Implementing a Virtual Private Network

(CompTIA Security + SY – 601)

Objectives:

- To add Routing and Remote Access functionality and configure the Sales users on the DC1 server
- To configure access policy
- To test the VPN connection
- To use Nmap to discover what ports are exposed on the VPN server

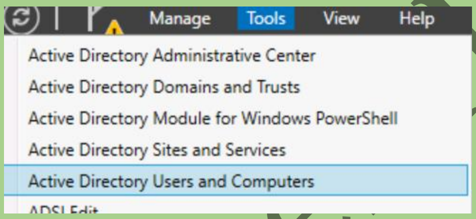
Resources:

- Kali Virtual Machine (PT1-Kali)
- Windows Virtual Machine (DC1 & MS1)
- Nmap

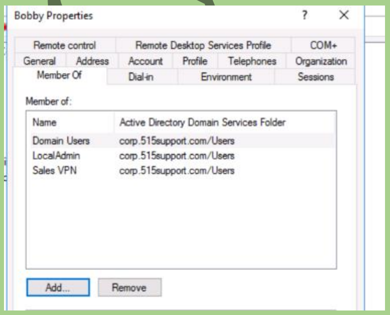
Instructions:

Configure the VPN server

- Sign-in to **DC1** VM
- From Server Manager, select **Tools > Active Directory Users and Computers** from **Server Manager** Browse to the **Users** container


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit

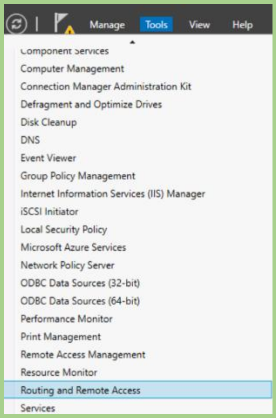
- Create a new global security group named Sales VPN
- Open the **Bobby** account, select the **Member Of** tab, and then add Bobby to the **Sales VPN** group



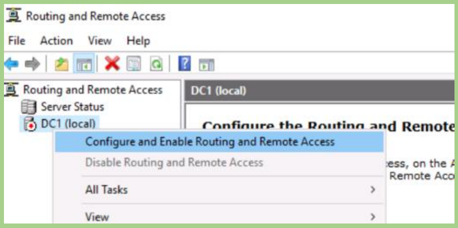
Member of:

Name	Active Directory Domain Services Folder
Domain Users	corp.515support.com/Users
LocalAdmin	corp.515support.com/Users
Sales VPN	corp.515support.com/Users

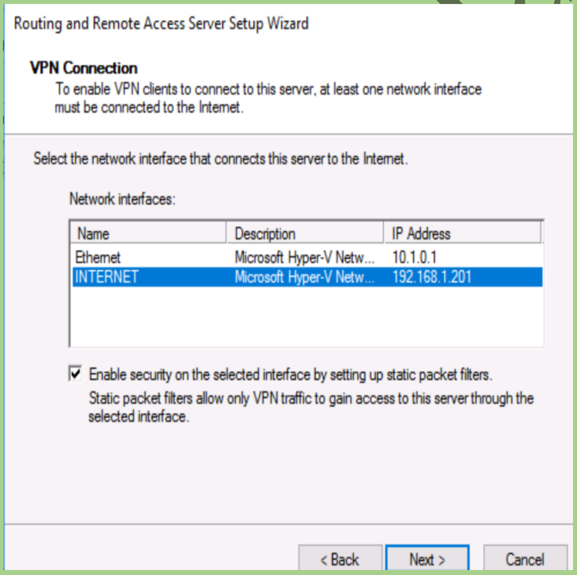
- ➢ From Server Manager, select **Tools > Routing and Remote Access**



- ➢ Right-click **DC1 (local)** and then select **configure and Enable Routing and Remote Access**. Select Next to start the wizard


Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
DC1 (local)
DC1 (local)
Configure the Routing and Remote
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
ess, on the
Remote Acc

- ➢ Select **Remote access (dial-up or VPN)** and then select Next
- ➢ Check the box for **VPN** and select **Next**
- ➢ When prompted select **INTERNET** interface as the internet connection


Routing and Remote Access Server Setup Wizard

VPN Connection

To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.

Select the network interface that connects this server to the Internet.

Network interfaces:

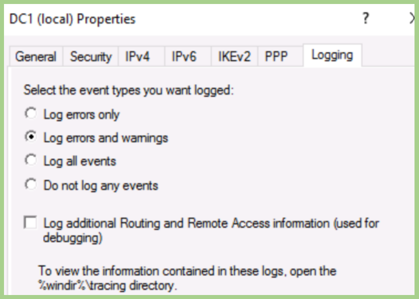
Name	Description	IP Address
Ethernet	Microsoft Hyper-V Netw...	10.1.0.1
INTERNET	Microsoft Hyper-V Netw...	192.168.1.201

☑ Enable security on the selected interface by setting up static packet filters.

Static packet filters allow only VPN traffic to gain access to this server through the selected interface.

- ➢ Accept all the remaining defaults and select **Finish**
- ➢ Acknowledge the policy message and accept the DHCP message when prompted

- When the RRAS service has started right-click the **DC1 (local)** node, select **Properties**. Select **Logging** tabs



DC1 (local) Properties

General | Security | IPv4 | IPv6 | IKEv2 | PPP | Logging

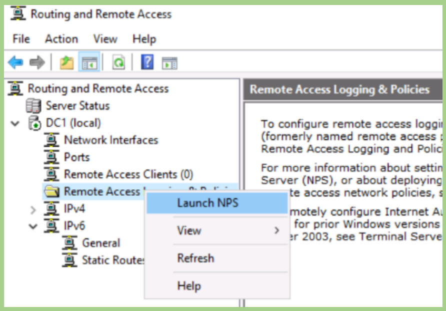
Select the event types you want logged:

○ Log errors only
● Log errors and warnings
○ Log all events
○ Do not log any events

□ Log additional Routing and Remote Access information (used for debugging)

To view the information contained in these logs, open the %windir%\tracing directory.

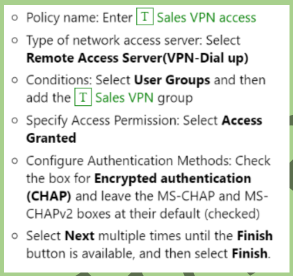
- Select the radio button for **Log all events** and then select **Ok** to close the properties box
- Select the Remote Access Logging & Policies node, and then right-click it and select **Launch NPS**



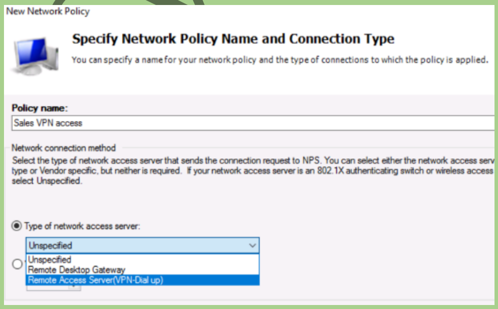
To configure remote access loggi
(formerly named remote access
Remote Access Logging and Polic

For more information about settin
Server (NPS), or about deploying
te access network policies,
motely configure Internet A
for prior Windows versions
er 2003, see Terminal Serve

- In the Network policy server console, select the **Network Policies** node
- Right-click the Network Policies node, and then select **New**. Use the following settings (unless otherwise stated accept the defaults):



- Policy name: Enter T Sales VPN access
- Type of network access server: Select **Remote Access Server(VPN-Dial up)**
- Conditions: Select **User Groups** and then add the T Sales VPN group
- Specify Access Permission: Select **Access Granted**
- Configure Authentication Methods: Check the box for **Encrypted authentication (CHAP)** and leave the MS-CHAP and MS-CHAPv2 boxes at their default (checked)
- Select **Next** multiple times until the **Finish** button is available, and then select **Finish**.



New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:
Sales VPN access

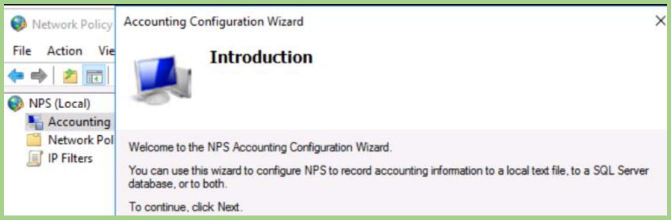
Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access serv type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access select Unspecified.

● Type of network access server:
Unspecified
Unspecified
Remote Desktop Gateway
Remote Access Server(VPN-Dial up)

- Observe the new policy in the Network Policies console

- ➢ In the NPS console, select **Accounting** and then select **Configure Accounting**



Accounting Configuration Wizard

Introduction

Welcome to the NPS Accounting Configuration Wizard.

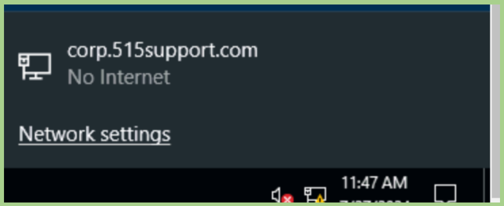
You can use this wizard to configure NPS to record accounting information to a local text file, to a SQL Server database, or to both.

To continue, click Next.

- ➢ Select Log to a text file on the local computer, accept the rest of the defaults and then complete the configurations

<u>Configure the VPN client</u>

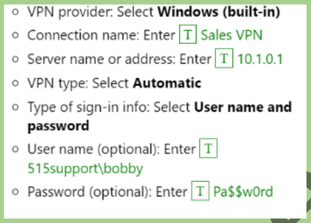
- ➢ Switch to the MS1; if necessary, sign-in
- ➢ Select **Other User** sign-in as **Bobby** using **Pa$$w0rd** as the password
- ➢ Minimize Server Manager. On the taskbar, in the notification area, click on the **Networks** icon and then select **Network settings**



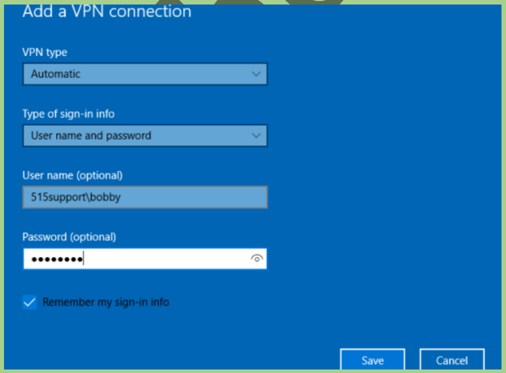
corp.515support.com
No Internet

Network settings

- ➢ From the settings page, select **VPN**, and then select **Add a VPN connection**. Configure the following values:



- ○ VPN provider: Select **Windows (built-in)**
- ○ Connection name: Enter T Sales VPN
- ○ Server name or address: Enter T 10.1.0.1
- ○ VPN type: Select **Automatic**
- ○ Type of sign-in info: Select **User name and password**
- ○ User name (optional): Enter T 515support\bobby
- ○ Password (optional): Enter T Pa$$w0rd



Add a VPN connection

VPN type: Automatic

Type of sign-in info: User name and password

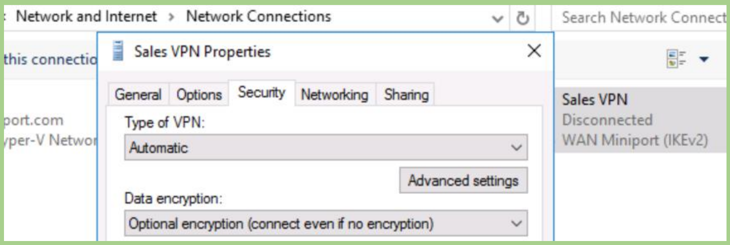
User name (optional): 515support\bobby

Password (optional): ••••••••

☑ Remember my sign-in info

- ➢ When all values are configured, select **Save**
- ➢ In the Settings window, select the link for **Change adapter options**

- Right-click the **Sales VPN**. Select **Properties** and then select **Security** tab



Network and Internet > Network Connections

Search Network Connect

this connectio

port.com
yper-V Networ

Sales VPN Properties

General | Options | Security | Networking | Sharing

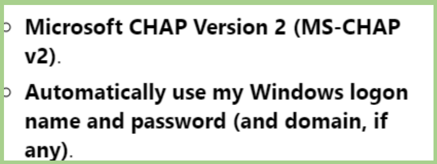
Type of VPN:
Automatic

Advanced settings

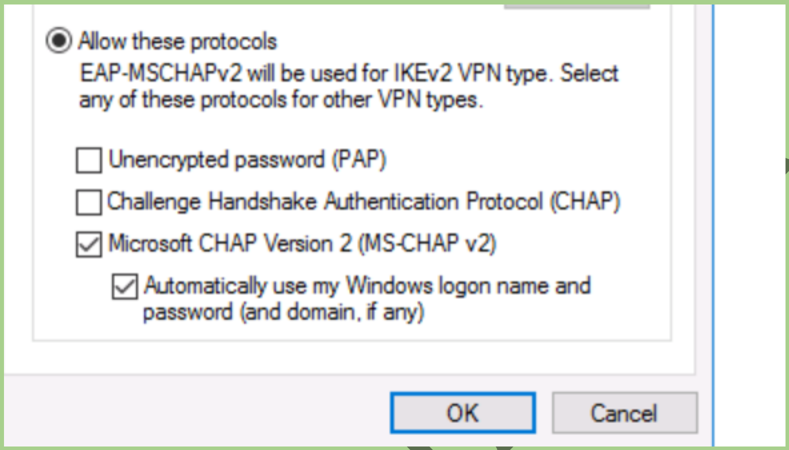
Data encryption:
Optional encryption (connect even if no encryption)

Sales VPN
Disconnected
WAN Miniport (IKEv2)

- Select the radio button for Allow these protocols and then check the boxes for the following:



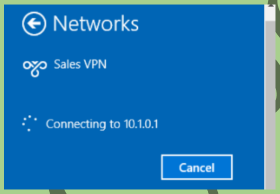
- **Microsoft CHAP Version 2 (MS-CHAP v2)**.
- **Automatically use my Windows logon name and password (and domain, if any)**.



