Using RADIUS Authentication for Remote Access VPN

This guide will show step by step instructions for configuring Remote Access VPN to utilize RADIUS authentication. There is also an appendix that includes instructions for integrating DUO MFA with a Check Point Remote Access Gateway.

We will use the following:

- R80.10 Security Management Server
- R80.10 Gateway running NGTX
- Windows Server 2012 for the RADIUS Server
- Windows Server 2012 for the DUO Proxy Server

Step 1: Configure your RADIUS connection on the Windows Server Side.

1. Open the Network Policy Server snap in. This should have been installed/enabled when you added the server as Network Policy Server.

\$	Network Policy Server	Ŀ	- 🗊 🗙
File Action View Help			
🗢 🔿 🖄 📰 🚺			
🚯 NPS (Local)	RADIUS Clients and Servers		
A Dilis Clients and Servers ADUIS Clients and Servers RADIUS Clients and Servers RADIUS Clients ADUIS Servers Die Policies Setwork Access Protection System Health Validato Recounting Accounting Templates Management	RADIUS Clients RADIUS Clients RADIUS Clients Configure RADIUS Clients Configure RADIUS Clients Remote RADIUS Server Groups Remote RADIUS server roups allow you to speedly where to forward connection requests when the local NPS server is configured as a RADIUS proxy. Configure Remote RADIUS Server Groups Configure Remote RADIUS Server Groups		

2. Create a RADIUS client by right clicking RADIUS clients and selecting "New". You will receive the following window shown below.

New RADIUS Client
attings Advanced
Phable this BADIUS client
Select an existing template:
¥
Name and Address
Friendly name:
Address (IP or DNS):
veny
Shared Secret
None
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
Manual Generate
Shared secret:
Confirm shared secret:
OK Cancel

3. Fill out the relevant information and take note of the "Shared Secret" you create as you will need it later.

	New RADIOS Client
ettings	Advanced
Enab	e this RADIUS client
Sele	t an existing template:
	k an ordering template.
Name	and Address
Check	y name: : Point Remote Access VPN
011001	
Addres	s (IP or DNS):
10.	Veriffy
Shared	Secret
Select	an existing Shared Secrets template:
None	
To man secret, secret	nually type a shared secret, click Manual. To automatically generate a share click Generate. You must configure the RADIUS client with the same share entered here. Shared secrets are case-sensitive. nual Generate secret:
To mai secret, secret Ma Sharec	nually type a shared secret, click Manual. To automatically generate a share click Generate. You must configure the RADIUS client with the same share entered here. Shared secrets are case-sensitive. nual O Generate secret:
To man secret secret Ma Shared Confim	nually type a shared secret, click Manual. To automatically generate a share click Generate. You must configure the RADIUS client with the same share entered here. Shared secrets are case-sensitive. nual Generate secret:
To mai secret secret Ma Shared Confim	nually type a shared secret, click Manual. To automatically generate a share click Generate. You must configure the RADIUS client with the same share entered here. Shared secrets are case-sensitive. nual Generate I secret: •••••• • shared secret:
To mai secret, secret Ma Shared Confim	nually type a shared secret, click Manual. To automatically generate a share click Generate. You must configure the RADIUS client with the same share entered here. Shared secrets are case-sensitive. nual O Generate secret: secret: secret:
To mail secret secret Ma Sharec Confin ••••	nually type a shared secret, click Manual. To automatically generate a share click Generate. You must configure the RADIUS client with the same share entered here. Shared secrets are case-sensitive. nual Generate I secret:

4. Click "OK" and proceed to the Network Policy Server window. Right click on "Network Policies" and select "New".

	New Network Policy
	Specify Network Policy Name and Connection Type You can specify a name for your network policy and the type of connections to which the policy is applied.
Policy name	:
Network conno Select the type type or Vendor select Unspec	ection method a of network access server that sends the connection request to NPS. You can select either the network access server rspecific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point field.
Time of not	
	twork access server:
Unspecifie	work access server:
Unspecifie Vendor spe	work access server: ad v ecflic:
Unspecifie Vendor spe	work access server: ed v ecfic:
Vendor spe 10	work access server: ad v sofic:
Vendor spe 10	work access server: ed v cfic:
Vendor spe 10	work access server: ad v sefic:
Vendor spe 10	work access server: ed v fin:

5. Enter a name for your policy and leave the network access server field "Unspecified". Then click "Next" on the Specify Conditions page select "Add".

	New Network Policy	x
	Specify Conditions Specify the conditions that determine whether this network policy is evaluated for a connection request. A min of one condition is required.	imum
	Select condition	x
Select a condit	ion, and then click Add.	
Groups		^
Wind The W group	ows Groups Indows Groups condition specifies that the connecting user or computer must belong to one of the selected s.	Ξ
Mach	ine Groups lachine Groups condition specifies that the connecting computer must belong to one of the selected groups.	
HCAP	Groups ser Groups condition specifies that the connecting user must belong to one of the selected groups.	
Loca The H requir netwo	tion Groups CAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups ed to match this policy. The HCAP protocol is used for communication between NPS and some third party rk access servers (NASs). See your NAS documentation before using this condition.	~
	Add Cancel	
	Add Edit Remove	•
	Previous Next Finish Cancel	

6. Select "Windows Groups" and then select "Add Groups". Enter your group name and click "Check Names":

Select Group	×
Select this object type:	
Group	Object Types
From this location:	
samuelshiflett.com	Locations
Enter the object name to select (examples):	
RadiusVPN	Check Names
Advanced OK	Cancel

7. Click "OK" and then "OK" again, then select "Next". On the next page select "Access granted".

	New Network Policy
	Specify Access Permission Configure whether you want to grant network access or deny network access if the connection request matches thi policy.
 Access gra	nted
Grant acce	ss if client connection attempts match the conditions of this policy.
 Access der	nied
Deny acces	ss if client connection attempts match the conditions of this policy.
Access is d	letermined by User Dial-in properties (which override NPS policy)
Grant or de	ny access according to user dial-in properties if client connection attempts match the conditions of this policy.

8. Click "Next". For authentication methods ensure that at least MS-CHAP-v2 or PAP are checked.

	New Network Policy
	Configure Authentication Methods Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.
EAP types are r EAP Types: Add Less secure User car Microsoft E	egotiated between NPS and the client in the order in which they are listed. Move Up Move Down Edit Remove authentication methods: norpsted Authentication version 2 (MS-CHAP-v2) n change password after it has expired norpsted Authentication (MS-CHAP)
User car Encrypted a Unencrypte Allow client: Perform mai	n change password after it has expired authentication (CHAP) d authentication (PAP, SPAP) s to connect without negotiating an authentication method. chine health check only Previous Next Finish Cancel

- 9. Click "Next". Select any additional constraints you'd like to add such as time of day restrictions.
- 10. Select "Vendor Specific" and click "Add".
- 11. Click "Add" on the next window.
- 12. Change the Vendor to Custom and select "Vendor-Specific". Click "Add" again.

	Add Vendor Specific Attribute	x
To add an attribute to the set	ings, select the attribute, and then click Add.	
To add a Vendor Specific attr	bute that is not listed, select Custom, and then click Add.	
Vendor:		
Custom	~	
Attributes:		
Name	Vendor	
Allowed-Certificate-OID	RADIUS Standard	
Generate-Class-Attribute	RADIUS Standard	
Generate-Session-Timeout	RADIUS Standard	
Tunnel-Tag	RADIUS Standard	
Vendor-Specific	RADIUS Standard	
Description:		
Specifies the support of propr	etary NAS features	
opositios the support of propi	day in a roadio.	
	Add Close	
	788	

13. Click "Add" again. Change the radio button to Enter Vendor Code and enter "2620". Select "Yes. It Conforms." Then click "Configure" attribute.

