



INTEGRATION GUIDE

How to Configure FortiGate 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: <u>https://clear.portnox.com/</u>
- 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 FortiGate SSL 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 FortiGate Web UI/CLI.

Add a new Radius Server

Navigate to Under "User & Authentication" > RADIUS Servers, create a new RADIUS Server:

- 1. Enter a name.
- 2. Enter Primary Radius Server IP.
- 3. Enter Secret.
- 4. Click "OK".
- 5. Enter the CLI.

FortiGate-VM64	E	5 >_ 🛛 - 🗘 - 👤 admin -
Dashboard	New RADIUS Server	
+ Network		FortiGate
Policy & Objects	Name Clear Radius 1 Authentication method Default Specify	ि FortiGate-VM64
Security Profiles	NASIP	
묘 VPN >	Include in every user group	Additional Information
💄 User & Authentication 🔹 🗸	undere under Stande Cas	API Preview
User Definition	PrimaryServer	
User Groups	IP/Name 10.11.12.13 2	⑦ Documentation
Guest Management	Secret 3	 Ø Online Help IC ■ Video Tutorials IC
LDAP Servers	Test Connectivity	
RADIUS Servers 🗧	Test User Credentials	
Authentication Settings		
FortiTokens	Secondary Server	
🗘 System 🚺 🕽	IP/Name	
Security Fabric	Secret	
Log & Report >	Test Connectivity	
	Test User Credentials	
	4 OK Cancel	

Within the CLI, change the authentication port to the relevant port used by CLEAR radius:

CLI Console (1) 🥒
FortiGate-VM64 # config system global
FortiGate-VM64 (global) # set radius-port 12345
FortiGate-VM64 (global) # end
FortiGate-VM64 # config user radius
FortiGate-VM64 (radius) # edit Clear\ Radius
FortiGate-VM64 (Clear Radius) # set auth-type auto
FortiGate-VM64 (Clear Radius) # set server 10.11.12.13
FortiGate-VM64 (Clear Radius) # set secret AABBCC123456RRTT
FortiGate-VM64 (Clear Radius) # end
FortiGate-VM64 # 🗌

Add a new User Group:

Under "User & Authentication" > User Groups, create a new group.

Under "Remote Groups", add relevant "Clear Radius" server:

FortiGate-VM64	• =
Dashboard	Edit User Group Add Group Match
Network	Name VPN. Group or Remote Server 🍰 Clear Radius
🖹 Policy & Objects	Type Firewall Groups Any Specify
Security Profiles	Members Lest X
므 VPN	> · · · · · · · · · · · · · · · · · · ·
User & Authentication	×
User Definition	Remote Groups
User Groups	🗘 🛉 Add 🕜 Edit 😑 Delete
Guest Management	Remote Server Group Name Group Name
LDAP Servers	
RADIUS Servers	
Authentication Settings	No results
FortiTokens	
🔹 System 🛛 🚺	
🔆 Security Fabric	>
네 Log & Report	

User Group)					
me Vi	PN_Group_or					FortiGate
	ewall					🕞 FortiGate-VM64
embers 🖁	test	+ *				Send SSL-VPN Configuration
mote Groups	S					Additional Information
+Add	🖋 Edit 🛛 💼 Dele	ete				API Preview
Remote	Server ≑	Group Name ≑				𝗞 References
Clear Rad		Group Hune +				>_ Edit in CLI
						 ⑦ Documentation Ø Online Help C Video Tutorials C
		(0			
				ОК	Cancel	

Allow "Firewall Policy" access:

Under "Policy & Objects" >> "Firewall Policy", create a new "Rule":

🕞 FortiGate-VM64	• =								
Dashboard	> +Create New & Ec	lit Delete Q Police	y Lookup Search			Q			
🕂 Network	> Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
Policy & Objects	*			Schedule	Service	Action	Ten	Security Provides	LOS
Firewall Policy	10	terface (ssl.root) → 🔛 VMNE							
IPv4 DoS Policy	SSL VPN 2 LAN	VPN_Group_or all	🚍 all	G always	ALL	 ACCEPT 	O Disabled	no-inspection	IIA 🕲
Addresses	Implicit 1								
Internet Service Database	Implicit Deny	🔳 all	🗐 all	Co always	ALL	Ø DENY			O Disabled
Services									
Schedules									
Virtual IPs									
IP Pools									
Protocol Options									
Traffic Shaping									
Security Profiles	>								
VPN	>								
User & Authentication	>								
🕈 System 🛛 🕕	>								
℅ Security Fabric	>								
네 Log & Report	>								

Edit that relevant rule:

Add "VPN_Group" under "Source".

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:

test	
••••	0

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:

