Authentication CheckPoint VPN Agent with Microsoft Azure MFA

COMPONENTS:

Check Point:
- Cluster VSX, Appliances 15400, Gaia R80.10 Take:225
- EndPoint Security VPN E82.20 Build 986101311 for windows
- Security Management Server R80.20 Take:103
- SmartConsole R80.20 Build 992000088

Microsoft:
- Windows Server 2016 Datacenter Version 1607 (OS Build 14393.2879)->NPS
- NPS Extension for Azure MFA->Installer
- Windows Server ->Azure AD Connect sync -> side on-premises
- Azure AD Connect sync service-> Side Azure
- Office365
- Laptop ThinkPad Lenovo Windows 10 Pro, Version 1909 (OS Build 18363.720)
DESCRIPTION:

This guide will show you the configuration for configure the 2-factor authentication with Microsoft Azure MFA and Check Point VPN agent. The connections required for configuration is the local domain connection with Azure AD and the NPS extension for Azure MFA, in addition to an NPS server that performs the authentication and authorization of users in the AD. The 2-factor authentication is done through the settings made in each user's Office 365 account. In this case, authentication was performed using an SMS code that receives the configured cell phone number.

CONFIGURATION:

Previous configurations:

1. Synchronization of domain local(on-premise) with Azure AD Connect sync, for this step Azure AD Connect sync must be installed on a Windows server and configured with admin credential (in the references there is a link with the necessary information about the configuration).
2. Users licensed and configure with MFA in Office 365.
3. Licensing for MFA authentication with Azure AD / Office 365 (in the references there is a link with the necessary information about the licenses).
4. Guarantee the communication between the FW or VS and the NPS over service RADIUS UDP/1645 or NEW-RADIUS UDP/1812.
   a. To verify the communication between the FW and the NPS server over service selected run fw monitor or tcpdump to see traffic.

Note: Communication between the FW or VS should not be with NAT.
Configurations Security Management Server:

In Security Management Server (SMS) configure a new RADIUS server type object, these are the only parameters to configure, for example, the NPS object, the RADIUS UDP / 1645 service, the shared secret (this is the same for the RADIUS client on NPS), versión of RADIUS (Ver. 2.0), and protocol PAP (this protocol because support double authentication with SMS code) and priority.

Open GuiDBedit under Global Properties->Properties->firewall_properties change “add_radius_groups” value to true.
Change “radius_groups_attr” value from 25 to 26. Save your changes and exit GuiDBedit.

Open SmartConsole, click on “Manage & Settings”->“Blades”->“Configure in SmartDashboard...”.
Click on the user icon in the Object Explorer in the bottom left, right click “External User Profiles” and select “New External User Profile -> Match all users”.
Select “Authentication” and change the Authentication Scheme to RADIUS. Then select the RADIUS server object you created.

Click “OK” and save your changes. Then close the SmartDashboard window.
In SmartConsole, open the gateway object for your Remote Access VPN Gateway, select “VPN Clients” and expand the menu. Then click “Authentication”.

![Virtual System Cluster Properties](image)
Configure a new “Multiple Authentication Clients Settings”, click “Add”->”New”. Type “Name” and “Display Name” and add a new “Authentication Methods”. Click “Add”, select “RADIUS” and then select the RADIUS server object you created. Select Ok and install policy.
Create a new object as LDAP group for the entire domain or access roles for specific users, this to allow access to AD users. Select the account unit and select “All Account-Unit’s Users” option.

Add the LDAP group to community "Remote Access" how as "Participant User Group" and click ok. So, create a new rule in the FW or VS where the VPN users connect and how source select "Add Legacy User Access..." and select the LDAP group. Now can configure "Destination" and "Services & Applications" especifics.
Configurations Windows Server (NPS):

The Windows server must be 2008 R2 SP1 or above.

The server must be in the local domain, the NPS function is enabled in Server Manager select "Manage" -> "Add Roles and Features" - > "Role-based or feature-based installation" - > Select server-> continue with the installation steps for the Network Policy Server, after install NPS, open again Server Manager and select "Tools"->"Network Policy Server".

![Network Policy Server](image)

Select "RADIUS Clients", right click and select "New". In this case, the VS is active on member one of the cluster. In other words, that member of the cluster receives requests from VPN users, the internal IP corresponding to the FW will be configured with the VS active.

![RADIUS Clients](image)

The shared secret is the same as when RADIUS object server is configured in Security Management Server. The vendor name in tab “Advanced” is “RADIUS Standard” and uncheck "Additional Options".

![Shared Secret](image)
Over "Policies", right click in "Connection Request Policies" and click new, specify a name of policy and select "Type of network access server" how "Unspecified", and then next.
Specify a condition or conditions for connection request, for this environment it was necessary to allow connections all day every day, click next.

```
09 April 2020

Author: Jesús Alberto Ortiz Herrera
Email: jesus.o@tb talent.com.mx
```
In “Authentication” select “Authenticate request on this server” and next.

In “Specify Authentication Methods” and “Configure Settings” not select anything and click next in both windows.
This is the final Windows, click Finish.
In "Network Policies" right click, select "New", specify a name of policy and select "Type of network access server" how "Unspecified", and then next.

Add a condition or conditions configured in step before. Select “Access granted” and click next.
In window for select Authentication Methods select the protocol to be used for authentication, in this case is with “PAP” for authentication over SMS code.

Click next and change the "Idle Timeout" and "Session Timeout" value to a value considered to the environment.
In Encryption check all options, exception the last option, uncheck “No encryption”.

Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied.

**Settings:**

- **RADIUS Attributes**
  - Standard
  - Vendor Specific

- **Routing and Remote Access**
  - Multilink and Bandwidth Allocation Protocol (BAP)
  - IP Filters

- **Encryption**
  - Basic encryption (MPPE 40-bit)
  - Strong encryption (MPPE 56-bit)
  - Strongest encryption (MPPE 128-bit)
  - No encryption

The encryption settings are supported by computers running Microsoft Routing and Remote Access Service.

If you use different network access servers for dial-up or VPN connections, ensure that the encryption settings you select are supported by your servers.

If No encryption is the only option selected, traffic from access clients to the network access server is not secured by encryption. This configuration is not recommended.
This is the last window, click Finish.

You have successfully created the following network policy:

**Policy NP**

**Policy conditions:**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day and time restrictions</td>
<td>Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00 Thursday 00:00-24:00</td>
</tr>
</tbody>
</table>

**Policy settings:**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method</td>
<td>Unencrypted authentication (PAP, SPAP) OR MS-CHAP v2 OR MS-CHAP v2 (User can change p...)</td>
</tr>
<tr>
<td>Access Permission</td>
<td>Grant Access</td>
</tr>
<tr>
<td>Framed-Protocol</td>
<td>PPP</td>
</tr>
<tr>
<td>Service-Type</td>
<td>Framed</td>
</tr>
<tr>
<td>Ignore User Dial-In Properties</td>
<td>False</td>
</tr>
<tr>
<td>RAP Percentage of Capacity</td>
<td>Reduce MultiLink if server reaches 50% for 3 minutes</td>
</tr>
</tbody>
</table>

To close this wizard, click Finish.
Configurations NPS Extension for Azure MFA:

The following is required for the server NPS:

- Windows Server 2008 R2 SP1 or above
- Directory ID from Azure tenant
- Communication with the next URLs over ports 80 and 443
  - [https://adnotifications.windowsazure.com](https://adnotifications.windowsazure.com)
  - [https://login.microsoftonline.com](https://login.microsoftonline.com)
  - [https://credentials.azure.com](https://credentials.azure.com)
  - [https://provisioningapi.microsoftonline.com](https://provisioningapi.microsoftonline.com)
  - [https://aadcdn.msauth.net](https://aadcdn.msauth.net)

In the same windows server where was installed NPS, download the extension for Azure MFA in the official site from Microsoft and execute the "setup.exe". Run the script "\AzureMfaNpsExtnConfigSetup.ps1" in "C:\Program Files\Microsoft\AzureMfa\Config", in PowerShell as admin.

This script performs:

- Create a self-signed certificate.
- Associate the public key of the certificate with the service entity in Azure AD.
- Store the certificate in the certificate store on the local computer.
- Grant access to the certificate’s private key to the network user.
- Restart NPS.

Log into Azure AD as admin, enter Azure Directory ID.

Note: If you do not enter the credentials as administrator, you will get an error like the following:
The successful setup looks like this:

Note: It is recommended to update MSOnline to its latest version 1.1.183.57.

In case the connection is not successful, there is a validation script which indicates where is the problem for which the successful connection was not achieved. This script belongs to Microsoft and will be located in the references, the steps to follow are in the link.

That is the result of Azure MFA NPS extension health check script.

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Result</th>
<th>Recommendations</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access To <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a></td>
<td>Test (Passed)</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Checking accessibility to <a href="https://administrations.windowsazure.com">https://administrations.windowsazure.com</a></td>
<td>Test Passed</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Checking if the current installed MFA NPS Extension version is the latest</td>
<td>Test Passed</td>
<td>NA</td>
<td>The current installed version is the latest which is 1.0.1.50</td>
</tr>
<tr>
<td>Checking if NPS Service is Running</td>
<td>Test Passed</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Checking if Azure MFA SPI is EAD in the tenant</td>
<td>Test Passed</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Checking if Azure MFA SPI is enabled in the tenant</td>
<td>Test Passed</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Checking if Azure Extension Registry have the correct values</td>
<td>Test Passed</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Checking Other NPS registries status</td>
<td>Test Passed</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Checking if there is a matched certificate with Azure MFA</td>
<td>Test Passed</td>
<td>NA</td>
<td>The matched Certificate have these fingerprints: 935292b79d5e05357f26e8152f13a9f1fe19c0748392eb720a52796f344172f6c33a6fdd8cc363b3d</td>
</tr>
</tbody>
</table>
Configurations EndPoint Security VPN:

When enabled "Multiple Login Options" in the FW or VS. In the agent appears different manners for configure the agent when crate a new site, in this case appear the option configured before on the VS when create a new site.

Since the site is created with the Microsoft authentication option selected, the local AD user and password are entered.
A new window appears waiting for the entry of the SMS code sent to the previously configured phone number.

![Endpoint Security](image)

When entering the SMS code, the connection is successful and appears in details that the user authenticated with Radius.

![Connected to Endpoint Security](image)
Logs:

NPS logs are seen in "Event Viewer" under "Server Roles" -> "Network Policy and Access Services" and "Applications and Services Logs" -> "Microsoft" -> "AzureMfa" -> "AuthN" and "AuthZ".

These are examples of errors that happened:

This error refers to the fact that there is no double factor authentication method for the user with which to log in. It is solved by verifying that the user is licensed in Azure AD and configuring MFA to the user in Office 365.
When the NPS fails to authenticate, it is recommended to review the selected protocol and keep in mind that MS-CHAPv2 only authenticates by phone call and codes through apps, in the FW the log appears as:

The log indicating that the authentication was successful in NPS is as follows:
When you don't create the rule in the FW to allow access to users belonging to the AD, the following log in the NPS appears "Network Policy Server discarded the request for a user"...

And the log that appears in the FW is as follows:
When authentication is successful, the log appears as the following:

![Log Details](image)

REFERENCES:

Remote Access VPN R80.20 Administration Guide


Azure AD Connect sync: Understand and customize synchronization

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-what-is

Integrate your existing NPS infrastructure with Azure Multifactor Authentication

https://docs.microsoft.com/pt-br/azure/active-directory/authentication/howto-mfa-nps-extension

Resolve error messages from the NPS extension for Azure Multi-Factor Authentication


MSOnline

https://docs.microsoft.com/en-us/powershell/module/msonline/?view=azureadps-1.0#msonline

Azure MFA NPS extensión health check script

NPS Extension for Azure MFA


Features and licenses for Azure Multi-Factor Authentication

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing