External Authentication with Watchguard XTM

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	

Watchguard XTM Integration Guide

This document describes how to integrate a Watchguard XTM with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Watchguard XTM provides Secure Remote Access and Firewalling to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Watchguard), without the complication of deploying hardware tokens or smartcards.
Two-Factor authentication is provided by the use of (your PIN and your Phone to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into any LDAP server and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing LDAP password. Utilising the LDAP password as the PIN, allows the User to enter their UserID, Domain password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. It provides a seemless login into the Windows Server environment by entering three pieces of information. SecurEnvoy utilises a web GUI for configuration, whereas Watchguard XTM uses a thick client (System Manger). All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Watchguard

Watchguard XTM v11.7.4

SecurEnvoy

Windows 2012 server
IIS installed with SSL certificate (required for management and remote administration)
Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v7.1.503

Index

1.0 Pre Requisites

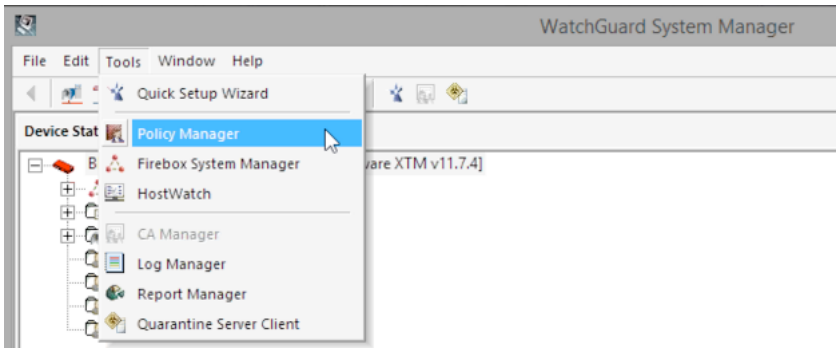
It is assumed that the Watchguard XTM has been installed and is authenticating VPN users with a username and password.

Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Routing and Remote Access server(s), additional open ports will be required.

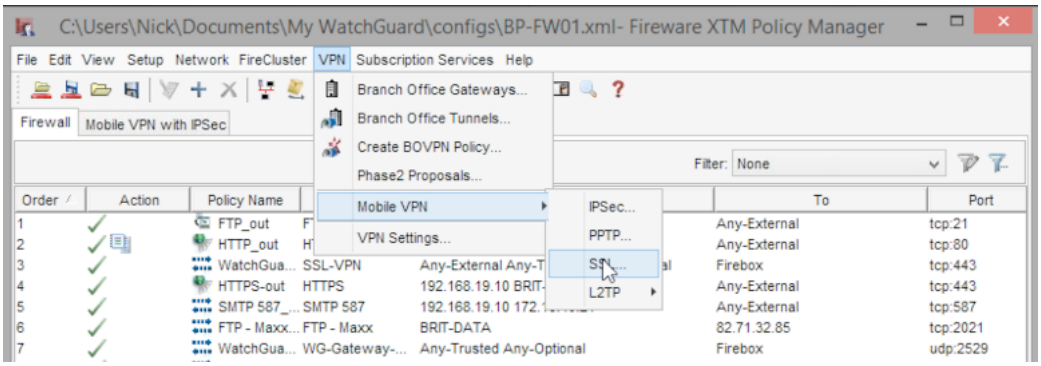
NOTE: *Add radius profiles for each Watchguard XTM that requires Two-Factor Authentication.*

1.1 Configuration of Watchguard XTM

To enable configuration launch the Watchguard System Manager.



