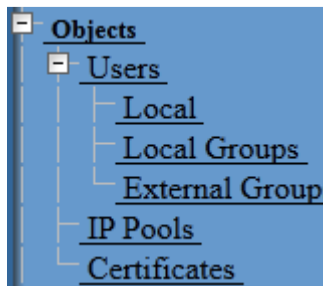


Dial-Up VPN auf eine Juniper

Gateway Konfiguration

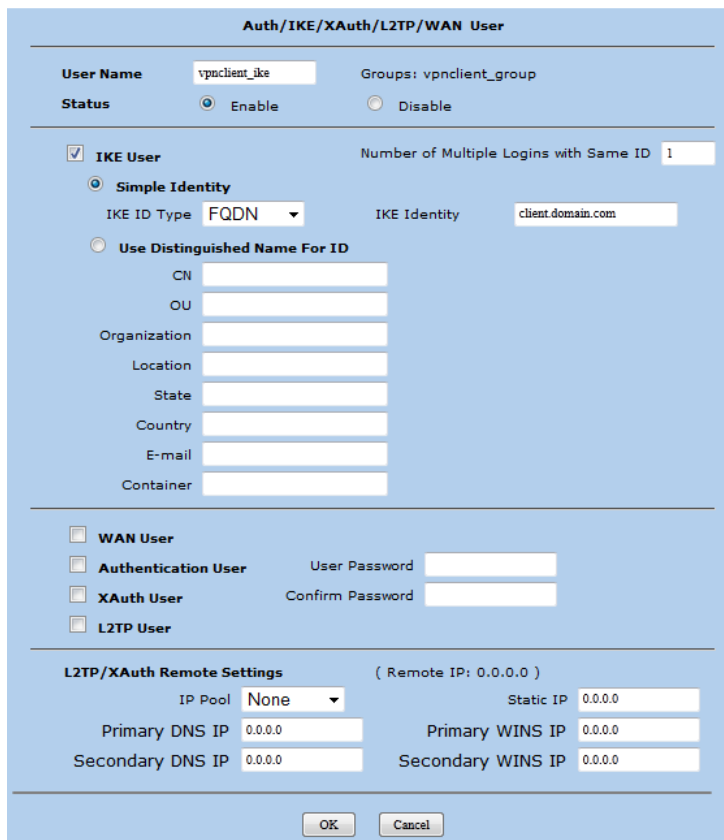
Phase 1 Konfiguration

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.



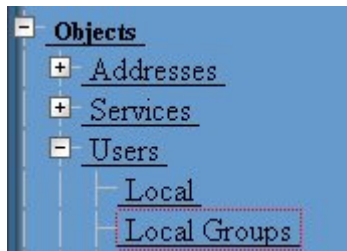
Click the New button and define the following parameters.

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

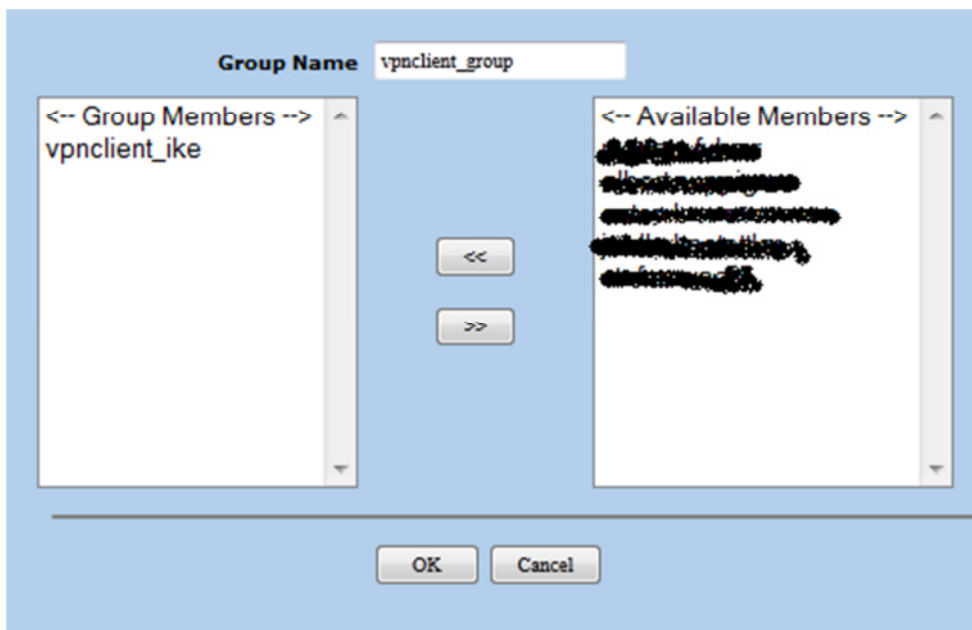
A screenshot of the 'Auth/IKE/XAuth/L2TP/WAN User' configuration form. The form is titled 'Auth/IKE/XAuth/L2TP/WAN User'. It contains several sections: 'User Name' (vpnclient_ike), 'Groups' (vpnclient_group), 'Status' (radio buttons for 'Enable' and 'Disable', with 'Enable' selected), 'IKE User' (checked), 'Number of Multiple Logins with Same ID' (1), 'Simple Identity' (selected), 'IKE ID Type' (FQDN), 'IKE Identity' (client.domain.com), 'Use Distinguished Name For ID' (radio buttons for 'CN', 'OU', 'Organization', 'Location', 'State', 'Country', 'E-mail', 'Container'), 'WAN User' (unchecked), 'Authentication User' (unchecked), 'XAuth User' (unchecked), 'L2TP User' (unchecked), 'L2TP/XAuth Remote Settings' (Remote IP: 0.0.0.0), 'IP Pool' (None), 'Static IP' (0.0.0.0), 'Primary DNS IP' (0.0.0.0), 'Primary WINS IP' (0.0.0.0), 'Secondary DNS IP' (0.0.0.0), 'Secondary WINS IP' (0.0.0.0). At the bottom are 'OK' and 'Cancel' buttons.

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.



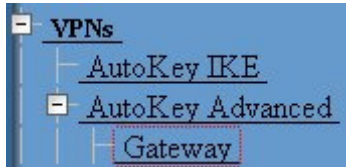
Click the New button and define the group name as vpnclient_group. Also add the vpnclient_ph1id user object as a group member.



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 ***** (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

☒ DPD

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

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

Threshold 5 (2~9999)

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	*****	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

☐ User Group

None ▾

None ▾

☐ External Authentication

None ▾

☐ Query Remote Setting

☒ Allow Any

☐ User

☐ User Group

Name

Name

☐ Bypass Authentication

Accounting Settings:

Accounting Server

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
▾	<input type="text"/>	0	<input type="button" value="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

VPN Name: vpnclient_tunnel

☒ Remote Gateway

☒ Predefined: vpnclient_gateway

☐ Create a Simple Gateway

Gateway Name:

Version: ☒ IKEv1 ☐ IKEv2

Type: ☒ Static IP Address/Hostname:

☐ Dynamic IP Peer ID:

☐ Dialup User User: None

☐ Dialup Group Group: None

Local ID: (optional)

Preshared Key: Use As Seed: ☐

Security Level: ☒ Standard ☐ Compatible ☐ Basic

Outgoing Interface: ethernet0/0

Gateway: None Tunnel Towards Hub: None

Binding to Tunnel: None

OK Cancel Advanced

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.

Security Level

Predefined: ☐ Standard ☐ Compatible ☐ Basic

User Defined: ☒ Custom

Phase 2 Proposal

nopfs-esp-3des-sha nopfs-esp-3des-md5 nopfs-esp-aes128-sha nopfs-esp-aes128-md5

Replay Protection: ☒

Transport Mode: ☐

Bind to: ☒ None ☐ Tunnel Interface: none ☐ Tunnel Zone: Untrust-Tun

Proxy-ID Check: ☐

DSCP Marking: ☒ Disable ☐ Enable Dscp Value: 0

VPN Group: None Weight: 0

VPN Monitor: ☐

Source Interface: default

Destination IP: default

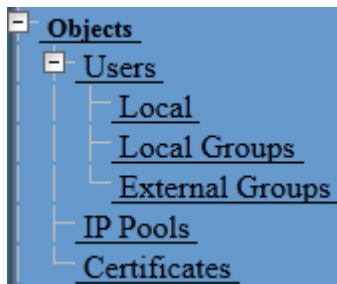
Optimized: ☐

Rekey: ☐

Return Cancel

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.



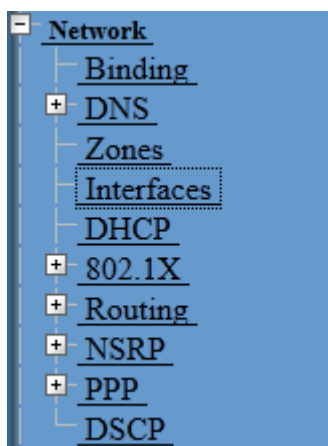
Clicking the New button and define an IP Pool. For example, you could define a pool named vpnclient with a start IP address of 192.168.1.241 and an end address of 192.168.1.249.

A screenshot of a configuration dialog box for creating an IP pool. It has a light blue background. The form contains three input fields: 'IP Pool Name' with the value 'vpnclient', 'Start IP' with the value '192.168.1.241', and 'End IP' with the value '192.168.1.249'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

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 Network / Interfaces das TRUST Interface auswählen.



Network > Interfaces > Edit

Interface: ethernet0/8 (IP/Netmask: 192.168.1.1/24)

Properties: **Basic** [Proxy ARP](#) [MIP](#) [DIP](#) [VIP](#) [Secondary IP](#) [IGMP](#) [Monitor](#) [802.1X](#) [IRDP](#)

Interface Name ethernet0/8 78fe.3d63.ee0c

As member of group none ▼

Zone Name Trust ▼

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

Properties: [Basic](#) **Proxy ARP** [MIP](#) [DIP](#) [VIP](#) [Secondary IP](#) [IGMP](#) [Monitor](#) [802.1X](#) [IRDP](#)

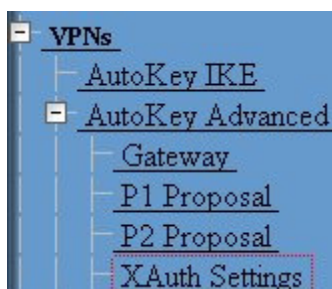
Add Proxy ARP Entry

IP Address Range ~

ip_min	ip_max	interface	vsys_name	Configure
192.168.1.241	192.168.1.249	ethernet0/8	Root	Remove

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.



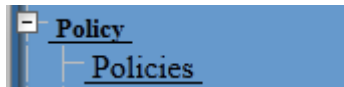
Define the following parameters.

- 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	<input type="text" value="480"/>	Minutes
<hr/>		
Default Authentication Server	<input type="text" value="Local"/>	
Query Client Settings on Default Server	<input type="checkbox"/>	
CHAP	<input type="checkbox"/>	
<hr/>		
Default Accounting Server	<input type="text" value="None"/>	
Default Accounting Off	<input type="checkbox"/>	
<hr/>		
IP Pool Name	<input type="text" value="vpnclient"/>	
DNS Primary Server IP	<input type="text" value="192.168.1.31"/>	
DNS Secondary Server IP	<input type="text" value="192.168.1.32"/>	
WINS Primary Server IP	<input type="text" value="0.0.0.0"/>	
WINS Secondary Server IP	<input type="text" value="0.0.0.0"/>	
<hr/>		
<div><input type="button" value="Apply"/> <input type="button" value="Cancel"/></div>		

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.

