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

3. Fill out the relevant information and take note of the “Shared Secret” you create as you will need it later.
4. Click “OK” and proceed to the Network Policy Server window. Right click on “Network Policies” and select “New”.

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

![Select Group dialog box]

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

![Specify Access Permission dialog box]
8. Click “Next”. For authentication methods ensure that at least MS-CHAP-v2 or PAP are checked.

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

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

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

1. Create a host object for the RADIUS server.
2. Create a RADIUS Server object.

![RADIUS Server Object]

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

![User Group]

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.

7. Change the `radius_groups_attr` from 25 to 26. Save your changes and exit GUIDBedit.
8. Reopen SmartConsole. Click on “Manage and Settings” followed by “Blades” and then click “Configure in SmartDashboard.” The legacy SmartDashboard client will open.
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 Properties](image)
10. Select “Authentication” and change the Authentication Scheme to RADIUS. Then select the RADIUS server object you created in 2.2.

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.
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”.
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”.

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:
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 being 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 configuring the proxy can be found here:

https://duo.com/docs/checkpoint?ikey=DIRUR3RRWHRDVFC84VDS&host=api-b7f86f92.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:
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.

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

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

7. Select Authentication on the left pane. Change the Authentication Scheme to RADIUS and select the RADIUS server object you created in Step 4.
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.
10. Select VPN Clients and expand the menu. Then click Authentication.

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