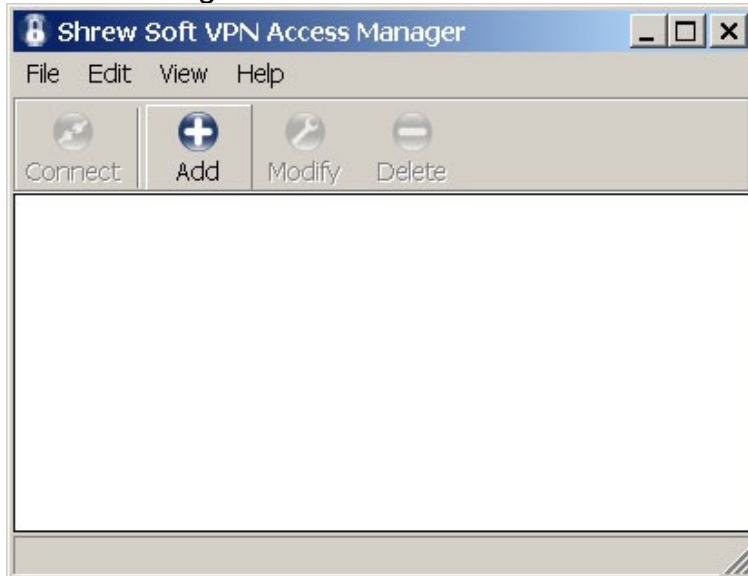


Shrew VPN-Client Konfiguration für Lancom 1611+

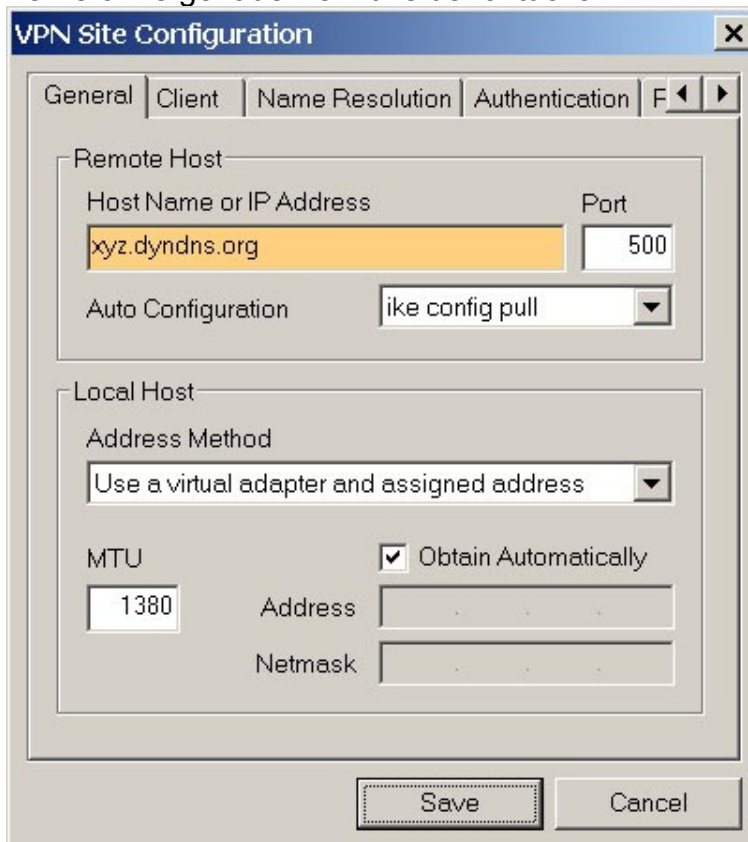
Access Manager starten und *Add* anklicken...



General-Tab

Hostnamen oder WAN-IP Adresse des Routers eintragen - weitere Einträge unverändert belassen.

(Hier helfen Tools wie bspw. DynDns bei nicht statischen öffentlichen IP-Adressen, die im LAN des Routers auf einem Rechner laufen, um den Router auch aus der Ferne ohne genaue Kenntnis der aktuellen WAN-IP erreichen zu können.)



Client-Tab

NAT Traversal und IKE Fragmentation deaktivieren.

The screenshot shows the 'Client' tab of the 'VPN Site Configuration' dialog box. The 'Firewall Options' section contains the following settings:

- NAT Traversal: **disable** (dropdown menu)
- NAT Traversal Port: 4500 (text box)
- Keep-alive packet rate: 15 Secs (text box)
- IKE Fragmentation: **disable** (dropdown menu)
- Maximum packet size: 540 Bytes (text box)

The 'Other Options' section contains three checked checkboxes:

- Enable Dead Peer Detection
- Enable ISAKMP Failure Notifications
- Enable Client Login Banner

At the bottom, there are 'Save' and 'Cancel' buttons.

Name Resolution-Tab

Unverändert belassen.

The screenshot shows the 'Name Resolution' tab of the 'VPN Site Configuration' dialog box. The 'WINS / DNS' section contains the following settings:

- Enable WINS Obtain Automatically
- WINS Server Address: (empty text box)
- Enable DNS Obtain Automatically
- DNS Server Address: (empty text box)
- DNS Suffix: (empty text box)
- Enable Split DNS Obtain Automatically

Below the 'Obtain Automatically' checkbox for Split DNS, there is a list box (currently empty) and three buttons: 'Add', 'Modify', and 'Delete'.

At the bottom, there are 'Save' and 'Cancel' buttons.

Authentication-Tab / Local Identity

Als *Authentication Method* "Mutual PSK" wählen. Als *Identification Type* "Fully Qualified Domain Name" wählen. Als *FQDN String* den bereits auf dem Lancom-Router eingetragenen Domänen-Namen eintragen. (Im Beispiel my.vpn.domain)

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Authentication' tab selected. The 'Authentication Method' is set to 'Mutual PSK'. The 'Local Identity' sub-tab is active, showing 'Identification Type' as 'Fully Qualified Domain Name' and 'FQDN String' as 'my.vpn.domain'. The 'Save' and 'Cancel' buttons are at the bottom.

Authentication-Tab / Remote Identity

Als *Identification Type* "IP Address" wählen.

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Authentication' tab selected. The 'Authentication Method' is set to 'Mutual PSK'. The 'Remote Identity' sub-tab is active, showing 'Identification Type' as 'IP Address'. The 'Address String' field is empty, and the checkbox 'Use a discovered remote host address' is checked. The 'Save' and 'Cancel' buttons are at the bottom.

Authentication-Tab / Credentials

Als *Preshared Key* den bereits auf dem Router gewählten Preshared Key (das Passwort) eintragen.

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Authentication' tab selected. Within this tab, the 'Credentials' sub-tab is active. The 'Authentication Method' is set to 'Mutual PSK'. Under the 'Credentials' sub-tab, there are three file selection fields: 'Server Certificate Authority File', 'Client Certificate File', and 'Client Private Key File', each with a browse button ('...'). Below these is a 'Pre Shared Key' field containing a masked password represented by ten asterisks. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

