



Remote Access Tutorial using ...

ZyXEL OTP Two-Way Factor Token,
ZyWALL 35-70 VPN Router,
ZyWALL VPN Client,
Authenex Radius ASAS Server

Tutorial written by:

Writer: ZyXEL Engineering Team

Company: www.zyxel.com

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

Table of contents

1	Disclaimer	3
2	Introduction	4
2.1	What is the problem?	4
2.2	Network topology	4
2.3	OTP Token, Radius Server and VPN Router product info	4
3	Solution with OTP, Radius Server and VPN Router configuration	5
3.1	Quick step by step	5
3.2	ZyWALL 35 VPN Router Configuration	5
	STEP 1: Configure Network Setting on the ZyWALL 35	5
	STEP 2: Configure the External Authentication Server	6
	STEP 3: Configuring the IPSec VPN Gateway (Phase 1) on the ZyWALL 35	6
	STEP 4: Configuring the IPSec VPN Connection (Phase2) on the ZyWALL	7
3.3	ASAS Radius Server Configuration	8
	STEP 1: Create a User Account on ASAS	8
	STEP 2: Assign an ZyWALL OTP Token to the New User	9
	STEP 3: Verify that the A-Key is properly Assigned to the User	9
	STEP 4: Update the OPT PIN	10
	STEP 5: Configure the NAS Devices	11
	STEP 6: Restart the ASAS Service	12
	STEP 7: Assign Resources to User	12
3.4	ZyWALL IPSec VPN Client Software configuration	13
	STEP 1: Configuring the VPN Gateway (Phase 1) on Client	13
	STEP 2: Configuring the VPN Tunnel (Phase 2) on Client	15
3.5	Verify OTP via Login from the VPN Client	16
	STEP 1: IPSec VPN Tunnel Establishing	16
	STEP 2: User Authentication via OTP	17
4	Contacts	19

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

1 Disclaimer

This tutorial is provided in this format for your convenience only. It is important to state that TheGreenBow has NO legal right over the content and instructions to configure either product listed in this document. This document is basically a copy of a ZyXEL web page called: "How to configure the VPN client (GreenBow) with OTP authentication over ZyWALL 35?" that you can google easily here:

[http://www.google.com/search?q=How+to+configure+the+VPN+client\(GreenBow\)+with+OTP+authentication+over+ZyWALL+35%3F](http://www.google.com/search?q=How+to+configure+the+VPN+client(GreenBow)+with+OTP+authentication+over+ZyWALL+35%3F).

Certification of the overall remote access architecture containing OTP Two-Way Factor token, Authenex Radius Server and ZyWALL 35 VPN Router has NOT been processed by TheGreenBow. However, ZyXELL did certify it. In any case, if you detect any errors in this tutorial (HowTo), we apologize to you in advance and would like you to post a request to our techsupport so we can take the appropriate action.

Doc.Ref	tgbvpn-tutorial-zyxell-otp-authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

2 Introduction

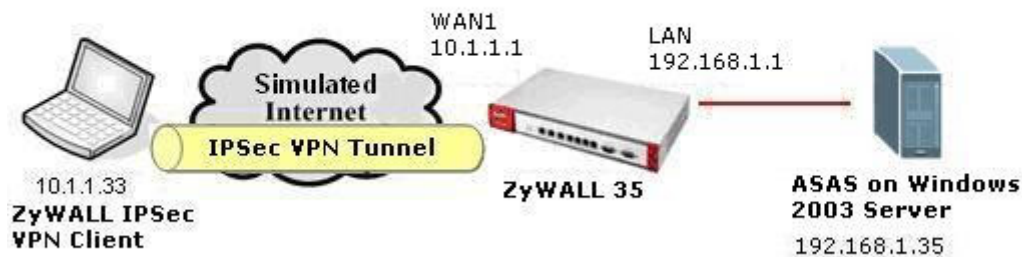
2.1 What is the problem?

How to configure the ZyWALL VPN Client software with OTP Authentication with RADIUS Server if the IPSec VPN gateway is a ZyNOS-based appliance (e.g. ZyWALL 35 or ZyWALL 70)?

2.2 Network topology

In this tutorial, we evaluated by using the ZyWALL Starter Kit which only comes with two ZyWALL OTP tokens. The ESN numbers are 73010234 and 73010235. We will create a new user Rex in order to login to ZyWALL with OTP.

For this tutorial, we'll use a ZyWALL 35 VPN Router and Authenex ASAS Radius Server.



