

INTEGRATION GUIDE

How to Configure WatchGuard to secure VPN access with Portnox CLEAR

Introduction

This document guides you step by step how to configure your VPN environment using Portnox CLEAR to enable secure and trusted cloud-based RADIUS access with an optional push-to-access MFA.

Preliminary Actions

Before configuring VPN authentication, you need to verify the following:

- 1) Verify your organization is registered on Portnox CLEAR Cloud Services: <https://clear.portnox.com/>
- 2) In the CLEAR portal, go to **Settings > Services** and expand **CLEAR RADIUS Service**. Then:
 - a. If the Enable Cloud RADIUS checkbox is not checked, click Edit and check the Enable Cloud RADIUS checkbox
 - b. Note the RADIUS server details which you will need when configuring VPN access:
 - **Cloud RADIUS IP** - this is the IP address of the CLEAR RADIUS server
 - **Authentication port**
 - **Shared Secret** - this is the RADIUS client shared secret
- 3) In the CLEAR portal, go to **Settings > Groups** and create a group for VPN users, or edit an existing one. In the **group settings > VPN Access** select the following:
 - Allowed authentication type = credentials.
 - (optional) Multi-Factor Authentication = push-to-access on mobile only.
Note, MFA on mobile devices require AgentP to be enrolled on the mobile device.
 - For implementation with AgentP, check the: validate risk score for all managed devices.

Configuring WatchGuard VPN

In the following steps, we configure the VPN authentication to be secured and protected based on RADIUS authentication. The following steps should be performed in the WatchGuard web interface.

Step 1 - Creating a RADIUS Authentication Server

- 1) Create a RADIUS authentication server by navigating to **Authentication > Servers > RADIUS**.

In the RADIUS Server window that appears:

- a. Check the **Enable RADIUS Server** check box.
- b. Enter the following CLEAR RADIUS server details, which you noted in Preliminary Actions, step 2(b):
 - In **IP Address**, enter the Cloud RADIUS IP.
 - In **Port**, enter the Authentication port.
 - In **Passphrase**, enter the Shared Secret.
- c. Set **Timeout** to 30 (seconds).
- d. Click **Save**.

