Windows Server 2019 Training – Final Project

By Alaa' Omar

(alaa.omer2009@gmail.com)

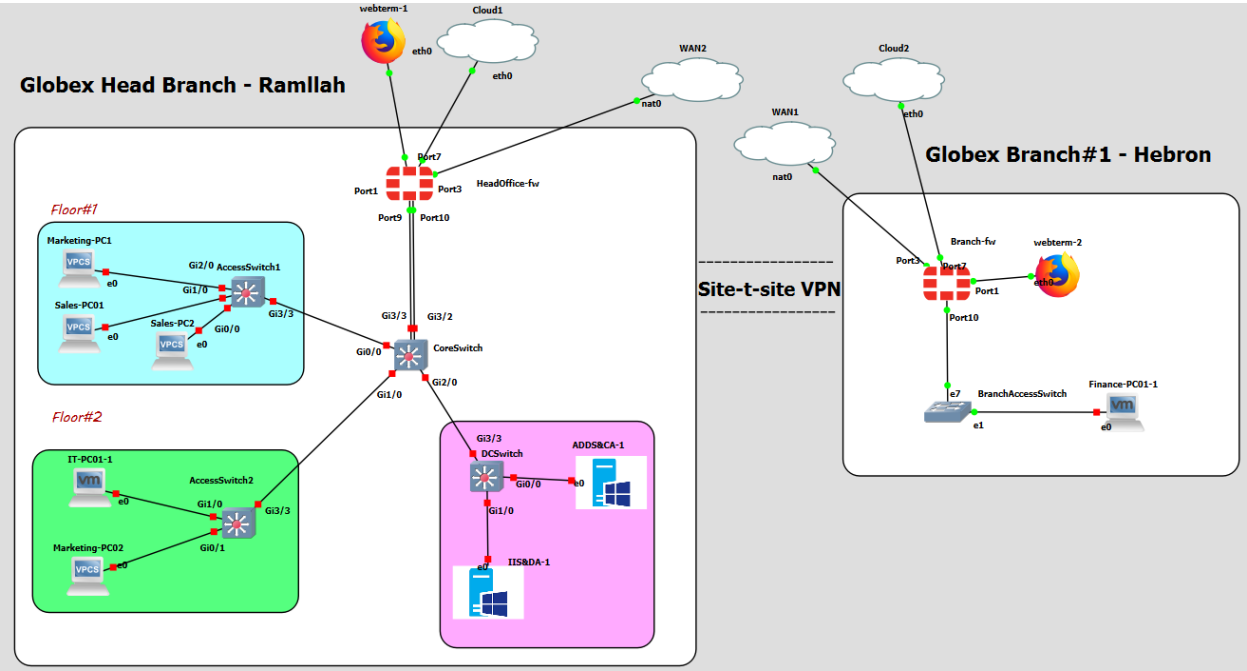


Figure 1 Globex Network Diagram

Table of Contents

Network Construction, and Hardware Configuration

Head Office Firewall

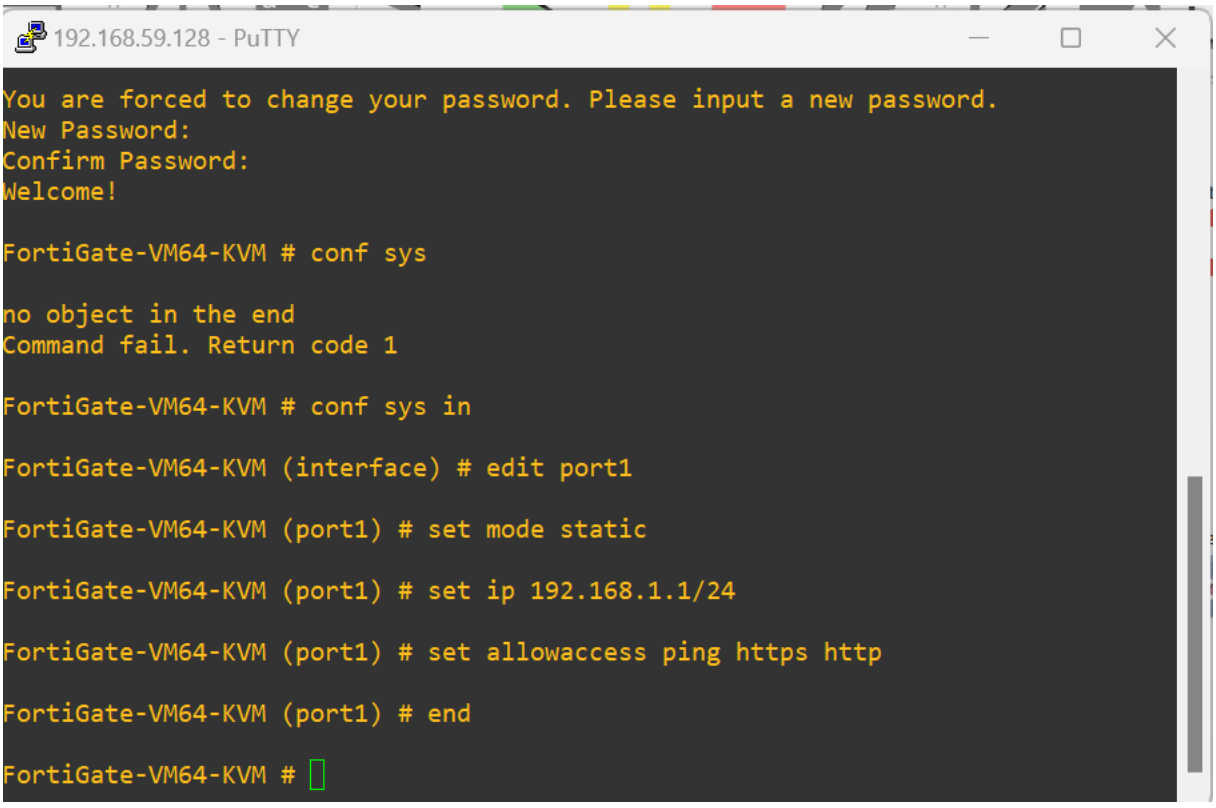
Firewall settings:

Ip address: 192.168.10.10

Username: admin

Password: admin

Firewall Configuration



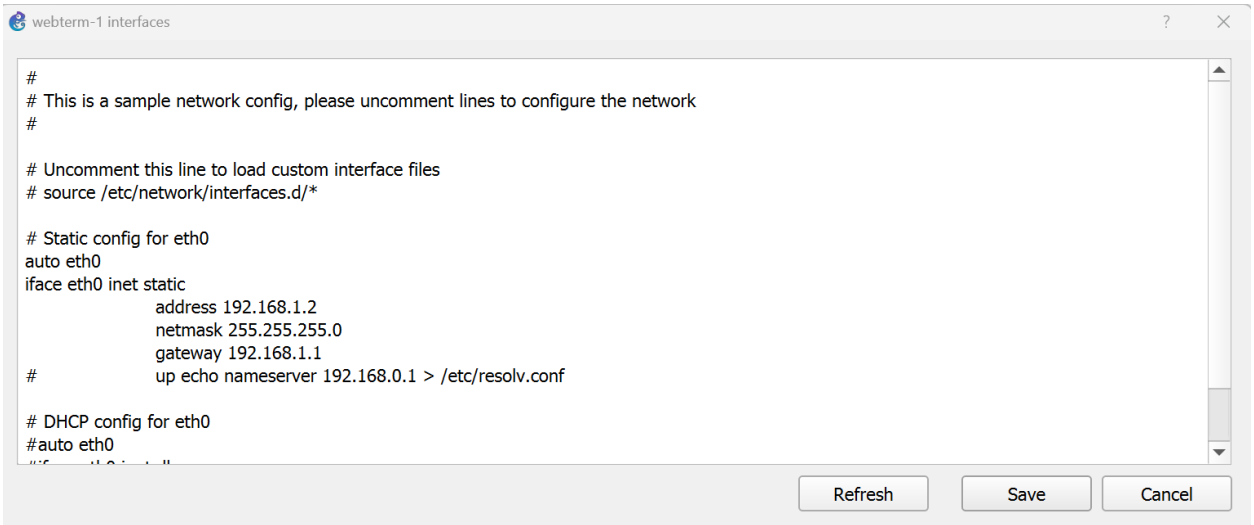


Figure 2 Webterm Configurations

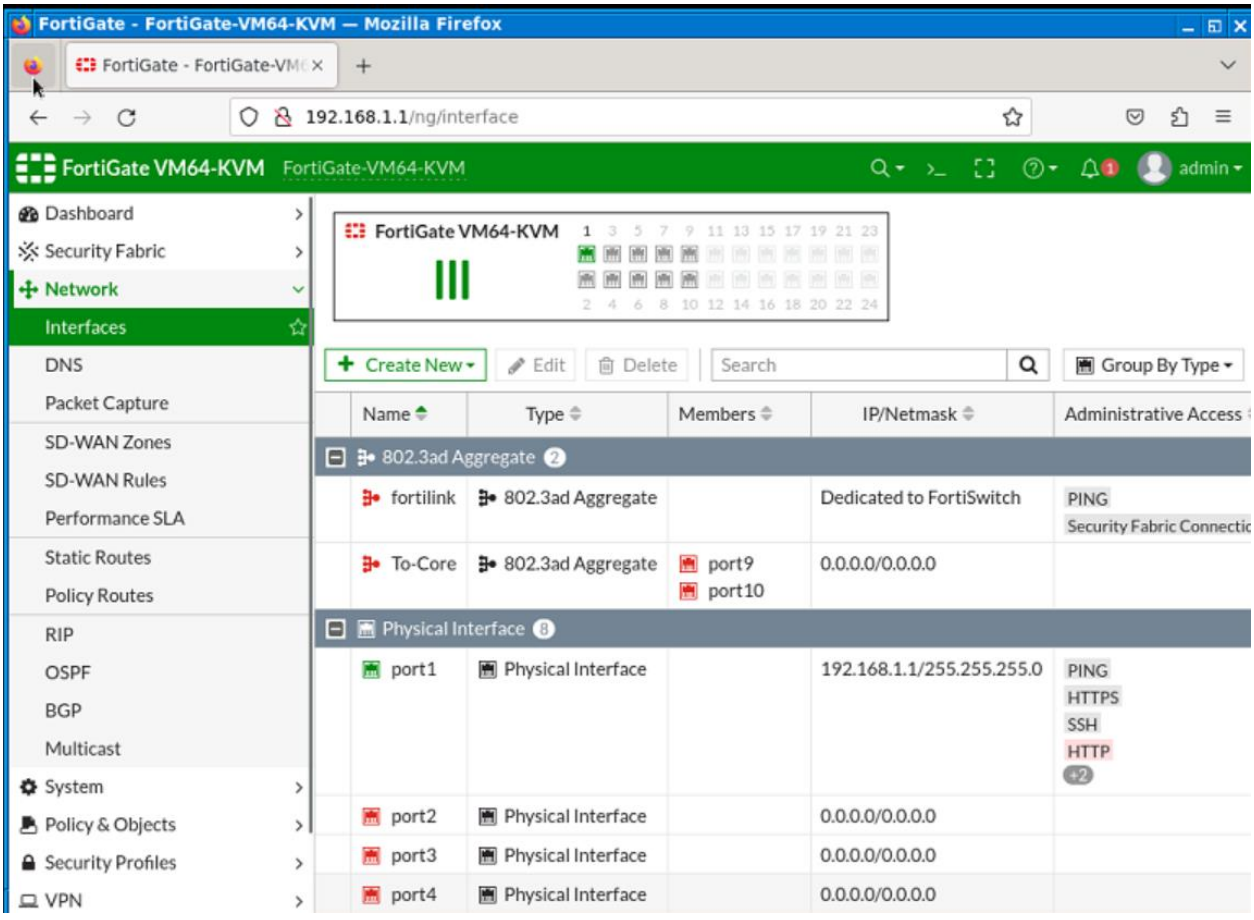
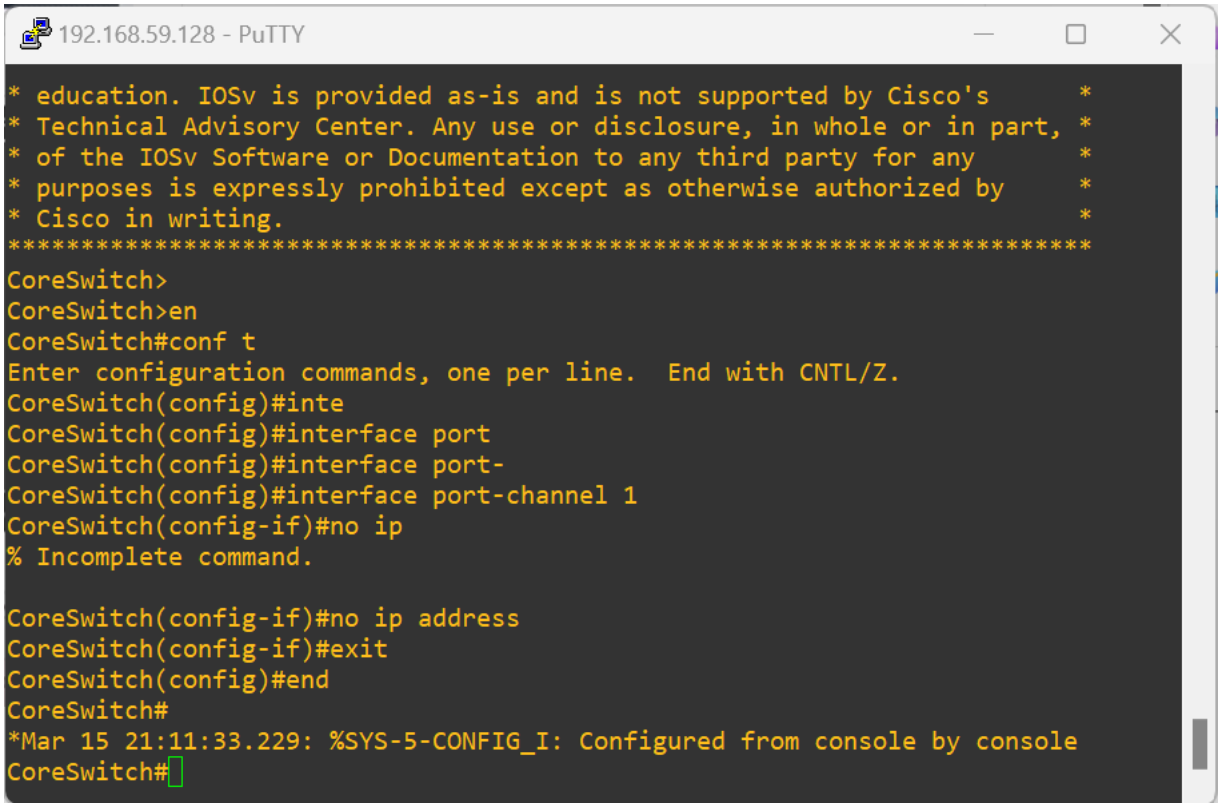


Figure 3 Firewall Configurations

Core Switch Configurations

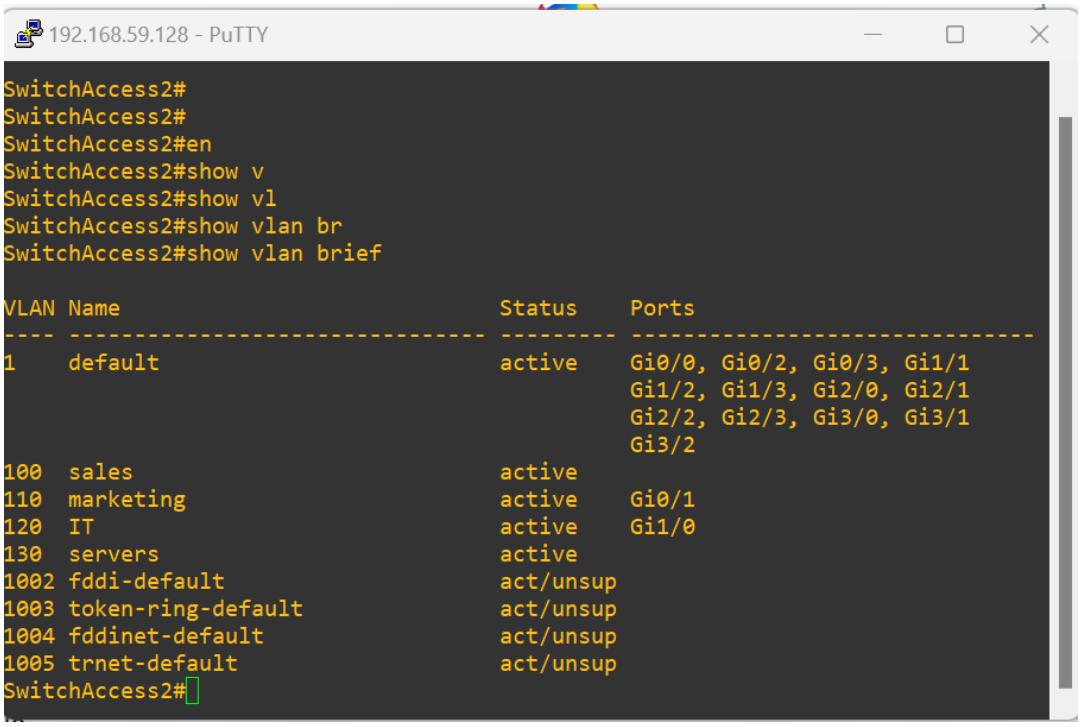


192.168.59.128 - PuTTY

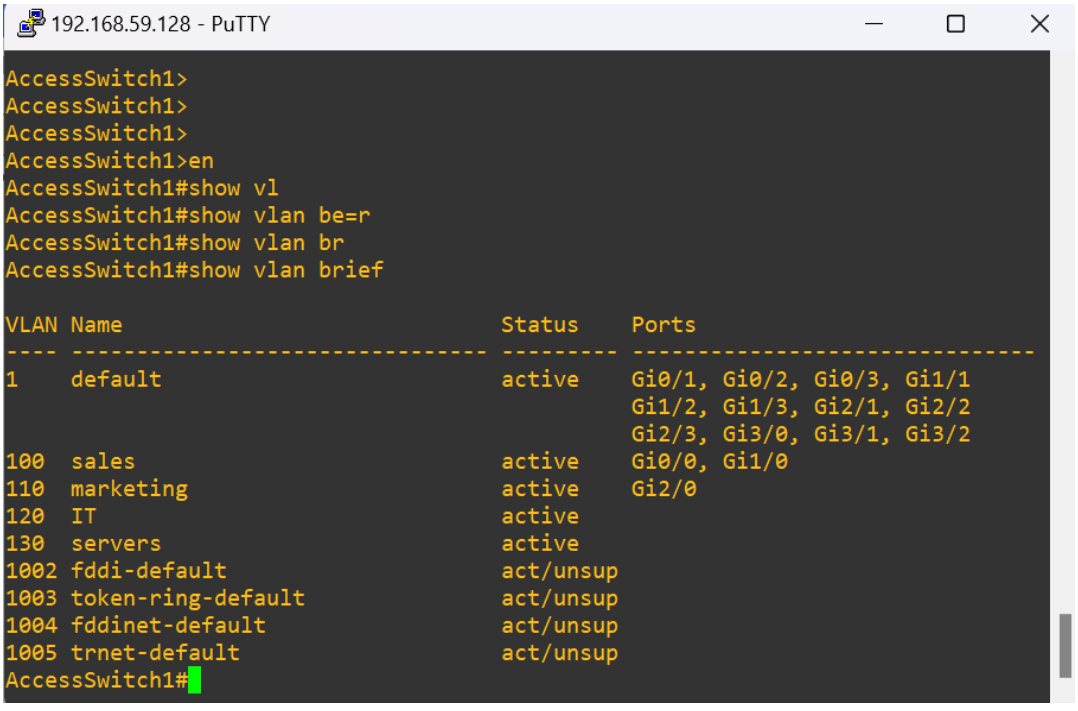
```
CoreSwitch(config-if)#switchport mode trunk
CoreSwitch(config-if)#
*Mar 15 21:27:35.959: %LINK-3-UPDOWN: Interface Port-channel1, changed state to
down
*Mar 15 21:27:36.961: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-chann
el1, changed state to down
*Mar 15 21:27:41.124: %LINK-3-UPDOWN: Interface Port-channel1, changed state to
up
*Mar 15 21:27:42.131: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-chann
el1, changed state to up
CoreSwitch(config-if)#
CoreSwitch(config-if)#sw
CoreSwitch(config-if)#switchport a
CoreSwitch(config-if)#switchport all
CoreSwitch(config-if)#switchport all
CoreSwitch(config-if)#switchport tr
CoreSwitch(config-if)#switchport trunk a
CoreSwitch(config-if)#switchport trunk allowed vl
CoreSwitch(config-if)#switchport trunk allowed vlan 100,110,120,130
CoreSwitch(config-if)#exit
CoreSwitch(config)#interface gigabitEthernet 2/0
CoreSwitch(config-if)#sw
CoreSwitch(config-if)#switchport all
CoreSwitch(config-if)#switchport tr
CoreSwitch(config-if)#switchport trunk all
CoreSwitch(config-if)#switchport trunk allowed vl
CoreSwitch(config-if)#switchport trunk allowed vlan 100,110,120,130
CoreSwitch(config-if)#exit
CoreSwitch(config)#interface gigabitEthernet 0/0
CoreSwitch(config-if)#sw
CoreSwitch(config-if)#switchport all
CoreSwitch(config-if)#switchport tr
CoreSwitch(config-if)#switchport trunk all
CoreSwitch(config-if)#switchport trunk allowed vlan 100,110,120,130
CoreSwitch(config-if)#exit
CoreSwitch(config)#interface gigabitEthernet 1/0
CoreSwitch(config-if)#sw
CoreSwitch(config-if)#switchport tr
CoreSwitch(config-if)#switchport trunk all
CoreSwitch(config-if)#switchport trunk allowed vlan 100,110,120,130
CoreSwitch(config-if)#exit
CoreSwitch(config)#
```

Figure 4 CoreSwitch Configurations

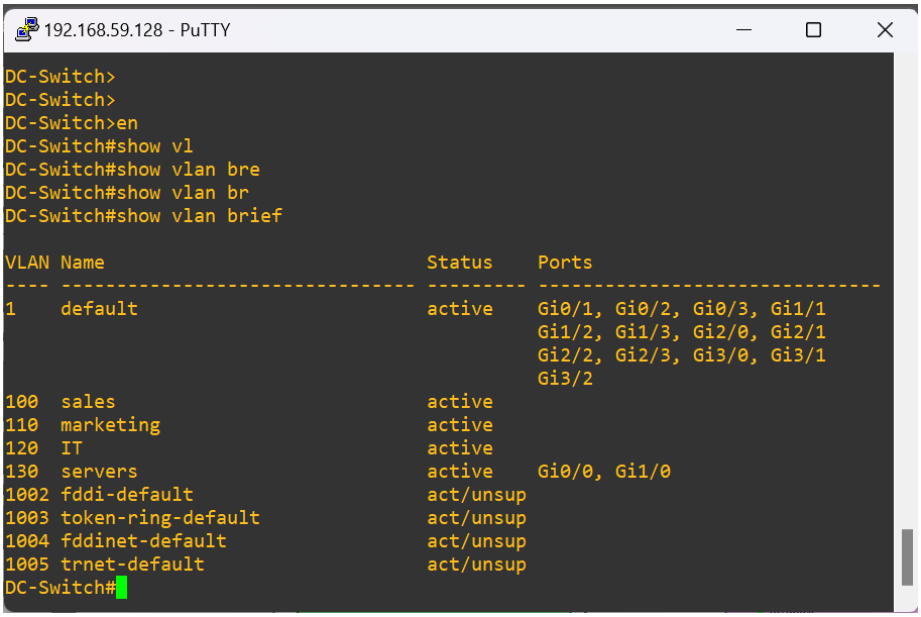
Switch Access 2 Configurations



Switch Access 1 Configurations



DC-Switch Configurations



PCS

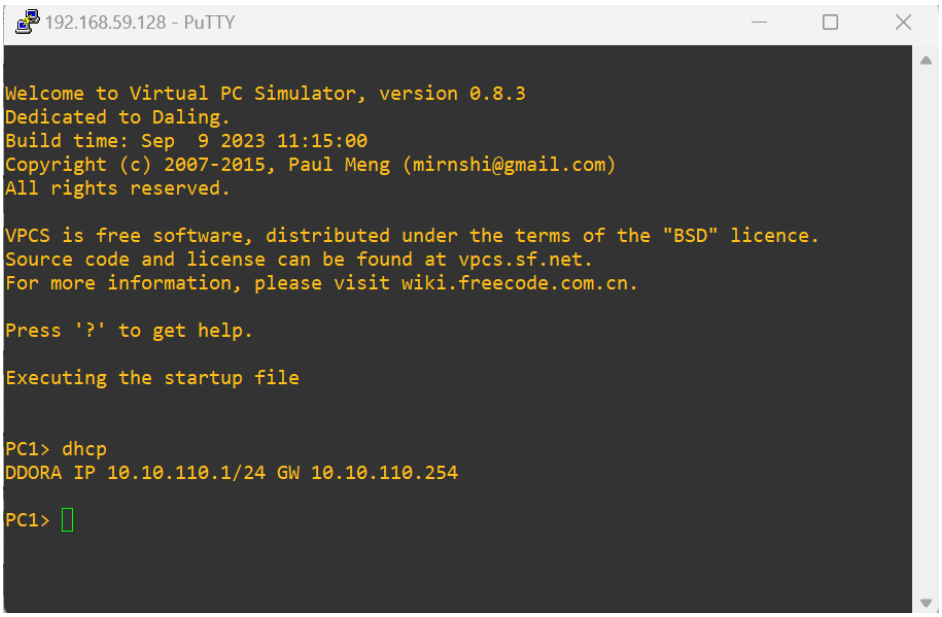


Figure 5 Marketing VLAN DHCP

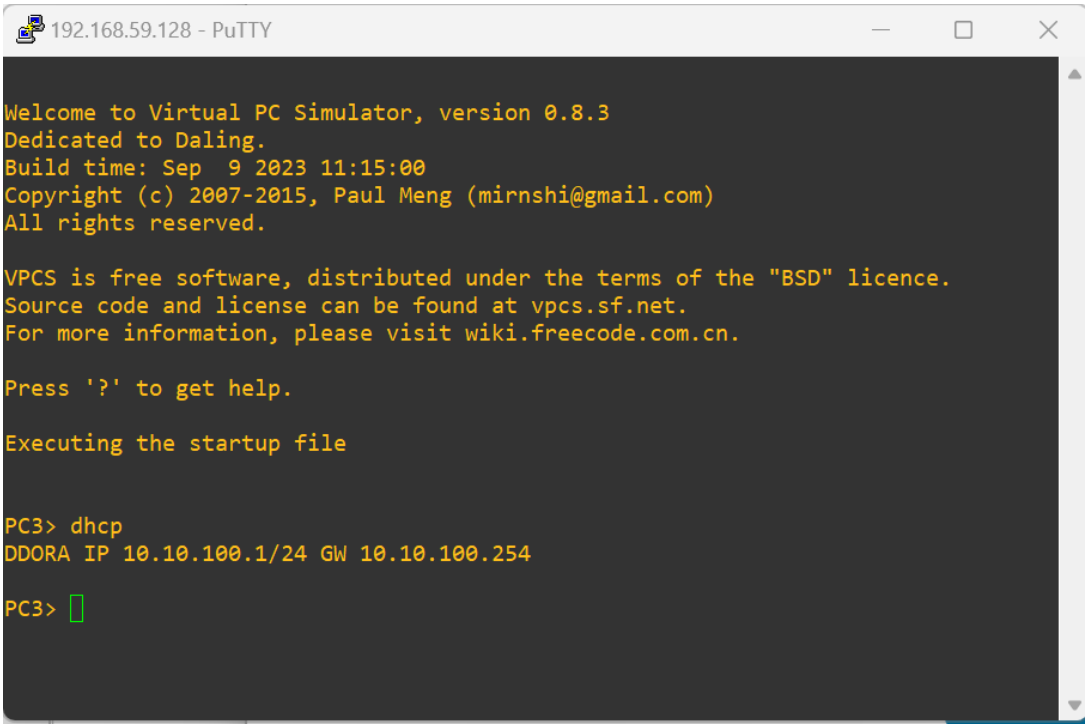


Figure 6 Sales VLAN DHCP

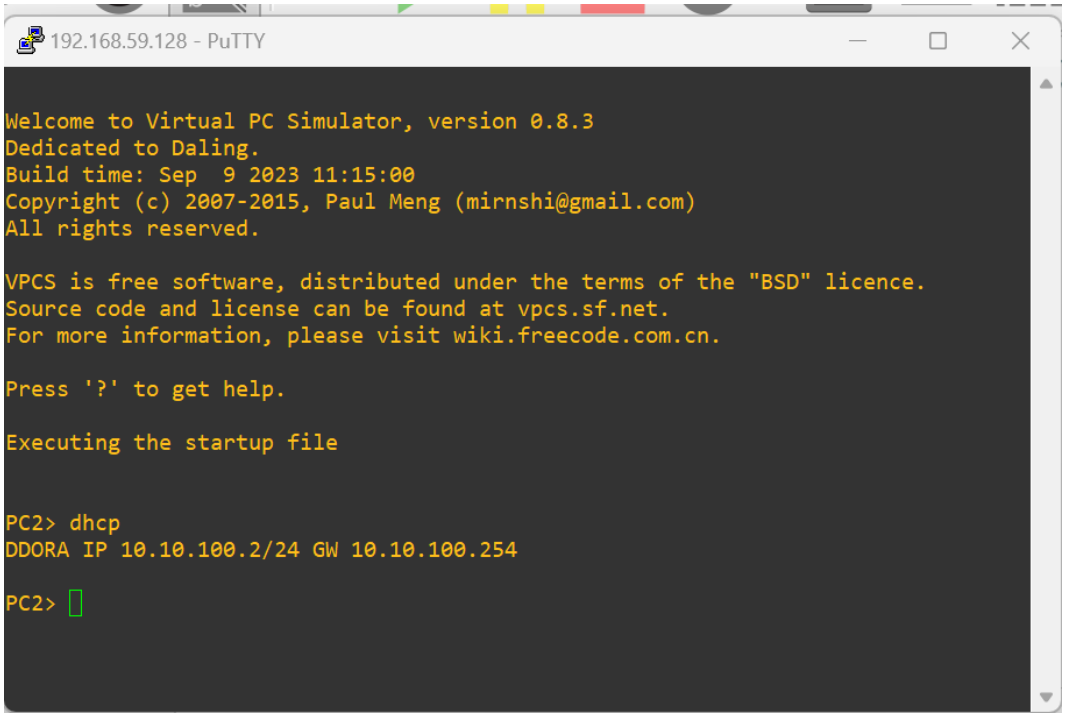


Figure 7 Sales PC2

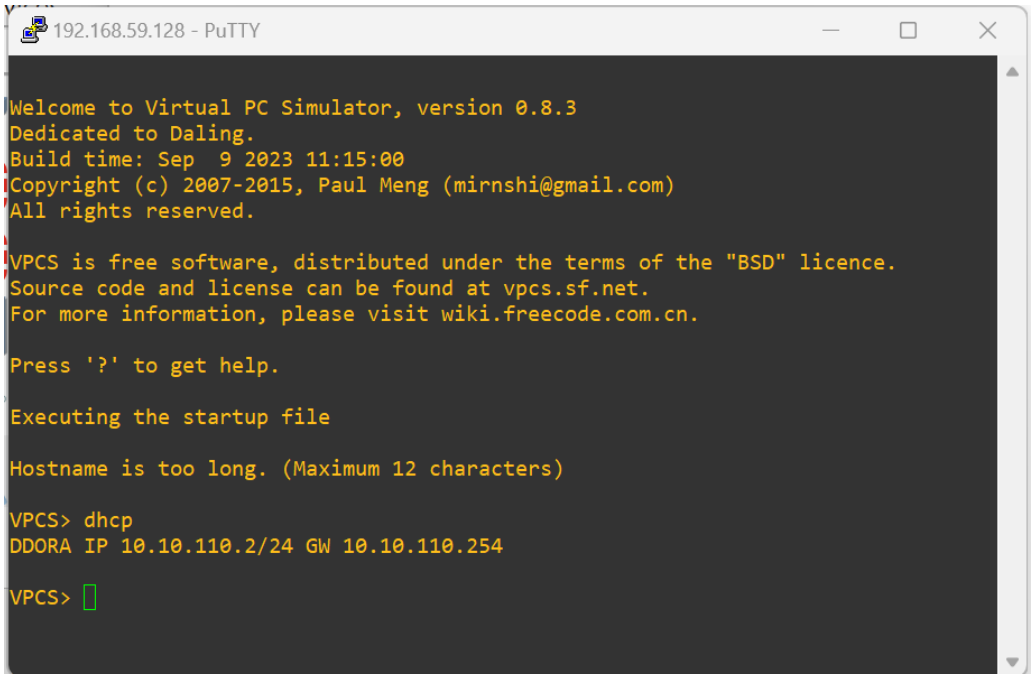


Figure 8 Marketing PC2

Internet Settings.

- Static route was added.
- A policy from vlans to WAN was added.

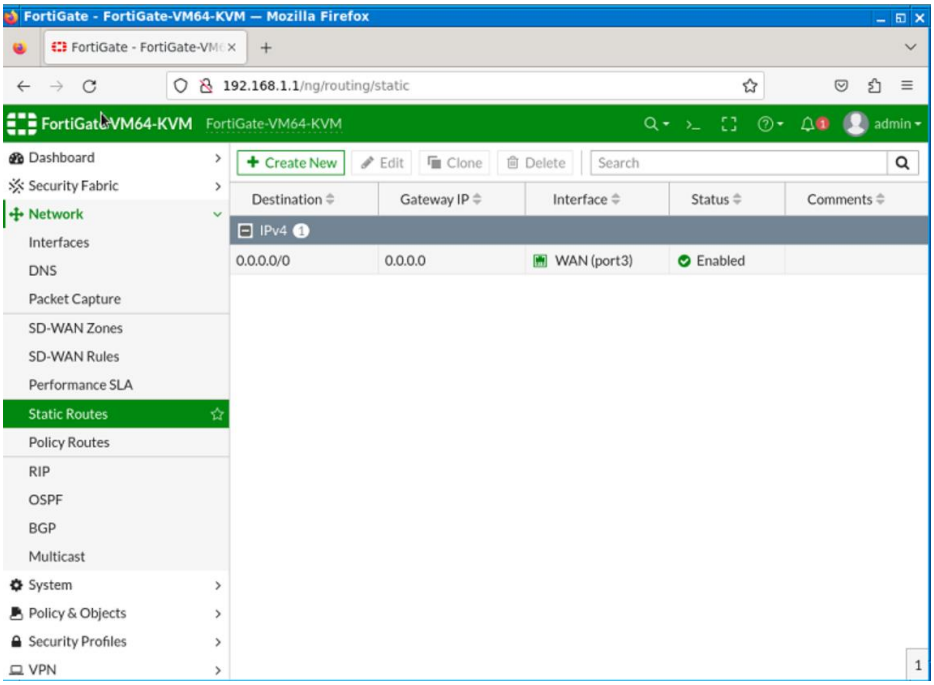
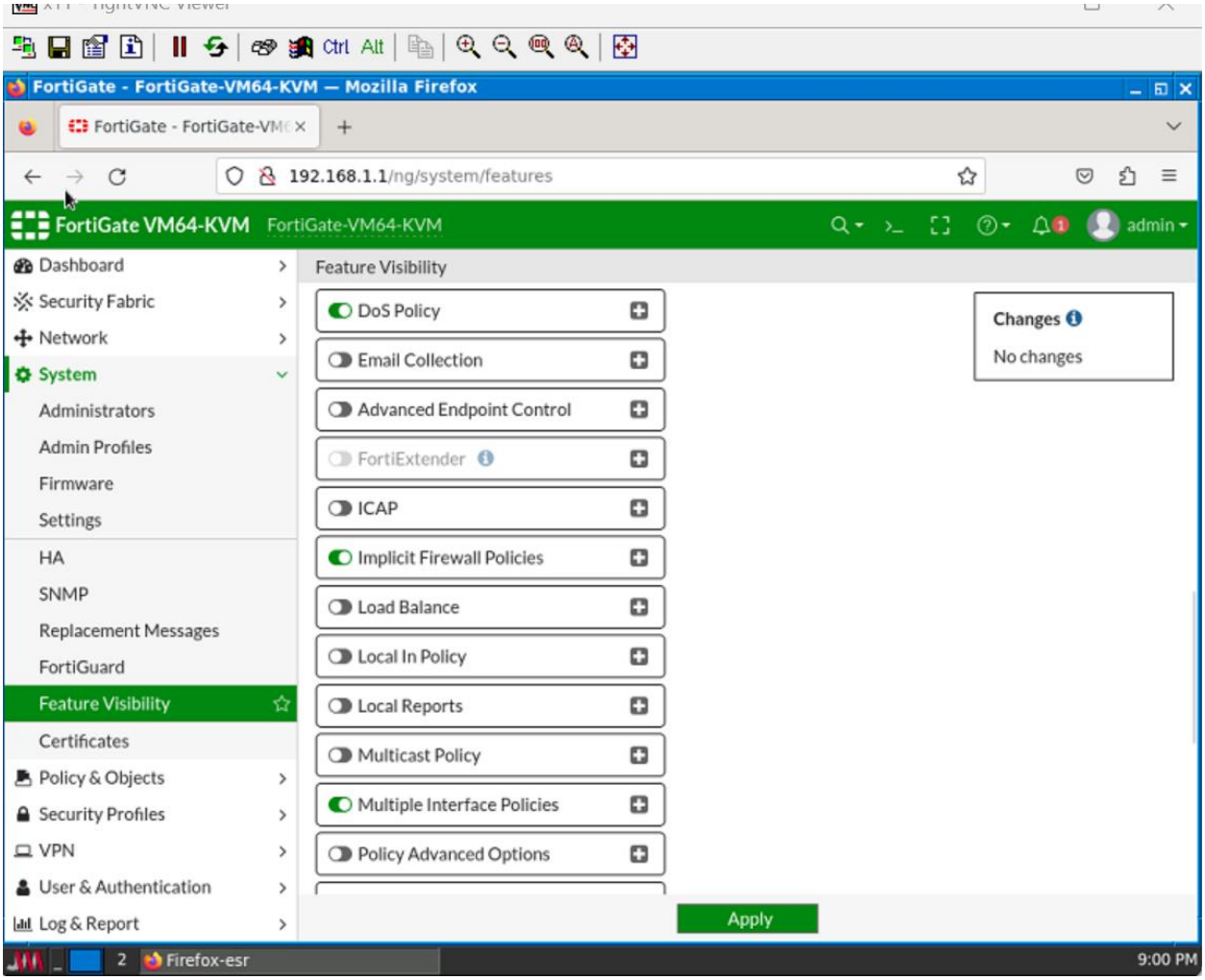


Figure 9 Firewall Static Route

But before adding the policy, from Feature visibility, I activate multiple interface policy.



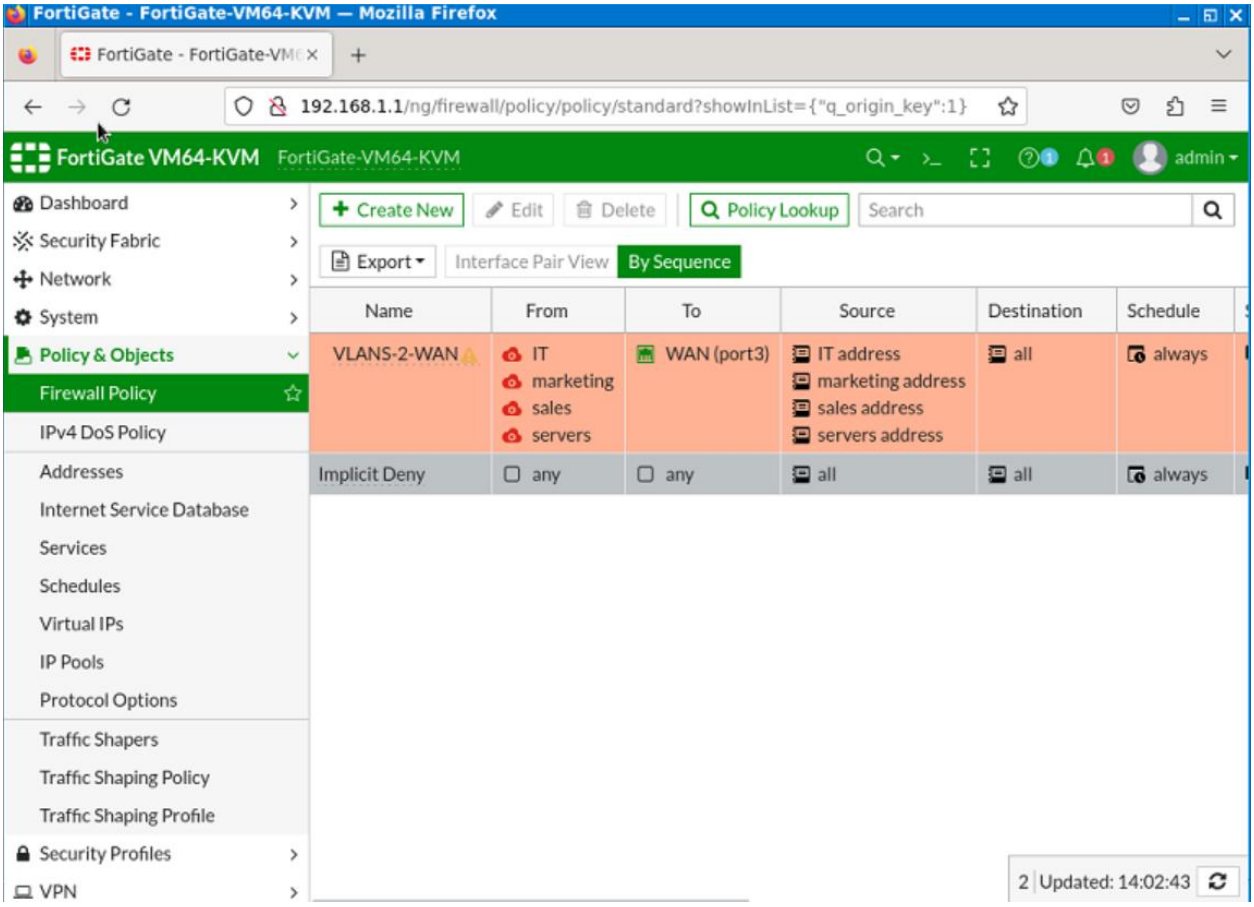


Figure 10 VLANS -to- WAN Policy

Hebron Office :

Firewall settings:

Ip address: 192.168.10.10

Username: admin

Password: admin

```
FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port1

FortiGate-VM64-KVM (port1) # set mode static

FortiGate-VM64-KVM (port1) # set ip 192.168.10.10/24

FortiGate-VM64-KVM (port1) # set allowaccess ping https http telnet ssh

FortiGate-VM64-KVM (port1) # end
```

Figure 11 Branch Firewall Console Settings

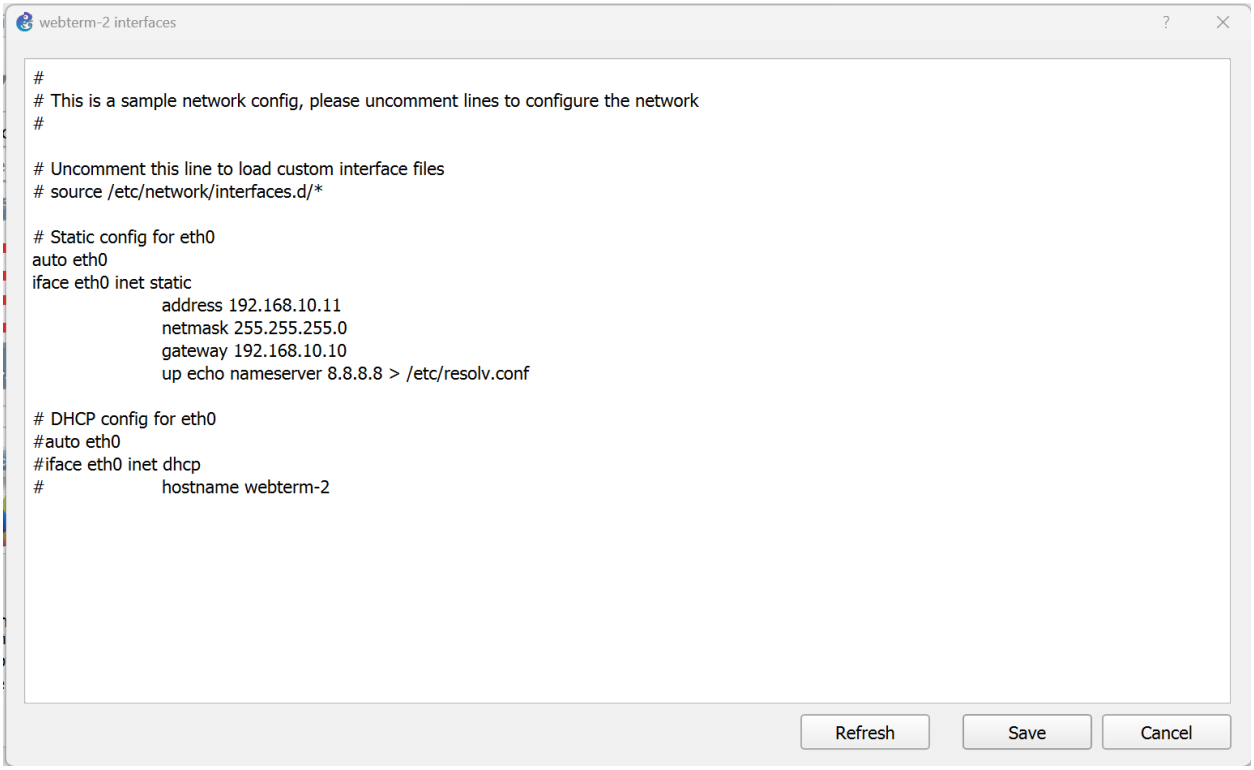


Figure 12 Webterm Settings

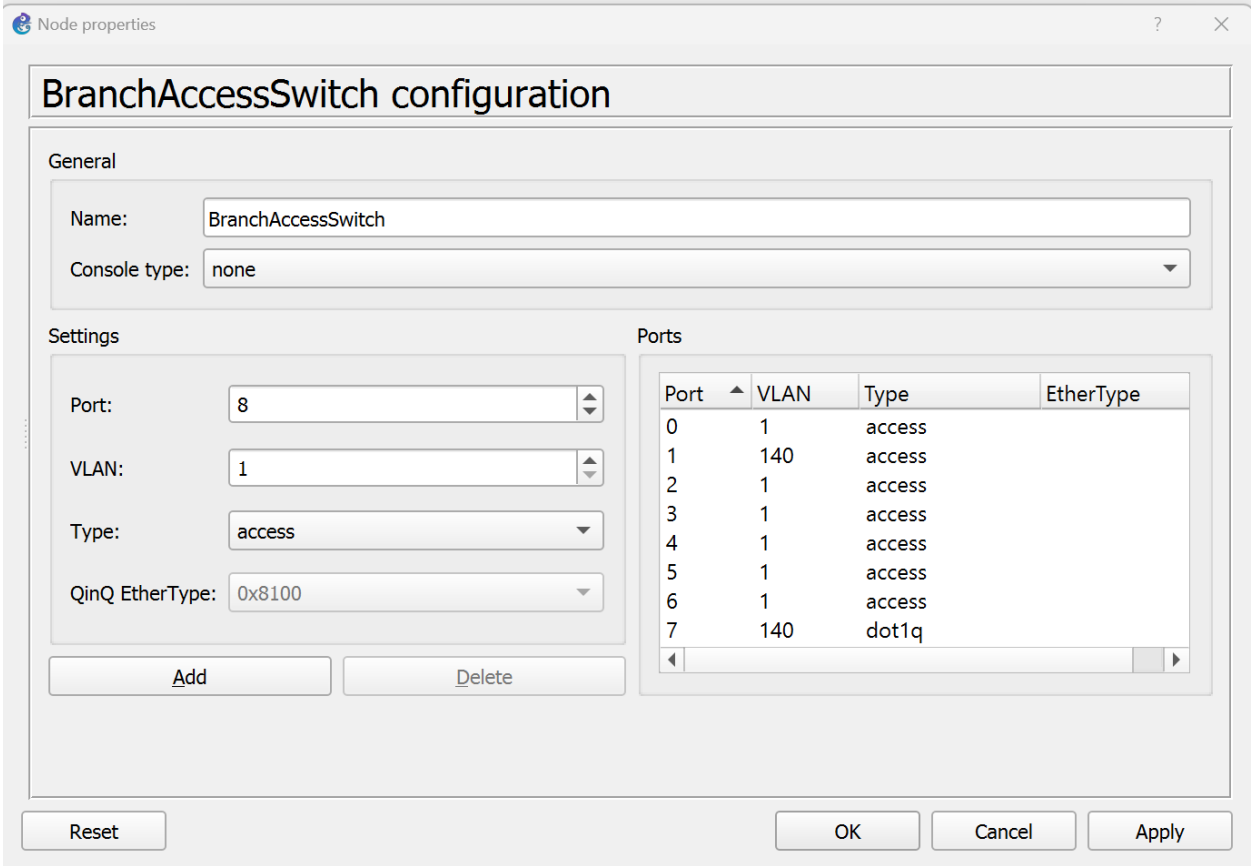


Figure 13 Branch Switch Configuration

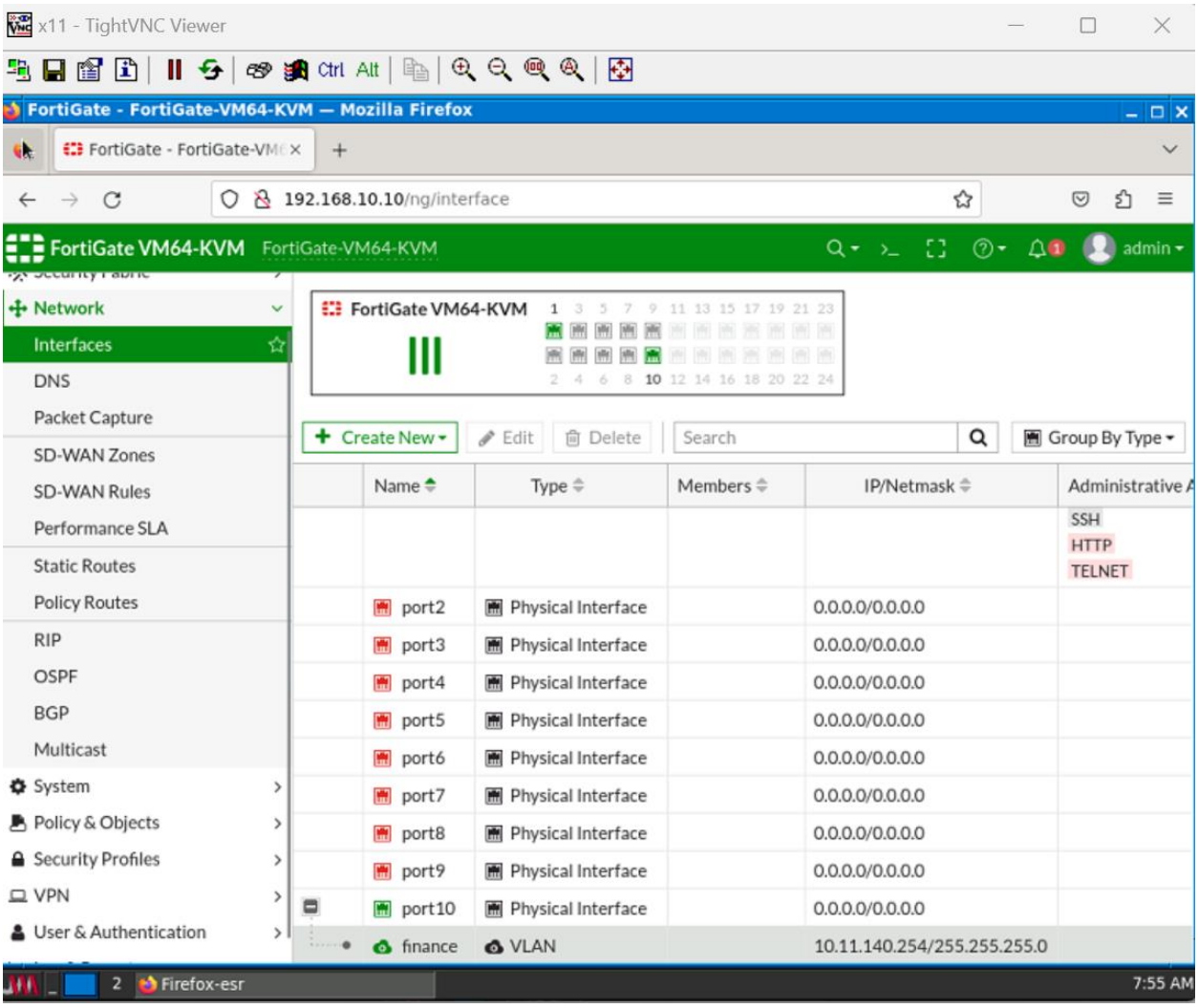


Figure 14 Firewall interfaces.

