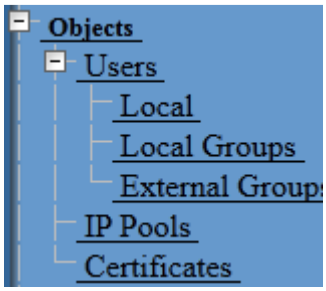
Dial-Up VPN auf eine Juniper

Gateway Konfiguration

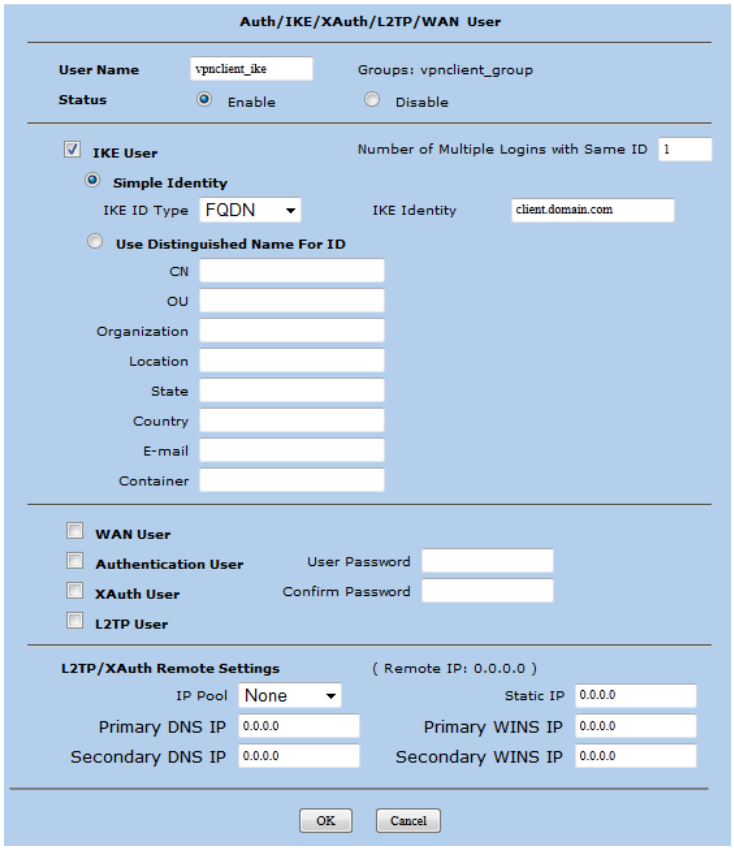
Phase 1 Konfiguration

Create a user that is used to define the phase1 id parameters. Navigate to the following screen using the tree pane on the left hand side of the browser interface.



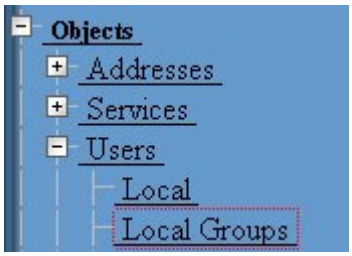
Click the New button and define the following parameters.

- User Name = vpnclient_ike
- Status = Enabled
- IKE User = Checked
    - Simple Identity = Selected
    - IKE ID Type = AUTO
    - IKE Identity = client.domain.com