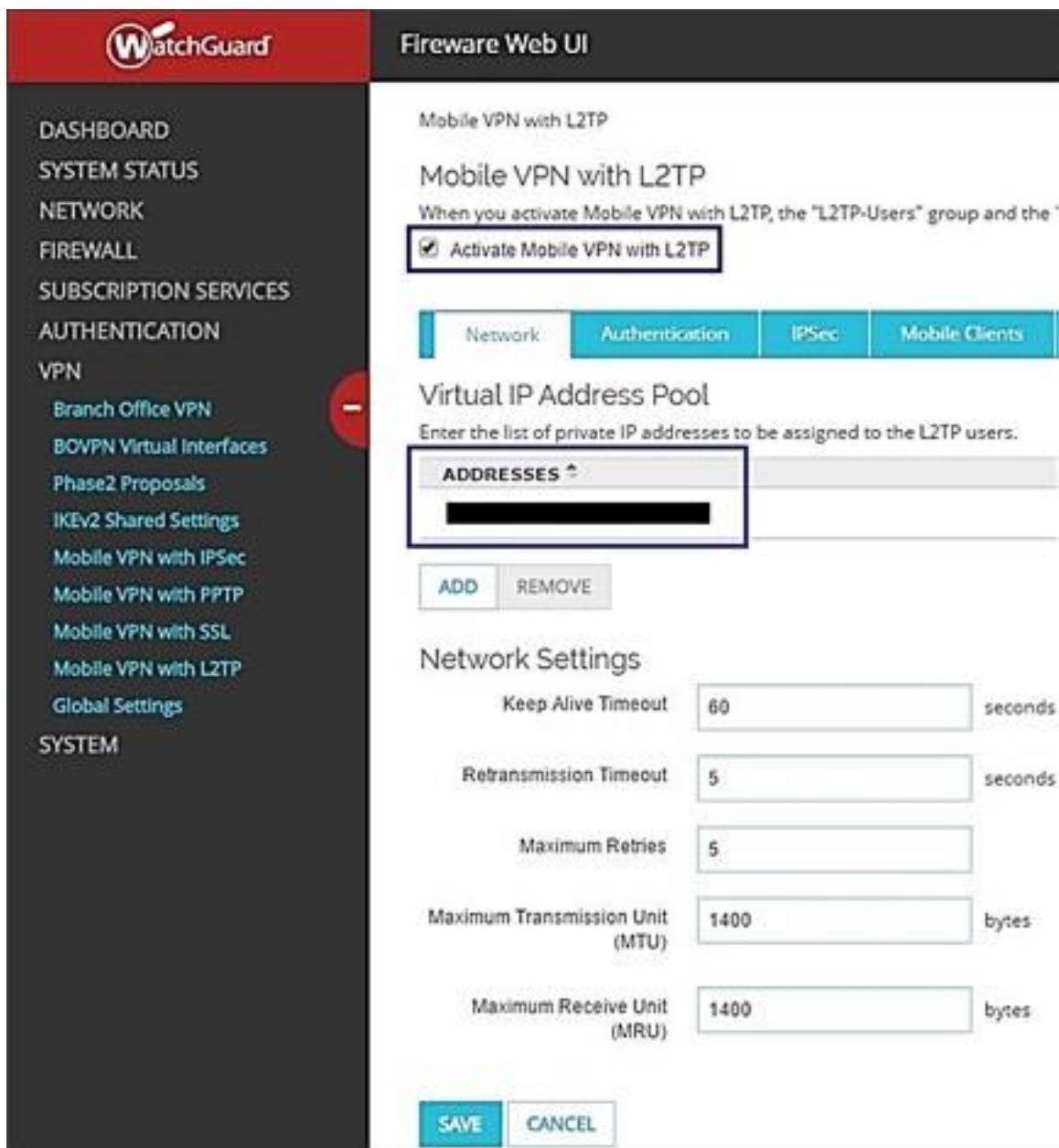
The screenshot displays the WatchGuard Fireware Web UI interface. The left sidebar contains a navigation menu with the following items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION (highlighted), Hotspot, Servers, Settings, Users and Groups, Web Server Certificate, Single Sign-On, Terminal Services, Authentication Portal, VPN, and SYSTEM. The main content area is titled 'Servers / RADIUS' and includes a warning: 'Before you configure your Firebox device to use a RADIUS authentication server, make Primary Server Settings'. Below this, the 'Enable RADIUS Server' checkbox is checked. A red box highlights the 'Primary Server Settings' form, which includes the following fields: IP Address (redacted), Port (redacted), Passphrase (masked with dots), Confirm (masked with dots), Timeout (30 seconds), Retries (3), Group Attribute (11), and Dead Time (10 Minutes).

Step 2 - Configuring the VPN connection mode

You can configure either of the following two VPN connection modes: **L2TP VPN** or **SSL VPN**.

Configuring L2TP VPN

- 1) Navigate to VPN > Mobile VPN with L2TP and click Configure.
- 2) Check the Activate Mobile VPN with L2TP check box.
- 3) In the **Network** tab, add the desired **Virtual IP Address Pool**.



WatchGuard Fireware Web UI

Mobile VPN with L2TP

Mobile VPN with L2TP

When you activate Mobile VPN with L2TP, the "L2TP-Users" group and the "

Activate Mobile VPN with L2TP

Network Authentication IPSec Mobile Clients

Virtual IP Address Pool

Enter the list of private IP addresses to be assigned to the L2TP users.

ADDRESSES
[REDACTED]

ADD REMOVE

Network Settings

Keep Alive Timeout 60 seconds

Retransmission Timeout 5 seconds

Maximum Retries 5

Maximum Transmission Unit (MTU) 1400 bytes

Maximum Receive Unit (MRU) 1400 bytes

SAVE CANCEL

- 4) In the Authentication tab:
 - a. Select **RADIUS** as the **Authentication Server**.

Mobile VPN with L2TP

Mobile VPN with L2TP

When you activate Mobile VPN with L2TP, the "L2TP-Users" group and the "WatchGuard L2TP"

Activate Mobile VPN with L2TP

Network Authentication IPsec Mobile Clients

Authentication Server Settings

Select one or more authentication servers which can be used to authenticate L2TP users. The f
configure additional authentication servers, click 'Configure'.