Vendor-Speci	ific Attribute Information
Attribute name: Vendor Specific	
Specify network access server	vendor.
◯ Select from list:	RADIUS Standard V
• Enter Vendor Code:	2620
Specify whether the attribute coverage of the specific attributes.	onforms to the RADIUS RFC specification for
• Yes. It conforms	
○ No. It does not conform	
Configure Attribute	
	OK Cancel

14. Enter "229" for the attributed number, select String for the attribute format and enter the name of the group you created. **This attribute name can't contain spaces.**

Configure VSA (RFC Compliant)
Vendor-assigned attribute number:
Attribute format:
String V
Attribute value:
RadiusVPN
OK Cancel

15. Click "OK" three times and then select "Next". Verify your settings and click "Finish".

New Network Policy
following network policy:
ETT\Radius VPN Users
ue A
ue ^ ancrypted authentication (PAP, SPAP) OR MS-CHAP v1 OR MS-CHAP v1 (User can change p
ue encrypted authentication (PAP, SPAP) OR MS-CHAP v1 OR MS-CHAP v1 (User can change p
ue ^ encrypted authentication (PAP, SPAP) OR MS-CHAP v1 OR MS-CHAP v1 (User can change p Int Access e w full network access
ue ^ ^ encrypted authentication (PAP, SPAP) OR MS-CHAP v1 OR MS-CHAP v1 (User can change p ant Access in Access ie wifull network access p

Step 2: Configure RADIUS Authentication for Remote Access VPN in SmartConsole

1. Create a host object for the RADIUS server.

New Host				Q, 😗 >
AD_RADI	US_SRV			
General Network Management NAT Advanced Servers	Machine IPv4 address: IPv6 address: Add Tag	10		Resolve from name
			OK	Cancel

2. Create a RADIUS Server object.

New RADIUS			♀ ⊗ ×
	D_RADIUS_AU ter Object Comment	ІТН	
General	General		
Accounting	Host:	AD_RADIUS_SRV	*
	Service:	🚔 RADIUS	*
	Shared secret:	•••••	
	Version:	RADIUS Ver. 2.0	*
	Protocol:	MS_CHAP2	*
	Priority:	1	
	🥑 Add Tag		
		ОК	Cancel

3. Create an empty group with the name *"RAD_yourattributename."* This needs to match the attribute name you specified in 1.14.

User Group		٩	8	
RAD_R Enter Obje	adiusVPN ct Comment			
Mailing List Address:				
$+ \mid \times$	Q Search			
Name	Comments			
Add Tag	No items found			
	ОК	Ca	ncel	

- 4. Publish your changes and close SmartConsole. It is recommended to take backup of your SMS prior to making the following changes.
- 5. Open GuiDBEdit.

6. Change add_radius_groups value under Global Properties > Properties > firewall_properties to true.

	T 1				-
Check Point Database	lool				- D
File View Objects Fields Search	Queries Help				
ච					
Tables Queries	Objec	t Name	Class Name	Last Modify Time	
Co 🛄 Tabla	. Eso	an port configuration	span port properties	Tue Oct 09 16:49:33 2018	
Administrators	n Indro	op down mapping container	drop down mapping container	Tue Oct 09 16:49:33 2018	
Anti-Malware	(in fire	wall properties	firewall properties	Tue Nov 20 00:55:15 2018	
Dektop Dektop Dektop Dektop Dektopont Goola Properties Desgo dopent Desgo d	ž		tda X		
Cald Name	Terr	Mahar	Value: 📶 🗸 🗸	Defects Mileline	Pietal description
	type	Value		Default value	Field description
SofawareLoader	string	SofawareLoader	OK Cancel	SofawareLoader	SofawareLoader
venuconinguration_mode	sung	Communicies) communicies	VPN Configuration Mode
accept_domain_tcp	boolean	faise -			accept_domain_tcp
accept_domain_udp	boolean	faise			accept_domain_udp
accept_rwi_connections	boolean	faise			accept_twil_connections
accept_icmp	boolean	faise			accept_icmp
accept_outgoing	boolean	talse			accept_outgoing
accept_outgoing_to_cp_services	boolean	true			accept_outgoing_to_cp_services
accept_outgoing_to_cp_services_p	string	before last	{first, last, before last}	before last	accept_outgoing_to_cp_services_p
accept_rip	boolean	false			accept_rip
acceptdecrypt	boolean	true		true	Enable Accept on Decrypt for Gateway to G
actions_limit_on	boolean	false			If true, the actions limit will be applied
active_resolver	boolean	true	true	true	active_resolver
add_ip_alt_name_for_ICA_certs	boolean	true		true	add_ip_alt_name_for_ICA_certs
add_ip_alt_name_for_opsec_certs	boolean	false			add_ip_alt_name_for_opsec_certs
add_nt_groups	boolean	false			add_nt_groups
add_radius_groups	boolean	false			Aada_hadiùs_ghôúpa clows
addresstrans	boolean	false			Gaddresstrationgs to activate Windows.
admin_expiration_global_data	owned object	admin_expiration_global_data	{admin_expiration_global_data,NULL}		admin_expiration_global_data