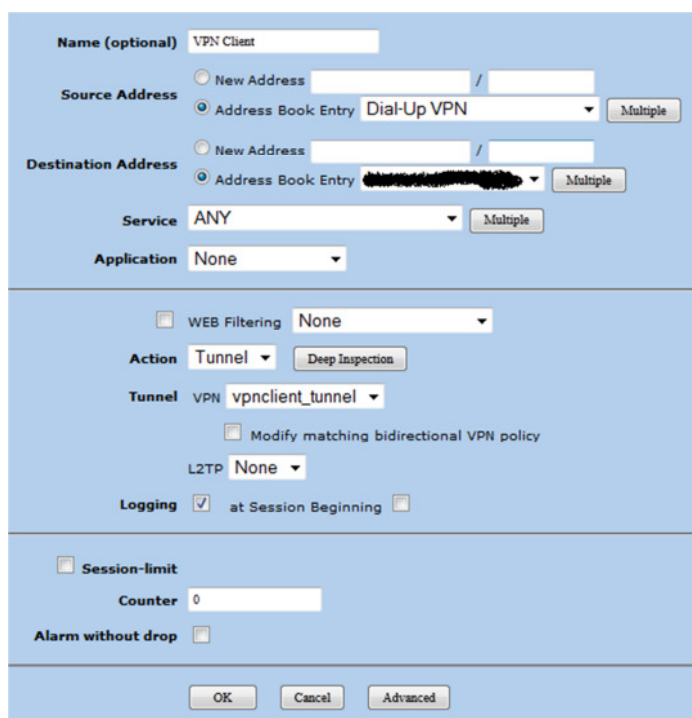
- From = Untrust
- To = Trust



The screenshot shows the 'From' dropdown set to 'Untrust' and the 'To' dropdown set to 'Trust'. There are 'Search' and 'New' buttons on the right, and a 'Go' button next to the 'To' dropdown.

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]



The screenshot shows the 'VPN Client' policy configuration dialog. The 'Name (optional)' field is 'VPN Client'. The 'Source Address' is set to 'Address Book Entry' with 'Dial-Up VPN' selected. The 'Destination Address' is set to 'New Address' with '192.168.1.0/24' entered. The 'Service' is 'ANY' and the 'Application' is 'None'. The 'Action' is 'Tunnel' with 'Deep Inspection' checked. The 'Tunnel' is 'vpnclient_tunnel'. The 'Logging' checkbox is checked with 'at Session Beginning' selected. The 'Session-limit' checkbox is unchecked, and the 'Counter' is '0'. The 'Alarm without drop' checkbox is unchecked. The 'OK', 'Cancel', and 'Advanced' buttons are at the bottom.

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.

Auth/IKE/XAuth/L2TP/WAN User

User Name

Status ☒ Enable ☐ Disable

☐ **IKE User** Number of Multiple Logins with Same ID

☒ **Simple Identity**

IKE ID Type IKE Identity

☐ **Use Distinguished Name For ID**

CN

OU

Organization

Location

State

Country

E-mail

Container

☐ **WAN User**

☐ **Authentication User** User Password

☒ **XAuth User** Confirm Password

☐ **L2TP User**

L2TP/XAuth Remote Settings (Remote IP: 0.0.0.0)

IP Pool Static IP

Primary DNS IP Primary WINS IP

Secondary DNS IP Secondary WINS IP

Name	Type	Group	Status	Identity	Configure	
vpnclient_auth	XAuth	-	Enabled	-	Edit	Remove
vpnclient_auth2	XAuth	-	Enabled	-	Edit	Remove
vpnclient_auth3	XAuth	-	Enabled	-	Edit	Remove
vpnclient_auth4	XAuth	-	Enabled	-	Edit	Remove
vpnclient_auth5	XAuth	-	Enabled	-	Edit	Remove
vpnclient_ike	IKE	vpnclient_group	Enabled	client.domain.com	In Use	

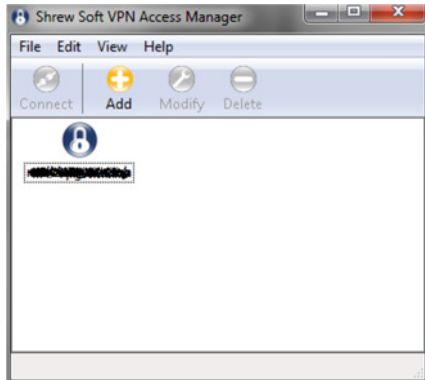
Client Konfiguration

Download des Clients

Den stable Client auf der folgenden Internetseite downloaden und installieren:

<http://www.shrew.net/download>

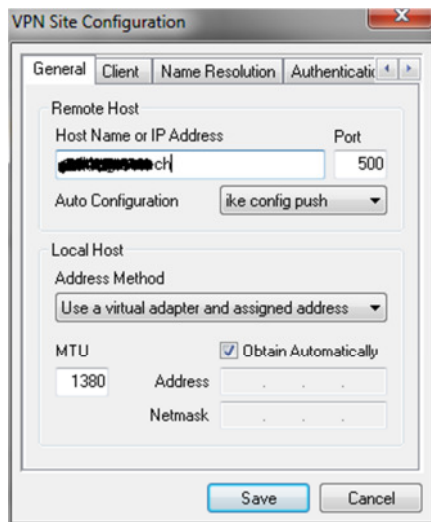
Client Configuration



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.

The image displays three screenshots of the 'VPN Site Configuration' dialog box, illustrating the configuration for the Phase 1 tab.

- Left Screenshot (Phase 1 Tab):** Shows the 'Proposal Parameters' section. The 'Exchange Type' is set to 'aggressive' and the 'DH Exchange' is set to 'group 2'. Other parameters include 'Cipher Algorithm' (auto), 'Cipher Key Length' (auto), 'Hash Algorithm' (auto), 'Key Life Time limit' (86400 Secs), and 'Key Life Data limit' (0 Kbytes). The 'Enable Check Point Compatible Vendor ID' checkbox is unchecked.
- Middle Screenshot (General Tab):** Shows the 'Firewall Options' section. 'NAT Traversal' is set to 'enable' with a port of 4500. 'Keep-alive packet rate' is 15 Secs. 'IKE Fragmentation' is set to 'enable' with a maximum packet size of 540 Bytes. Under 'Other Options', 'Enable Dead Peer Detection', 'Enable ISAKMP Failure Notifications', and 'Enable Client Login Banner' are all checked.
- Right Screenshot (Name Resolution Tab):** Shows the 'WINS / DNS' section. 'Enable WINS' is unchecked, but 'Obtain Automatically' is checked. 'WINS Server Address' is empty. 'Enable DNS' is checked, and 'Obtain Automatically' is checked. 'DNS Server Address' is empty. 'DNS Suffix' is empty. 'Enable Split DNS' is checked, and 'Obtain Automatically' is checked. There are 'Add', 'Modify', and 'Delete' buttons for the DNS list.

Phase 2 Tab

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

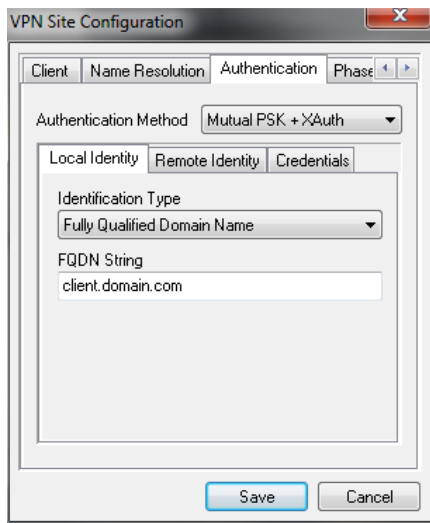
The image displays a screenshot of the 'VPN Site Configuration' dialog box, showing the 'Phase 2' tab. The 'Proposal Parameters' section is visible, with the following settings:

- 'Transform Algorithm' set to 'auto'
- 'Transform Key Length' set to 'auto' (Bits)
- 'HMAC Algorithm' set to 'auto'
- 'PFS Exchange' set to 'disabled'
- 'Compress Algorithm' set to 'disabled'
- 'Key Life Time limit' set to 3600 Secs
- 'Key Life Data limit' set to 0 Kbytes

The 'Save' and 'Cancel' buttons are at the bottom.

