

## Securepoint Security Systems

Version 2007nx Release 3



•• SECUREPOINT

## Content

1	Site-to-Site with pre-shared key (PSK) and static IP addresses.....	3
2	Site-to-Site with PSK, dynamic IP addresses and DynDNS.....	4
3	Site-to-Site with PSK, one static and one dynamic IP address .....	5
4	Roadwarrior connection with PSK and Greenbow VPN client.....	6
5	Roadwarrior connection with certificate and Greenbow VPN client.....	7
6	Roadwarrior L2TP connection for Windows XP or Windows Vista with certificate.....	8
6.1	Vista without client-side NAT .....	8
6.2	Vista with client-side NAT .....	9
7	Description of the values .....	10
7.1	Phase 1 Main Mode .....	10
7.2	Phase 2 Quick Mode .....	12

# 1 Site-to-Site with pre-shared key (PSK) and static IP addresses

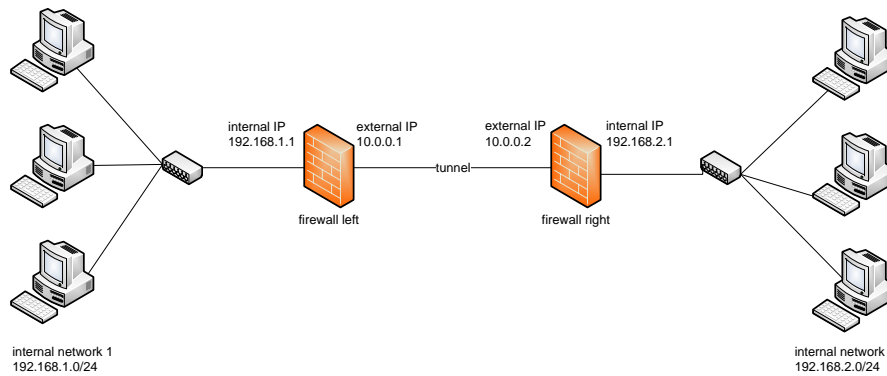


fig. 1 site-to-site with PSK and static IPs at both firewalls

Phase 1: Main Mode [left.securepoint.local>ToRight]

Local gateway: defaultroute Start automatically:

Local gateway ID: eth0

Route over gateway:  Dead peer Detection:

Remote host/gatew.: 10.0.0.2 DynDns Name:

Remote host/gatew. ID: 10.0.0.2

Local key:  Local certificate:  Advanced

IKE

Encryption: 3des Strict:

Authentication: md5

DH Group: 1024

IKE life: 1 Hours

Keyingtries: Three times

Save configuration

fig. 2 Phase 1 - left firewall

Phase 1: Main Mode [right.securepoint.local>ToLeft]

Local gateway: defaultroute Start automatically:

Local gateway ID: eth0

Route over gateway:  Dead peer Detection:

Remote host/gatew.: 192.168.1.1 DynDns Name:

Remote host/gatew. ID: 192.168.1.1

Local key:  Local certificate:  Advanced

IKE

Encryption: 3des Strict:

Authentication: md5

DH Group: 1024

IKE life: 1 Hours

Keyingtries: Three times

Save configuration

fig. 4 Phase 1 - right firewall

Phase 2: Quick Mode [left.securepoint.local>ToRight]

Native IPsec

Local Net / Mask	Remote Net / Mask
192.168.1.0 24	192.168.2.0 24

Modify Delete New

ESP

Encryption: 3des

Authentication: md5

PFS:

Key-Life: 8 Hours

fig. 3 Phase 2 - left firewall  
no entry in section L2TP

Phase 2: Quick Mode [right.securepoint.local>ToLeft]

Native IPsec

Local Net / Mask	Remote Net / Mask
192.168.2.0 24	192.168.1.0 24

Modify Delete New

ESP

Encryption: 3des

Authentication: md5

PFS:

Key-Life: 8 Hours

fig. 5 Phase 2 - right firewall  
no entry in section L2TP

## 2 Site-to-Site with PSK, dynamic IP addresses and DynDNS

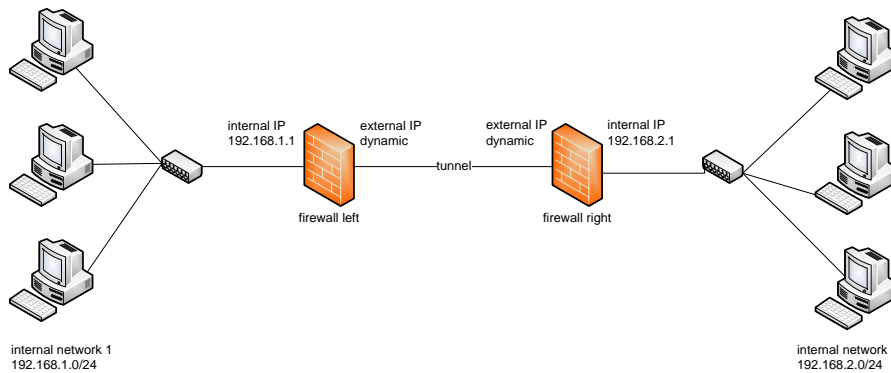


fig. 6 site-to-site with PSK and dynamic IP addresses

**Phase 1: Main Mode [left.securepoint.local>ToRight]**

Local gateway: defaultroute Start automatically

Local gateway ID: @left.dyndns.org

Route over gateway: Dead peer Detection

Remote host/gatew.: right.dyndns.org DynDns Name

Remote host/gatew. ID: @right.dyndns.org

Local key: [masked] Local certificate: [empty] Advanced

**IKE**

Encryption: 3des Strict

Authentication: md5

DH Group: 1024

IKE life: 1 Hours

Keyingtries: Three times

Save configuration

fig. 7 Phase 1 - left firewall

**Phase 1: Main Mode [right.securepoint.local>ToLeft]**

Local gateway: defaultroute Start automatically

Local gateway ID: @right.dyndns.org

Route over gateway: Dead peer Detection

Remote host/gatew.: left.dyndns.org DynDns Name

Remote host/gatew. ID: @left.dyndns.org

Local key: [masked] Local certificate: [empty] Advanced

**IKE**

Encryption: 3des Strict

Authentication: md5

DH Group: 1024

IKE life: 1 Hours

Keyingtries: Three times

Save configuration

fig. 9 Phase 1 - right firewall

**Phase 2: Quick Mode [left.securepoint.local>ToRight]**

**Native IPsec**

Local Net / Mask	Remote Net / Mask
192.168.1.0 / 24	192.168.2.0 / 24

Modify Delete New

**ESP**

Encryption: 3des

Authentication: md5

PFS:

Key-Life: 8 Hours

fig. 8 Phase 1 - left firewall  
no entry in section L2TP

**Phase 2: Quick Mode [right.securepoint.local>ToLeft]**

**Native IPsec**

Local Net / Mask	Remote Net / Mask
192.168.2.0 / 24	192.168.1.0 / 24

Modify Delete New

**ESP**

Encryption: 3des

Authentication: md5

PFS:

Key-Life: 8 Hours

fig. 10 Phase 2 - right firewall  
no entry in section L2TP

### 3 Site-to-Site with PSK, one static and one dynamic IP address

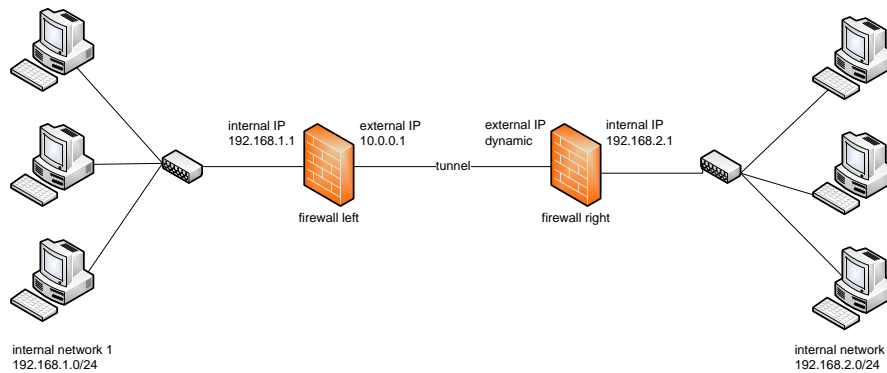


fig. 11 site-to-site with PSK - left static IP, right dynamic IP

**Phase 1: Main Mode [left.securepoint.local>ToRight]**

Local gateway: defaultroute Start automatically:

Local gateway ID: @left.dyndns.org

Route over gateway:  Dead peer Detection:

Remote host/gatew.: right.dyndns.org DynDns Name:

Remote host/gatew. ID: @right.dyndns.org

Local key:  Local certificate:  Advanced

**IKE**

Encryption: 3des Strict:

Authentication: md5

DH Group: 1024

IKE life: 1 Hours

Keyingtries: Three times

Save configuration

fig. 12 Phase 1 - left Firewall (static IP)

**Phase 1: Main Mode [right.securepoint.local>ToLeft]**

Local gateway: defaultroute Start automatically:

Local gateway ID: eth0

Route over gateway:  Dead peer Detection:

Remote host/gatew.: 192.168.1.1 DynDns Name:

Remote host/gatew. ID: 192.168.1.1

Local key:  Local certificate:  Advanced

**IKE**

Encryption: 3des Strict:

Authentication: md5

DH Group: 1024

IKE life: 1 Hours

Keyingtries: Three times

Save configuration

fig. 14 Phase 1 - right firewall (dynamic IP)

**Phase 2: Quick Mode [left.securepoint.local>ToRight]**

**Native IPsec**

Local Net / Mask	Remote Net / Mask
192.168.1.0 24	192.168.2.0 24

Modify Delete New

**ESP**

Encryption: 3des

Authentication: md5

PFS:

Key-Life: 8 Hours

fig. 13 Phase 2 - left firewall  
no entry in section L2TP

**Phase 2: Quick Mode [right.securepoint.local>ToLeft]**

**Native IPsec**

Local Net / Mask	Remote Net / Mask
192.168.2.0 24	192.168.1.0 24

Modify Delete New

**ESP**

Encryption: 3des

Authentication: md5

PFS:

Key-Life: 8 Hours

fig. 15 Phase 2 - right firewall  
no entry in section L2TP

## 4 Roadwarrior connection with PSK and Greenbow VPN client

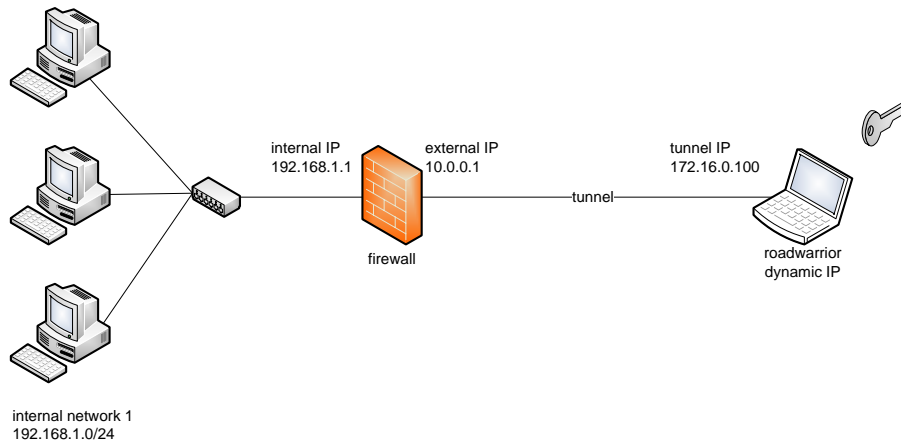


fig. 16 Roadwarrior connection with assigned tunnel IP and PSK

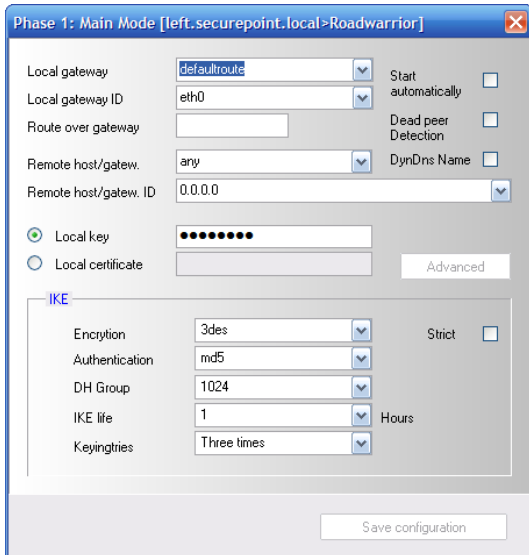


fig. 17 Phase 1 - firewall

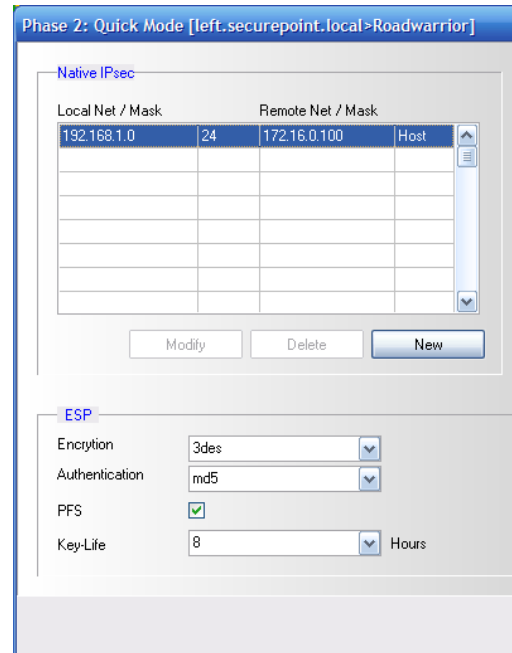


fig. 18 Phase 2 – firewall  
no entry in section L2TP

## 5 Roadwarrior connection with certificate and Greenbow VPN client

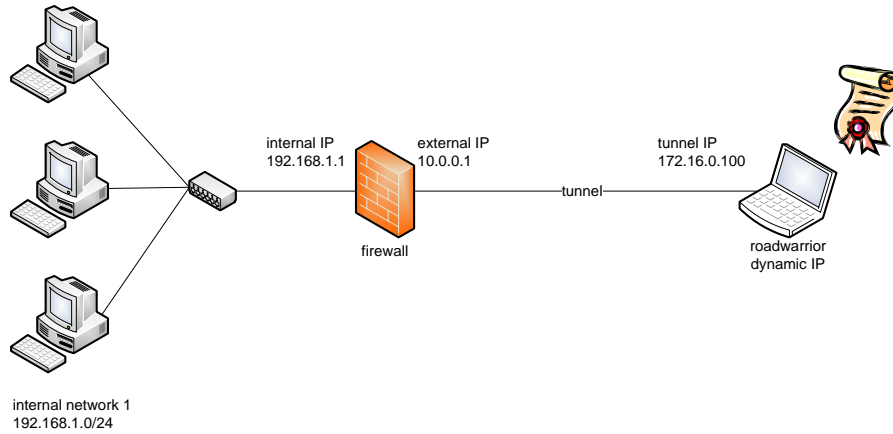


fig. 19 Roadwarrior connection with assigned tunnel IP and certificate

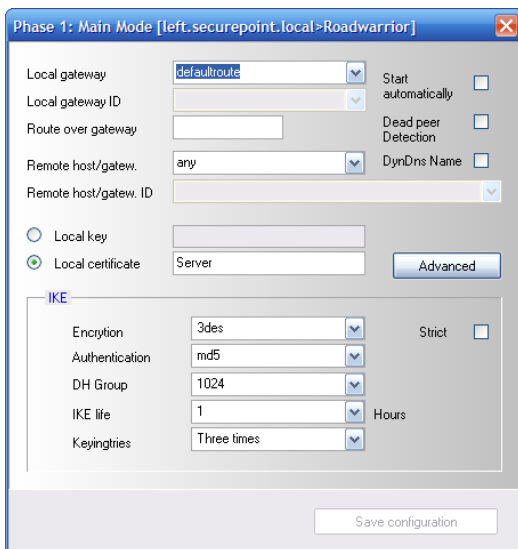


fig. 20 Phase 1 – firewall with certificate

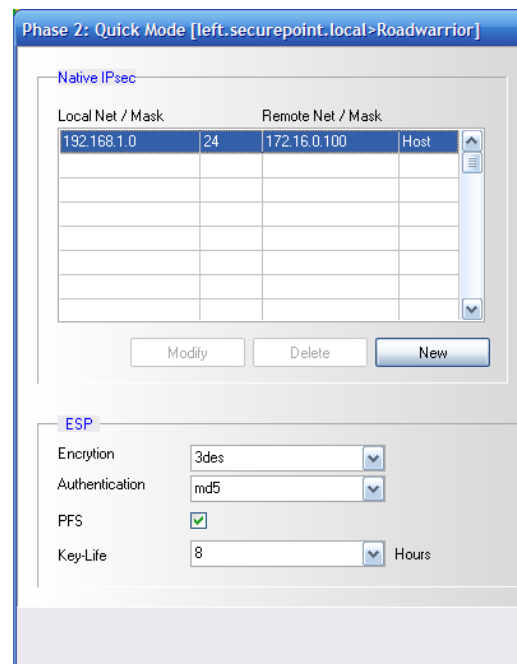


fig. 21 Phase 2 – firewall  
no entry in section L2TP

## 6 Roadwarrior L2TP connection for Windows XP or Windows Vista with certificate

### 6.1 Vista without client-side NAT

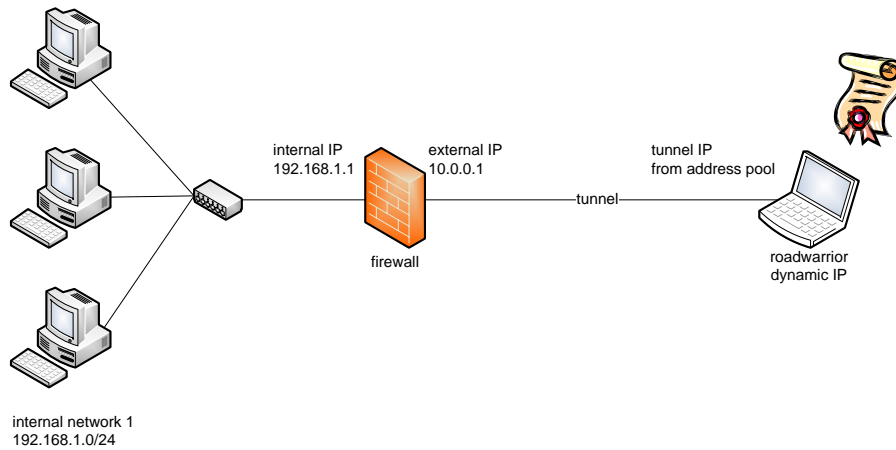


fig. 22 Roadwarrior L2TP connection with certificate and changing tunnel IP

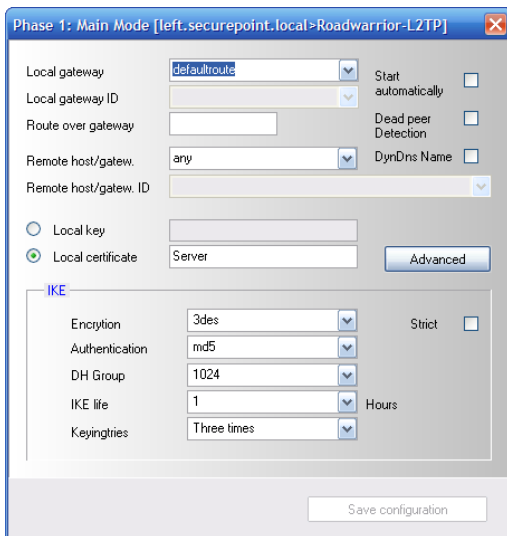


fig. 23 Phase 1 - firewall

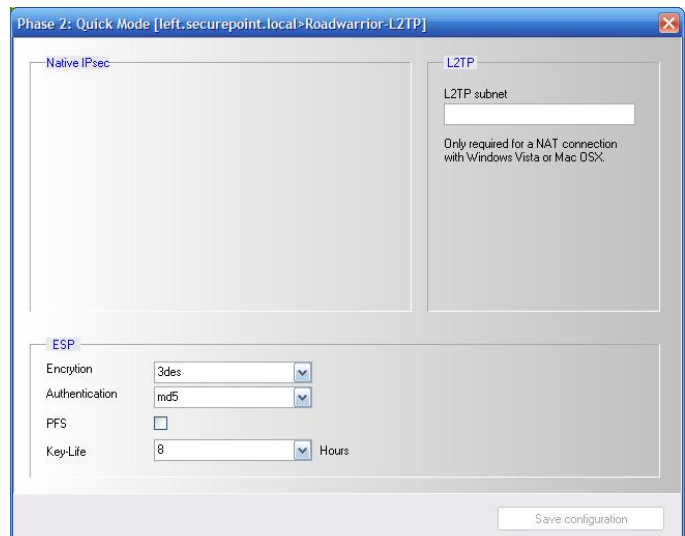


fig. 24 Phase 2 – firewall though L2TP connection no subnet entry

## 6.2 Vista with client-side NAT

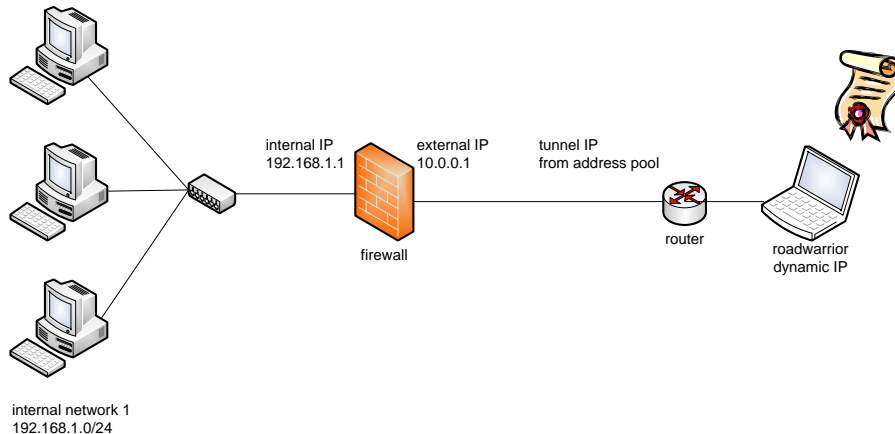


fig. 25 Roadwarrior L2TP connection with certificate and changing tunnel IP

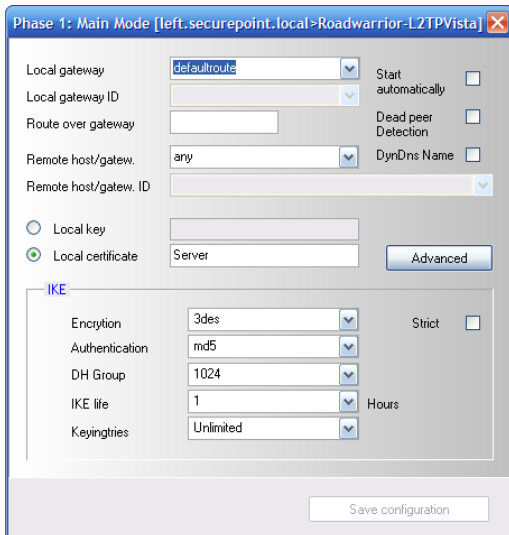


fig. 26 Phase 1 - firewall

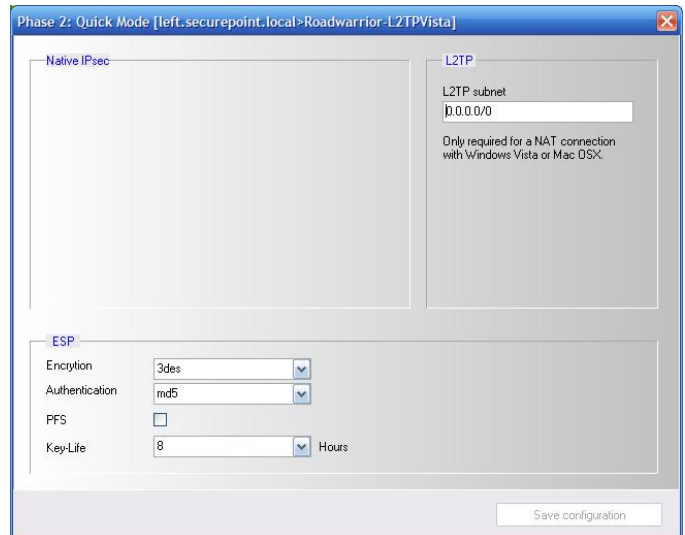


fig. 27 Phase2 - firewall with subnet entry

## 7 Description of the values

### 7.1 Phase 1 Main Mode

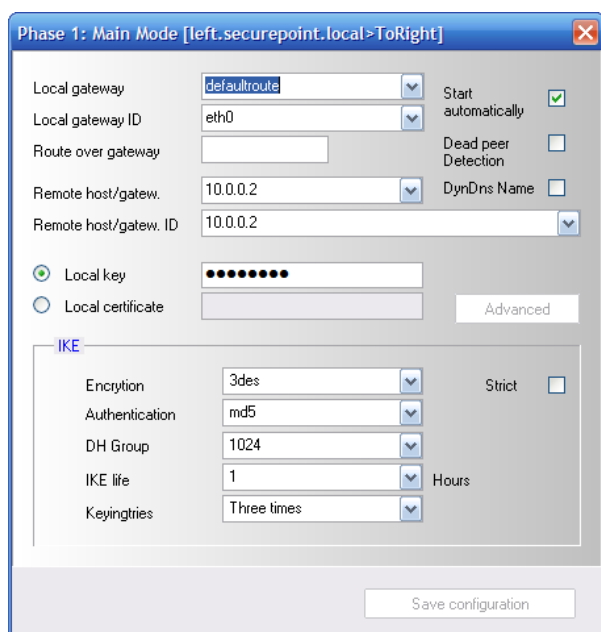


fig. 28 Dialog Phase 1 - Main Mode

#### Input- and choice boxes

Local gateway	The way the firewall reaches the remote gateway. (default: <b>defaulttroute</b> , the defaulttroute of the operating system).
Local gateway ID	Part of the authentication. <b>Eth0</b> or <b>PPP0</b> means: The IP address of the interface should be considered in the authentication. Possible values are: <ul style="list-style-type: none"> <li>– IP- addresses</li> <li>– Host names (Resolution over DNS)</li> <li>– Host names (with prefixed @ symbol without DNS resolution)</li> <li>– When using certificates: DistinguishedName (DN) or e-mail address, host name, which are posted in the certificate.</li> </ul>
Route over gateway	Alternative route for the IPsec connection (the value <b>local gateway</b> has to be changed into an IP address or in an interface name).
Remote host/gatew.	Description of the remote gateway. Possible values are: <ul style="list-style-type: none"> <li>– Host name</li> <li>– IP address</li> </ul> <p>If the remote gateway is unknown the value is set to <b>any</b> (roadwarrior connection).</p>

Remote host/gatew. ID	Part of the authentication. Possible values are: <ul style="list-style-type: none"> <li>– IP addresses</li> <li>– Host names (Resolution over DNS)</li> <li>– Host names (with prefixed @ symbol without DNS resolution)</li> <li>– When using certificates: DistinguishedName (DN) or e-mail address, host name, which are posted in the certificate.</li> </ul>
Start automatically	If checked, this gateway is the initiator of the connection. If not checked the gateway waits for a connection from outside (roadwarrior connection).
Dead Peer Detection	The tunnel will be checked for functionality every 10 seconds. If <b>Start automatically</b> is checked, the tunnel is declared to dead after three unsuccessful checks. The gateway will attempt to restart the connection. If <b>Start automatically</b> isn't checked the connection will be cleared.
DynDNS Name	If a host name is insert in the field <b>Remote host/gateway</b> and the <b>DynDNS</b> box is checked, the firewall will check, if the IP address of the host has changed. In this case the connection will be reestablished.
Local key	The preshared key (PSK or secret) of the connection. Conduce to the authentication.
Local certificate	The certificate, which is used for authentication. Following values are adjustable for the certificate: <ul style="list-style-type: none"> <li>– CERT: The Distinguished Name (DN) is used automatically as ID for authentication.</li> <li>– Subject: equates CERT but the <b>Remote Host/Gateway ID</b> can be selected.</li> <li>– Host name: The host name posted in the certificate will be used.</li> <li>– IP: The IP posted in the certificate will be used.</li> <li>– E-Mail: The e-mail address posted in the certificate will be used.</li> </ul>
<b>Section IKE</b>	
Encryption	Select the encryption method for phase 1.
Authentication	Select hash method for phase 1.
DH-Group	Diffie-Hellman Group. Method for secure determination of a shared key by using a symmetric cryptographic technique. (The value applies for phase 1 and phase 2.) for example: DH Group 2 = 1024 DH Group 5 = 1536
IKE life	Time given in hours in which the terms of phase 1 will be newly negotiated.

<b>Keyingtries</b>	How many attempts to reach the remote gateway (at intervals of 20 seconds).
<b>Strict</b>	Only accept these parameters if the remote host tries to start the connection. Otherwise other parameters can be used for encryption, authentication and DH.

## 7.2 Phase 2 Quick Mode

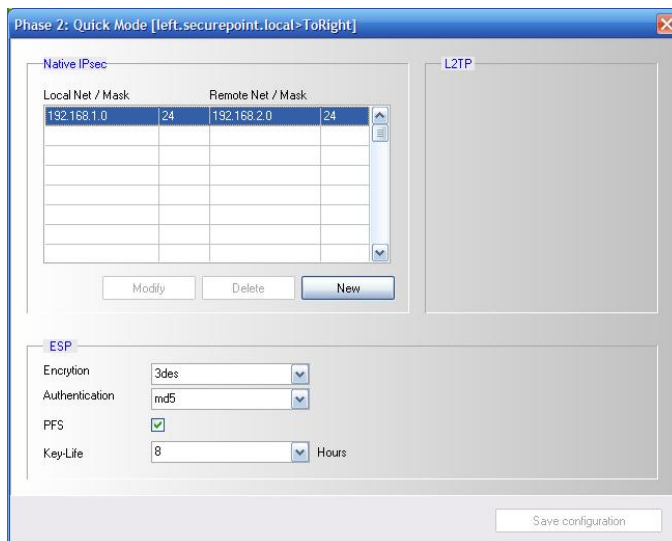


fig. 29 Dialog Phase 2 - Quick Mode

### Input- and choice boxes

<b>Locale Net / Mask</b>	Relevant for Site-to-Site and native roadwarrior connections.
<b>Remote Net / Mask</b>	Networks which shall be interconnected by IPsec.

### Section ESP

<b>Encryption</b>	Select the encryption method for phase 2.
<b>Authentication</b>	Select hash method for phase 2.
<b>PFS</b>	Perfect Forward Secrecy Assures that nobody can suggest previous and successive used keys of an IPsec connection.
<b>KeyLife</b>	Time given in hours in which the terms of phase 2 will be newly negotiated.

### Section L2TP

<b>L2TP</b>	Only relevant for L2TP connections on Windows Vista or Mac OSX when the client is positioned behind a "NATing" router. In this case, you have to post the network behind the router (subnet mask as bit count; for example: 192.168.1.0/24). If the network is unknown or changing, you have to post the value 0.0.0.0/0.
-------------	---