2.3 OTP Token, Radius Server and VPN Router product info

It is critical that users find all necessary information about products used in the tutorial. All product info, User Guide and knowledge base can be found there.

ZyWALL OTP tokens	http://www.zyxel.com/web/product_family_detail.php?PC1indexflag=20040908175941&CategoryGroupNo=96C9CDE6-F2AA-4D84-9D62-311A7CCD996C&display=7999
ZyWALL 35	http://www.zyxel.com/web/product_family_detail.php?PC1indexflag=20040908175941&display=6244&CategoryGroupNo=53C4D3B9-98B3-4F1F-A7B2-BED2BBA2A7CA
ZyWALL 70	http://www.zyxel.com/web/product_family_detail.php?PC1indexflag=20040908175941&display=6244&CategoryGroupNo=53C4D3B9-98B3-4F1F-A7B2-BED2BBA2A7CA
ZyWALL VPN Client Software	http://www.zyxel.com/web/product_family_detail.php?PC1indexflag=20040908175941&CategoryGroupNo=288CE451-0F22-461F-B312-7CF3C12AAFF8&display=6244
Authenex ASAS Radius server	http://www.authenex.com/authenex-products/asas-system.html

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

3 Solution with OTP, Radius Server and VPN Router configuration

3.1 Quick step by step

In the following tutorial, we will employ the ZyXEL Two-Way Factor Authentication solution (ZyWALL OTP pack) to enhance password security by using the IPSec VPN application provided by ZyWALL 35.

In order to use this application, you are required to configure your ZyWALL and ASAS according to the following steps:

1. Install the ASAS authentication server on a computer. (Note: Please refer to the ASAS installation guide in Chapter 2 or the installation documentation in electronic format comes with the ZyXEL OTP Pack installation CD.)
2. Create a user account on the ASAS server.
3. Import each token's database file from the ZyXEL OTP installation CD over into the ASAS authentication server.
4. Assign the users to the OTP tokens over the administration interface in the ASAS server.
5. Configure the ASAS as a RADIUS server in the ZyWALL administration GUI Security > Auth Server > RADIUS
6. Give the OTP tokens away to the users who will remote login into the ZyWALL.

Note: ZyWALL OTP pack is a stand-alone product, which is not bundled with the ZyWALL series.

3.2 ZyWALL 35 VPN Router Configuration

STEP 1: Configure Network Setting on the ZyWALL 35

Launch a web browser window and logon into the ZyWALL35's web configurator. Configure the LAN and WAN interfaces according to your application scenario and network topology you plan.

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

The screenshot shows the ZyWALL 35 web interface. The 'System Information' section includes: Model (ZyWALL 35), BootBase Version (V1.08 | 01/30/2005), Firmware Version (V4.02(WZ.1) | 05/24/2007), Up Time (169:33:53), System Time (2007-09-03 09:47:52 GMT), Device Mode (Router), and Firewall (Disabled). The 'System Resources' section shows: Flash (9/16 MB), Memory (33/44 MB), Sessions (17/10000), and CPU (1%). The 'Interfaces Status' table is as follows:

Interface	Status	IP/Netmask	IP Assignment	Renew
WAN 1	100M/Full	10.1.1.1/ 255.255.255.0	Static	
WAN 2	Down	0.0.0.0/ 0.0.0.0	DHCP client	Renew
Dial Backup	Down	0.0.0.0/ 0.0.0.0	N/A	Dial
LAN	100M/Full	192.168.1.1/ 255.255.255.0	DHCP server	N/A
WLAN	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A
DMZ	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A

The 'Security Services' section shows: Turbo Card (Not Installed), IDP/Anti-Virus Definitions (v1.420 (N/A)), IDP/Anti-Virus Expiration Date (License Inactive), Anti-Spam Expiration Date (License Inactive), Content Filter Expiration Date (License Inactive), Intrusion Detected (N/A), Virus Detected (N/A), Spam Mail Detected (N/A), and Web Site Blocked (N/A). The 'Latest Alerts' section shows three alerts: WAN connection is down on 2007-09-03 09:44:16, 2007-09-03 09:39:51, and 2007-09-03 09:39:33.

STEP 2: Configure the External Authentication Server

- 1) Click Security > Auth Server from the left panel and navigate to the RADIUS setting page.
- 2) Enter the ASAS Server IP address in the Server IP Address and the Shared Secret in Key.

