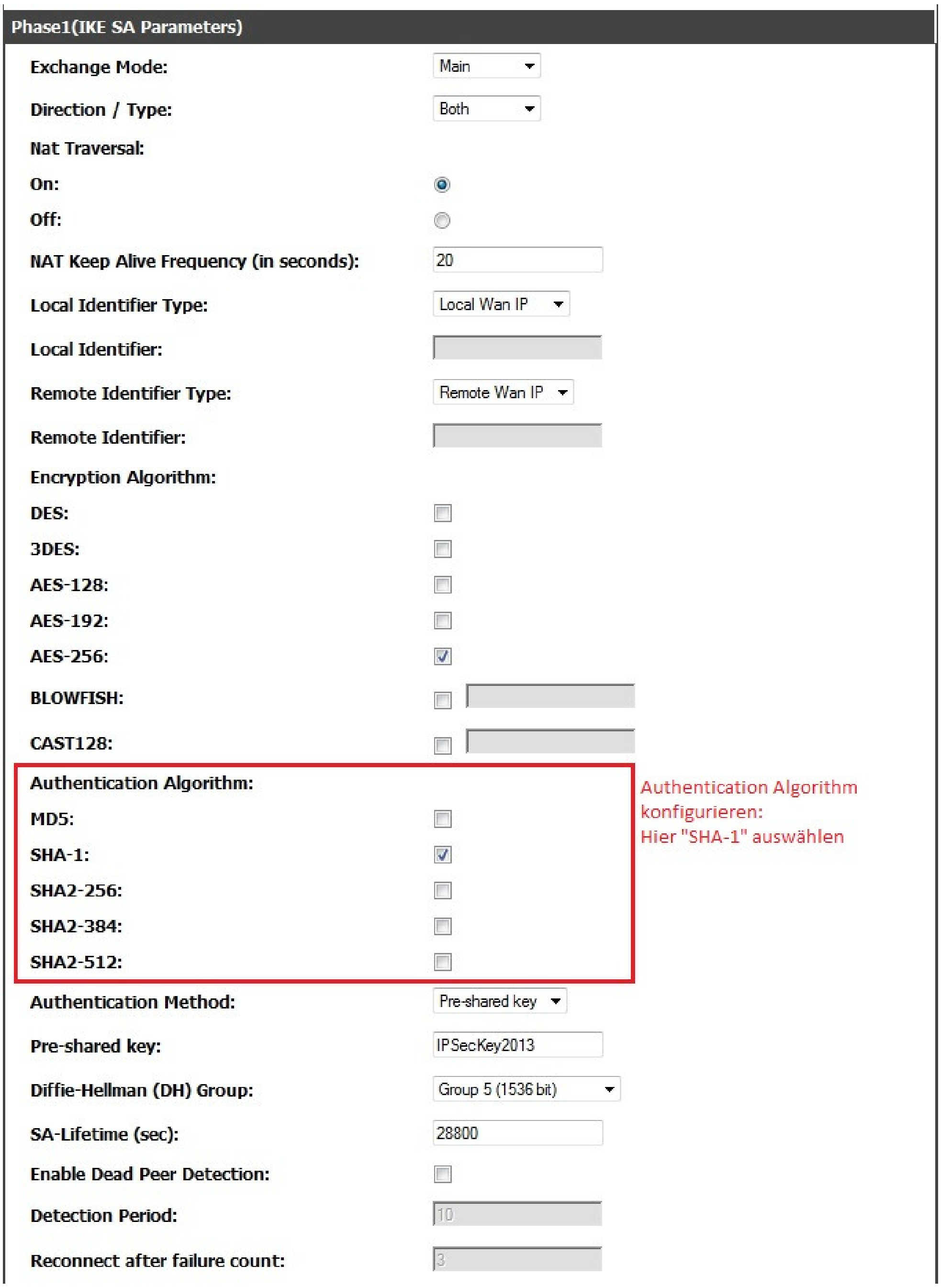
Phase1(IKE SA Parameters)

Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	●
Off:	○
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	
Encryption Algorithm:	
DES:	□
3DES:	□
AES-128:	□
AES-192:	□
AES-256:	☑
BLOWFISH:	□
CAST128:	□
Authentication Algorithm:	
MD5:	□
SHA-1:	☑
SHA2-256:	□
SHA2-384:	□
SHA2-512:	□
Authentication Method:	Pre-shared key
Pre-shared key:	IPSecKey2013
Diffie-Hellman (DH) Group:	Group 5 (1536 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	□
Detection Period:	10
Reconnect after failure count:	3

Encryption Algorithm konfigurieren:

Auswahl von AES-256

Als Authentication Algorithm wählen Sie „SHA-1“:

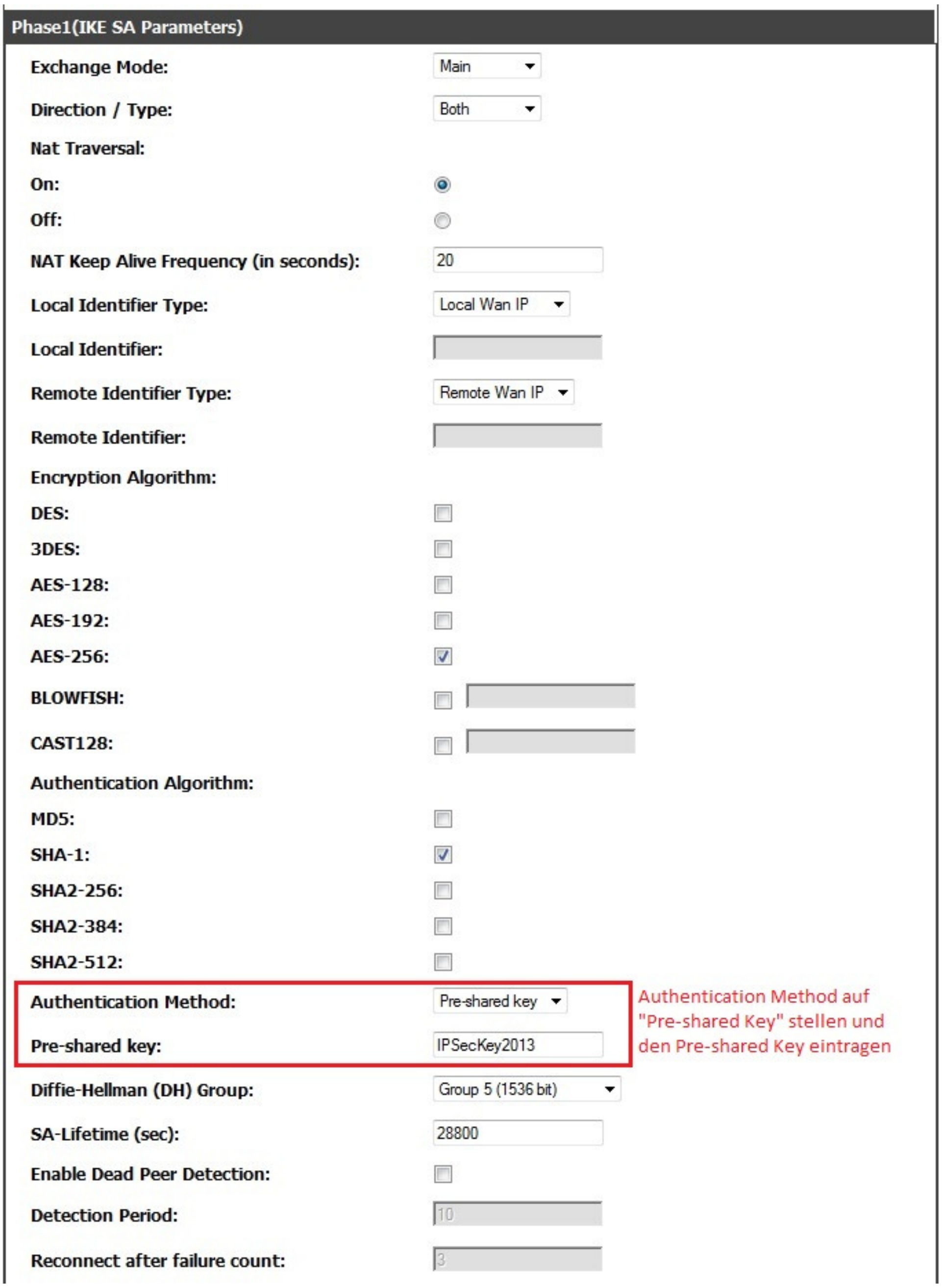


Phase1(IKE SA Parameters)

Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	●
Off:	○
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	
Encryption Algorithm:	
DES:	□
3DES:	□
AES-128:	□
AES-192:	□
AES-256:	☑
BLOWFISH:	□
CAST128:	□
Authentication Algorithm:	
MD5:	□
SHA-1:	☑
SHA2-256:	□
SHA2-384:	□
SHA2-512:	□
Authentication Method:	Pre-shared key
Pre-shared key:	IPSecKey2013
Diffie-Hellman (DH) Group:	Group 5 (1536 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	□
Detection Period:	10
Reconnect after failure count:	3

Authentication Algorithm konfigurieren:
Hier "SHA-1" auswählen

Als „Authentication Method“ wählen Sie „Pre-shared Key“ und vergeben Sie einen Pre-shared Key, hier: „IPSecKey2013“:

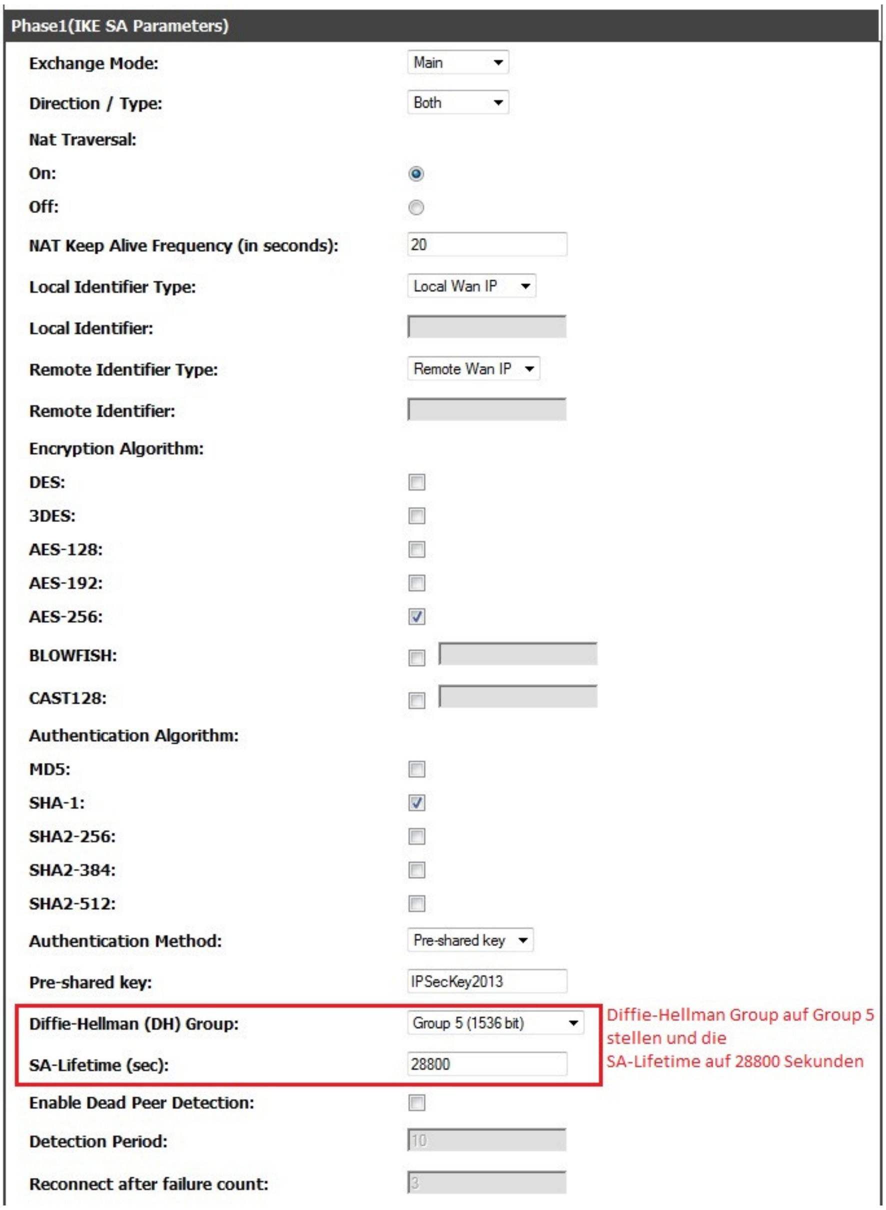


Phase1(IKE SA Parameters)

Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	●
Off:	○
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	
Encryption Algorithm:	
DES:	□
3DES:	□
AES-128:	□
AES-192:	□
AES-256:	☑
BLOWFISH:	□
CAST128:	□
Authentication Algorithm:	
MD5:	□
SHA-1:	☑
SHA2-256:	□
SHA2-384:	□
SHA2-512:	□
Authentication Method:	Pre-shared key
Pre-shared key:	IPSecKey2013
Diffie-Hellman (DH) Group:	Group 5 (1536 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	□
Detection Period:	10
Reconnect after failure count:	3

Authentication Method auf "Pre-shared Key" stellen und den Pre-shared Key eintragen

Als Diffie-Hellman Group wählen Sie „Group 5 (1536 Bit)“ und setzen die SA-Lifetime auf „28800“ Sekunden:

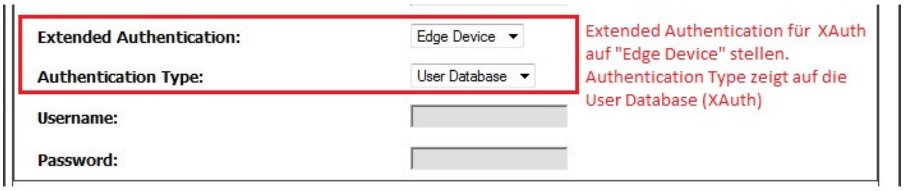


Phase1(IKE SA Parameters)

Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	●
Off:	○
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	
Encryption Algorithm:	
DES:	☐
3DES:	☐
AES-128:	☐
AES-192:	☐
AES-256:	☑
BLOWFISH:	☐
CAST128:	☐
Authentication Algorithm:	
MD5:	☐
SHA-1:	☑
SHA2-256:	☐
SHA2-384:	☐
SHA2-512:	☐
Authentication Method:	Pre-shared key
Pre-shared key:	IPSecKey2013
Diffie-Hellman (DH) Group:	Group 5 (1536 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	☐
Detection Period:	10
Reconnect after failure count:	3

Diffie-Hellman Group auf Group 5 stellen und die SA-Lifetime auf 28800 Sekunden

Als Extended Authentication wählen Sie „Edge Device“ und bei Authentication Type: „User Database“:

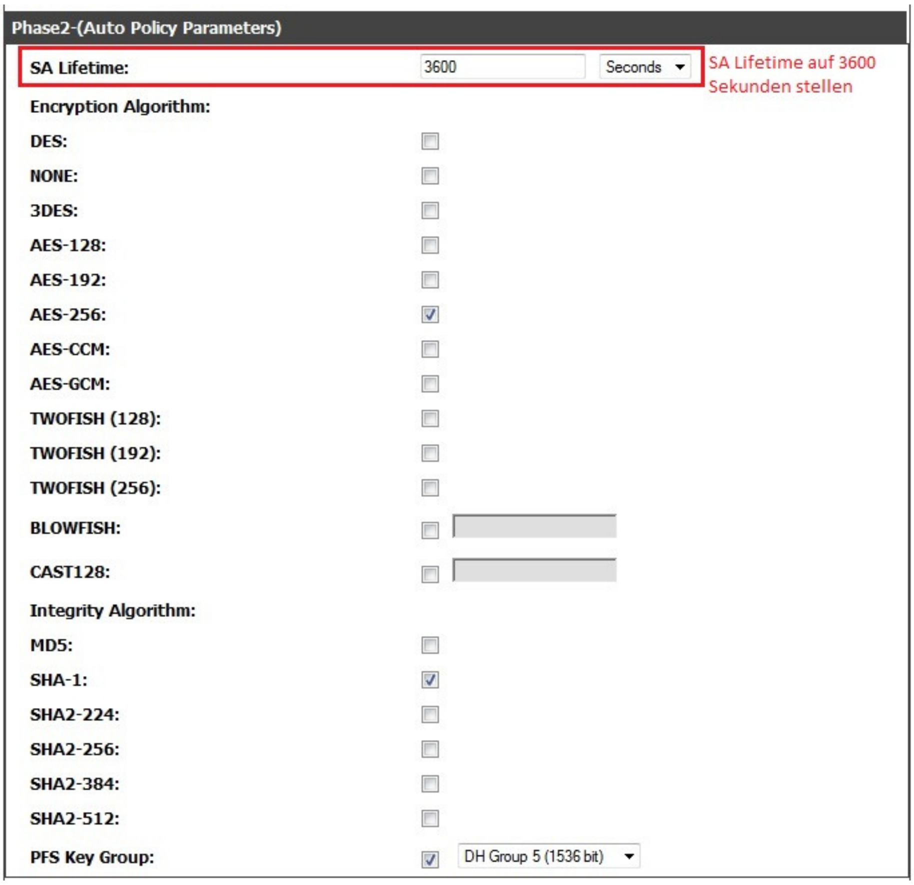


Extended Authentication:	Edge Device
Authentication Type:	User Database
Username:	
Password:	

Extended Authentication für XAuth auf "Edge Device" stellen. Authentication Type zeigt auf die User Database (XAuth)

Konfiguration der Phase2:

Festlegen der SA Lifetime auf „3600“ Sekunden:

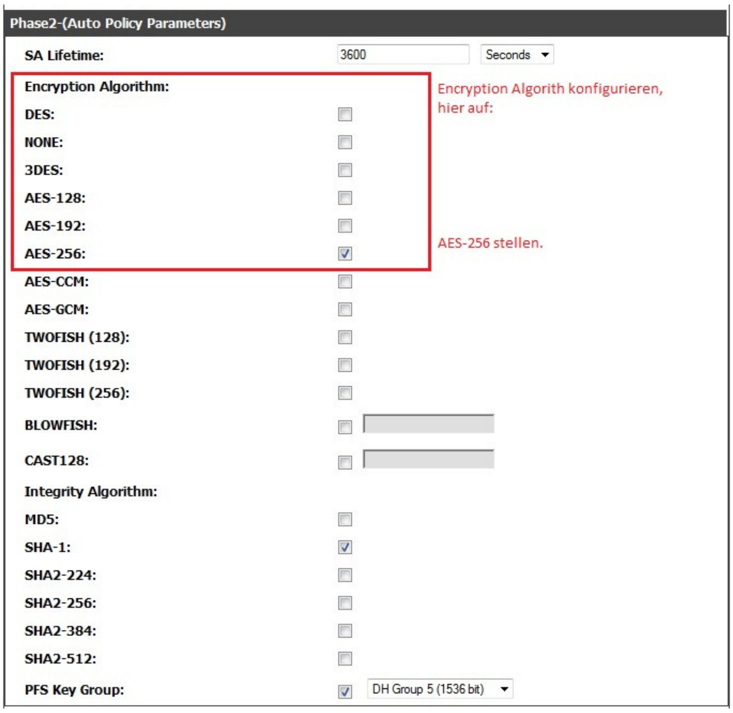


Phase2-(Auto Policy Parameters)

SA Lifetime:	3600	Seconds ▾
Encryption Algorithm:		
DES:	□	
NONE:	□	
3DES:	□	
AES-128:	□	
AES-192:	□	
AES-256:	☑	
AES-CCM:	□	
AES-GCM:	□	
TWOFISH (128):	□	
TWOFISH (192):	□	
TWOFISH (256):	□	
BLOWFISH:	□	
CAST128:	□	
Integrity Algorithm:		
MD5:	□	
SHA-1:	☑	
SHA2-224:	□	
SHA2-256:	□	
SHA2-384:	□	
SHA2-512:	□	
PFS Key Group:	☑	DH Group 5 (1536 bit) ▾

SA Lifetime auf 3600 Sekunden stellen

Konfiguration des Encryption Algorithm, auch hier wählen Sie „AES-256“ aus:



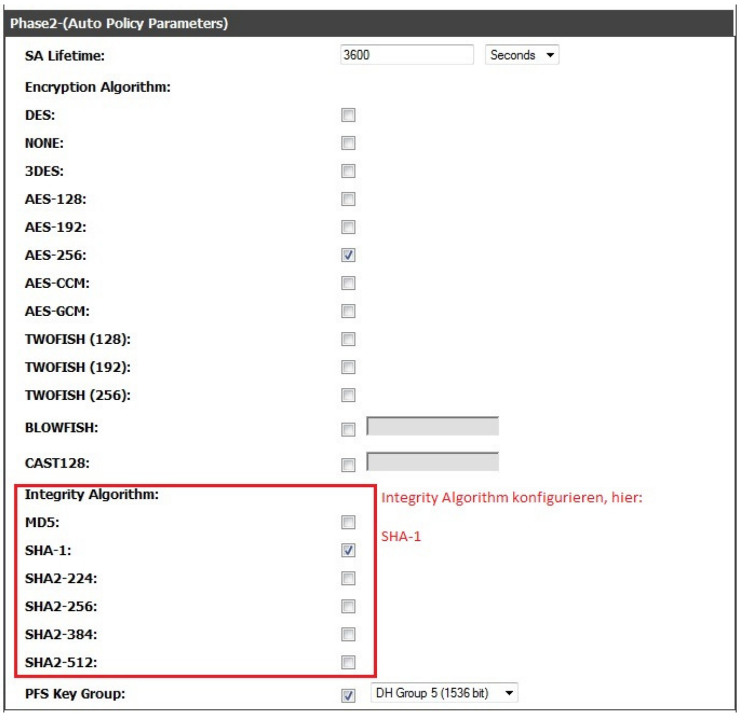
Phase2-(Auto Policy Parameters)

SA Lifetime:	3600 Seconds
Encryption Algorithm:	
DES:	□
NONE:	□
3DES:	□
AES-128:	□
AES-192:	□
AES-256:	☑
AES-CCM:	□
AES-GCM:	□
TWOFISH (128):	□
TWOFISH (192):	□
TWOFISH (256):	□
BLOWFISH:	□
CAST128:	□
Integrity Algorithm:	
MD5:	□
SHA-1:	☑
SHA2-224:	□
SHA2-256:	□
SHA2-384:	□
SHA2-512:	□
PFS Key Group:	☑ DH Group 5 (1536 bit)

Encryption Algorith konfigurieren, hier auf:

AES-256 stellen.

