Exercise 1 - Remote Network Device Configuration

Let's look at HTTP, NTP, RDP, and SIP as examples of protocols. On the pfsense firewall, you'll set up features like an NTP server, remote logging, and integrating the firewall with Active Directory. You'll also learn about many databases and the services they provide

In this exercise,

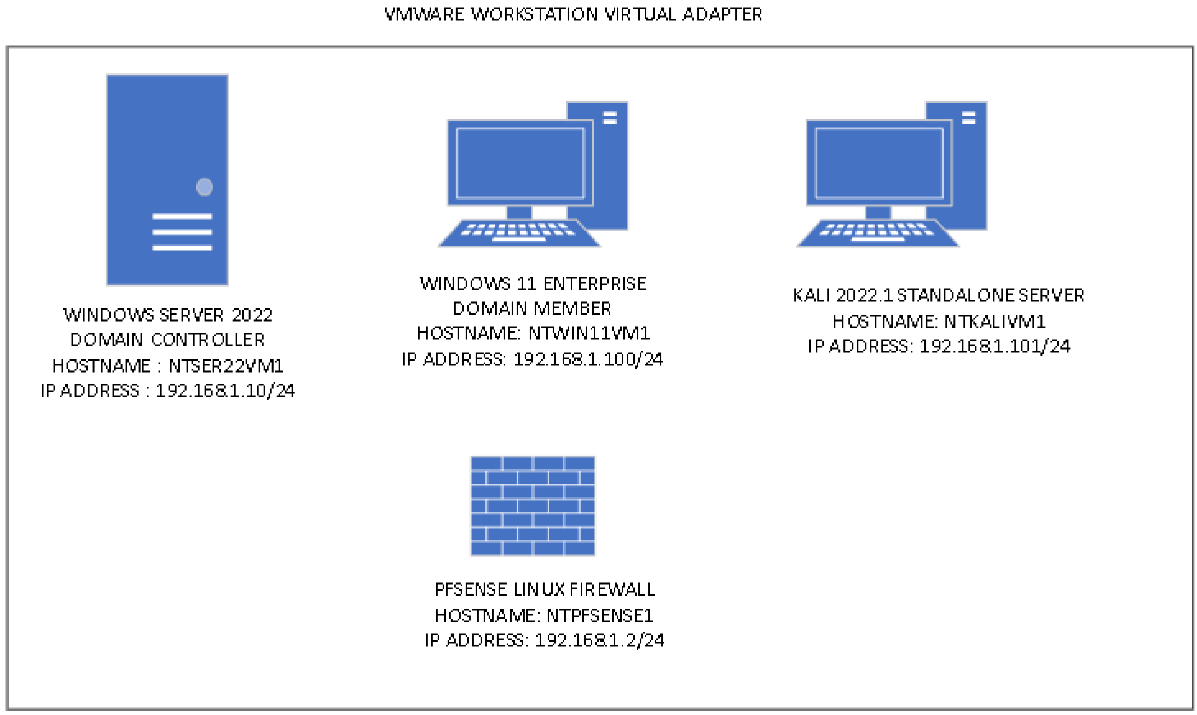
1. Configure Pfsense as NTP Server
2. Enable Remote Logging Server Option on Pfsense Firewall
3. Integrate Pfsense Firewall with Active Directory using LDAP Protocol
4. Use RDP for Remote Connection

HTTP and HTTPS Protocol

HTTP is a network protocol that operates at the OSI model's application layer. It is a client/server protocol that is mostly used to communicate between a web server and a web browser. When you, as a client, use your web browser to go to a specific URL, a request is sent to the web server, and you wait for a response. HTTP runs on TCP port 80, and the secure version of the protocol (HTTPS) encrypts communication via SSL certificates. TCP port 443 is used for HTTPS. Rather of HTTP, most webpages are published using HTTPS.

HTTP can also be used to access various network devices' GUIs (graphical user interfaces). You had previously used the pfsense firewall's GUI interface in a previous task. The pfsense firewall was opened using the URL https://192.168.1.2, which means the “The firewall” was accessed using the HTTPS protocol.

Topology


VMWARE WORKSTATION VIRTUAL ADAPTER
WINDOWS SERVER 2022
DOMAIN CONTROLLER
HOSTNAME : NTSER22VM1
IP ADDRESS : 192.168.1.10/24
WINDOWS 11 ENTERPRISE
DOMAIN MEMBER
HOSTNAME: NTWIN11VM1
IP ADDRESS: 192.168.1.100/24
KALI 2022.1 STANDALONE SERVER
HOSTNAME: NTKALIVM1
IP ADDRESS: 192.168.1.101/24
PFSENSE LINUX FIREWALL
HOSTNAME: NTPFSENSE1
IP ADDRESS: 192.168.1.2/24

DOMAIN = networktute.com

- NTPFSENSE1 = Linux - Virtual Firewall)
- NTSER22VM1 = Windows Server 2022 – Domain Controller
- NTWIN11VM1 = Windows 11 – Domain Member
- NTKALIVM1 = Kali 2022.1 - Standalone Server

Prerequisite

- *VMware Workstation 16 Pro*
    - When making this tutorial, we used the “Windows Server 2019” VM Template and “Windows 10 & later” VM Template. Since VMware didn’t have the updated templates.
- *Microsoft Windows Server 2022*
- *Microsoft Windows 11*
- *PFSense Linux Firewall*

Task 1: Configure Pfsense as NTP Server

The Network Time Protocol (NTP) is used to synchronize clocks between NTP clients and servers. UDP protocol port 123 is used. NTP servers that are open to the public have access to a lot of information. Atomic and GPS clocks that are extremely accurate. It is not necessary for every client on the network to be enabled. One device can be designated to function as an NTP server and access these public NTP servers. This server will synchronize time with the public NTP server in your environment. After that, all clients will point to the NTP server and obtain precise time. Domain controllers are commonly utilized as NTP servers in domain setups. Because of the debug and log messages, it's critical to have accurate time on the devices. If the moment has come, incorrect, it will be harder to troubleshoot issues on the network.

Now on the pfsense firewall, the NTP server will be configured. Pfsense is also an NTP client that synchronizes time with a public NTP server, but it will be used here as a local NTP server.

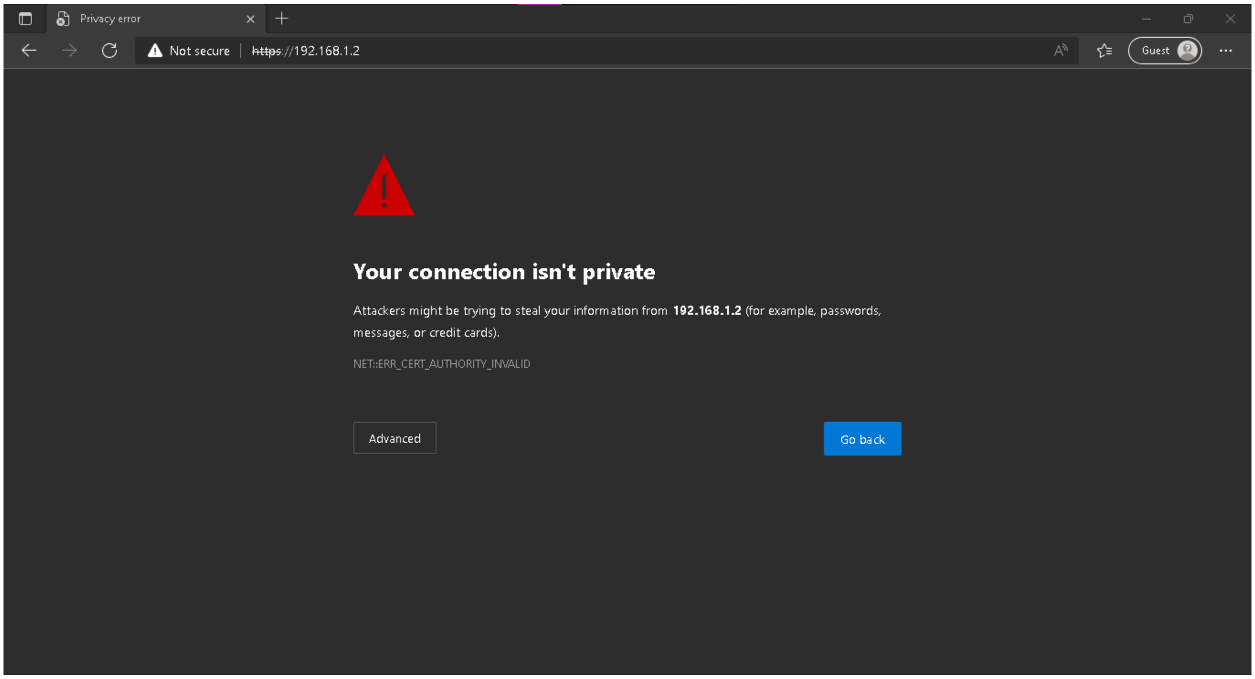
Step 1:

Connect to **NTWIN1VM1**. Open **Microsoft Edge** from the taskbar.

In the **Microsoft Edge** browser, click in the address bar and type:

```
https://192.168.1.2
```

Press **Enter**.



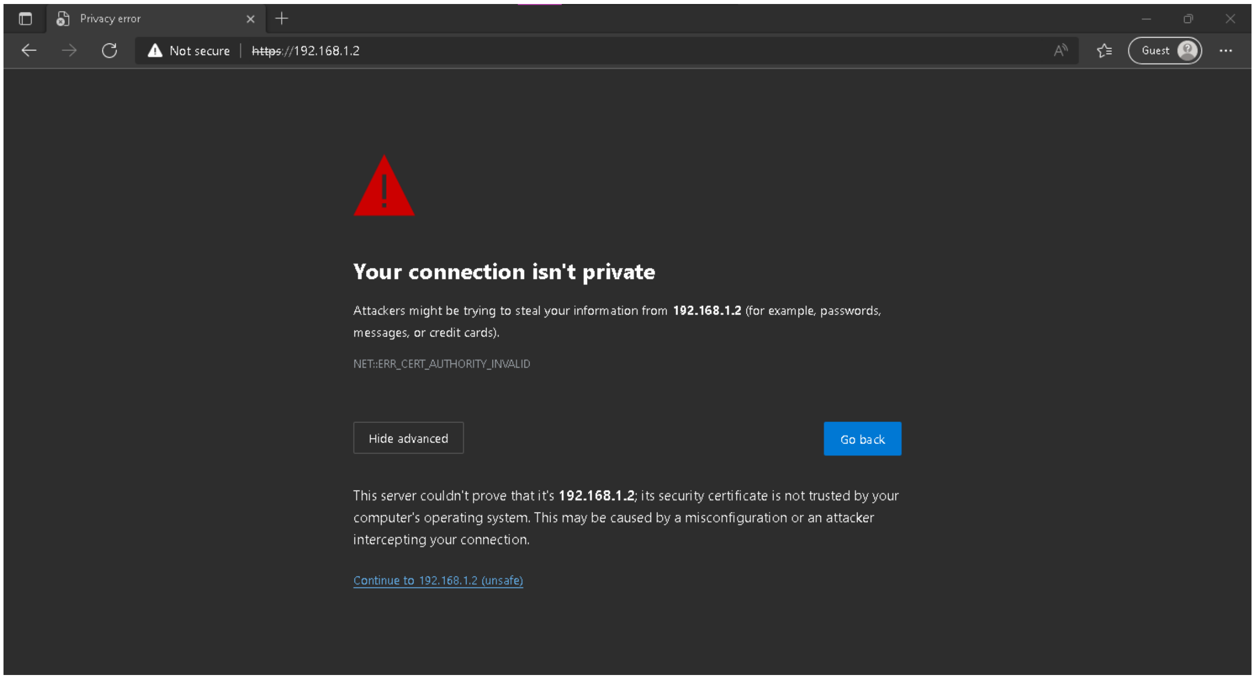
Your connection isn't private

Attackers might be trying to steal your information from **192.168.1.2** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

Step 2:

Click **Advanced** in the **Microsoft Edge** browser and click the **Continue to 192.168.1.2** (**unsafe**) link



Your connection isn't private

Attackers might be trying to steal your information from **192.168.1.2** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **192.168.1.2**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

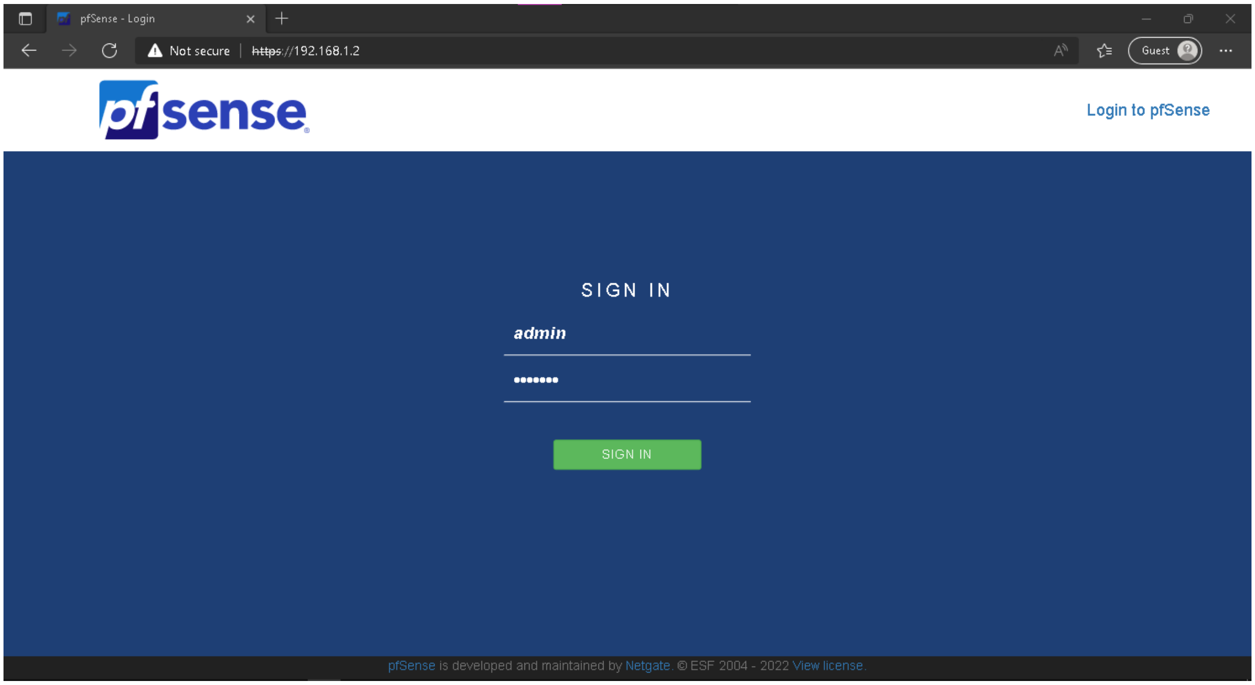
Continue to 192.168.1.2 (unsafe)

Step 3:

On the **pfsense** web page, log in with the following credentials:

Username: **admin**
Password: **pfsense**

Click **SIGN IN**.

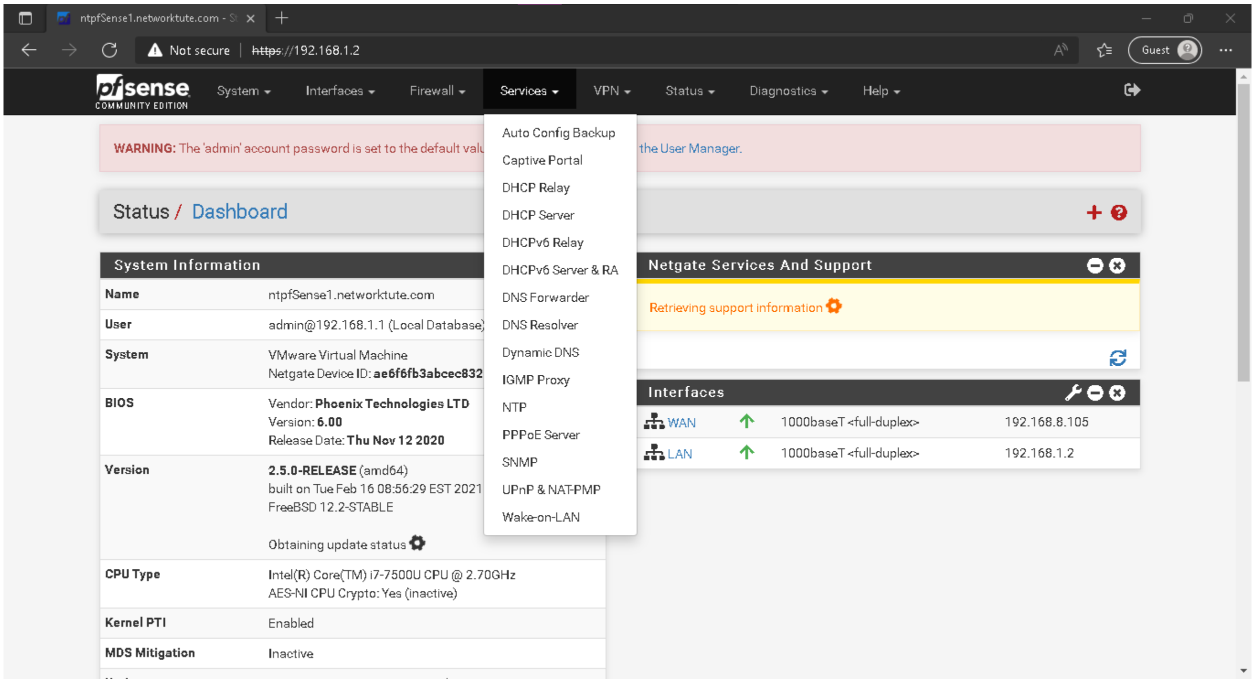


Username: *admin*
Password: •••••••

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license

Step 4:

On the web page, click the **Services** menu drop-down and select **NTP**.



WARNING: The 'admin' account password is set to the default valu the User Manager.

Status / Dashboard

System Information

Name	ntpfSense1.networktute.com
User	admin@192.168.1.1 (Local Database)
System	VMware Virtual Machine Netgate Device ID: **ae6f6fb3abcec832**
BIOS	Vendor: **Phoenix Technologies LTD** Version: **6.00** Release Date: **Thu Nov 12 2020**
Version	**2.5.0-RELEASE** (amd64) built on Tue Feb 16 08:56:29 EST 2021 FreeBSD 12.2-STABLE Obtaining update status
CPU Type	Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
MDS Mitigation	Inactive

Netgate Services And Support

Retrieving support information

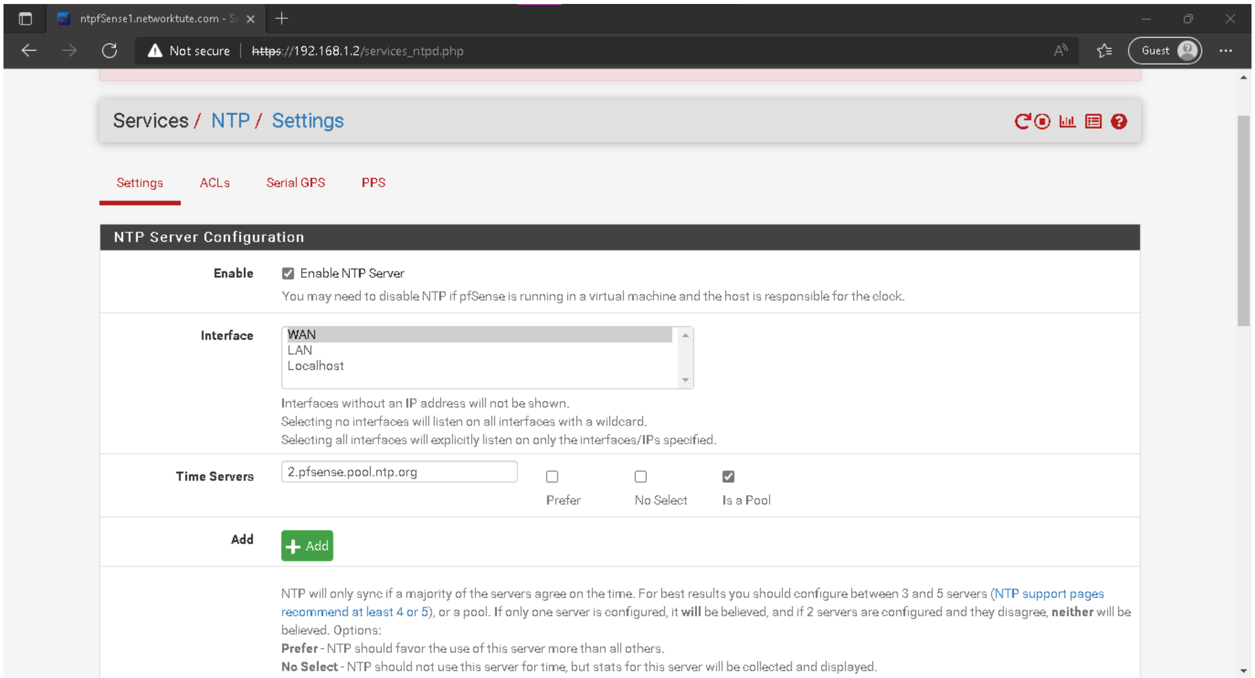
Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.8.105
LAN	↑	1000baseT <full-duplex>	192.168.1.2

Step 5:

Select the interface on which you wish to enable the NTP server on the **Services** / **NTP** / **Settings** page (where all NTP requests will arrive). This is generally the LAN interface, but you'll choose WAN because it's part of the 192.168.8.0/24 network, which includes all of the other servers.

Under **NTP Server Configuration**, select **WAN** for the **Interface** field.


ntpfSense1.networktute.com - S
Not secure
https://192.168.1.2/services_ntpd.php
Guest
Settings
ACLs
Serial GPS
PPS
+ Add

Services / NTP / Settings

NTP Server Configuration

Enable ☑ Enable NTP Server
You may need to disable NTP if pfSense is running in a virtual machine and the host is responsible for the clock.

Interface
WAN
LAN
Localhost

Interfaces without an IP address will not be shown.
Selecting no interfaces will listen on all interfaces with a wildcard.
Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time Servers 2.pfsense.pool.ntp.org □ Prefer □ No Select ☑ Is a Pool

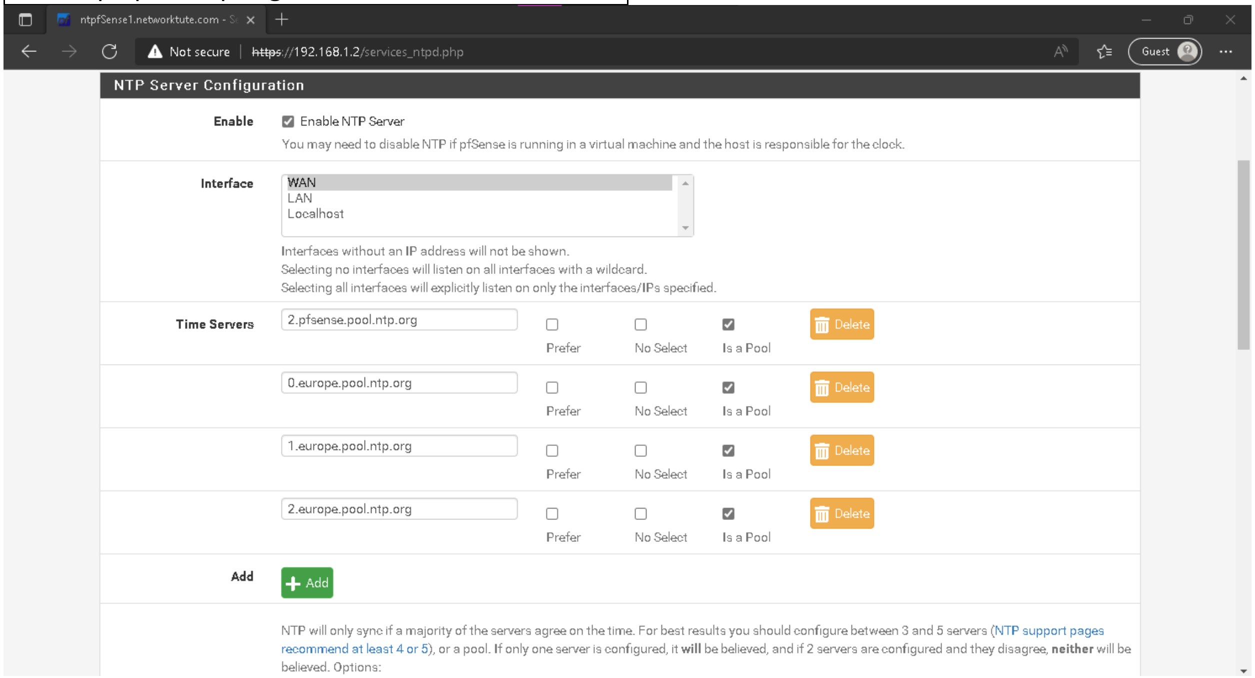
Add

NTP will only sync if a majority of the servers agree on the time. For best results you should configure between 3 and 5 servers (NTP support pages recommend at least 4 or 5), or a pool. If only one server is configured, it **will** be believed, and if 2 servers are configured and they disagree, **neither** will be believed. Options:
Prefer - NTP should favor the use of this server more than all others.
No Select - NTP should not use this server for time, but stats for this server will be collected and displayed.

Step 6:

Under the **Time Servers** field, click +**Add** thrice and enter the following name:

0.europe.pool.ntp.org
1.europe.pool.ntp.org
2.europe.pool.ntp.org


ntpfSense1.networktute.com - S
Not secure
https://192.168.1.2/services_ntpd.php
Guest
Delete
Delete
Delete
Delete
+ Add

NTP Server Configuration

Enable ☑ Enable NTP Server
You may need to disable NTP if pfSense is running in a virtual machine and the host is responsible for the clock.

Interface
WAN
LAN
Localhost

Interfaces without an IP address will not be shown.
Selecting no interfaces will listen on all interfaces with a wildcard.
Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time Servers
2.pfsense.pool.ntp.org □ Prefer □ No Select ☑ Is a Pool
0.europe.pool.ntp.org □ Prefer □ No Select ☑ Is a Pool
1.europe.pool.ntp.org □ Prefer □ No Select ☑ Is a Pool
2.europe.pool.ntp.org □ Prefer □ No Select ☑ Is a Pool

Add

NTP will only sync if a majority of the servers agree on the time. For best results you should configure between 3 and 5 servers (NTP support pages recommend at least 4 or 5), or a pool. If only one server is configured, it **will** be believed, and if 2 servers are configured and they disagree, **neither** will be believed. Options:

Scroll down and click **Save**.

Note: You can now configure your devices to use 192.168.1.2 as the NTP server. It's extremely helpful for debugging and log messages to have precise time on your devices**.**

Simple Network Management Protocol (SNMP)

Another network layer protocol that works on the application layer of the OSI model is the Simple Network Management Protocol (SNMP). It's used to send and receive many types of management data between network devices or hosts and the Network Management System (NMS). It's one of the most widely used network protocols for monitoring routers, switches, Windows and Linux servers, and other network devices.

The SNMP manager, SNMP agent, MIB (Management Information Base), and managed device are all critical components of any SNMP monitoring solution.

The managed device's SNMP agent is in charge of communicating with the SNMP Manager, which is typically installed on the network management system. The SNMP agent's principal function is to collect various management data and reports. As SNMP traps or as a response to the SNMP manager, transmit them to the SNMP manager. query. MIB is a set of managed device parameters that are sent back and forth between devices. both the agent and the manager

Task 2: Enable Remote Logging Server Option on Pfsense Firewall

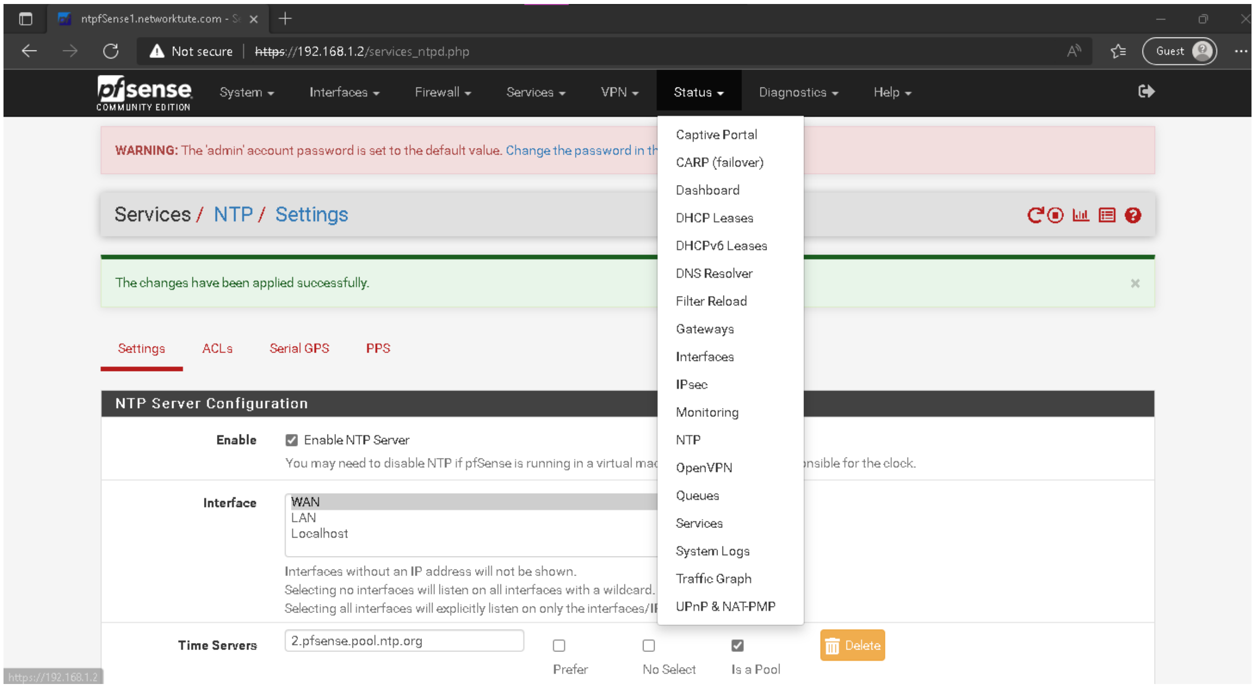
The System Logging Protocol (Syslog) is used to deliver various log and event messages to the syslog server, which is a remote server. The transport protocol is UDP, and the port number is 161. Because it collects logs from all devices in one location, it may also be used as a monitoring protocol. These log messages can then be used by monitoring software that operates the syslog server to generate various alerts and notifications.

The syslog server may be utilized without any monitoring software as a stand-alone solution, however tracking all log messages would be difficult. Using the pfsense firewall, you will define the syslog server on a network device in this operation.

Step 1:

Connect to **NTWIN11VM1**. You should be on the pfsense page in **Microsoft Edge**.

Click the **Status** menu drop-down and select **System Logs**.



WARNING: The 'admin' account password is set to the default value. Change the password in th

Services / NTP / Settings

The changes have been applied successfully.

NTP Server Configuration

Enable ☑ Enable NTP Server

You may need to disable NTP if pfSense is running in a virtual mac nsible for the clock.

Interface WAN
LAN
Localhost

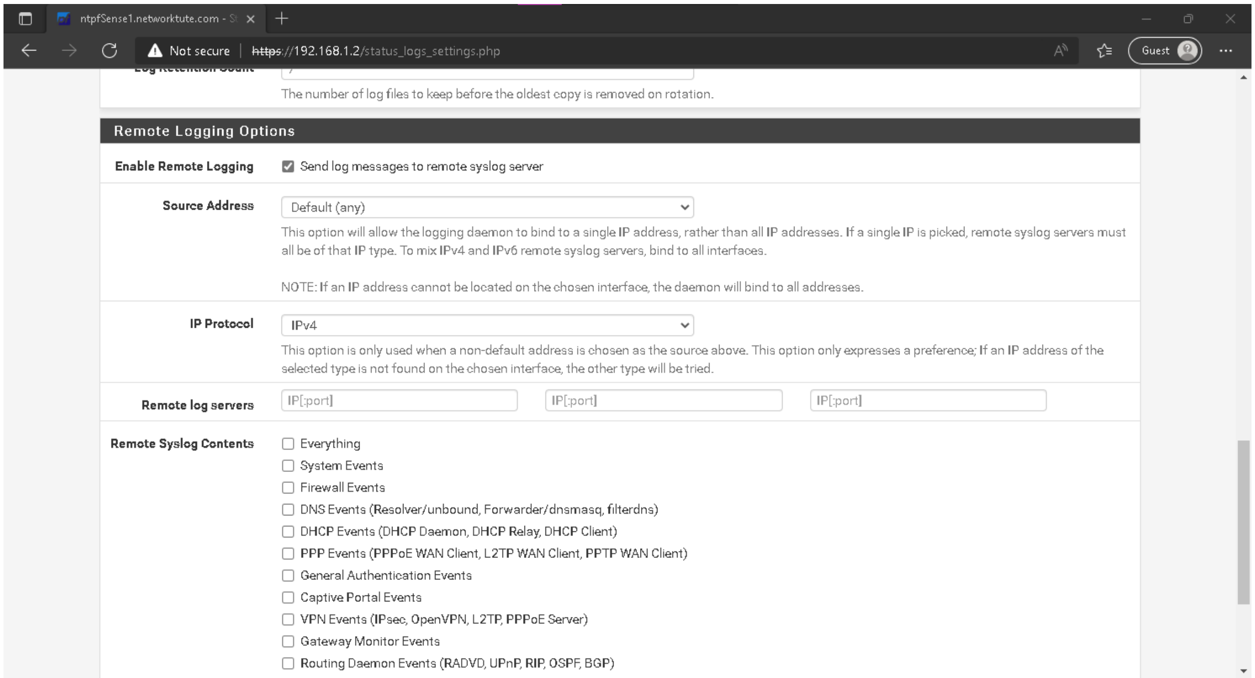
Interfaces without an IP address will not be shown.
Selecting no interfaces will listen on all interfaces with a wildcard.
Selecting all interfaces will explicitly listen on only the interfaces/IP

Time Servers 2.pfsense.pool.ntp.org □ Prefer □ No Select ☑ Is a Pool

Step 2:

On the Status / **System Logs / System / General** page, click on the **Settings tab**.

Scroll down to the **Remote Logging Options** section and select the **Send log messages to remote syslog server** checkbox.


ntpfSense1.networktute.com - S
Not secure
https://192.168.1.2/status_logs_settings.php
Guest

The number of log files to keep before the oldest copy is removed on rotation.

Remote Logging Options

Enable Remote Logging ☑ Send log messages to remote syslog server

Source Address Default (any)

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers IP[:port] IP[:port] IP[:port]

Remote Syslog Contents
□ Everything
□ System Events
□ Firewall Events
□ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
□ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
□ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
□ General Authentication Events
□ Captive Portal Events
□ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
□ Gateway Monitor Events
□ Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)

Step 3:

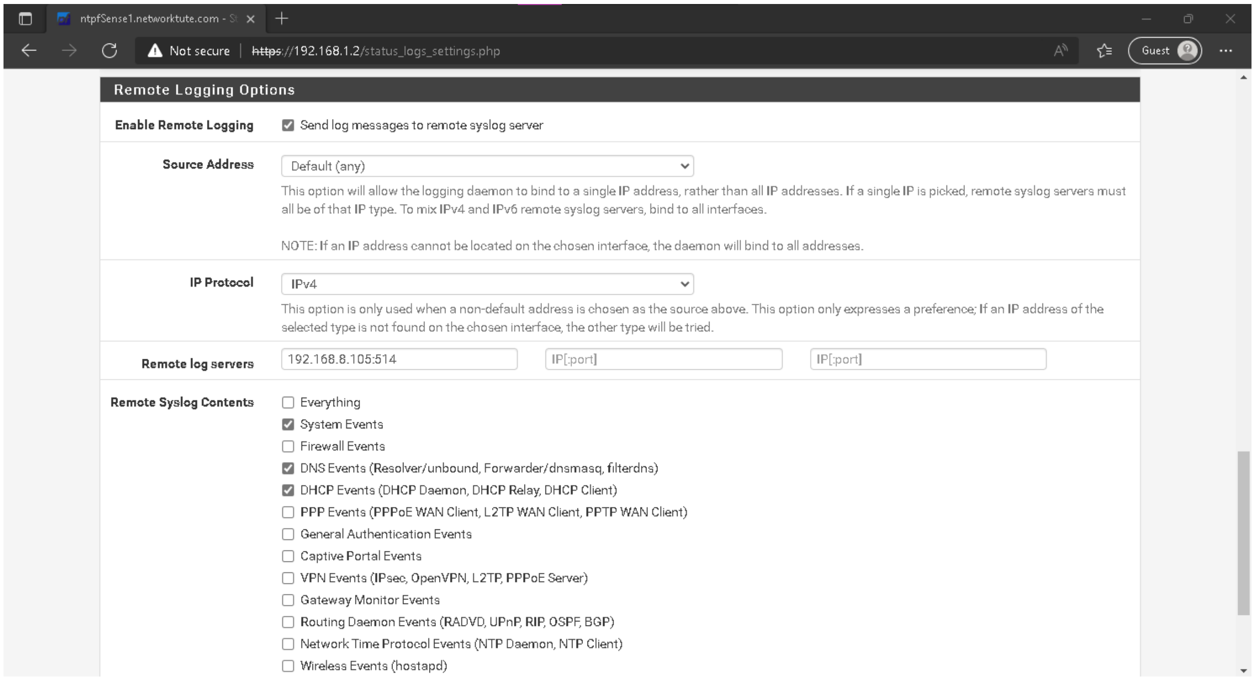
Apply the following settings:

- For **Source Address**, select **WAN**.
- Enter the following IP address for the **Remote log servers'** field:

  192.168.8.105:514

- Enable the following checkboxes for the **Remote Syslog Contents** field:
  - **System Events**
  - **DNS Events (Resolver/unbound, Forwarder/dnsmasq,filterdns)**
  - **DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)**

Scroll down and click **Save**.


ntpfSense1.networktute.com - S
Not secure
~~https~~://192.168.1.2/status_logs_settings.php
Guest

Remote Logging Options

Enable Remote Logging ☑ Send log messages to remote syslog server

Source Address: Default (any)

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol: IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers: 192.168.8.105:514 | IP[:port] | IP[:port]

Remote Syslog Contents

☐ Everything
☑ System Events
☐ Firewall Events
☑ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
☑ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
☐ General Authentication Events
☐ Captive Portal Events
☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
☐ Gateway Monitor Events
☐ Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
☐ Network Time Protocol Events (NTP Daemon, NTP Client)
☐ Wireless Events (hostapd)

Note: Log messages can be forwarded to the remote server after the above parameters are applied. You would use the command logging 192.168.1.100 if you only have SSH or console access to a device, such as a Cisco router.

Task 3: Integrate Pfsense Firewall with Active Directory using LDAP Protocol

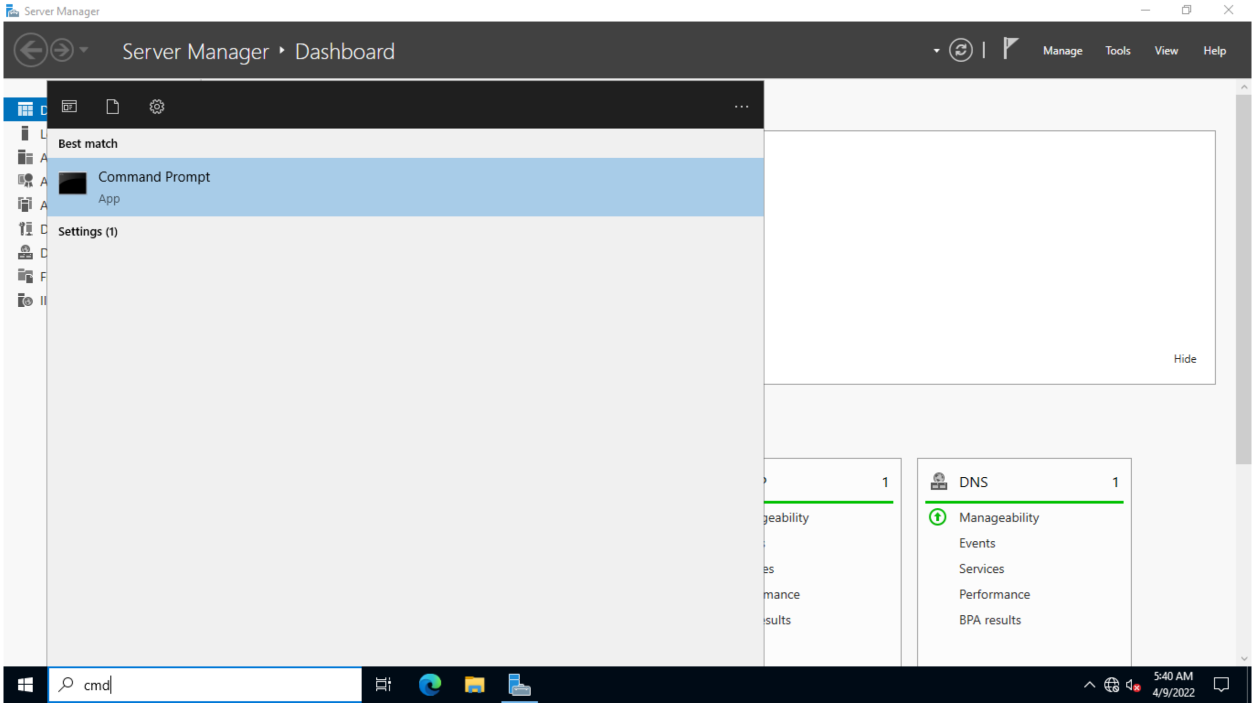
Different applications, such as OpenLDAP, Microsoft Active Directory, and similar software, use the Lightweight Directory Access Protocol (LDAP) to authenticate and authorize users. It operates on two ports: TCP/UDP 389, which is insecure and unencrypted, and TCP/UDP 636, which is secure and encrypted and runs over SSL.

In this task, the pfsense firewall will be integrated with NTSER22VM1, which has a running domain and active directory.

Step 1:

Connect to **NTSER22VM1**.

Click on the Start menu and type: ***cmd***

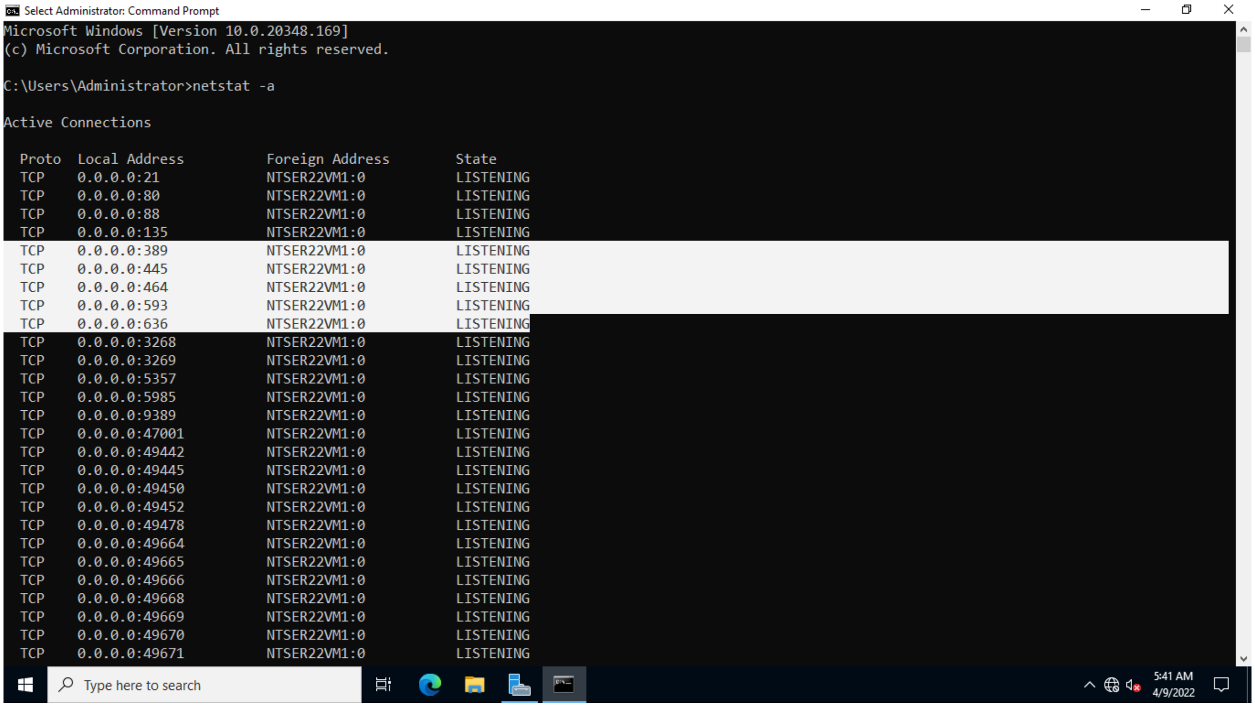


Step 2:

On the **Command Prompt** window, type the following command and press **Enter**. ***netstat -a***

After a few seconds, press **Ctrl+C** to stop listing all opened ports.

Scroll back to the beginning of the list and check if ports **389** and **636** are open.



```
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:80             NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:88             NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:135            NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:389            NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:445            NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:464            NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:593            NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:636            NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:3268           NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:3269           NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:5357           NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:5985           NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:9389           NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:47001          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49442          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49445          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49450          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49452          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49478          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49664          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49665          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49666          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49668          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49669          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49670          NTSER22VM1:0           LISTENING
  TCP    0.0.0.0:49671          NTSER22VM1:0           LISTENING
```

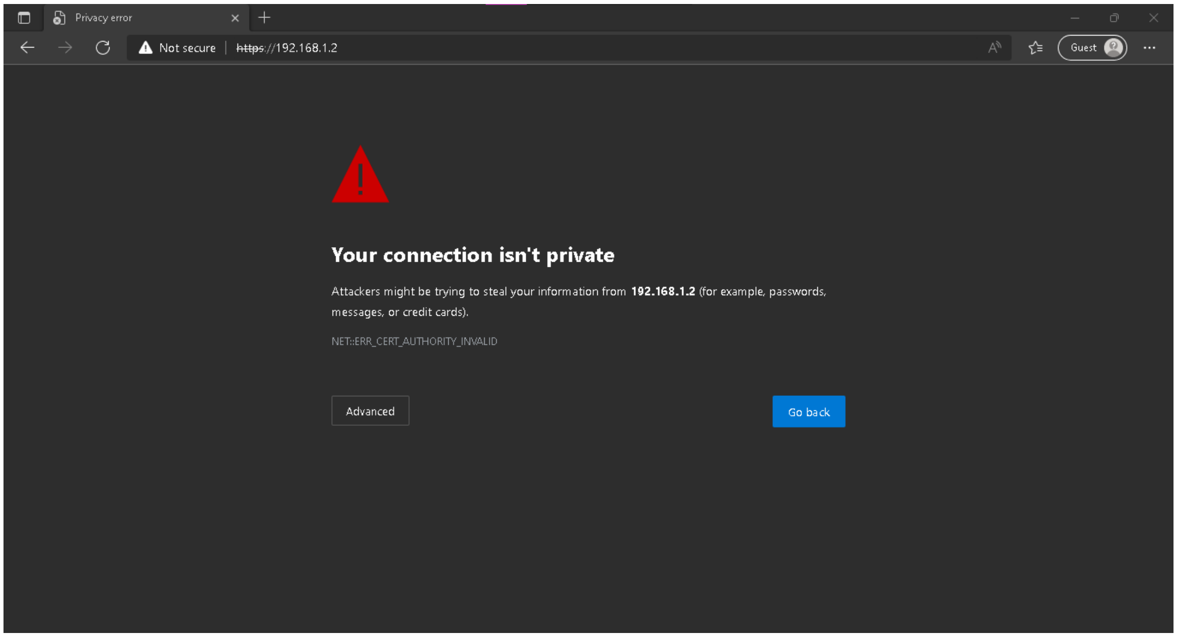
Note: From the output, it can be seen that server **NTSER22VM1**, the domain controller, is listening on ports 389 and 636.

Step 3:

Open Microsoft Edge from the taskbar and click in the address bar and type:

```
https://192.168.1.2
```

Press **Enter**.



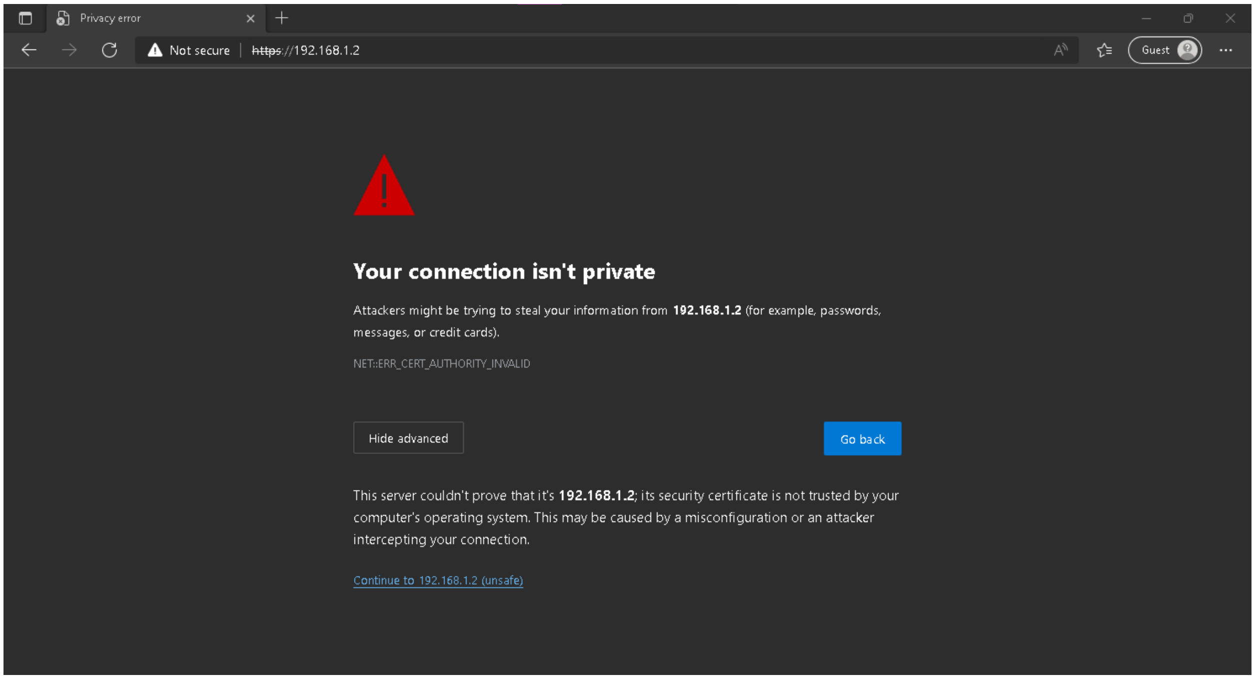
Your connection isn't private

Attackers might be trying to steal your information from **192.168.1.2** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

Step 4:

Click **Advanced** in the **Microsoft Edge** browser and click the **Continue to 192.168.1.2** (**unsafe**) link.