7. Change the radius_groups_atttr from 25 to 26. Save your changes and exit GUIDBedit.

Tables Queries Table Administrators Administrators Costop	Table: Queies: Object Na Table: Administrators Administrators Administrators Destop Destop Capacity Capacity Destop Capacity Destop Capacity Destop Destop Capacity Destop Dest		Class Name span_port_properties drog_down_mapping_container firewall_properties	Last Modify Time Tue Oct 09 164933 2018 Tue Oct 09 164933 2018 Tue Oct 09 164933 2018 Tue Nov 20 0055/15 2018
E - E QOS	Туре	Value	Value: 26	Default Value
r_access_enable_p	string	first		first
raccessenable	boolean	true	UK Cancel	true
radius_connect_timeout	unumber	120	o- unit_max	120
radius_groups_attr	number	25	0~255	25
radius_ignore	container		0~255	
radius_retrant_num	unumber	2	0~uint_max	2
radius_retrant_timeout	unumber	5	0~uint_max	5
radius_send_framed	boolean	false		

8. Reopen SmartConsole. Click on "Manage and Settings" followed by "Blades" and then click "Configure in SmartDashboard." The legacy SmartDashboard client will open.

<u>⊡</u> : • ∣	🎲 Objects 🔹 🔮 Install Po	itey
SATEWAYS & SERVERS SECURITY POLICIES LOGS & MONITOR	** * ⁽¹⁾ Permissions & Admin (1) (1) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (3) (4) (5) (5) (5) (6) (7) <tr< th=""><th>strators General Global Properties Inspection Settings Application Control & URL Filtering Advanced Settings Content Awareness</th></tr<>	strators General Global Properties Inspection Settings Application Control & URL Filtering Advanced Settings Content Awareness
KANAGE & SETTINGS		Advanced Settings Image: Contract Prevention Advanced Settings Image: Contract Prevention
		Configure in SmartDashboard Mobile Access Configure in SmartDashboard
		Check Point SmartDashboard® R80.10
		Server: 10.95.128.10
		30%
	1	Connecting to server

9. Click on the user icon in the Object Explorer in the bottom left. Then right click "External User Profiles" and select "New External User Profile > Match all users".

External User Profile Proper	rties	?	×
General Properties Authentication Location Time Encryption	This External User Profile will apply to all users which are not defined in the internal Users Database or any known LDAP Account Unit and do not match any other External User Profile. External User Profile name: generic* Black Comment:	. ~	
	Expiration Date: 12/31/2030 (m/d/yyyy)		
	<u>OK</u>	ancel	

10. Select "Authentication" and change the Authentication Scheme to RADIUS. Then select the RADIUS server object you created in 2.2.

External User Profile Prope	rties	? ×
General Properties Authentication Location Time Encryption	Authentication Scheme: RADIUS Settings:	
	Select a RADIUS Server or Group of Servers:	
	ОК	Cancel

- 11. Click "OK" and save your changes. Then close the SmartDashboard window.
- 12. In SmartConsole, open the gateway object for your Remote Access VPN Gateway.

