



XROADS NETWORKS

---

Network Appliance How To Guide: IPSec VPN Client

# How To Guide

EDGE NETWORK APPLIANCE

# How To Guide VPN Client

---

© XRoads Networks  
17165 Von Karman • Suite 112  
888-9-XROADS

---

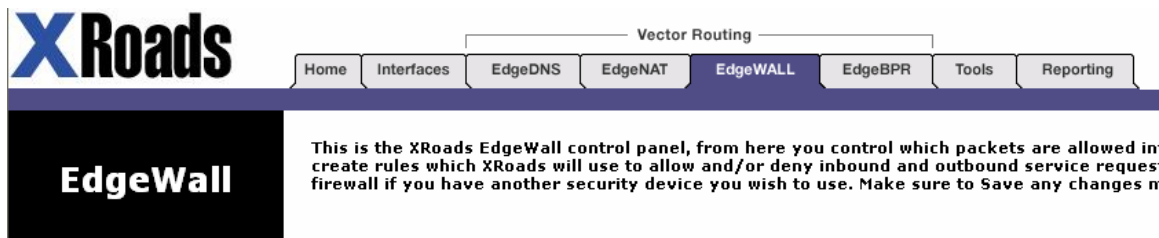
# Table of Contents

<b>VPN Client Overview</b>	<b>3</b>
<b>C O M P O N E N T S</b>	
<b>Setting Up The VPN Client</b>	<b>4</b>
<b>Configuring the Edge Appliance</b>	<b>9</b>
<b>IPSec Client Failover</b>	<b>10</b>

# Edge Configuration Series

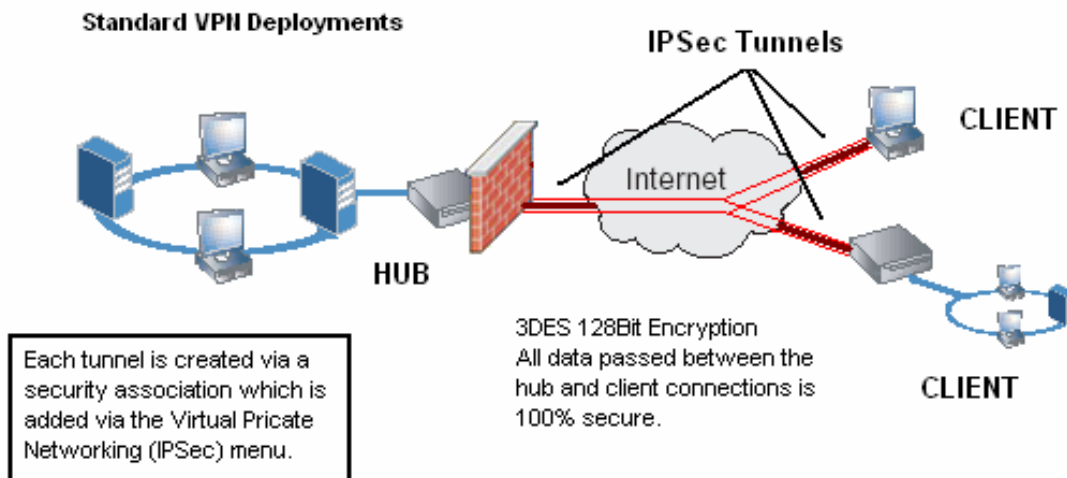
## VPN Client Overview

XRoads Networks, in conjunction with TheGreenBow Company have developed a full featured IPSec Client for the Microsoft Windows platform. This client allows any Windows PC (95, NT, 2000, XP) to connect to an Edge appliance through a secure VPN tunnel. Configuration of the VPN is performed under the EdgeWALL tab of the web interface.



### VPN Client Overview (Network Diagram)

The typical method for setting up a VPN client tunnel is between an Edge appliance acting as a hub and a remote EdgeVPN software client. The hub must always have a static IP address; the client may have a dynamic address as it initiates the VPN connection.



The next sections detail the setup and configuration of a VPN client and how to setup VPN failover. VPN failover only works with other VPN clients which comply with our VPN failover specifications, manual restart is required otherwise.

## Setting Up The VPN Client (Example Configuration)

This section provides a step-by-step overview of how to setup the VPN client on a Windows platform.

### Installing The Software

The first step is to install the software on the Windows PC. This requires downloading the software from the XRoads Networks website to the local hard drive and then double-clicking on the downloaded application to begin the installation process.