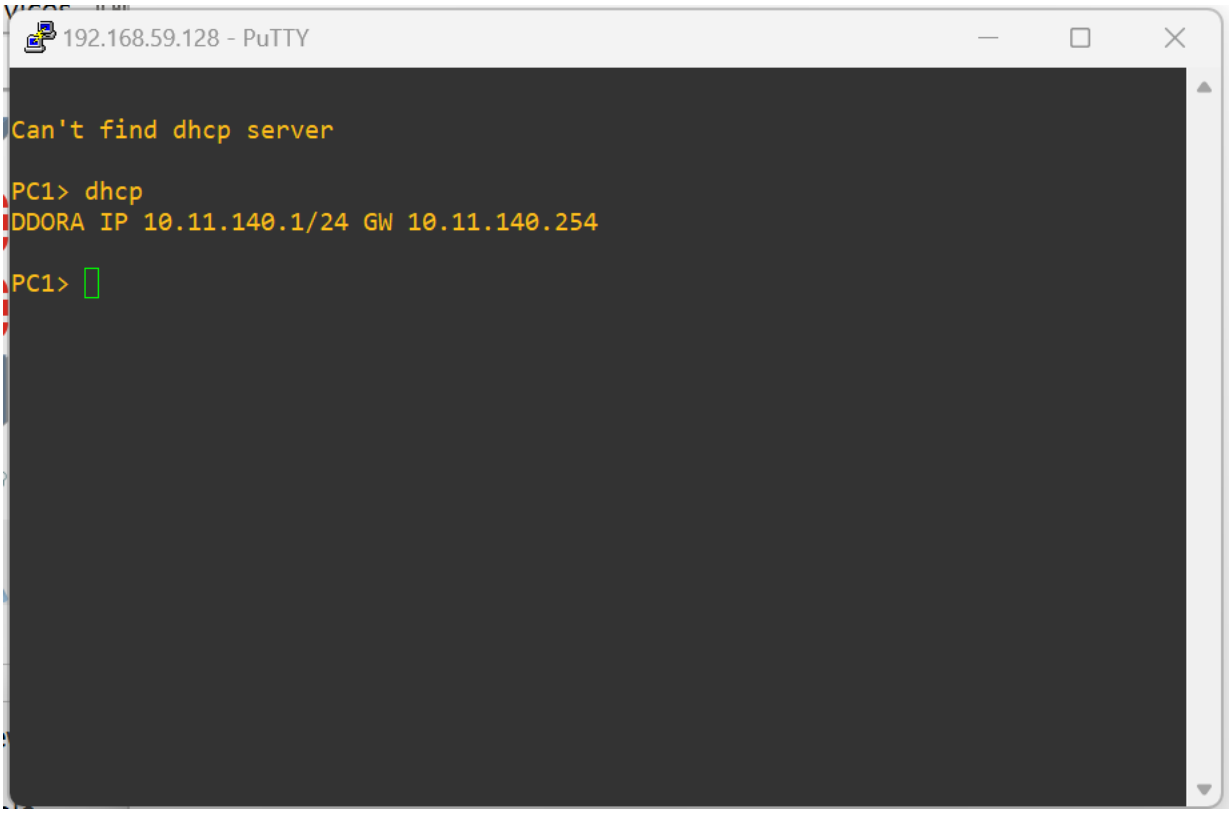


Figure 15 Activate DHCP Marketing VLAN

Hebron Branch – Internet Settings

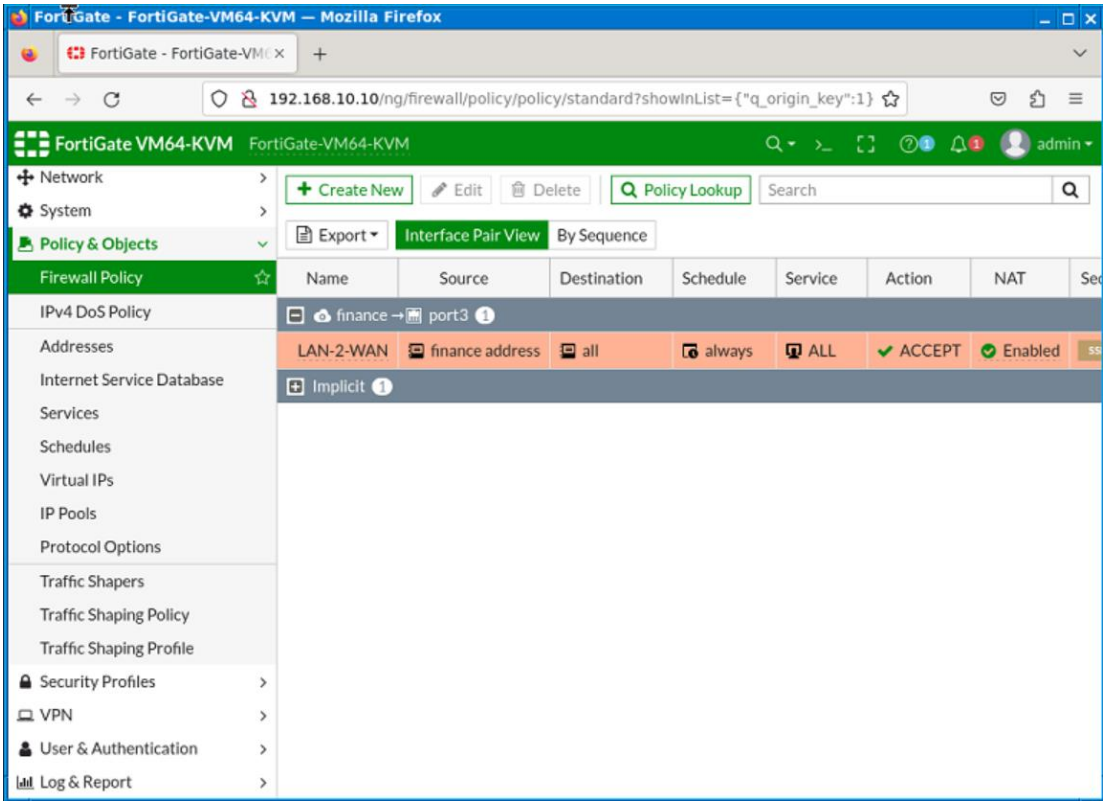


Figure 16 LAN To WAN Policy

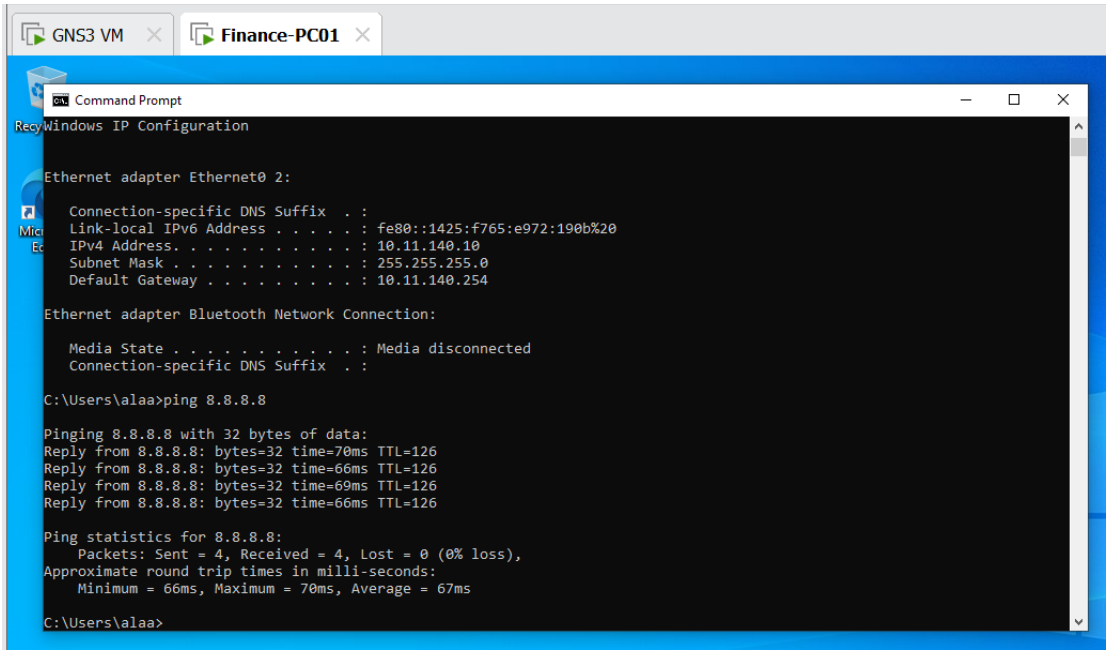


Figure 17 Finance PC02 (IP Configuration)

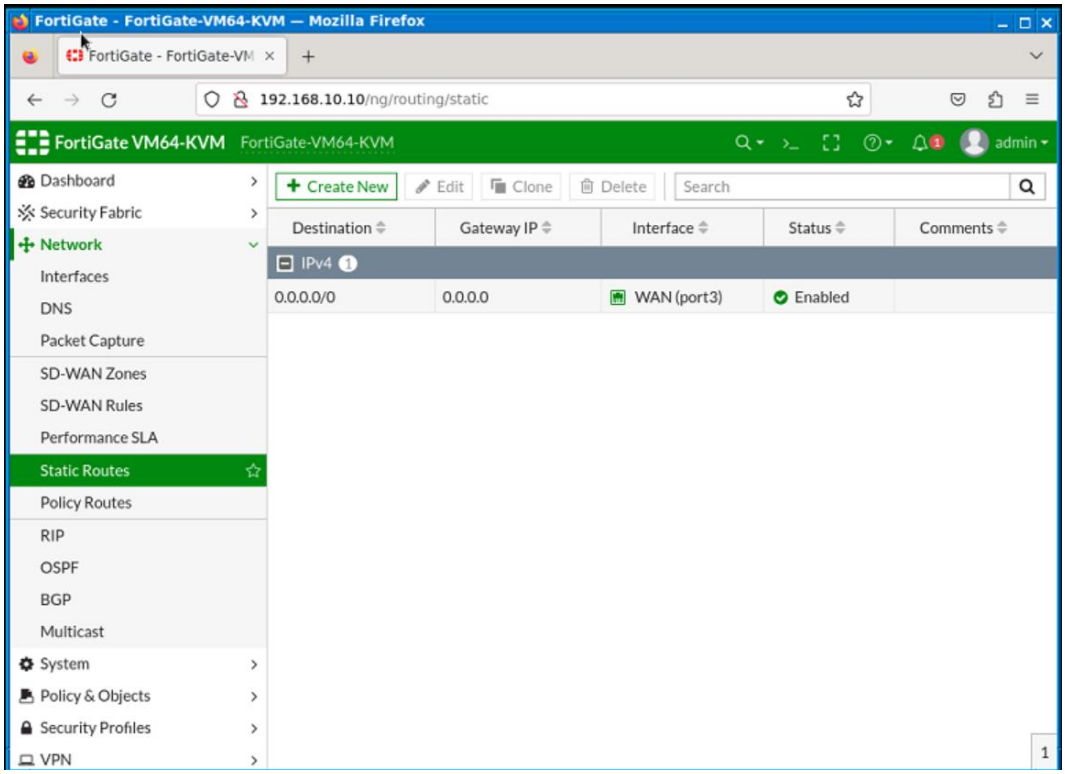


Figure 18 Branch Static Route

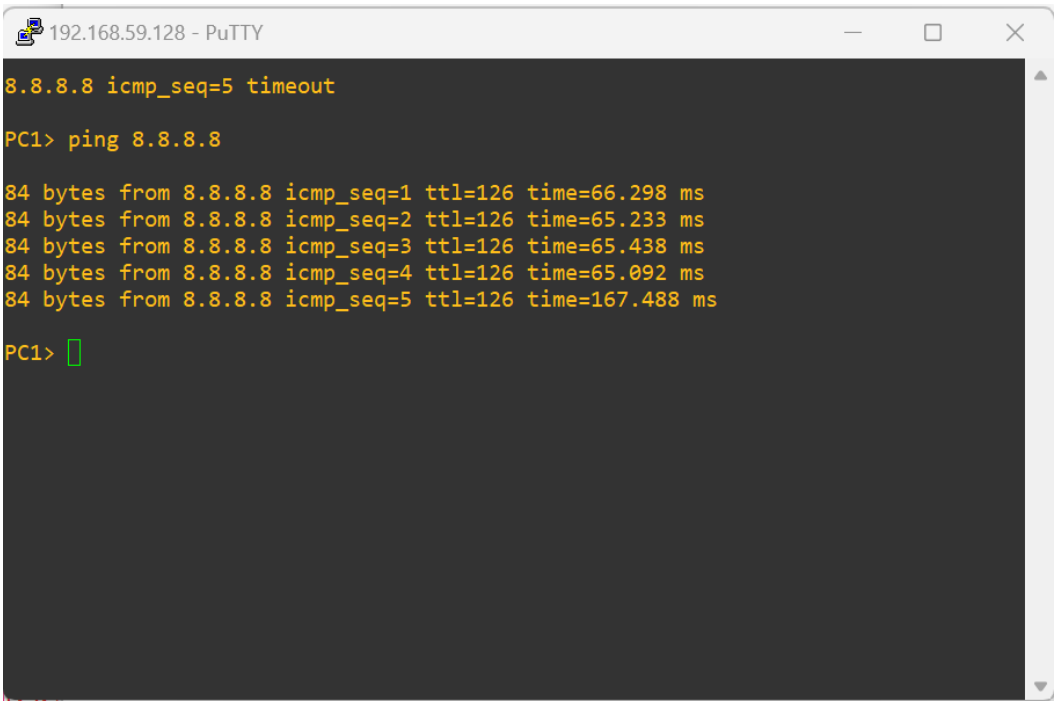


Figure 19 Testing Internet

Security, Permissions and Operational Requirements:

Configure Security policies.

Security Profile	App/Web	Action	VLAN	Time
Web Filter	facebook	Warning	Sales, Marketing	All Time
Web Filter	youtube	Limit	Marketing	All Time
Web Filter	hacking	Allow 3 Website	IT	08:00 - 09:00 All day
Web Filter	phishing	Warning 3 Website	IT	15:00-16:00 Saturday
Web Filter	Word "destroy"	Block	Sales, Marketing	All day
App Control	Azureus	Allow	marketing	1/4/2024-1/7/2024
App Control	Winmx	Allow	IT	All day
App Control	WorldOfTanks	Allow	Sales, Marketing	All day
App Control	https	Enable	Sales, Marketing, IT	All day
Antivirus	ftp	Enable	Sales, Marketing, IT	Saturday, Sunday
Intrusion Prevention	Sev 3 Sev 5	block	Sales, Marketing, IT	All Day

1. Antivirus, ftp allows

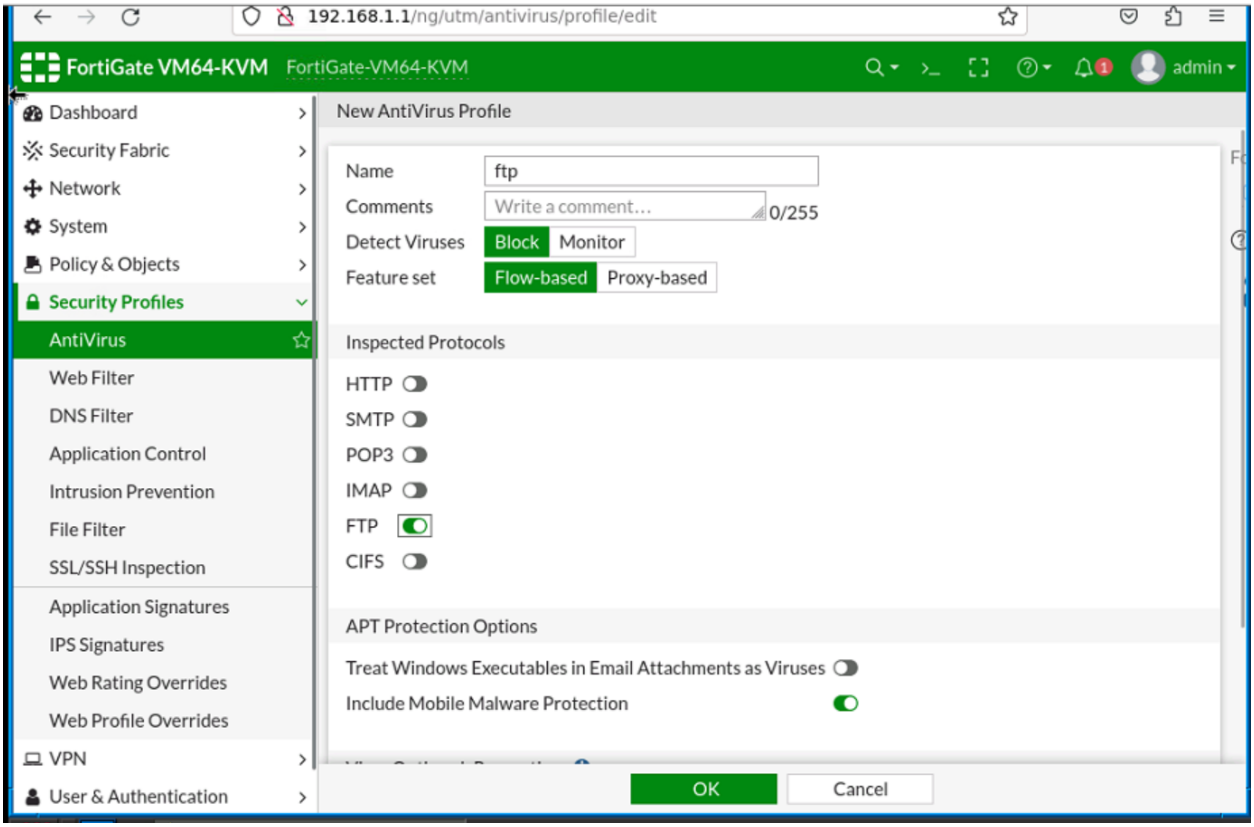


Figure 20 Antivirus Enable FTP

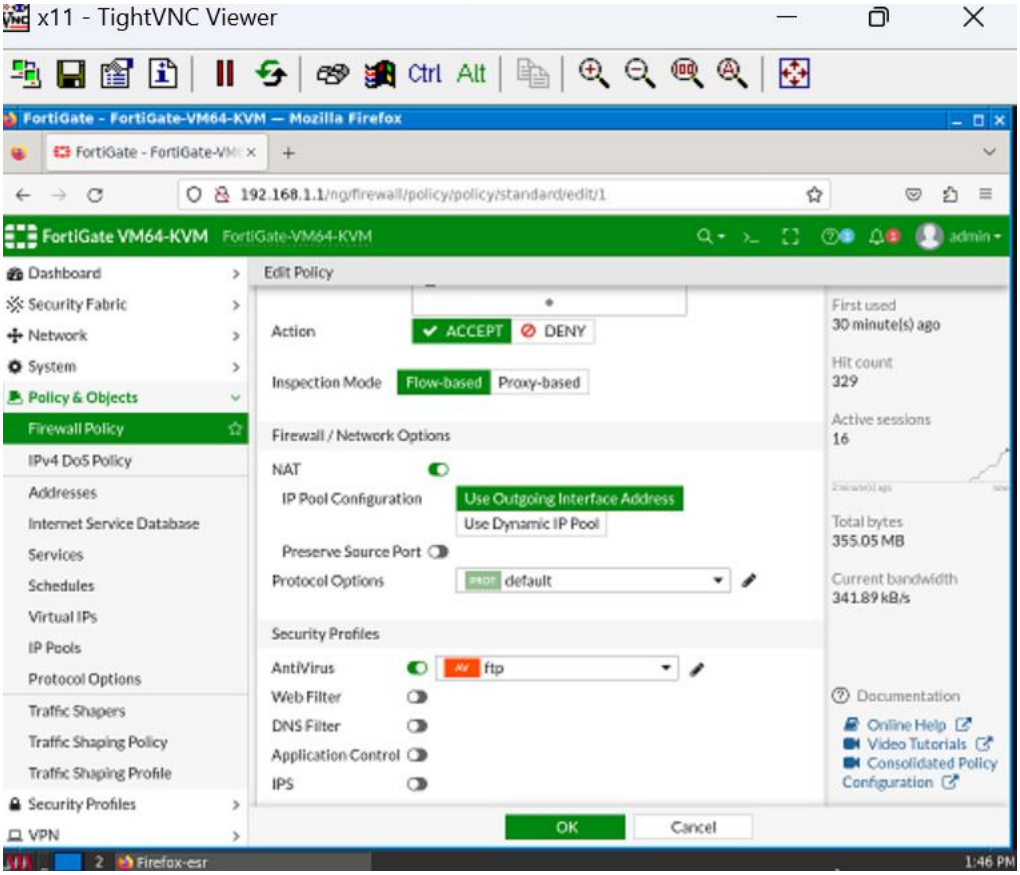
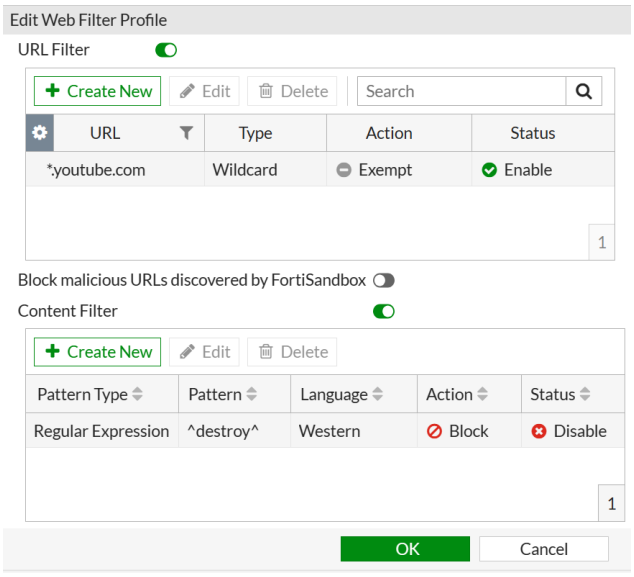


Figure 21 Link Antivirus to Firewall Policy

Marketing Firewall Policy

Web Filter profile (youtube) and block destroy as in the picture



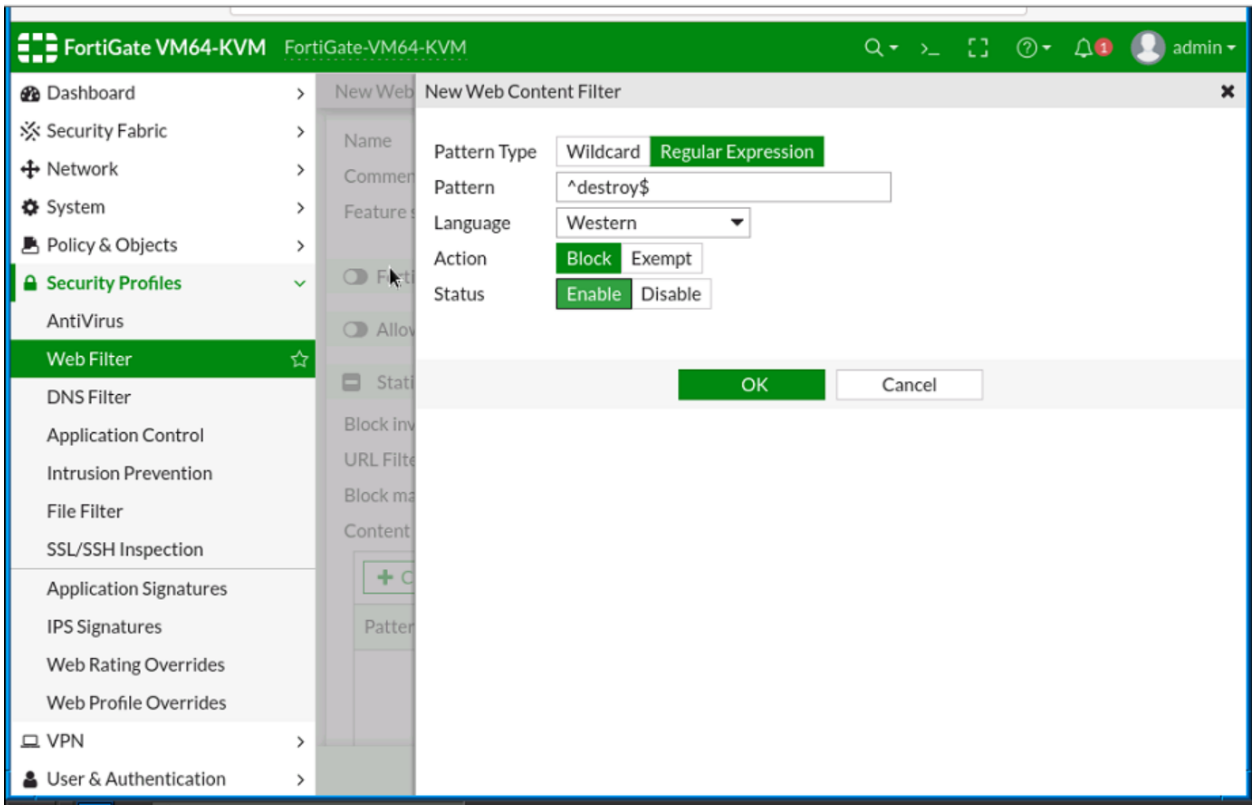
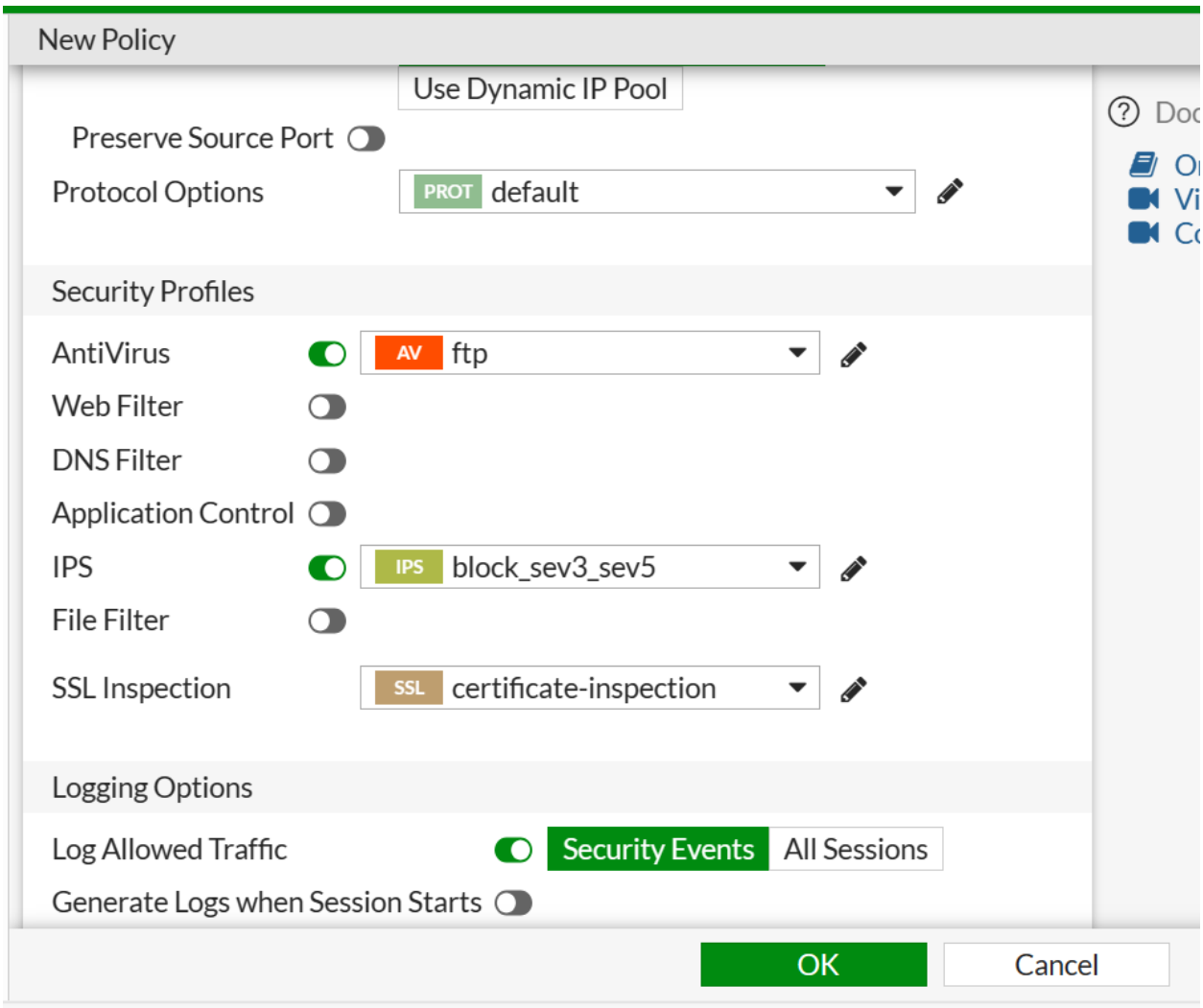
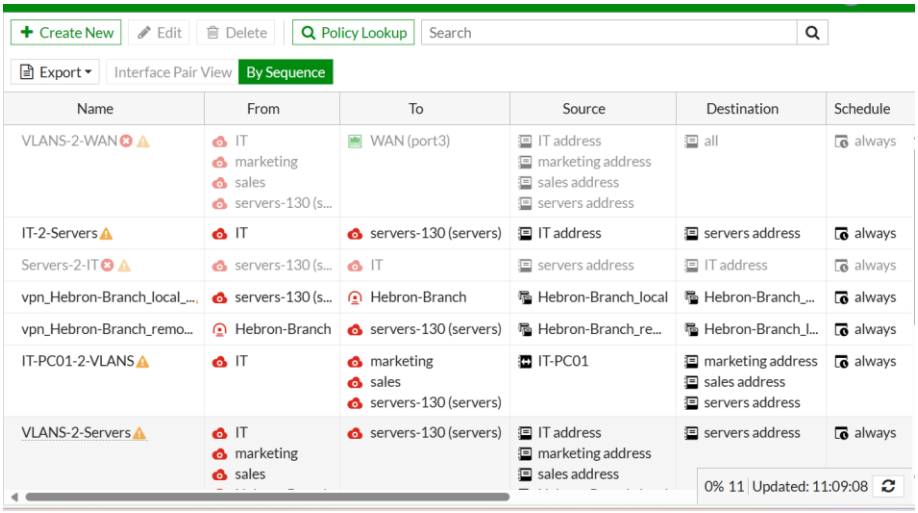


Figure 22 Web Filter destroy word block

Marketing_Sales_IT Policy



Policies Summary



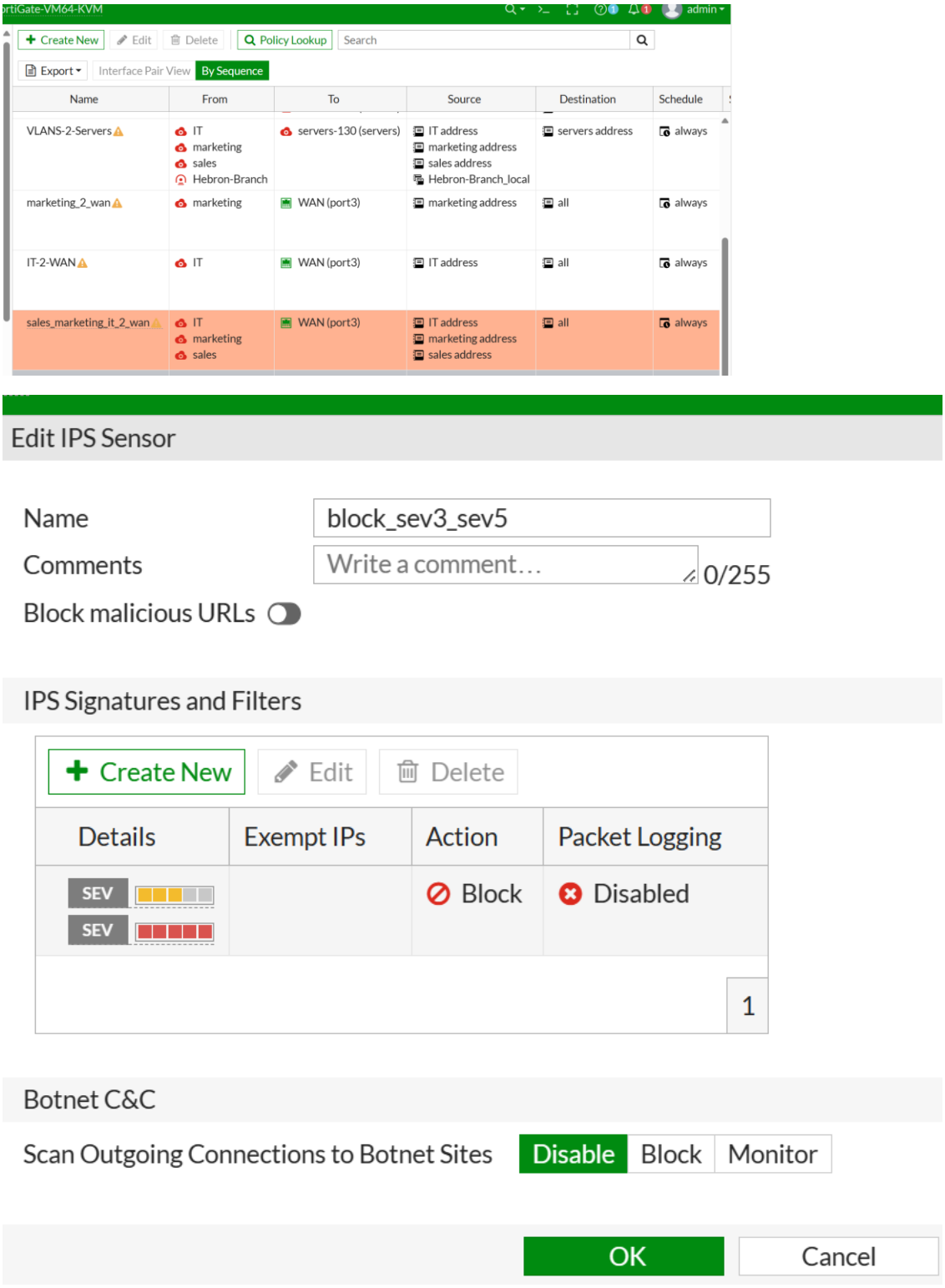


Figure 23 Block SEV3 and SEV5

App Control, Azureus, Allow (marketing firewall policy)

