Palo Alto configuration

Contents

Palo Alto configuration0
Guide for implementing SMS PASSCODE protection with Palo Alto Networks1
Creating profiles1
RADIUS Server Profile2
Authentication Profile
Applying SMS Passcode for GlobalProtect VPN4
PAN-OS 7.0.x - PAN-OS 7.1.56
End-user IP7





Guide for implementing SMS PASSCODE protection with Palo Alto Networks. This document outlines the process of configuring a Palo Alto Networks GlobalProtect VPN with SMS PASSCODE RADIUS protection.

Creating profiles

Start by creating a RADIUS Server Profile and an Authentication Profile.

paloalto
 Setup High Availability Config Audit Password Profiles Administrators Administrators Administrators Authentication Profile Authentication Sequence User Identification VM Information Sources Certificate Management Response Pages Log Settings Server Profiles SIMP Trap Syslog Email
 RADIUS RADIUS TACACS+ LDAP Kerberos Cocal User Database Scheduled Log Export Software GlobalProtect Client Dynamic Updates Licenses Support Master Key and Diagnostics





RADIUS Server Profile

Navigate to Device \rightarrow Server Profiles \rightarrow RADIUS and add a new RADIUS profile

Name is a friendly name of your own choice.

Set RADIUS timeout to 10-20 seconds and retries to 1.

The Authentication port 1812 is the standard RADIUS port (UDP).

Shared secret must match the shared secret entered in the NPS radius client. When done, click "OK".

RA	DIUS Server Pro	file				0
	Name SMSPasscode_ServerProfile					
Administrator Use Only						
	Don	nain				
	Time	out 20				
	Ret	ries 1				
			letrieve user group			
	Servers					
	Name		IP Address	Secret	Port	
	SMSPasscode		10.10.10.10	******	1812	
	+ Add Dele	ete				
					ок	Cancel





Authentication Profile

Navigate to Device \rightarrow Authentication Profile and add a new Authentication Profile.

Configure the profile with the RADIUS server profile you just created.

Authentication Pro	file	0
Name	SMSPasscode_AuthProfile	
Authentication	Advanced	
Туре	RADIUS	-
Server Profile	SMSPasscode_ServerProfile	-
	Retrieve user group from RADIUS	
User Domain	n	
Username Modifie	r %USERINPUT%	-
Single Sign On		
Kerberos Re	alm	
Kerberos Key	tab Click "Import" to configure this field X Import	
	ок	Cancel

Under 'Advanced' – select 'all' in the Allow List (user filtering will be handled by SMS PASSCODE).



Authentication Profile					0
Name SMS	Passcode_Auth	Profile			
Authentication A	lvanced				
Allow List	_				
Allow List 🔺					
🗹 🥵 all					
+ Add Delete					
- Account Lockout					
Failed Attempts	0				
Lockout Time (min)	0				
				ОК	Cancel
				- SA	Cancel

Applying SMS Passcode for GlobalProtect VPN

Navigate to the Network \rightarrow GlobalProtect \rightarrow Gateway

paloalto	Dashboard	ACC	Monitor	Policies	Objects	Network	Device
Interfaces Zones Virtual Wires Virtual Routers DHCP DHCP Coloration DHS Proxy Vision Coloration Colora	Name GP-Gateway			Location	Local In etherne	terface	Dence
Gateways							

Configure the GlobalProtect Gateway to use the Authentication Profile you created earlier.

General Client Configuration Satellite Configuration	Name G	iP-Gateway
Client Configuration Net	twork Settings	
Satellite Configuration		
	Interface	ethernet1/1
	IP Address	10.35.100.99/16
	SSL/TLS Service Profile	SSL-TLS-Profile
Aut	thentication	
	Authentication Profile	SMSPasscode_AuthProfile
	Authentication Message	Enter login credentials
	Certificate Profile	None

To avoid duplicate login prompts, it is recommended to configure the GlobalProtect Portal with an LDAP or Kerberos Authentication Profile.





PAN-OS 7.0.x - PAN-OS 7.1.5

For devices running PAN-OS version between 7.0.x and 7.1.5 (PAN-54196) add the following DWORD in the registry on the RADIUS server. For devices running PAN-OS 7.1.5 or newer, they should not make this registry key.:

For SMS PASSCODE 7.2 and earlier: HKLM\Software\SMS PASSCODE\RADIUS\RetransmissionEnableFiltering

For SMS PASSCODE 8.0 HKLM\Software\SMS PASSCODE\RADIUS\Connection Request Policies\RetransmissionEnableFiltering The DWORD must have a value of "0"

BRetransmissionEnableFiltering REG_DWORD 0x00000000 (0)



End-user IP

With PAN-OS 7.0 and SMS PASSCODE version 8.0 you can retrieve the end-user IP address from GlobalProtect VPN logins and log them to the SMS PASSCODE Authentication Monitoring. This can also be used for location- and behavior aware authentication.

From the SMS PASSCODE Configuration Tool, under RADIUS settings, navigate to the 'Miscellaneous' tab and set the End-user IP attribute to 26.

😪 Default RADIUS Settings 📃 🗕 💌
Authentication Authorization Miscellaneous
Text settings Code Page used for encoding:
65001
Custom challenge message:
End-user IP
Collect end-user IP address from RADIUS attribute:
26 🗘
Challenna (Reserves
Auto-detect challenne /reenonee euronot (default)
C Do not use challenge/response
Reset to factory settings Ok Cancel

On the firewall, enter the following CLI command:

set authentication radius-vsa-on client-source-ip

For more information on end-user IP, please refer to the SMS PASSCODE Administrator's Guide.