● Allow these protocols
EAP-MSCHAPv2 will be used for IKEv2 VPN type. Select any of these protocols for other VPN types.

□ Unencrypted password (PAP)
□ Challenge Handshake Authentication Protocol (CHAP)
☑ Microsoft CHAP Version 2 (MS-CHAP v2)
☑ Automatically use my Windows logon name and password (and domain, if any)

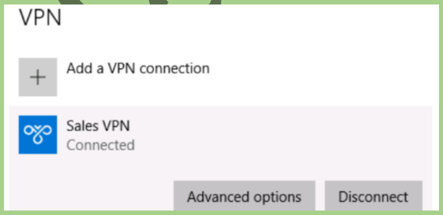
- Select **OK** to close the **Sales VPN** Properties
- On the network settings page, select the **Sales VPN**, icon and select **Connect**



Networks

Sales VPN

Connecting to 10.1.0.1



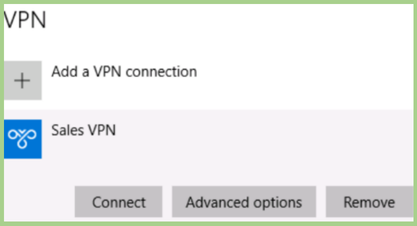
VPN

Add a VPN connection

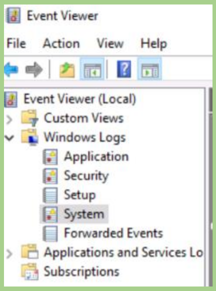
Sales VPN
Connected

- Switch to the DC1. In the Routing and Remote Access console, select **Remote Access Client** node

- ➢ Switch to the **MS1 VM** and then select **Disconnect** to end the VPN configuration test



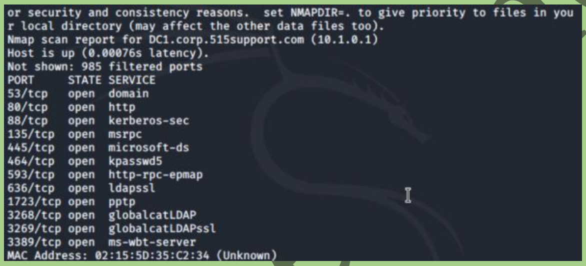
- ➢ Switch back to DC1, and from Server Manager, select **Tools > Event Viewer**



- ➢ Open the **System** log

<u>Investigating the VPN server</u>

- ➢ Switch to the PT1-Kali VM
- ➢ Open a terminal using the menu at the top of the desktop
- ➢ Run the following Nmap scan to determine what VPN port is open: nmap 10.1.0.1



```
or security and consistency reasons.  set NMAPDIR=. to give priority to files in you
r local directory (may affect the other data files too).
Nmap scan report for DC1.corp.515support.com (10.1.0.1)
Host is up (0.00076s latency).
Not shown: 985 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1723/tcp open  pptp
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 02:15:5D:35:C2:34 (Unknown)
```

Observations:

- ➢ **User Group Configuration**: Created a new global security group named Sales VPN and added the user Bobby to this group.
- ➢ **VPN Server Configuration**: Enabled and configured Routing and Remote Access on the DC1 server, set up for VPN access.
- ➢ **Access Policy Configuration**: Configured network policies and logging for VPN access.
- ➢ **VPN Client Configuration**: Configured VPN connection settings on the MS1 client machine for the Sales VPN.
- ➢ **Connectivity Testing**: Successfully connected and disconnected from the VPN to test the configuration.

- **Nmap Scan**: Conducted an Nmap scan from the PT1-Kali VM to identify open VPN ports on the VPN server (10.1.0.1).

Results:

- **Group Setup**: Successfully created and assigned the Sales VPN group.
- **VPN Functionality**: The DC1 server was correctly configured for VPN access and remote access policies were set.
- **Logging Enabled**: VPN server logging was set to log all events for detailed monitoring.
- **Successful VPN Connection**: The Sales VPN connection was successfully configured and tested on the MS1 machine.
- **Port Discovery**: Nmap scan results indicated open ports associated with the VPN service on the server.

Conclusion:

The lab effectively demonstrated the steps necessary to implement and configure a Virtual Private Network (VPN) on a Windows server environment. Key aspects included setting up user groups, configuring VPN server and client settings, and ensuring security policies and logging were properly applied. The successful testing of the VPN connection confirmed that the configuration was correct and functional.

Future Work:

- **Enhance Security**: Implement additional security measures such as multi-factor authentication (MFA) for VPN access.
- **Monitoring and Alerts**: Set up automated monitoring and alerting for VPN access and potential security breaches.
- **Regular Audits**: Conduct regular security audits and vulnerability assessments to ensure the VPN setup remains secure.
- **User Training**: Provide training for users on secure VPN usage and best practices for remote access.