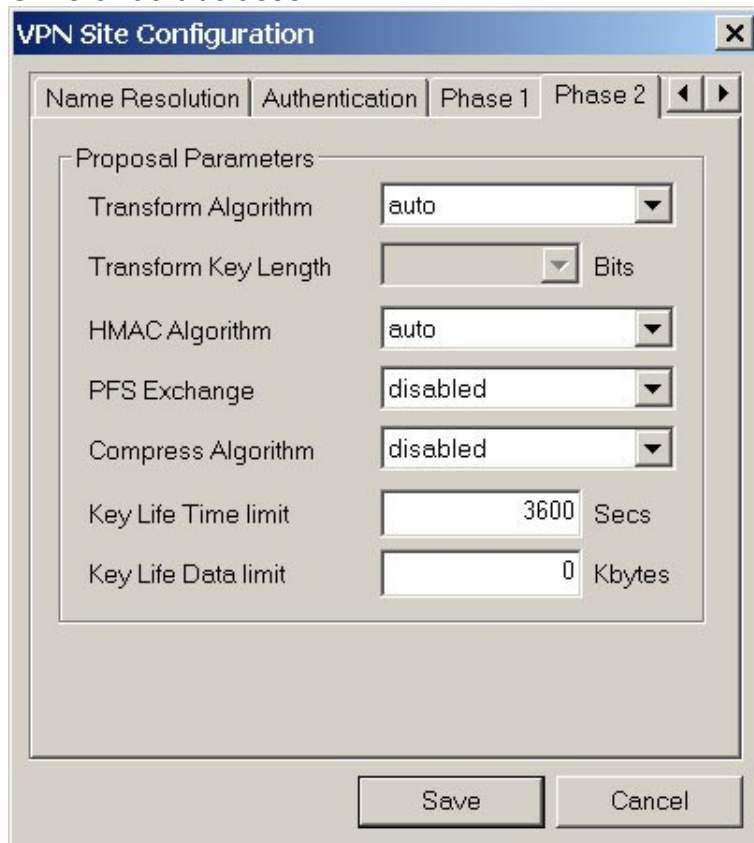
Phase 1-Tab

Unverändert belassen.

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Phase 1' tab selected. The 'Proposal Parameters' section contains the following settings: 'Exchange Type' is 'aggressive', 'DH Exchange' is 'group 2', 'Cipher Algorithm' is 'auto', 'Cipher Key Length' is set to a dropdown menu followed by 'Bits', 'Hash Algorithm' is 'auto', 'Key Life Time limit' is '86400 Secs', and 'Key Life Data limit' is '0 Kbytes'. There is an unchecked checkbox for 'Enable Check Point Compatible Vendor ID'. At the bottom are 'Save' and 'Cancel' buttons.

Phase 2-Tab

Unverändert belassen.



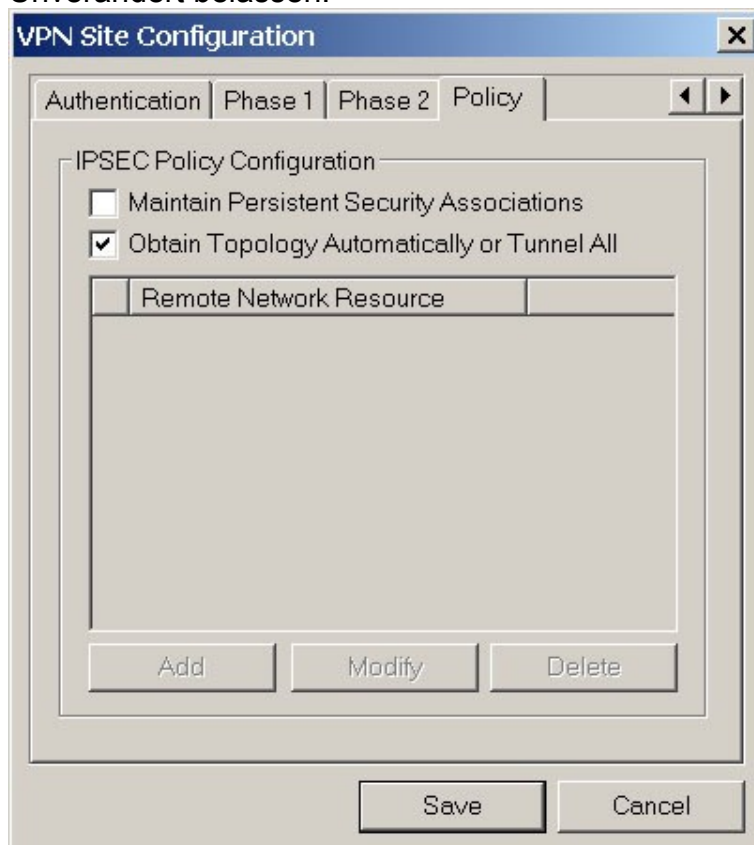
The image shows the 'VPN Site Configuration' dialog box with the 'Phase 2' tab selected. The 'Proposal Parameters' section contains the following settings:

- Transform Algorithm: auto
- Transform Key Length: [dropdown] Bits
- HMAC Algorithm: auto
- PFS Exchange: disabled
- Compress Algorithm: disabled
- Key Life Time limit: 3600 Secs
- Key Life Data limit: 0 Kbytes

Buttons: Save, Cancel

Policy-Tab

Unverändert belassen.



The image shows the 'VPN Site Configuration' dialog box with the 'Policy' tab selected. The 'IPSEC Policy Configuration' section contains the following settings:

- Maintain Persistent Security Associations
- Obtain Topology Automatically or Tunnel All

Remote Network Resource

Buttons: Add, Modify, Delete

Buttons: Save, Cancel

Fertig!