The installation process is automated, simply click the 'Finish' button when the installation has been completed. To obtain the licensing information, please contact an XRoads Networks representative and/or reseller.

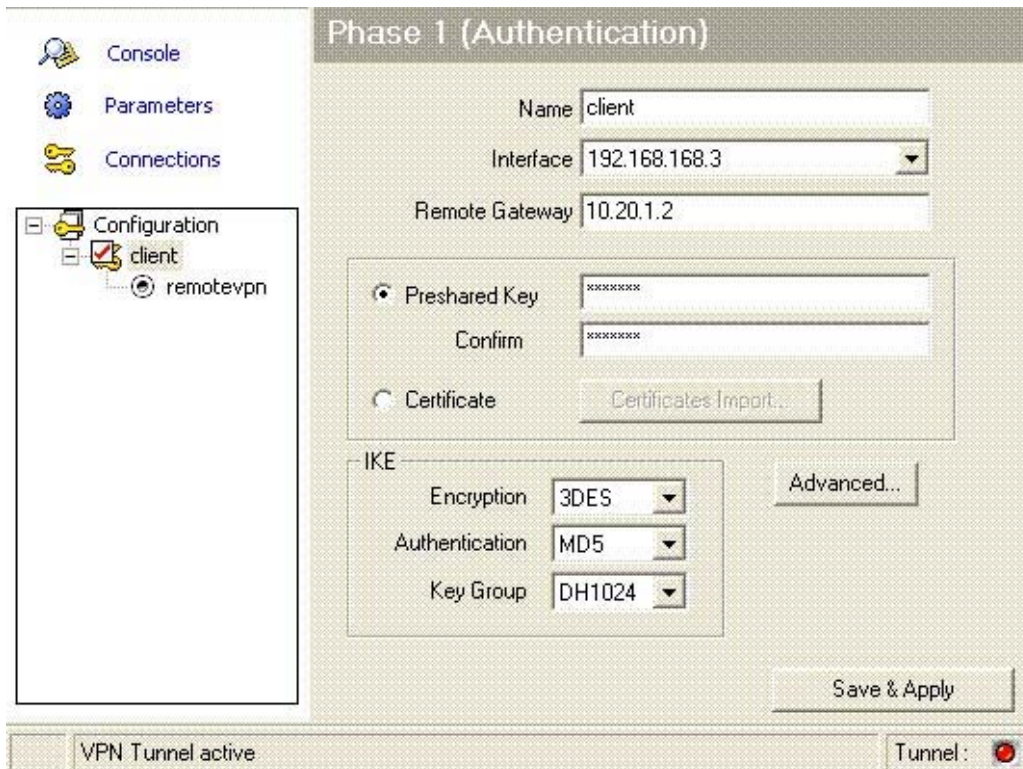
Once the installation has been completed, open the application by clicking on the icon which should have been created on the desktop. This icon is generally called, the GreenBow VPN Client, or something similar.

The procedure for creating a VPN tunnel is fairly simple, here is a list of the information required:

- What will be the name of the connection?
- What key type will you use? (Shared Secret is recommended)
- If Shared Secret, what is the key? (letters/numbers only)
- What is the WAN IP addresses of the Edge appliance?
- What is the LAN IP addresses/networks of the Edge appliance?
- Which interface will the VPN client use (if multiple)?
- What IP address will the VPN client use once connected?

## Phase 1 Configuration

Once opened the first step is to configure a new connection.



The following steps outline how to create a new connection.

Step 1) Enter a client name

Step 2) Select the interface that the VPN client will use (if multiple).

Step 2) Enter the WAN IP address of the remote Edge appliance.