Für den Integrity Algorithm wählen Sie „SHA-1“:



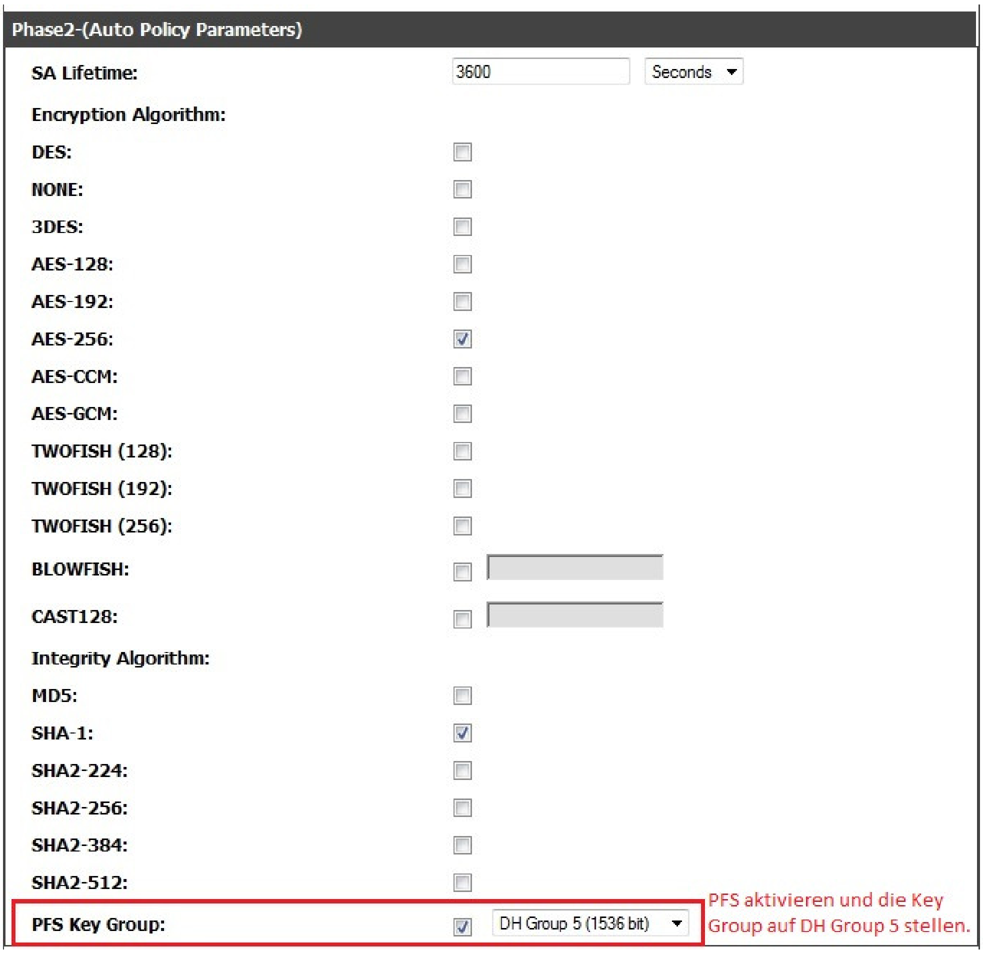
Phase2-(Auto Policy Parameters)

SA Lifetime:	3600 Seconds
Encryption Algorithm:	
DES:	□
NONE:	□
3DES:	□
AES-128:	□
AES-192:	□
AES-256:	☑
AES-CCM:	□
AES-GCM:	□
TWOFISH (128):	□
TWOFISH (192):	□
TWOFISH (256):	□
BLOWFISH:	□
CAST128:	□
Integrity Algorithm:	
MD5:	□
SHA-1:	☑
SHA2-224:	□
SHA2-256:	□
SHA2-384:	□
SHA2-512:	□
PFS Key Group:	☑ DH Group 5 (1536 bit)

Integrity Algorithm konfigurieren, hier:

SHA-1

Aktivieren Sie PFS (Perfect Forward Secrecy) und wählen Sie die Diffie Hellman Group
„DH Group 5 (1536 Bit)“:

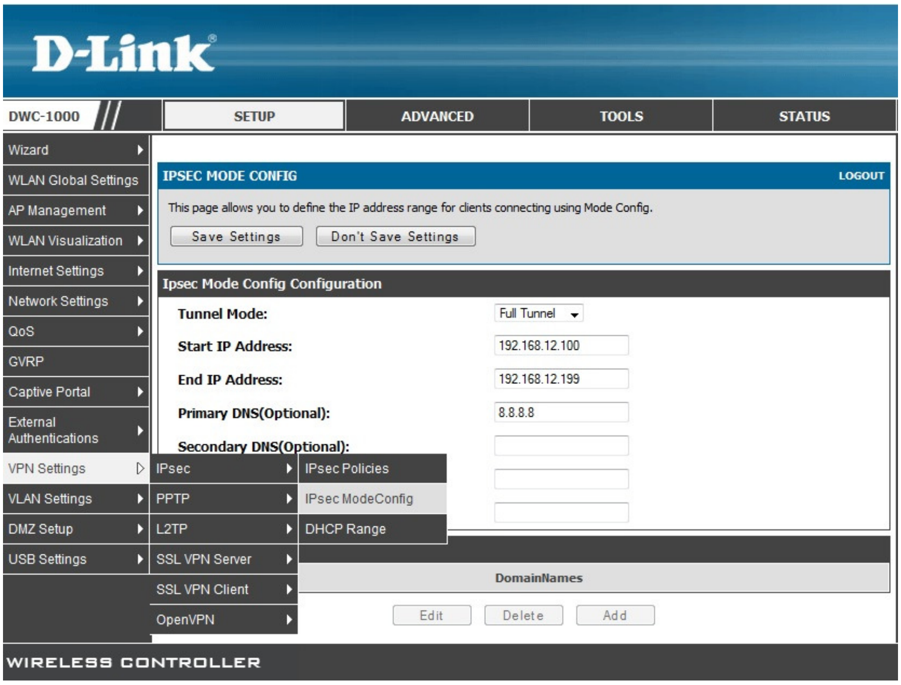


Phase2-(Auto Policy Parameters)

SA Lifetime:	3600 Seconds
Encryption Algorithm:	
DES:	□
NONE:	□
3DES:	□
AES-128:	□
AES-192:	□
AES-256:	☑
AES-CCM:	□
AES-GCM:	□
TWOFISH (128):	□
TWOFISH (192):	□
TWOFISH (256):	□
BLOWFISH:	□
CAST128:	□
Integrity Algorithm:	
MD5:	□
SHA-1:	☑
SHA2-224:	□
SHA2-256:	□
SHA2-384:	□
SHA2-512:	□
PFS Key Group:	☑ DH Group 5 (1536 bit)

PFS aktivieren und die Key Group auf DH Group 5 stellen.

2.) Konfiguration der IPsec Mode Konfiguration
Öffnen Sie die Einstellungen zu IPsec Mode Config.
>Setup >VPN Settings > IPsec > IPsec Mode Config



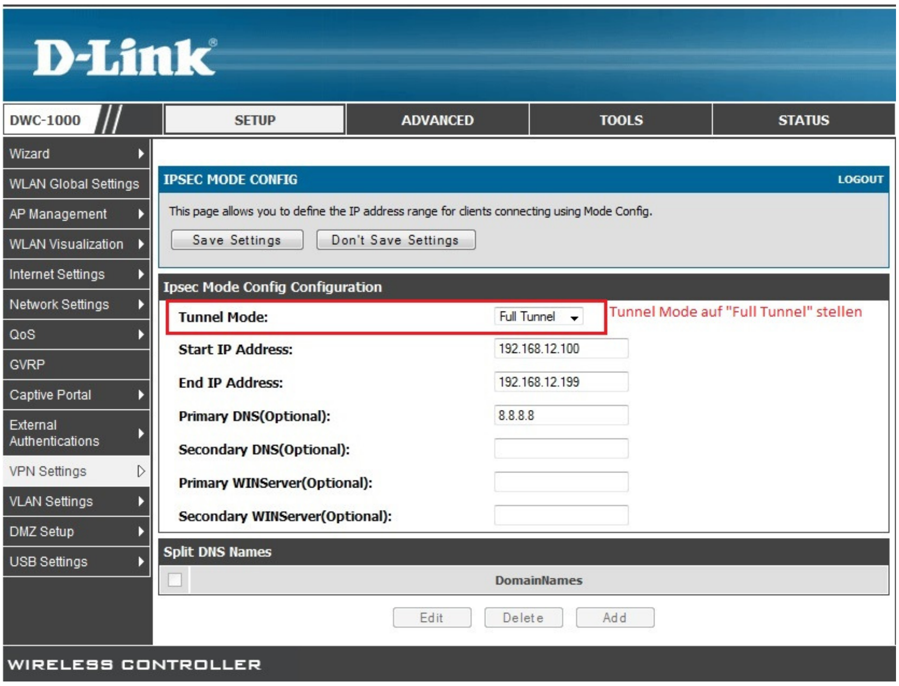
IPSEC MODE CONFIG

This page allows you to define the IP address range for clients connecting using Mode Config.

Ipsec Mode Config Configuration

Tunnel Mode: Full Tunnel
Start IP Address: 192.168.12.100
End IP Address: 192.168.12.199
Primary DNS(Optional): 8.8.8.8
Secondary DNS(Optional):

Legen Sie über „Add“ eine neue IPsec Mode Config Configuration an:
Wählen Sie bei Tunnel Mode: „Full Tunnel“ aus



IPSEC MODE CONFIG

This page allows you to define the IP address range for clients connecting using Mode Config.

Ipsec Mode Config Configuration

Tunnel Mode: Full Tunnel
Start IP Address: 192.168.12.100
End IP Address: 192.168.12.199
Primary DNS(Optional): 8.8.8.8
Secondary DNS(Optional):
Primary WINServer(Optional):
Secondary WINServer(Optional):

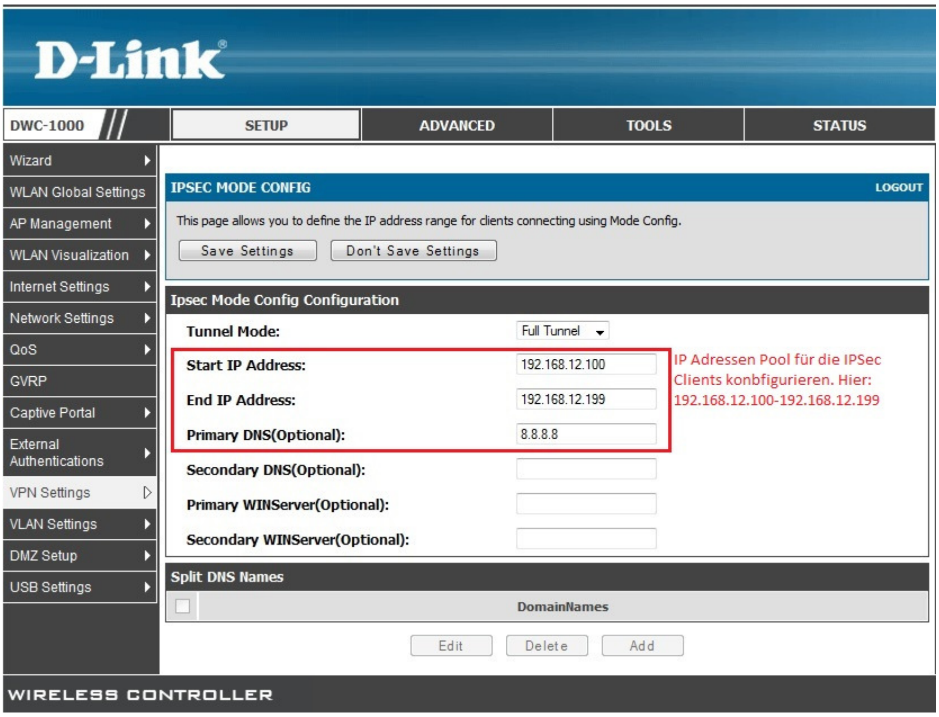
Split DNS Names

Tunnel Mode auf "Full Tunnel" stellen

Tragen Sie bei Start IP Address die IP Adresse ein mit der der Pool für die IPsec Clients beginnen soll, hier: „192.168.12.100“.

Bei End IP Address tragen Sie die letzte zu vergebende IP Adresse des Pools ein, hier: 192.168.12.199.

Die Eingabe der DNS Server ist optional, hier wurde beispielsweise der Google-DNS „8.8.8.8“ eingetragen.



IPSEC MODE CONFIG

This page allows you to define the IP address range for clients connecting using Mode Config.

Ipsec Mode Config Configuration

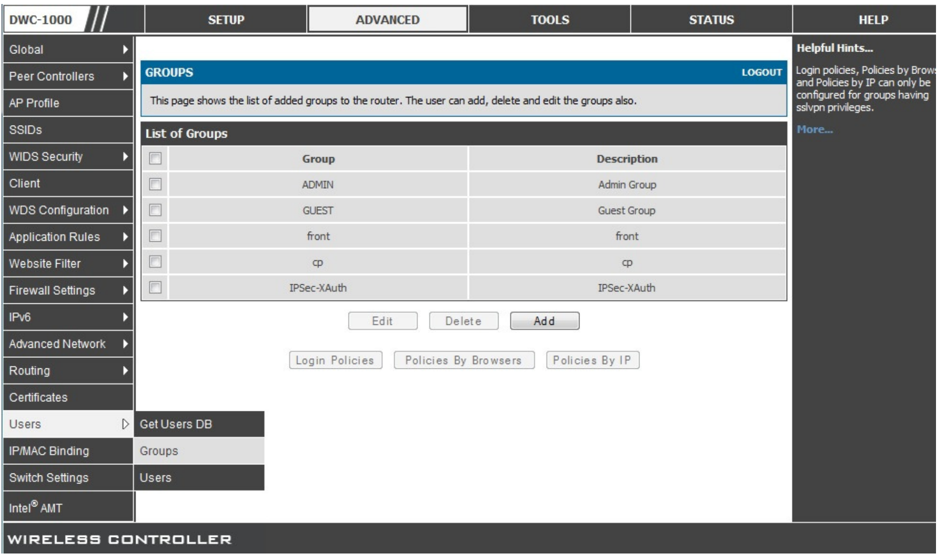
Tunnel Mode:	Full Tunnel
Start IP Address:	192.168.12.100
End IP Address:	192.168.12.199
Primary DNS(Optional):	8.8.8.8
Secondary DNS(Optional):	
Primary WINServer(Optional):	
Secondary WINServer(Optional):	

IP Adressen Pool für die IPSec Clients konbfigurieren. Hier: 192.168.12.100-192.168.12.199

Split DNS Names

□	DomainNames

3.) Anlegen einer Benutzerdatenbank
Wechseln Sie in die Group Einstellungen
> Advanced > Users > Groups



GROUPS

This page shows the list of added groups to the router. The user can add, delete and edit the groups also.

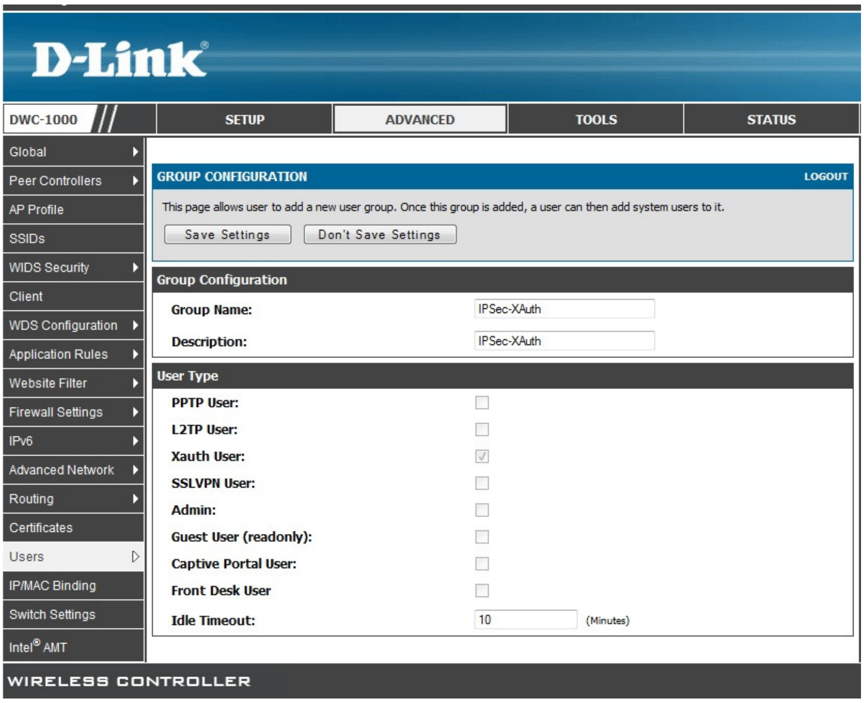
List of Groups

□	Group	Description
□	ADMIN	Admin Group
□	GUEST	Guest Group
□	front	front
□	cp	cp
□	IPSec-XAuth	IPSec-XAuth

Helpful Hints...

Login policies, Policies by Brows and Policies by IP can only be configured for groups having sslvpn privileges.

Fügen Sie hier über „Add“ eine neue Gruppe für die IPsec-User hinzu. Vergeben Sie der Gruppe einen Namen, z.B. „IPSec-XAuth“:



GROUP CONFIGURATION

This page allows user to add a new user group. Once this group is added, a user can then add system users to it.

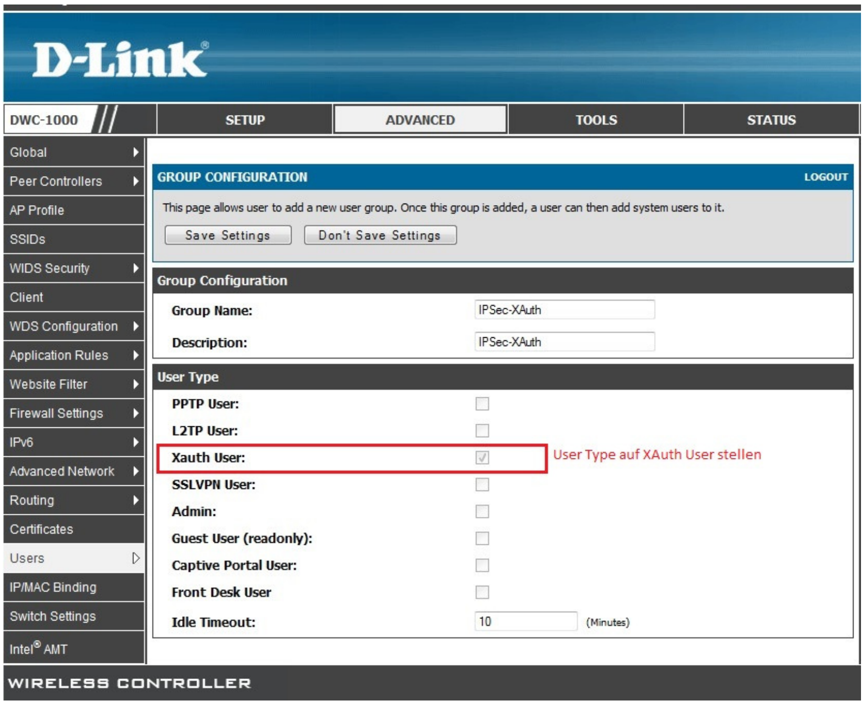
Group Configuration

Group Name:	IPSec-XAuth
Description:	IPSec-XAuth

User Type

PPTP User:	☐
L2TP User:	☐
Xauth User:	☑
SSLVPN User:	☐
Admin:	☐
Guest User (readonly):	☐
Captive Portal User:	☐
Front Desk User	☐
Idle Timeout:	10 (Minutes)

Wählen Sie als User Type „Xauth User“ aus:



GROUP CONFIGURATION

This page allows user to add a new user group. Once this group is added, a user can then add system users to it.

Group Configuration

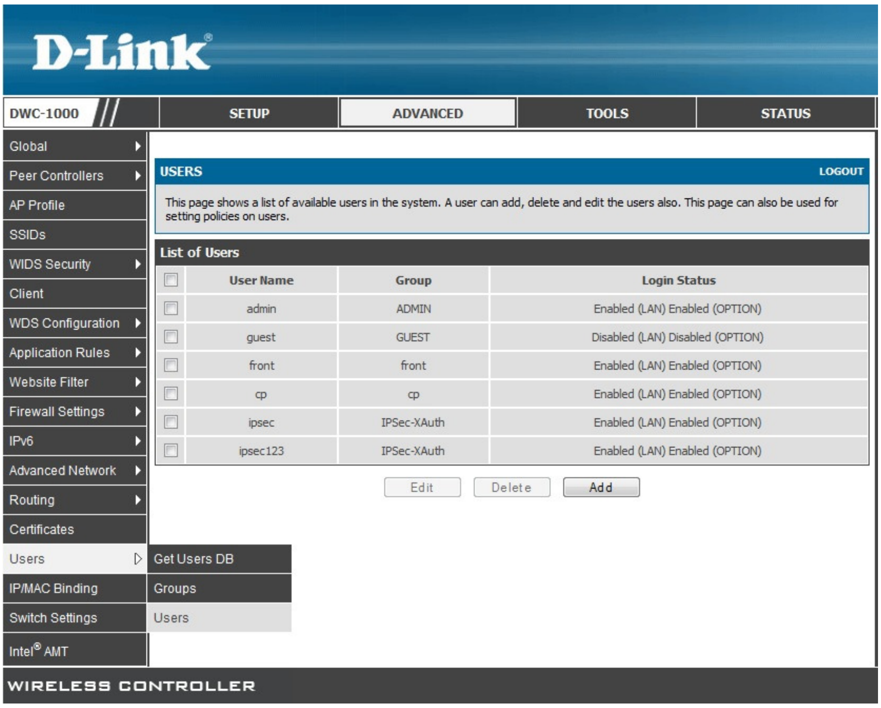
Group Name:	IPSec-XAuth
Description:	IPSec-XAuth

User Type

PPTP User:	☐
L2TP User:	☐
Xauth User:	☑
SSLVPN User:	☐
Admin:	☐
Guest User (readonly):	☐
Captive Portal User:	☐
Front Desk User	☐
Idle Timeout:	10 (Minutes)

User Type auf XAuth User stellen

4.) Anlegen eines IPsec Benutzers
Wechseln Sie in die „Users“ Einstellungen.
> Advanced > Users > Users



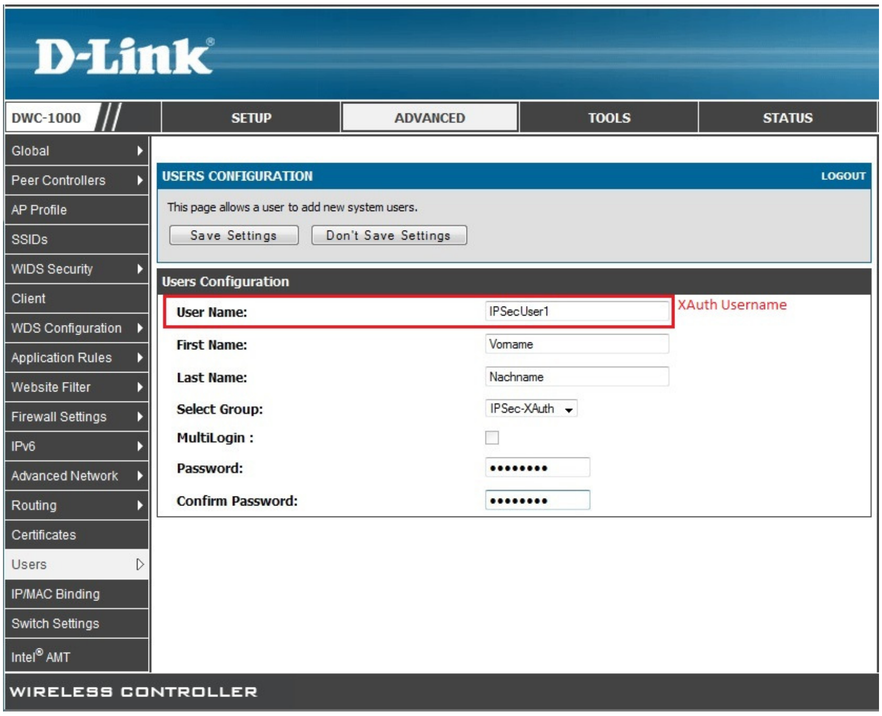
USERS

This page shows a list of available users in the system. A user can add, delete and edit the users also. This page can also be used for setting policies on users.

List of Users

□	User Name	Group	Login Status
□	admin	ADMIN	Enabled (LAN) Enabled (OPTION)
□	guest	GUEST	Disabled (LAN) Disabled (OPTION)
□	front	front	Enabled (LAN) Enabled (OPTION)
□	cp	cp	Enabled (LAN) Enabled (OPTION)
□	ipsec	IPSec-XAuth	Enabled (LAN) Enabled (OPTION)
□	ipsec123	IPSec-XAuth	Enabled (LAN) Enabled (OPTION)

Über „Add“ können Sie einen neuen Benutzer erstellen:
Vergeben Sie einen User Name, hier „IPSecUser1“:



USERS CONFIGURATION

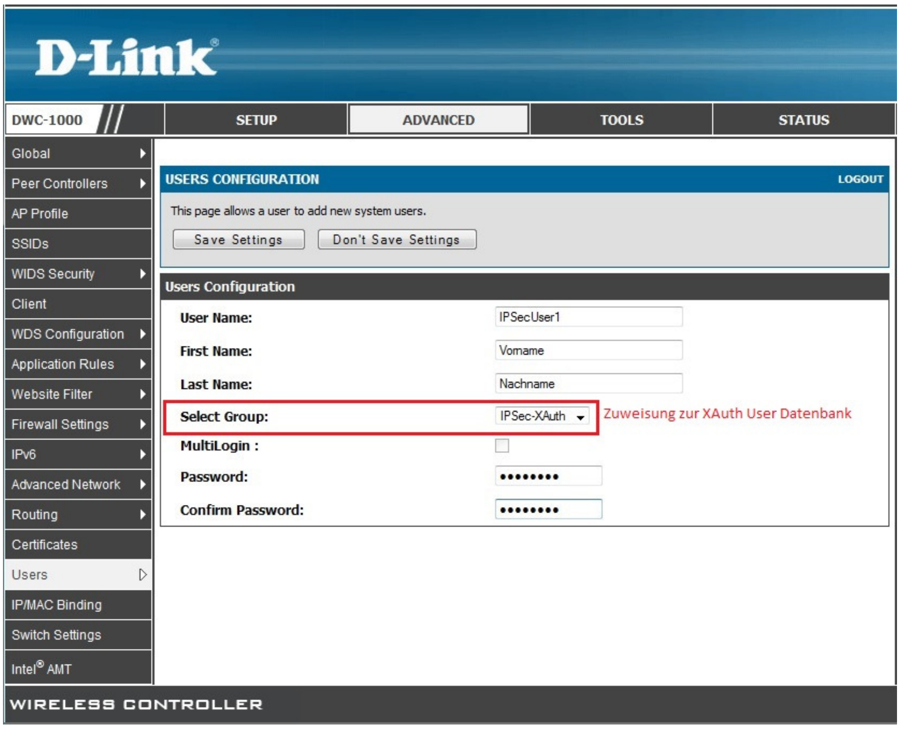
This page allows a user to add new system users.

Users Configuration

User Name:	IPSecUser1
First Name:	Vorname
Last Name:	Nachname
Select Group:	IPSec-XAuth
MultiLogin :	□
Password:	••••••••
Confirm Password:	••••••••

XAuth Username

Weisen Sie dem Benutzer eine Gruppe zu, hier soll der eben angelegte User der vorher angelegten Xauth Gruppe zugewiesen werden. Wählen Sie daher bei Select Group „IPSec-XAuth“ aus.



USERS CONFIGURATION

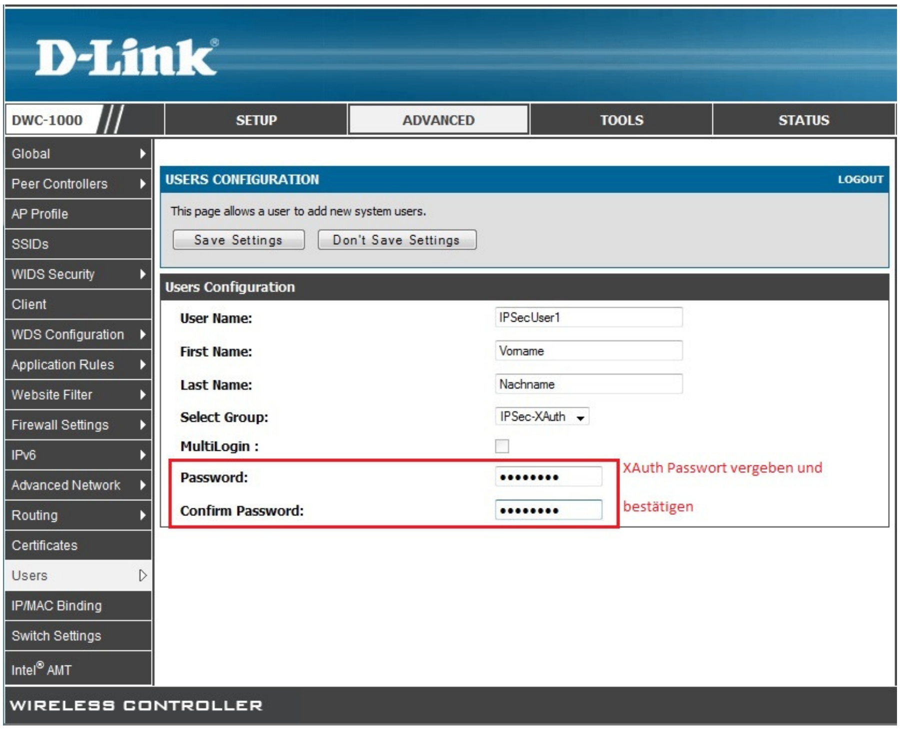
This page allows a user to add new system users.

Users Configuration

User Name: IPSecUser1
First Name: Vorname
Last Name: Nachname
Select Group: IPSec-XAuth
MultiLogin : □
Password: ••••••••
Confirm Password: ••••••••

Zuweisung zur XAuth User Datenbank

Vergeben Sie dem Benutzer ein Passwort: hier „ipsec123“ und bestätigen Sie dieses durch erneute Eingabe.



USERS CONFIGURATION

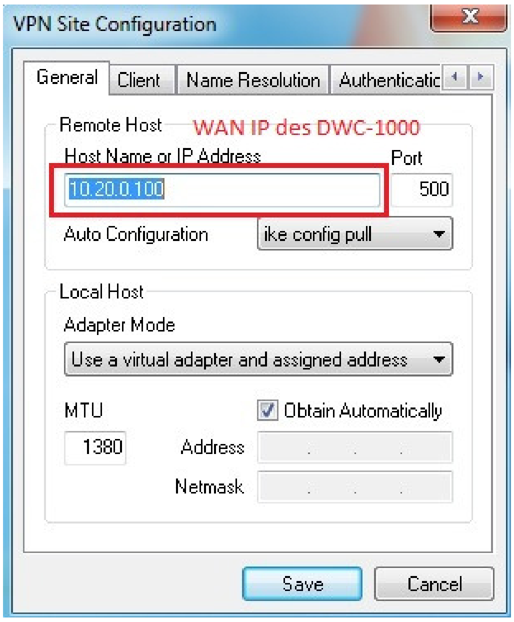
This page allows a user to add new system users.

Users Configuration

User Name: IPSecUser1
First Name: Vorname
Last Name: Nachname
Select Group: IPSec-XAuth
MultiLogin : □
Password: ••••••••
Confirm Password: ••••••••

XAuth Passwort vergeben und bestätigen

5.) Konfiguration des „Shrewsoft“ Clients
Als IP Address geben Sie die WAN IP des DWC-1000 ein, hier: „10.20.0.100“(*)



WAN IP des DWC-1000

VPN Site Configuration

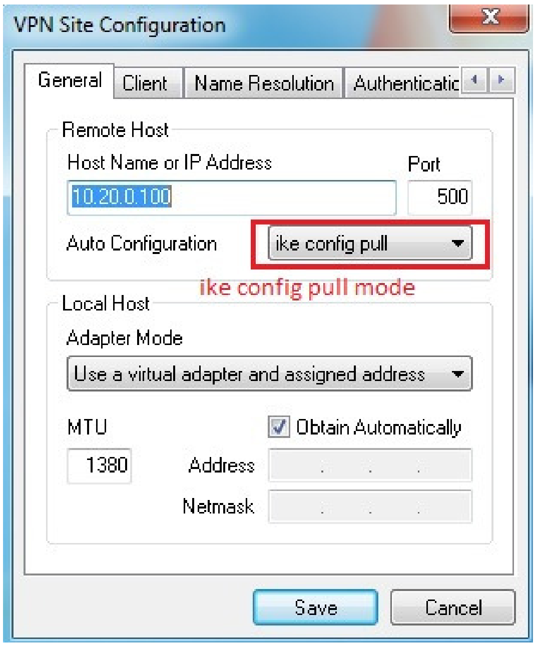
General | Client | Name Resolution | Authenticatic

Remote Host
Host Name or IP Address: 10.20.0.100
Port: 500
Auto Configuration: ike config pull

Local Host
Adapter Mode: Use a virtual adapter and assigned address
MTU: 1380
☑ Obtain Automatically
Address: . . .
Netmask: . . .

(*) Geben Sie hier bitte Ihre WAN IP Adresse des DWC-1000 oder z.B. den DynDNS Namen ein.

Wählen Sie bei Auto Configuration „ike config pull“ aus, damit die Client die Konfiguration vom Server zieht.



ike config pull mode

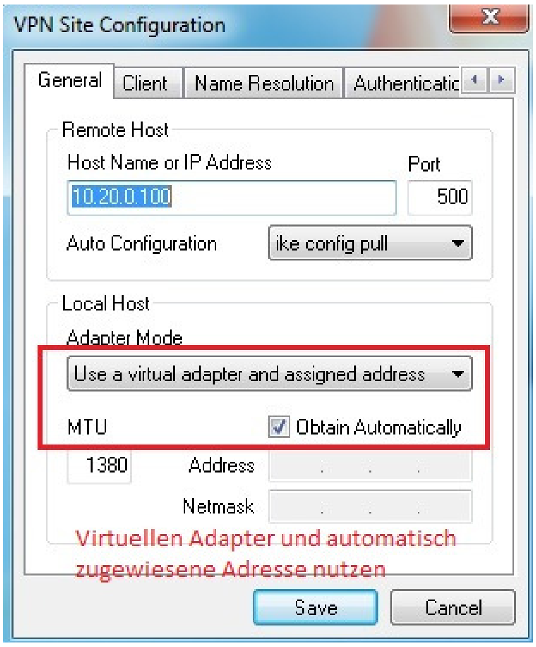
VPN Site Configuration

General | Client | Name Resolution | Authenticatic

Remote Host
Host Name or IP Address: 10.20.0.100
Port: 500
Auto Configuration: ike config pull

Local Host
Adapter Mode: Use a virtual adapter and assigned address
MTU: 1380
☑ Obtain Automatically
Address: . . .
Netmask: . . .

Wählen Sie bei Adapter Mode: „use a virtual adapter and assigned address“ aus und aktivieren Sie „Obtain Automatically“.



Remote Host

Host Name or IP Address: 10.20.0.100

Port: 500

Auto Configuration: ike config pull

Local Host

Adapter Mode: Use a virtual adapter and assigned address

MTU: 1380

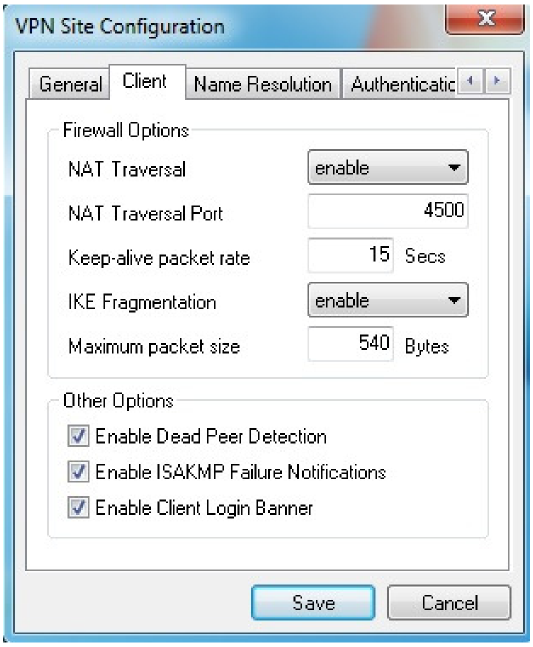
☑ Obtain Automatically

Address: . . .

Netmask: . . .

Virtuellen Adapter und automatisch zugewiesene Adresse nutzen

Auf dem Reiter „Client“ sind keine Änderungen notwendig



Firewall Options

NAT Traversal: enable

NAT Traversal Port: 4500

Keep-alive packet rate: 15 Secs

IKE Fragmentation: enable

Maximum packet size: 540 Bytes

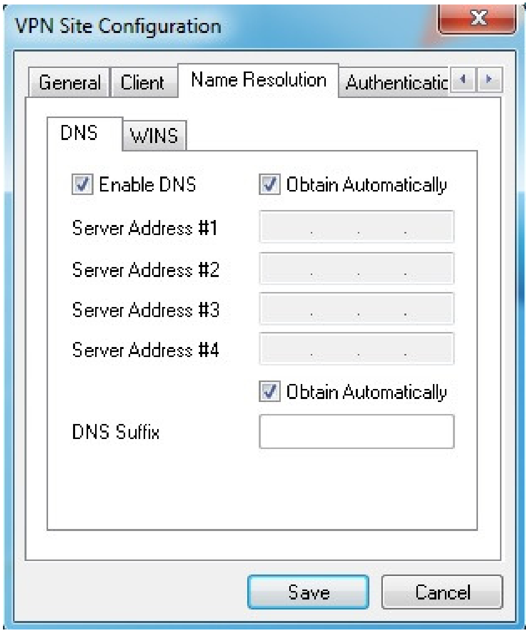
Other Options

☑ Enable Dead Peer Detection

☑ Enable ISAKMP Failure Notifications

☑ Enable Client Login Banner

Auf dem Reiter „Name Resolution“ sind ebenfalls keine Änderungen notwendig



☑ Enable DNS ☑ Obtain Automatically

Server Address #1 . . .

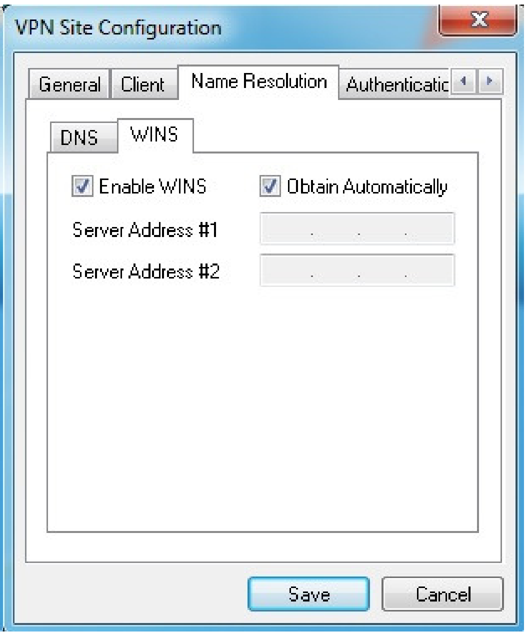
Server Address #2 . . .

Server Address #3 . . .

Server Address #4 . . .

☑ Obtain Automatically

DNS Suffix

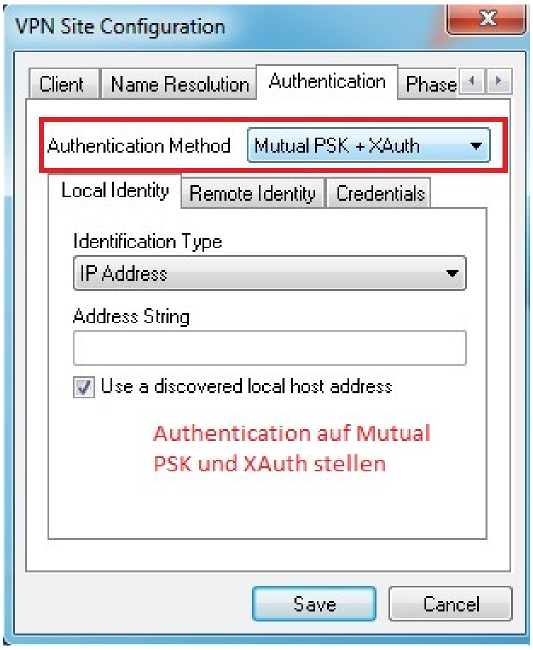


☑ Enable WINS ☑ Obtain Automatically

Server Address #1 . . .

Server Address #2 . . .

Auf dem Reiter „Authentication“ wählen Sie als Authentication Method: „Mutual PSK + Auth“:


VPN Site Configuration
Client | Name Resolution | Authentication | Phase
Local Identity | Remote Identity | Credentials
Save
Cancel

Authentication Method: Mutual PSK + XAuth

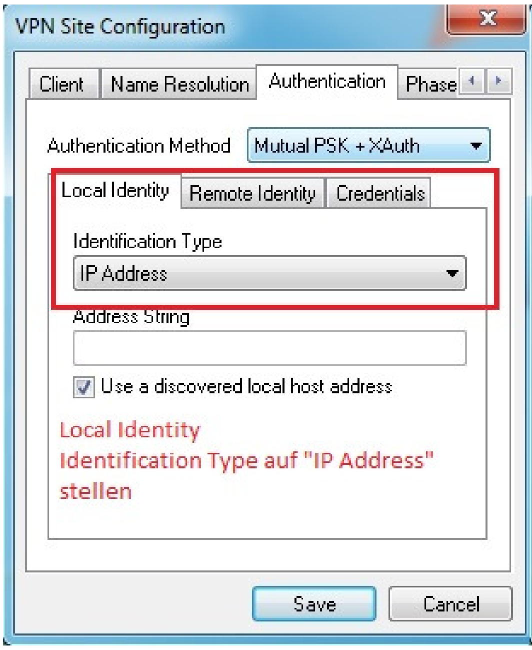
Identification Type: IP Address

Address String

☑ Use a discovered local host address

Authentication auf Mutual PSK und XAuth stellen

Unter Local Identity wählen Sie bitte als Identification Type „IP Address“ aus und aktivieren Sie „use a discovered local host address“:



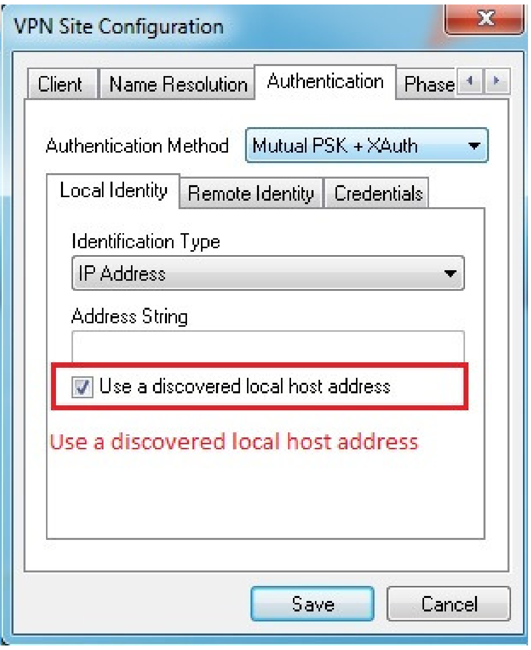
Authentication Method: Mutual PSK + XAuth

Identification Type: IP Address

Address String:

☑ Use a discovered local host address

Local Identity
Identification Type auf "IP Address" stellen



Authentication Method: Mutual PSK + XAuth

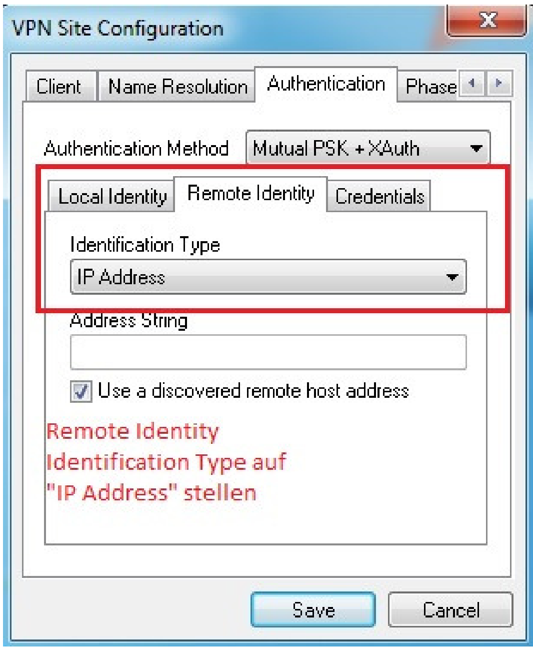
Identification Type: IP Address

Address String:

☑ Use a discovered local host address

Use a discovered local host address

Unter Remote Identity wählen Sie bitte als Identification Type „IP Address“ aus und aktivieren Sie „use a discovered local host address“:



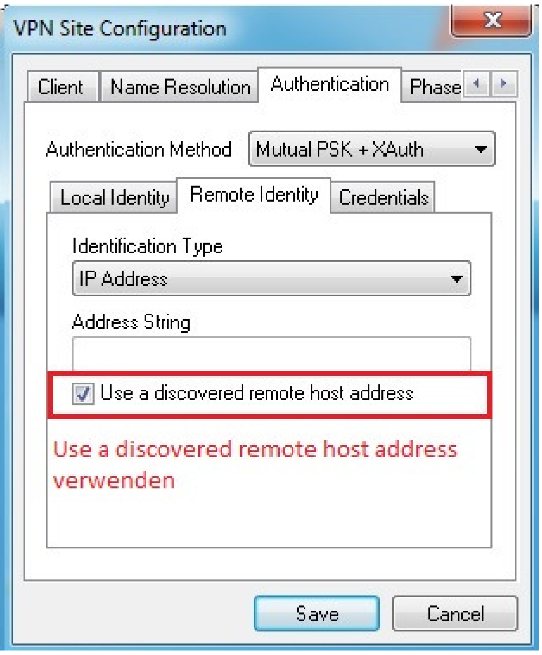
Authentication Method: Mutual PSK + XAuth

Identification Type: IP Address

Address String:

☑ Use a discovered remote host address

Remote Identity
Identification Type auf "IP Address" stellen



Authentication Method: Mutual PSK + XAuth

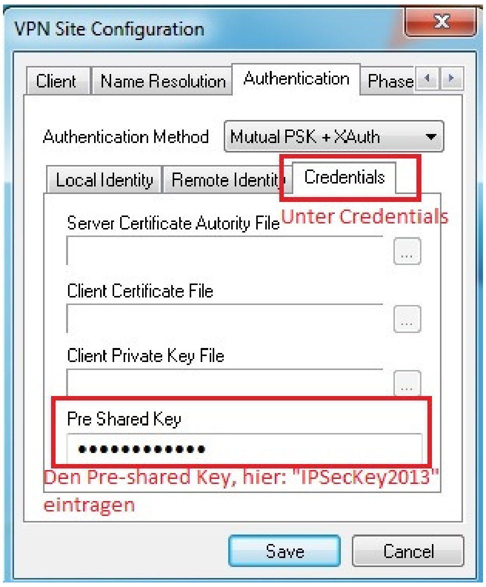
Identification Type: IP Address

Address String:

☑ Use a discovered remote host address

Use a discovered remote host address verwenden

Unter Credentials tragen Sie als Pre-shared key, den im DWC-1000 vergebenen Pre-shared key ein, hier: „IPSecKey2013“



VPN Site Configuration

Client | Name Resolution | Authentication | Phase

Authentication Method: Mutual PSK + XAuth

Local Identity | Remote Identity | Credentials

Unter Credentials

Server Certificate Autority File:

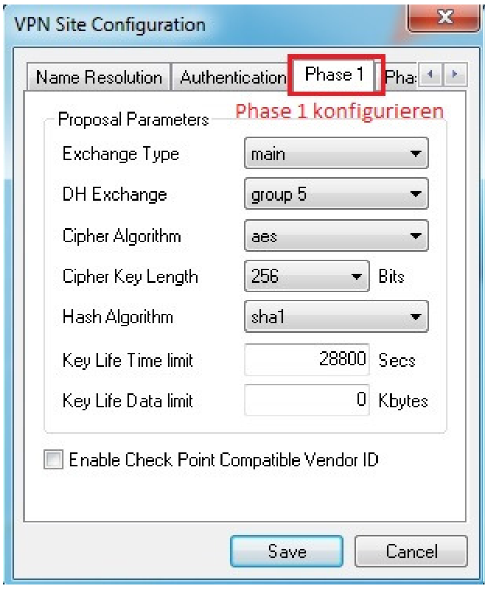
Client Certificate File:

Client Private Key File:

Pre Shared Key: ●●●●●●●●●●●●

Den Pre-shared Key, hier: "IPSecKey2013" eintragen

Konfiguration der Phase1, konfigurieren Sie die Proposals wie im DWC-1000 eingerichtet:



VPN Site Configuration

Name Resolution | Authentication | Phase 1 | Pha:

Phase 1 konfigurieren

Proposal Parameters

Exchange Type: main

DH Exchange: group 5

Cipher Algorithm: aes

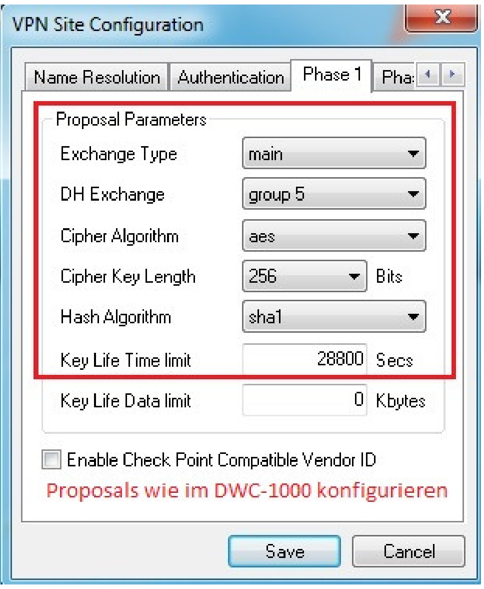
Cipher Key Length: 256 Bits

Hash Algorithm: sha1

Key Life Time limit: 28800 Secs

Key Life Data limit: 0 Kbytes

□ Enable Check Point Compatible Vendor ID



VPN Site Configuration

Name Resolution | Authentication | Phase 1 | Pha:

Proposal Parameters

Exchange Type: main

DH Exchange: group 5

Cipher Algorithm: aes

Cipher Key Length: 256 Bits

Hash Algorithm: sha1

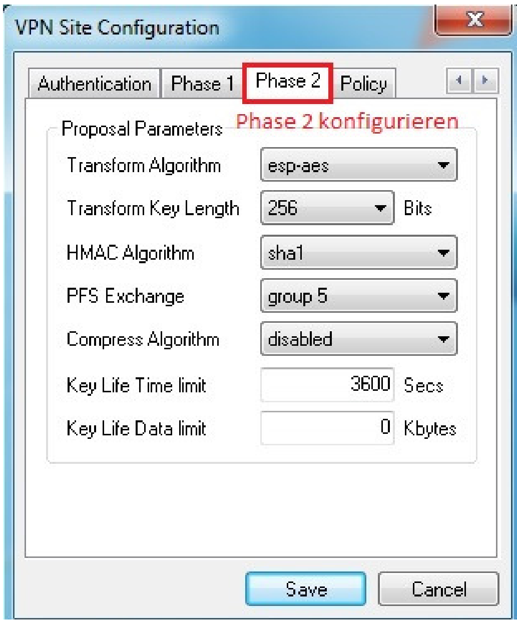
Key Life Time limit: 28800 Secs

Key Life Data limit: 0 Kbytes

□ Enable Check Point Compatible Vendor ID

Proposals wie im DWC-1000 konfigurieren

Konfiguration der Phase2, konfigurieren Sie die Proposals wie im DWC-1000 eingerichtet:

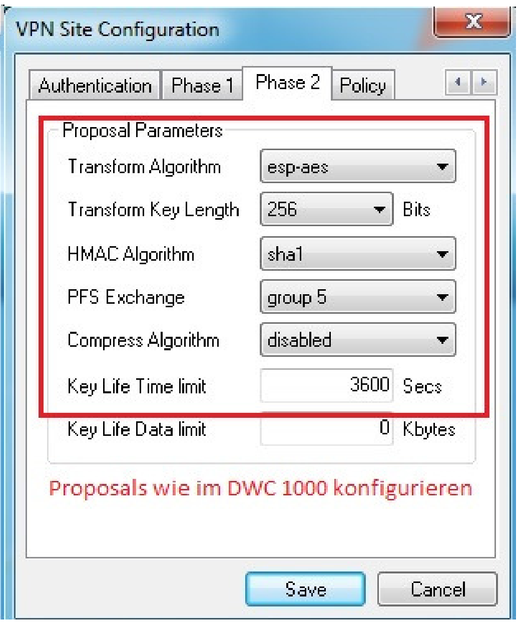


VPN Site Configuration

Phase 2 konfigurieren

Proposal Parameters

- Transform Algorithm: esp-aes
- Transform Key Length: 256 Bits
- HMAC Algorithm: sha1
- PFS Exchange: group 5
- Compress Algorithm: disabled
- Key Life Time limit: 3600 Secs
- Key Life Data limit: 0 Kbytes



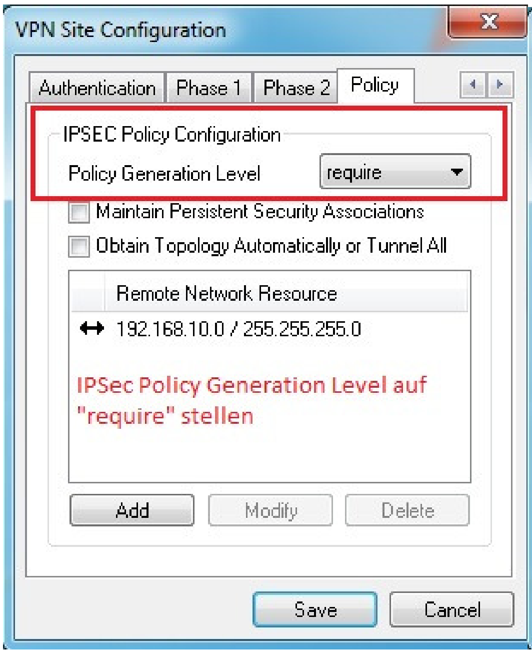
VPN Site Configuration

Proposal Parameters

- Transform Algorithm: esp-aes
- Transform Key Length: 256 Bits
- HMAC Algorithm: sha1
- PFS Exchange: group 5
- Compress Algorithm: disabled
- Key Life Time limit: 3600 Secs
- Key Life Data limit: 0 Kbytes

Proposals wie im DWC 1000 konfigurieren

Auf dem Reiter „Policy“ wählen Sie für die IPSec Policy Configuration beim Policy Generation Level „require“ aus.
Tragen Sie zudem das Remote Network, also das lokale Subnetz des DWC-1000, ein.



