



INTEGRATION GUIDE

How to Configure Check Point 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
 - Accounting 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 Check Point SSL VPN

1 item available

OK

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 Check Point console.

1) Add custom Radius Service:



N 🔓 9

Cancel

OK

Cancel

- 2) Create RADIUS server object to match Portnox CLEAR RADIUS details (Cloud RADIUS IP > Host, Authentication port ->Service, Shared Secret)
- 3) Configure Protocol to MS-CHAP v2 and click OK.

RADIUS Server P	roperties - Production_Cloud	?	×
General Accor	unting		
Name:	Production_Cloud		
Comment:			
Color:	Pink ~		
Host:	묘 Production_ > New		
Service:	UDP Rad-Centraal_Production_Po <		
Shared Secret:	•••••		
Version:	RADIUS Ver. 2.0 Compatible \sim		
Protocol:	MS-CHAP v2 ~		
Priority:	1 (1 is highest)		
	ОК	(Cancel

- 4) Open Checkpoint Gateway object
- 5) Verify Mobile Access is enabled

General Properties	Check Point Gateway	- General Prop	perties				
Topology							
·· NAT	Machine						
HTTPS Inspection HTTP/HTTPS Proxy	Name: gw	-9992df			Color:	Black	
Platform Portal	IPv4 Address: 192	2.168.77.34	Resolve from N	lame			
· VPN Clients	IPv6 Address:						
- Mobile Access - Logs	Comment:						
Optimizations Hit Count	Secure Internal Commu	unication					
- Other	Communication	Certificate State	: Trust established		Te	est SIC Status	s
	Platform						
			(and D77.00	OS: Gaia		~ (Get
	Software Blades - Network Security Bl	ades: SG103	Version: R/7.20	ment Blades: SM1	003	~	
	Network Security (3)	ades: SG103 Management (4	Manage	ment Blades: SM1	003 r <u>eness</u>	~	
	Network Security Bl	ades: SG103 Management (4	Manage	ment Blades: SM1 <u>Identity Awar</u> Provides user	003 r <u>eness</u> and machine	visibility	
	Network Security Bl Network Security Bl Network Security (3) Firewall	ades: SG103 Management (4	Manage Manage Application C URL Filtering Data Loss Pi	ment Blades: SM1 Identity Awaa Provides user across softwa creation of ide	003 reness and machine re blades. Er titty-based a	visibility nables the ccess	
	Network Security Bl Network Security Bl Network Security (3) Firewall Policy S Mobile Acce	ades: SG103 Management (4 Server	Manage Manage Manage URL Filtering Data Loss P Threat Emula	Ment Blades: SM1 Identity Awaa Provides user across softwa creation of ide policies for app acrosts	003 reness and machine re blades. Er tity-based a blication and	visibility nables the cccess resource	
	Network Security Bl Network Security Bl Network Security (3) Firewall Firewall Policy S Mobile Acco	ades: SG103 Management (4 Server ass	Manage Manage Application C URL Filtering Data Loss P Threat Emula Advanced Networkii Clustering	ment Blades: SM1 Provides user across softwa creation of ider policies for app control	003 reness and machine re blades. Er htity-based a blication and	visibility nables the ccess resource	
	Network Security B Network Security B Network Security (3) Firewall Policy S Nobile Acco IPS Anti-Bot	ades: SG103 Management (4 Gerver 255	Manage Manage O	Ment Blades: SM1	003 reness and machine re blades. Er triby-based a blication and	visibility nables the cccess resource	
	Network Security B Network Security B Network Security (3) Firewall Policy S Mobile Acce IPS Anti-Bot Anti-Furus	ades: SG103 Management (4	Manage Application C URL Filtering Data Loss Pi Threat Emula Advanced Networkii Clustering: Dynamic SecureXL	ment Blades: SM1	003 reness and machine re blades. Er thy-based a blication and	visibility nables the ccess resource	
	Network Security B Network Security B Network Security (3) Firewall Policy S Mobile Acce IPS Anti-Bot Anti-Virus Email Secu	ades: SG103 Management (4 Server 255	Manage Manage One of the second	ment Blades: SM1	003 reness and machine re blades. Er tity-based a blication and blicatio	visibility nables the cceass resource	
	Network Security B Network Security B Network Security (3) Firewall Policy S Mobile Acce IPS Anti-Bot Anti-Stan Email Secu	ades: SG103 Management (4 Server ess rity	Manage Manage Application C URL Filtering Data Loss Pi Threat Emula Advanced Networkin Clustering: O Dynamic SecureXL QoS	ment Blades: SM1 Provides user across softwar creation of ide policies for app policies for app	003 reness and machine re blades. Er titty-based a blication and	visibility nables the iccess resource	
	Network Security Bl Network Security Bl Pricewall Policy S Mobile Acce IPS Anti-Bot Anti-Span & Email Secu	ades: SG103 Management (4 Server ess rity	Manage Application C URL Filtering Data Loss P Threat Emula Advanced Networkii Clustering: Dynamic SecureXL QoS	ment Blades: SM1 Hentity Awa Provides user across softwa creation of ider policies for app social More Info	003 reness and machine re blades. Er http:-based a blication and blication and	visibility nables the ccess resource	

6) Under 'Mobile Access' - enable 'Web - SSL VPN with web browsers'



7) Under 'Mobile Access Authentication' – Choose RADIUS authentication method and point to Portnox CLEAR RADIUS object created earlier.

General Properties Authentication for Mobile Access Topology Authentication Method HTTPS Inspection Defined on user record (Legacy Authentication) HTTPATTTPS Provy Usemame and password Platform Pottal Image: Production_cloud HTTPATTS Provy RADIUS Production_cloud Image: Production_cloud Office Mode Personal certificate Mobile Access Two-Factor Authentication with DynamicID Office Mode Global settings (under "Authentication to Gateway" on the Mobile Access tab) Portal Settings Custom settings for this gateway SSL Clients Custom settings for this gateway Cation settings Allow DynamicID for mobile devices	
Image: Authentication Method Image: HTTPS Inspection Image: HTTP Inspection	
HTTPS Inspection ○ Defined on user record (Legacy Authentication) HTTPS / HTTPS Proxy ○ Usemame and password IP Jafform Portal ○ Usemame and password IP Jefform Portal ○ Usemame and password IP Jefform Portal ○ Renote Access Image: Authentication ○ SecuriD Image: Authentication ○ SecuriD Image: Authentication ○ Personal certificate Image: Authentication ○ Personal certificate Image: Authentication ○ Global settings (under "Authentication to Gateway" on the Mobile Access tab) Image: Portal Customizatio ○ Custom settings for this gateway Image: SSL Citerts ○ Custom settings for this gateway Image: Portal Customization ○ Allow DynamicID for mobile devices	
Platform Portal Usemame and password Users VPN VPN Authentication -Office Mode Remote Access O Personal certificate Mobile Access Venduction_cloud Ve	
Global settings SL Clients Custom settings for this gateway Configure SL Clients Custom settings for this gateway Configure Allow DynamicID for mobile devices	
Authentication Office Mode Remote Access Office Mode Remote Access Office Mode Rothertication Office Mode Portal Settings SSL Cients Ocustom settings for this gateway Configure. Mathertication Link Translation Mathertication Authentication Authentication Authentication Authentication to Gateway" on the Mobile Access tab) Office Mode Portal Settings SSL Cients Ocustom settings for this gateway Configure. Allow DynamicID for mobile devices	
Remote Access OPersonal certificate Mobile Access Audvertication Office Mode Portal Customizatio Portal Settings SSL Clients Outsom settings for this gateway Configure Allow DynamicID for mobile devices Link Translation	
Mobile Access Mobile Access Mobile Access Multipretication Office Mode Potal Customizatio SL Clierts HTTP Proxy Name Resolution Link Translation Unit Translation	
Authentication Office Mode Ordice Mode Ordice Customizatio Office Mode Ordica Customization Office Mode O	
Office Mode Office Mo	
Stat Stating Stat Stating Stat Stating State State State State State State State State State State State State	
Name Resolution Init Translation Allow DynamicID for mobile devices Init Translation	
Enderlief Councilier	
Certificate Authentication for mobile devices	
Logs Require client certificate when using Mobile applications	
Ht Count Require client certificate when using ActiveSync applications	
(B). Anisi	
	 _

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:

	() This sys	tem is for authorized use only.
Gaia Portal R80.10	Username: Password:	test LOGIN →

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:

		portnox [∞]
	1 This system is for authorized use only.	NEW SIGN IN Your device attempted to access the corporate network. Please confirm.
	Username: test	portnox2
Gaia Portal R80.10	Password.	Aug 14, 2020 3:27 PM
		⊗ DENY