Check Point Gateway -			? ×
General Properties Phetwork Management HTTPS Inspection HTTPS Inspection HTTP/HTTPS Proxy Anti-Bot and Anti-Virus Platform Potal UserCheck USE Platform Potal UserCheck PPS Platform Potal UserCheck USE Platform Potal UserCheck USE Disc VPN USERCHECK Disc VPN USERCHECK Disc VPN USERCHECK Disc VPN USERCHECK Disc VPN Disc	Machine Name: IPv4 Address: IPv6 Address: Comment: Secure Internal Communication: Platform Hardware: Open server Network Security (11) Managem Firewall Ploce VPN Policy Server Mobile Access Application Control Fire Control Fir		Color: Black Dynamic Address Communication Gaia Get Advanced Networking & Clustering: Dynamic Routing SecureXL QoS Monitoring
	ULL Filtering Data Loss Prevention Firewall World's most prove protocols and servi	Identity Awareness Content Awareness for Content Awareness	hundreds of applications,

13. Select "VPN Clients" and expand the menu. Then click "Authentication".

These settings will depend on what version of Endpoint Security/Endpoint connect you have installed, new versions (E80.65 and above support multiple authentication schemes). This guide will utilize the single authentication only option with RADIUS as the authentication method.

14. Check the box "Allow older clients to connect to this gateway" and then click "Settings".

Single Authentication Client	s Settings	?	×
General Properties			
Allow newer clients that	at support Multiple Login Options to use this authentication method		
Display Name:	Standard		
Authentication Methods —			
Authentication method:	RADIUS		~
Server:	AD_RADIUS_AUTH		\sim
🗹 Ask user for passw	ord (will be used to automatically answer the first challenge)		
Client Display:	Customize		
	ОК	Ca	ncel

If you are using clients above E80.65 check the top box "Allow newer clients that support Multiple Login Options to use this authentication method. The display name is what your users will see.

- 15. Change the authentication method to RADIUS and select the server you created in 2.2 as the server.
- 16. Check the box that says "Ask user for password (will be used to automatically answer the first challenge". If you leave this unchecked, your end user will be prompted for a username, then a password and they will need to complete two prompts instead of one.
- 17. Customize what fields your end user sees and the instructions they receive by clicking on "Customize".

Client Display	? ×
Headline:	Please user your Active Directory credentials to log on. These are the same credentials you use to login to your workstation.
Username Label:	User name
Password Label:	Password
	OK Cancel

18. Click "OK" on each open window and install policy to the Remote Access gateway.

Your users should now be able to authenticate via their Active Directory Credentials and RADIUS:

😚 Connected to Cloud	Lab			×
Endpoint Sec	urity			K Point [®]
	Connection succ	eeded		100%
	Disconnect	Close	<< Deta	ails
Resolving site name Retrieving site information Checking if a client updat	n e is available			^
User radiusses authentica	ited by Radius authe	ntication		
Loading compliance verific	ation policy			~

Troubleshooting

If you are unable to authenticate, walk through this guide again and verify the following:

- IP Addresses
- Generic* user profile configuration
- Authentication settings on the gateway object
- Verify connectivity from the gateway to the RADIUS server.
- You may need to add rules to the gateway and other network devices to allow this communication over port 1812.
- You can also verify that the RADIUS request is beings sent by the gateway using "tcpdump -nni *interfacename* host *yourradiusserver*" as you attempt the connection.
- If there is latency or a delay while the gateway waits for a response from the RADIUS server, you may need to increase the timeout according to sk112933. It is recommended to contact TAC for assistance before performing this change to verify that the connection is timing out.
- Verify that the user belongs to the proper security group that you specified in 1.6.
- Check the logs for why the authentication failed. The RADIUS server may not be responding, or the user may not be authorized. The log entry should tell you what caused the failure.