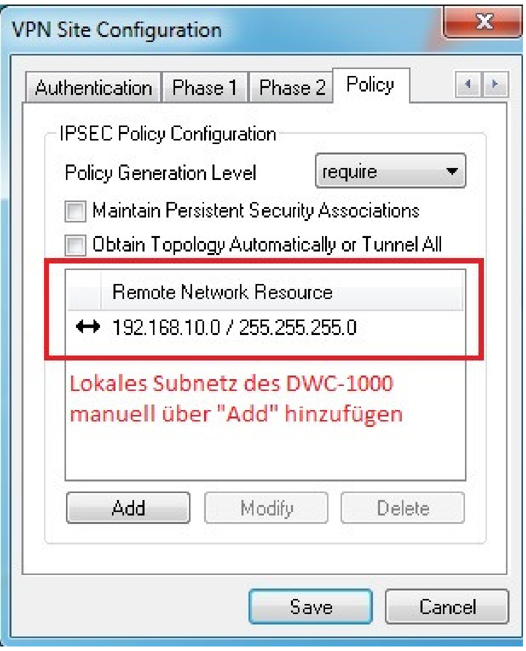
VPN Site Configuration

IPSEC Policy Configuration

- Policy Generation Level: require
- □ Maintain Persistent Security Associations
- □ Obtain Topology Automatically or Tunnel All

Remote Network Resource
↔ 192.168.10.0 / 255.255.255.0

IPSec Policy Generation Level auf "require" stellen



VPN Site Configuration

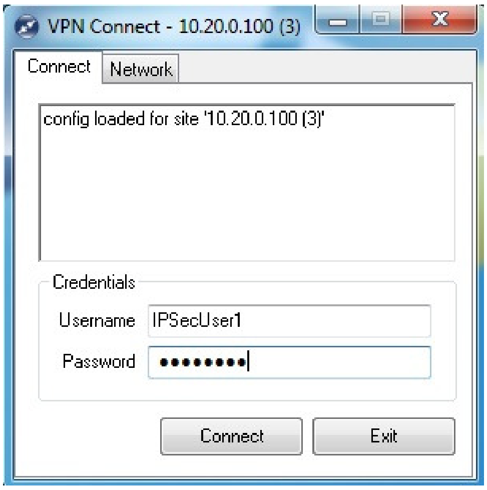
IPSEC Policy Configuration

- Policy Generation Level: require
- □ Maintain Persistent Security Associations
- □ Obtain Topology Automatically or Tunnel All

Remote Network Resource
↔ 192.168.10.0 / 255.255.255.0

Lokales Subnetz des DWC-1000 manuell über "Add" hinzufügen

Verbindung herstellen, geben Sie als Username, den im DWC angelegten User an: „IPSecUser1“ und als Passwort, das im DWC hinterlegte Passwort „ipsec123“.



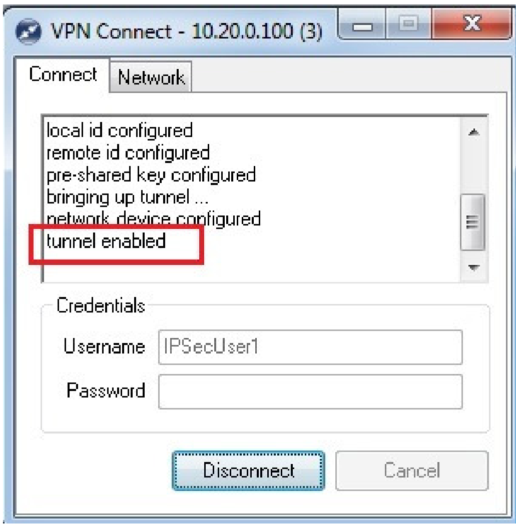
config loaded for site '10.20.0.100 (3)'

Credentials

Username: IPSecUser1

Password: ••••••••

Der Tunnel ist aufgebaut, wenn Sie „tunnel enabled“ angezeigt bekommen, und unter Network sehen, dass der Tunnel „established“ ist.

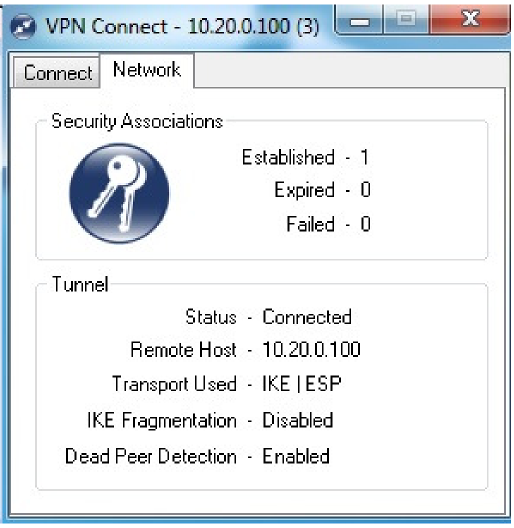


```
local id configured
remote id configured
pre-shared key configured
bringing up tunnel ...
network device configured
tunnel enabled
```

Credentials

Username: IPSecUser1

Password:



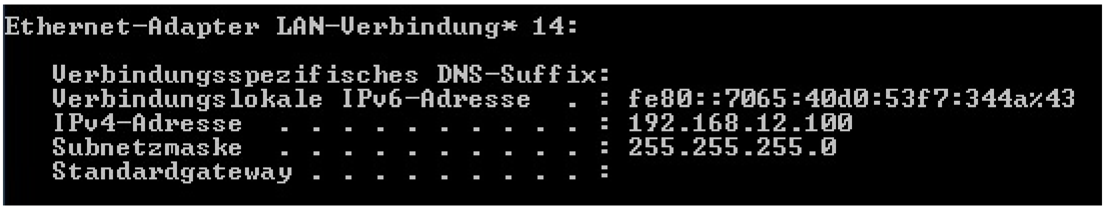
Security Associations

Established - 1
Expired - 0
Failed - 0

Tunnel

Status - Connected
Remote Host - 10.20.0.100
Transport Used - IKE | ESP
IKE Fragmentation - Disabled
Dead Peer Detection - Enabled

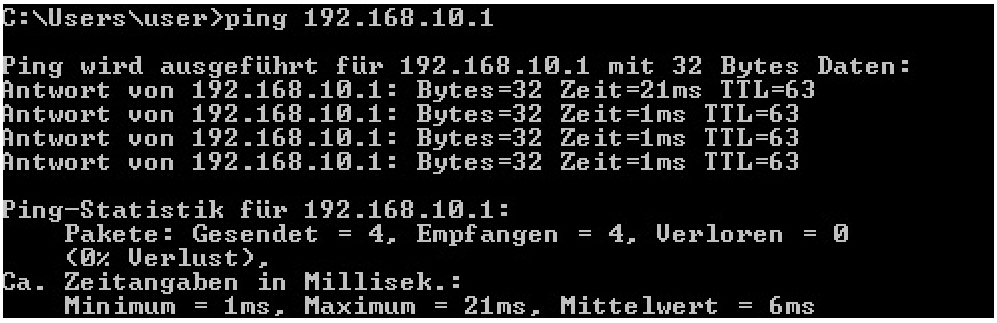
Die IP Adresse des Clients können Sie über ipconfig überpüpfen, der Client sollte eine IP Adresse des IPsec Pools des DWC-1000 erhalten. (192.168.12.100)



```
Ethernet-Adapter LAN-Verbindung* 14:

   Verbindungsspezifisches DNS-Suffix:
   Verbindungslokale IPv6-Adresse  . : fe80::7065:40d0:53f7:344a%43
   IPv4-Adresse  . . . . . . . . . . : 192.168.12.100
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Standardgateway . . . . . . . . . :
```

Sie können nun ein Device im Subnetz des DWC-1000 anpingen, oder den DWC-1000 selbst.



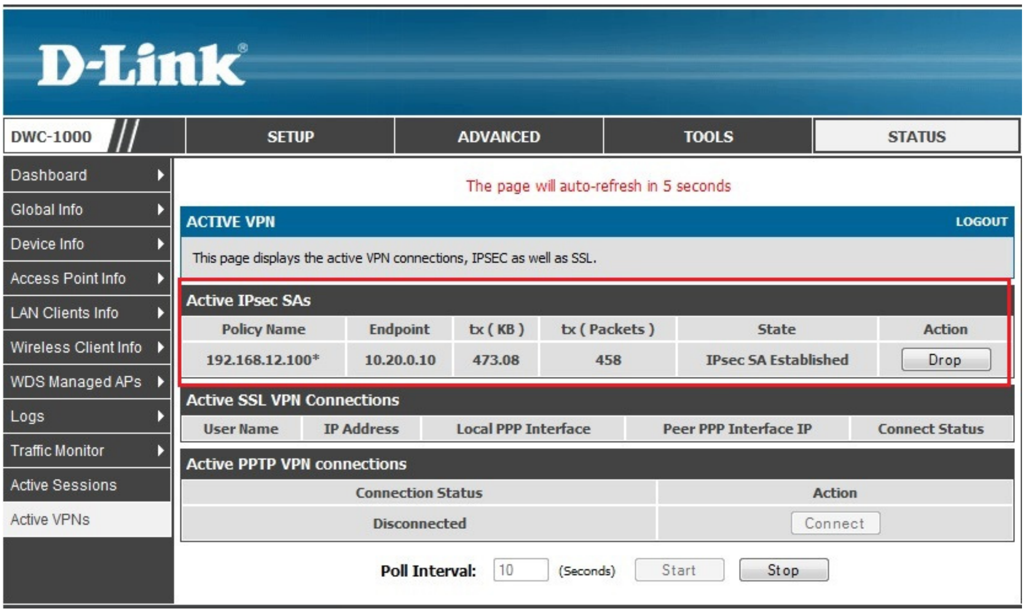
```
C:\Users\user>ping 192.168.10.1

Ping wird ausgeführt für 192.168.10.1 mit 32 Bytes Daten:
Antwort von 192.168.10.1: Bytes=32 Zeit=21ms TTL=63
Antwort von 192.168.10.1: Bytes=32 Zeit=1ms TTL=63
Antwort von 192.168.10.1: Bytes=32 Zeit=1ms TTL=63
Antwort von 192.168.10.1: Bytes=32 Zeit=1ms TTL=63

Ping-Statistik für 192.168.10.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 21ms, Mittelwert = 6ms
```

Im DWC-1000 sehen Sie die Übersicht der verbundenen Clients unter:

> Status > Active VPNs



The page will auto-refresh in 5 seconds

ACTIVE VPN

This page displays the active VPN connections, IPSEC as well as SSL.

Active IPsec SAs

Policy Name	Endpoint	tx (KB)	tx (Packets)	State	Action
192.168.12.100*	10.20.0.10	473.08	458	IPsec SA Established	Drop

Active SSL VPN Connections

User Name	IP Address	Local PPP Interface	Peer PPP Interface IP	Connect Status

Active PPTP VPN connections

Connection Status	Action
Disconnected	Connect

Poll Interval: 10 (Seconds) Start Stop