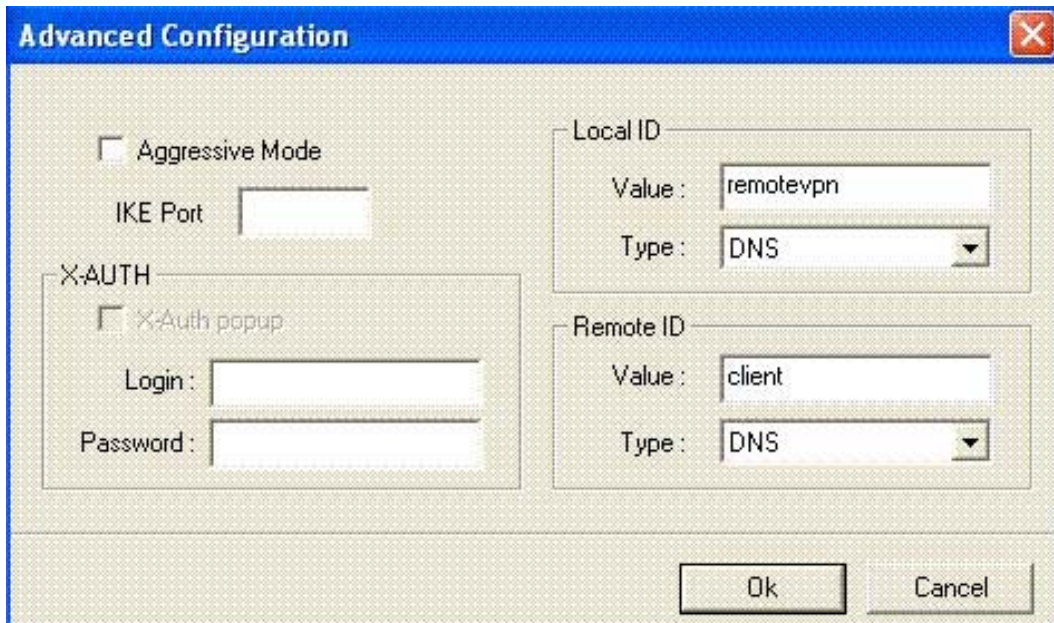
Step 3) Enter the preshared key (this is the same key that will be entered on the Edge appliance)

Step 4) Select 3DES, MD5 (could use SHA1), and DH1024 as the IKE parameters.

Now that the basics have been setup, click the 'Advanced' button.

## Phase 1 – Advanced Configuration

By clicking on the 'Advanced' button from the Phase 1 configuration page, the following dialog box will appear.



The image shows a dialog box titled "Advanced Configuration" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Aggressive Mode:** A checkbox labeled "Aggressive Mode" is currently unchecked.
- IKE Port:** A text input field for "IKE Port" is empty.
- X-AUTH:** A section containing:
  - A checkbox labeled "X-Auth popup" is unchecked.
  - A "Login:" text input field is empty.
  - A "Password:" text input field is empty.
- Local ID:** A section containing:
  - A "Value:" text input field containing the text "remotevpn".
  - A "Type:" dropdown menu currently set to "DNS".
- Remote ID:** A section containing:
  - A "Value:" text input field containing the text "client".
  - A "Type:" dropdown menu currently set to "DNS".

At the bottom of the dialog, there are two buttons: "Ok" and "Cancel".

The following steps outline how to configure the advanced settings.

Step 1) Enter a Local ID value, which is equal to the 'Connection Name' used when configuring the Edge appliance.