Appendix: Using DUO MFA as a RADIUS Server for Remote Access VPN Authentication

This guide can easily be adapted to use a third-party RADIUS server (in this case DUO). DUO is typically deployed with a proxy server running on either Linux or Windows Server. In our case we will use a DUO proxy server running Windows Server 2012 R2. The specific steps for configure the proxy can be found here:

https://duo.com/docs/checkpoint?ikey=DIRUR3RRWHRDVFC84VDS&host=apib7f86f92.duosecurity.com#overview

The above guide provides the majority of the steps for configuring the DUO and the Check Point configuration. However, it is designed for Mobile Access. The rest of this guide will assume that the DUO proxy server has already been configured to authenticate to DUO with an AD client as the primary factor:

; Complete documentation about the Duo Auth Proxy can be found here: ; <u>https://duo.com/docs/authproxy_reference</u>
; MAIN: Include this section to specify global configuration options. ; Reference: <u>https://duo.com/docs/authproxv_reference#main-section</u> [main] debug=true
; CLIENTS: Include one or more of the following configuration sections. ; To configure more than one client configuration of the same type, append a ; number to the section name (e.g. [ad_client2])
[ad_client]
host= service_account_username= service_account_password= search_dn=CN=Users, security_group_dn=
; SERVERS: Include one or more of the following configuration sections.
; To configure more than one server configuration of the same type, append a ; number to the section name (e.g. radius_server_auto1, radius_server_auto2)
<pre>[radius server auto] ikey= skey= api_host= radius_ip_1= radius_secret_1= failmode=secure client=ad_client port=1812</pre>

Configuring a Check Point Gateway to use DUO

1. Create a new host by selecting New... > Host... in the Object Explorer.



2. Fill in the Name and IP address of the DUO proxy server. Click OK.

Host		୯ ଡ ଼ା ×
Duo Serv Enter Object C	er omment	
General Network Management NAT Advanced	Machine IPv4 address:	Resolve from name
Servers		OK Cancel

3. Create a RADIUS server object by clicking "New.. > More... > Server > More > RADIUS" in the Object Explorer.

X Search		2 items	Q Search ← ☆	* New ▼
Suite Comments			Object Categor	Network Host Network Group
		Network O Service Custom Ap VPN Comm Data Type User	ibject , is/Ci plication/Site , unit unity ,	More 3148 ategories 8148 ties 2 62 6 4
IF-MAP RADIUS	Data Center > OPSEC Application > LDAP Account Unit > More >	Server Resource Time UserCheck Limit	ts Inte	3 eractions 13 4
RADIUS Group SecuRemote DNS SecurID Subordinate CA TACACS Trusted CA OSEIS	Encryption	÷		

4. Select the Host you created in Step 2 as the Host. The Service must be NEW-RADIUS. The Shared secret was configured in the DUO proxy configuration file. Select RADIUS Ver 2.0 and PAP as the protocol.

RADIUS			⊲
	uoProxyRadiu	S	
General	General		
Accounting	Host:	DuoProxy	*
	Service:	🚔 NEW-RADIUS	*
	Shared secret:	•••••	
	Version:	RADIUS Ver. 2.0	*
	Protocol:	PAP	*
	Priority:	1	
	🖉 Add Tag		
		ОК Са	ncel

5. Go to Manage and Settings followed by Blades and then Click "Configure in SmartDashboard". The legacy SmartDashboard client will open.

<u>©:</u> -	🗊 Objects 🔹 🕑 Install Policy	🌐 Discard Session 🕶 🏐 Publish
CORE A	 ₩ Permissions & Administrators ₩ Blades • Q Exercions Ø Revisions Ø Tags Ø Preferences Ø Sync with UserCenter 	General Global Properties Inspection Settings Application Control & URL Filtering Advanced Settings Co Content Awareness Advanced Settings Threat Prevention Advanced Settings Data Loss Prevention Configure in SmartDashboard Mobile Access Configure in SmartDashboard

Server: 10.95.128.10
30%
Connecting to server

6. Click on the "User" icon in the Object Explorer in the bottom left. Then right click "External User Profiles" and select "New External User Profile > Match all users".

External User Profile Prope	rties	? ×
External User Profile Prope General Properties Authentication Location Time Encryption	rties This External User Profile will apply to all users which are not defini in the internal Users Database or any known LDAP Account Unit a do not match any other External User Profile. External User Profile name: generic* Comment: Expiration Date Expiration Date: 12/31/2030 r/m (m/d/yyyy)	ed and Black ~
		OK Cancel

7. Select Authentication on the left pane. Change the Authentiation Scheme to RADIUS and select the RADIUS server object you created in Step 4.