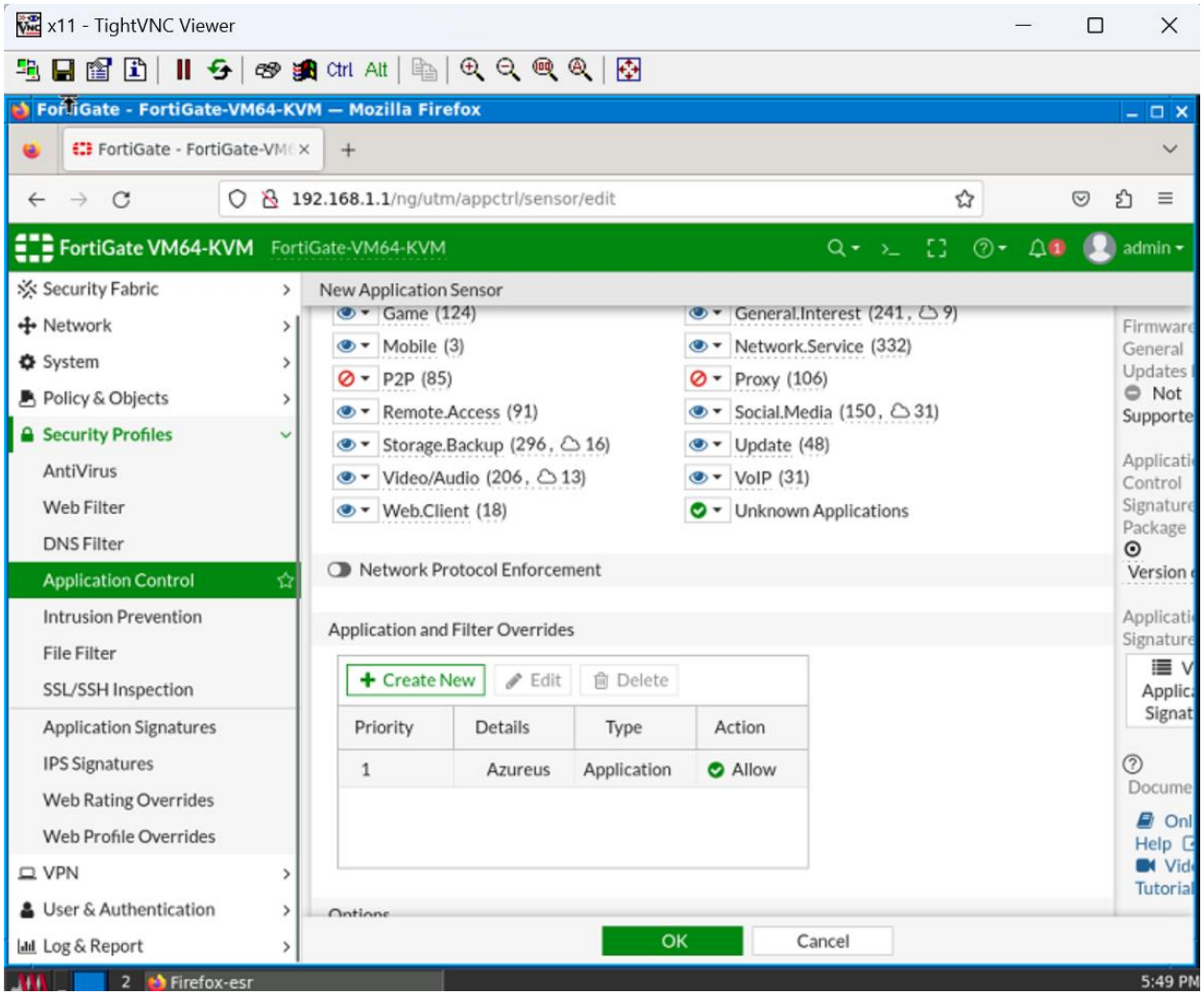


Figure 24 App Control, Azureus, Allow

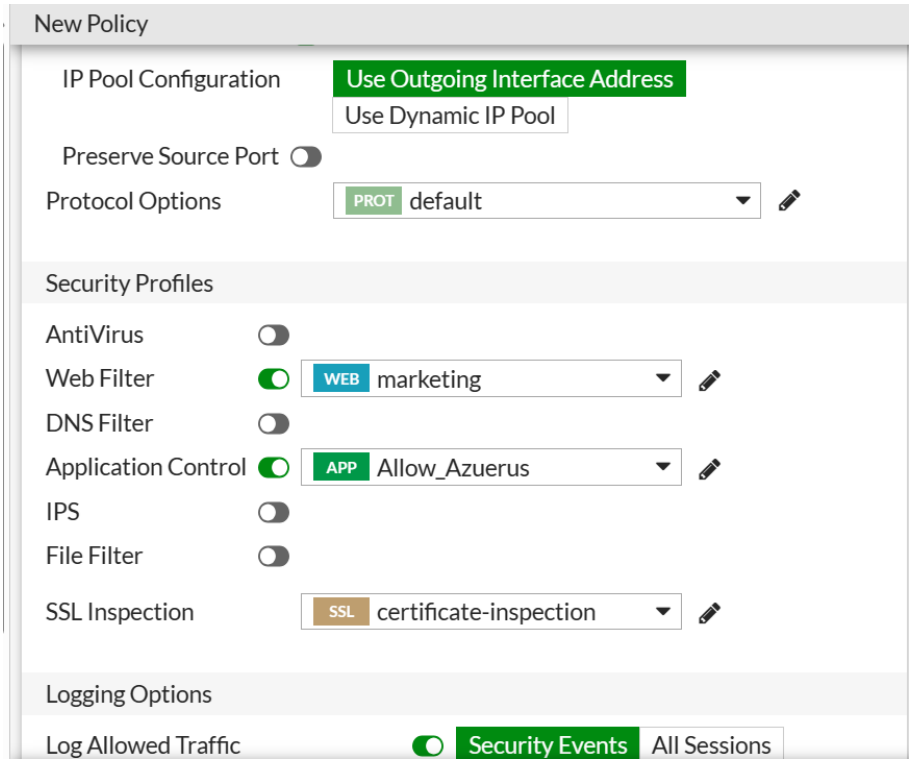


Figure 25 Marketing Policy

App control, Allow Winmx

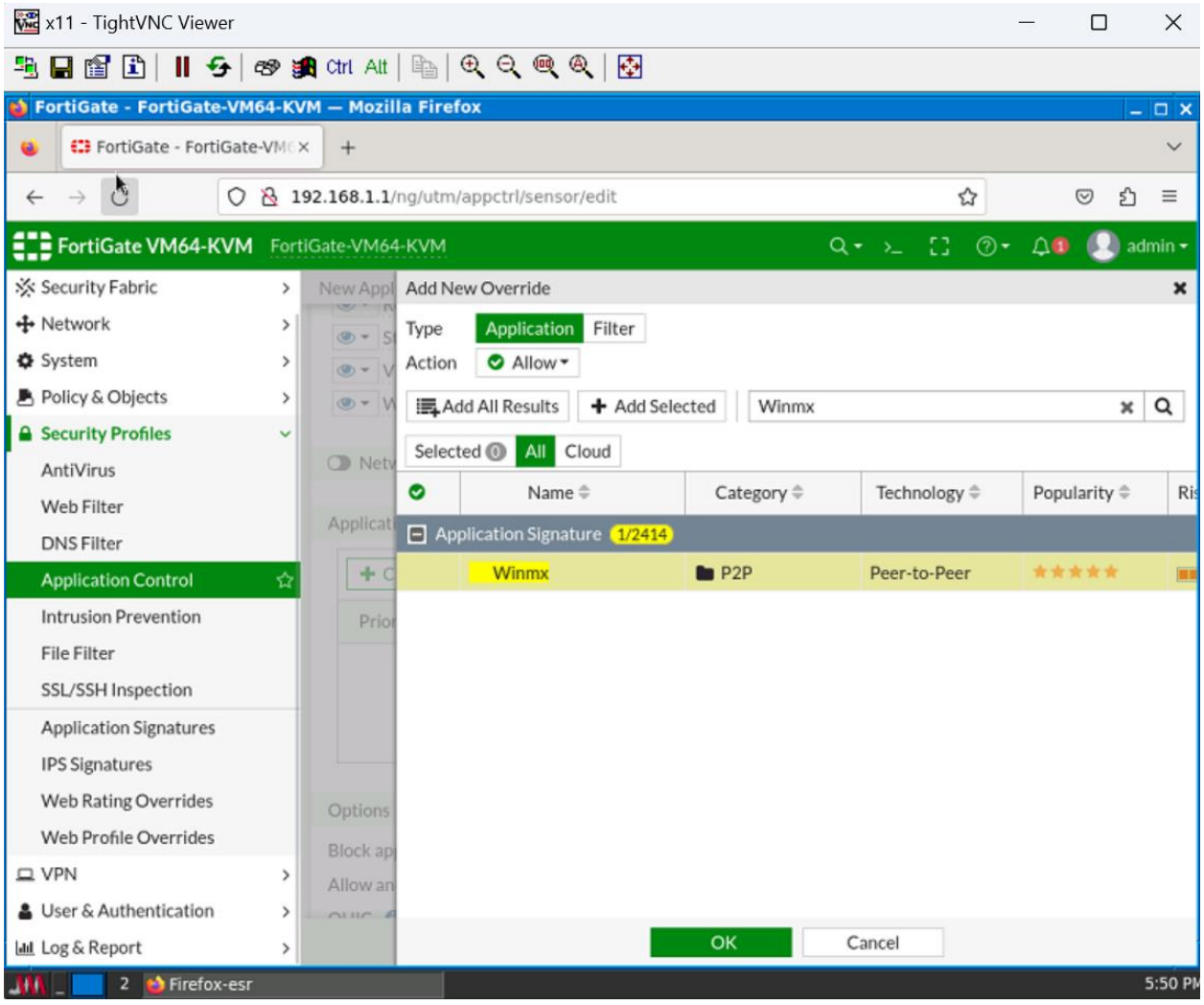


Figure 26 App control, Allow Winmx

App Control, WorldOfTanks, Allow

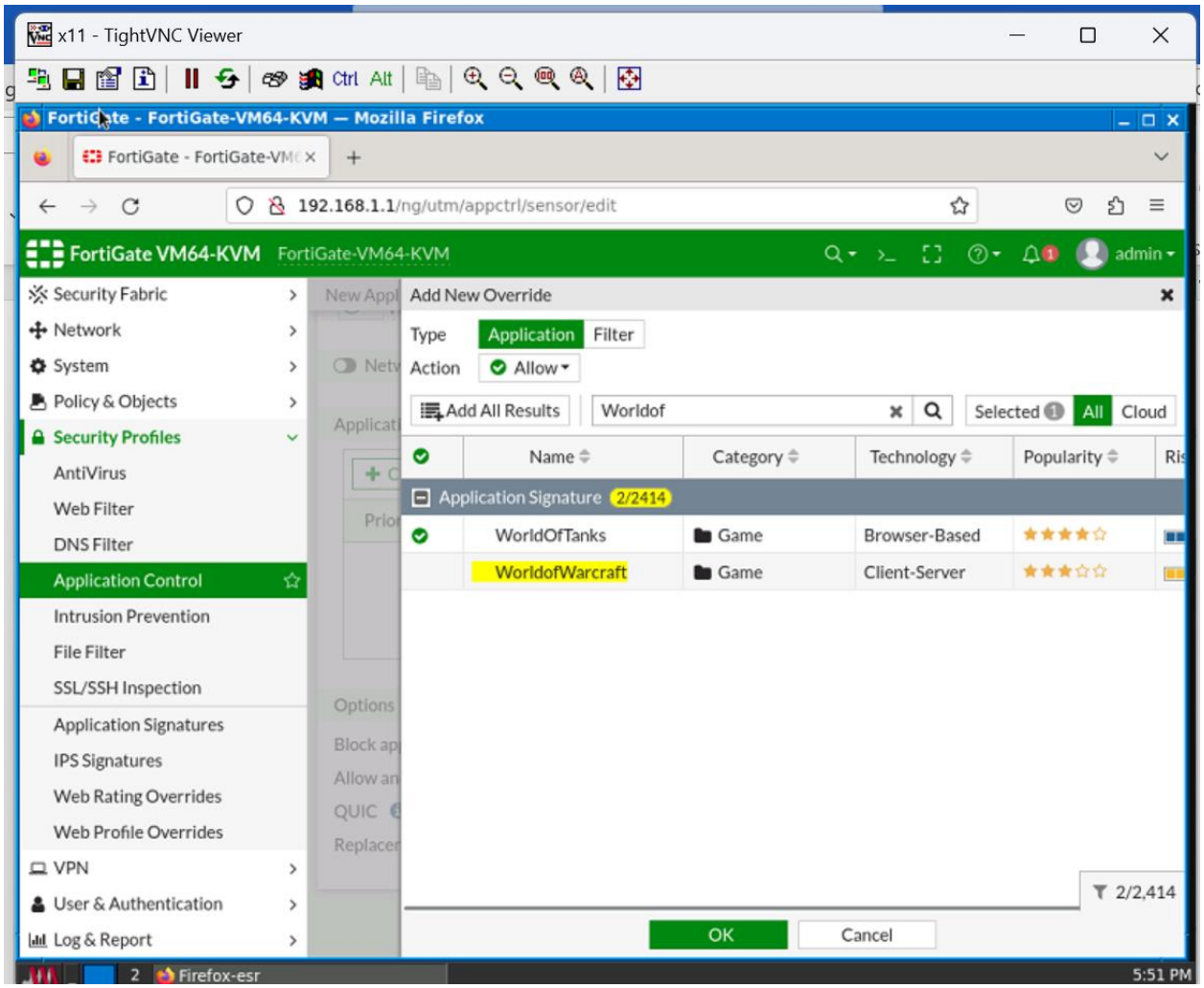


Figure 27 App Control, WorldOfTanks, Allow

App Control, https, Enable

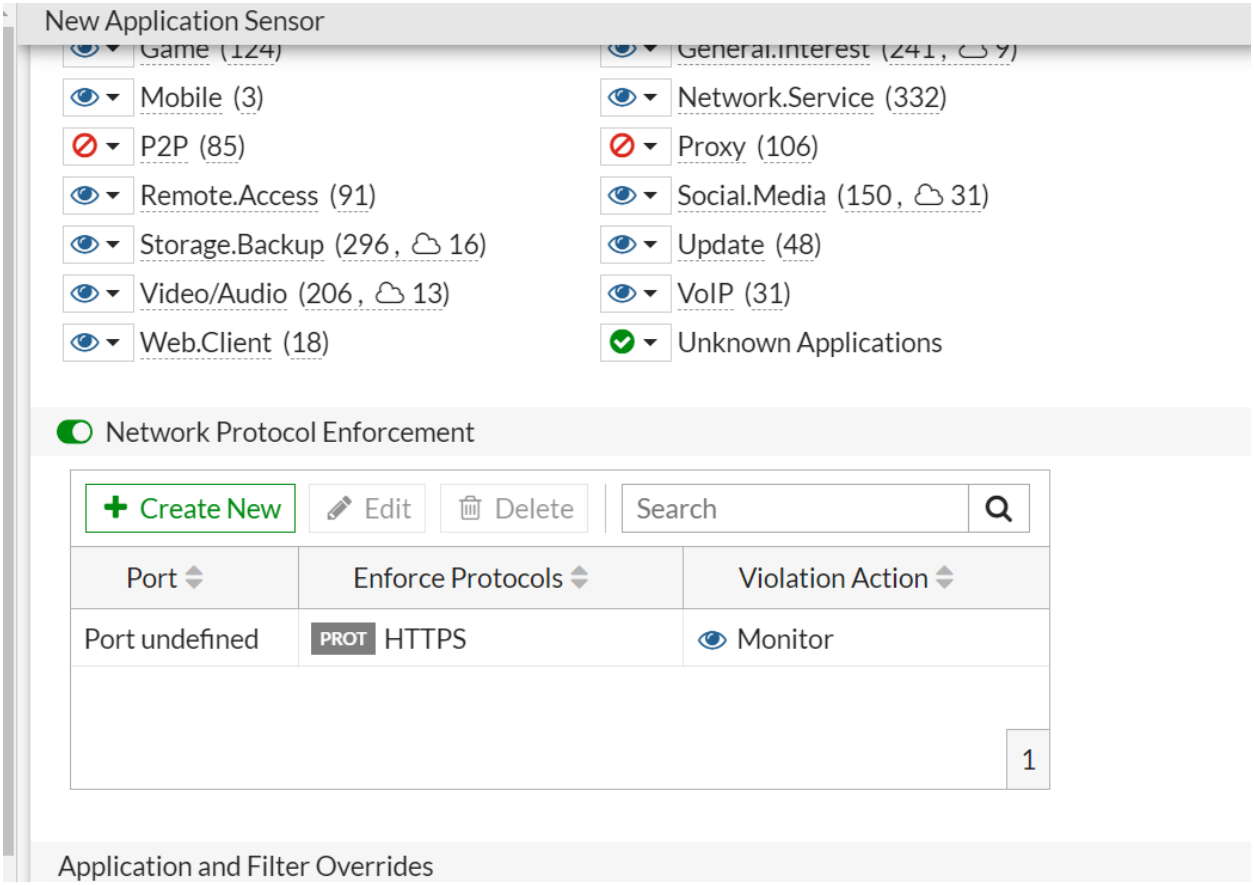


Figure 28 App Control, https, Enable

The above profiles are connected to the Marketing_sales_it firewall policy

IT-2-WAN Policy

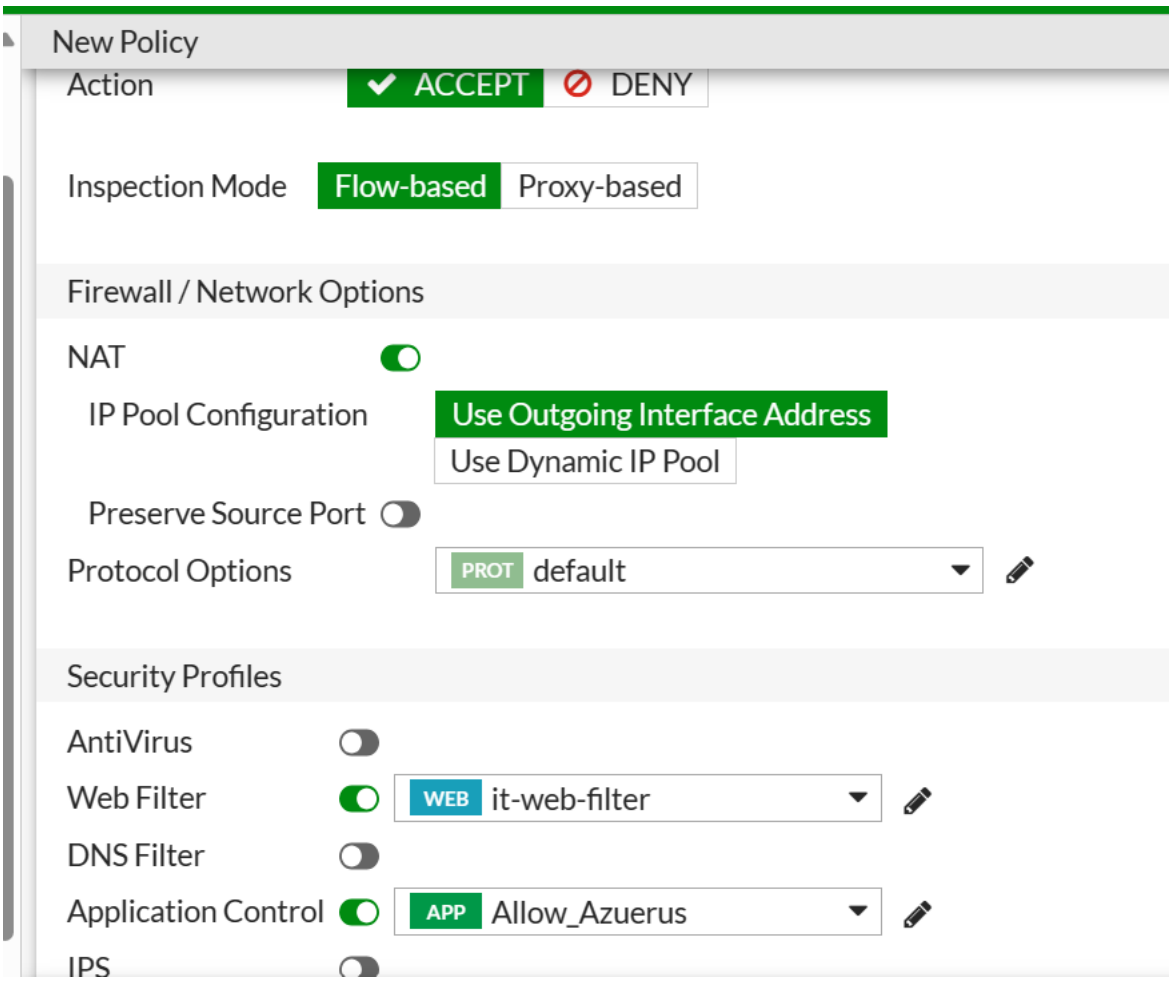


Figure 29 it-2-wan

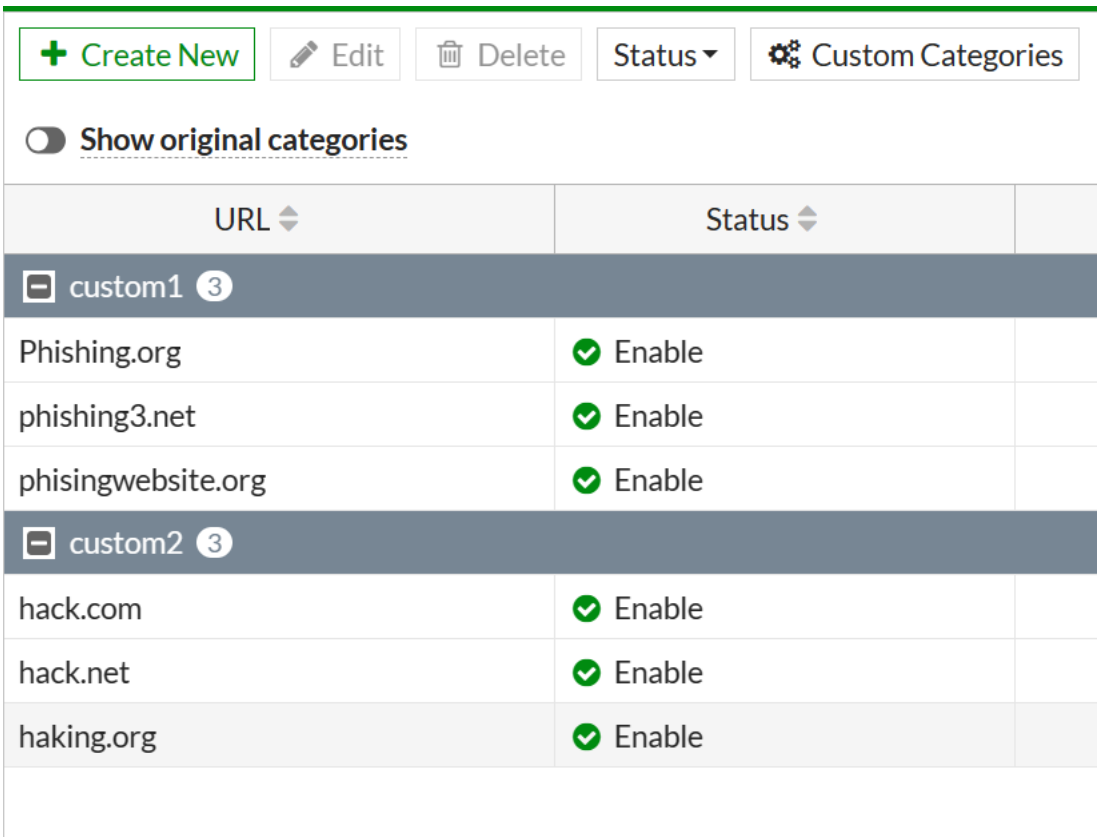
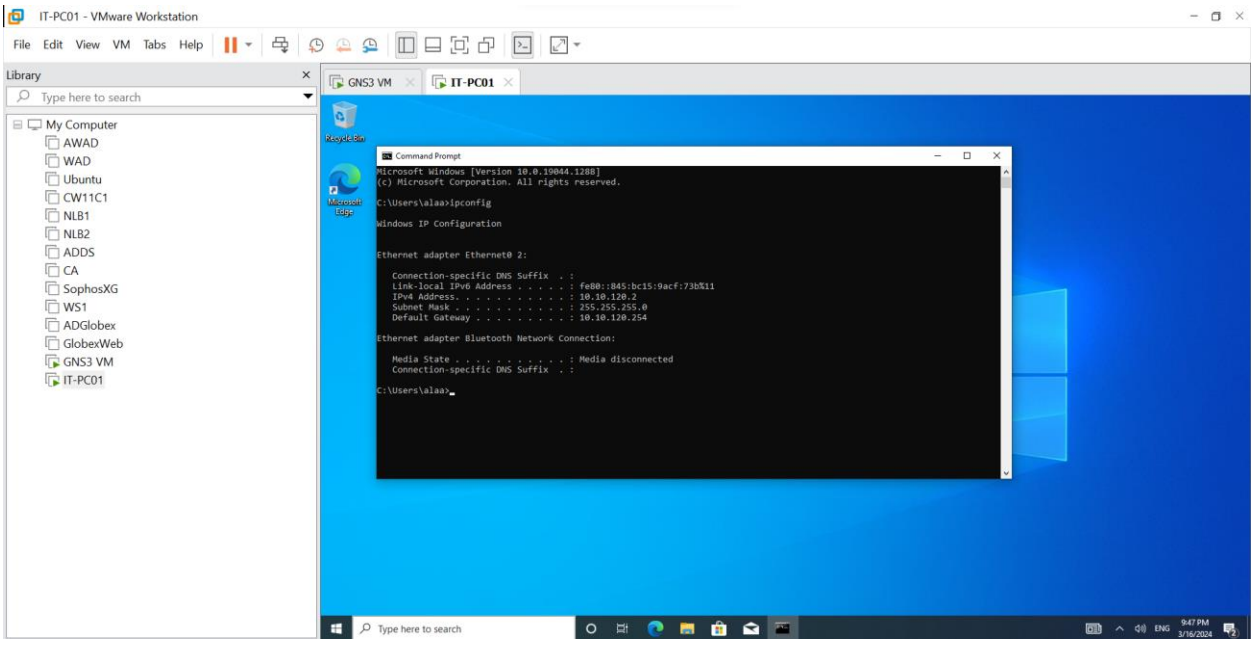


Figure 30 it_web_profile

IT-PC01 Configuration

The figure below shows that the PC takes an IP from DHCP, but after that using MAC binding in the firewall, I assign it a static IP mapped to its MAC address (10.10.120.10)



1) Setting Fixed IP with MAC Address ITPC01

IP Address Assignment Rules

+ Create New | Edit | Delete | Search

Add from DHCP Client List

Type	Match Criteria	Action	IP
MAC Address	MAC address: 00:0c:29:8c:a9:d2	Reserve IP	10.10.120.10
Implicit	Unknown MAC Addresses	Assign IP	

Figure 31 Setting Fixed IP with MAC Address ITPC01

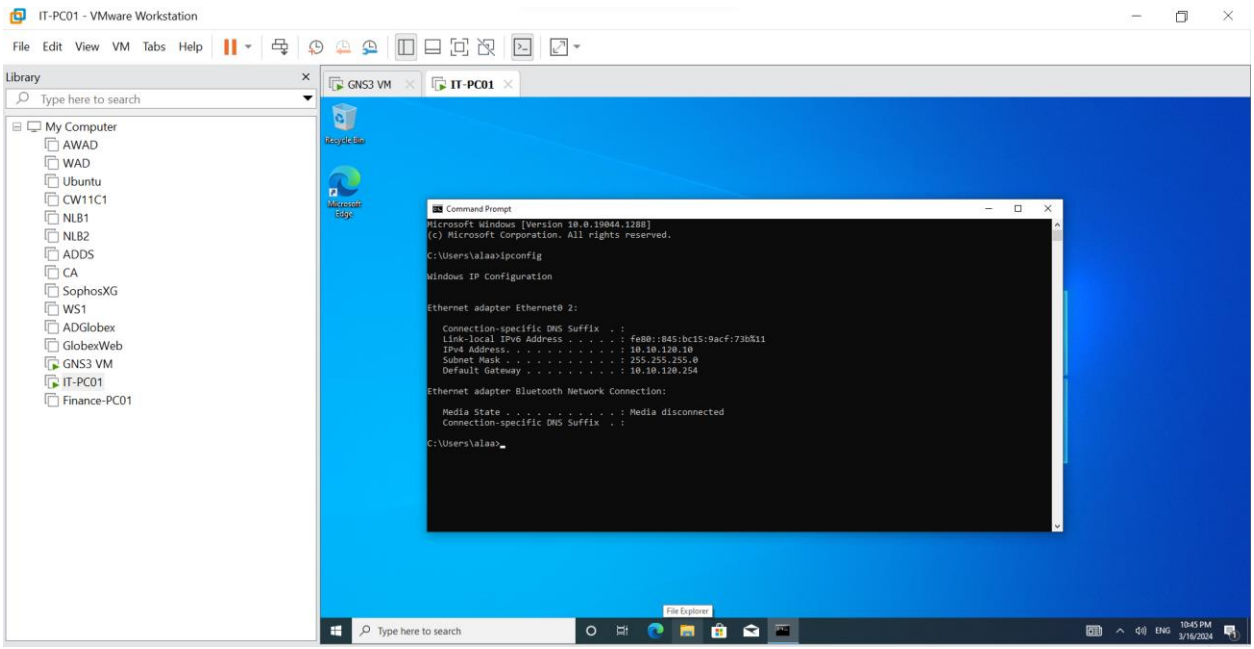


Figure 32 IP Config After MAC Binding

Finance-PC01

2) Bind Finance PC01 wit IP 10.10.140.10

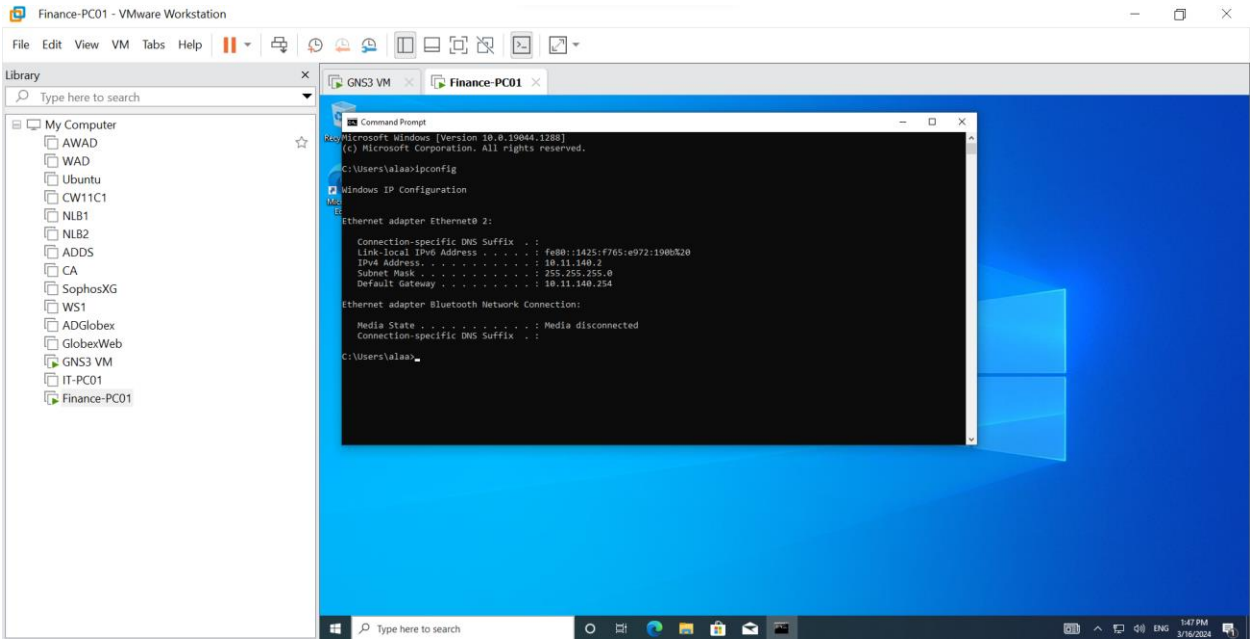


Figure 33 Finance PC After Binding IP

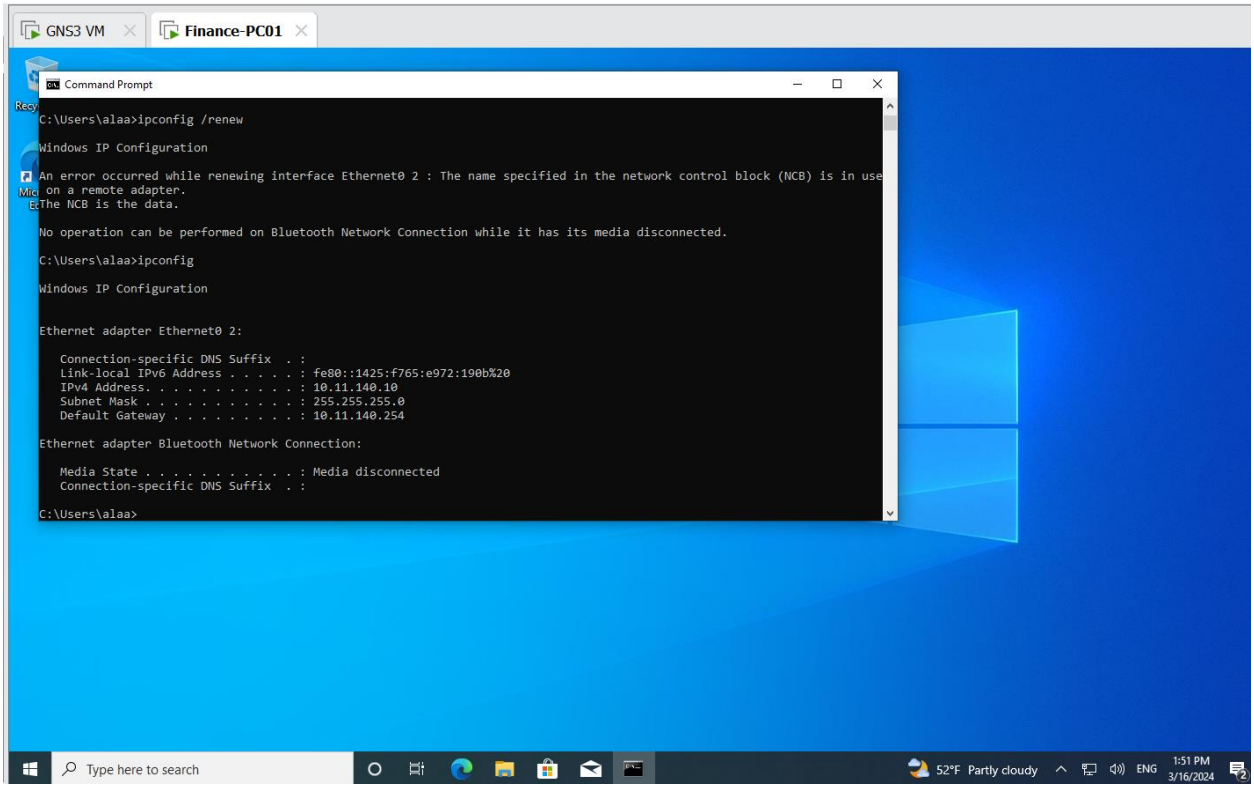
IP Address Assignment Rules

+ Create New | Edit | Delete | Search

Add from DHCP Client List

Type	Match Criteria	Action	IP
MAC Address	MAC address: 00:0C:29:28:4E:09	Reserve IP	10.11.140.10
Implicit	Unknown MAC Addresses	Assign IP	

Figure 34 Binding MAC with IP (Firewall)


GNS3 VM
Finance-PC01
Command Prompt
C:\Users\alaa>ipconfig /renew
Windows IP Configuration
An error occurred while renewing interface Ethernet0 2 : The name specified in the network control block (NCB) is in use on a remote adapter.
The NCB is the data.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.
C:\Users\alaa>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::1425:f765:e972:190b%20
IPv4 Address. . . . . : 10.11.140.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.11.140.254
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\alaa>
Type here to search
52°F Partly cloudy
ENG
1:51 PM
3/16/2024

Read only admin (Head Firewall).

This is done using two steps:

- Add Admin Profile with read only permissions called read_only
- Add a new user called Ali and assign the profile to him.

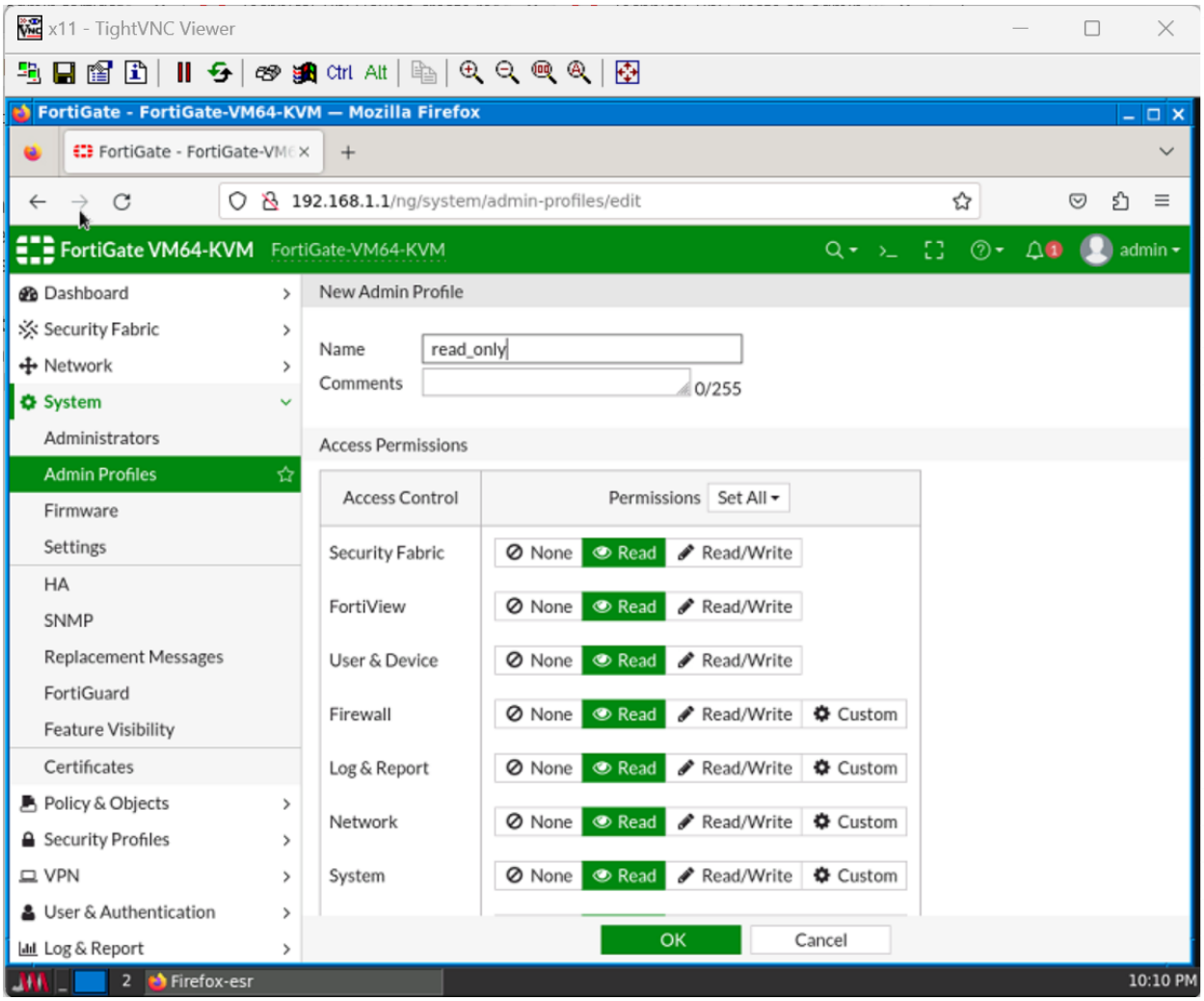


Figure 35 Add New Admin Profile

Step2: Assign the read only profile to the user ali, by creating a new user form system/administrators/create new user.

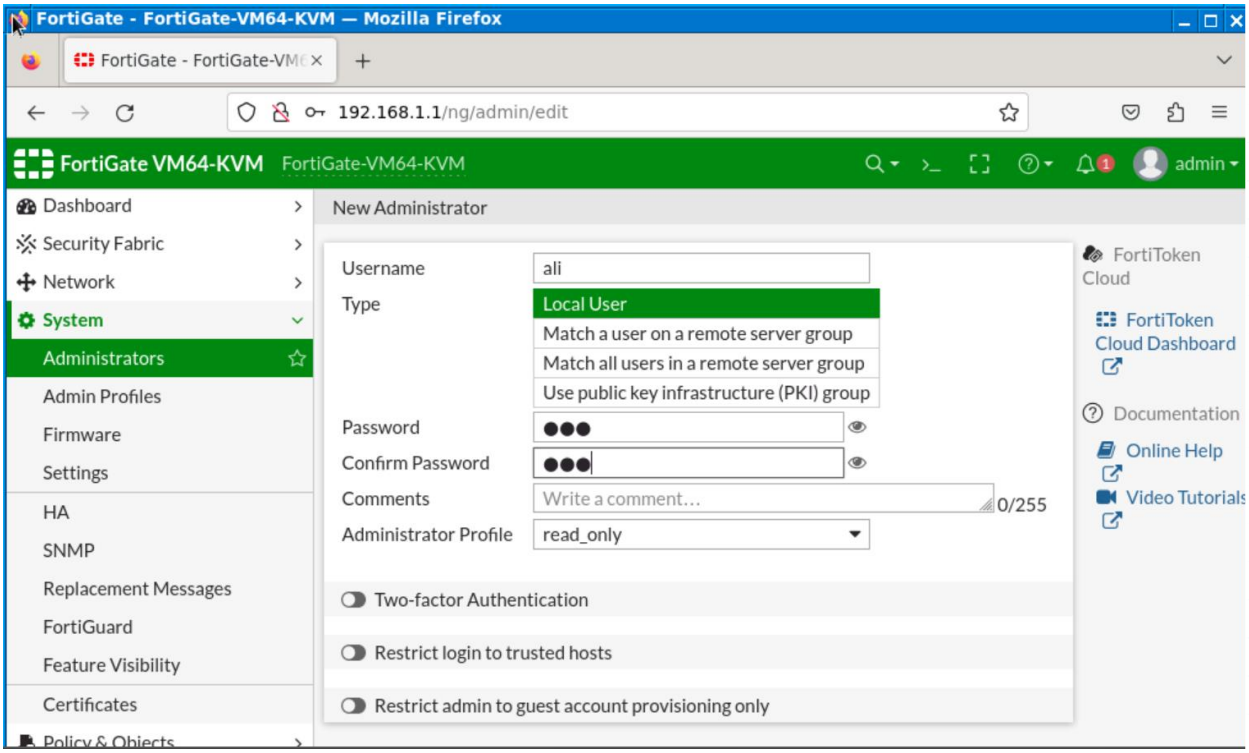


Figure 36 Ali User

Servers VLAN

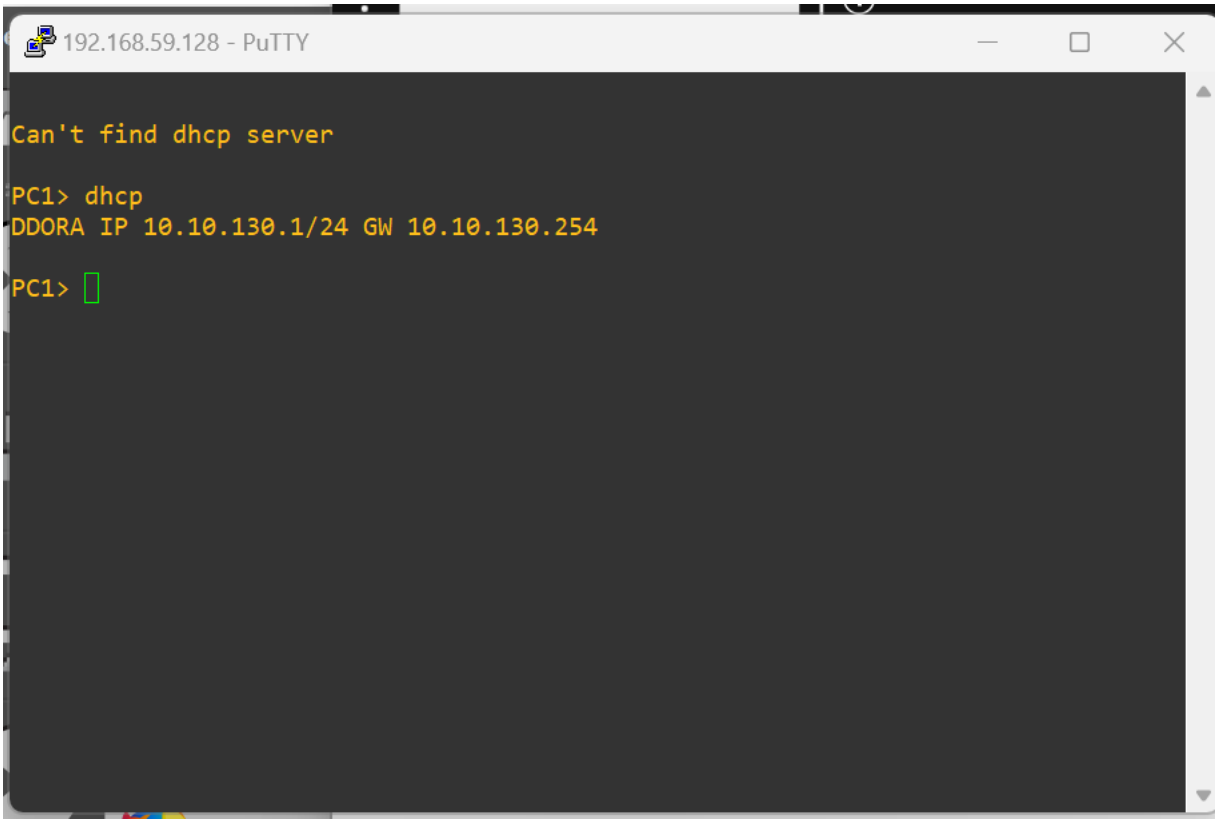


Figure 37 Servers VLANS DHCP

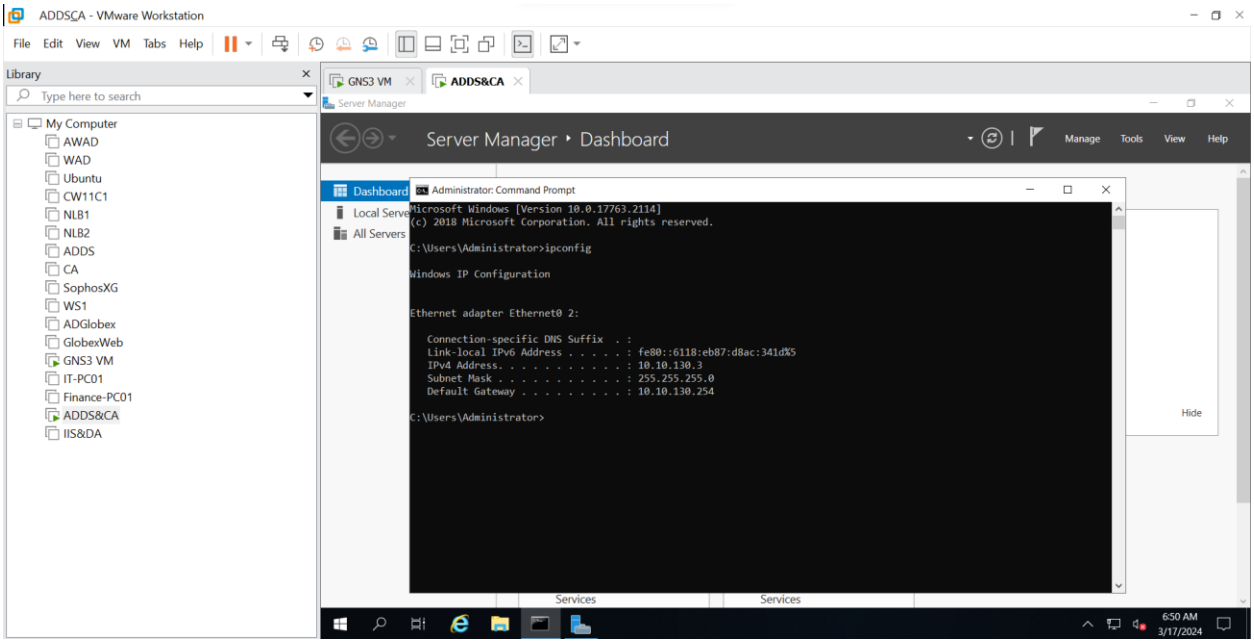


Figure 38 ADDS IP Settings

IPSEC Site to Site VPN

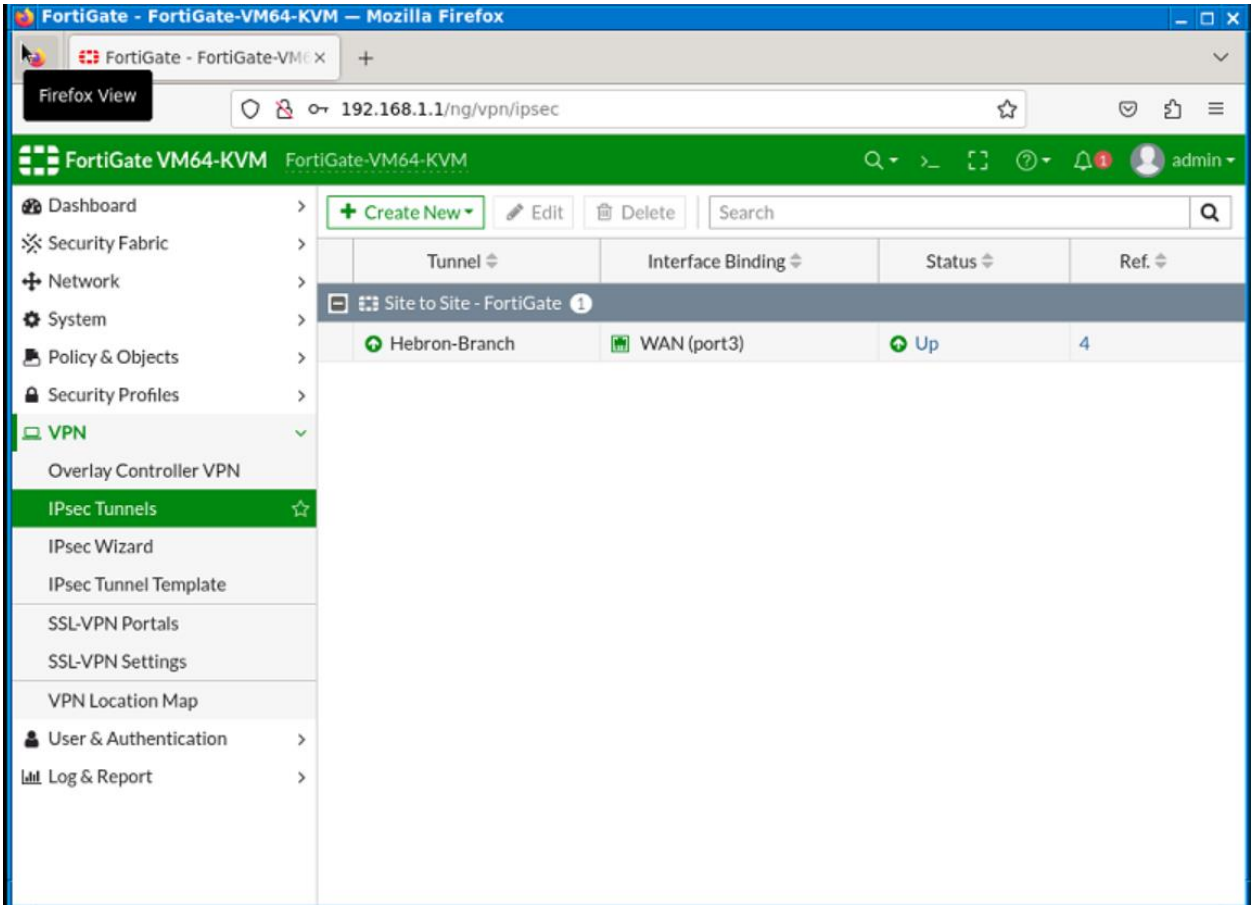


Figure 39 Site to Site VPN (Head Firewall)

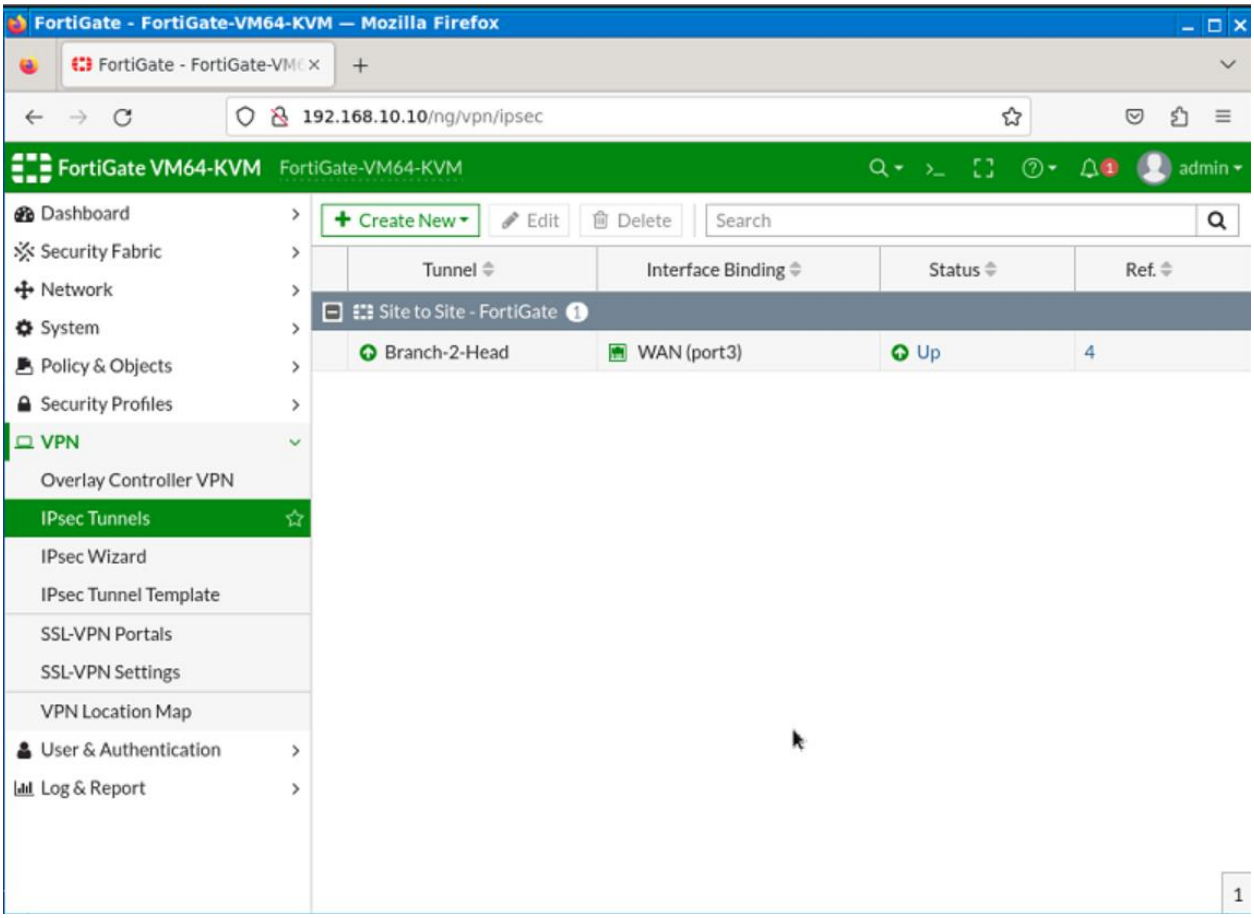


Figure 40 Site to Site VPN Branch Firewall

3) IPC01 and Finance PC02 join to the Domain.

The finance PC joins the domain successfully, However the ITPC01 can ping the ADDS globex.it and when trying to join domain it could not authenticate username and password, this may be because of a limitation in the Virtual machine resources. A policy from VLAN to servers is added so can the VLANS to access ADDS and IIS.

VLANS-2-Servers	IT marketing sales Hebron-Branch	servers-130 (servers)	IT address marketing address sales address Hebron-Branch_local	servers address	always

Figure 41 VLAN to Servers Policy

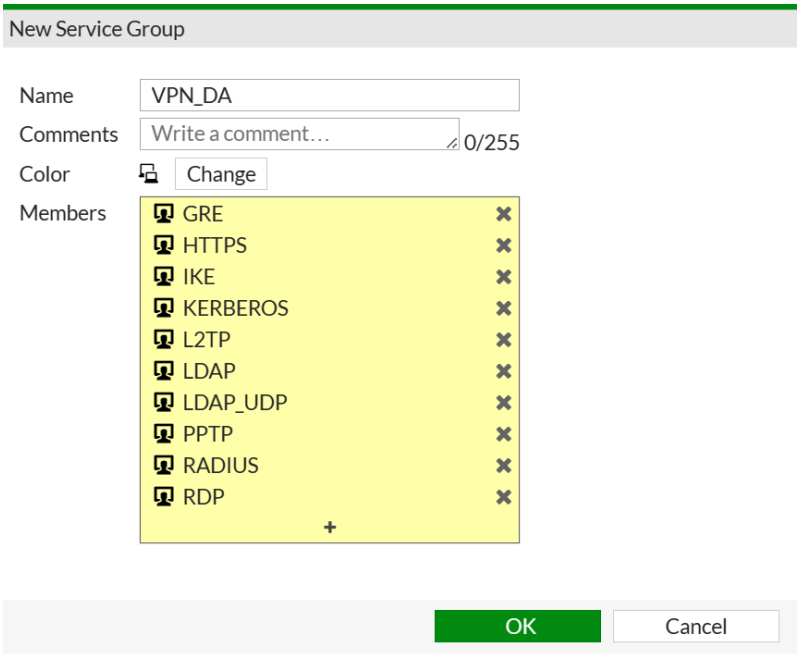


Figure 42 VLAN to SERVERS PORTS

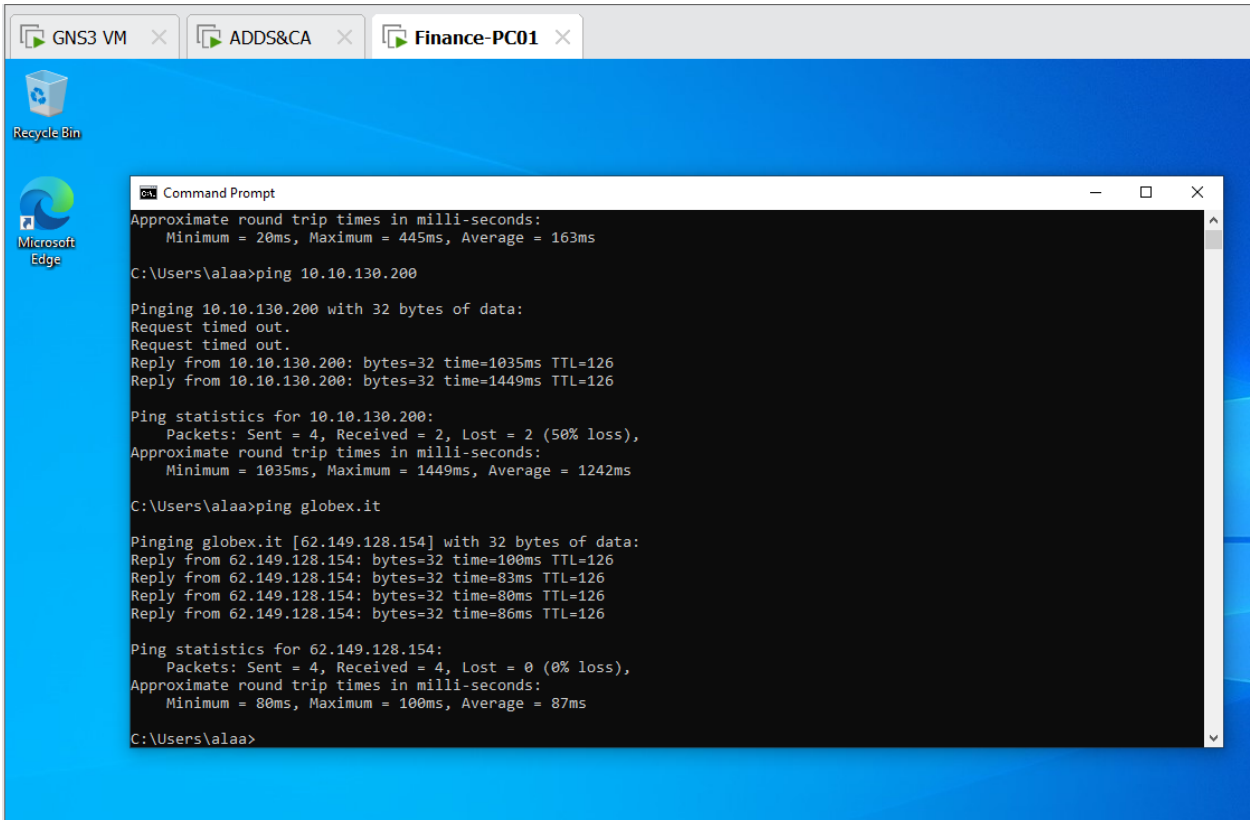


Figure 43 Ping globex.it

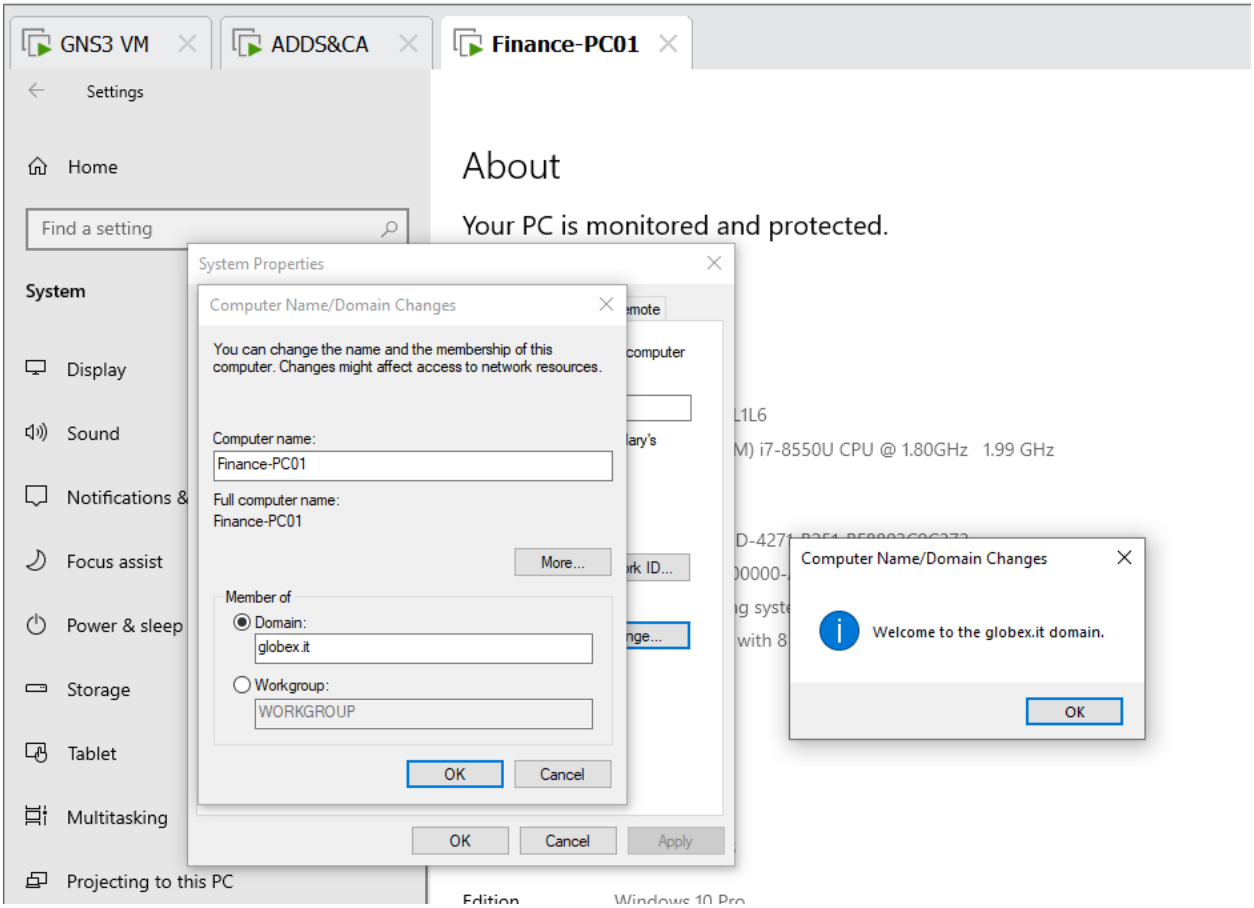


Figure 44 Successful Join of Finance PC02

ADDS – Users and groups.

Organizational Units

OU	Description
Servers	Organizational units for serves
marketing	Organizational units for marketing department users
sales	Organizational units for sales department users
IT	Organizational units for IT department users
Finance	Organizational units for Finance department users
Allowed PCS	Organizational units for Allowed Computers
Denied PCS	Organizational units for denied Computers
Shared Folders	Organizational units for Shared Folders Security groups: • Marketing • Finance • IT • Sales • administration
Security Groups	Organizational units for the following Security groups (Direct Access): • DA-Clients

The picture shows the OUS created using the Active directory for each Department.

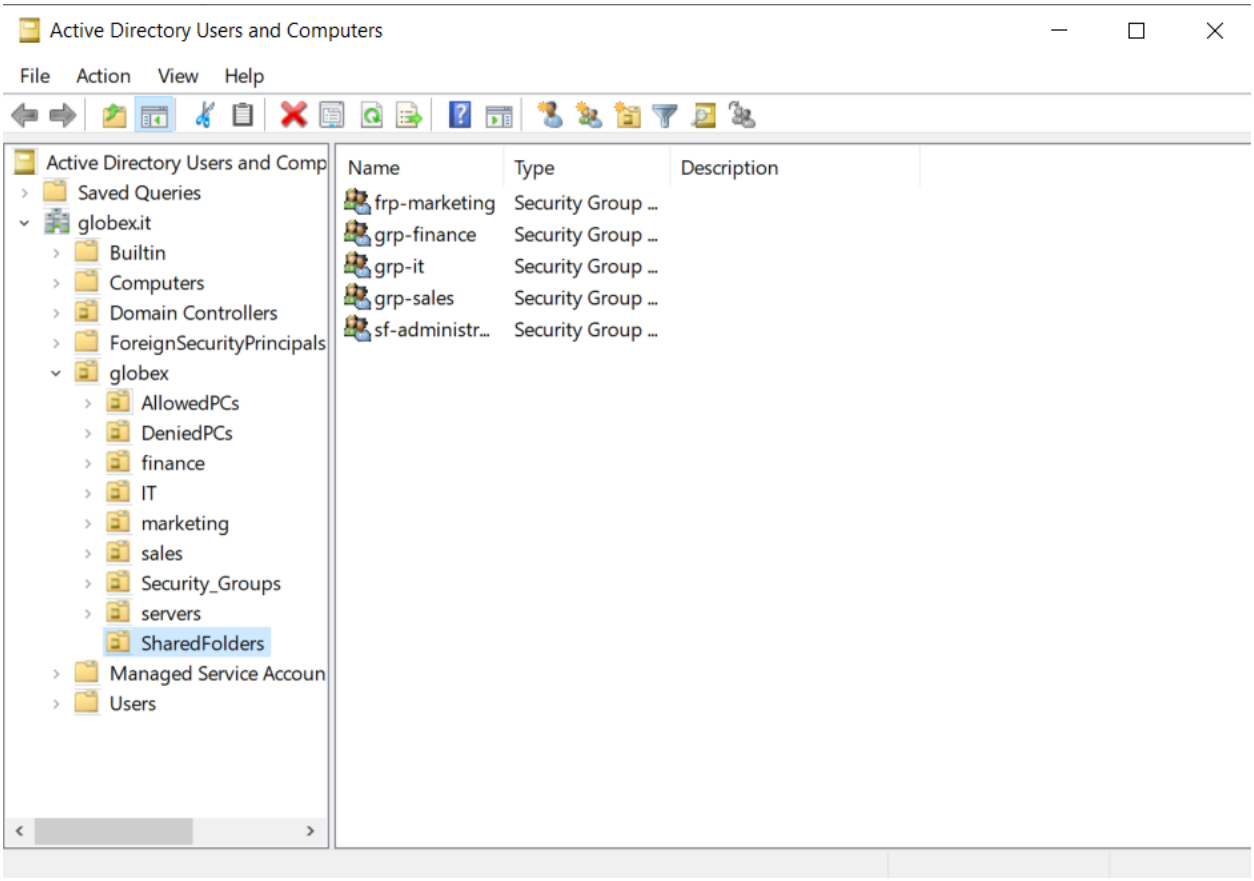
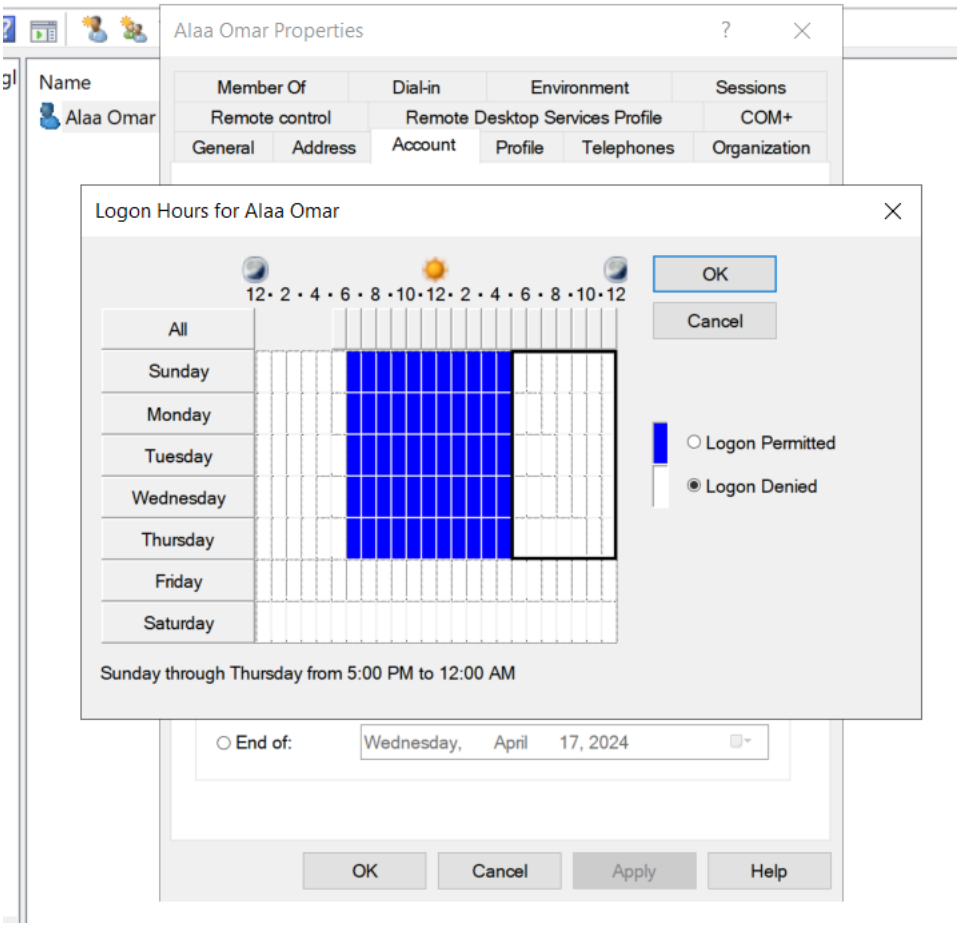


Figure 45 Active Directory OUs

Created Users:

User	Department
somar@globex.it	finance
aissa@glbex.it	IT
aomar@globex.it	marketing
lnairat@globex.it	sales

User Properties



Group Policy:

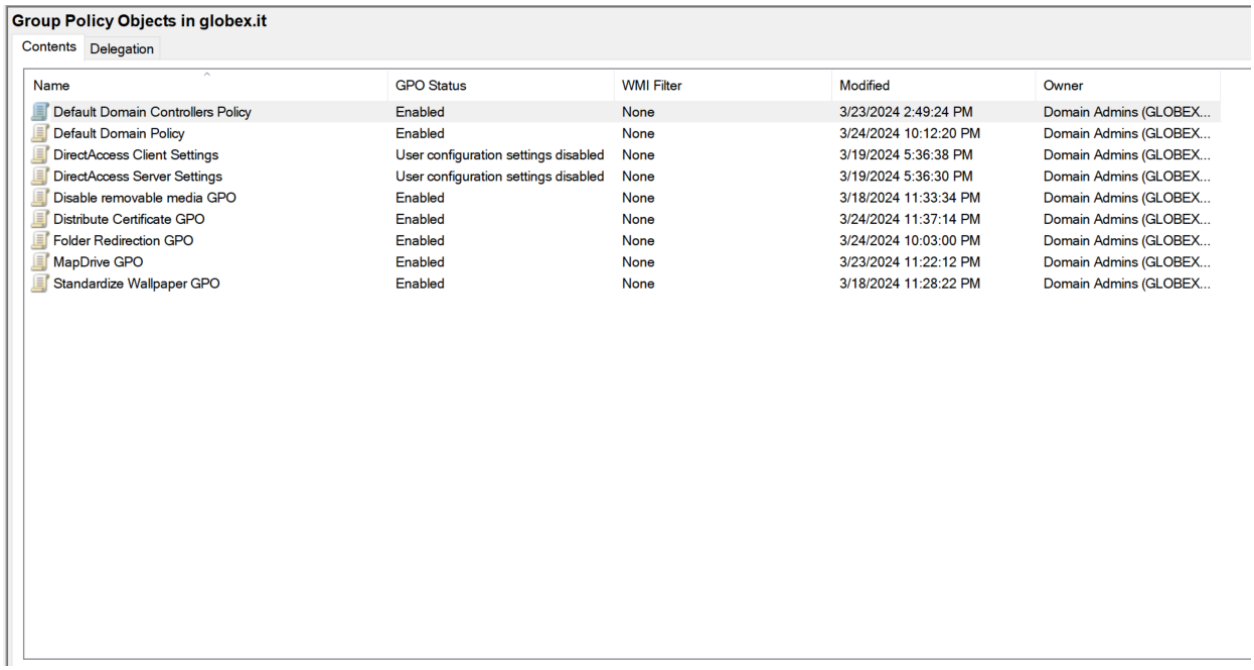
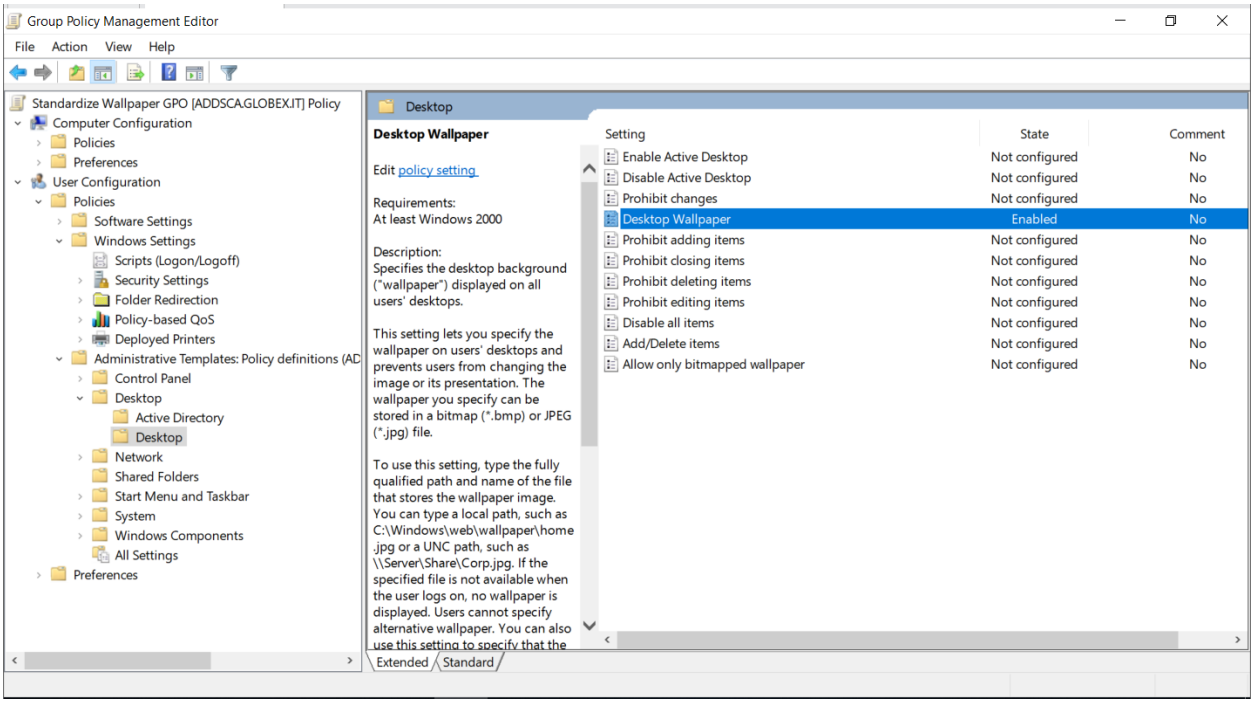
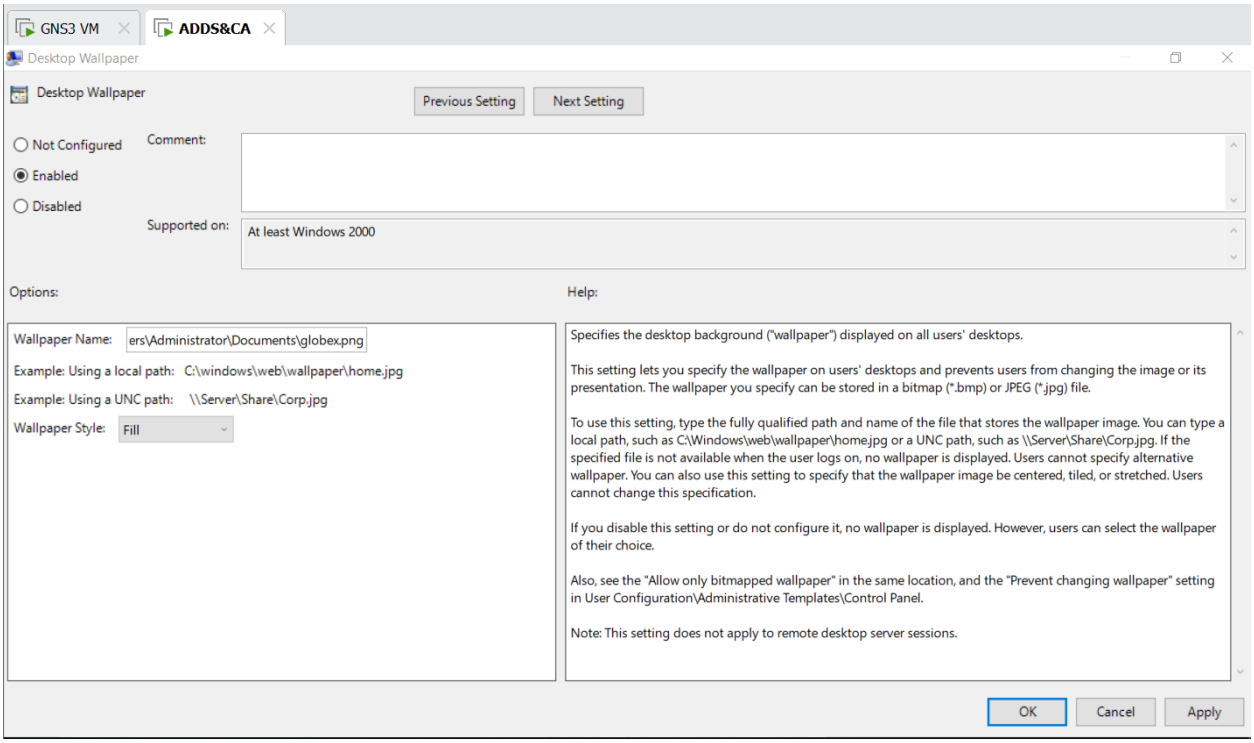


Figure 46 Group Policy Summary

Standardize Wallpaper

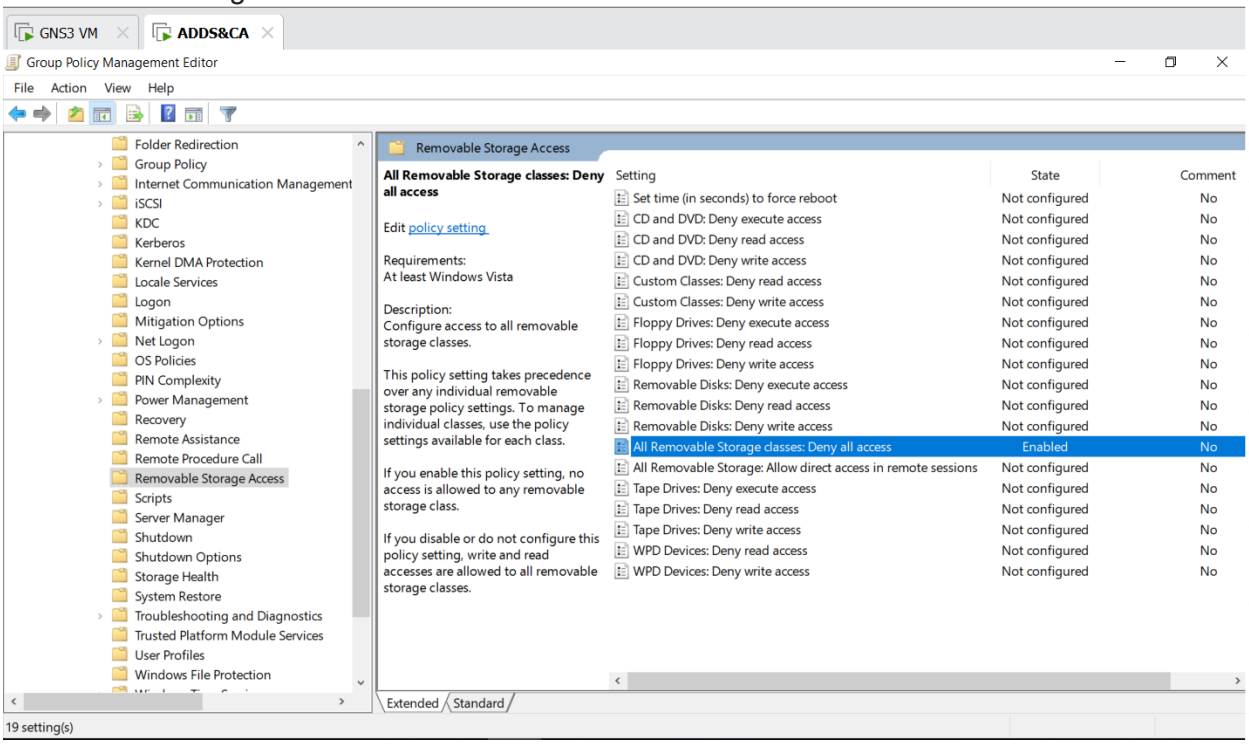
Path: In the Group Policy Management Editor, navigate to User Configuration > Policies > Administrative Templates > Desktop > Desktop > Desktop Wallpaper

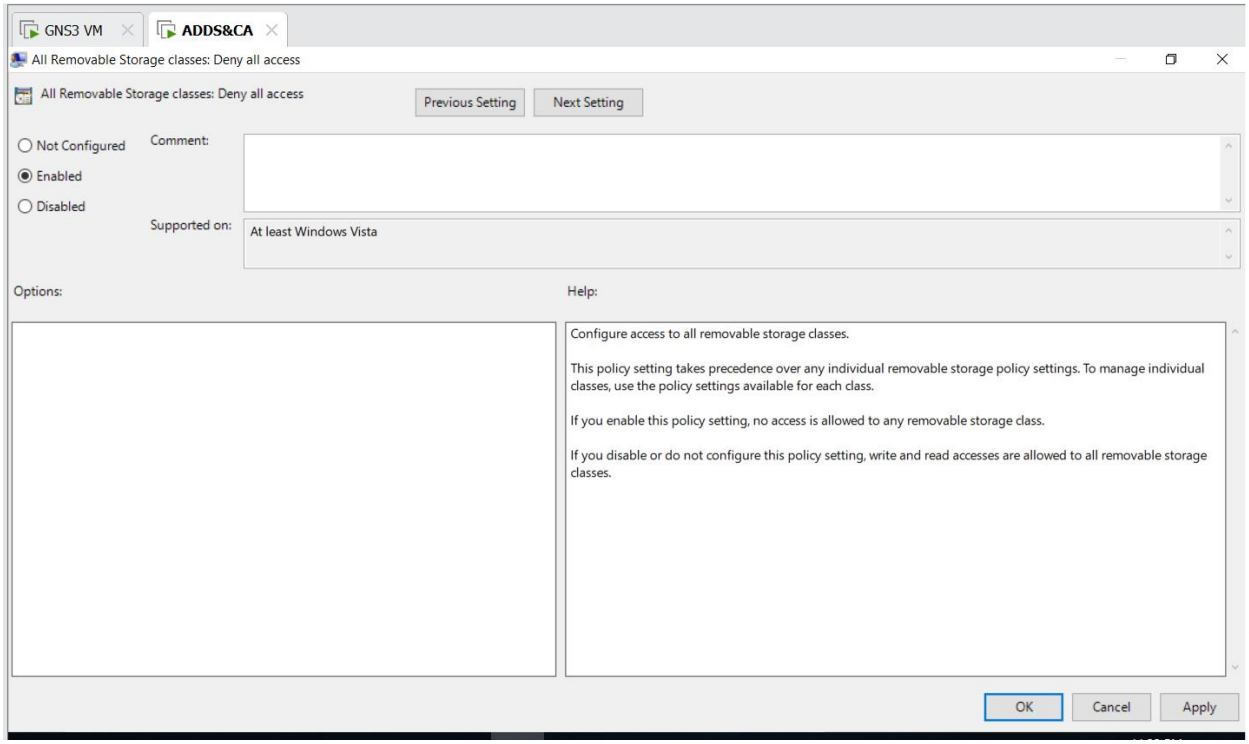




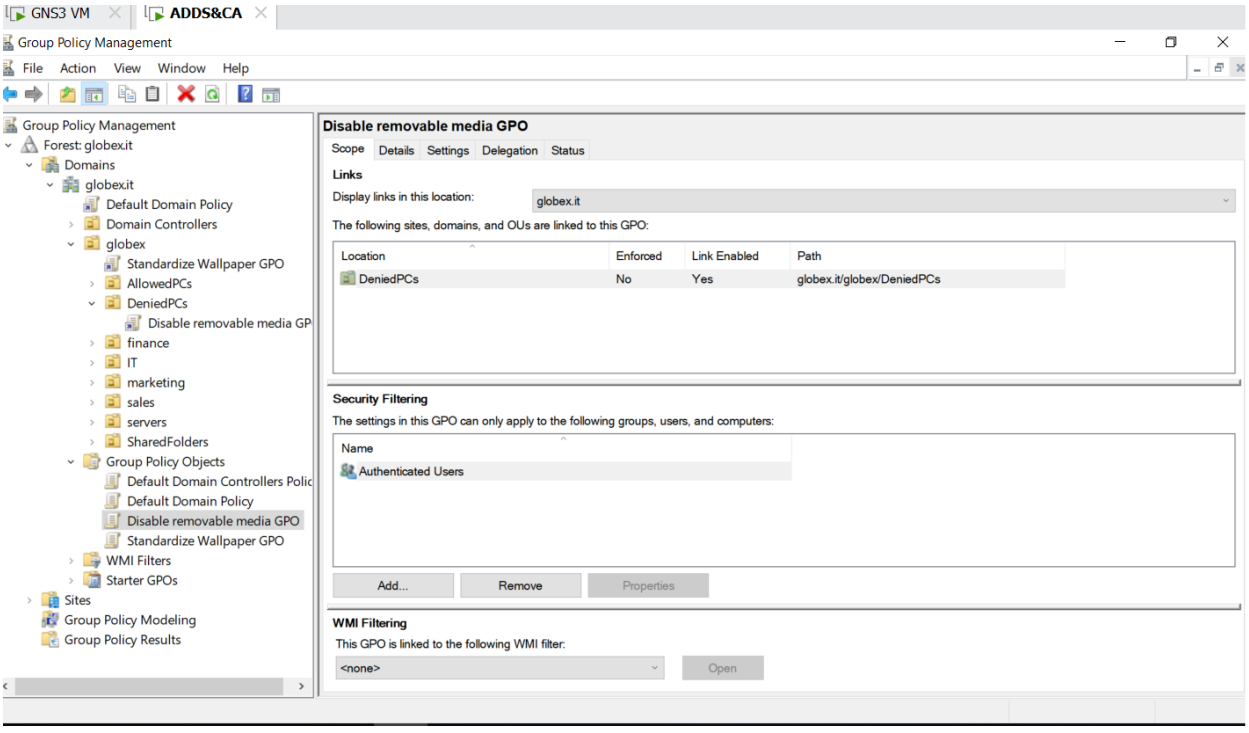
Disable removable Storage.

Path: Computer Configuration > Policies > Administrative Templates > System > Removable Storage Access

1. 

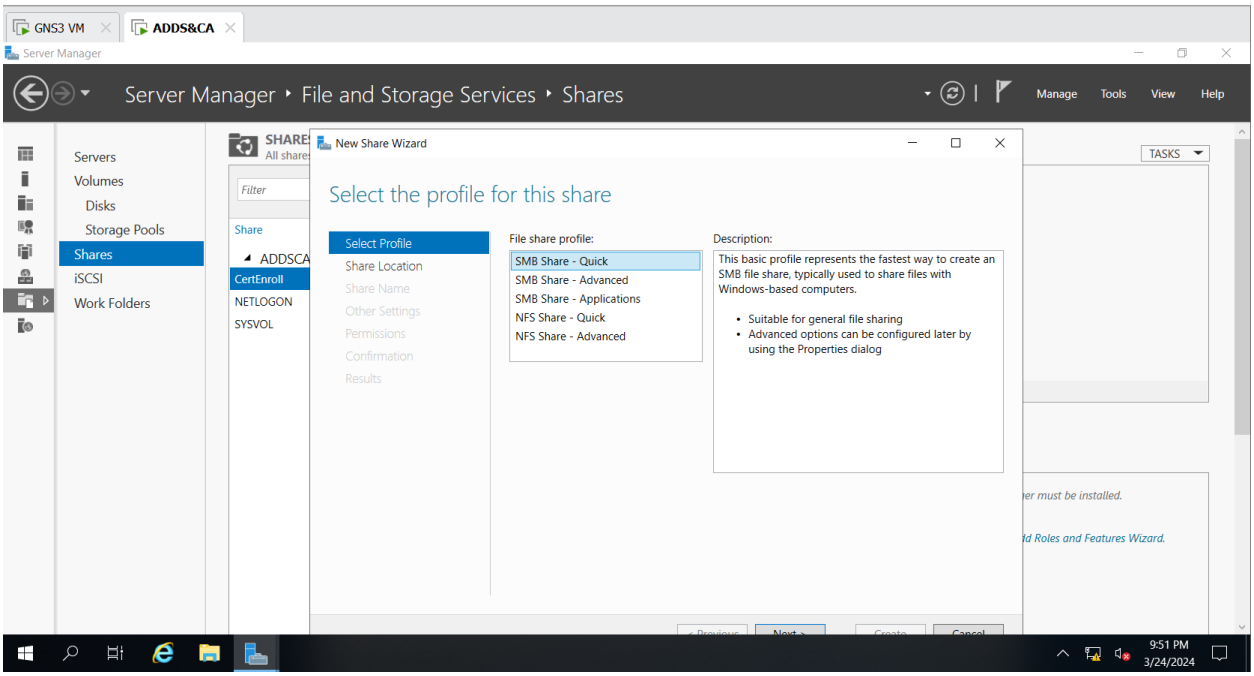


Prevent removable storage devices for all departments expect IT.

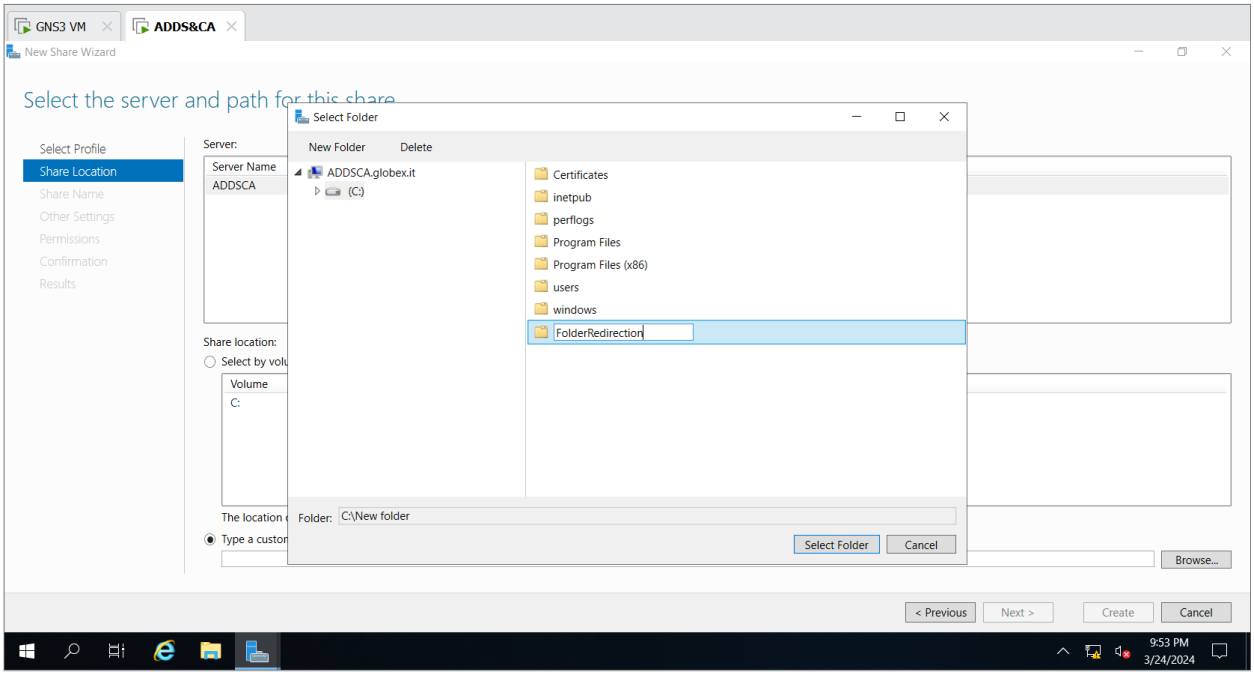


Folder Redirection Group Policy

Step1: Create a new share.

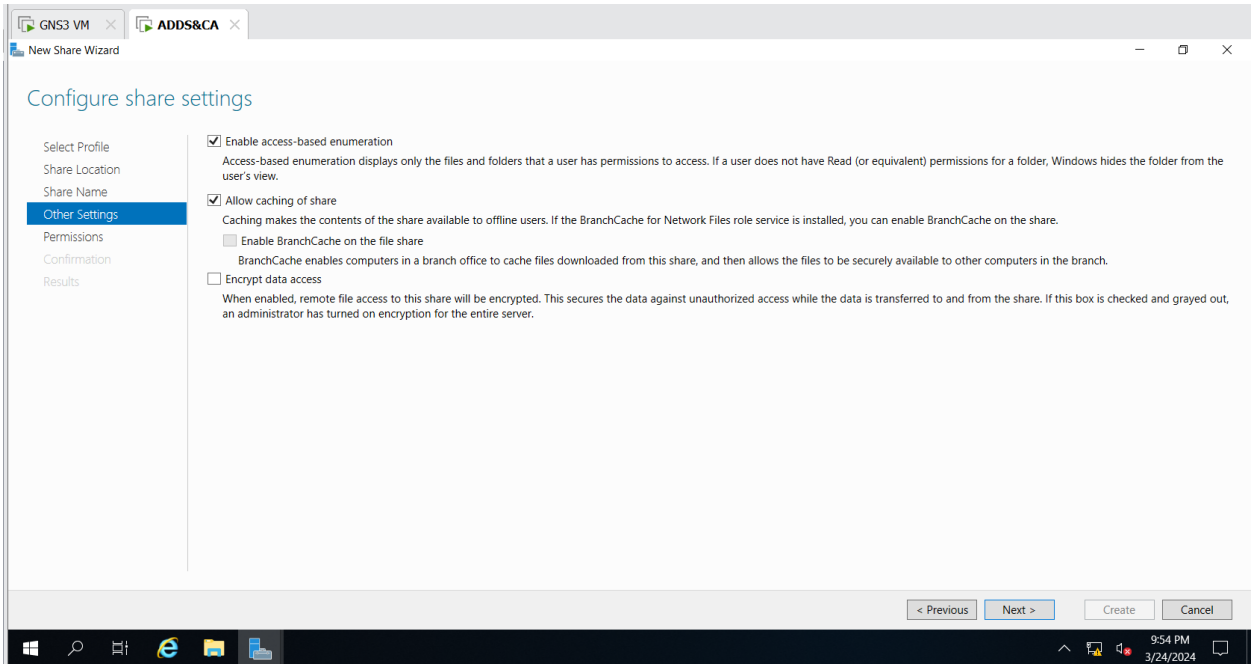


Step2: Create a folder redirection custom path.

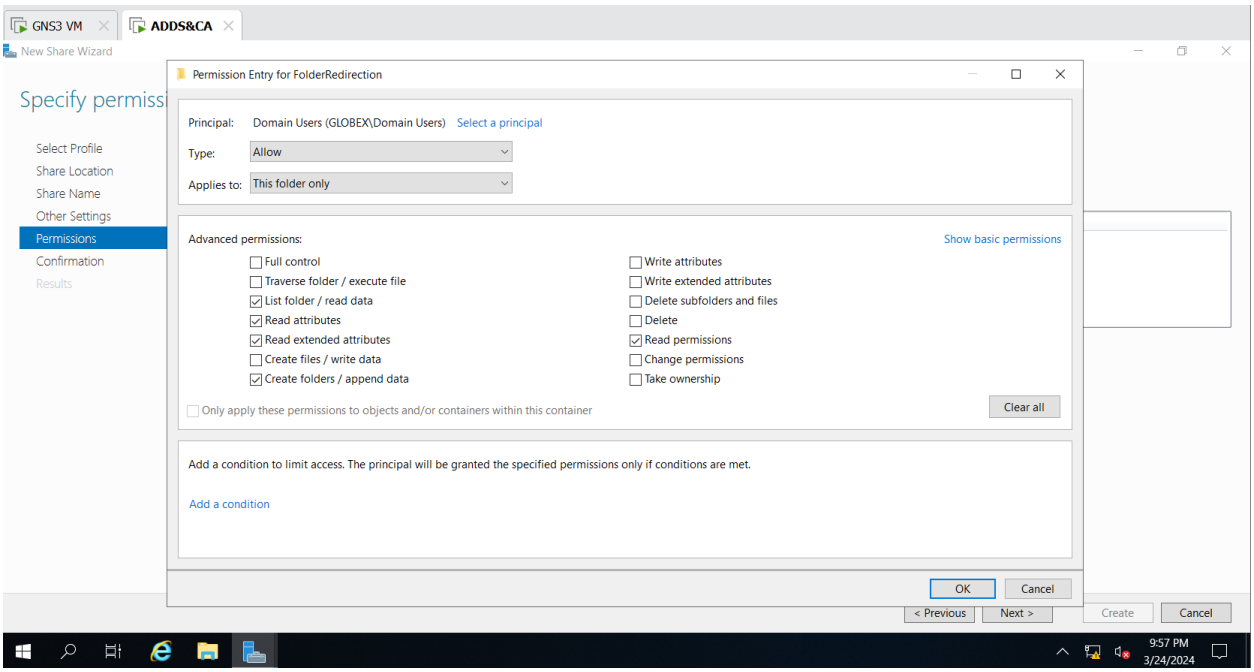


Remote path: \\ADDSCA\FolderRedirection$

Step3: Enable configuration.

