My setup

Windows 10 Client with Checkpoint Remote Access (Client E87.20) Checkpoint Single Gateway in Azure, running R81.20 Build 703, no other JHF installed Checkpoint SMS in Azure, running R81.20, no other JHF installed Azure Enterprise App (gallery app) "Check Point Remote Secure Access VPN" Date of testing: 2023/04/05

Intention

I wanted to setup a Remote Access environment where users can authenticate against a SAML Identity Provider and the authorization is also provided by that IdP, so that there is no need for a LDAP server to get the group memberships.

Pre-configuration steps

I followed this configuration guide:

https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_RemoteAccessVP N_AdminGuide/Content/Topics-VPNRG/SAML-Support-for-Remote-Access-VPN.htm?Highlight=saml

I have <u>not</u> configured these steps:

- Step 4 point 11 "On each Security Gateway of version R81.10 and lower, download a script that is required to use the feature." (because my setup uses R81.20)
- Step 5: Install and Configure Remote Access VPN Clients
- Everything that is related to a LDAP configuration to get group memberships through LDAP

The following parts are only an additional piece, because the documentation is sometime not that good in describing the details of the required steps. So pleas<u>e use the mentioned guide above from</u> <u>Checkpoint and I hope that my additional information can help you to get it up and running.</u>

Enterprise App – role and app registration

Create a AAD group for Remote Access users, add your users to that group.

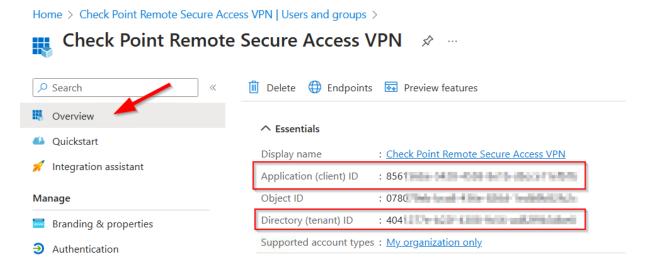
Use the link "application registration" to define a role and App permissions.

Home > Contoso Enterprise applic	ations > Enterprise applications All applications > Check Point	Remote Secure Access VPN	
Check Point Remo	ote Secure Access VPN Users and gr	oups …	
Overview Deployment Plan	 Add user/group Edit assignment Remove The application will appear for assigned users within My App 	\mathscr{P} Update credentials $\parallel \equiv \equiv$ Columns $\mid \not \mathrel{R}$ Got feedback? s. Set 'visible to users?' to no in properties to prevent this. \rightarrow	0
X Diagnose and solve problems	Assign users and groups to app-roles for your application here	. To create new app-roles for this application, use the application registration.	
III Properties	P First 200 shown, to search all users & gro		
A Owners	Display Name	Object Type	Role assigned
Roles and administrators	MOD Administrator	User	Default Access
Users and groups	RE RemoteAccess	Group	RemoteUsers
Single sign-on			

Create an App secret so that Checkpoint Management + Gateway is able to read user and group details. Save the value in your password tresor.

Home > Check Point Remote Secure Ac	cess VPN Users and groups > Chec	k Point Remote Secure Acces	5 VPN	
💡 Check Point Remote	e Secure Access VPN	Certificates & se	ecrets 🖈 …	
₽ Search «	🖗 Got feedback?			
 Overview Quickstart Integration assistant 			the authentication service when receiv ificate (instead of a client secret) as a c	ving tokens at a web addressable location (using an HTTPS redential.
Manage	Application registration certification	tes, secrets and federated credenti	als can be found in the tabs below.	×
 Branding & properties Authentication Certificates & secrets 	Certificates (0) Client secrets			
 Token configuration API permissions 	A secret string that the application i	uses to prove its identity when i	equesting a token. Also can be referred	i to as application password.
Expose an API	Description	Expires	Value ①	Secret ID
App roles	CP-App	7/4/2023	_Na**************	038074c0-de9c-4904-9040-ac9521d20b6d 🗈 📋
A Owners				

You'll also need the Application ID & Directory ID



Add permission to this app registration, so that the App can read some user / group related data:

Checkpoint Remote Access SAML Authentication & Authorization with Azure AD

O Search	« 💍 Refresh 🕴 🛜 Got feed	lback?				
Overview						
Quickstart Integration assistant	The "Admin consent requi will be used. <u>Learn more</u>	red" column shows th	e default value for an organization	. However, user consent can be customized per pe	ermission, user, or app. This column may	not reflec
inage	Configured permissions					
anage Branding & properties	- Configured permissions	all APIs when they a	are granted permissions by users	s/admins as part of the consent process. The li	ist of configured permissions should i	nclude
Branding & properties	Applications are authorized to o		are granted permissions by users ore about permissions and conse		ist of configured permissions should i	nclude
Branding & properties	Applications are authorized to o	ion needs. Learn mo	ere about permissions and conse		ist of configured permissions should i	nclude
Branding & properties Authentication Certificates & secrets	Applications are authorized to o all the permissions the application	ion needs. Learn mo	ere about permissions and conse	int	ist of configured permissions should i nt requ Status	nclude
Branding & properties Authentication Certificates & secrets Token configuration	Applications are authorized to G all the permissions the application + Add a permission ✓ G	ion needs. Learn mo	for Contoso	int		nclude
Branding & properties Authentication Certificates & secrets Token configuration API permissions	Applications are authorized to all the permissions the application + Add a permission G API / Permissions name	ion needs. Learn mo irant admin consent Type	for Contoso	int		
Branding & properties Authentication	Applications are authorized to all the permissions the application + Add a permission	ion needs. Learn mo irant admin consent Type 3 Application	for Contoso Description	Admin conser	nt requ Status	

Create a new role:

Check Point F	Remote	e Secure Acce	ess VPN App rol	es 🖈 …			
^O Search	~	+ Create app role	🔗 Got feedback?				
Overview		App roles					
Quickstart		App roles are custom	roles to assign permissions to u	sers or apps. The application defines and	publishes the app role	s and interprets them	
🐔 Integration assistant		as permissions during					
lanage		How do I assign App	p roles				
Branding & properties		Display name	Description	Allowed member types	Value	ID	State
Authentication		RemoteUsers	RemoteUsers	Users/Groups	RemoteUsers	fbea3299-1d8e-4b4a	Enabled
Certificates & secrets		msiam_access	msiam_access	Users/Groups		6996bac3-b464-498c	Enabled
Token configuration							

Go one step back to your Enterprise App, open "Users and Groups".

Select your Remote User group and "Edit assignement". Select the previous created role.

Enterprise Application			
«	🕂 🕂 Add user/group 🛛 🧷 Edit assignment 📋 Remove	Description of the second se	
Overview			
Deployment Plan	The application will appear for assigned users within My App	s. Set 'visible to users?' to no in properties to prevent this. $ ightarrow$	
Diagnose and solve problems			
anage	Assign users and groups to app-roles for your application nere.	To create new app-roles for this application, use the application registration.	
	Assign users and groups to app-roles for your application nere.	To create new app-roles for this application, use the application registration.	
Properties		To create new app-roles for this application, use the application registration. Object Type	Role assigned
Properties	P First 200 shown, to search all users & gro		Role assigned Default Access
anage Properties Covners Roles and administrators Users and groups	First 200 shown, to search all users & gro Display Name	Object Type	

Enterprise App - Single SignOn

You need to add a a new claim:

Claim name: "group_attr"

Value: "user.assignedroles"

Home > Check Point Remote Secure Access VPN | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims			
+ Add new claim + Add a group claim \equiv Columns \aleph	Got feedback?		
Required claim			
Claim name	Туре	Value	
Unique User Identifier (Name ID)	SAML	user.userprincipalname [•••
Additional claims			
Claim name	Туре	Value	
group_attr	SAML	user.assignedroles	•••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd	SAML	user.mail	• • •
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname	•••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname	•••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname	•••

 \checkmark Advanced settings

Smart Console – object to read identities from AAD

Switch to Smart Console and add a new User/Identity, type "Azure AD".

New ▼ Network Host Network Group Cloud	bjects			
More		Network Object Service Custom Application/Site VPN Community Data Type User/Identity Cloud Server Resource Time UserCheck		LDAP Group Access Role Identity Tag User Group User User Template
		LSM Profile Limit	•	Identity Provider LDAP Account Unit Azure AD

"Application Key" is the secret value:

The connection needs to be successful, otherwise reload the browser from Azure AD (the secret value needs to be hided by some "****".

Another possible fault can be, that the API permission is not set or granted.

Azure AD	୦ ୧ ×					
CP-App Enter Object Comment						
▲ Changes will be applied after publish.						
• Service Principal A	uthentication					
Application ID:	856 Developed and the second					
Application Key:	•••••					
Directory ID:	404					
 Azure AD User Aut 	hentication					
Username:						
Password:						
Test Connection Connected Note: when using the Azure AD feature, each security gateway saves locally all the entities from the Azure repository, regardless of the gateway's region.						
🖉 Add Tag						
	OK Cancel					

Publish now your changes.

Open your gateway, blade Identity Awareness, check "Remote Access".

Checkpoint Remote Access SAML Authentication & Authorization with Azure AD

Check Point Gateway - cpgw		0 ×
General Properties	Identity Sources	
HTTPS Inspection	Browser-Based Authentication Settings	
HTTP/HTTPS Proxy	Browser-Based Authentication is not enabled on this Gateway.	
Platform Portal	Portal URL:	
 Identity Awareness Mail Transfer Agent 	Active Directory Query Settings	
-IPSec VPN -VPN Clients	Domains to get identities from are not selected	
Logs	Identity Agents Settings	
Fetch Policy Optimizations	Learn more	
- Hit Count	Terminal Servers Settings	
🗄 Other	Terminal servers are not enabled on this Gateway.	
	Download agent	
	RADIUS Accounting Settings	
	Identity Collector Settings	
	Identity Web API Settings	
	Remote Access	
< >>	OK Cancel	

Smart Console – Internal User Group / Access Role

Create an "Internal User Group" and take care oft he name.

The name needs this syntax: "EXT_ID_" followed by your role name, leave the rest empty.

User Group		८ छ । 🗖 🗙
EXT_ID_ Enter Object	RemoteUsers Comment	
Mailing List Address:		
+ × Q Search		No items found
Name	 Comments 	
	No items found	
Add Tag		
e nuu rug		
	OK	Cancel

Use that internal group in your Access Role:

Access Role				Q 😧 X
Enter Object	eUsers ct Comment			
** Networks Users	 Any user All identified users Specific users/groups: 			
Machines	+ ×		🔍 Search	
Remote Access Clients	Name Image: Contract of the second	Type / Source Directory Internal User Group	Unique Identifier	
			ОК	Cancel

In case for access without Remote Access, you can check "Browser-Based Authentication".

General Properties Network Management HTTPS Inspection HTTP/HTTPS Proxy ICAP Server The portal is accessible only through internal interfaces.	Check Point Gateway - cpgw		3 ×
Platform Portal Portal URL:			

Keep in mind, that you'll have to add in your access role the native user or group from Azure AD. The Internal User Group (starting with "EXT_ID_" is only necessary for Remote Access).

Create a policy with that Access ROle as the Source and whatever destination / service you will allow.

User is connected – PDP monitor

When the user is connected, you can view the details with "pdp monitor" and check the assigned role and groups:

```
[Expert@cpgw:0]# pdp monitor all
Session: 0cfe0c18
Session UUID: {1A1A3A7F-DB65-638F-C47C-9E3D08F0537F}
Ip: 172.16.10.3
Users:
LogUsername: AlexW@M365x96201156.OnMicrosoft.com
  Groups: All Users; EXT_ID_RemoteUsers
  Roles: RemoteUsers
   Client Type: Remote Access
  Authentication Method: Trust
  Distinguished Name:
  Connect Time: Wed Apr 5 13:21:44 2023
Next Reauthentication: Wed Apr 5 14:59:53 2023
  Next Connectivity Check: -
  Next Ldap Fetch: -
Packet Tagging Status: Not Active
Published Gateways: Local
[Expert@cpgw:0]#
```