

# VPN IPsec - Client-to-Site

- Configuration Serveur

- Configuration générale

« Tunnel name » : Nom du tunnel

« Interface » : Interface d'écoute du tunnel

## Local Group Setup

« Local security groupe type » : Subnet

« IP Address » : Adresse du réseau local

« Subnet Mask » : Masque du réseau local

## Remote client Setup

« Remote client » : Domain Name(FQDN)

« Domain Name » : Domaine DNS sur lesquels les clients distants seront

The screenshot shows a configuration interface for a VPN. At the top, there are two radio buttons: 'Tunnel' (unselected) and 'Group VPN' (selected). Below this, the 'Group No.' is set to '1'. The 'Tunnel Name' field contains 'lan vpn'. The 'Interface' dropdown menu shows 'WAN1'. The 'Enable' checkbox is checked. The 'Local Group Setup' section has 'Local Security Group Type' set to 'Subnet', 'IP Address' set to '192.168.0.0', and 'Subnet Mask' set to '255.255.255.0'. The 'Remote Client Setup' section has 'Remote Client' set to 'Domain Name(FQDN)' and 'Domain Name' set to 'lan.local'.

- Configuration phase 1 et 2

## Phase 1 :

Group : Group 1 - 768 bit

Encryption : AES-128

Authentication : MD5

Sa Life Time : 28800

## Phase 2 :

Group : Group 2 - 1024 bit

Encryption : AES-128

Authentication : SHA1

Sa Life Time : 3600

Preshared Key : « Mot de passe » complexe à renseigner

The image shows the 'IPSec Setup' window. It is configured for 'IKE with Preshared key'. The settings are as follows:

Setting	Value
Keying Mode	IKE with Preshared key
Phase 1 DH Group	Group 1 - 768 bit
Phase 1 Encryption	AES-128
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800 seconds
Perfect Forward Secrecy	<input checked="" type="checkbox"/>
Phase 2 DH Group	Group 2 - 1024 bit
Phase 2 Encryption	AES-128
Phase 2 Authentication	SHA1
Phase 2 SA Life Time	3600 seconds
Preshared Key	VPNtestMSID07130
Minimum Preshared Key Complexity	<input checked="" type="checkbox"/> Enable
Preshared Key Strength Meter	Visual bar showing strength (mostly red/yellow)

At the bottom left, there is an 'Advanced -' button.

- Advanced

Cocher :

- « Aggressive Mode »
- « Keep-Alive »
- « NetBIOS Broadcast »
- « NAT Traversal »

The image shows the 'Advanced' configuration window. It contains the following settings:

Setting	Value
<input checked="" type="checkbox"/> Aggressive Mode	
<input type="checkbox"/> Compress (Support IP Payload Compression Protocol(IPComp))	
<input checked="" type="checkbox"/> Keep-Alive	
<input type="checkbox"/> AH Hash Algorithm	MD5
<input checked="" type="checkbox"/> NetBIOS Broadcast	
<input checked="" type="checkbox"/> NAT Traversal	

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

## • Configuration Client

Télécharger le logiciel Shrew soft VPN client for Windows

<https://www.shrew.net/download/vpn>

- Configuration Générale

### Remote host :

« Host name or IP address » : IP WAN du réseau distant

« Port » : 500

« Auto configuration » : Disable

### Local Host :

« Adaptateur mode » : Use an existing adapter and current address

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Client' tab selected. The 'Remote Host' section has 'Host Name or IP Address' set to '176.167.251.30' (highlighted with a red box), 'Port' set to '500', and 'Auto Configuration' set to 'disabled'. The 'Local Host' section has 'Adapter Mode' set to 'Use an existing adapter and current address'. Below this, there are fields for 'MTU' (1380), 'Address' (with a checkbox for 'Obtain Automatically'), and 'Netmask'. At the bottom are 'Save' and 'Cancel' buttons.

- Configuration des ports et paramètre réseau « Client »

### Firewall Options :

« NAT Traversal » : Enable

« NAT Traversal Port » : 4500

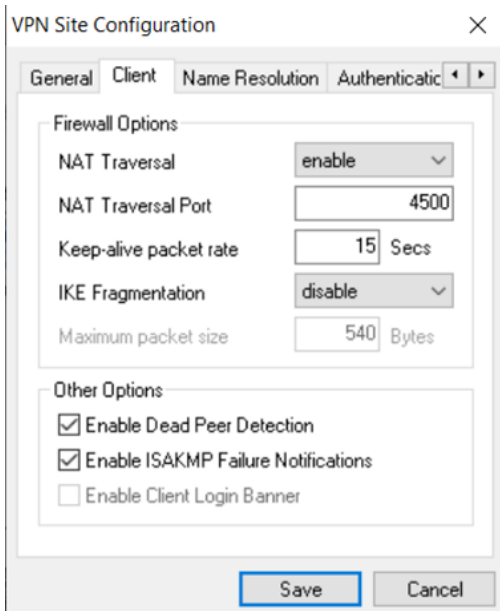
« IKE Fragmentation » : Disable

### Other options:

Cocher :

« Enable dead peer detection »

« Enable ISAKMP Failure Notification »



VPN Site Configuration

General Client Name Resolution Authentication

Firewall Options

NAT Traversal: enable

NAT Traversal Port: 4500

Keep-alive packet rate: 15 Secs

IKE Fragmentation: disable

Maximum packet size: 540 Bytes

Other Options

☒ Enable Dead Peer Detection

☒ Enable ISAKMP Failure Notifications

☐ Enable Client Login Banner

Save Cancel

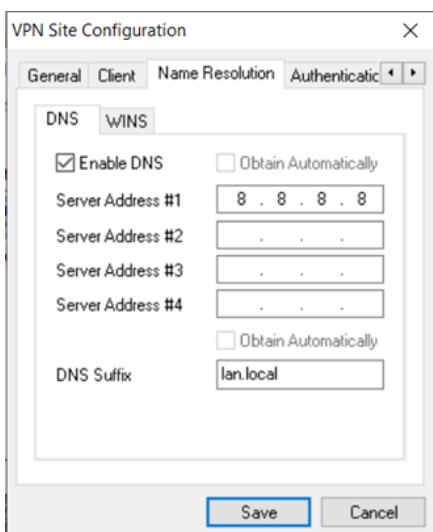
#### o Configuration DNS

Cocher Enable DNS

Servers Address #1 : 8.8.8.8

DNS Suffix : Nom du domaine renseigner sur le routeur

Onglet WINS, décocher la case.



VPN Site Configuration

General Client Name Resolution Authentication

DNS WINS

☒ Enable DNS ☐ Obtain Automatically

Server Address #1: 8 . 8 . 8 . 8

Server Address #2: . . .

Server Address #3: . . .

Server Address #4: . . .

☐ Obtain Automatically

DNS Suffix: lan.local

Save Cancel

#### o Configuration de l'authentification

Authentication Method : Mutual PSK

Onglet « Local identity »

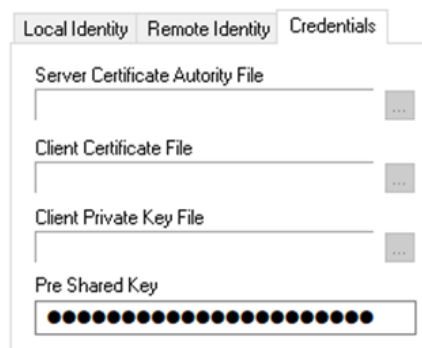
« Identification type » : Fully Qualified Domain Name.

« FQDN String » : Nom du domaine renseigner sur le routeur



Onglet « Credentials »

Pre Shared Key  Entrer la clé partager configurer sur le serveur.



- Configuration de la phase 1

Exchange Type : Aggressive

DH Exchange : Group 1

Cipher Algorithm : AES

Cipher Key Length : 128

Hash Algorithm : MD5

Key Life Time Limit : 28800



- Configuration de la phase 2

Transform Algorithm : ESP-AES

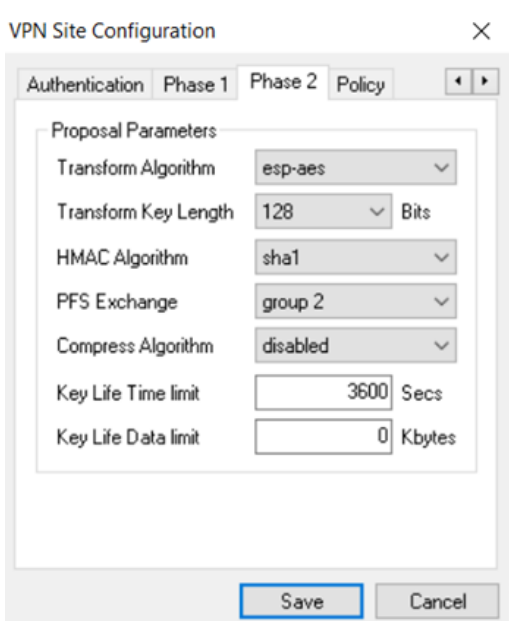
Transform Key Length : 128

HMAC Algorithm : sha1

PFS Exchange : Groupe 2

Compress Algorithm : Disable

Key Life Time Limit : 3600



- Configuration du réseau distant

« Policy Generation Level » -> Auto

Décocher « Obtain topology Automatically or tunnel All »

« Add » □ Ajouter l'adresse du réseau local distant avec son masque

VPN Site Configuration ✕

Authentication Phase 1 Phase 2 Policy ◀ ▶

IPSEC Policy Configuration

Policy Generation Level auto ▼

☐ Maintain Persistent Security Associations

☐ Obtain Topology Automatically or Tunnel All

Remote Network Resource

↔ 192.168.0.0 / 255.255.255.0

IP LAN (Distant)

Add Modify Delete

Save Cancel

Revision #4

Created 11 May 2023 15:38:56 by Corentin Roche

Updated 30 April 2024 08:22:20 by Corentin Roche