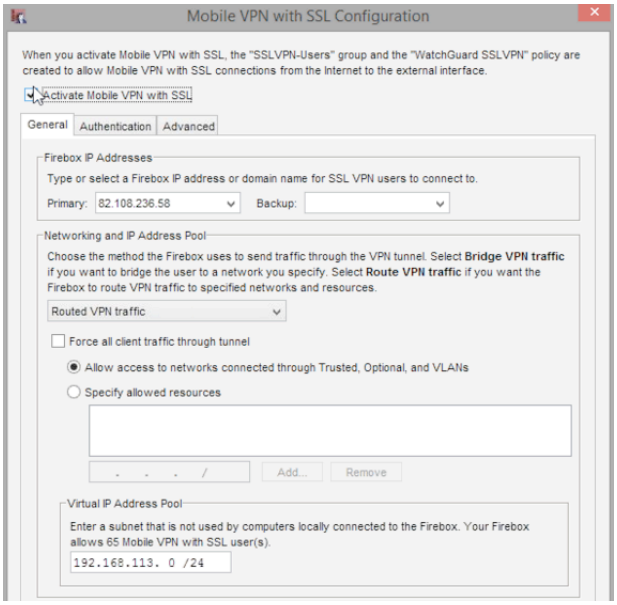
Navigate to VPN Menu, select Mobile VPN and SSL.



1.2 Configuration of Watchguard XTM SSL VPN

Within the Mobile VPN with SSL configuration, on the General tab, select "Activate" and configure the IP address that user will connect to.

Click OK when complete.



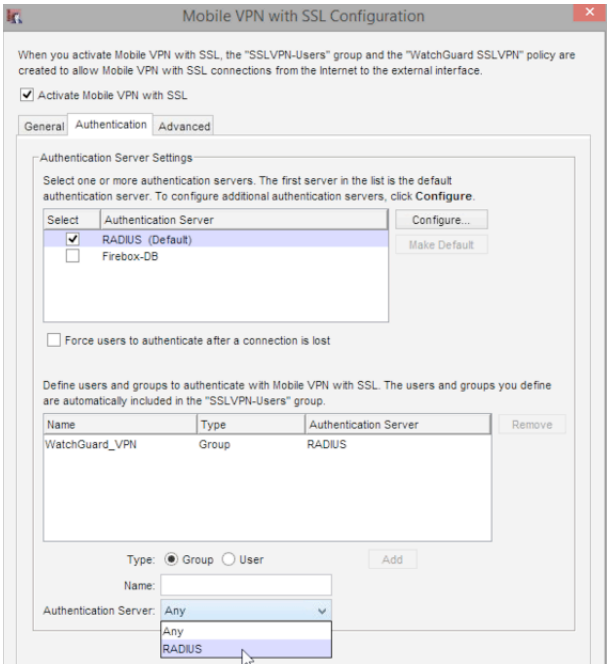
Select the Authentication tab.

Then select RADIUS as the authentication server.

If required an LDAP group can be assigned as the authentication group to use RADIUS.

In this example a "WatchGuard_VPN" group was created on Active Directory (LDAP).

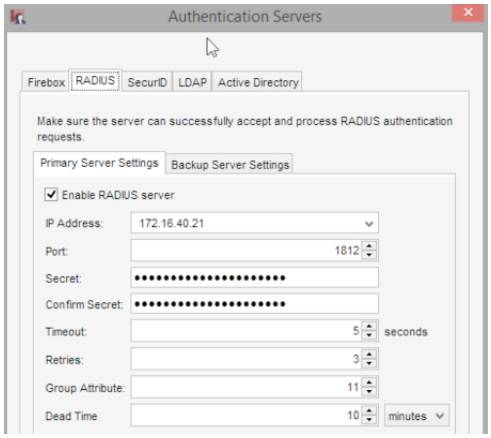
Click "Configure" to set RADIUS parameters.



Then select RADIUS. Enable RADIUS and set IP address details, port and "Shared secret" for the SecurEnvoy server.

It is recommended that a timeout of at least 5 seconds is used.

Click OK to complete.



Once complete, additional rules are automatically added to the Firewall configuration to allow SSL VPN users access.

WatchGuard SSLVPN	SSL-VPN	Any-External Any-Trusted Any-Optional
Allow SSLVPN-Users	Any	SSLVPN-Users

Save configuration, when complete.

2.0 Configuration of SecurEnvoy - PIN configuration

To help facilitate an easy to use environment, SecurEnvoy can utilise the existing LDAP password as the PIN. This allows the users to only remember their Domain password. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone via SMS.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click **"Config"**

Select **Windows** – Microsoft Password is the PIN under PIN Management

This will now use the users existing password as the PIN.

Click **"Update"** to confirm the changes

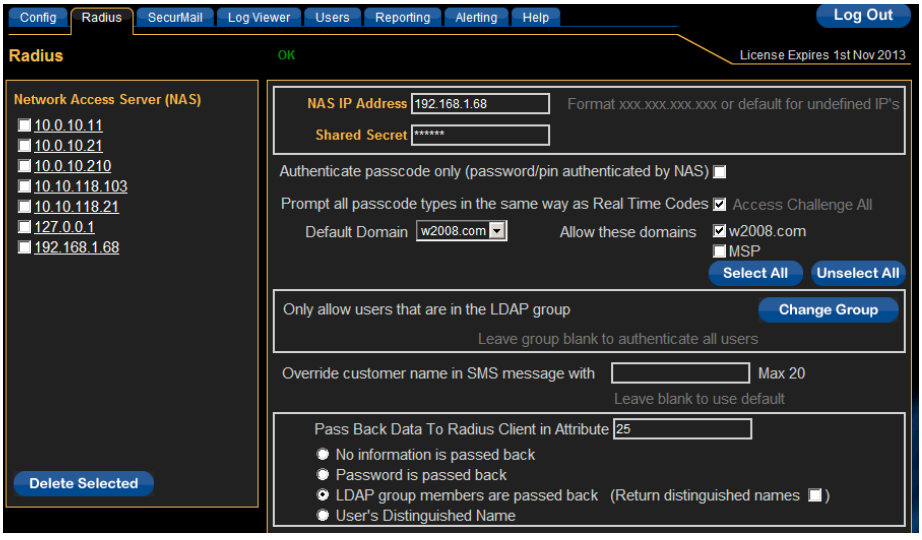
2.1 Configuration of SecurEnvoy - RADIUS configuration

Click the **"Radius"** Button

Enter IP address and Shared secret for each Watchguard XTM that wishes to use **SecurEnvoy** Two-Factor authentication.

Make sure that "Access-Challenge All" is selected.

As a Watchguard_VPN group was configured upon the Watchguard XTM device, select LDAP group members are passed back.
Leave the (Return distinguished names) unticked.



Click **"Update"** to confirm settings.

Click **"Logout"** when finished. This will log out of the Administrative session.

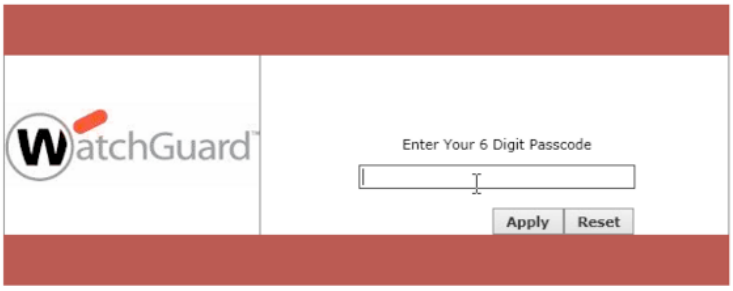
3.0 Test logon

Navigate to the URL that is supplied by your Watchguard XTM administrator.

Enter your Domain UserID and Domain password

Click "Login"

You will then be prompted to enter your 6 digit passcode.



Enter your 6 digit passcode, from SMS, email or soft token etc.
Click "Apply" to complete the logon process.

Once the authentication request is complete, the user is provided with access.