SELECT	AUTHENTICATION SERVER
<input checked="" type="checkbox"/>	RADIUS (Default)
<input type="checkbox"/>	Firebox-DB

MAKE DEFAULT

Authentication Users and Groups

Define users and groups to use in policies and aliases. Make sure the user or group name you

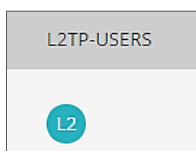
NAME	TYPE
L2TP-Users	Group

ADD REMOVE

SAVE CANCEL

- b. Make sure the **Name** of the VPN authentication group listed in WatchGuard, is identical to the VPN authentication group's name in the CLEAR portal (which you noted in Preliminary Actions, step (4)).

For example:



CLEAR L2TP VPN group

Authentication Users and Groups

Define users and groups to use in policies and aliases. Make sure the user or gr

NAME	TYPE
L2TP-Users	Group

ADD REMOVE

WatchGuard L2TP VPN group

- 5) In the **IPSec** tab, check the Enable IPSec check box and configure the following:
 - a. In Phase 1 Settings tab:
 - Select **Use Pre-shared key** and enter the key that will be used for the L2TP connection.
 - Select at least one Phase 1 transform.

Mobile VPN with L2TP

Mobile VPN with L2TP

When you activate Mobile VPN with L2TP, the "L2TP-Users" group and the "WatchGuard L2TP" policy are created to allow

Activate Mobile VPN with L2TP

Network
Authentication
IPSec
Mobile Clients

Enable IPSec

Phase 1 Settings
Phase 2 Settings

Credential Method

Use Pre-Shared Key

Use IPSec Firebox Certificate

Show All Certificates

ID	CERTIFICATE NAME	ALGORITHM

Transform Settings

PHASE 1 TRANSFORM	KEY GROUP
MD5-DES	Diffie-Hellman Group 1

ADD
EDIT
REMOVE
MOVE UP
MOVE DOWN

- b. In **Phase 2 Settings** tab, select at least one Phase 2 IPsec proposals.

Mobile VPN with L2TP

Mobile VPN with L2TP

When you activate Mobile VPN with L2TP, the "L2TP-Users" group and the "WatchGuard L2TP" policy are created

Activate Mobile VPN with L2TP

Network Authentication IPsec Mobile Clients

Enable IPsec

Phase 1 Settings Phase 2 Settings

Perfect Forward Secrecy

Enable Perfect Forward Secrecy Diffie-Hellman Group 1

IPsec Proposals

PHASE 2 PROPOSALS
ESP-AES-SHA1
ESP-3DES-SHA1

ESP-AES-SHA1 ADD REMOVE MOVE UP MOVE DOWN

SAVE CANCEL

- 6) Click **save**.

Configuring SSL VPN

- 1) Navigate to **VPN > Mobile VPN** with SSL and check the **Activate Mobile VPN with SSL** check box.
- 2) In **General** tab, select the **Primary IP** address or domain name for SSL users to connect to.

The screenshot displays the WatchGuard Fireware Web UI interface for configuring Mobile VPN with SSL. The left sidebar shows the navigation menu with 'VPN' selected and 'Mobile VPN with SSL' highlighted. The main content area is titled 'Mobile VPN with SSL' and includes a checked checkbox for 'Activate Mobile VPN with SSL'. Below this, the 'General' tab is active, showing the 'Firebox IP Addresses or Domain Names' section with a 'Primary' IP address field and a 'Secondary' IP address field. The 'Networking and IP address pool' section has a dropdown set to 'Routed VPN traffic' and radio buttons for traffic handling options. The 'ALLOWED NETWORK ADDRESSES' section shows a table with one entry: an empty IP field, a slash, and the number '24', with 'ADD' and 'REMOVE' buttons. The 'Virtual IP Address Pool' section has a text input field containing '192.168.113.0' and a dropdown set to '24'. A 'SAVE' button is located at the bottom.

WatchGuard Fireware Web UI

Mobile VPN with SSL

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group at

Activate Mobile VPN with SSL

General Authentication Advanced

Firebox IP Addresses or Domain Names

Type a firebox IP or domain name for SSL VPN users to connect to.

Primary

Secondary

Networking and IP address pool

Choose the method the Firebox uses to send traffic through the VPN

Routed VPN traffic

Force all client traffic through tunnel

Allow access to all Trusted, Optional, and Custom networks

Specify allowed resources

ALLOWED NETWORK ADDRESSES

IP Address	Subnet	ADD	REMOVE
<input type="text"/>	/ 24	ADD	REMOVE

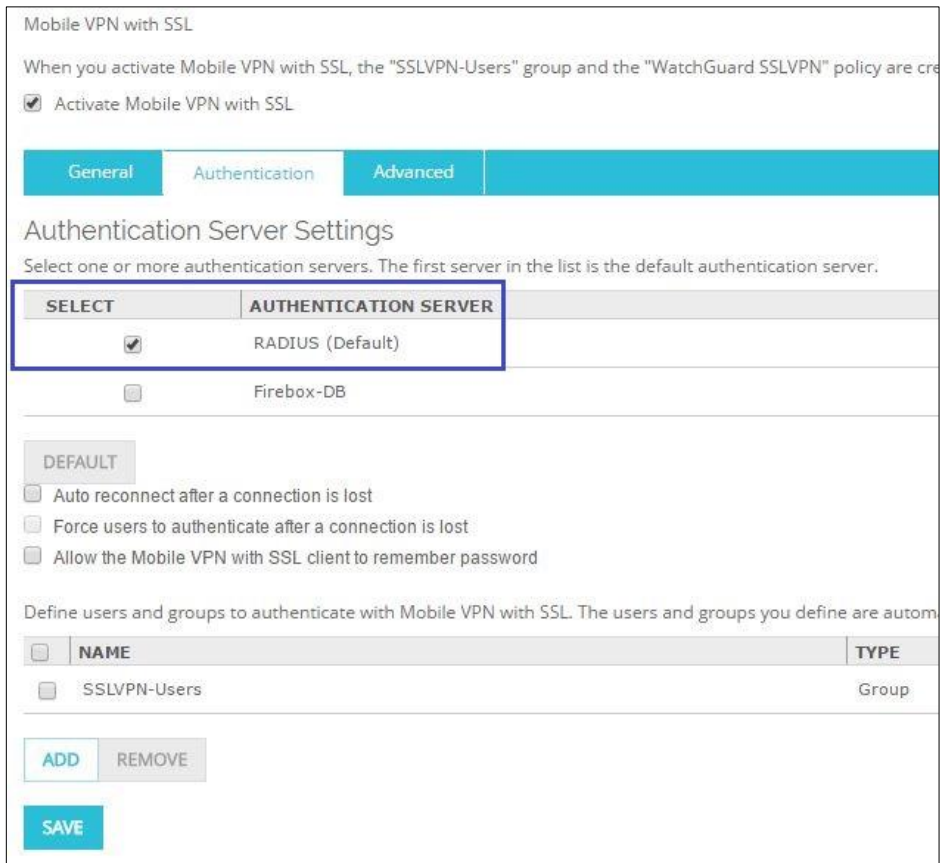
Virtual IP Address Pool

Enter a subnet to be used as virtual address pool. Your Firebox allows

192.168.113.0 / 24

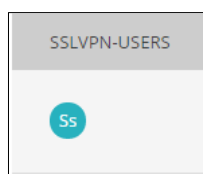
SAVE

- 3) In the Authentication tab:
 - a. Select **Radius** as the **Authentication Server**.

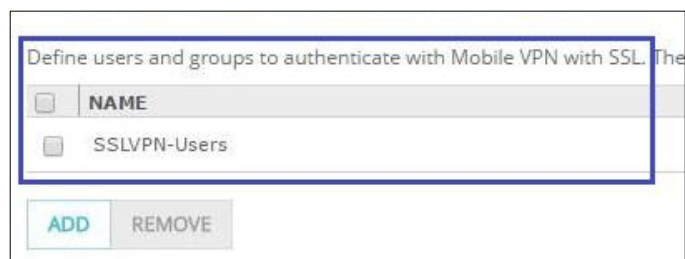


- b. Make sure the **Name** of the VPN authentication group listed in WatchGuard, is identical to the VPN authentication group's name in the CLEAR portal (which you noted in Preliminary Actions, step (4)).

For example:



CLEAR SSL VPN group



WatchGuard SSL VPN group

- 4) Click **save**.

Instructions for Supplying VPN Credentials

Supplying VPN Credentials without MFA

For successful VPN authentication using Portnox CLEAR RADIUS, users are required to provide their username + password:



Supplying VPN Credentials with push-to-access MFA

For successful VPN authentication using Portnox CLEAR RADIUS and push-to-access MFA, users are required to provide their username + password and allow the push notification on their mobile device:

