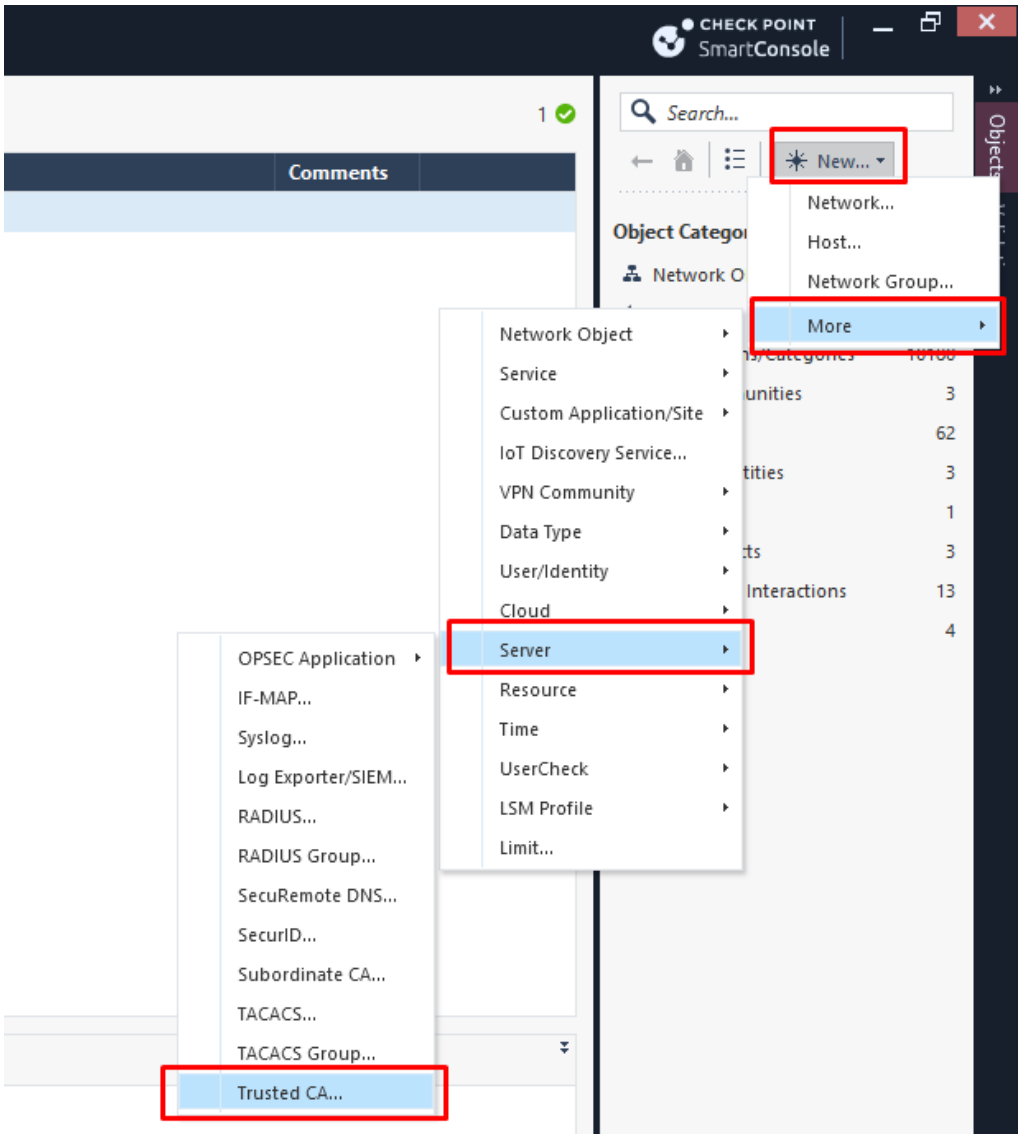
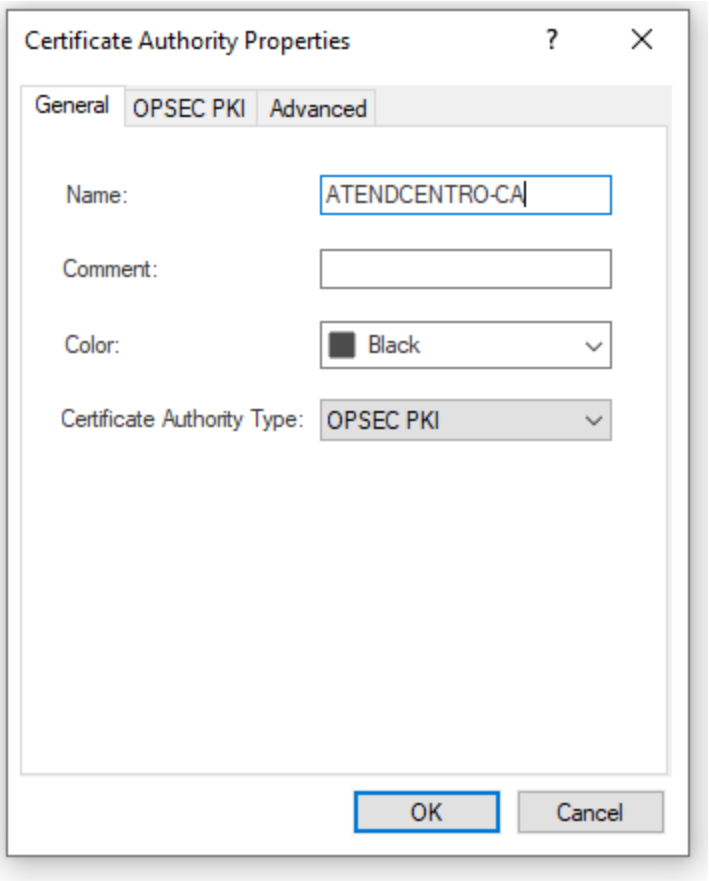
The purpose of this document is to demonstrate how to configure an Interoperable Device object to be used in a VPN Community where the remote peer is from another vendor (SonicWall in this case) and uses a dynamic IP.