AUTHENTICATION SERVER

The screenshot shows the 'AUTHENTICATION SERVER' configuration page. The 'Local User Database' tab is selected, and the 'RADIUS' sub-tab is active. The 'Authentication Server' section is checked 'Active' and has the following settings: Server IP Address (192.168.1.35), Port Number (1812), and Key (1234). The 'Accounting Server' section is unchecked 'Active' and has the following settings: Server IP Address (empty), Port Number (1813), and Key (1234). 'Apply' and 'Reset' buttons are at the bottom.

STEP 3: Configuring the IPSec VPN Gateway (Phase 1) on the ZyWALL 35

Navigate to Security > VPN > and click Add in order to add a new IPSec VPN Gateway for VPN Client.

We will assign 0.0.0.0 for the Secure Gateway Address since we don't know the IP address of the remote client. 0.0.0.0 represents for any IP address will be accepted.

Check the Enable Extended Authentication checkbox.

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

VPN - GATEWAY POLICY - EDIT

Property

Name:

NAT Traversal

Gateway Policy Information

My ZyWALL

My Address: (Domain Name or IP Address)

My Domain Name: (See [DDNS](#))

Primary Remote Gateway: (Domain Name or IP Address)

Enable IPsec High Availability

Redundant Remote Gateway: (Domain Name or IP Address)

Fall back to Primary Remote Gateway when possible

Fall Back Check Interval*: (100-36400 seconds)

*Fall Back Check Interval: The time interval for checking availability of Primary Remote Gateway. IPsec SA life time will be superseded by this value when it is larger than this value.

Authentication Key

Pre-Shared Key:

Certificate: (See [My Certificates](#))

Local ID Type:

Content:

Peer ID Type:

Content:

Extended Authentication

Enable Extended Authentication

Server Mode (Search [Local User](#) first then [RADIUS](#))

Client Mode

User Name:

Password:

IKE Proposal

Negotiation Mode:

Encryption Algorithm:

Authentication Algorithm:

SA Life Time (Seconds):

Key Group:

Enable Multiple Proposals

Associated Network Policies

#	Name	Local Network	Remote Network
	VPNClient	192.168.1.0 / 255.255.255.0	Any

STEP 4: Configuring the IPsec VPN Connection (Phase2) on the ZyWALL

Navigate to Security > VPN, and click Add in order to create a new IPsec VPN Connection for the remote VPN client.

We will assign 0.0.0.0 for the Secure Gateway Address since we don't know the IP address of the remote client. 0.0.0.0 represents for any IP address will be accepted.

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

VPN - NETWORK POLICY - EDIT

3.3 ASAS Radius Server Configuration

STEP 1: Create a User Account on ASAS

- 1) Login to the ASAS server as an administrator and create a new user via Manage Users > Add User.
- 2) Fill in the user name in the Login ID field.
- 3) Click the Add button in order to complete the configuration in this step.

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

STEP 2: Assign an ZyWALL OTP Token to the New User

- 1) Navigate to Manage A-Keys > Assign A-Keys in order to assign the specific ZyWALL OTP Token to the newly created user.
- 2) Pick up a ZyWALL OTP token that is available from the right panel and click the Assign button to complete the authentication key assignment.

A-Key ID	Description
73010234	[User]
73010235	[User]

STEP 3: Verify that the A-Key is properly Assigned to the User

- 1) Navigate to Manage Users > Search Users page; leave the input fields empty and click the Get Results button in order to retrieve the user & A-Key binding list.

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

- 2) Ensure the ZyWALL OTP token is correctly assigned to the user account you created.

The screenshot shows the Authenex ASAS Web Management Console v3.1.0.0. The main area is titled 'User Management' and contains a search form with fields for Login ID, Last Name, First Name, User Status (set to 'All'), Group, and Description. Below the search form is a table of users:

Login ID	Last Name	First Name	ESN	Description	Email Addr	Current Status	Action
admin73010234			73010234			ACTIVE	Unassign Delete Undelete
rex			73010235			ACTIVE	Unassign Delete Undelete
rex						DELETED	Unassign Delete Undelete

STEP 4: Update the OPT PIN

- 1) Navigate to Manage A-Keys > Search A-Keys; leave the ESN field empty and click the Search button in order to browse the entire ZyWALL OTP token list.
- 2) In the search result page, pick up the ZyWALL OTP token you want to update the PIN code of.
- 3) Select PIN Set Mode from the OPT Mode dropdown list.
- 4) Enter the password in the OTP PIN text field with 4-24 alphanumeric characters length.
- 5) Re-enter the password in the Verify OTP PIN text field.