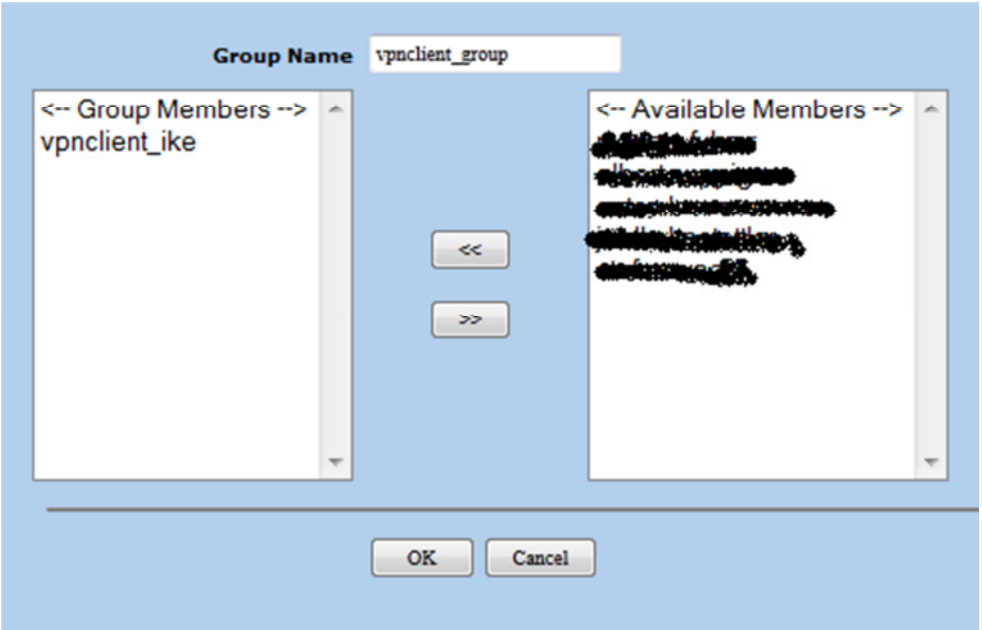


Local Key Group erstellen

Create a Local Group that can be assigned to an Auto Key Advanced Gateway. Navigate to the following screen using the tree pane on the left hand side of the browser interface.



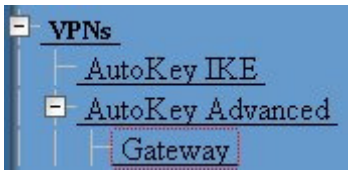
Click the New button and define the group name as vpnclient_group. Also add the vpnclient_ph1id user object as a group member.



Group Name	Group type	Members	Configure	
vpnclient_group	ike	vpnclient_ike	Edit	

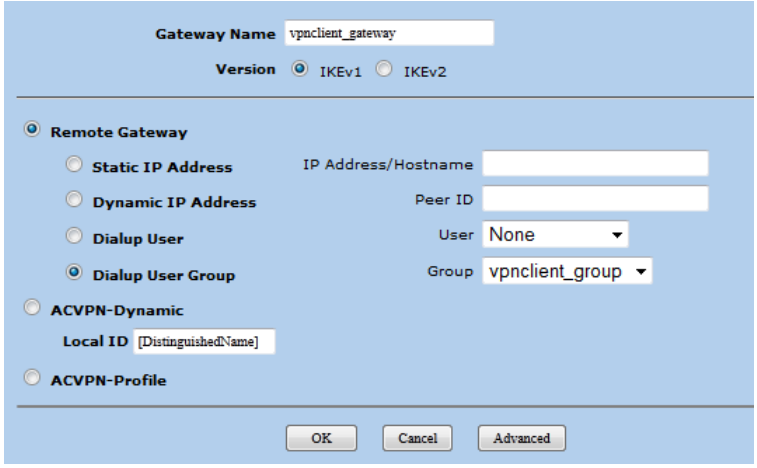
Auto Key Advanced Gateway erstellen

Create an auto key advanced gateway to configure the phase1 parameters. Navigate to the following screen using the tree pane on the left hand side of the browser interface.



Click the New button and define the following parameters.

- Gateway Name = vpnclient_gateway
- Security Level = Custom
- Remote Gateway Type = Dialup User Group
- Group = vpnclient_group
- Preshared Key = mypresharedkey
- Local ID = „FQDN“ – z.B. firewall.domain.com



Define Advanced Parameters

Click the Advanced button and define the following parameters.

- Security Level - Custom
  - Phase 1 Proposal
    - pre-g2-3des-sha
    - pre-g2-3des-md5
    - pre-g2-aes128-sha
    - pre-g2-aes128-md5
- Mode = Aggressive
- Enable NAT-Traversal = Checked
  - Keepalive Frequency = 20
- Peer Status Detection
  - DPD = Selected
    - Interval = 30
    - Retry = 5

When finished click Return.

IKEv2 Auth Method

Self None

Peer None

Preshared Key •••••••••••••••••• Use As Seed

Local ID [redacted] (optional)

Outgoing Interface ethernet0/0

Security Level

Predefined Standard Compatible Basic

User Defined Custom

Phase 1 Proposal

pre-g2-3des-sha | pre-g2-3des-md5 | pre-g2-aes128-sha | pre-g2-aes128-md5

Mode (Initiator) Main (ID Protection) Aggressive

Enable NAT-Traversal

UDP Checksum

Keepalive Frequency 20 Seconds (0~300)

Peer Status Detection

Heartbeat

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

Reconnect 0 Seconds (60~9999, 0: default)

Threshold 5 (2-9999)

DPD

Interval 30 Seconds (3~28800, 0: disable)

Retry 5 (1~127)

Always Send

Reconnect Interval 0 (60~9999) Seconds, 0 Disable

Preferred Certificate(optional)

Local Cert None

Peer CA None

Peer Type X509-SIG

Use Distinguished Name for Peer ID

CN

OU

Organization

Location

State

Country

E-mail

Container

Return Cancel

Define Xauth Parameters

You will now see your auto key advanced gateway listed. Click non the Xauth button in the Configure column.