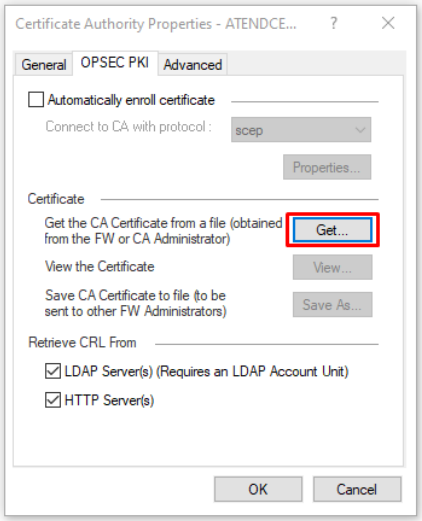
This is the certificate exported from the remote peer that will be imported into the Check Point management.

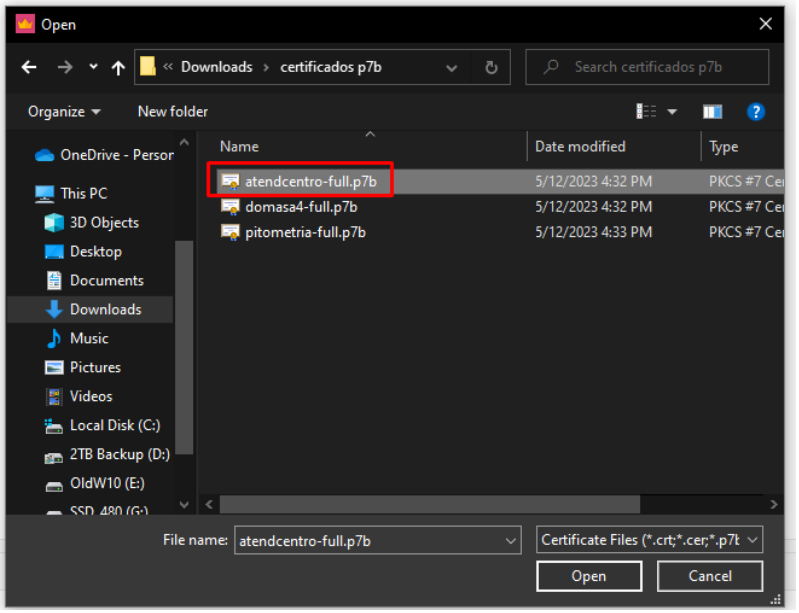
Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
atendcentro-full.p7b	PKCS #7 Certificates	3 KB	No	4 KB	21%	5/12/2023 4:32 PM
domasa4-full.p7b	PKCS #7 Certificates	3 KB	No	4 KB	21%	5/12/2023 4:32 PM
pitometria-full.p7b	PKCS #7 Certificates	3 KB	No	4 KB	21%	5/12/2023 4:33 PM

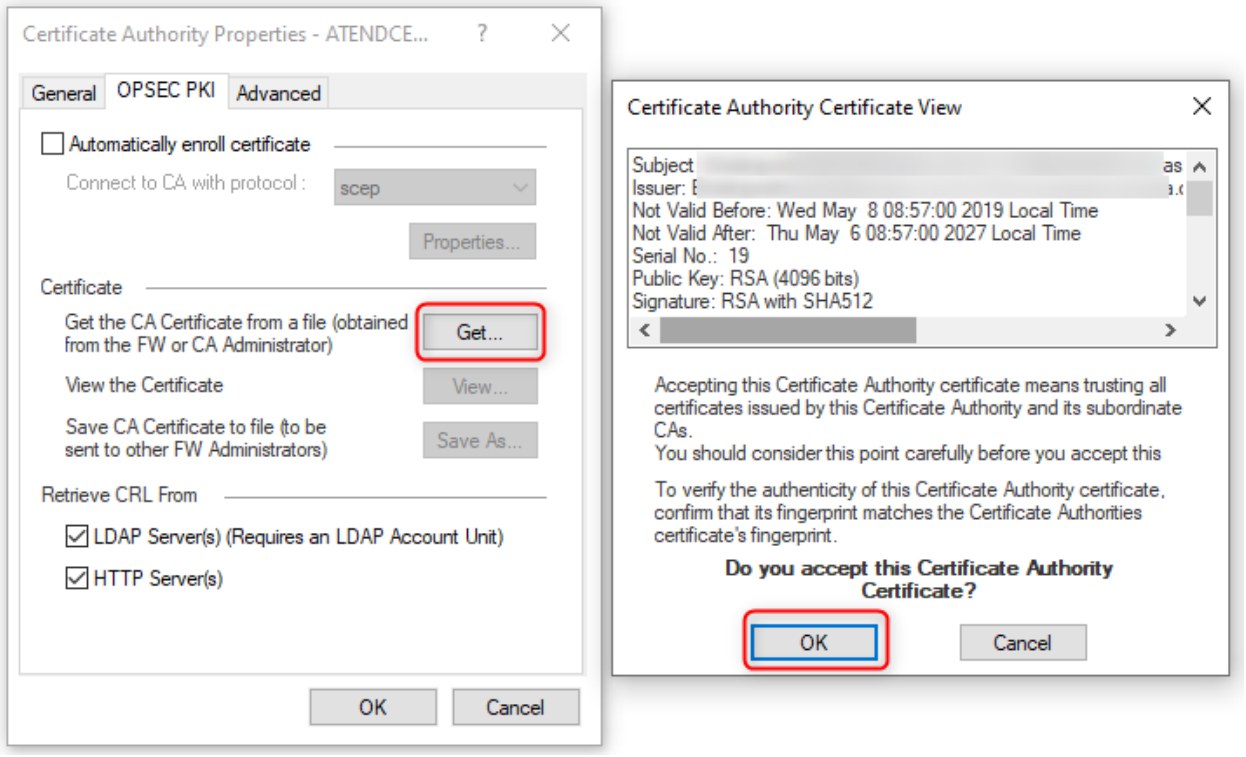
Before selecting which certificate will be used in the Interoperable Device peer object, import it as a Trusted CA following the procedure below.



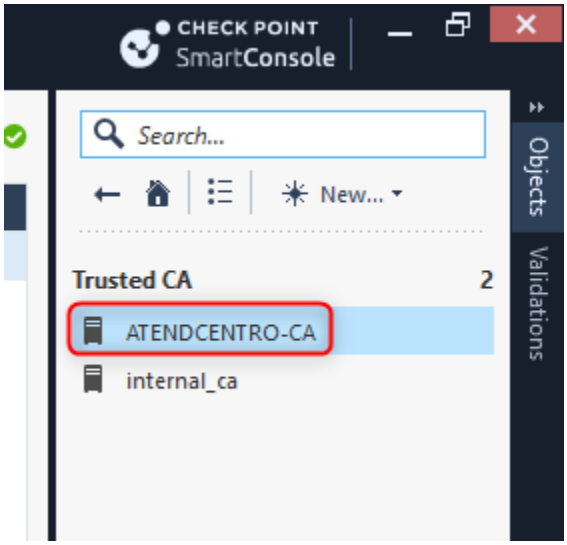

Certificate Authority Properties
General
OPSEC PKI
Advanced
Name:
ATENDCENTRO-CA
Comment:
Color:
Black
Certificate Authority Type:
OPSEC PKI
OK
Cancel


Certificate Authority Properties - ATENDCE...
General
OPSEC PKI
Advanced
Automatically enroll certificate
Connect to CA with protocol :
scep
Properties...
Certificate
Get the CA Certificate from a file (obtained from the FW or CA Administrator)
Get...
View the Certificate
View...
Save CA Certificate to file (to be sent to other FW Administrators)
Save As...
Retrieve CRL From
LDAP Server(s) (Requires an LDAP Account Unit)
HTTP Server(s)
OK
Cancel

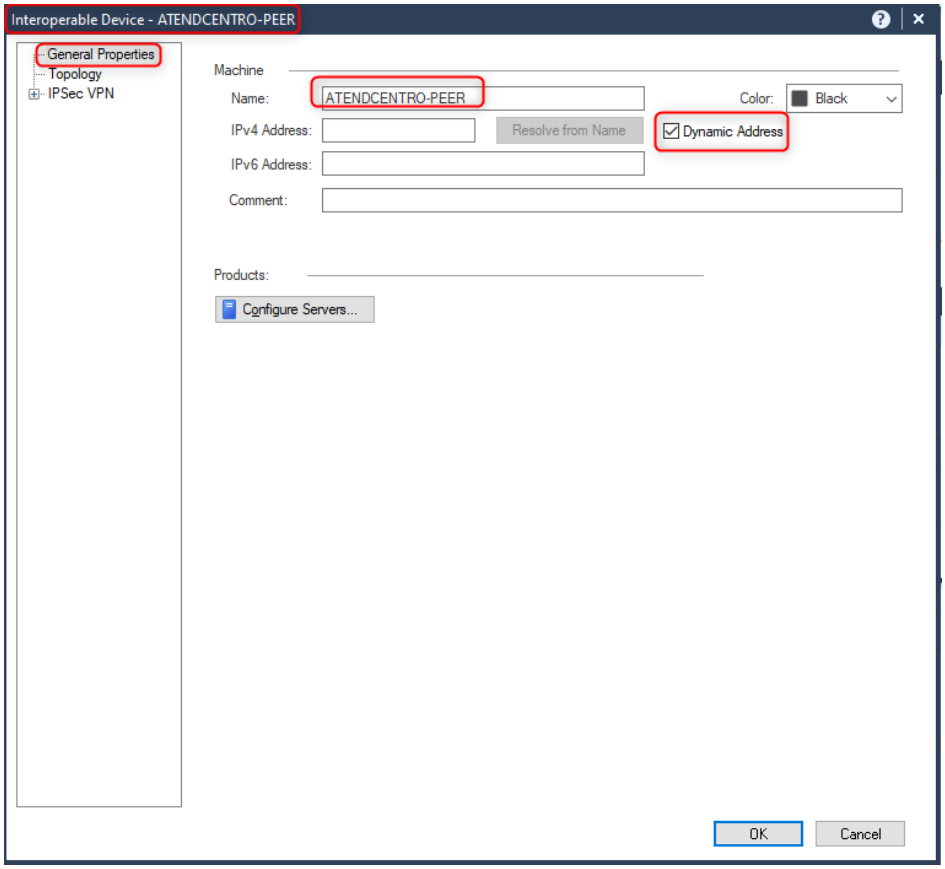

Open
Downloads
certificados p7b
Search certificados p7b
Organize
New folder
OneDrive - Persor
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
2TB Backup (D:)
OldW10 (E:)
Name
Date modified
Type
atendcentro-full.p7b
5/12/2023 4:32 PM
domasa4-full.p7b
5/12/2023 4:32 PM
pitometria-full.p7b
5/12/2023 4:33 PM
File name:
atendcentro-full.p7b
Certificate Files (*.crt;*.cer;*.p7b
Open
Cancel



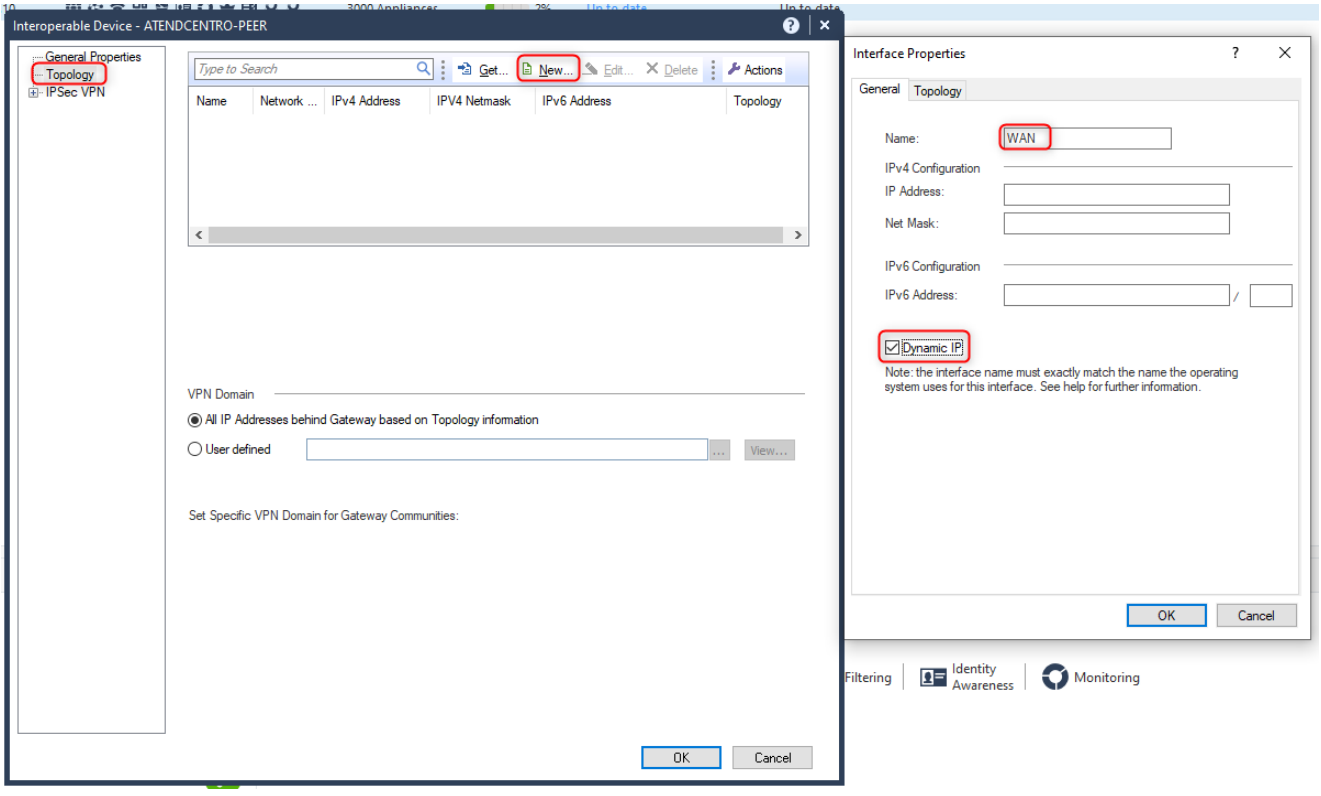
After creating the Trusted CA, it can be seen alongside the internal CA.