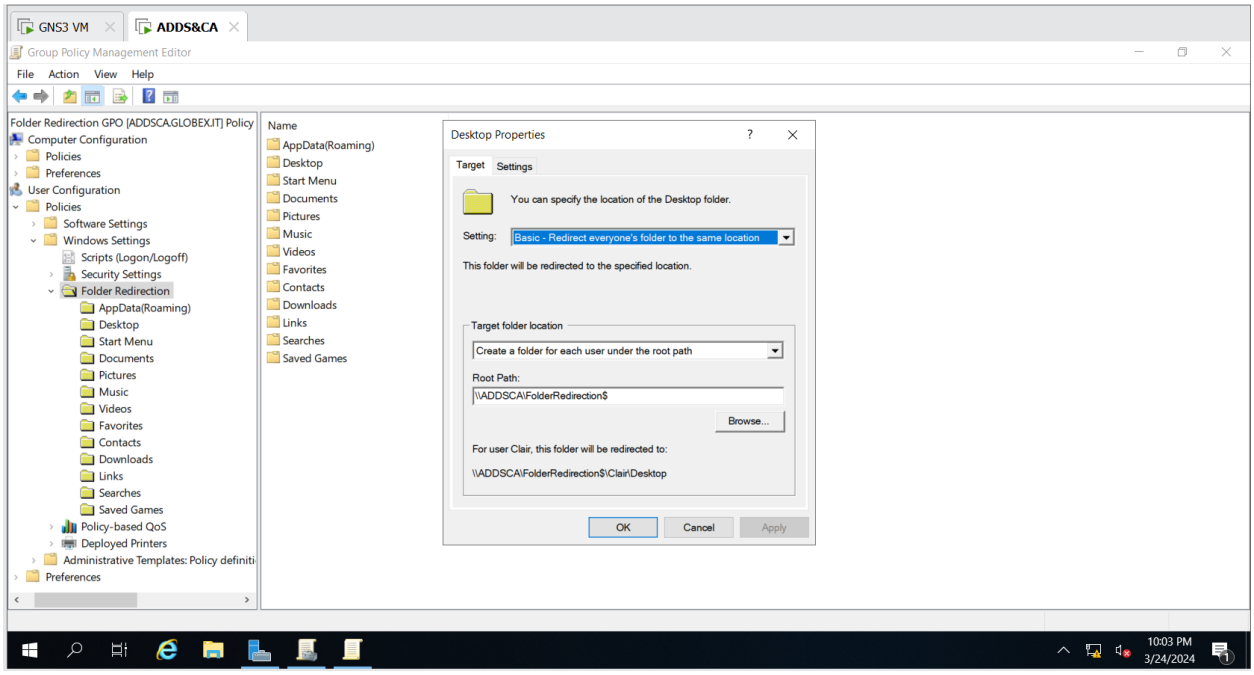


Step4: Specify permissions.

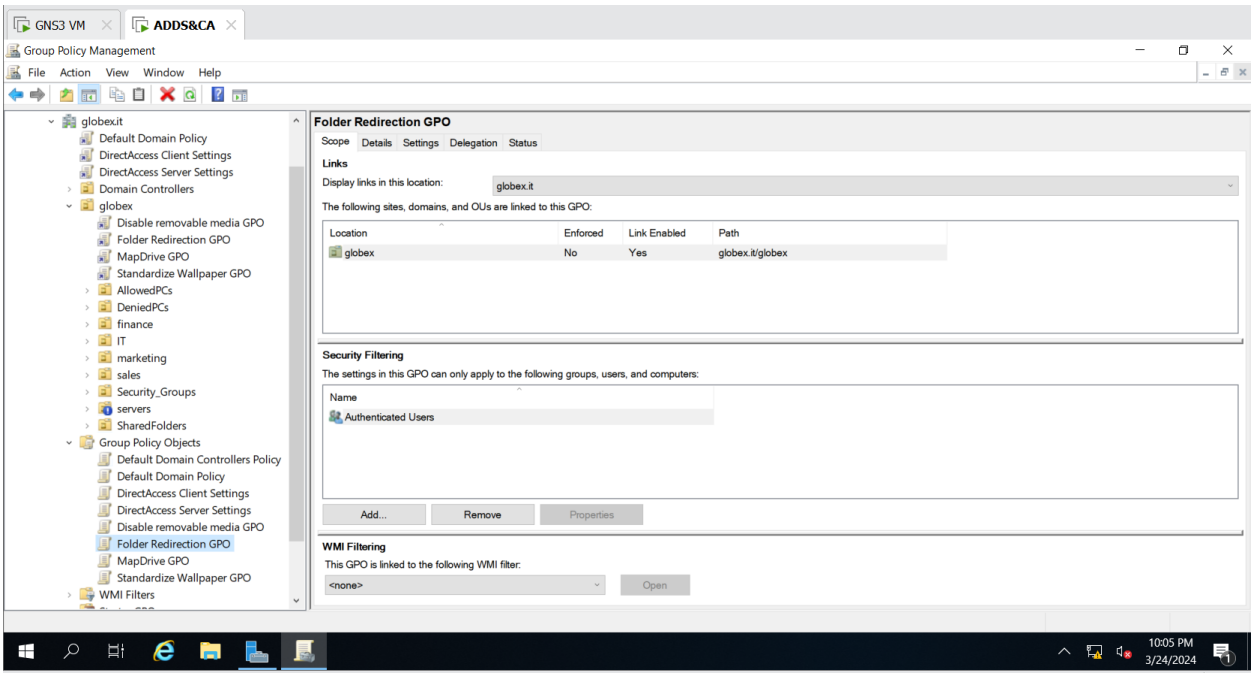


Step5: Add a group policy for Folder redirection.

Open User Configuration > Policies > Windows Settings > Folder Redirection

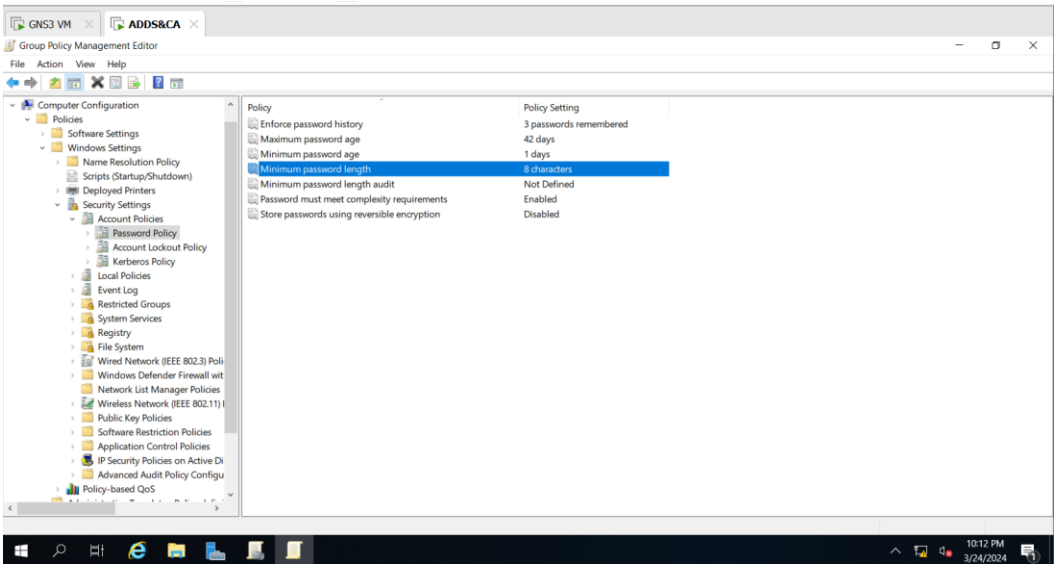


Step6: Link the group policy to Globex OU



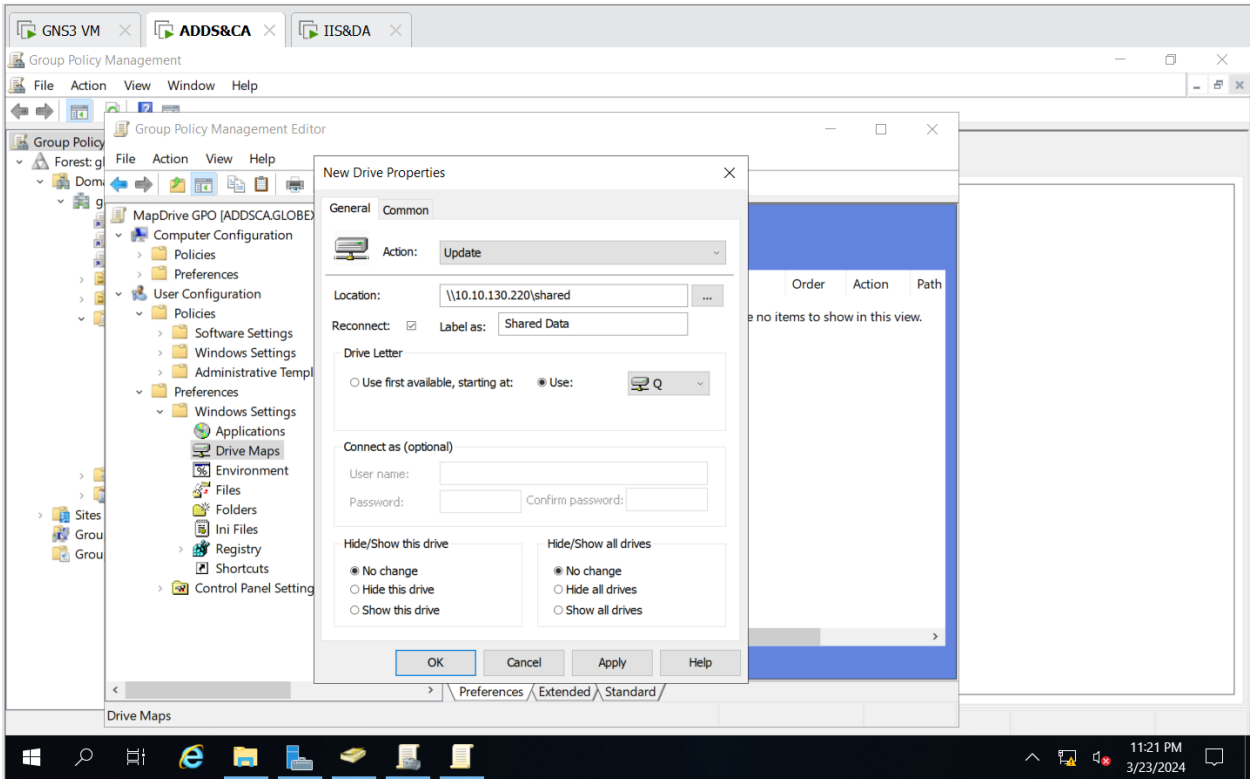
Password Policy

- Right-click the Default Domain Policy folder and click Edit.
- Navigate to Computer Configuration a Policies a Windows Settings a Security Settings Account Policies a Password Policy
- Set Enforce password history for 3 passwords.
- Set minimum length of 8 characters.



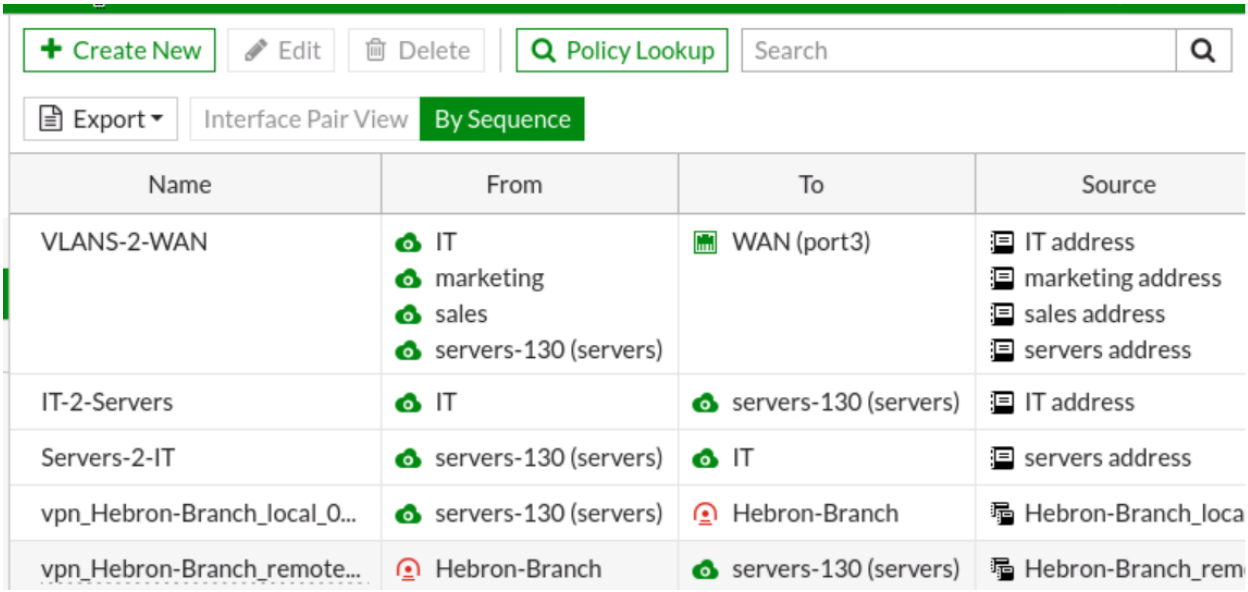
Map Drive Policy :

Navigate to User Configuration -> Preferences -> Windows Settings -> Drive Mappings. Right Click Drive Mappings, Select New – > Mapped Drive. Then Configure Drive Mapping Properties as in the picture.



Join Domain IT PC

Add Policy to access servers VLAN.



ITPC to all vlans

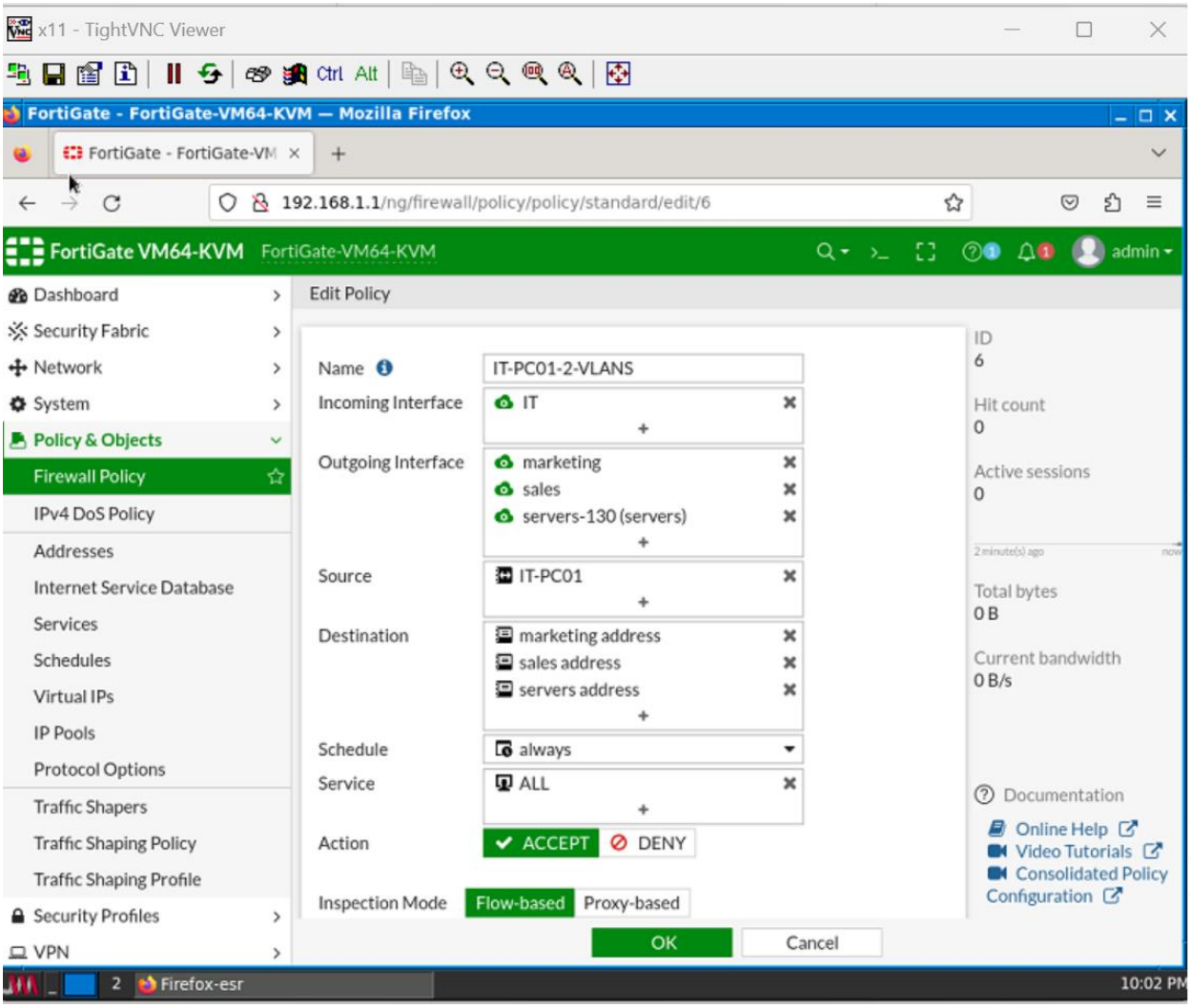


Figure 47 IT- to- VLANS Policy

```
C:\Users\alaa>ping 10.10.120.254 -t

Pinging 10.10.120.254 with 32 bytes of data:
Reply from 10.10.120.254: bytes=32 time=18ms TTL=255
Reply from 10.10.120.254: bytes=32 time=13ms TTL=255
Reply from 10.10.120.254: bytes=32 time=18ms TTL=255
Reply from 10.10.120.254: bytes=32 time=637ms TTL=255
Reply from 10.10.120.254: bytes=32 time=1627ms TTL=255
Reply from 10.10.120.254: bytes=32 time=992ms TTL=255
```

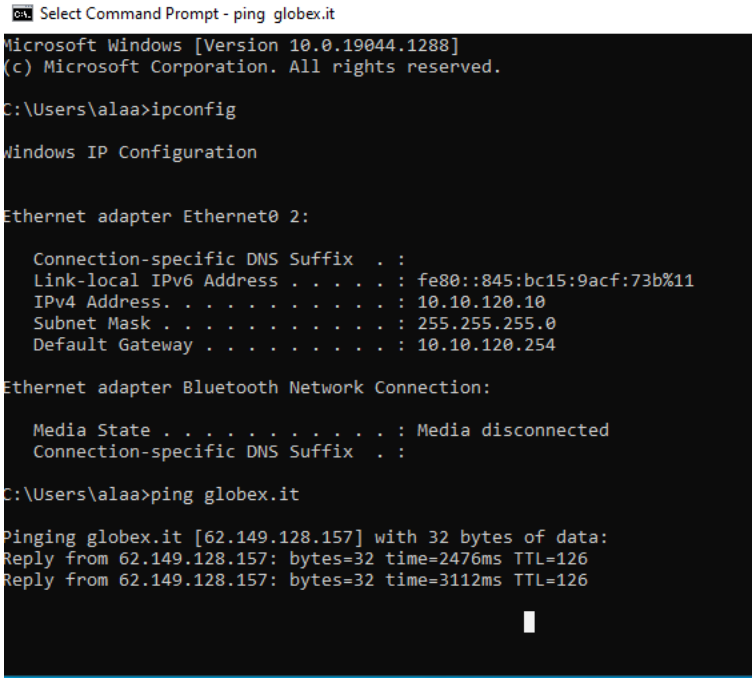


Figure 48 ITPC01 Ping globex.it Success

2. All Vlans To servers

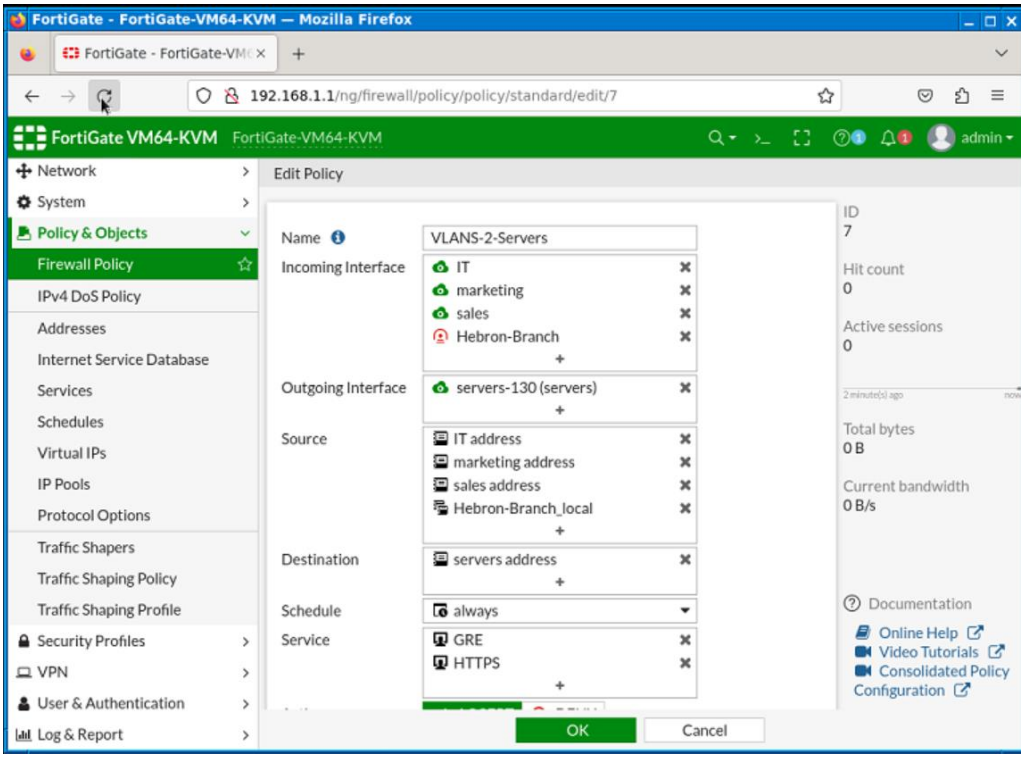


Figure 49 VLANS to Servers Policy

Configuring IIS&DA

- Join Domian (the same vlan) no policies are needed.