Name	Peer Type	Address/ID/User Group	Local ID	Security Level	Configure		
vpnclient_gateway	Dialup	vpnclient_group	[redacted]	Custom	Edit	Xauth	-

Define the following parameters.

- Xauth Server = Selected
  - Allowed Authentication Type = Generic
  - Local Authentication = Selected
    - Allow Any = Selected

When finished click OK.

None

XAuth Server

Authentication Settings:

Allowed Authentication Type: Generic | CHAP Only | CHAP & PAP

Use Default Xauth Settings

Local Authentication
- Allow Any
- User: None
- User Group: None

External Authentication: None — Query Remote Setting
- Allow Any
- User: Name
- User Group: Name

Bypass Authentication

Accounting Settings:

Accounting Server: None

Accounting Off

XAuth Client

Allowed Authentication Type: Any | CHAP Only | SecurID

User Name

Password

Update DHCP Server

Prefix Delegation to IPv6 Interfaces

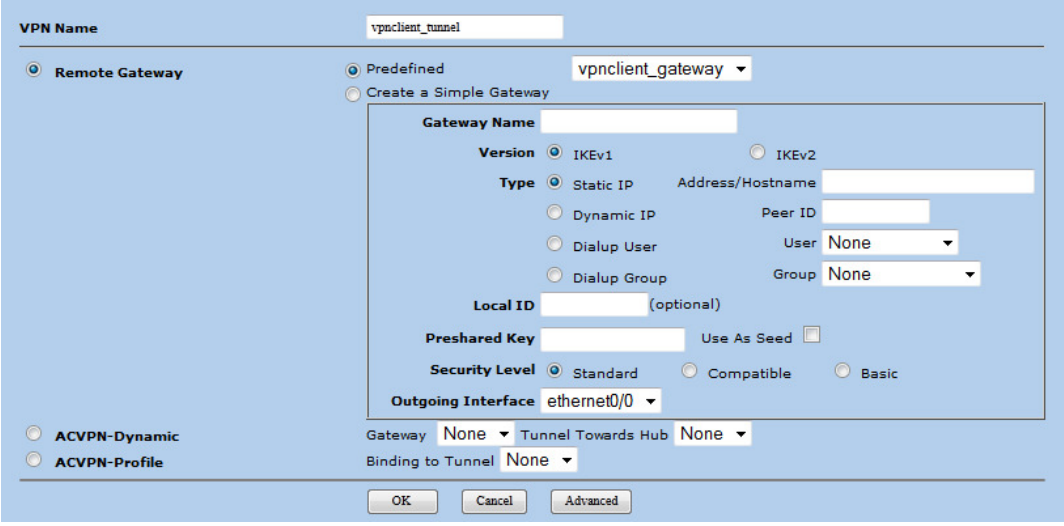
Interface	SLA ID	SLA Length	Action
		0	Add
No entry available			

OK | Apply | Cancel

Erstellen eines Auto Key IKE Gateways (Phase 2)

Clicking the New button and define the following parameters.

- VPN Name = vpnclient_tunnel
- Security Level = Custom
- Remote Gateway Predefined = vpnclient_gateway

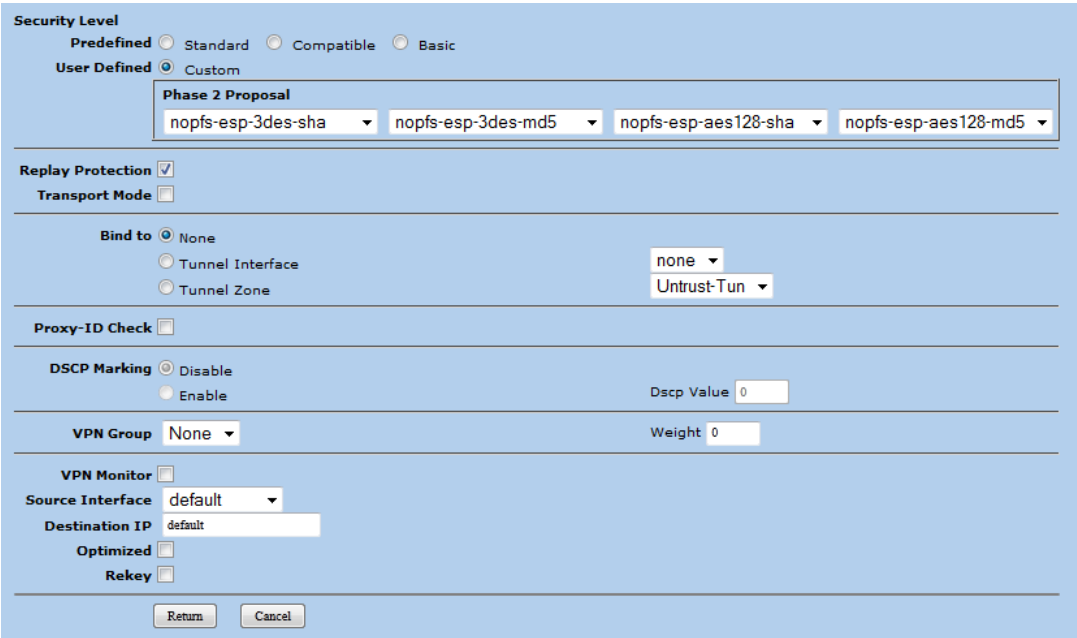


Define Advanced Parameters

Click the Advanced button and define the following parameters.

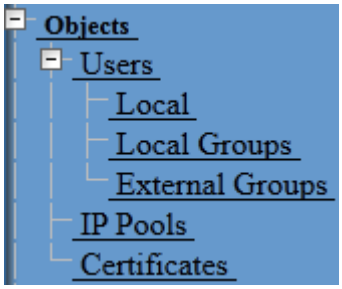
- Security Level = Custom
  - nopfs-esp-3des-sha
  - nopfs-esp-3des-md5
  - nopfs-esp-aes128-sha
  - nopfs-esp-aes128-md5
- Replay Protection = Checked

When finished click Return.

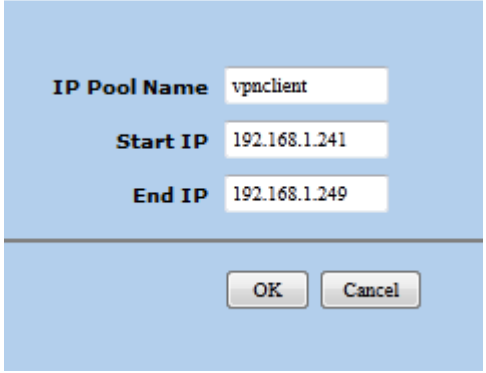


Erstellen eines Client IP Pools

Create a pool of addresses to be assigned to VPN clients. Navigate to the following screen using the tree pane on the left hand side of the browser interface.



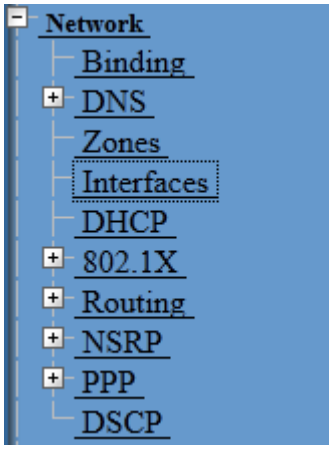
Clicking the New button and define an IP Pool. For example, you could define a pool named vpnclient with a start IP address of 192.168.1.241 and and end address of 192.168.1.249.

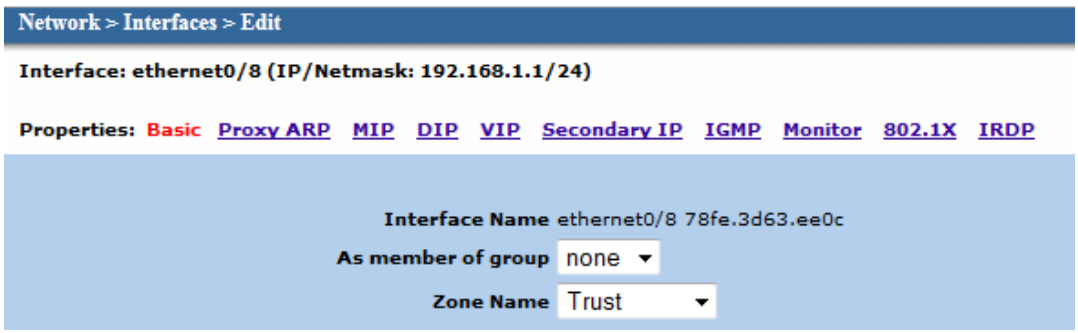


Name	Start IP	End IP	In use	Configure	
vpnclient	192.168.1.241	192.168.1.249	1	-	-

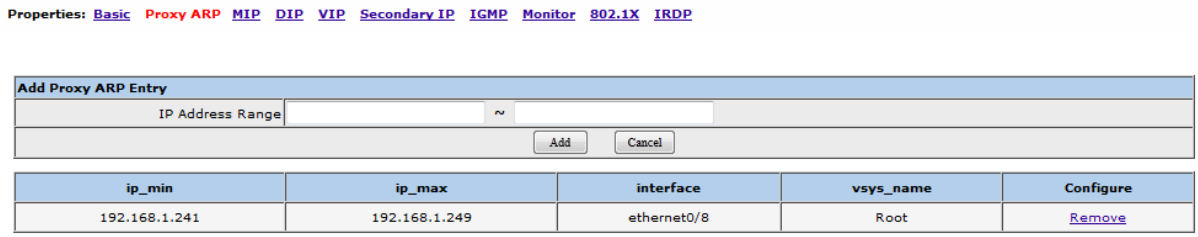
Eintragen der Proxy ARP Adressen des Client Pools

Unter Netzwork / Intrafces das TRUST Interface auswählen.



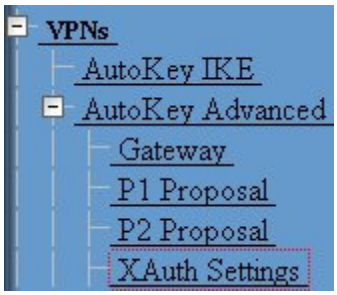


Hier den Eintrag Proxy ARP auswählen und den selben IP Range wie bei IP Pool als Proxy ARP erfassen:



Set Client Configuration Parameters

The client configuration parameters are stored in the global Auto Key Advanced XAuth parameters. Navigate to the following screen using the tree pane on the left hand side of the browser interface.



Define the following parameters.

- Reserve Private IP for XAuth User - 480 minutes
- Default Authentication Server = Local
- Query Client Settings on Default Server - Unchecked
- CHAP - Unchecked
- IP Pool Name = vpnclient
- DNS Primary Server IP = [private DNS server address]
- DNS Secondary Server IP = [private DNS secondary address]
- WINS Primary Server IP = [private WINS server address]
- WINS Secondary Server IP = [private WINS secondary address]

Reserve Private IP for XAuth User	480 Minutes
Default Authentication Server	Local
Query Client Settings on Default Server	☐
CHAP	☐
Default Accounting Server	None
Default Accounting Off	☐
IP Pool Name	vpnclient
DNS Primary Server IP	192.168.1.31
DNS Secondary Server IP	192.168.1.32
WINS Primary Server IP	0.0.0.0
WINS Secondary Server IP	0.0.0.0

Apply Cancel

Configure IPsec Policies

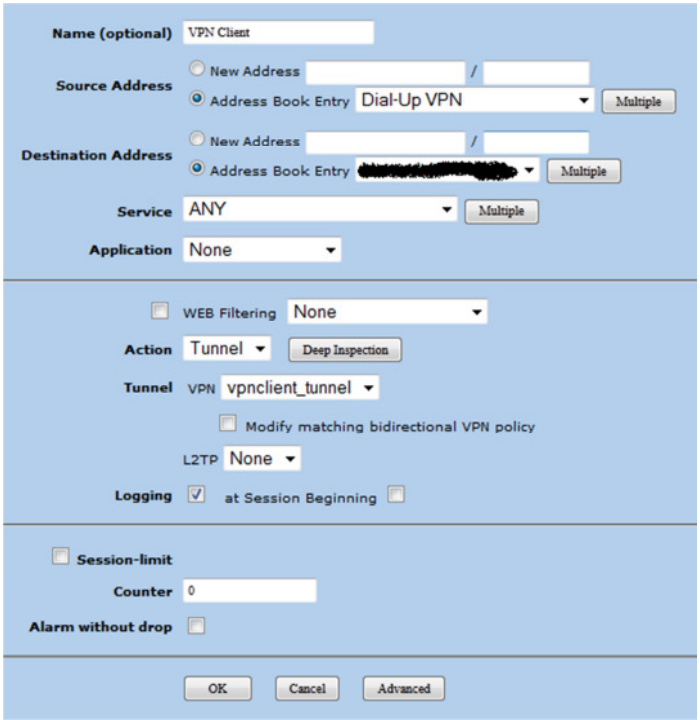
The last step for the tunnel configuration is to define policies that allow protected traffic to pass into your private network from the client. Navigate to the following screen using the tree pane on the left hand side of the browser interface.

To create a new IPsec Policy, the from and to zones must be specified. An IPsec VPN Client policy is defined. Select the following zones and click the New button.

- From = Untrust
- To = Trust

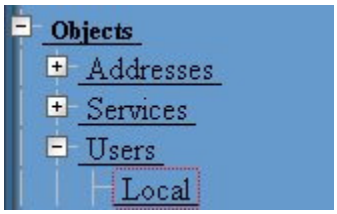
Define the following parameters.

- Name = vpnclient_inbound
- Source Address
    - Address Book Entry = Dial-UP VPN
- Destination Address
    - New Address = 192.168.1.0/24 (oder Netzwerk Unter Objects erfassen)
- Service = ANY
- Application = None (means ANY)
- Action = Tunnel
- Tunnel = vpnclient_tunnel [Auto Key IKE vpn name]



VPN Benutzer erfassen

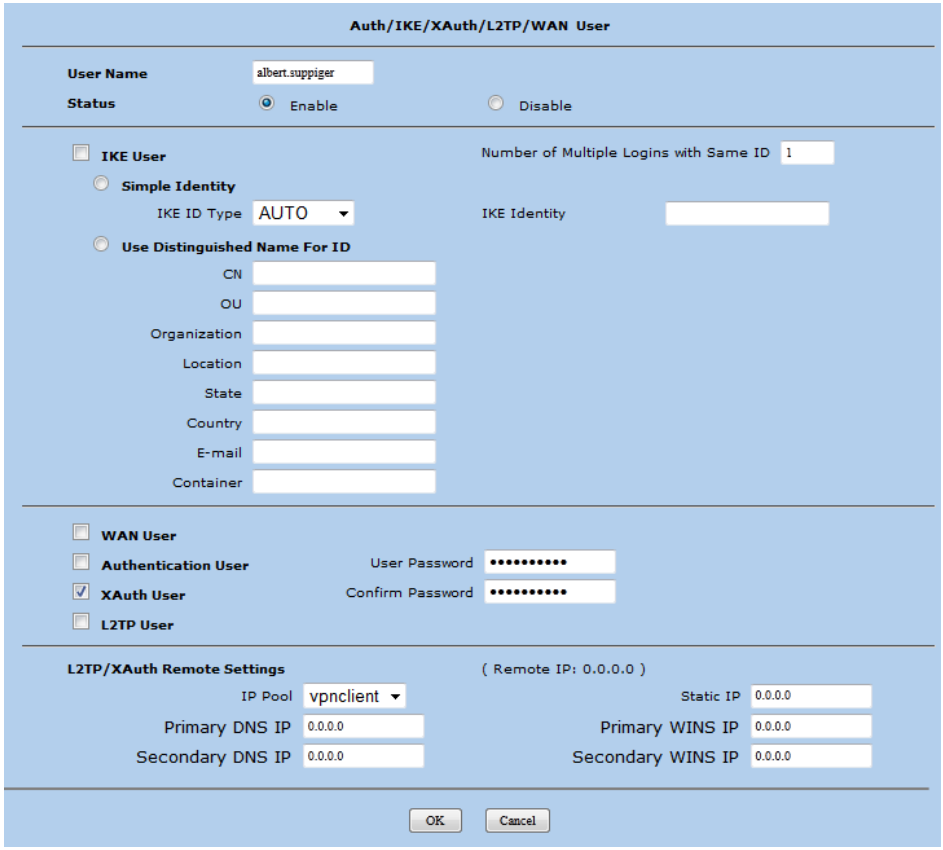
Create local user accounts that will be used during Xauth. Navigate to the following screen using the tree pane on the left hand side of the browser interface.



Click the new button and define the following parameters.

- User Name - joe (the xauth user name)
- Status - Enable
- XAuth User - Checked
    - User Password - **** (the xauth user password)
    - Confirm Password - **** (the same user password)

When finished press OK.