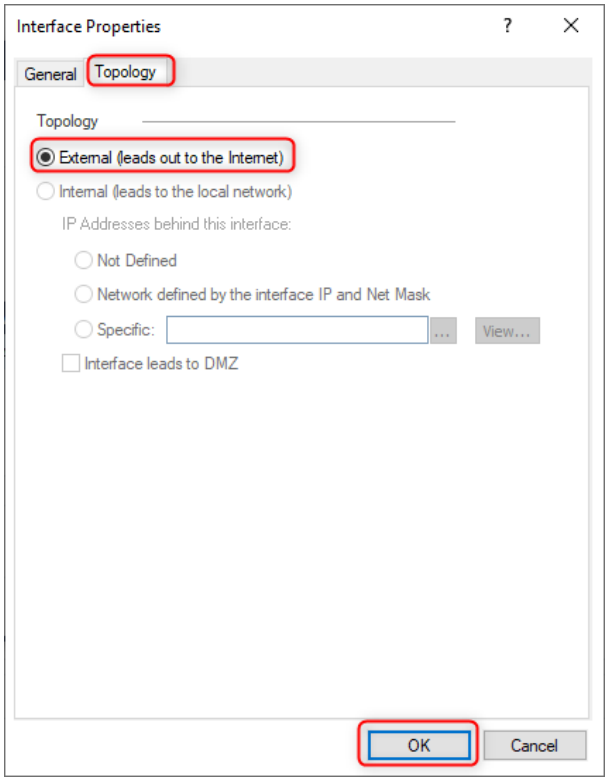
When creating the Interoperable Device object, in the General Properties tab, set a name and keep the 'Dynamic Address' option checked.



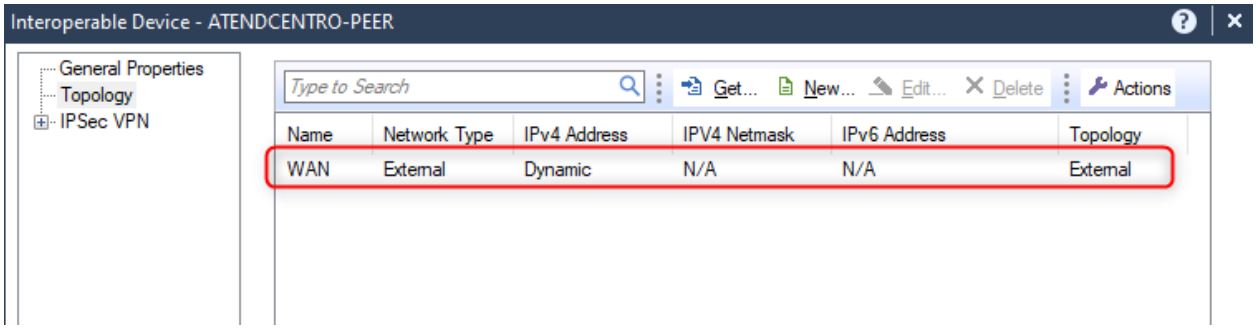
In the Topology tab, click on New to add an interface. In this case, the WAN interface will have a dynamic IP, so we keep the 'Dynamic IP' option selected.



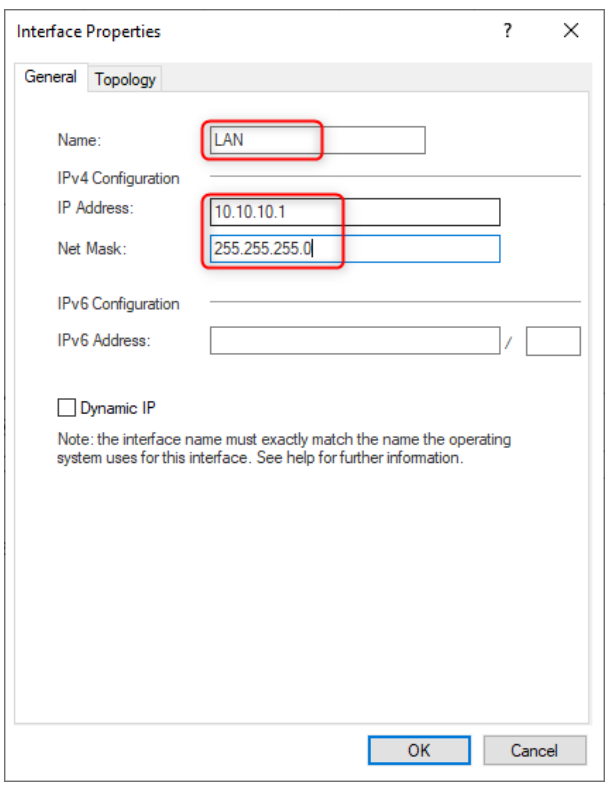
In the Topology tab, keep the 'External' option selected for this interface and click on OK.

