

# RV042 / RV042G

- [VPN IPsec - Client-to-Site](#)

# 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 is set to 'WAN1'. The 'Enable' checkbox is checked. A horizontal line separates this section from the 'Local Group Setup' section. In the 'Local Group Setup' section, the 'Local Security Group Type' dropdown is set to 'Subnet'. The 'IP Address' field contains '192.168.0.0' and the 'Subnet Mask' field contains '255.255.255.0'. Another horizontal line separates this from the 'Remote Client Setup' section. In the 'Remote Client Setup' section, the 'Remote Client' dropdown is set to 'Domain Name(FQDN)' and the 'Domain Name' field contains 'lan.local'.

- Configuration phase 1 et 2

## Phase 1 :

Group : Group 1 - 768 bit

Encryption : AES-128

Authentification : MD5

Sa Life Time : 28800

## Phase 2 :

Group : Group 2 - 1024 bit

Encryption : AES-128

Authentification : SHA1

Sa Life Time : 3600

Preshared Key : « Mot de passe » complexe à renseigner

The image shows the 'IPSec Setup' window. It has two main sections: Phase 1 and Phase 2. Phase 1 is configured with 'IKE with Preshared key' as the Keying Mode, 'Group 1 - 768 bit' for DH Group, 'AES-128' for Encryption, 'MD5' for Authentication, and '28800' seconds for SA Life Time. Phase 2 is configured with 'Group 2 - 1024 bit' for DH Group, 'AES-128' for Encryption, 'SHA1' for Authentication, and '3600' seconds for SA Life Time. A 'Preshared Key' field contains 'VPNtestMSID07130'. There is a 'Perfect Forward Secrecy' checkbox checked. A 'Minimum Preshared Key Complexity' checkbox is also checked and labeled 'Enable'. Below this is a 'Preshared Key Strength Meter' with a bar showing a mix of red and yellow segments. An 'Advanced -' button is at the bottom left.

IPSec Setup

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 : ☒

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 : ☒ Enable

Preshared Key Strength Meter :

Advanced -

o Advanced

Cocher :

« Aggressive Mode »

« Keep-Alive »

« NetBIOS Broadcast »

« NAT Traversal »

The image shows the 'Advanced' configuration window. It contains several checkboxes: 'Aggressive Mode' (checked), 'Compress (Support IP Payload Compression Protocol(IPComp))' (unchecked), 'Keep-Alive' (checked), 'AH Hash Algorithm' (unchecked, with a dropdown menu showing 'MD5'), 'NetBIOS Broadcast' (checked), and 'NAT Traversal' (checked). At the bottom are 'Save' and 'Cancel' buttons.

Advanced

☒ Aggressive Mode

☐ Compress (Support IP Payload Compression Protocol(IPComp))

☒ Keep-Alive

☐ AH Hash Algorithm MD5

☒ NetBIOS Broadcast

☒ NAT Traversal

Save Cancel

## • Configuration Client

Télécharger le logiciel Shrew soft VPN client for Windows

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

o 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

#### ◦ 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

#### ◦ Configuration de l'authentification

Authentication Method : Mutual PSK

Onglet « Local identity »

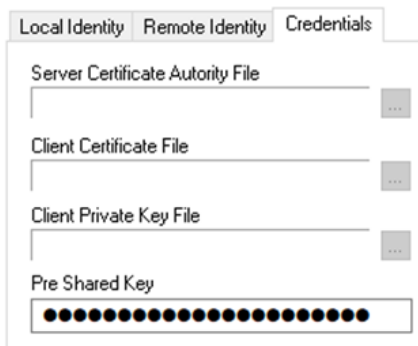
« Identification type » : Fully Qualified Domain Name.

« 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

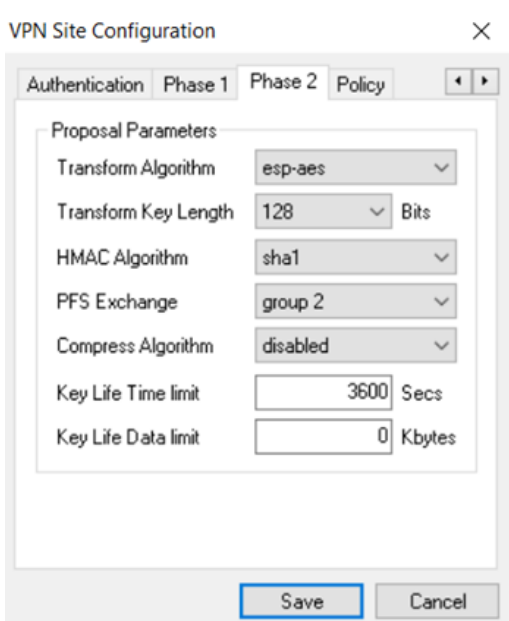
Transform Key Length : 128

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

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