Name	Type	Group	Status	Identity	Configure	
[redacted]	XAuth	-	Enabled	-	Edit	Remove
[redacted]	XAuth	-	Enabled	-	Edit	Remove
[redacted]	XAuth	-	Enabled	-	Edit	Remove
[redacted]	XAuth	-	Enabled	-	Edit	Remove
[redacted]	XAuth	-	Enabled	-	Edit	Remove
vpnclient_ike	IKE	vpnclient_group	Enabled	client.domain.com	In Use	

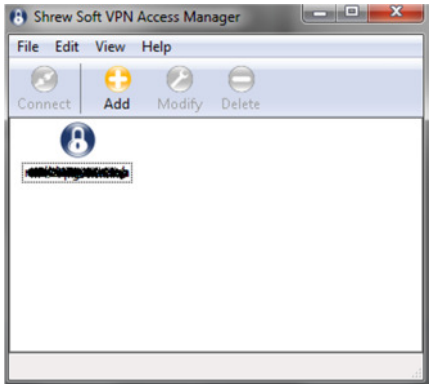
Client Konfiguration

Download des Clients

Den stable Client auf der folgenden Internetseite downloaden und installieren:

http://www.shrew.net/download

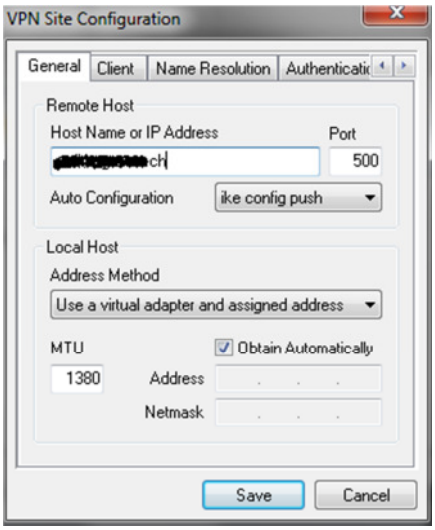
Client Configuration



The client configuration in this example is straight forward. Open the Access Manager application and create a new site configuration. Configure the settings listed below in the following tabs.

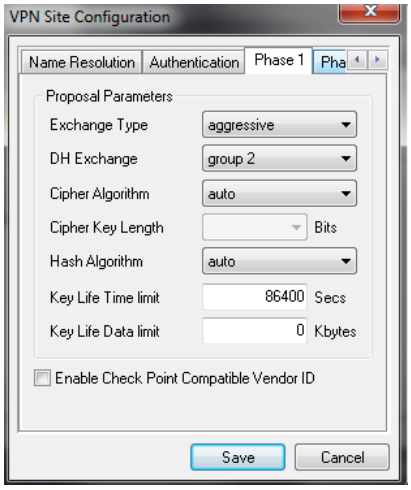
General Tab

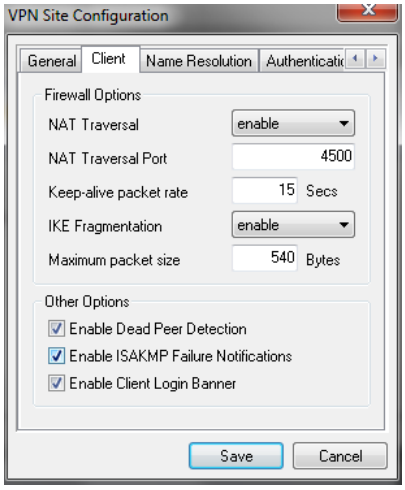
The Remote Host section must be configured. This *Host Name or IP Address* is defined to match the Junipers public interface address. The *Auto Configuration* mode should be set to *ike config push*.

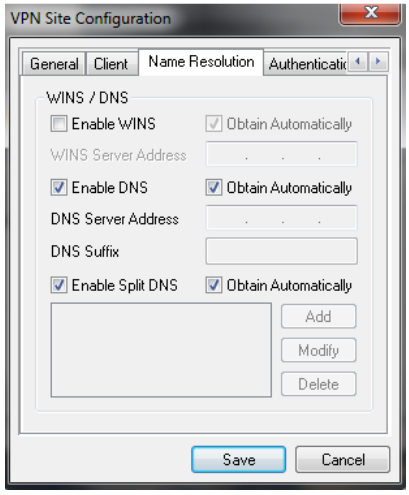


Phase 1 Tab

The Proposal section must be configured. The *Exchange Type* is set to *aggressive* and the *DH Exchange* is set to *group 2* to match the Auto Key IKE Advanced definition.

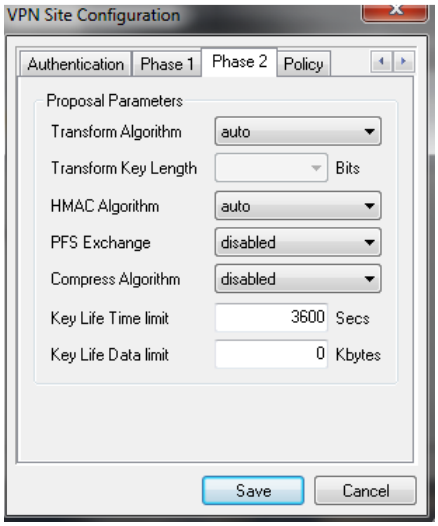






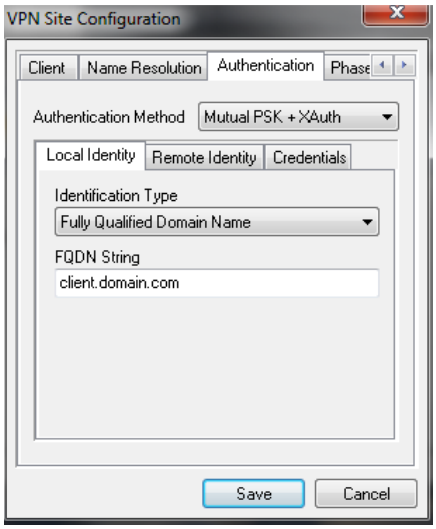
Phase 2 Tab

The Phase 2 settings must NOT be configured. Leave all settings by default.



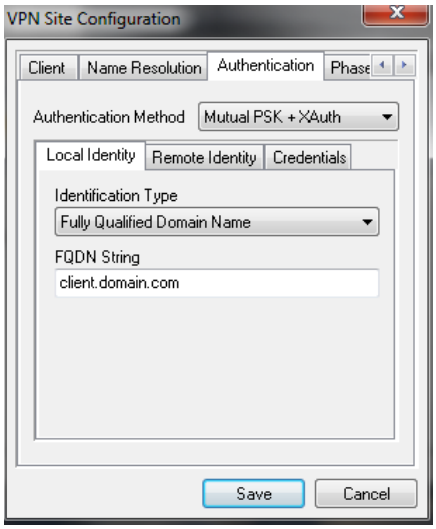
Authentication Tab

The client authentication settings must be configured. The Authentication Method is defined as *Mutual PSK + XAuth*.



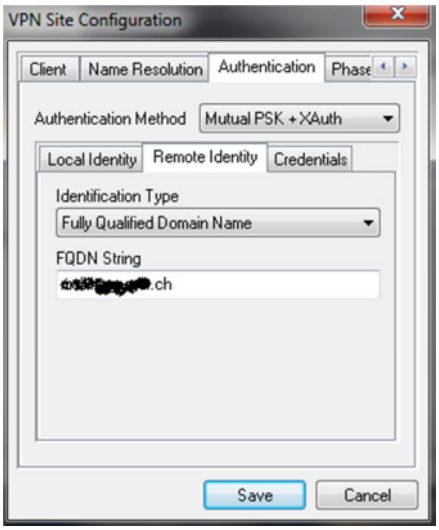
Local Identity Tab

The Local Identity parameters are defined as *Fully Qualified Domain Name* with a *FQDN String* of "client.domain.com" to match the Phase1 User ID value.



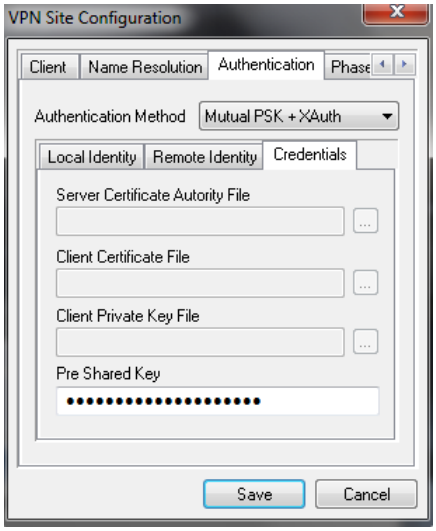
Remote Identity Tab

The Remote Identity parameters are defined as *Fully Qualified Domain Name* with a *FQDN String* of "vpngw.domain.com" to match the Auto Key Advanced Gateway ID value.



Credentials Tab

The Credentials *Pre Shared Key* is defined as "mypresharedkey" to match the Auto Key Advanced Gateway Preshared Key value.



Policy Tab

The IPsec Policy information must be manually configured when communicating with Juniper gateways. Create an include Topology entry for each IPsec Policy network created on the gateway. For our example, a single Topology Entry is defined to include the 192.168.1.0/24 network.