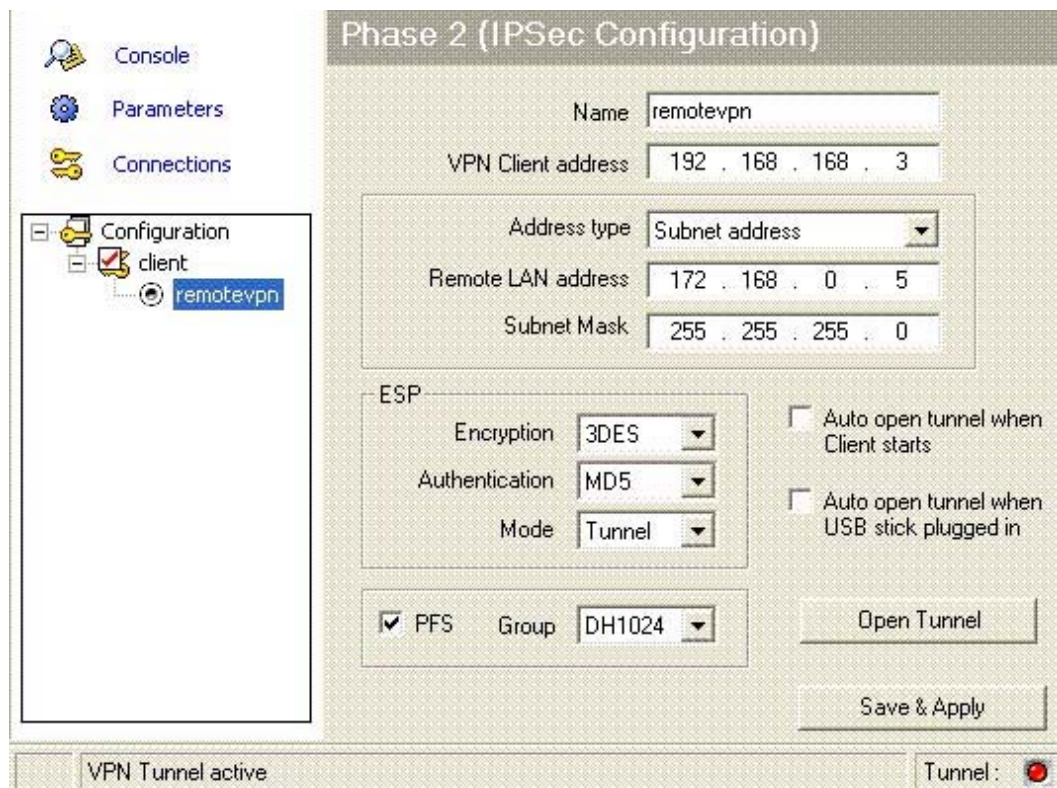
Step 2) Select the Local ID Type: DNS

Step 3) Enter a Remote ID value, which is equal to the client Name that was specified in the Phase 1 configuration.

Step 4) Select the Remote ID Type: DNS

## Phase 2 Configuration

Now that the Phase 1 configuration is complete, it is time to create the Phase 2 configuration.



Step 1) Enter the Phase 2 Name, which is equal to the 'Connection Name' used when configuring the Edge appliance.

Step 2) Enter the IP address that the VPN client will use to connect to the remote Edge appliance. Generally this should be the same as the Interface value selected during the Phase 1 configuration.

Step 3) Enter the Address type equal to "Subnet address" as this will define the LAN network of the remote Edge appliance.

Step 4) Enter the LAN address that this VPN client will use after connecting to the remote Edge device. NOTE: This must be an available IP address assigned to the LAN network of the remote Edge appliance.

Step 5) Enter the subnet assigned to the LAN network of the remote Edge appliance.

Step 6) Configure the ESP parameters equal to the following:

Encryption = 3DES

Authentication = MD5 (could use SHA1)

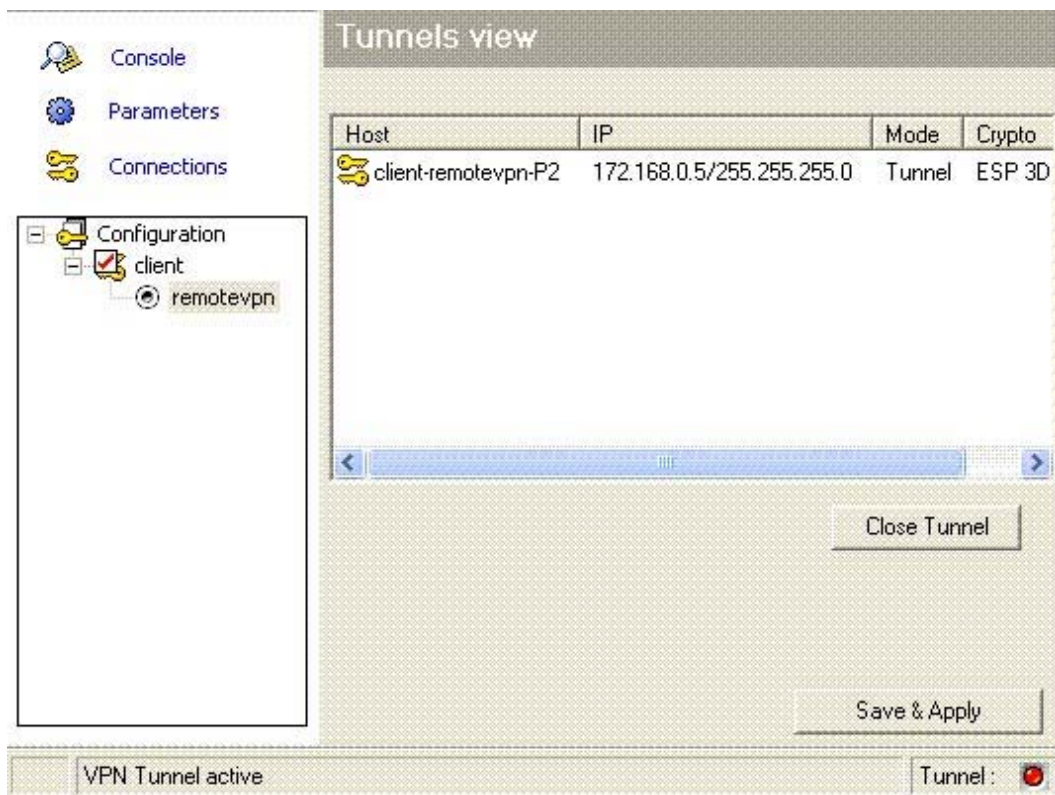
Mode = Tunnel

Step 7) Enable PFS (Perfect Forwarding Security) by clicking the checkbox, then select DH1024 from the drop-down box.