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

Authenex
ASAS Web Management Console v3.1.0.0

A-Key Information
There are only 2 Active Admin A-Keys. You will not be able to change the access level of this A-Key.

ESN: 73010235
Access Level: Master

OTP Information
 OTP Mode: Pin Set Mode
 OTP Counter: 19
 OTP PIN: ****
 Verify OTP PIN: ****

A-Key Lost Found
[A-Key Lost](#)

OTP Resynchronization
 Current OTP value:
 Max Resynch Attempts: 100

STEP 5: Configure the NAS Devices

- 1) Click Server Configuration > NAS Entries > Add NAS Entry in order to specify which device will be given access to the authentication server.
- 2) Give the ZyWALL a name, specify the IP Address of the ZyWALL and the shared secret.
- 3) Click the Add button in order to finish the NAS Device configuration.

Doc.Ref	tgbvpn-tutorial-zyxell-otp-authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

Authenex
Strong Authentication & Encryption Applications

ASAS Web Management Console v3.1.0.0

Edit NAS Entry

Name:

NAS Information

IP Address:

Shared Secret:

Confirm Shared Secret:

Group Information

RADIUS Attribute:

Group Option

Single group. Format: eng

Single group. Format: KEY=eng

Multiple groups. Format: eng,salse;acct,... Group Delimiter:

Multiple groups. Format: KEY=eng,salse;acct,... Group Delimiter:

Group KEY:

Additional Information

Ignore Unknown Users Support Rechallenge

STEP 6: Restart the ASAS Service

Select Start > Programs > Authenex > ASAS Server > Restart Services to reboot the ASAS Server and apply the configuration.

STEP 7: Assign Resources to User

- 1) Click Manage Users > Search Users; leave all fields empty and click the Get Results button to retrieve the user account list.
- 2) Click on the user account you created first and the Update User page will appear.
- 3) Add the ZyWALL device to Resource(s) Allowed list.
- 4) Click the Update User button to complete the entire ASAS setting.

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further

3.4 ZyWALL IPSec VPN Client Software configuration

STEP 1: Configuring the VPN Gateway (Phase 1) on Client

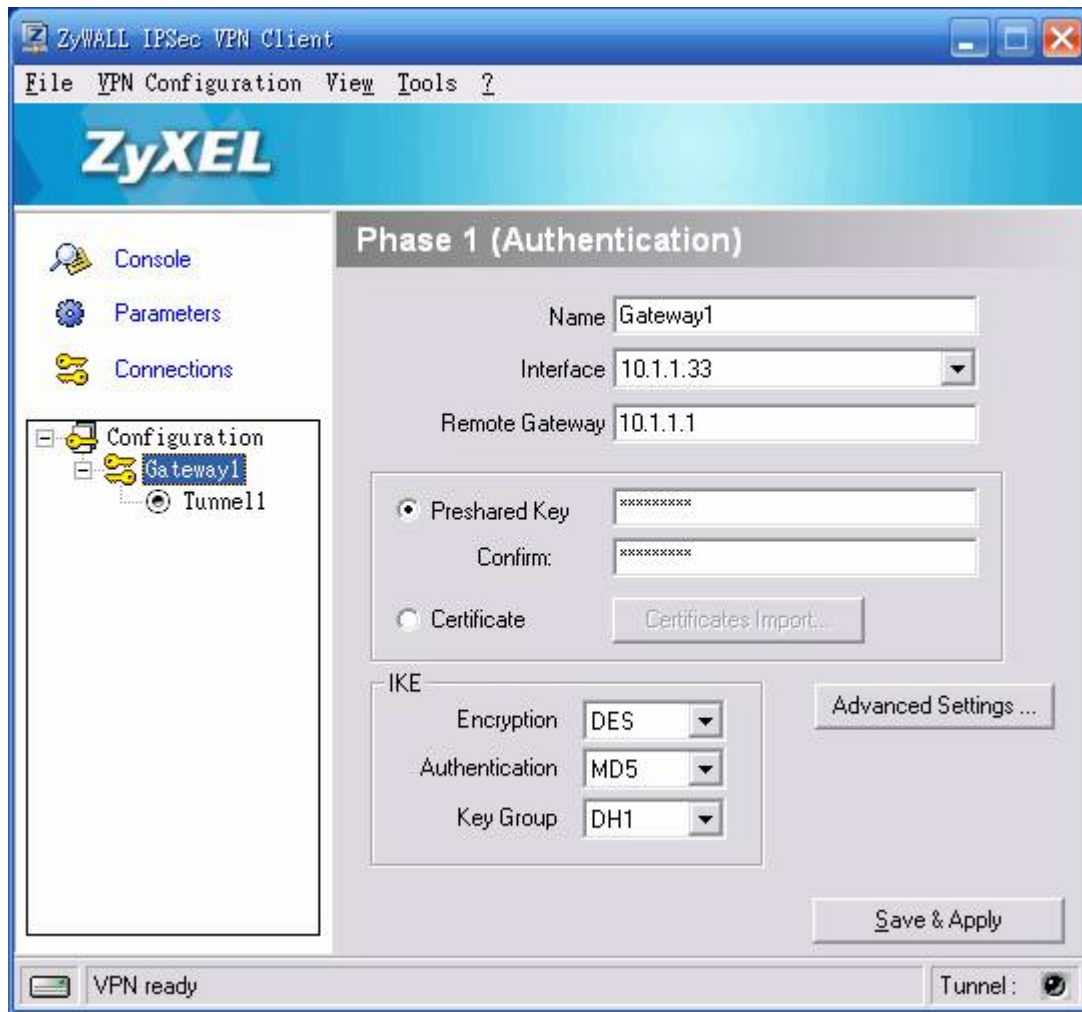
Launch the ZyWALL IPSec VPN Client and right click on Configuration and select New Phase1.