External User Profile Prope	rties	?	×
General Properties	Authentication Scheme: RADIUS Settings: Settings: Select a RADIUS Server or Group of Servers: DuoProxyRadius v		

- 8. Click "OK" and save your changes. Then close the SmartDashboard window.
- 9. In SmartConsole, open the gateway object for your Remote Access VPN Gateway.

Check Point Gateway -			🕄 ×
General Properties P. Network Management NAT HTTPS Inspection HTTP/HTTPS Proxy Anti-Bot and Anti-Virus Platform Portal I- Identity Awareness UserCheck I- IPS I- IPSec VPN I- VPN Clients Mobile Access Monitoring Software bia I- Logs Fetch Policy I- Optimizations Ht Count I- Other	Machine Name: IPv4 Address: IPv6 Address: Comment: Secure Internal Communication: Platform Hardware: Open server Network Security (11) Manageme IST ISCon J(Pa)	Resolve from Name Trust established Version: R80.10 ✓ OS: ent (0) I IPS I Apti-Ret	Color: Black v Dynamic Address Communication Gaia V Get Advanced Networking & Clustering: Duramic Routing
	If See VFN Policy Server Mobile Access Application Control URL Filtering Data Loss Prevention	Anti-Virus Anti-Virus Threat Extraction Anti-Spam & Email Security Identity Awareness Content Awareness	 Oynamic Housing SecureXL QoS Monitoring

10. Select VPN Clients and expand the menu. Then click Authentication.

General Properties	Compatibility with Older clients	
Network Management NAT	1 For a list of clients supporting single authentication option only, please see sk 111583	
- HTTPS Inspection HTTP/HTTPS Proxy	Allow older clients to connect to this gateway	- 44 *
- Anti-Bot and Anti-Virus	Authentication Method: Usemame and Password	ettings
	Multiple Authentication Clients Settings	
UserCheck IPS	For a list of newer clients that support Multiple Login Options, see sk111583	
IPSec VPN	🕂 Add 🖄 Edit 🗙 Remove 👚 Up 🐥 Down	
VPN Clients Authentication Office Mode	Display Order Display Name Authentication Factors	
Mobile Access		
Monitoring Software bla		
Logs		
Fetch Policy		
Uptimizations		
- Other		
SMTP		
···· SAM		
Connection Persist		
Permissions to Inst.		
— Legacy Authentica	DynamicID Settings	
User Directory	🔽 Line Clobel Cottones (Lindes "A discribediantic of Cotomes") on the Middle Assessments)	
ISP Redunders		
More Settinge	Edit	

11. Check the box that says Allow older clients to connect to this gateway and then click Settings...

Single Authentication Client	Settings		?	×
General Properties				
Allow newer clients that	t support Multiple Login Options to use this authentication method			
Display Name:	Standard			
Authentication Methods				
Authentication method:	RADIUS			~
Server:	DuoProxyRadius		[\sim
Ask user for passw	ord (will be used to automatically answer the first challenge)			
Client Display:	Customize			
		ОК	Can	cel

- 12. Select the RADIUS server you created in Step 4 as the server. Click OK.
- 13. Publish your changes and install policy to the Remote Access gateway. Your user should now be prompted for both their password via the Check Point client and an authorization via the DUO client.

Endpoint S	Security [,]	
Site:	Cloud Lab	v
Authentication		
Please provide user na User name	ame and password to authenticate	
Please provide user na User name Password	ame and password to authenticate sshiflett	





Additional Steps

At this point, your users should be able to use DUO to authenticate to the VPN. However, the default RADIUS timeouts are too short in some cases leading to users failing to approve the push notification in time. For this reason it is recommended that you increase the RADIUS timeout values according to sk102557. DUO also recommends the timeout settings found here https://help.duo.com/s/article/1170?language=en_US.