NOTE: You may select the 'Auto open tunnel' to start the VPN automatically when the client starts.

Once the Phase 2 configuration is complete, make sure to select the 'Save & Apply' button to save the configuration.

You should now be able to view the connection by clicking on the 'Connections' link:



Before starting the tunnel, the Edge appliance must be configured, refer to the next section for the Edge configuration.

## Configuring the Edge Appliance (Example Configuration)

Now that the client has been configured, it is time to create the VPN tunnel on the Edge appliance. The following steps outline that process.

### Tunnel Creation

Access the web GUI interface for the Edge appliance and select the EdgeWALL tab. Then select the 'Virtual Private Networking (IPSec)' selection from the drop-down menu. Then use the steps below to create a new client tunnel.

The screenshot shows the configuration interface for a VPN tunnel. The left sidebar lists the sections: Edge Security, Connection Name, Shared Secret Key, Dynamic Tunnel, VPN Interface, and Tunnel Local Network. The main content area shows the following settings:

- Edge Security:** Virtual Private Networking (IPSec)
- Connection Name:** remotevpn (Used to define this tunnel)
- Shared Secret Key:** testing (When using 'Shared Secret' enter a key value here, or leave blank to auto-generate. NOTE: This key must match the remote tunnel definition.)
- Dynamic Tunnel:** Enable, client Remote ID (When using clients which do not have static IP addresses)
- VPN Interface:** WAN1 (Select the outbound interface)
- Tunnel Local Network:** 172.168.168.0 (Enter the LAN network to tunnel) with a local network mask of 255.255.255.0

The following steps outline how to create a new client tunnel. This process should work for all remote IPSec VPN clients.

Step 1) Enter a connection name (should be the same as the Phase 2 name created in the software client).

Step 2) Select shared secret key.

Step 2) Select either MD5 or SHA1, must be the same as what was used when setting up the client software.

Step 3) Enter the preshared key (this is the same key that will be entered on the Edge appliance)

Step 4) Enable 'Dynamic Tunnel' as this will ensure that the client can connect from any location or IP address configuration.

Step 5) Select the WAN interface which the client will connect on, make sure that this matches with the IP address provided to the client as the Remote Gateway under the Phase 1 client configuration.

Step 6) Enter the Local Network that will be tunneled. In almost all cases, this will be the LAN network of the Edge appliance to which the client is connecting (should be

the same network from which the Remote LAN address is assigned during the Phase 2 client configuration)

The screenshot shows a configuration panel with a dark blue header and white text. It contains the following fields and controls:

- Remote VPN Device:** A text input field with a question mark icon and a placeholder IP address (four empty boxes separated by dots). A tooltip below it says "(Enter the WAN address of the remote device)".
- Remote VPN Network:** A text input field with a question mark icon and a placeholder IP address (four empty boxes separated by dots). A tooltip below it says "(Enter the network address of the remote network)".
- Remote VPN Network Mask:** A dropdown menu with "255.255.255.0" selected and a question mark icon. A tooltip below it says "(Remote VPN network mask)".
- Remote Probe Address:** A text input field with a question mark icon and a placeholder IP address (four empty boxes separated by dots). A tooltip below it says "(This is the remote devices LAN address, it is used for the VPN heartbeat)".
- Failover VPN:** A text input field with a question mark icon containing the text "remotevpn". A tooltip below it says "(Used to define the failover VPN tunnel, defaults to the Connection Name above)".
- VPN Hub/Client:** Two radio buttons: "Client Side" (unselected) and "Hub Side" (selected). A tooltip below it says "(Select the VPN tunnel type)".
- At the bottom, there are two buttons: "Add / Update" and "View Tunnels >>".

Step 7) Enter the Failover VPN name (generally the same as the Connection Name).

Step 8) Set the Edge appliance as the Hub Side of the VPN connection.

## IPSec Client Failover

Creating a failover tunnel is possible by creating a secondary tunnel on the Edge appliance using the same parameters as what was outlined above.

The only exceptions would be that the WAN interface would be different.

This would also require that the Remote Gateway, specified during the Phase 1 configuration of the client, use a DNS name instead of the IP address of the WAN interface of the Edge appliance.