Enter the name and the IP address of Remote Gateway.

Enter the Pre-shared Key and ensure the number you just entered is matched with the one you entered on the ZyWALL in phase1 configuration. In this tutorial, we employ the Pre-shared key 123456789.

Confirming the encryption, authentication and key group to match the settings on ZyWALL.

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further



Click the Advanced Settings... button and check the X-Auth checkbox to enable the extended authentication on VPN client. Ensure the Local and Remote ID are reflecting to the settings on ZyWALL.

Phase 1 Advanced

ZyXEL

Advanced features

Config Mode Redund.GW

Aggressive Mode NAT-T

X-Auth

X-Auth PopUp Login

Hybrid Mode Password

Local and Remote ID

Choose the type of ID: Set the value for the ID:

Local ID

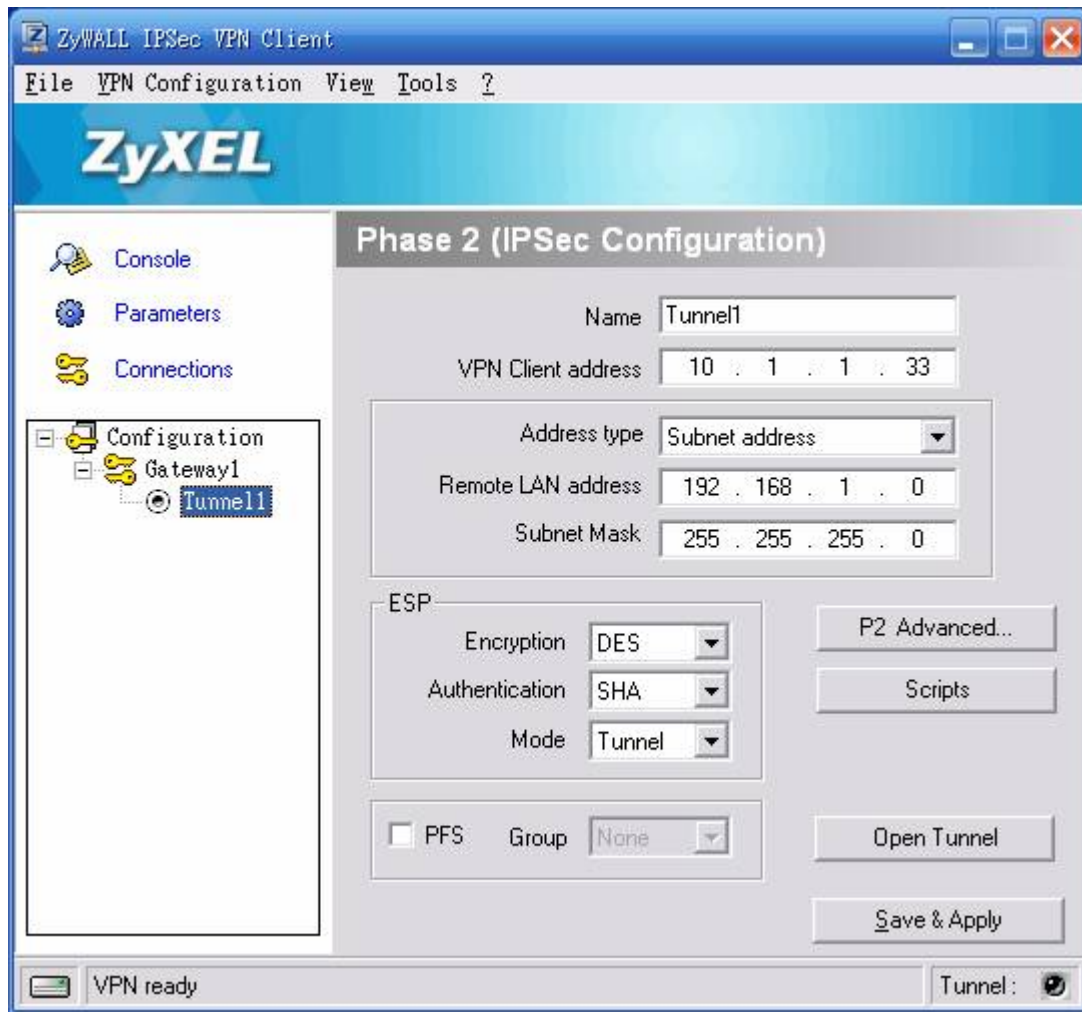
Remote ID

STEP 2: Configuring the VPN Tunnel (Phase 2) on Client

Right click on the Gateway1 and select Add Phase 2 in order to create a new tunnel.

Fill in all the required fields on this page, including Address type and all ESP fields. Ensure the encryption method, authentication method, and mode are matched with the settings on ZyWALL.

Click 'Save & Apply' in order to complete the setting.