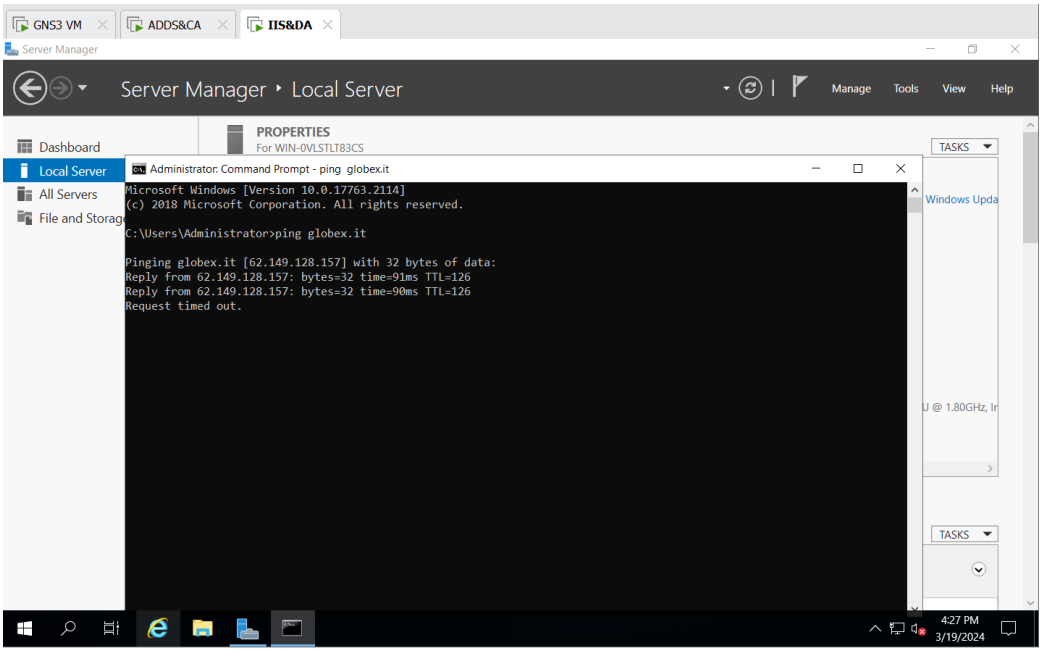


Figure 50 Ping globex.it Success

Join Domain

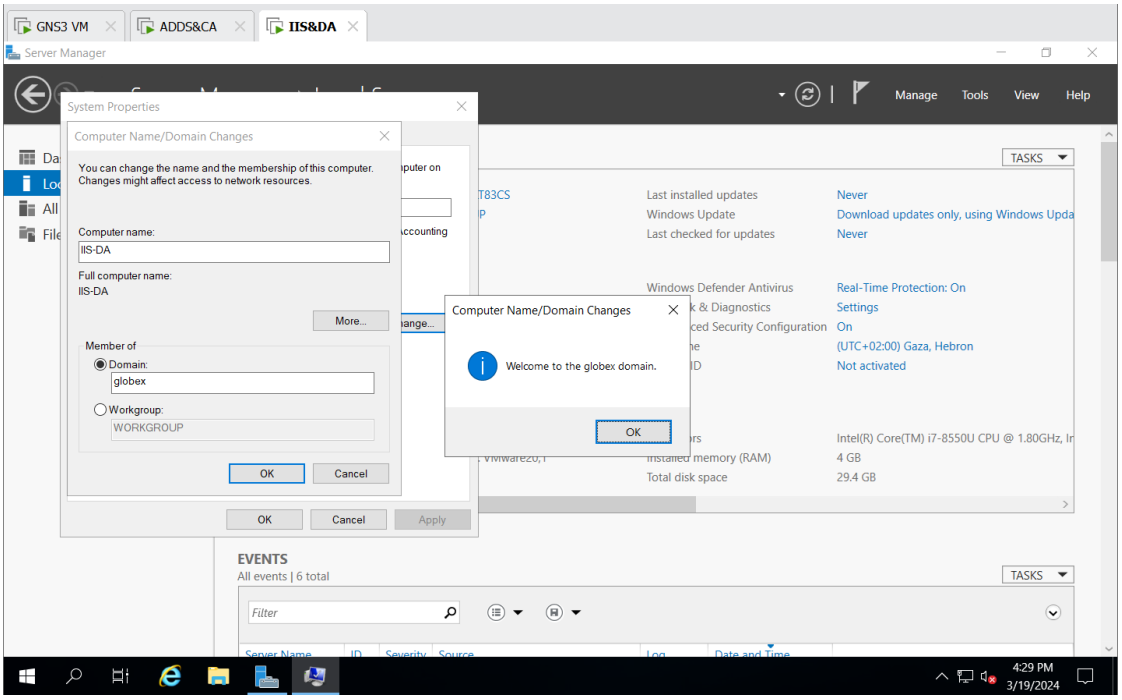


Figure 51 Successful Join to Domain

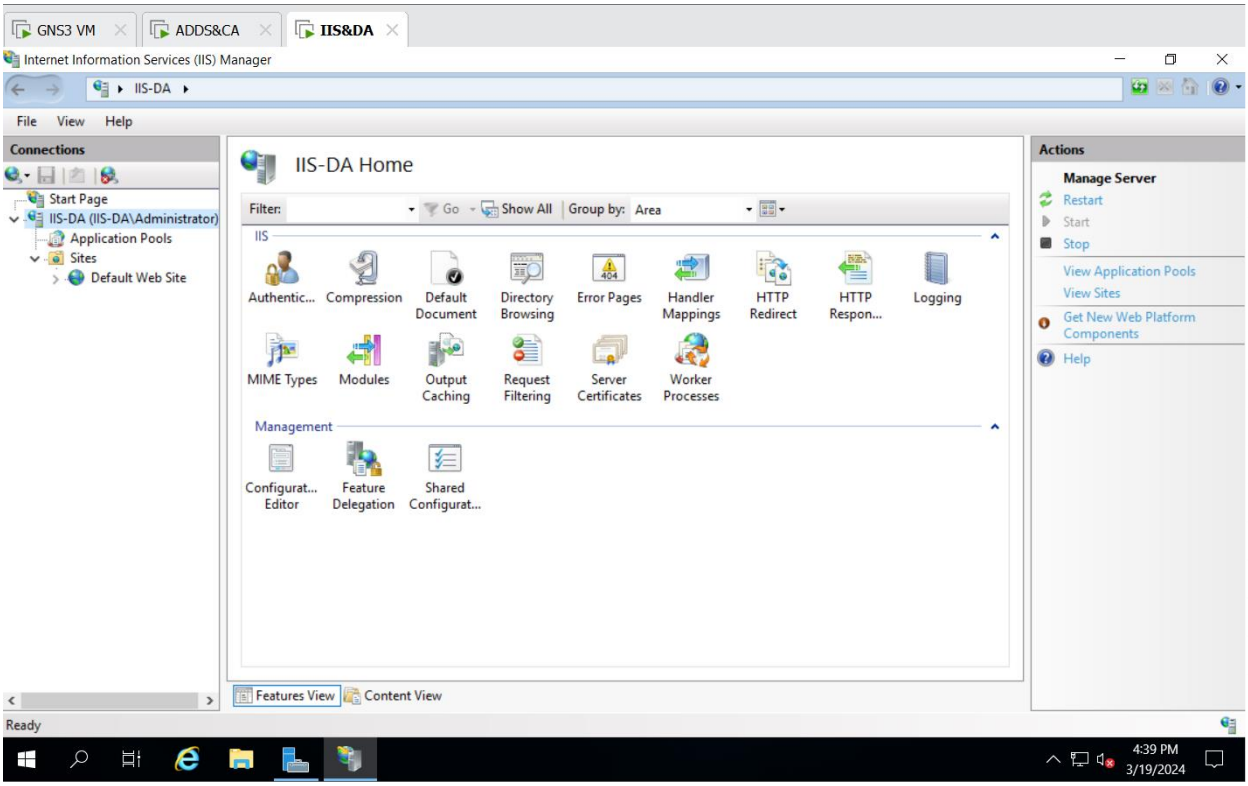


Figure 52 IIS Role

DA Configuration

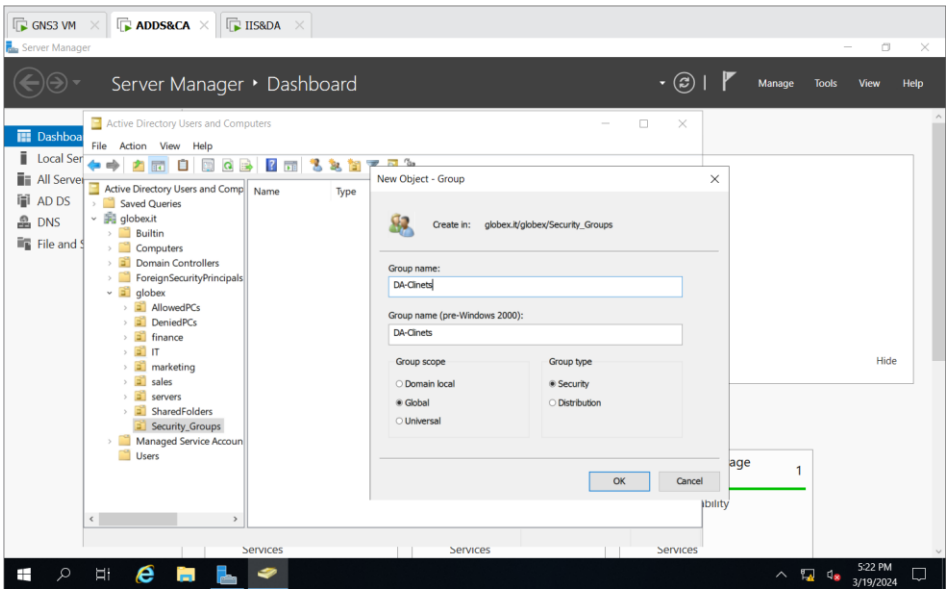


Figure 53 Create a Group for DA Computers

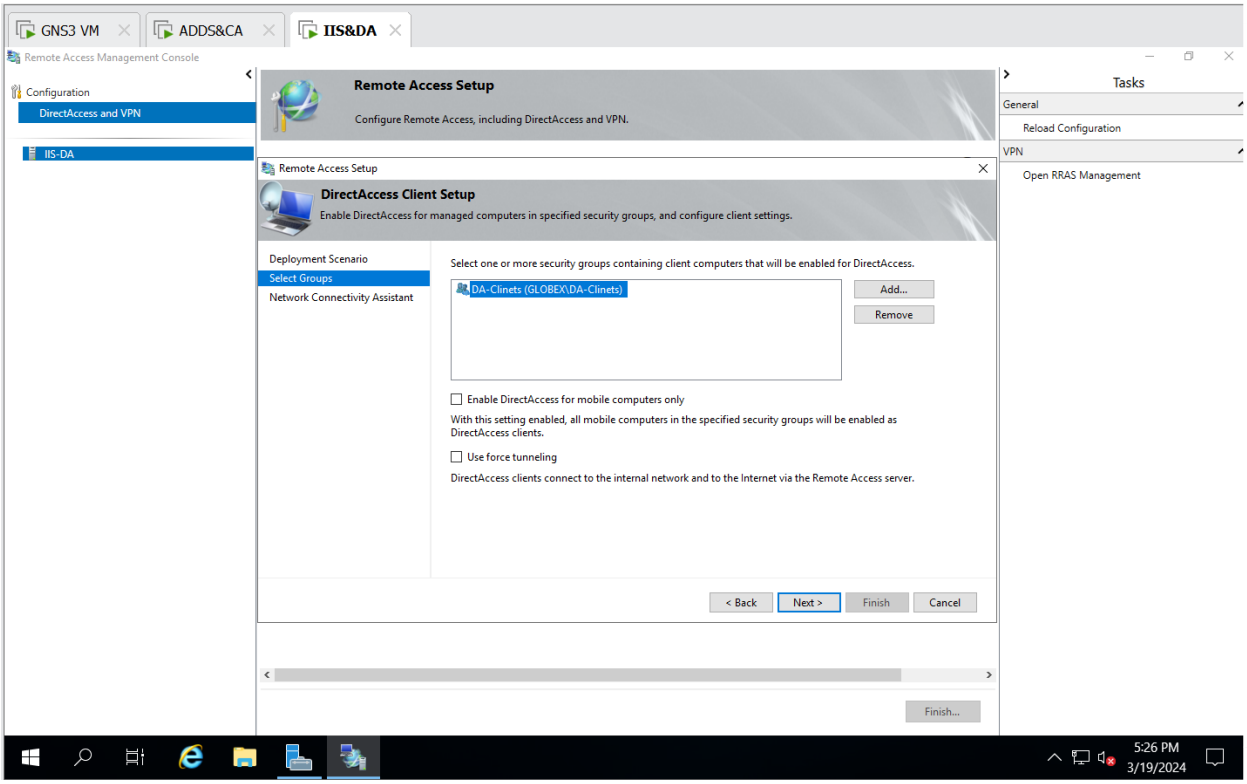


Figure 54 DA Configurations

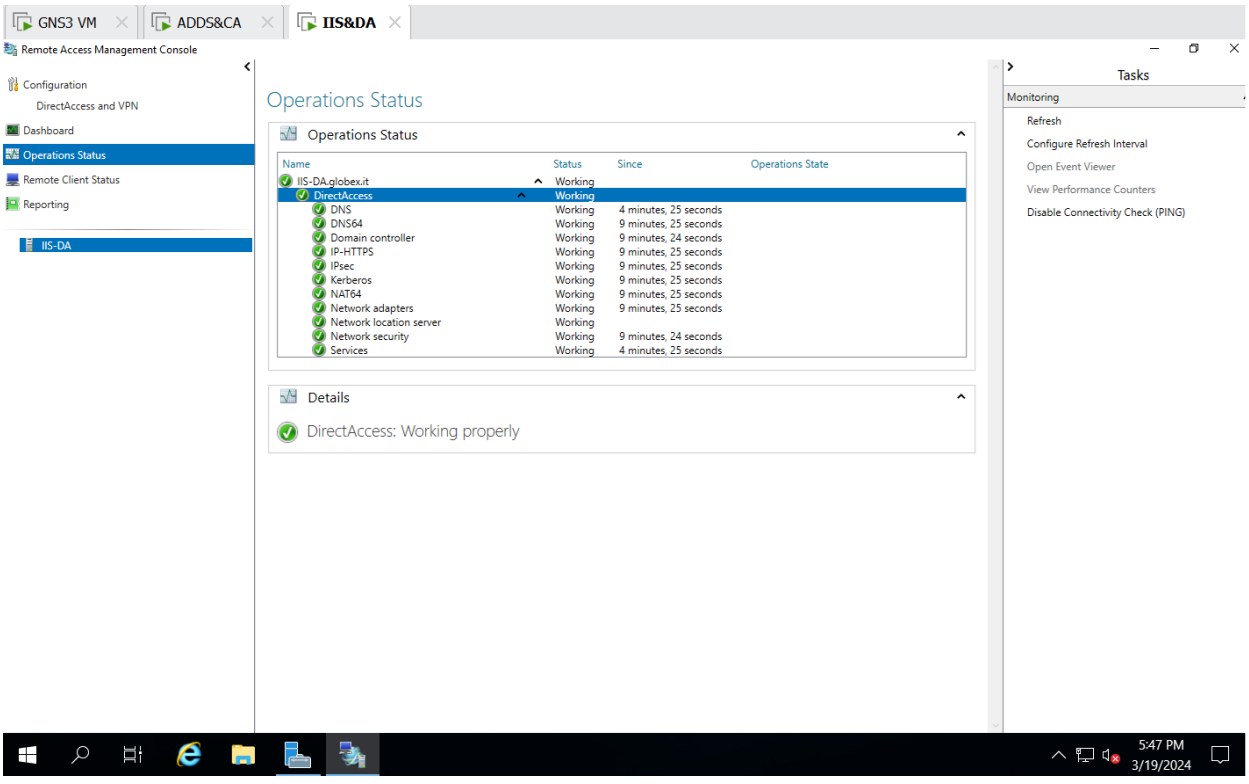


Figure 55 Successful Configurations

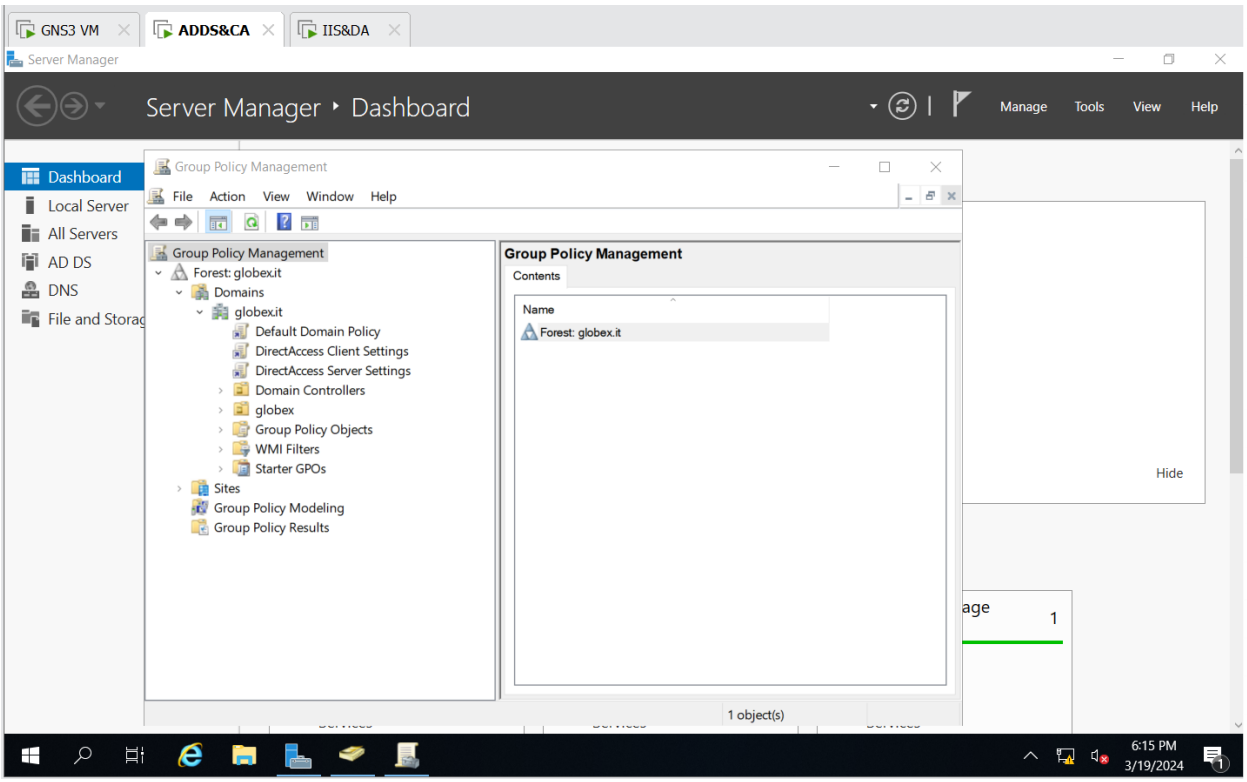


Figure 56 Automatic Created Policies

VPN PORTS: GRE, 1701,1723,500,443,47,4500

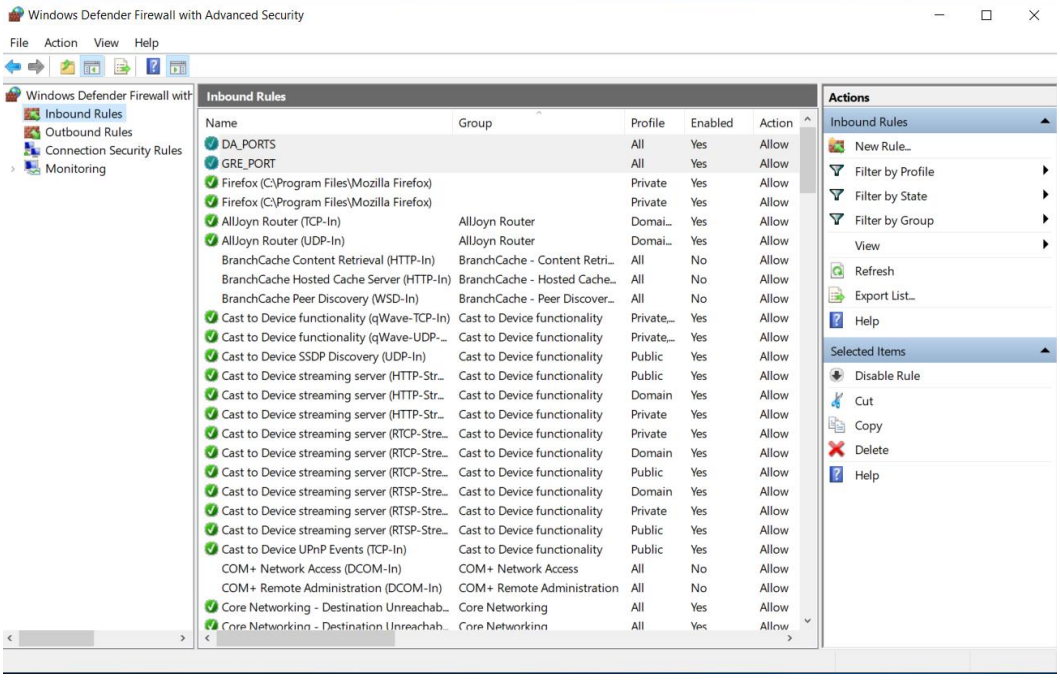
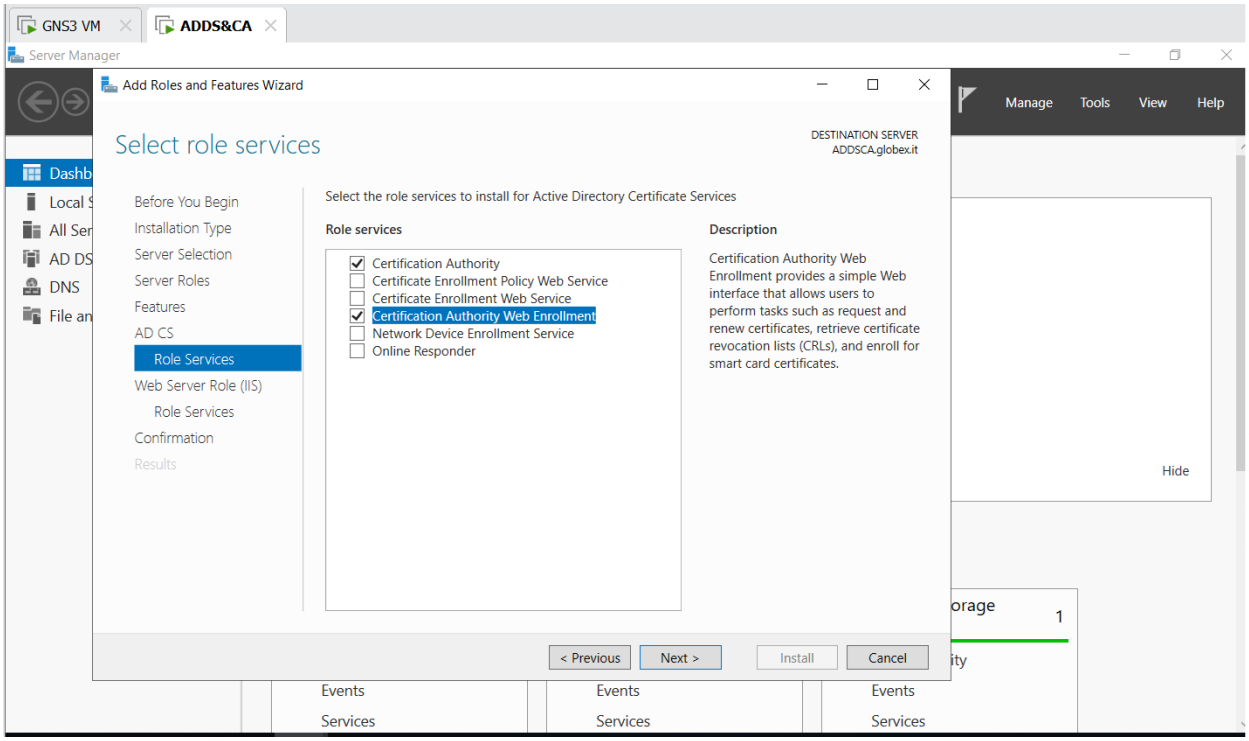
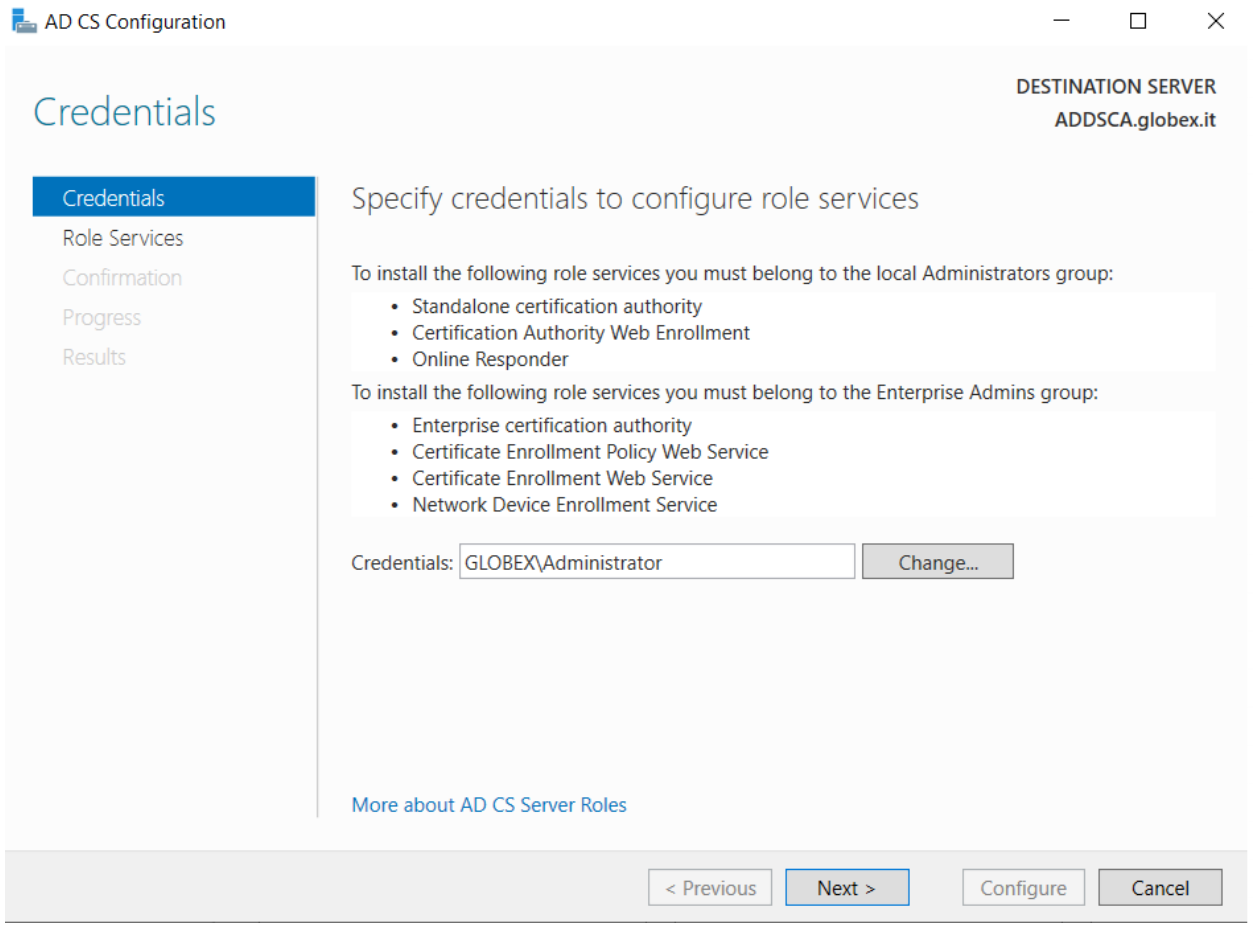
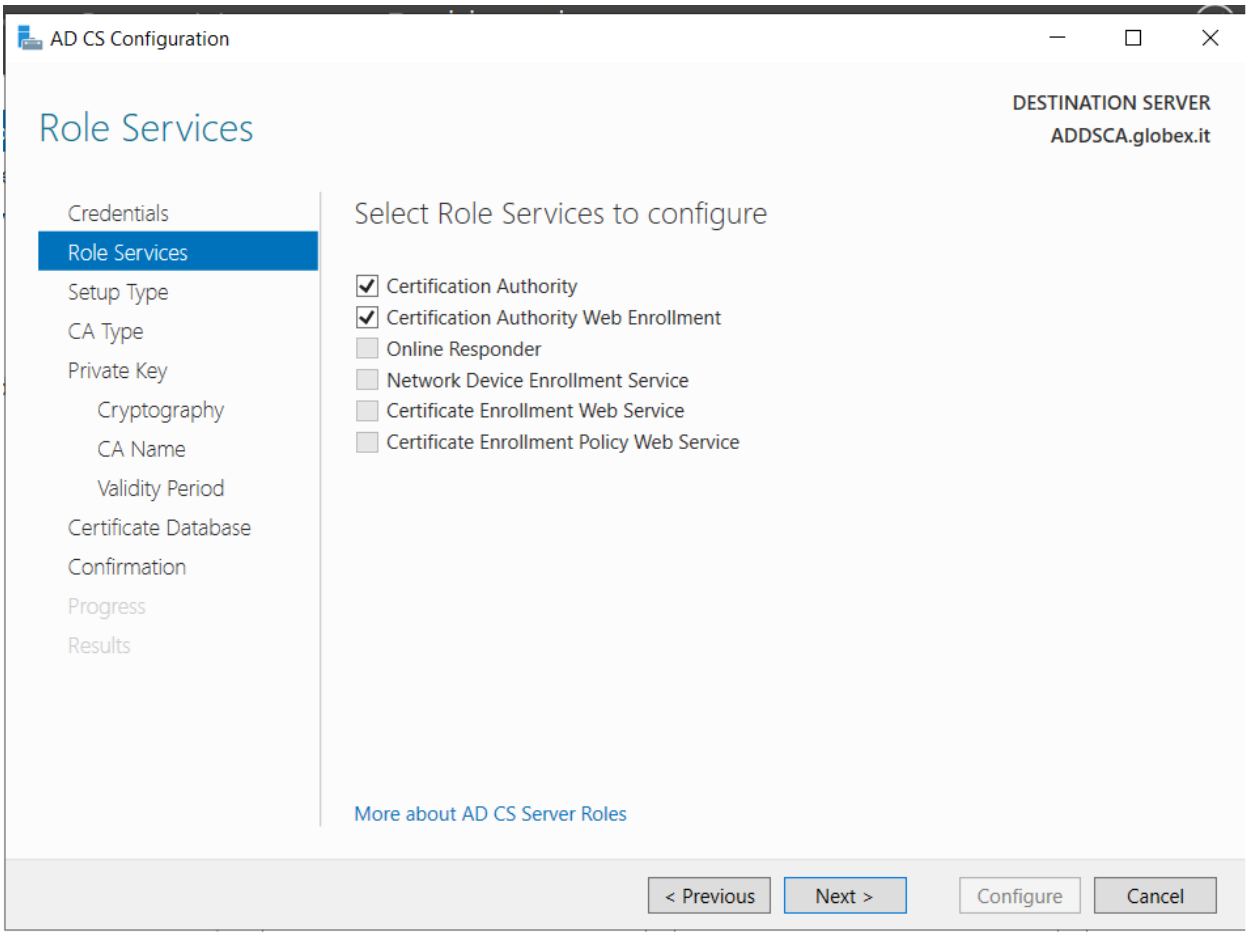


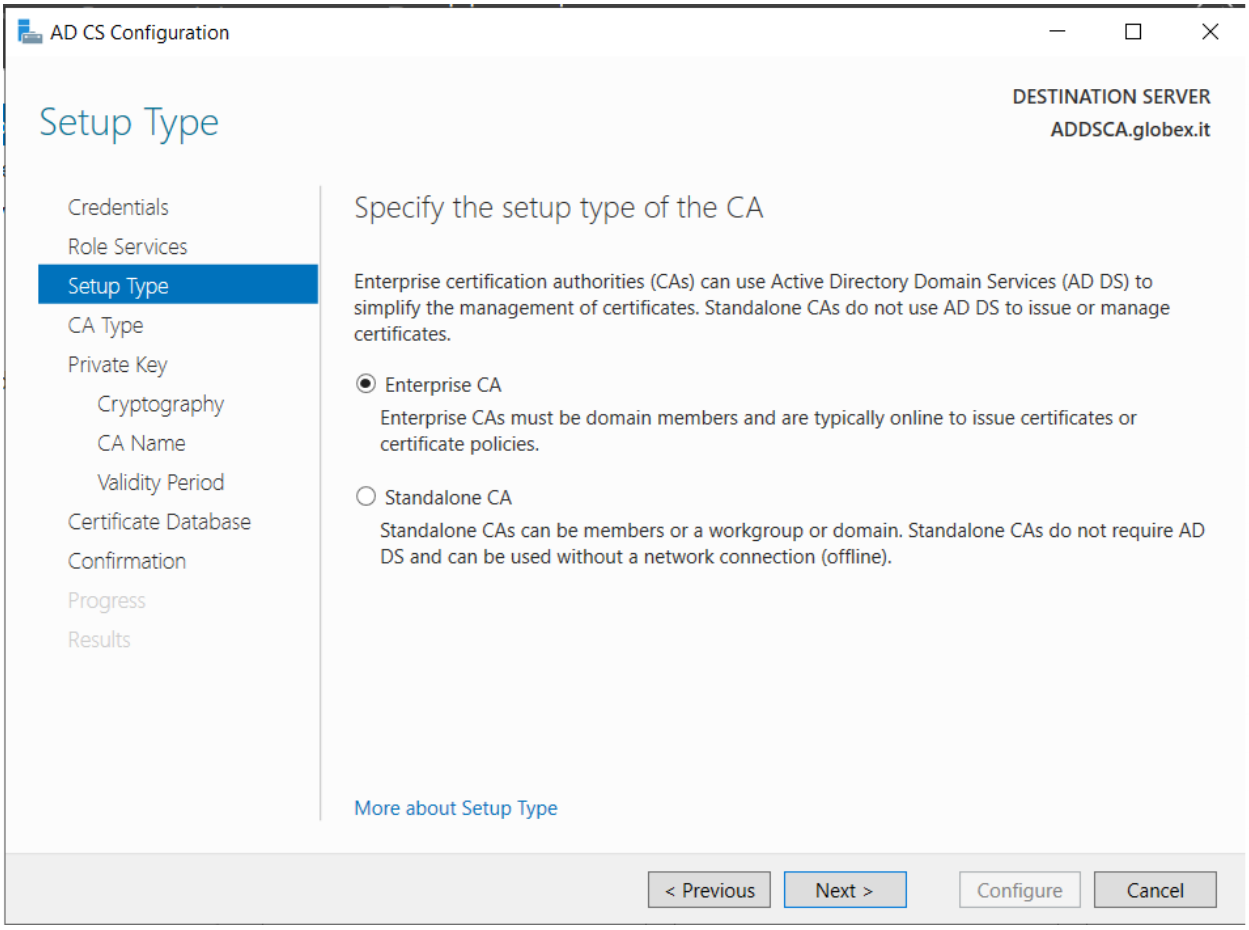
Figure 57 VPN_PORTs

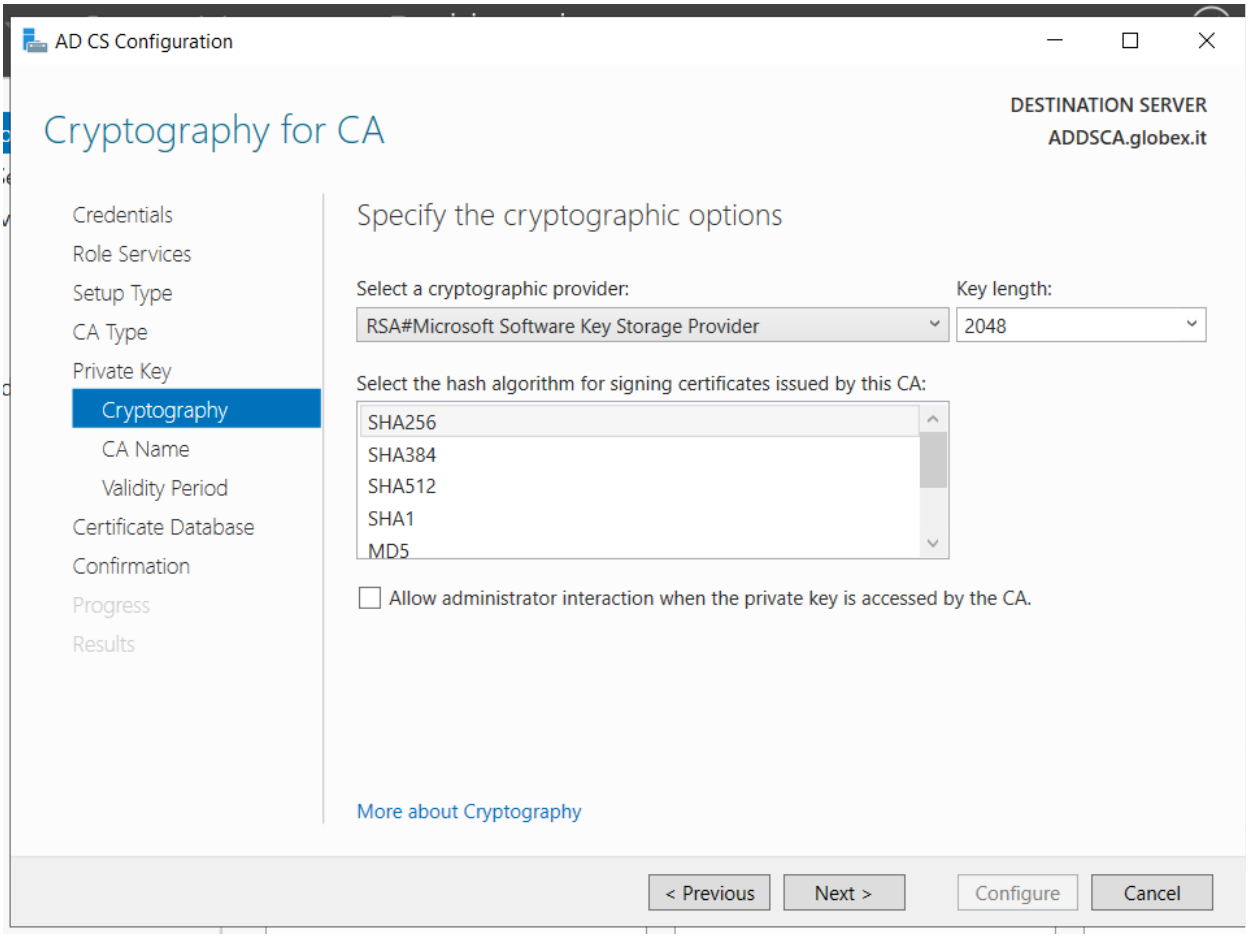
Certificate Authority Configuration:

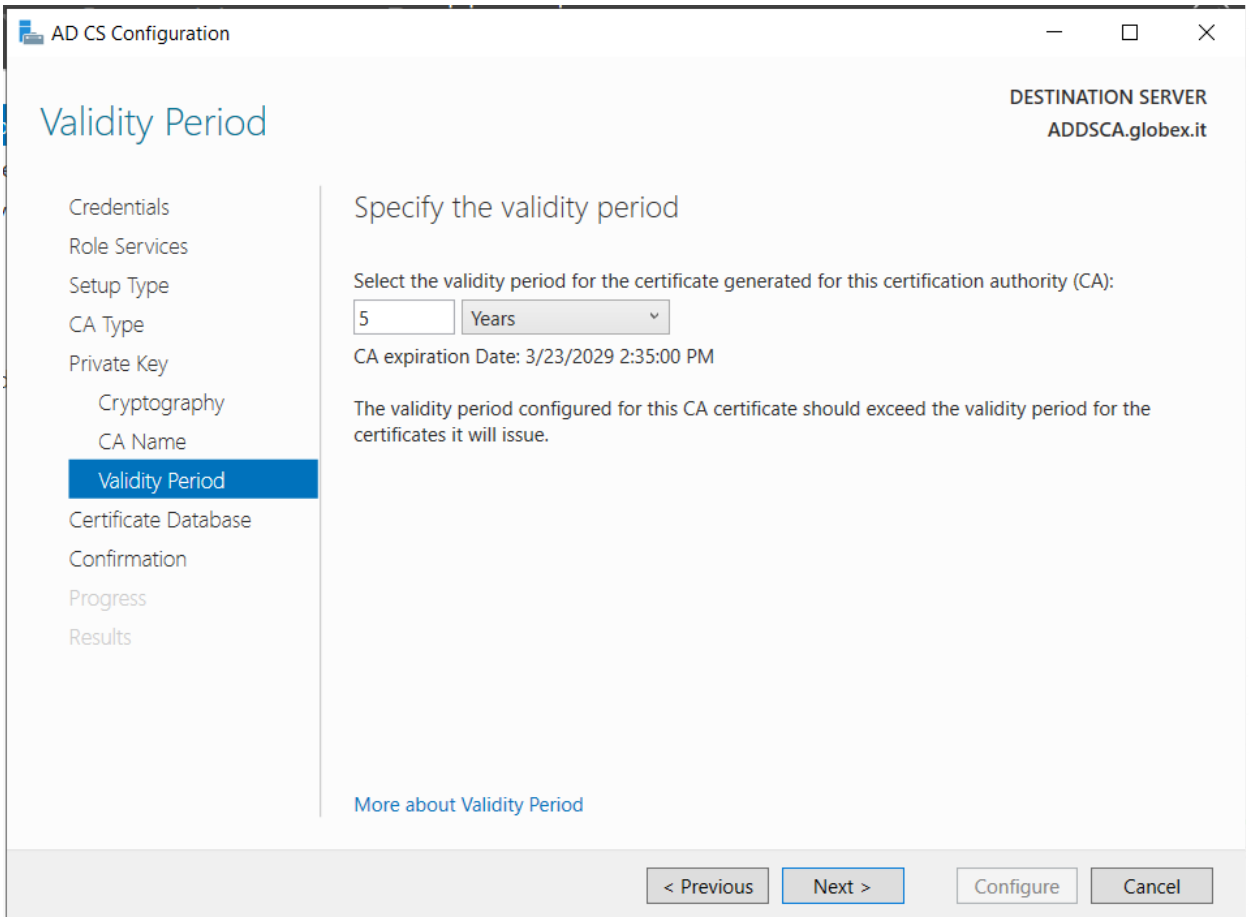


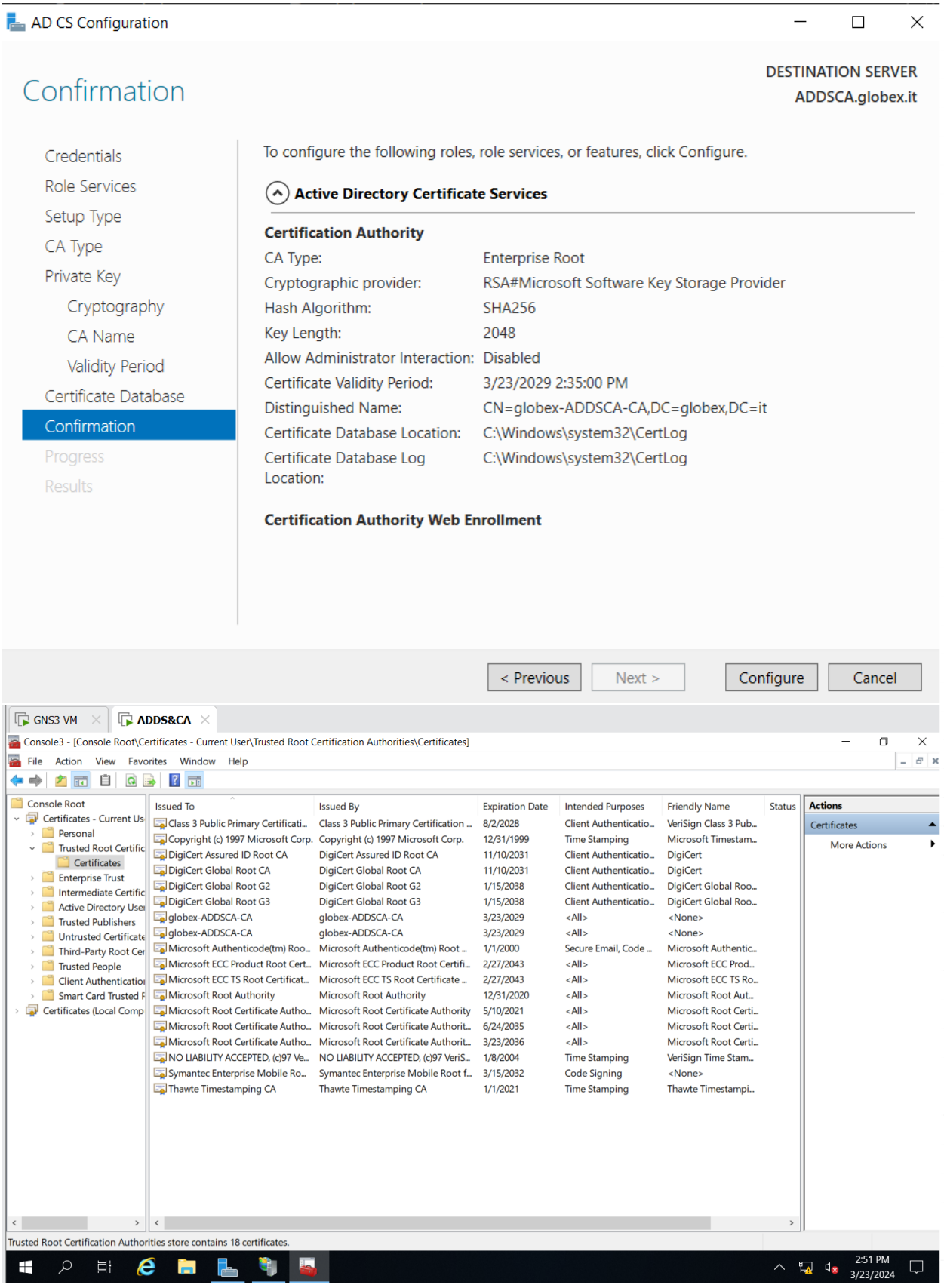

AD CS Configuration
Credentials
DESTINATION SERVER
ADDSCA.globex.it
Credentials
Role Services
Confirmation
Progress
Results
Specify credentials to configure role services
To install the following role services you must belong to the local Administrators group:
Standalone certification authority
Certification Authority Web Enrollment
Online Responder
To install the following role services you must belong to the Enterprise Admins group:
Enterprise certification authority
Certificate Enrollment Policy Web Service
Certificate Enrollment Web Service
Network Device Enrollment Service
Credentials: GLOBEX\Administrator
Change...
More about AD CS Server Roles
< Previous
Next >
Configure
Cancel


AD CS Configuration
Role Services
DESTINATION SERVER
ADDSCA.globex.it
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Select Role Services to configure
Certification Authority
Certification Authority Web Enrollment
Online Responder
Network Device Enrollment Service
Certificate Enrollment Web Service
Certificate Enrollment Policy Web Service
More about AD CS Server Roles
< Previous
Next >
Configure
Cancel

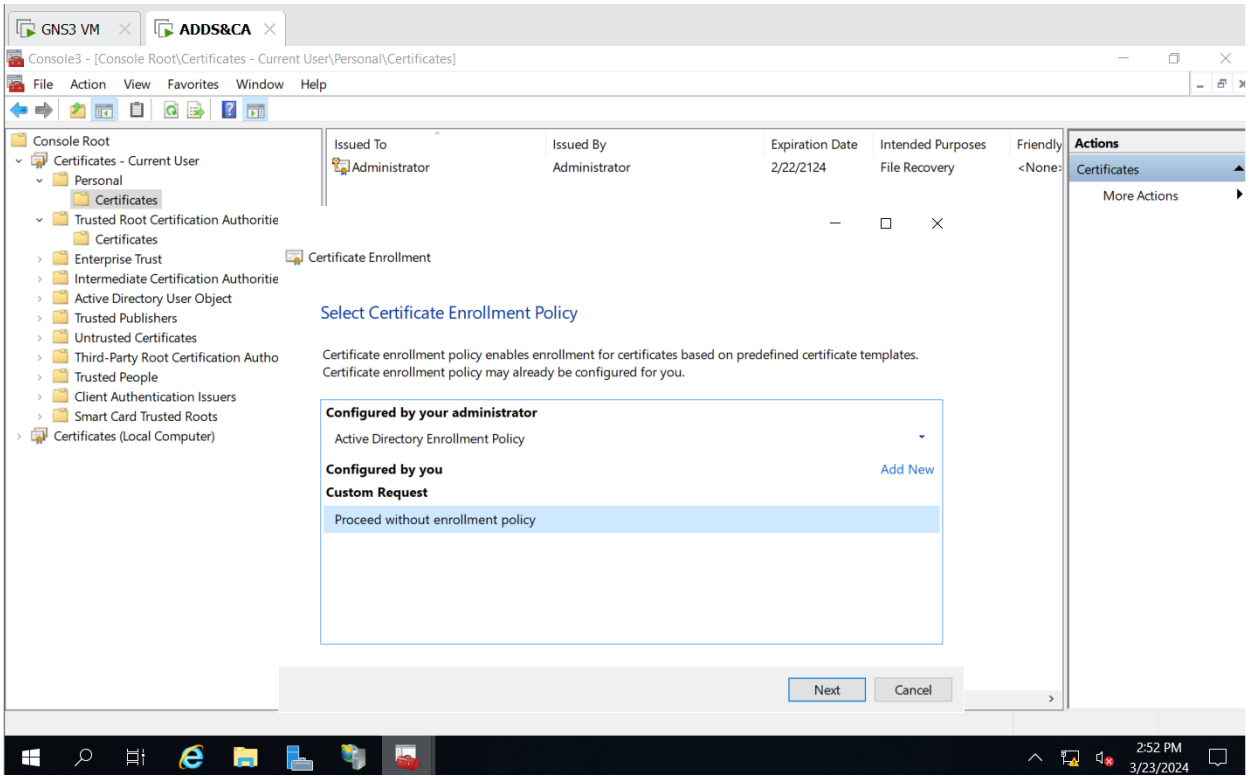

AD CS Configuration
Setup Type
DESTINATION SERVER
ADDSCA.globex.it
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the setup type of the CA
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.
Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.
Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).
More about Setup Type
< Previous
Next >
Configure
Cancel

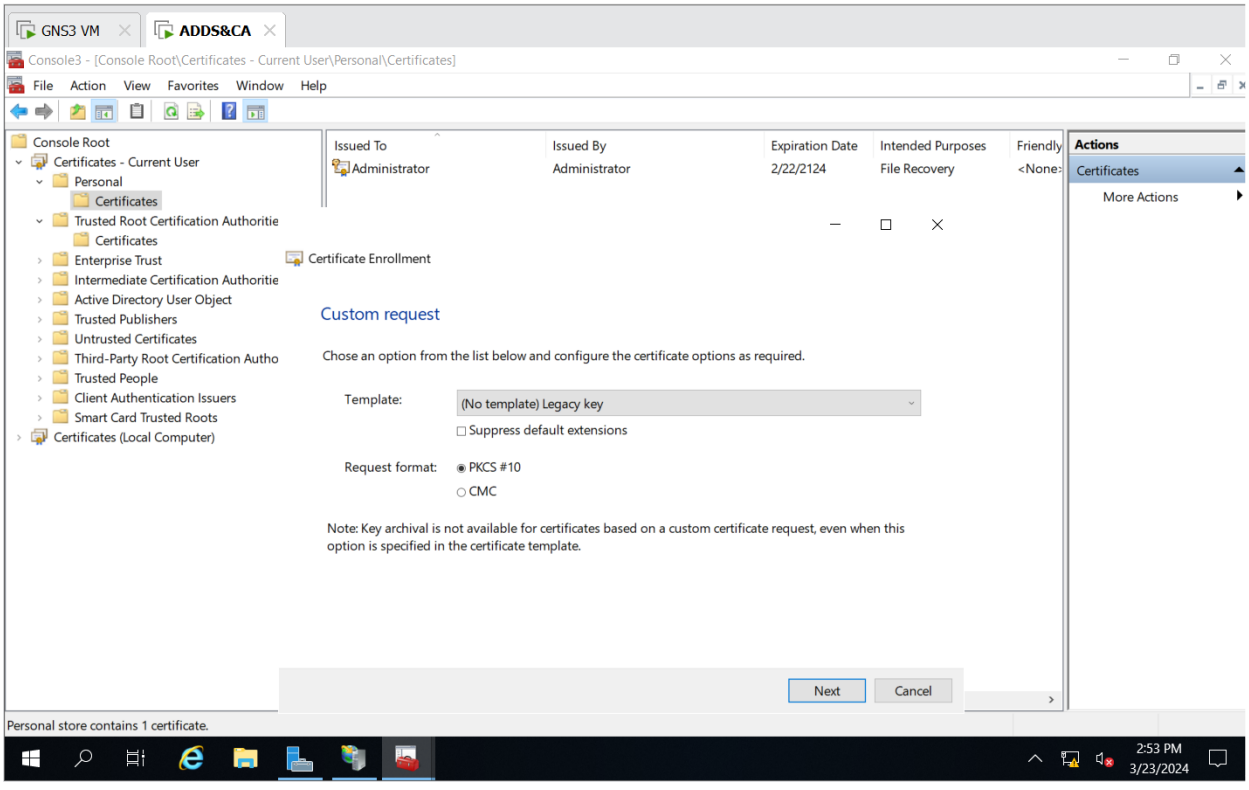

AD CS Configuration
Cryptography for CA
DESTINATION SERVER
ADDSCA.globex.it
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the cryptographic options
Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider
Key length:
2048
Select the hash algorithm for signing certificates issued by this CA:
SHA256
SHA384
SHA512
SHA1
MD5
Allow administrator interaction when the private key is accessed by the CA.
More about Cryptography
< Previous
Next >
Configure
Cancel

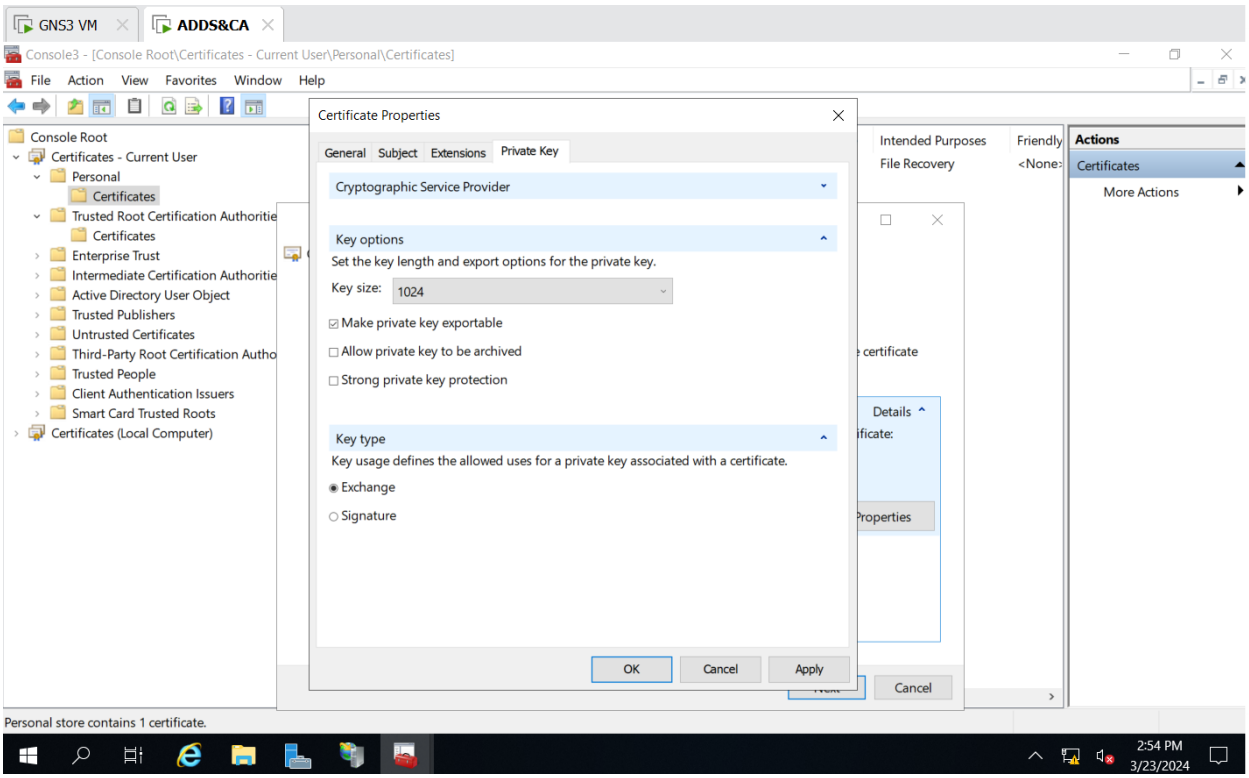

AD CS Configuration
Validity Period
DESTINATION SERVER
ADDSCA.globex.it
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the validity period
Select the validity period for the certificate generated for this certification authority (CA):
5
Years
CA expiration Date: 3/23/2029 2:35:00 PM
The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.
More about Validity Period
< Previous
Next >
Configure
Cancel

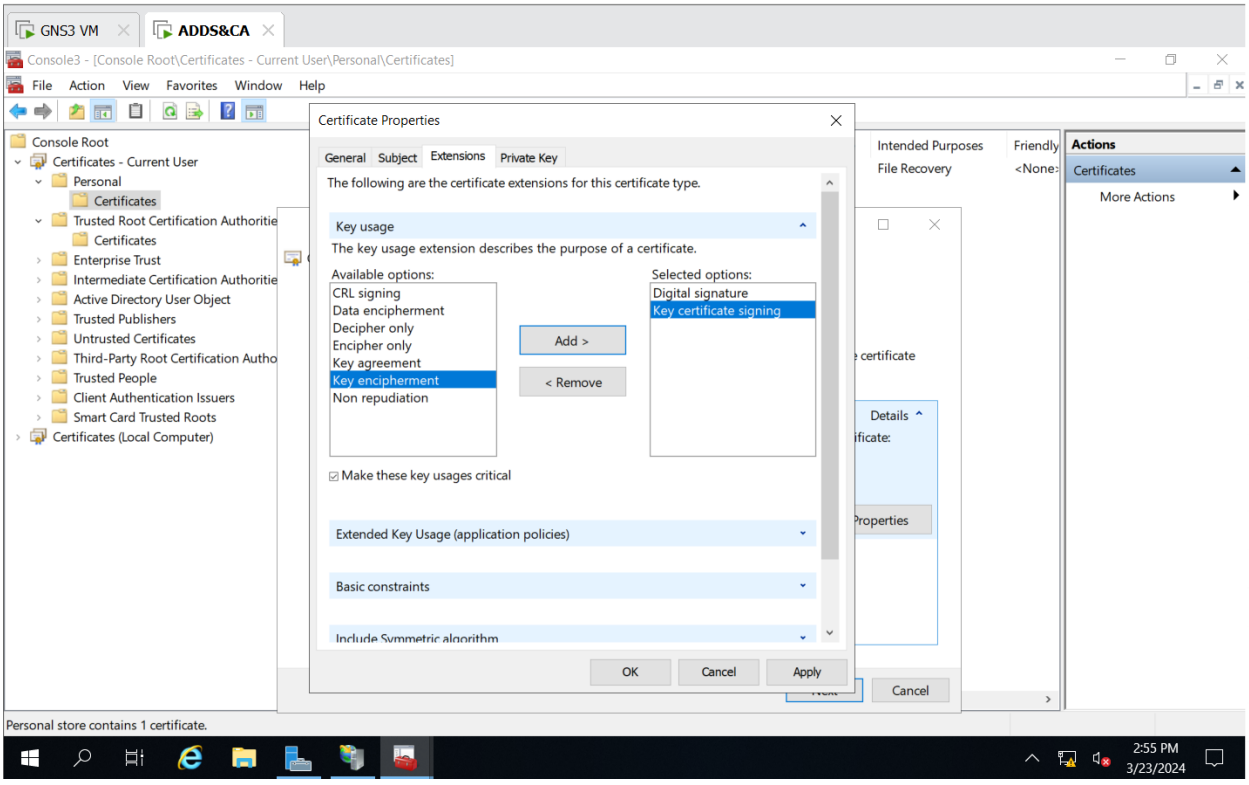

AD CS Configuration
Confirmation
DESTINATION SERVER
ADDSCA.globex.it
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
To configure the following roles, role services, or features, click Configure.
Active Directory Certificate Services
Certification Authority
CA Type: Enterprise Root
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA256
Key Length: 2048
Allow Administrator Interaction: Disabled
Certificate Validity Period: 3/23/2029 2:35:00 PM
Distinguished Name: CN=globex-ADDSCA-CA,DC=globex,DC=it
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog
Certification Authority Web Enrollment
< Previous
Next >
Configure
Cancel
GNS3 VM
ADDS&CA
Console3 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current Us
Personal
Trusted Root Certific
Certificates
Enterprise Trust
Intermediate Certific
Active Directory User
Trusted Publishers
Untrusted Certificate
Third-Party Root Cer
Trusted People
Client Authenticatio
Smart Card Trusted F
Certificates (Local Comp
Issued To | Issued By | Expiration Date | Intended Purposes | Friendly Name | Status
Class 3 Public Primary Certificati... | Class 3 Public Primary Certification ... | 8/2/2028 | Client Authenticatio... | VeriSign Class 3 Pub...
Copyright (c) 1997 Microsoft Corp. | Copyright (c) 1997 Microsoft Corp. | 12/31/1999 | Time Stamping | Microsoft Timestam...
DigiCert Assured ID Root CA | DigiCert Assured ID Root CA | 11/10/2031 | Client Authenticatio... | DigiCert
DigiCert Global Root CA | DigiCert Global Root CA | 11/10/2031 | Client Authenticatio... | DigiCert
DigiCert Global Root G2 | DigiCert Global Root G2 | 1/15/2038 | Client Authenticatio... | DigiCert Global Roo...
DigiCert Global Root G3 | DigiCert Global Root G3 | 1/15/2038 | Client Authenticatio... | DigiCert Global Roo...
globex-ADDSCA-CA | globex-ADDSCA-CA | 3/23/2029 | <All> | <None>
globex-ADDSCA-CA | globex-ADDSCA-CA | 3/23/2029 | <All> | <None>
Microsoft Authenticode(tm) Roo... | Microsoft Authenticode(tm) Root ... | 1/1/2000 | Secure Email, Code ... | Microsoft Authentic...
Microsoft ECC Product Root Cert... | Microsoft ECC Product Root Certifi... | 2/27/2043 | <All> | Microsoft ECC Prod...
Microsoft ECC TS Root Certificat... | Microsoft ECC TS Root Certificate ... | 2/27/2043 | <All> | Microsoft ECC TS Ro...
Microsoft Root Authority | Microsoft Root Authority | 12/31/2020 | <All> | Microsoft Root Aut...
Microsoft Root Certificate Autho... | Microsoft Root Certificate Authority | 5/10/2021 | <All> | Microsoft Root Certi...
Microsoft Root Certificate Autho... | Microsoft Root Certificate Authorit... | 6/24/2035 | <All> | Microsoft Root Certi...
Microsoft Root Certificate Autho... | Microsoft Root Certificate Authorit... | 3/23/2036 | <All> | Microsoft Root Certi...
NO LIABILITY ACCEPTED, (c)97 Ve... | NO LIABILITY ACCEPTED, (c)97 VeriS... | 1/8/2004 | Time Stamping | VeriSign Time Stam...
Symantec Enterprise Mobile Ro... | Symantec Enterprise Mobile Root f... | 3/15/2032 | Code Signing | <None>
Thawte Timestamping CA | Thawte Timestamping CA | 1/1/2021 | Time Stamping | Thawte Timestampi...
Actions
Certificates
More Actions
Trusted Root Certification Authorities store contains 18 certificates.
2:51 PM
3/23/2024

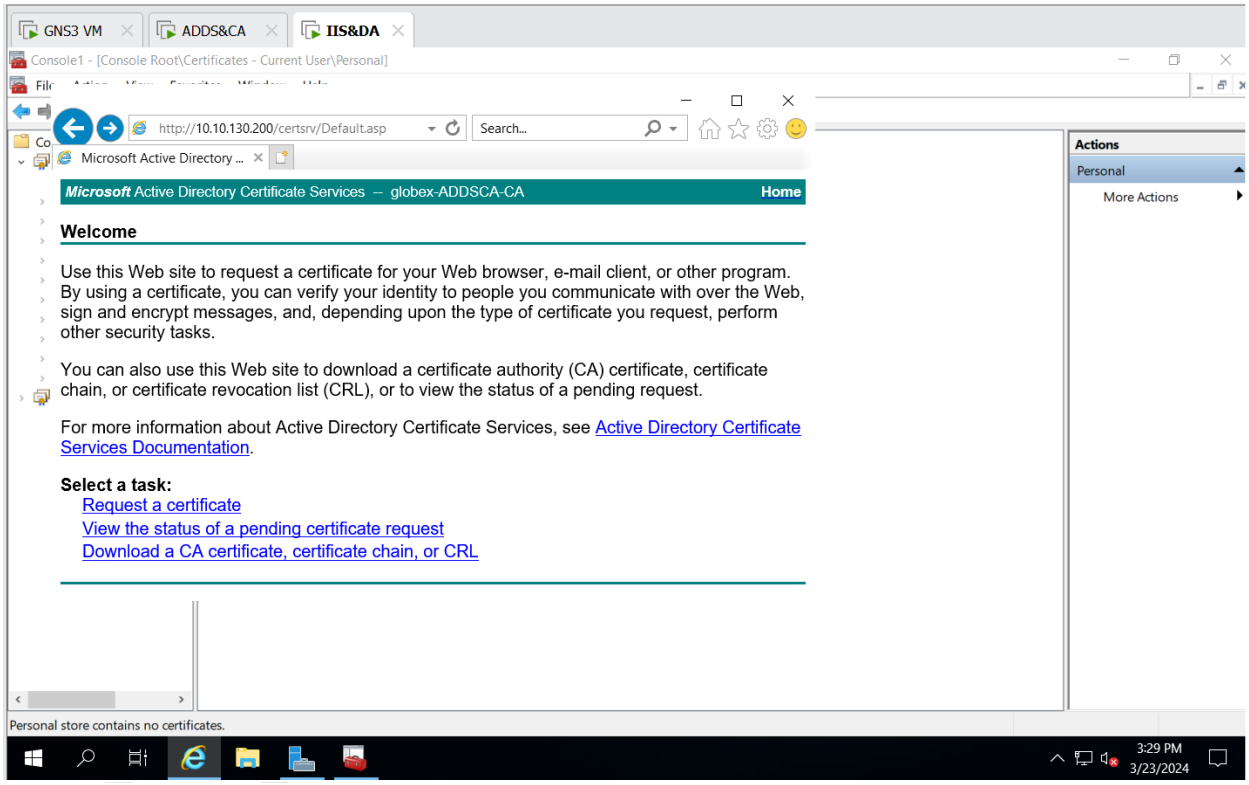
Steps for creating Custom Certificate:

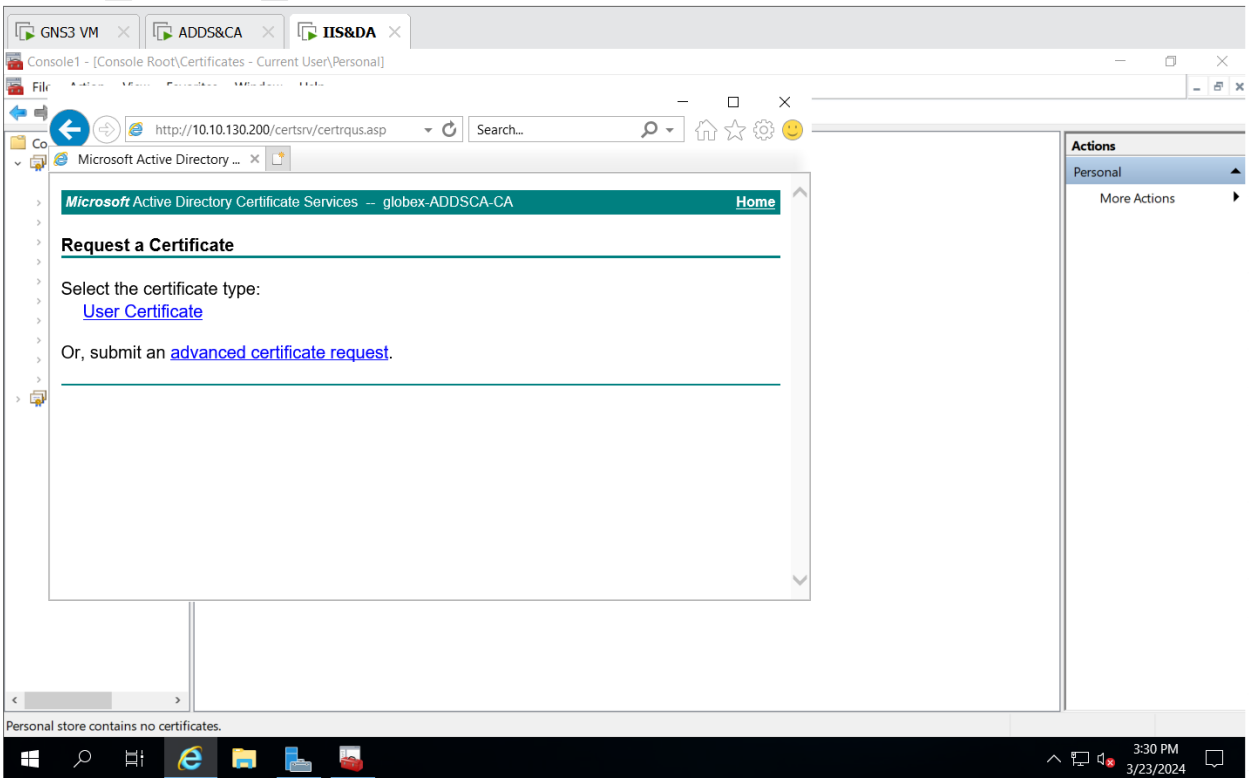


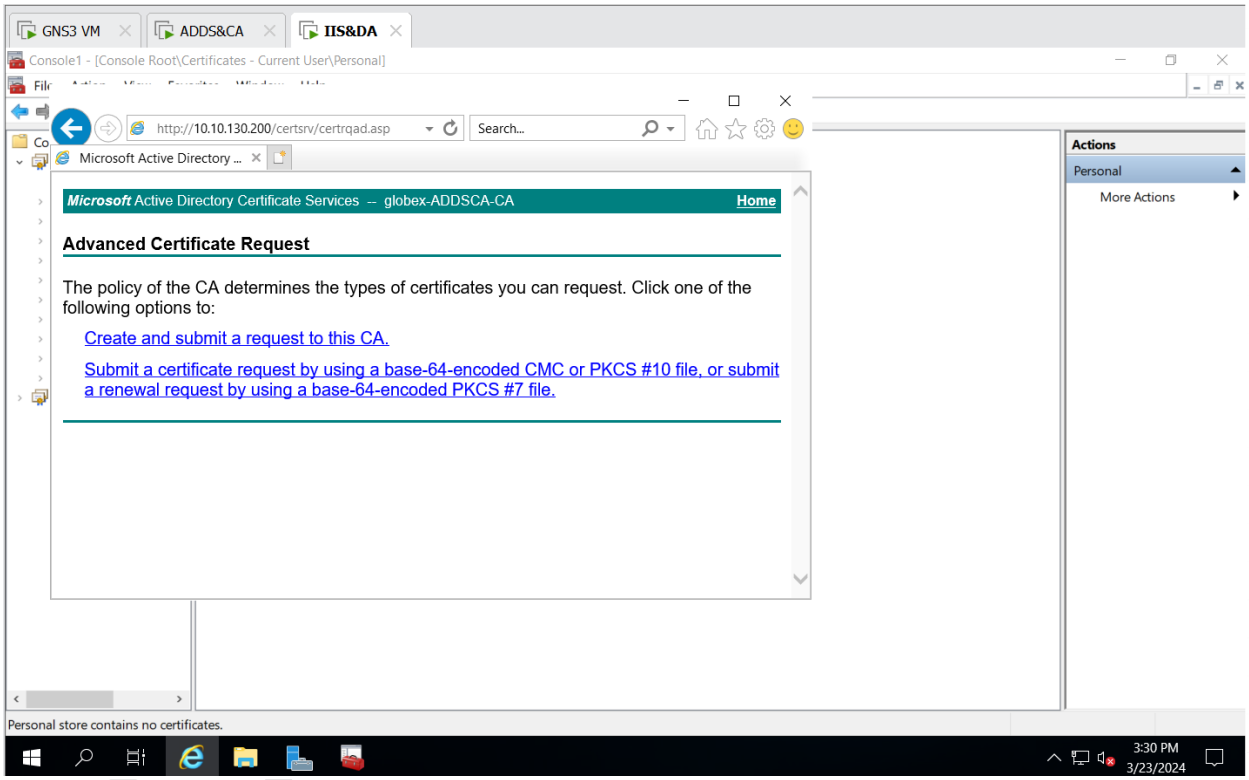


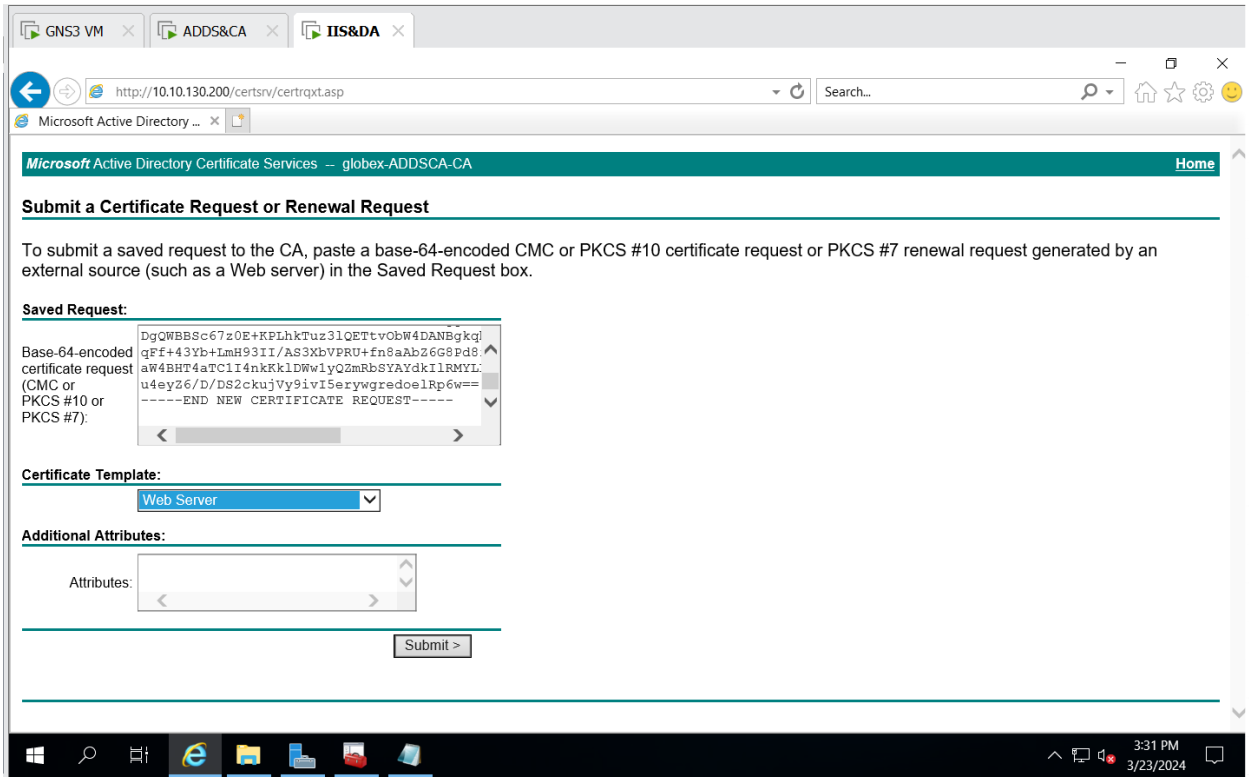

GNS3 VM
ADDS&CA
Console3 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Smart Card Trusted Roots
Certificates (Local Computer)
Certificate Properties
General Subject Extensions Private Key
Cryptographic Service Provider
Key options
Set the key length and export options for the private key.
Key size: 1024
Make private key exportable
Allow private key to be archived
Strong private key protection
Key type
Key usage defines the allowed uses for a private key associated with a certificate.
Exchange
Signature
OK
Cancel
Apply
Intended Purposes
File Recovery
Friendly
<None>
Actions
Certificates
More Actions
Details
Properties
Cancel
Personal store contains 1 certificate.
2:54 PM
3/23/2024

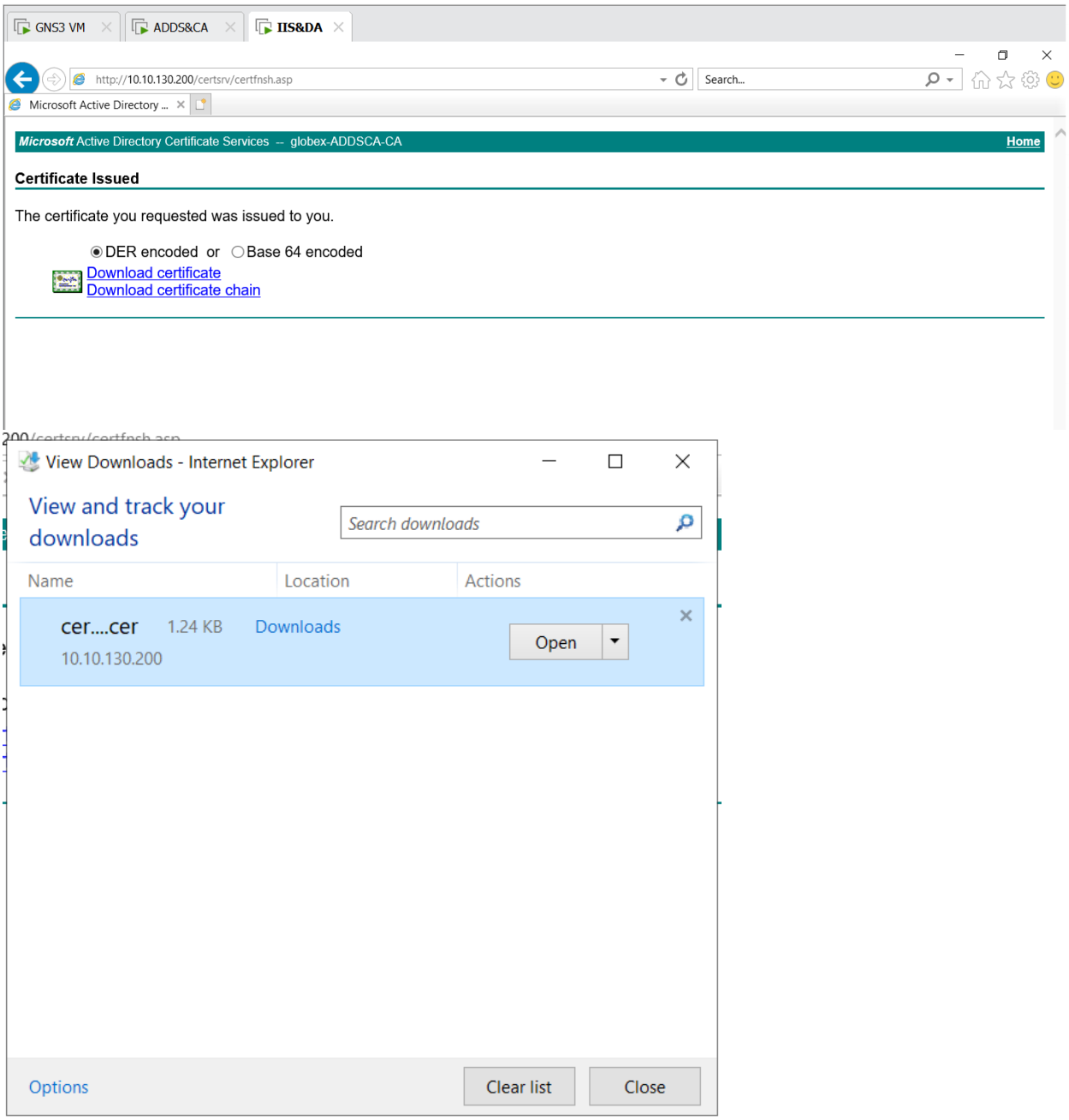

GNS3 VM
ADDS&CA
Console3 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Smart Card Trusted Roots
Certificates (Local Computer)
Certificate Properties
General Subject Extensions Private Key
The following are the certificate extensions for this certificate type.
Key usage
The key usage extension describes the purpose of a certificate.
Available options:
CRL signing
Data encipherment
Decipher only
Encipher only
Key agreement
Key encipherment
Non repudiation
Add >
< Remove
Selected options:
Digital signature
Key certificate signing
Make these key usages critical
Extended Key Usage (application policies)
Basic constraints
Include Symmetric algorithm
OK
Cancel
Apply
Intended Purposes
File Recovery
Friendly
<None>
Actions
Certificates
More Actions
Details
Properties
Cancel
Personal store contains 1 certificate.
2:55 PM
3/23/2024

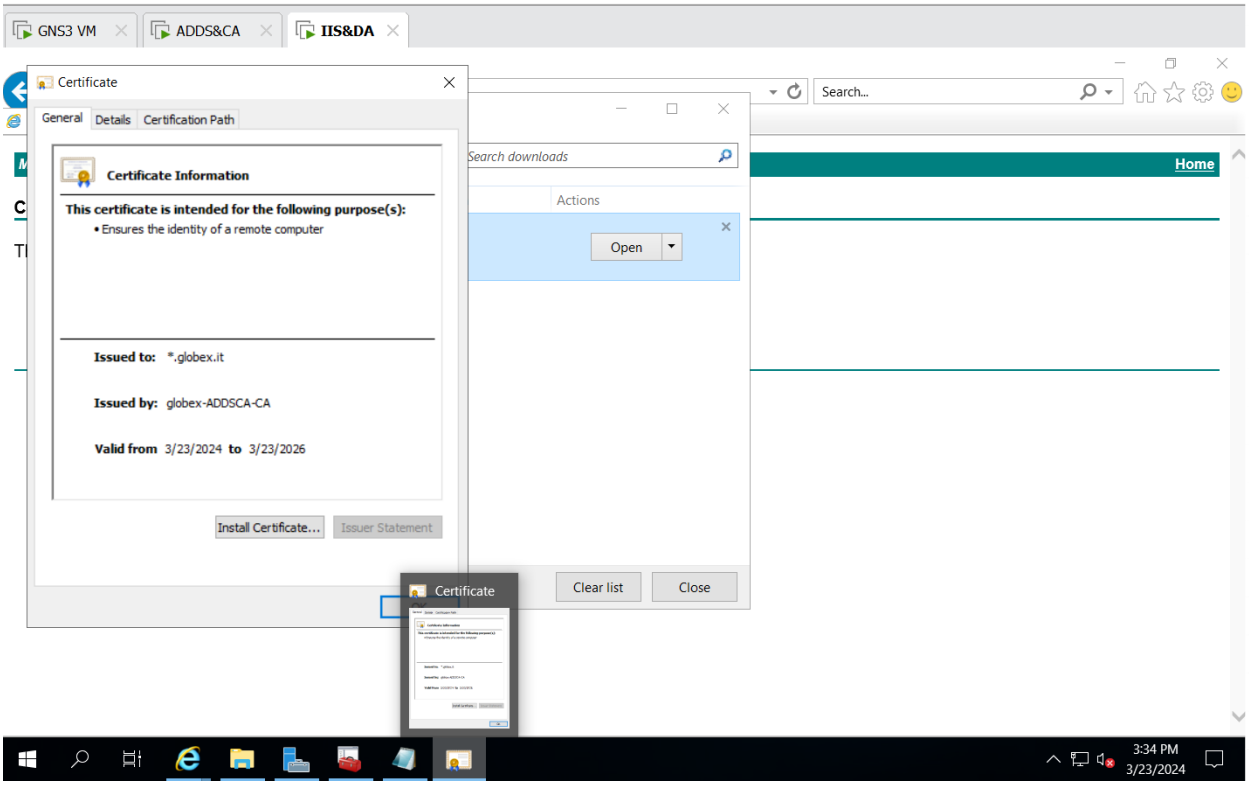

GNS3 VM
ADDS&CA
IIS&DA
Console1 - [Console Root\Certificates - Current User\Personal]
http://10.10.130.200/certsrv/Default.asp
Search...
Microsoft Active Directory ...
Microsoft Active Directory Certificate Services -- globex-ADDSCA-CA
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL
Actions
Personal
More Actions
Personal store contains no certificates.
3:29 PM
3/23/2024

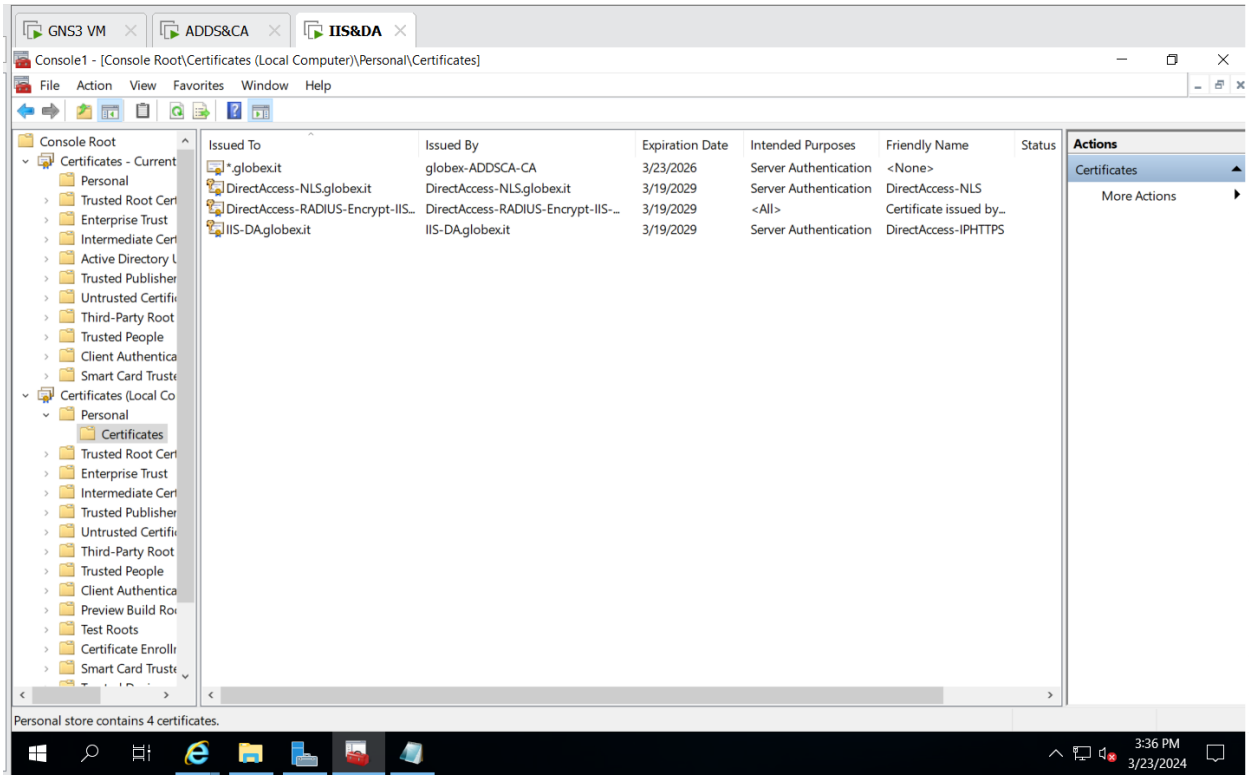

GNS3 VM
ADDS&CA
IIS&DA
Console1 - [Console Root\Certificates - Current User\Personal]
http://10.10.130.200/certsrv/certrqus.asp
Search...
Microsoft Active Directory ...
Microsoft Active Directory Certificate Services -- globex-ADDSCA-CA
Home
Request a Certificate
Select the certificate type:
User Certificate
Or, submit an advanced certificate request.
Actions
Personal
More Actions
Personal store contains no certificates.
3:30 PM
3/23/2024


GNS3 VM
ADDS&CA
IIS&DA
Console1 - [Console Root\Certificates - Current User\Personal]
http://10.10.130.200/certsrv/certrqad.asp
Search...
Microsoft Active Directory ...
Actions
Personal
More Actions
Microsoft Active Directory Certificate Services -- globex-ADDSCA-CA
Home
Advanced Certificate Request
The policy of the CA determines the types of certificates you can request. Click one of the following options to:
Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
Personal store contains no certificates.
3:30 PM
3/23/2024

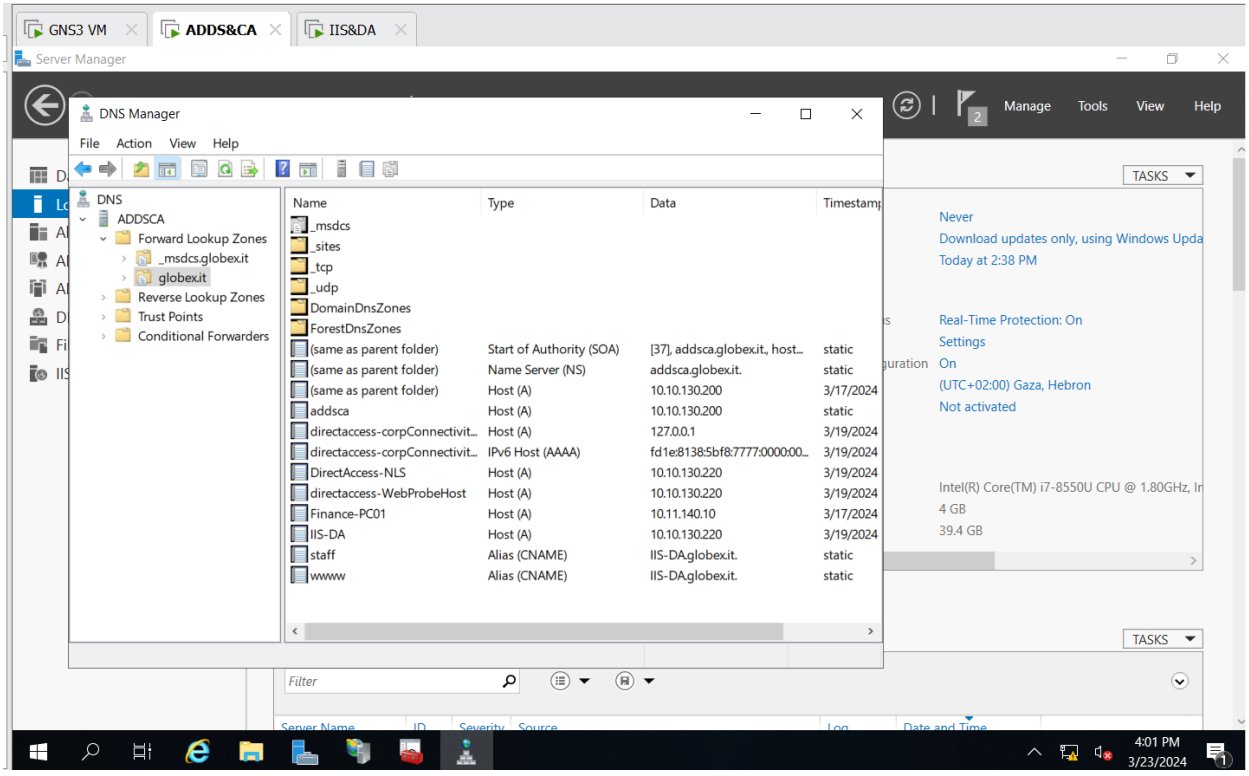

GNS3 VM
ADDS&CA
IIS&DA
http://10.10.130.200/certsrv/certrqxt.asp
Search...
Microsoft Active Directory ...
Microsoft Active Directory Certificate Services -- globex-ADDSCA-CA
Home
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.
Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
DgQWBBSc67z0E+KPLhkTuz3lQETtvObW4DANBgkq
qFf+43Yb+LmH93II/AS3XbVPRU+fn8aAbZ6G8Pd8
aW4BHT4aTC1I4nkKklDWw1yQZmRbSYAYdkIlRMYL
u4eyZ6/D/DS2ckujVy9ivI5erywgredoelRp6w==
-----END NEW CERTIFICATE REQUEST-----
Certificate Template:
Web Server
Additional Attributes:
Attributes:
Submit >
3:31 PM
3/23/2024

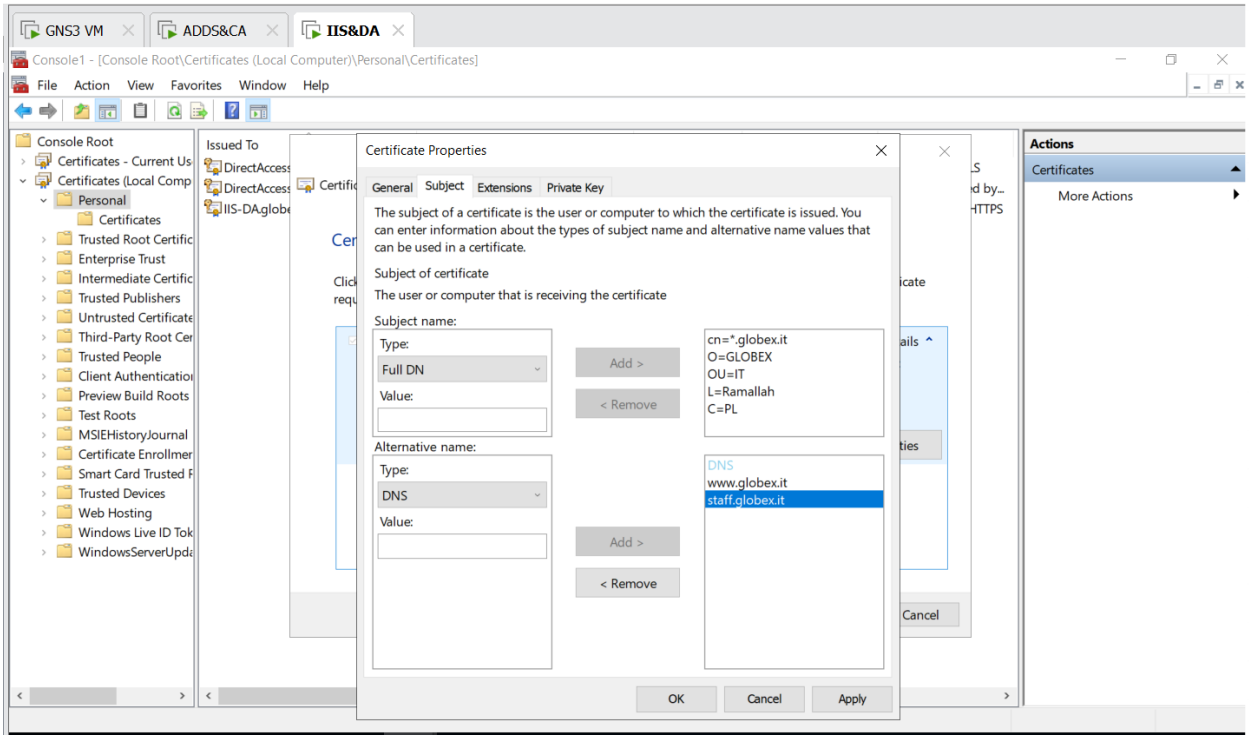

GNS3 VM
ADDS&CA
IIS&DA
http://10.10.130.200/certsrv/certfnsh.asp
Search...
Microsoft Active Directory ...
Microsoft Active Directory Certificate Services -- globex-ADDSCA-CA
Home
Certificate Issued
The certificate you requested was issued to you.
DER encoded or Base 64 encoded
Download certificate
Download certificate chain
View Downloads - Internet Explorer
View and track your downloads
Search downloads
Name
Location
Actions
cer....cer
1.24 KB
Downloads
10.10.130.200
Open
Options
Clear list
Close


GNS3 VM
ADDS&CA
IIS&DA
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
Issued to: *.globex.it
Issued by: globex-ADDSCA-CA
Valid from 3/23/2024 to 3/23/2026
Install Certificate...
Issuer Statement
Search downloads
Actions
Open
Clear list
Close
Search...
Home
3:34 PM
3/23/2024


GNS3 VM
ADDS&CA
IIS&DA
Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current
Personal
Certificates
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
Status
*.globex.it
globex-ADDSCA-CA
3/23/2026
Server Authentication
<None>
DirectAccess-NLS.globex.it
DirectAccess-NLS.globex.it
3/19/2029
Server Authentication
DirectAccess-NLS
DirectAccess-RADIUS-Encrypt-IIS...
DirectAccess-RADIUS-Encrypt-IIS-...
3/19/2029
<All>
Certificate issued by...
IIS-DA.globex.it
IIS-DA.globex.it
3/19/2029
Server Authentication
DirectAccess-IPHTTPS
Actions
Certificates
More Actions
Personal store contains 4 certificates.
3:36 PM
3/23/2024

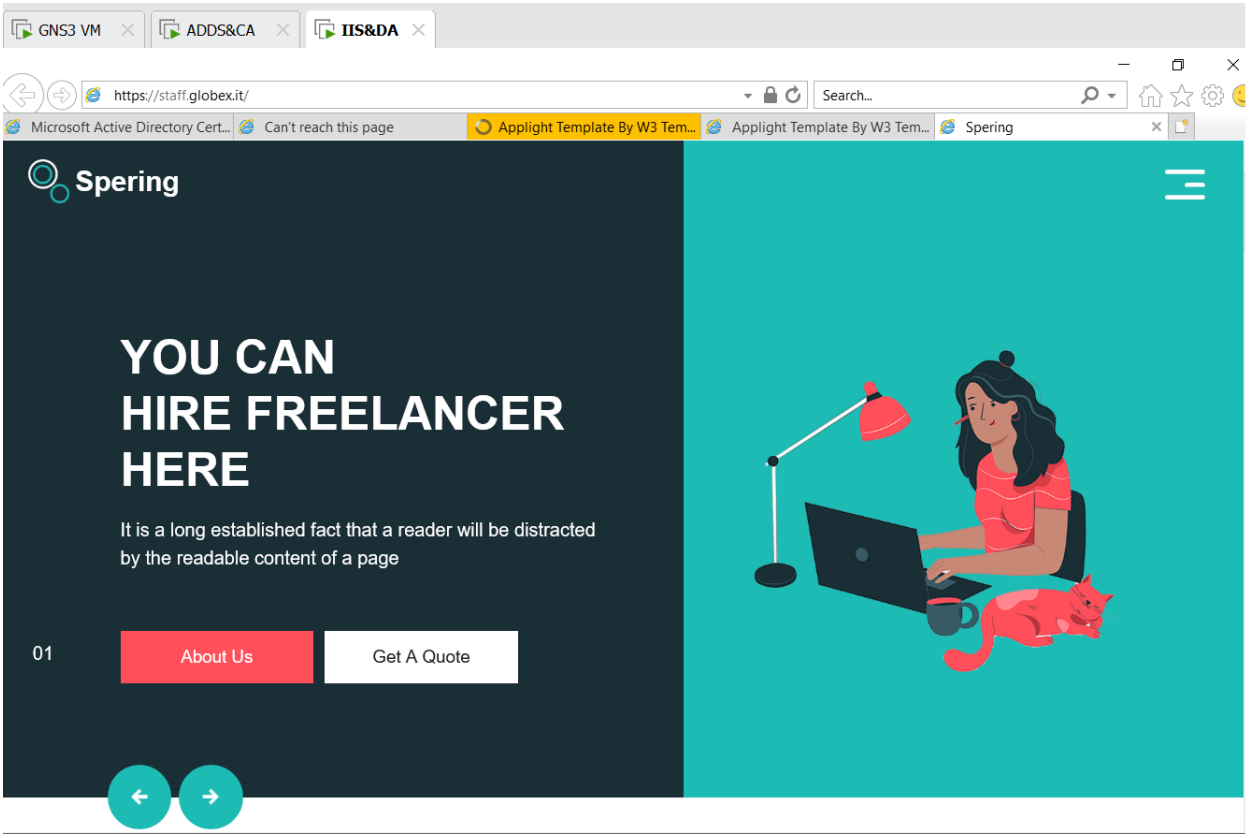
Creating DNS records for the websites



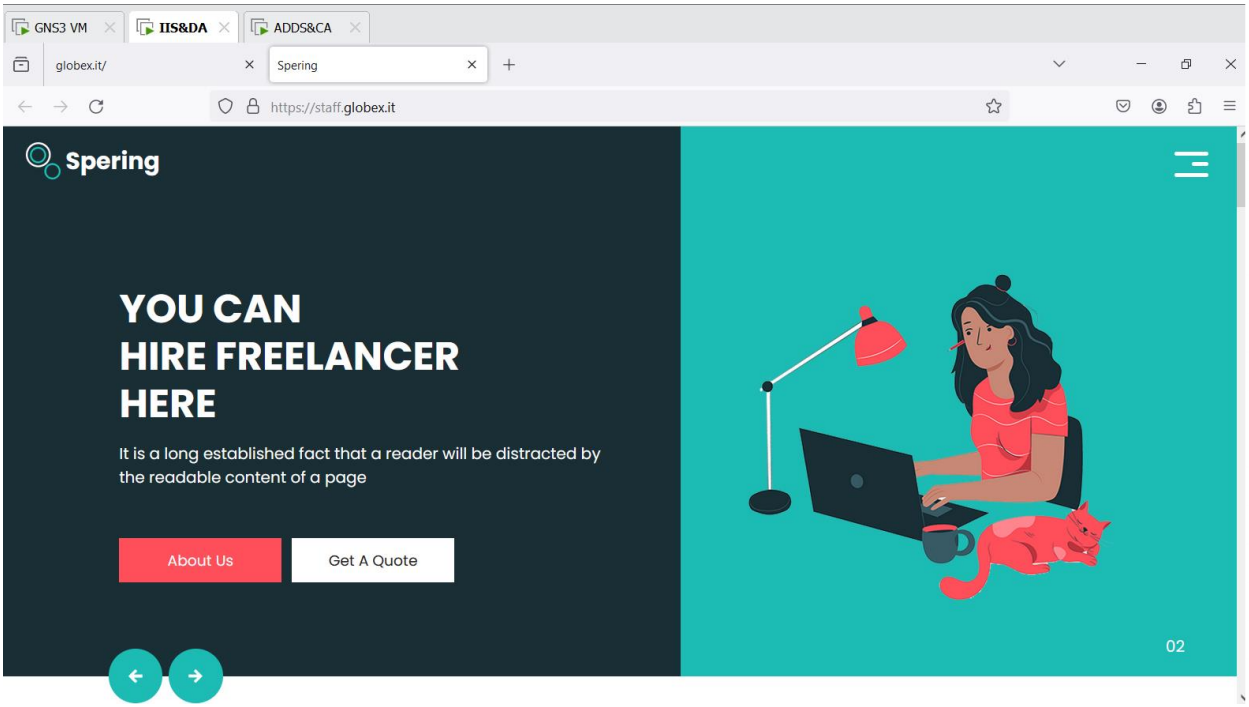


https://staff.globex.it

Websites using HTTPS certificates (internet explorer).

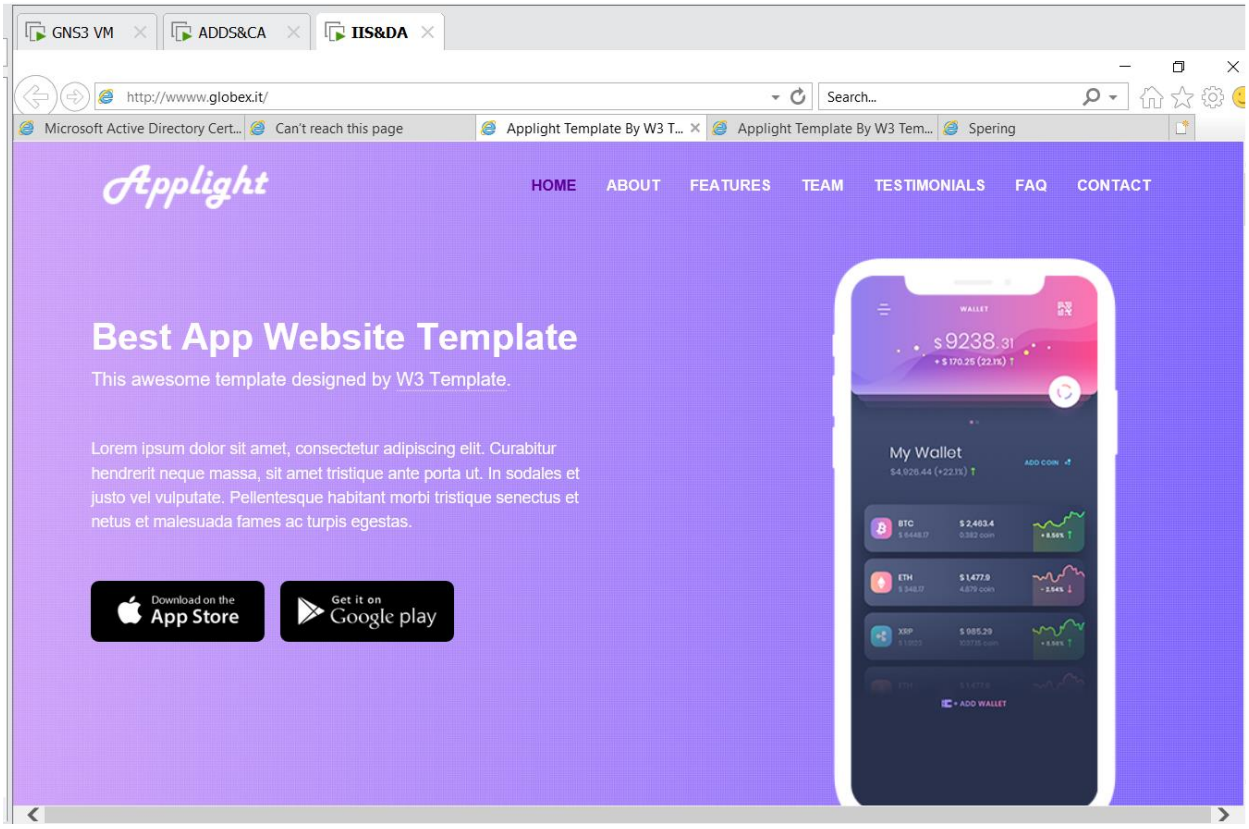


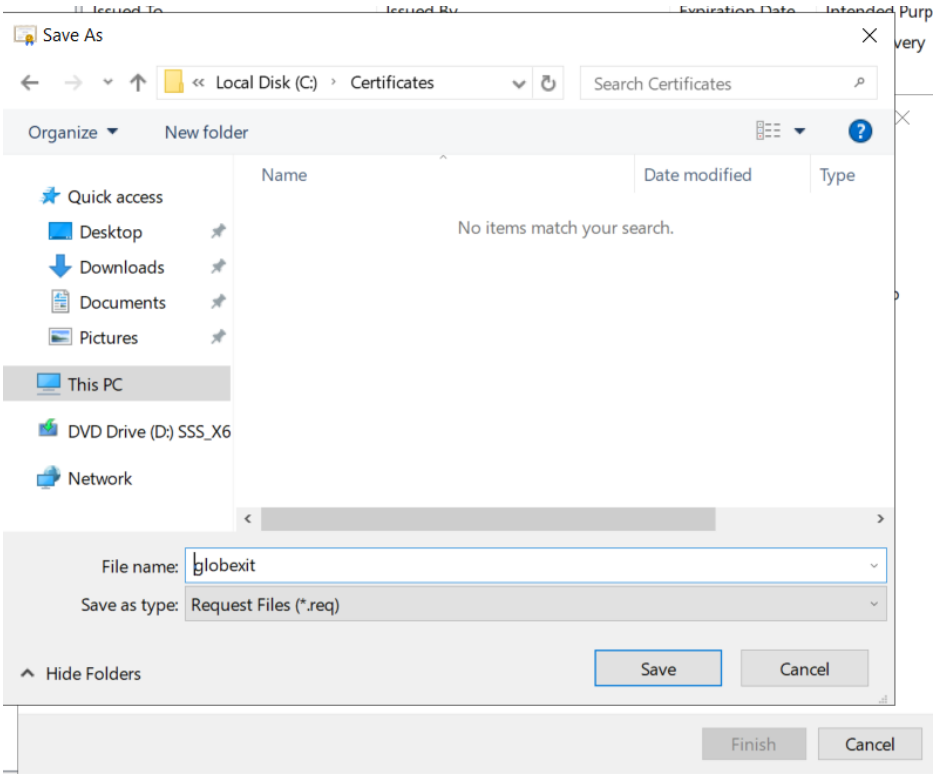
Website https working properly on Firefox.



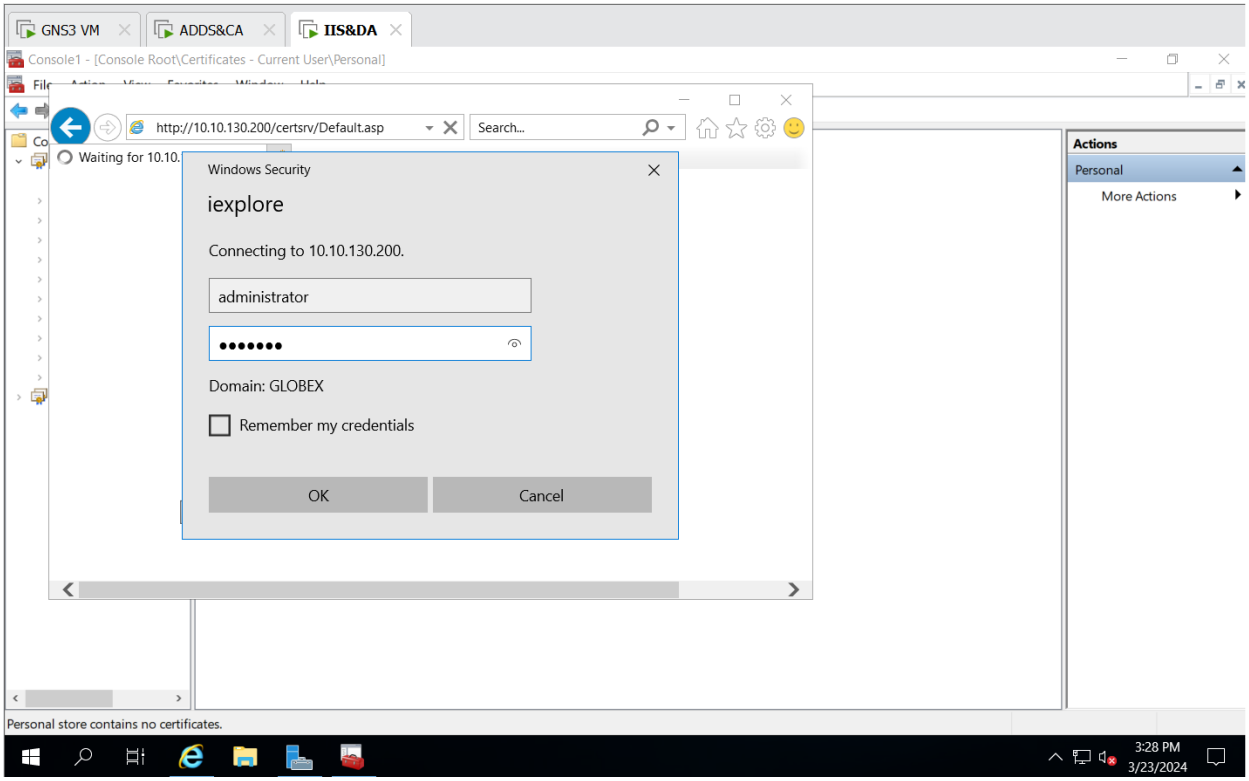
https://www.globex.it

1. Internet explorer



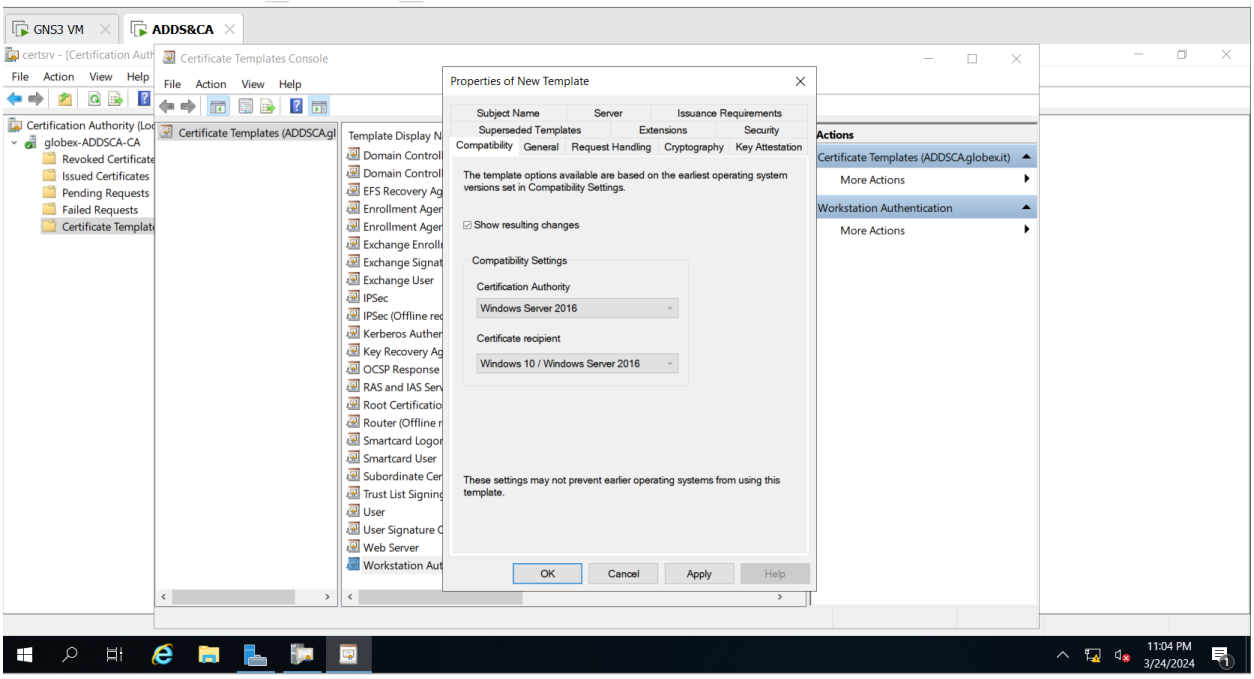


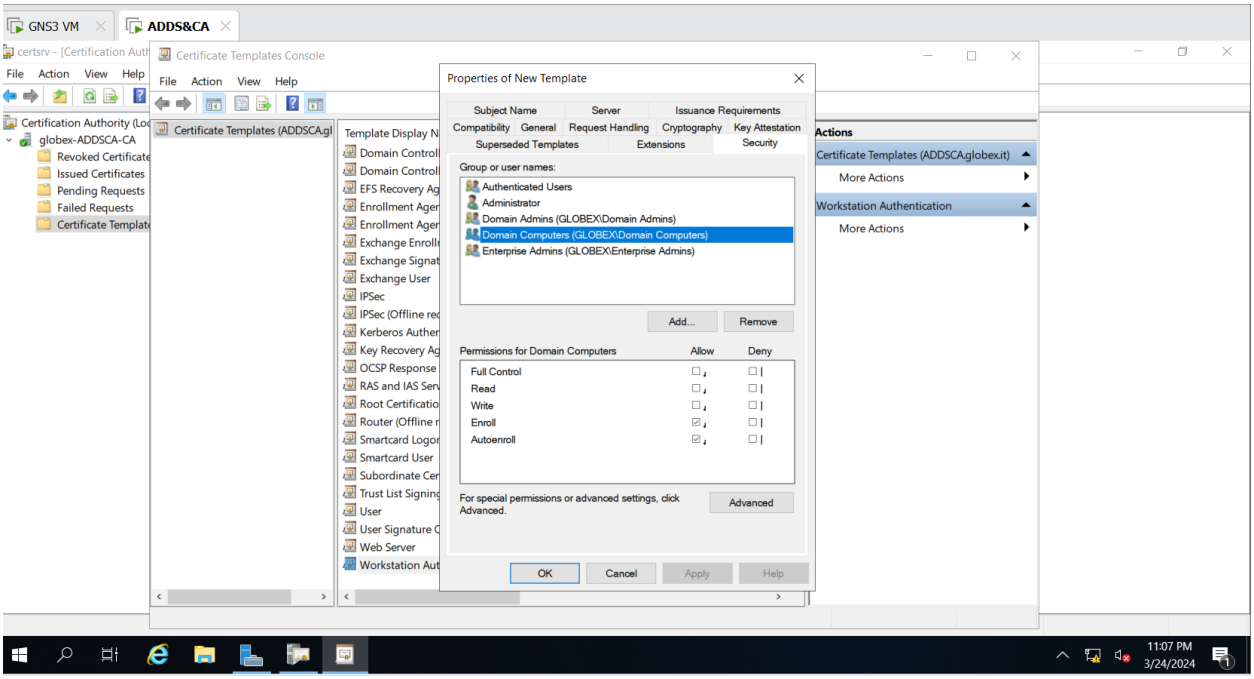
Open certificate Authority from IIS using

