Check Point Security Gateway 2FA RADIUS Authentication Setup

You can deploy TekRADIUS with Check Point Security Gateway for Multi-Factor RADIUS Authentication for VPN sessions.

Check Point Configuration

To configure your Checkpoint, log in to the SmartDashboard. Click on the main management button and select Manage > Network Objects > New > Node > Host.

Enter the name and IP address of TekRADIUS server on the General Properties page. Click OK to save the new host, and then click the Close button in the Network Objects window.

NAT Other	Machine	TekRADIUS	
	IPv4 Address:	192.168.1.10	Resolve from Name
	IPv6 Address:		
	Comment:		
	Products: -		

Go back to the main management button and select Manage > Servers and OPSEC Applications > New > RADIUS.

On the General tab, give the server a name such as TekRADIUS. Select the host you created earlier. Be sure to select New-RADIUS as the protocol. This option uses the "new" port of 1812. Click OK and Close.

Name:	TekRADIUS
Comment:	
Color:	Crange 👻
Host:	R. TekRADIUS ▼ New
Service:	UDP NEW-RADIUS
Shared Secret:	•••••
Version:	RADIUS Ver. 1.0 Compatible
Protocol:	PAP 🔹
Priority:	1 (1 is highest)

Create an External User profile. On the main menu, select Manage > Users and Administrators > New > External User Profile > Match all users.

TekRADIUS - Check Point Security Gateway 2FA RADIUS Authentication Setup

Show:	All		•
ි ලි ලි ලි ලි ල ල ල ල ල ල ල ල ල	efault rp_usertest sertest oconfig_administrat	ors.	
Ne	W User by Template Administrator	ve Edit.	
Ne	W User by Template Administrator Administrator Grou External User Profil	ve Edit.	

Click on the Authentication page and choose Radius as the Authentication Scheme and Select the TekRADIUS host you created earlier.

Next, click on the Mobile Access tab and the Policy page. Right click on the Policy and select Edit. Move the generic* from **Available Members to Selected Members**.

Configure the Mobile Access VPN

Configure the Checkpoint SSL-VPN, bring up the Authentication page under Mobile Access. Select the RADIUS and the TekRADIUS server setup previously. Click OK. And then the Install Policy button.

General Properties	Authentication for Mobile Access								
Topology NAT HTTPS Inspection HTTP/HTTPS Proxy Platform Portal VENC Clocete	Authentication Method © Defined on user record (Legacy Authentication) © Usemame and password								
- Mobile Access	RADIUS TekRADIUS View								
Authentication Office Mode	© SecurlD								
Portal Customizatio	Personal certificate								
Portal Settings SSL Clients HTTP Proxy	Two-Factor Authentication with DynamicID								
Name Resolution Link Translation	Global settings (under "Authentication to Gateway" on the Mobile Access tab)								
Endpoint Complian Check Point Secur	Custom settings for this gateway								
⊕ Logs Optimizations	☑ Allow DynamicID for mobile devices								
Hit Count ⊛- Other	Certificate Authentication for mobile devices								
	Require client certificate when using Mobile applications								
	Require client certificate when using ActiveSync applications								

Configuring the IPSec VPN for RADIUS

Configure the Checkpoint IPSec -VPN. Click on the IPSec VPN tab and click on Gateways in the left window.

Right click on your Gateway and select Edit. Click on VPN Clients and then Authentication. Click on RADIUS and select the TekRADIUS server you added as RADIUS server above. Click OK. And then the Install Policy button.

TekRADIUS Configuration

You can authenticate built-in user profiles or Active Directory users *(Commercial editions only)* with TekRADIUS. Google Authenticator will be used as Second Level Authentication in this example. Please note that Google Authenticator is supported only in commercial editions of TekRADIUS.

Add a client entry for Check Point Security Gateway in TekRADIUS Manager / Clients tab. Enter IP address of the Check Point Security Gateway and the shared secret key specified earlier in Check Point Security Gateway configuration.

TekRADIUS Manager 5.	2 [3P]									-	Ц
<u>Service</u> <u>H</u> elp											
Users 본 Groups	Clients	💭 Settings	E Log	Sessions	E Dict	ionary [Reports	(N) Counters	🗊 SQL	2 Proxy	
IAS	Secret	Ve	ndor	Username Pa	rt E	nabled	Interim Upd	late Group	Descrip	tion	
92.168.1.20	test	iet	f			Yes	30	Default			
92.100.1.51	lest		I			ies	Ū	Delaut			
IADIUS Client Prope AS	rties Secret	Usernan	ne Part	Group		Descriptio	n	Vendor	Enabled	Interim Up	date Pe
ADIUS Client Prope AS 92.168.1.20	rties Secret test	Usernan	ne Part	Group	lt v	Descriptio	n	Vendor	Enabled	Interim Up	date Pe
ADIUS Client Prope AS 92.168.1.20 ∨ ill Command	rties Secret test	Usernan	ne Part	Group	lt v	Descriptio	n PoD & CoA I	Vendor ietf Key Attributes	Enabled ∨ Yes ∨	Interim Up	date Pe secor

Windows Auth. Proxy feature will be used in this sample configuration. You can enable Windows Auth. Directory Proxy at Settings / Service Parameters. TekRADIUS must be installed on domain member server for proper operation.

FekRADIUS Manager 5.5 [SP]	- 🗆 X
<u>F</u> ile <u>S</u> ervice <u>H</u> elp	
💄 Users 🖓 Groups 🏗 Clients 🗔 Settings 🗐 Log 🗳 Sessions 📕 Dictionary	y 🖩 Reports 🔊 Counters 🗊 SQL 🎅 Proxy
🗩 DB Connection 🔋 Database 🔠 Accounting Table 🔹 Service Parameters	s 🖂 Alerting
Service Parameters	
Listen IP Address : Any ~	Default EAP Method : PEAP-EAP-MS-CHAP-v2 V
Authentication Port Transport : 1812 🔹 UDP&TCP V	Smart Card Reader : No reader found 🗸 😈
TLS Port Mutual Certificate : 2083 🖨 🗌 Deneme 🗸 🍄 😈	Keep Domain Name : 🗹
Startup Logging : Automatic (Delay V Developer V	DHCP Server Enabled :
Secure Shutdown :	Keep DHCP History : 🗸
Authentication Failure Count : 0 🗢	Send Failure Cause : 🗌
Req. Local Cert. for EAP-TLS :	Add User-Name to
SSCC Enabled Validity Period :	Access-Accept Messages :
Authentication Proxy : Windows Domain / Server V	Periodic Credit Update :
Domain : KAPLAN	
Accounting Enabled Port :	1
HIIP Interface Enabled Port : V 8080 V ILS Enabled : V	
HTTP Session Timeout : 300 🖨 seconds	
	Save Settings
Configure TekRADIUS.	

Some of users do not want to have extra authentication; only username/password. In TekRADIUS we have two group profiles matching active directory groups with or without OTP. You need two extra AD groups in your AD; Standard for plain Active Directory authentication, Access-2FA for Google-Authenticator after AD authentication and a dummy group called "TekRADIUS-Default". Group profile configuration in TekRADIUS;

TekRADIUS Group "Default" (This is entry group)

- Active-Directory-Group = TekRADIUS-Default (Check)
- Next-Group = RAS-RDP-Access (Check)

TekRADIUS Group "RAS-RDP-Access" (This one authenticates plain AD users, falls back to RAS-RDP-Access-2FA if authentication fails)

- Active-Directory-Group = Standard (Check)
- Success-Reply-Type = Accept (Check)
- Next-Group = RAS-RDP-Access-2FA

ers	Groups	Clients	Settings	Applica	ation Log	A	ctive Sessions	Dictionary	Editor	Report	ing	Counters	SQL	Prox	у	
rows	se Groups						Group RAS-RI	DP-Access (Enabled	d) (b						
Grou Grou Ih Blan Defa RAS RAS- setti Teac Wire	p-Na V Ip Name k ault -RDP-Acces RDP-Acces manale thers ad	like ∨ ess-2FA is-2FA-GA					Attribute NAS-IP-Addr Next-Group Active-Direct Success-Rep	ess ory-Group ly-Type	Type Check Check Check	Va : 17 : RA : St : Ad	alue 72.20 AS-RI anda ccept	.50.159 DP-Access ard	-2FA			
				_												