3.5 Verify OTP via Login from the VPN Client

STEP 1: IPSec VPN Tunnel Establishing

Launch the ZyWALL IPSec VPN client.

Right click the icon of VPN client from the system tray and select Connection Panel.

Click the Open button in advance to establish the VPN tunnel.

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further



STEP 2: User Authentication via OTP

Click on the Open button and the Authentication window pops up.

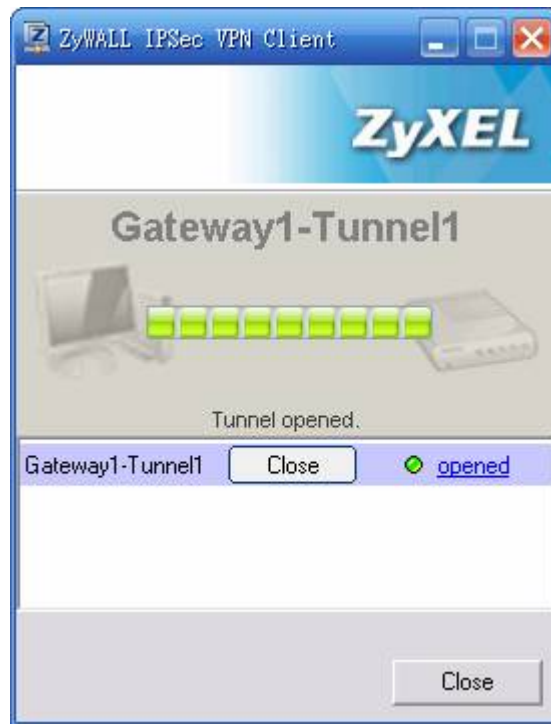
Enter the login name and password. The password here is the combination of OTP pin + OTP for which we already manipulated the OTP PIN as 1234 on the STEP 4 Update the OPT PIN in the ASAS Server Configuration session.



Once the OTP works correctly, you will see the welcome message pop-up as on the following screenshot.

Once the OTP works correctly, the IPSec VPN tunnel will be opened.

Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
Doc.version	1.0 – Mar 2009
VPN version	4.x and further



THEGREENBOW 010110101	Doc.Ref	tgbvpn-tutorial-zyxell-otp- authenex-radius-en
	Doc.version	1.0 – Mar 2009
	VPN version	4.x and further

4 Contacts

Technical support at http://www.zyxel.com/web/support_feedback.php or support@thegreenbow.com