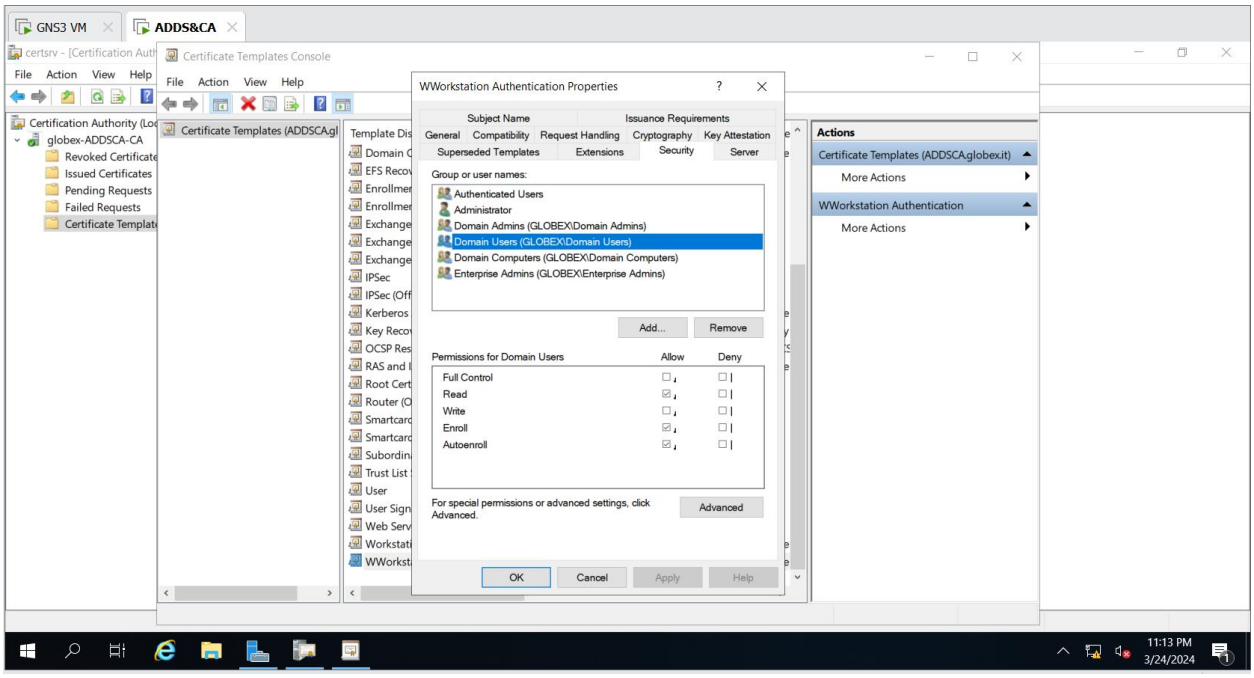


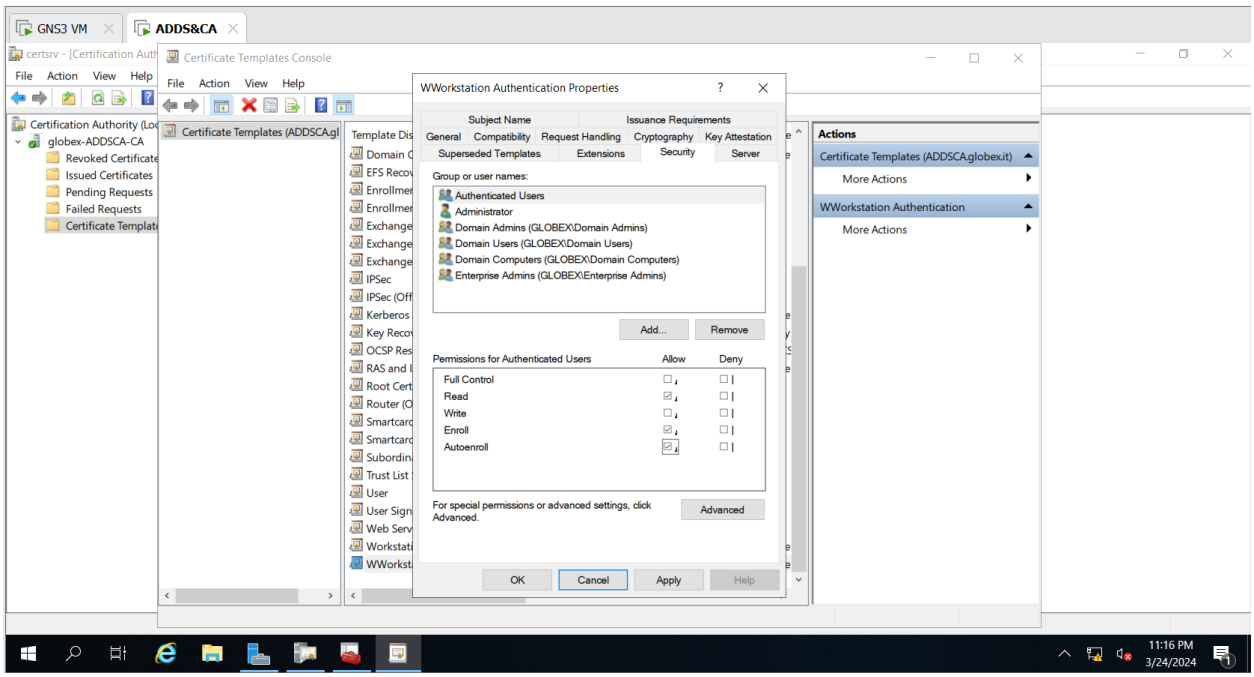
Workstation Communication CA

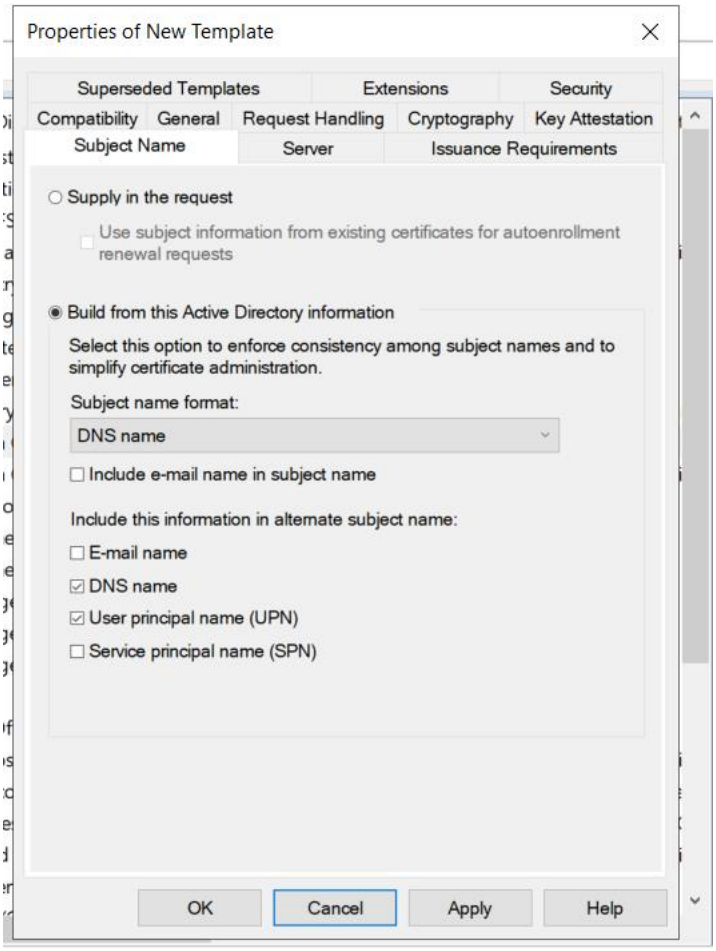
- We added another certificate from CA by duplicating the Workstation certificate and modifying the settings like in the pictures (compatibility settings, security settings enrolment, and DNS settings) , then we issue a certificate using Microsoft management console MMC. The steps also apply for Domain Controller certificates.

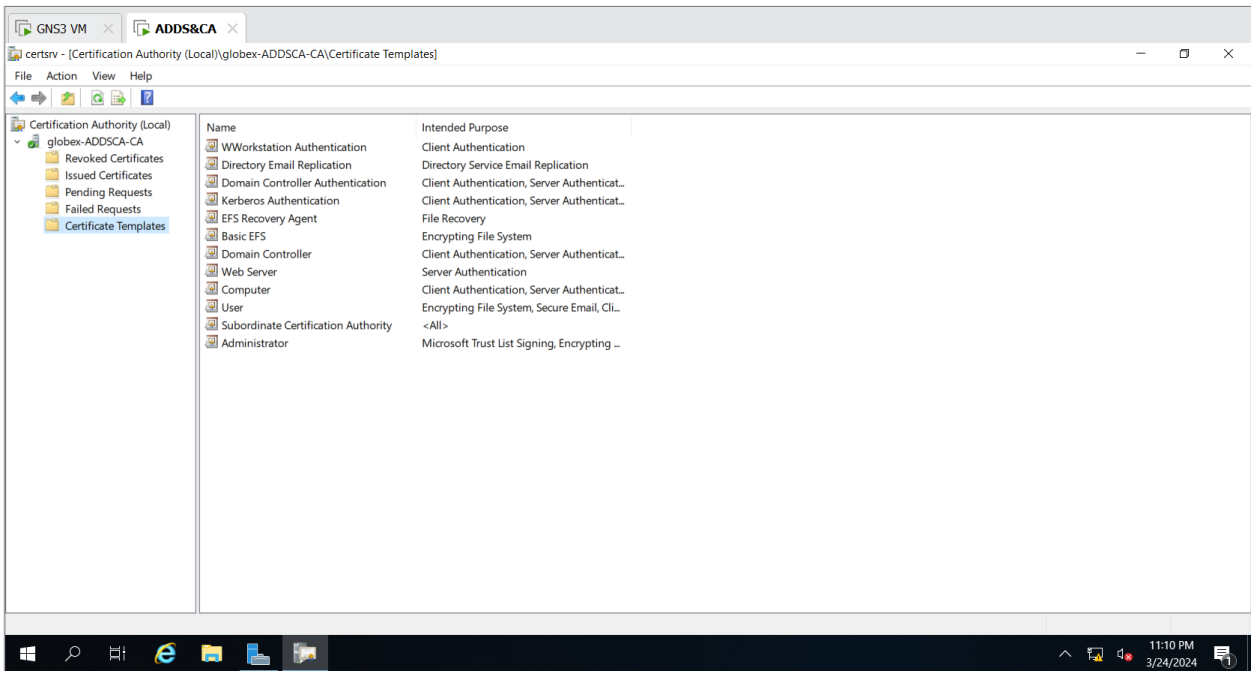


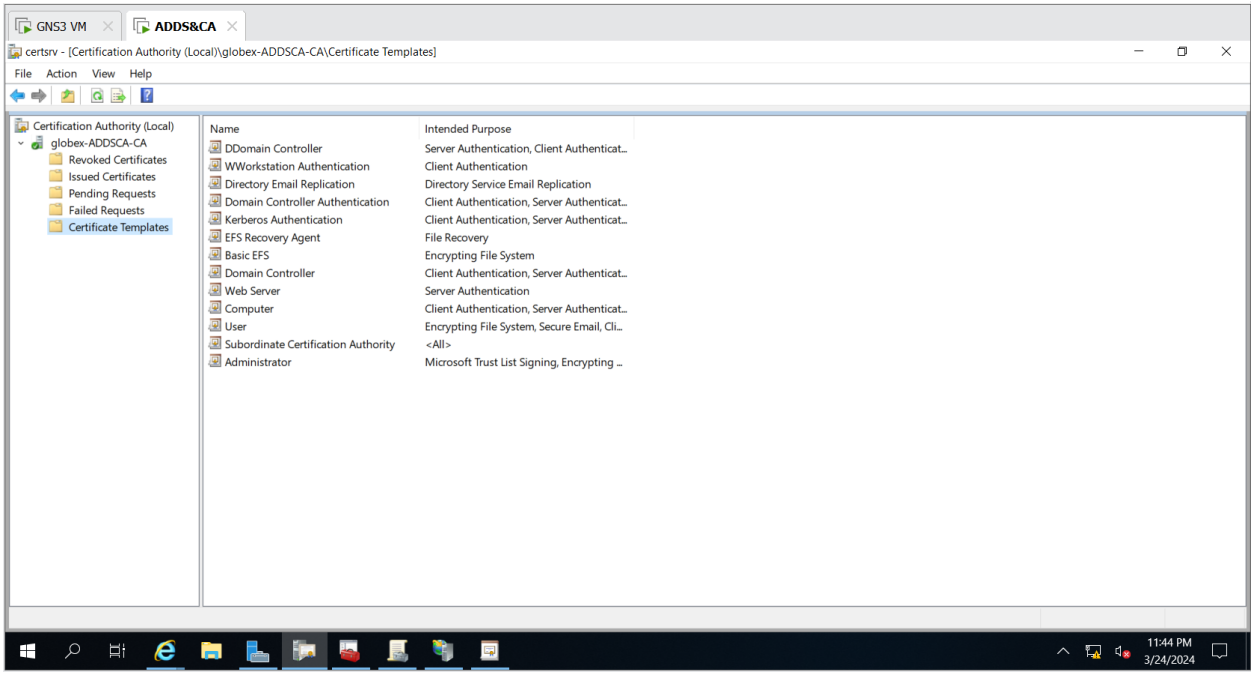


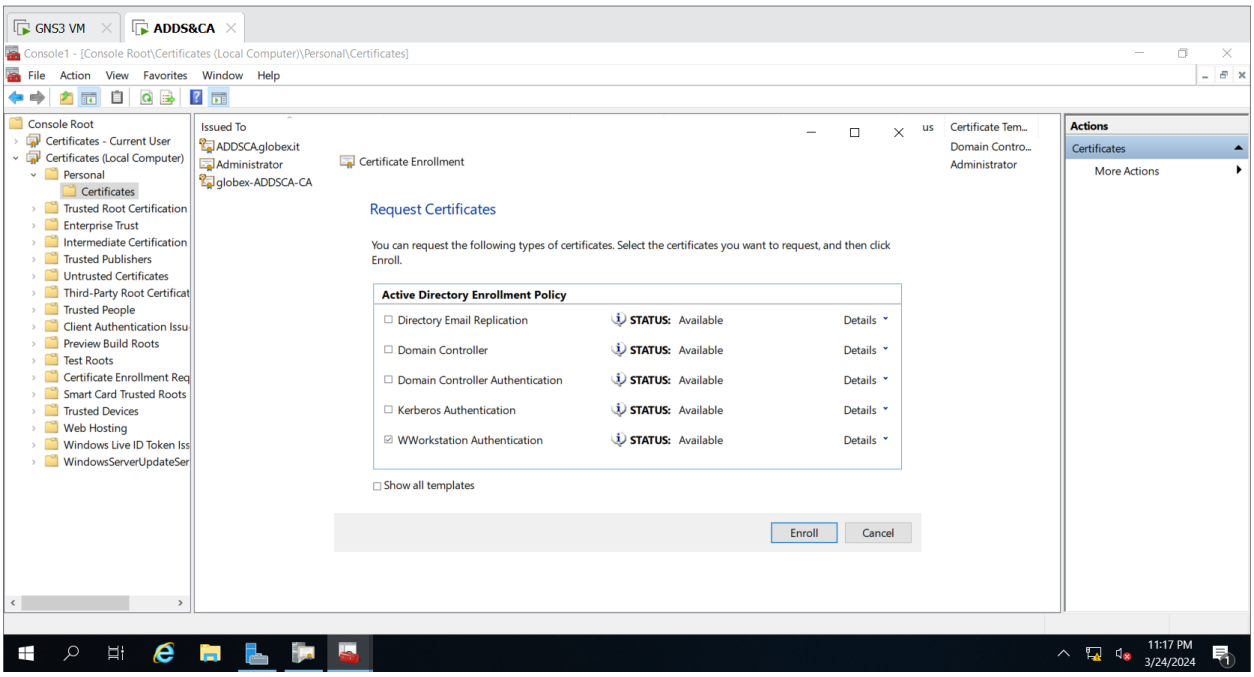

GNS3 VM
ADDS&CA
Certificate Templates Console
File Action View Help
WWorkstation Authentication Properties
Subject Name
Issuance Requirements
General Compatibility Request Handling Cryptography Key Attestation
Superseded Templates Extensions Security Server
Group or user names:
Authenticated Users
Administrator
Domain Admins (GLOBEX\Domain Admins)
Domain Users (GLOBEX\Domain Users)
Domain Computers (GLOBEX\Domain Computers)
Enterprise Admins (GLOBEX\Enterprise Admins)
Add... Remove
Permissions for Domain Users Allow Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply Help
Actions
Certificate Templates (ADDSCA.globex.it)
More Actions
WWorkstation Authentication
More Actions
11:13 PM
3/24/2024

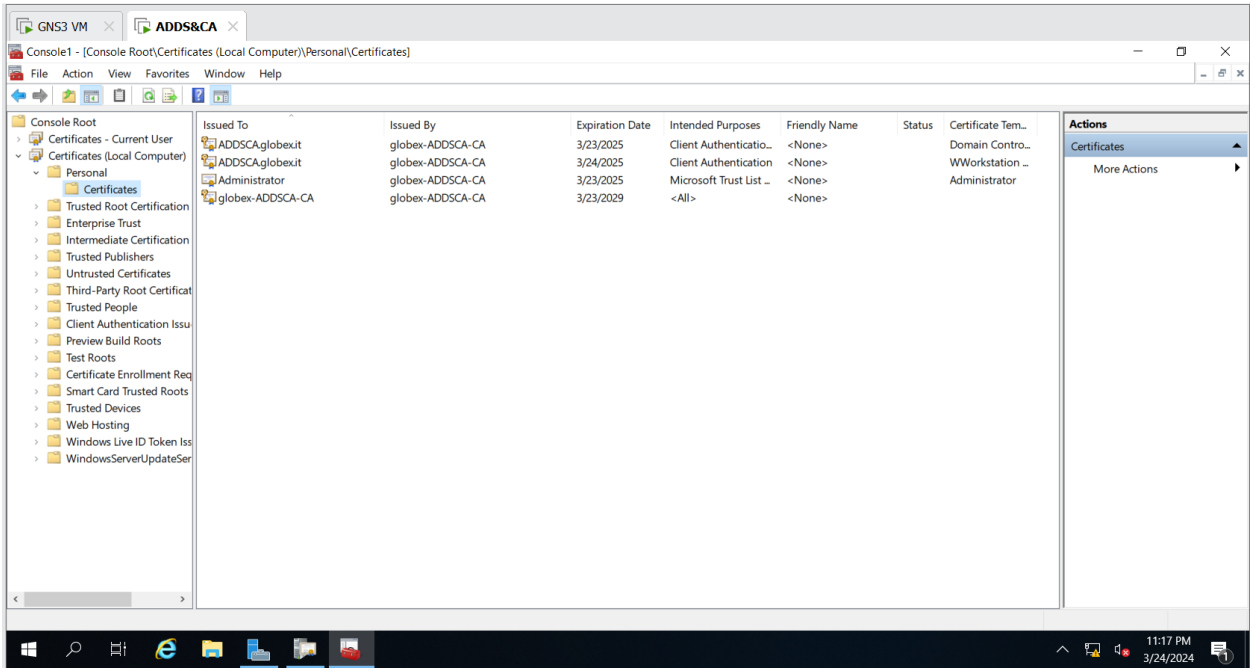

GNS3 VM
ADDS&CA
Certificate Templates Console
File Action View Help
WWorkstation Authentication Properties
Subject Name
Issuance Requirements
General Compatibility Request Handling Cryptography Key Attestation
Superseded Templates Extensions Security Server
Group or user names:
Authenticated Users
Administrator
Domain Admins (GLOBEX\Domain Admins)
Domain Users (GLOBEX\Domain Users)
Domain Computers (GLOBEX\Domain Computers)
Enterprise Admins (GLOBEX\Enterprise Admins)
Add... Remove
Permissions for Authenticated Users Allow Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK Cancel Apply Help
Actions
Certificate Templates (ADDSCA.globex.it)
More Actions
WWorkstation Authentication
More Actions
11:16 PM
3/24/2024

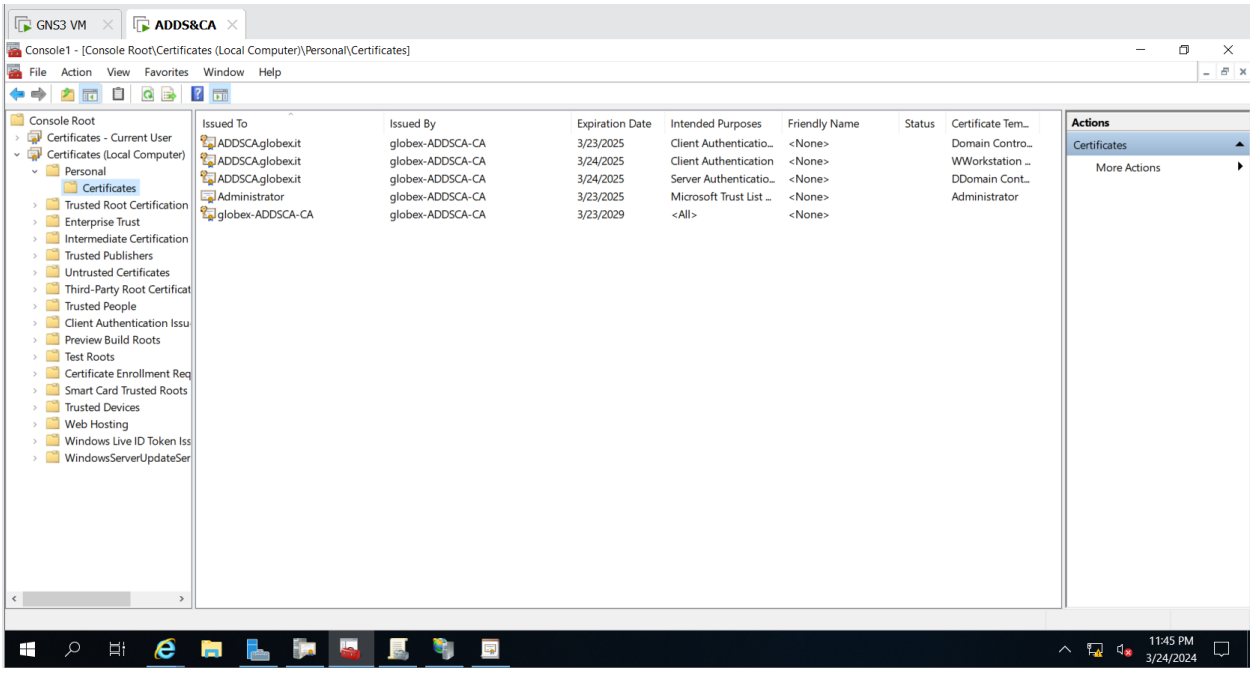

Properties of New Template
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Supply in the request
Use subject information from existing certificates for autoenrollment renewal requests
Build from this Active Directory information
Select this option to enforce consistency among subject names and to simplify certificate administration.
Subject name format:
DNS name
Include e-mail name in subject name
Include this information in alternate subject name:
E-mail name
DNS name
User principal name (UPN)
Service principal name (SPN)
OK
Cancel
Apply
Help

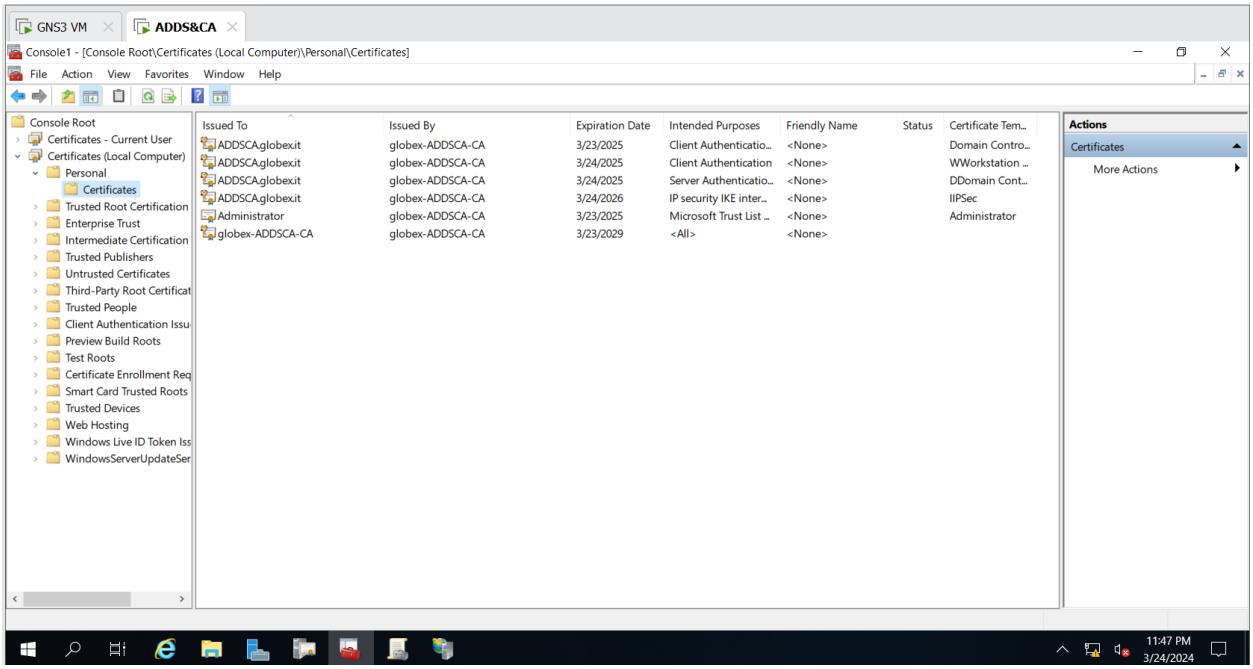

GNS3 VM
ADDS&CA
certsrv - [Certification Authority (Local)\globex-ADDSCA-CA\Certificate Templates]
File
Action
View
Help
Certification Authority (Local)
globex-ADDSCA-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended Purpose
WWorkstation Authentication
Client Authentication
Directory Email Replication
Directory Service Email Replication
Domain Controller Authentication
Client Authentication, Server Authenticat...
Kerberos Authentication
Client Authentication, Server Authenticat...
EFS Recovery Agent
File Recovery
Basic EFS
Encrypting File System
Domain Controller
Client Authentication, Server Authenticat...
Web Server
Server Authentication
Computer
Client Authentication, Server Authenticat...
User
Encrypting File System, Secure Email, Cli...
Subordinate Certification Authority
<All>
Administrator
Microsoft Trust List Signing, Encrypting ...
11:10 PM
3/24/2024


GNS3 VM
ADDS&CA
certsrv - [Certification Authority (Local)\globex-ADDSCA-CA\Certificate Templates]
File Action View Help
Certification Authority (Local)
globex-ADDSCA-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended Purpose
DDomain Controller
Server Authentication, Client Authenticat...
WWorkstation Authentication
Client Authentication
Directory Email Replication
Directory Service Email Replication
Domain Controller Authentication
Client Authentication, Server Authenticat...
Kerberos Authentication
Client Authentication, Server Authenticat...
EFS Recovery Agent
File Recovery
Basic EFS
Encrypting File System
Domain Controller
Client Authentication, Server Authenticat...
Web Server
Server Authentication
Computer
Client Authentication, Server Authenticat...
User
Encrypting File System, Secure Email, Cli...
Subordinate Certification Authority
<All>
Administrator
Microsoft Trust List Signing, Encrypting ...
11:44 PM
3/24/2024


GNS3 VM
ADDS&CA
Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issu
Preview Build Roots
Test Roots
Certificate Enrollment Req
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Iss
WindowsServerUpdateSer
Issued To
ADDSCA.globex.it
Administrator
globex-ADDSCA-CA
Certificate Enrollment
Certificate Tem...
Domain Contro...
Administrator
Request Certificates
You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.
Active Directory Enrollment Policy
Directory Email Replication
STATUS: Available
Details
Domain Controller
STATUS: Available
Details
Domain Controller Authentication
STATUS: Available
Details
Kerberos Authentication
STATUS: Available
Details
WWorkstation Authentication
STATUS: Available
Details
Show all templates
Enroll
Cancel
Actions
Certificates
More Actions
11:17 PM
3/24/2024


GNS3 VM
ADDS&CA
Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issu
Preview Build Roots
Test Roots
Certificate Enrollment Req
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Iss
WindowsServerUpdateSer
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
Status
Certificate Tem...
ADDSCA.globex.it
globex-ADDSCA-CA
3/23/2025
Client Authenticatio...
<None>
Domain Contro...
ADDSCA.globex.it
globex-ADDSCA-CA
3/24/2025
Client Authentication
<None>
WWorkstation ...
Administrator
globex-ADDSCA-CA
3/23/2025
Microsoft Trust List ...
<None>
Administrator
globex-ADDSCA-CA
globex-ADDSCA-CA
3/23/2029
<All>
<None>
Actions
Certificates
More Actions
11:17 PM
3/24/2024

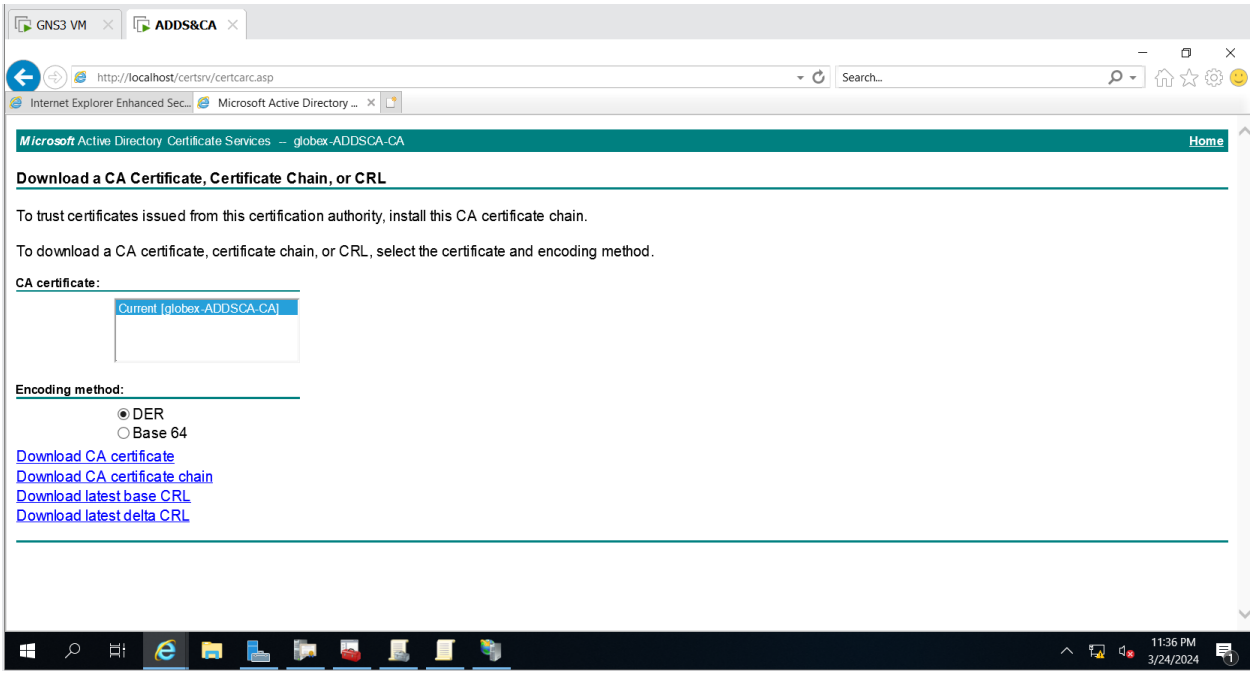

GNS3 VM
ADDS&CA
Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issu
Preview Build Roots
Test Roots
Certificate Enrollment Req
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Iss
WindowsServerUpdateSer
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
Status
Certificate Tem...
ADDSCA.globex.it
globex-ADDSCA-CA
3/23/2025
Client Authenticatio...
<None>
Domain Contro...
ADDSCA.globex.it
globex-ADDSCA-CA
3/24/2025
Client Authentication
<None>
WWorkstation ...
ADDSCA.globex.it
globex-ADDSCA-CA
3/24/2025
Server Authenticatio...
<None>
DDomain Cont...
Administrator
globex-ADDSCA-CA
3/23/2025
Microsoft Trust List ...
<None>
Administrator
globex-ADDSCA-CA
globex-ADDSCA-CA
3/23/2029
<All>
<None>
Actions
Certificates
More Actions
11:45 PM
3/24/2024

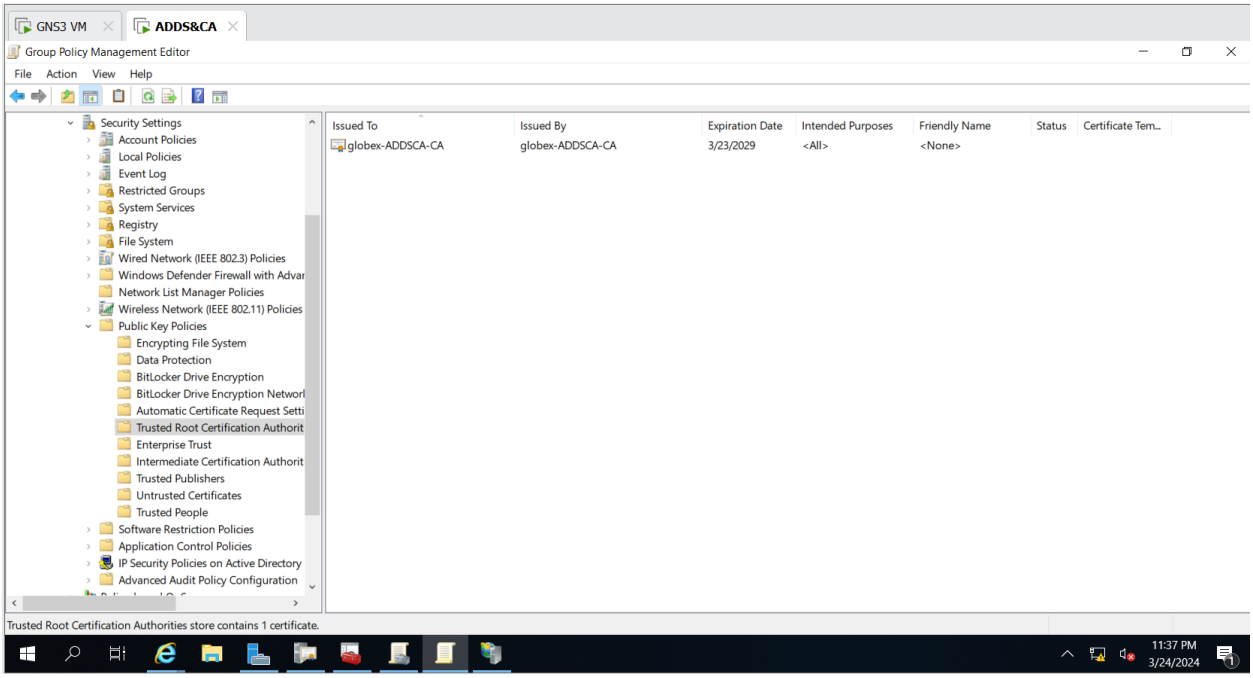


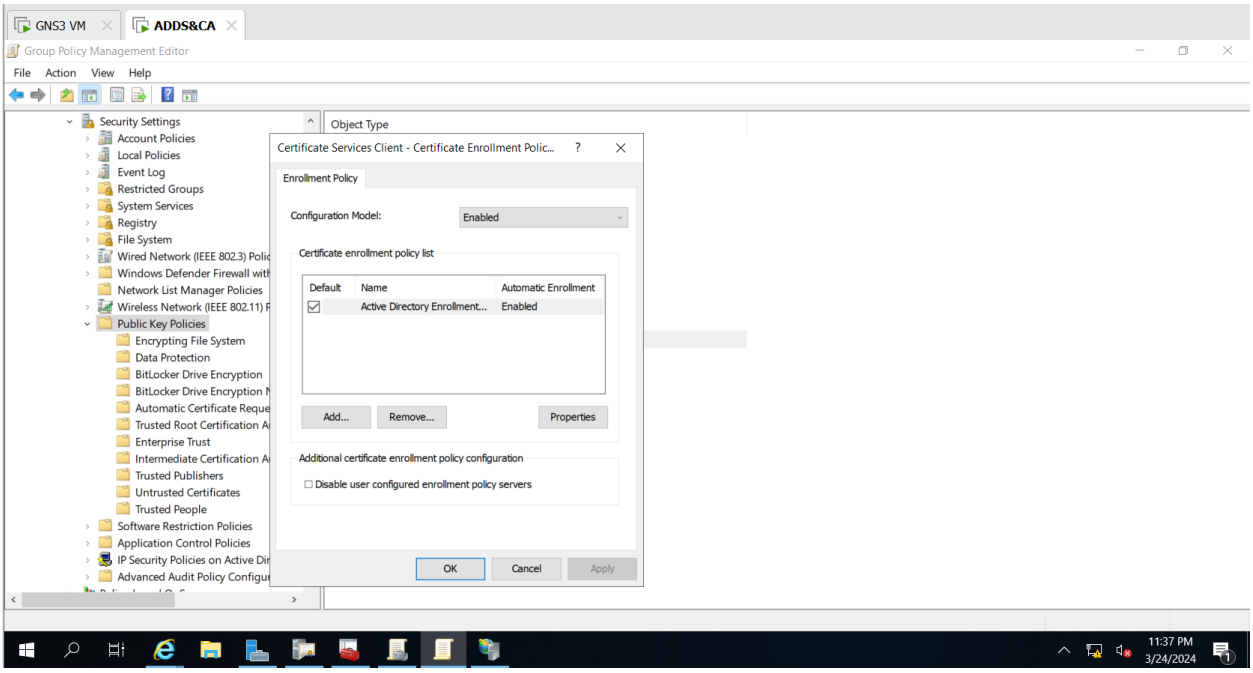
Add Group Policy to distribute certificate.

First I downloaded the main certificate on the ADDS server to be placed in the group policy and distributed to clients.

Path: Public Key Policies → trusted root certification authority → Enrollment Policy.

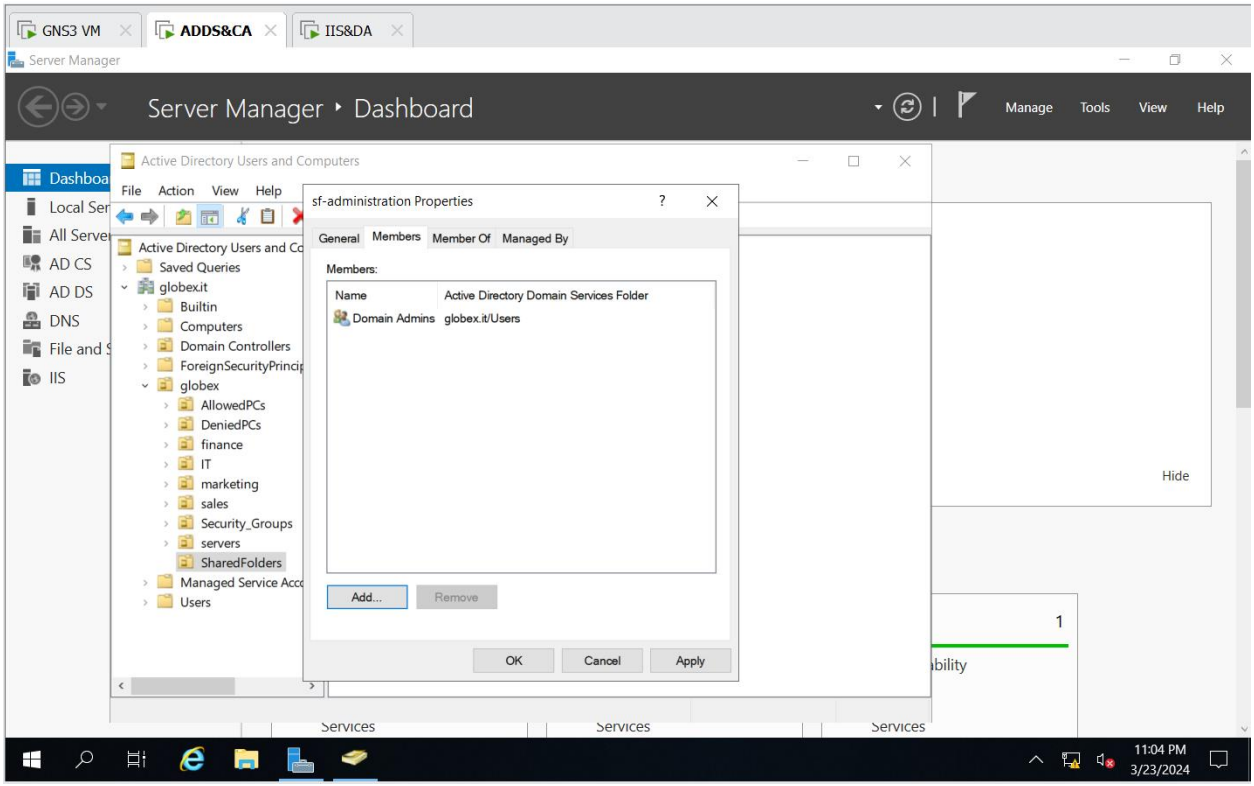


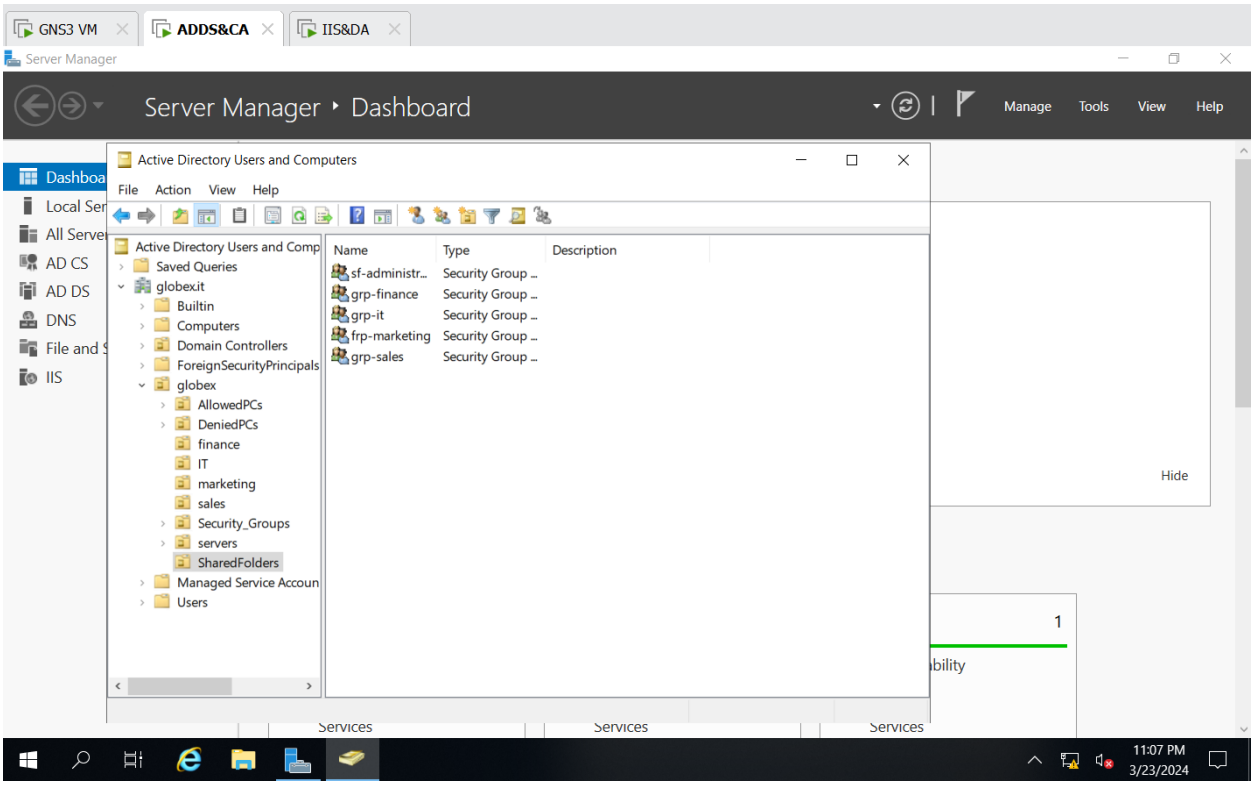




Shared folders

First, I created a OU for shared folders, and added a group for each department, and one for the administration.


GNS3 VM
ADDS&CA
IIS&DA
Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Active Directory Users and Computers
File Action View Help
sf-administration Properties
General Members Member Of Managed By
Members:
Name
Active Directory Domain Services Folder
Domain Admins
globex.it/Users
Add...
Remove
OK
Cancel
Apply
Active Directory Users and Co
Saved Queries
globex.it
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
globex
AllowedPCs
DeniedPCs
finance
IT
marketing
sales
Security_Groups
servers
SharedFolders
Managed Service Acc
Users
Dashboa
Local Ser
All Server
AD CS
AD DS
DNS
File and S
IIS
Hide
1
Services
Services
Services
11:04 PM
3/23/2024


GNS3 VM
ADDS&CA
IIS&DA
Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Active Directory Users and Computers
File Action View Help
Active Directory Users and Comp
Saved Queries
globex.it
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
globex
AllowedPCs
DeniedPCs
finance
IT
marketing
sales
Security_Groups
servers
SharedFolders
Managed Service Accoun
Users
Name
Type
Description
sf-administr...
Security Group ...
grp-finance
Security Group ...
grp-it
Security Group ...
frp-marketing
Security Group ...
grp-sales
Security Group ...
Dashboa
Local Ser
All Server
AD CS
AD DS
DNS
File and S
IIS
Hide
1
Services
Services
Services
11:07 PM
3/23/2024

Step two: for each created folder, I updated the owner to sf_administration group, disable inheritance, and add a certain group that matches the folder with the proper permissions.