TekRADIUS Group "RAS-RDP-Access-2FA" (Sends challenge for Google-Authenticator phase if AD authentication is successful)

- Active-Directory-Group = Access-2FA (Check)
- Next-Group = RAS-RDP-Access-2FAGA (Check)
- Success-Reply-Type = Challenge (Check)

TekRADIUS Manager LT 5.4 [SP] File Service Help			- 🗆 X
Users Groups Clients Settings Application Log	Active Sessions Dictionary	Editor Reporting Counters	SQL Proxy
Browse Groups	Group RAS-RDP-Access-	2FA (Enabled)	
Group-Na 🗸 like 🗸	Attribute	Type Value	
Group Name 1h 3h Blank Default RAS-RDP-Access RAS-RDP-Access-2FA RAS-RDP-Access-2FA RAS-RDP-Access-2FA Ras-RDP-Access-2FA Wired	NAS-IP-Address Next-Group Active-Directory-Group Success-Reply-Type	Check 172.20.50.159 Check RAS-RDP-Acces Check Access-2FA Check Challenge	s-2FA-GA
RAS-RDP-Access-2FA-GA 🕂 🖌 📝	Check V Active-	Directory-Group V	× 🛊 🖗 ×
Group 'RAS-RDP-Access-2FA' selected.		TekRADIU	S LT Service is stopped 🕼:

TekRADIUS Group "RAS-RDP-Access-2FAGA" (This is the final phase for Google-Authenticator)

• Authentication-Method = Google-Authenticator (Check)

sers -	Groups	Clients	Settings	Application Loc	A	ctive Sessions	Dictionary	Editor	Reporting	Counters	SOL	Proxy		
Brows	se Groups		-			Group RAS-RI	DP-Access-2	2FA-GA	(Enabled)					
Grou Grou 1h 3h Blan Defa RAS RAS setti Teac Wire	Ip-Na V up Name ault I-RDP-Acco I-RDP-Acco Imanale chers ad	ess ess-2FA ess-2FA	GA			Attribute NAS-IP-Addr Next-Group Authenticatio	ess n-Method	Type Check Check Check	Value 172.2 Wirec Goog	0.50.159 I le-Authentic	cator			
	PDP-Acce	cc-2FA-G	•	□ <u> </u>		Check	V Active-	Director	-Group \	0		V 🛤	д.	>

Primary group for a user must be Access-2FA in this configuration and TekRADIUS HTTP interface should display GA initiator icon when a user logins to TekRADIUS HTTP interface with AD credentials.

TekRADIUS sends an Accept Reply-Type after authentication of the credentials and active directory membership.

If a third level authentication is required; just return 'Challenge' as Reply-Type on Google Authenticator and configure another authentication method using groups.

You must initialize Google Authenticator prior to make an authentication attempt. Connect to TekRADIUS HTTP interface with Active Directory username and password and initialize Google Authenticator by clicking on QR code icon next to the username. Scan displayed QR code by using mobile Google Authenticator application and click on QR code image on the HTTP interface.

User Informatio	on		
Username:	gakaplan 🖁		
Credit remaining:	0 second(s)		
Expires on:	N/A		
User status:	Offline		
HW Address:	N/A		
Connected since:	N/A		
Reporting			
Grouping Order:	No Groupin	▼ Acct-Output ▼ Asc	•
Start date Time:	12.10.2017	00 ▼ 00 ▼	
End date Time:	12.10.2017	00 🔻 00 🔻	
Filter by:	Acct-Output	▼ Like ▼	
Compact:			
		🔤 CSV 📘	Report Logout

TekRADIUS User Reports