Authentication Tab

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

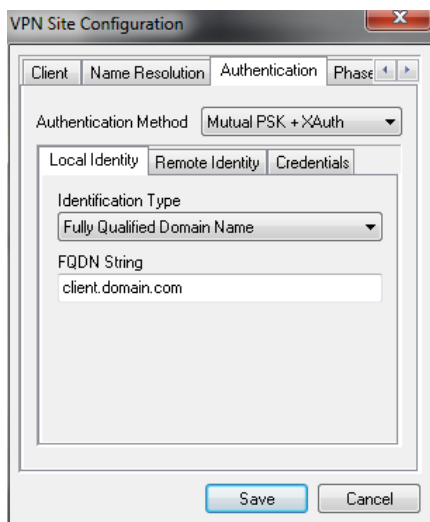


The image shows the 'VPN Site Configuration' dialog box with the 'Authentication' tab selected. The 'Authentication Method' is set to 'Mutual PSK + XAuth'. Below this, the 'Local Identity' sub-tab is active. The 'Identification Type' is set to 'Fully Qualified Domain Name', and the 'FQDN String' is 'client.domain.com'. The 'Save' and 'Cancel' buttons are at the bottom.

Client	Name Resolution	Authentication	Phase
Authentication Method: Mutual PSK + XAuth			
Local Identity Remote Identity Credentials			
Identification Type: Fully Qualified Domain Name			
FQDN String: client.domain.com			
Save Cancel			

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.

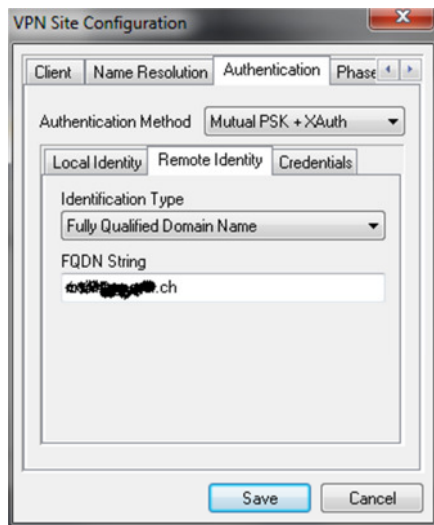


This image is identical to the one above, showing the 'VPN Site Configuration' dialog box with the 'Authentication' tab selected. The 'Authentication Method' is set to 'Mutual PSK + XAuth'. Below this, the 'Local Identity' sub-tab is active. The 'Identification Type' is set to 'Fully Qualified Domain Name', and the 'FQDN String' is 'client.domain.com'. The 'Save' and 'Cancel' buttons are at the bottom.

Client	Name Resolution	Authentication	Phase
Authentication Method: Mutual PSK + XAuth			
Local Identity Remote Identity Credentials			
Identification Type: Fully Qualified Domain Name			
FQDN String: client.domain.com			
Save Cancel			

Remote Identity Tab

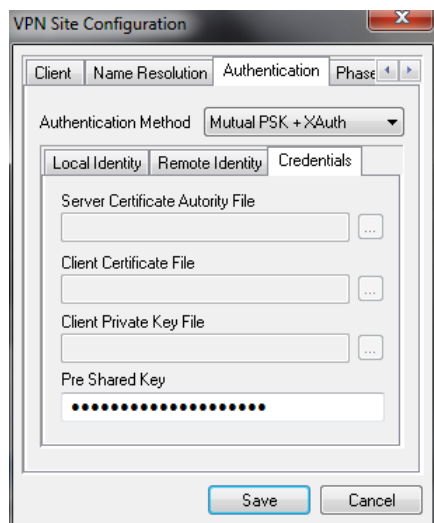
The Remote Identity parameters are defined as *Fully Qualified Domain Name* with a *FQDN String* of "vpngw.domain.com" to match the Auto Key Advanced Gateway ID value.



The image shows the 'VPN Site Configuration' dialog box with the 'Remote Identity' tab selected. The 'Authentication Method' is set to 'Mutual PSK + XAuth'. Under the 'Remote Identity' sub-tab, the 'Identification Type' is set to 'Fully Qualified Domain Name'. The 'FQDN String' field contains the text 'vpngw.domain.com'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Credentials Tab

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



The image shows the 'VPN Site Configuration' dialog box with the 'Credentials' tab selected. The 'Authentication Method' remains 'Mutual PSK + XAuth'. Under the 'Credentials' sub-tab, there are four fields: 'Server Certificate Authority File', 'Client Certificate File', 'Client Private Key File', and 'Pre Shared Key'. Each of the first three fields has a browse button (three dots). The 'Pre Shared Key' field contains the text 'mypresharedkey'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

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.