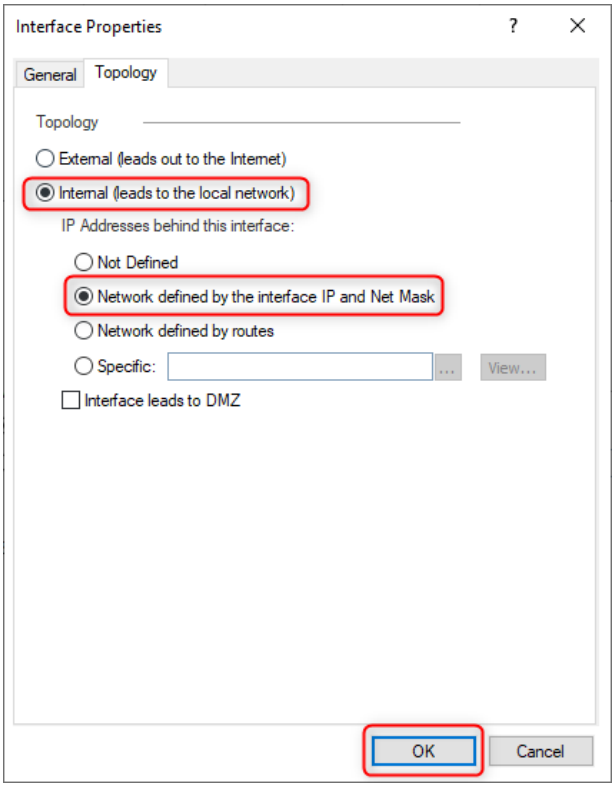


You will be able to see the newly created interface in the topology. Now let's repeat the process for the LAN interface.

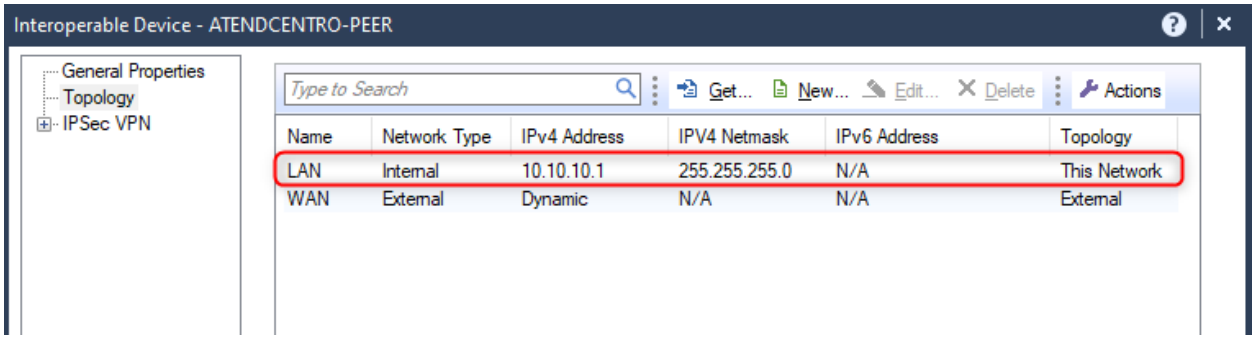


For the LAN interface, we will configure a fixed IP. Set the name, IP, and subnet mask for the interface. In the Topology tab, select the 'Internal' option, and then choose 'Network defined by the interface IP and Net Mask'. Click on OK.

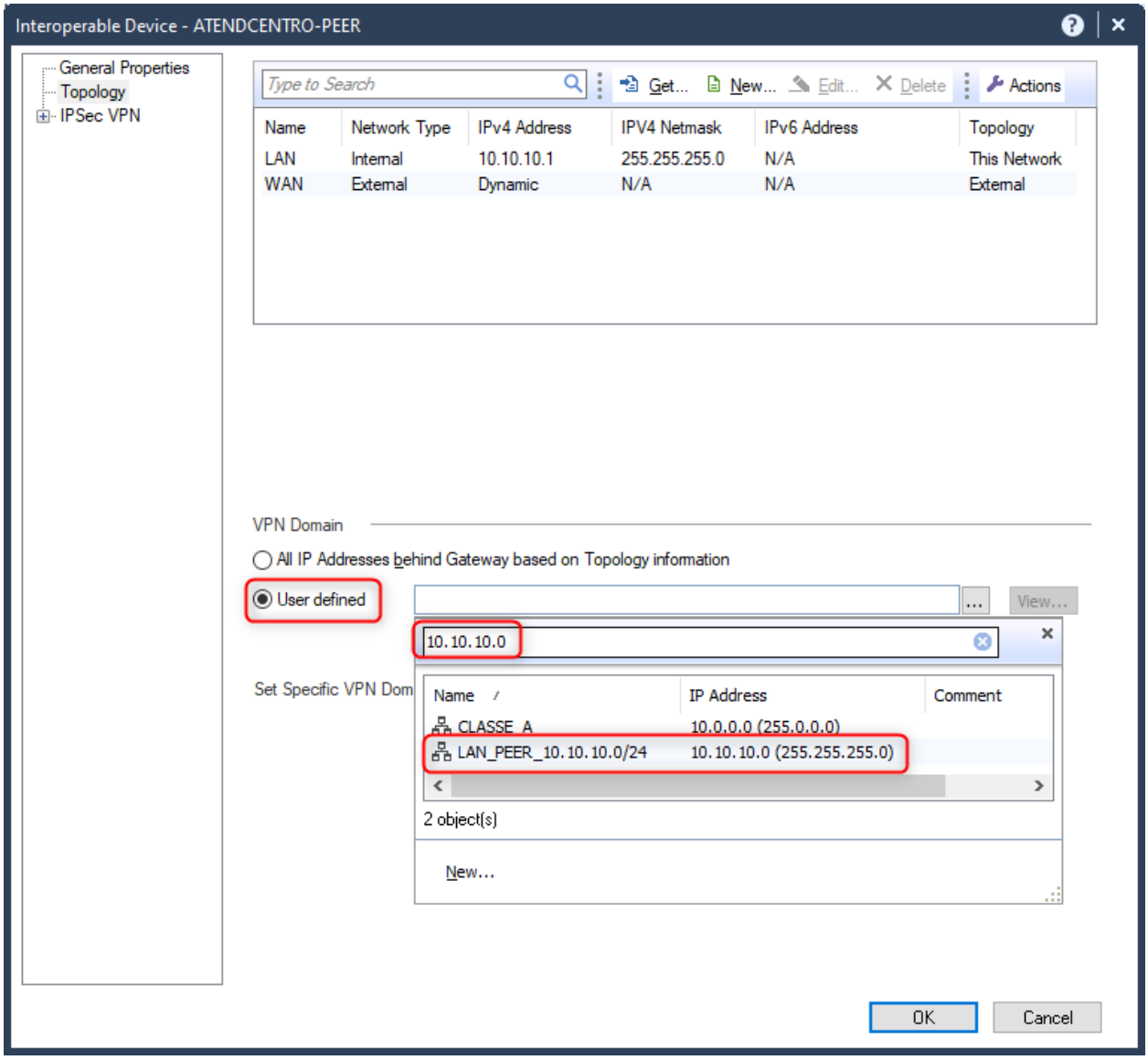




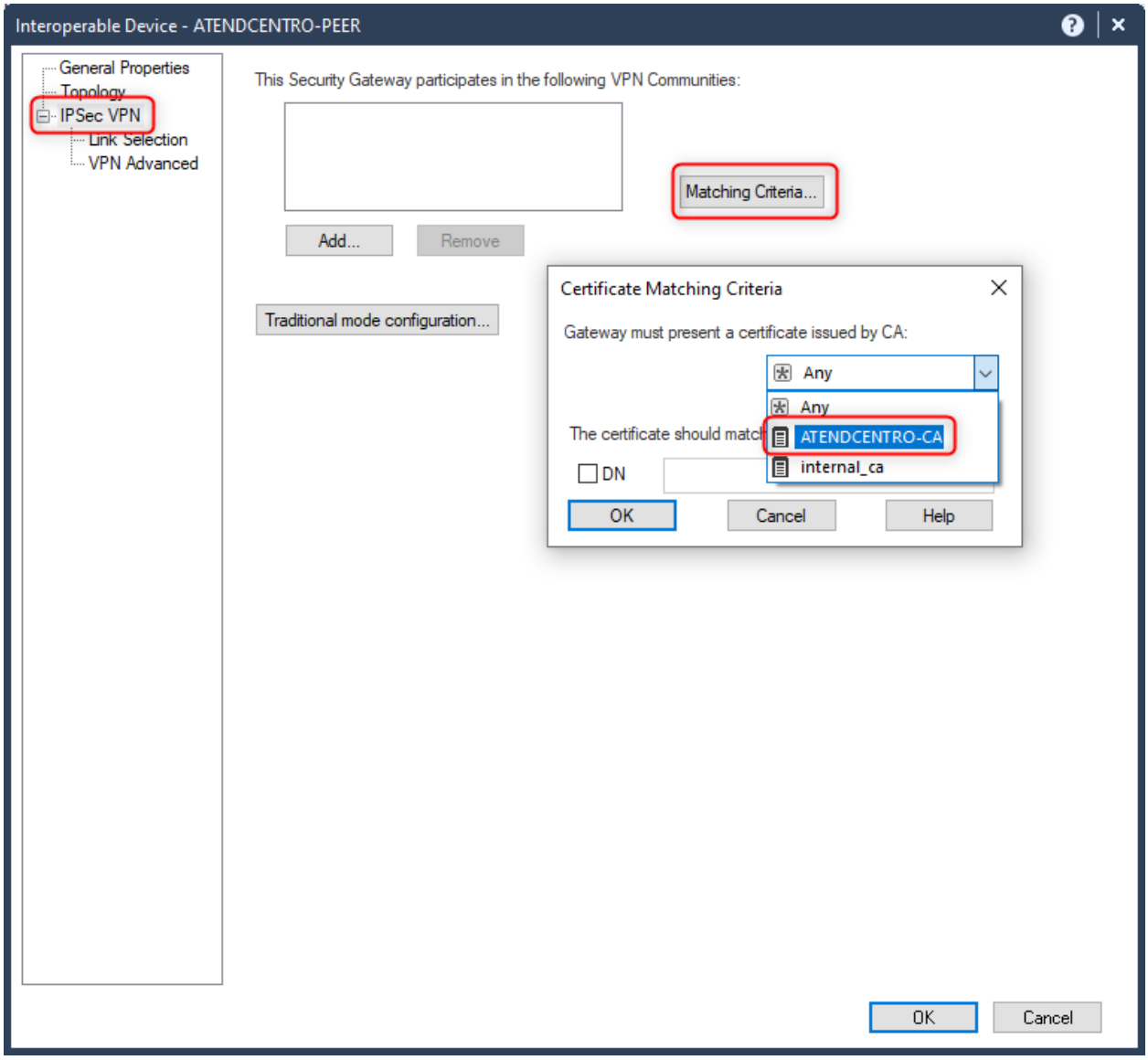
Now we can see the two interfaces that form the topology of the remote peer.



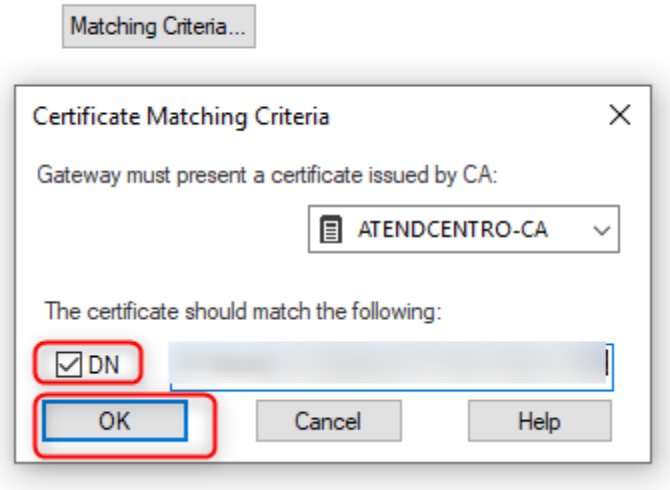
Still in the Topology section, let's define the VPN Domain. In this case, it's the same network as the LAN of the previously defined peer. If the object doesn't exist, create it.



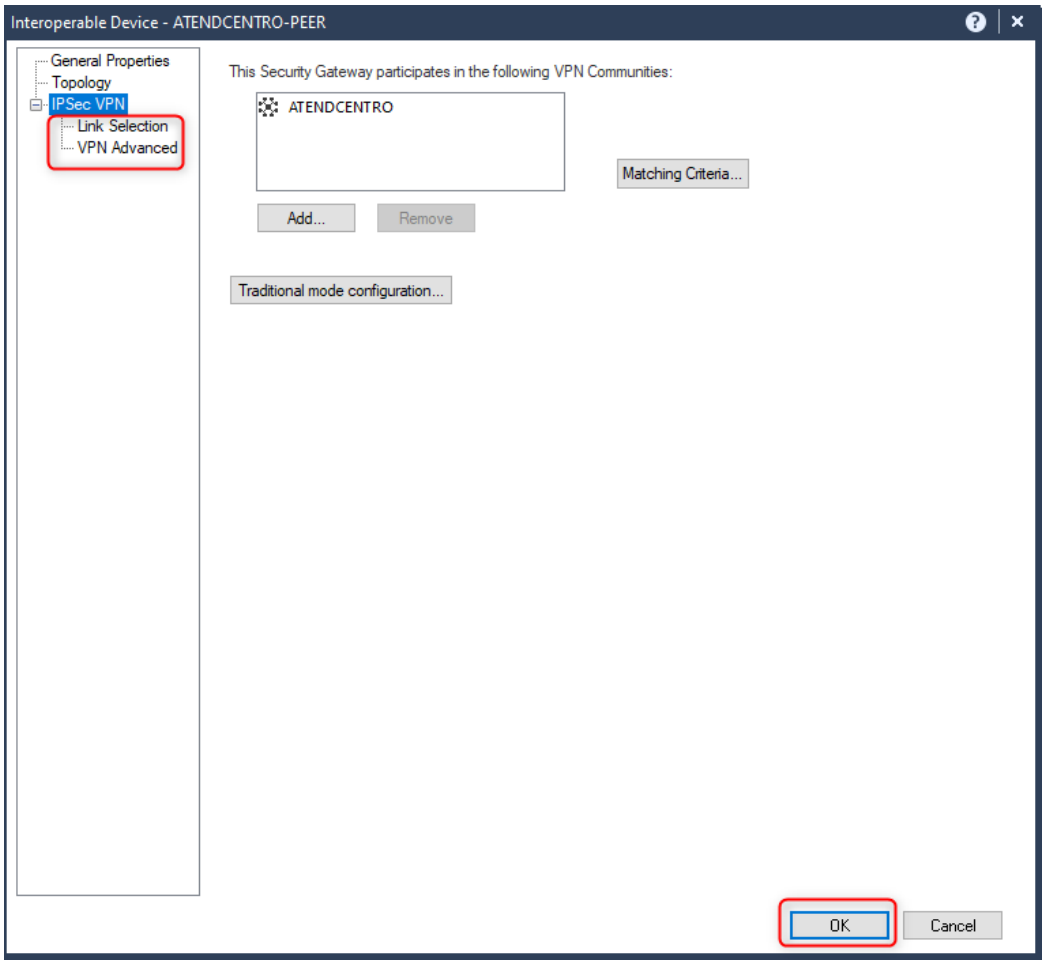
Now, in the IPSec VPN option, click on 'Matching Criteria' and select the previously imported certificate for the peer.



It is also necessary to check the 'DN' option and provide the DN (Distinguished Name) that is listed on the certificate.



No changes are required in the Link Selection and VPN Advanced options. Just click OK to finalize the configuration of the Interoperable Device object for the remote peer with a dynamic IP.



Now, you just need to proceed with the remaining configurations of the Community as usual and install the policies. It is also necessary to import the Management Server's certificate to the remote peer.