Your connection isn't private

Attackers might be trying to steal your information from **192.168.1.2** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **192.168.1.2**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

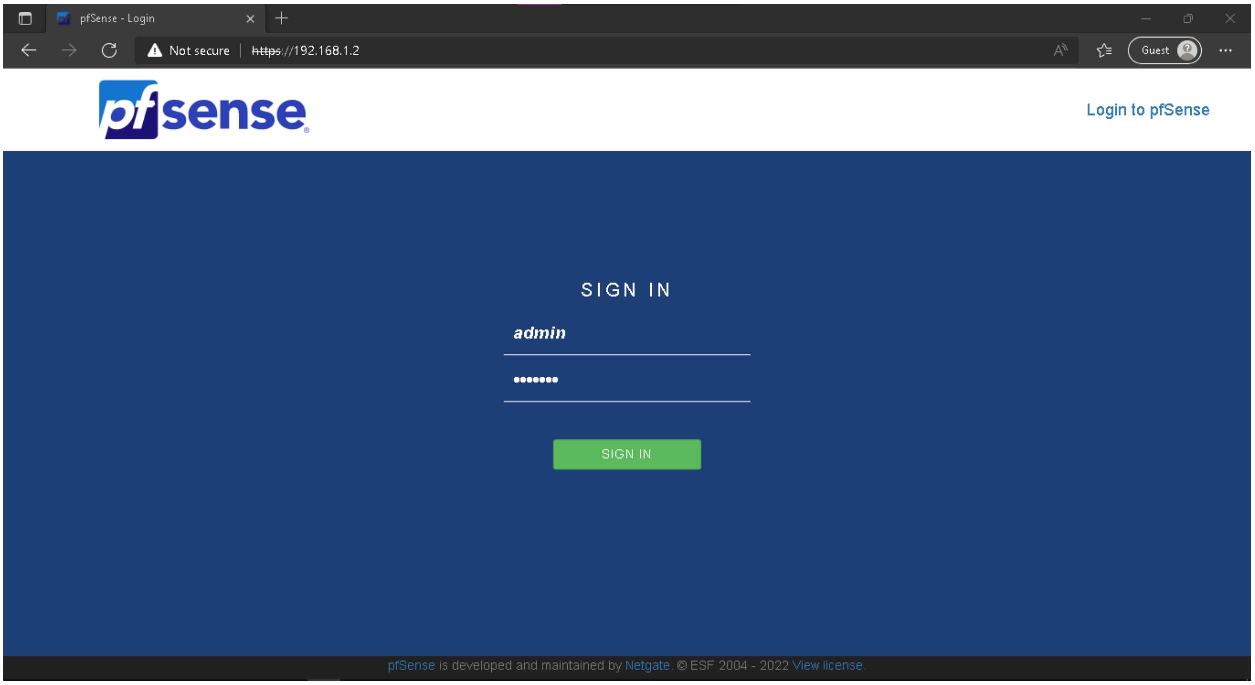
Continue to 192.168.1.2 (unsafe)

Step 5:

On the **pfsense** web page, log in with the following credentials:

Username: admin
Password: **pfsense**

Press **Enter**.



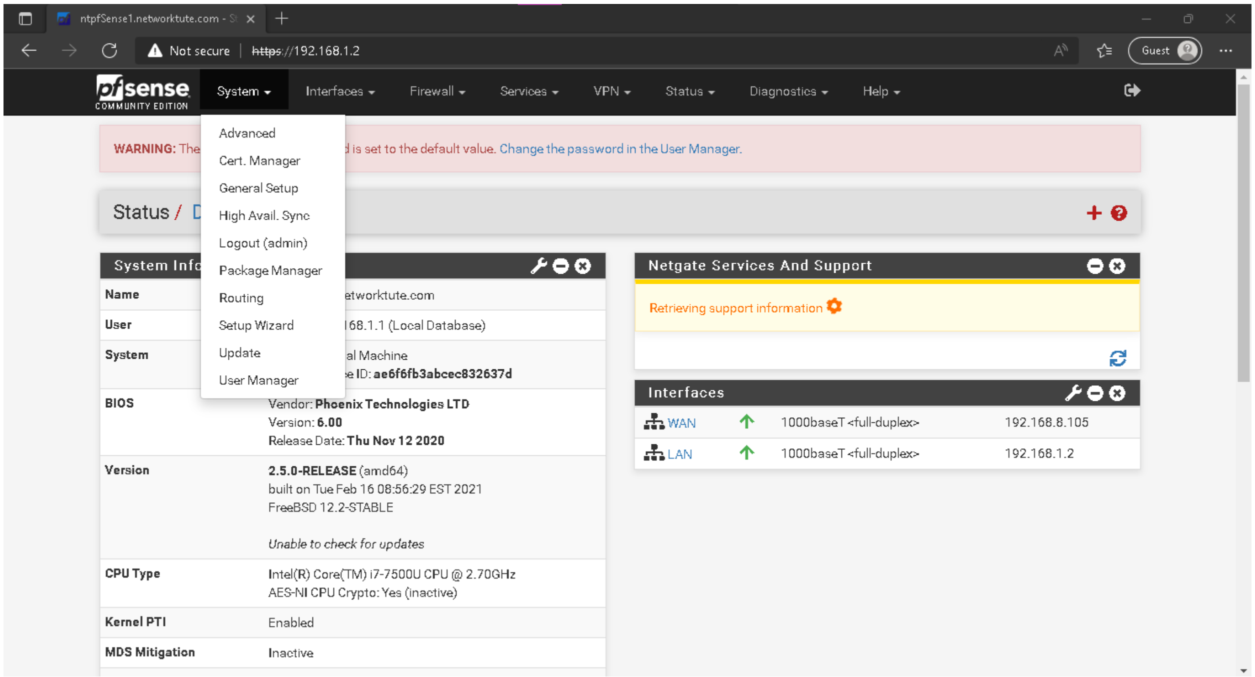
admin

•••••••

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

Step 6:

On the web page, click the **System** menu drop-down and select **User Manager**.



WARNING: The … d is set to the default value. Change the password in the User Manager.

Status / D

System Info

Name	…etworktute.com
User	…68.1.1 (Local Database)
System	…al Machine …e ID: ae6f6fb3abcec832637d
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.5.0-RELEASE (amd64) built on Tue Feb 16 08:56:29 EST 2021 FreeBSD 12.2-STABLE *Unable to check for updates*
CPU Type	Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
MDS Mitigation	Inactive

Netgate Services And Support

Retrieving support information

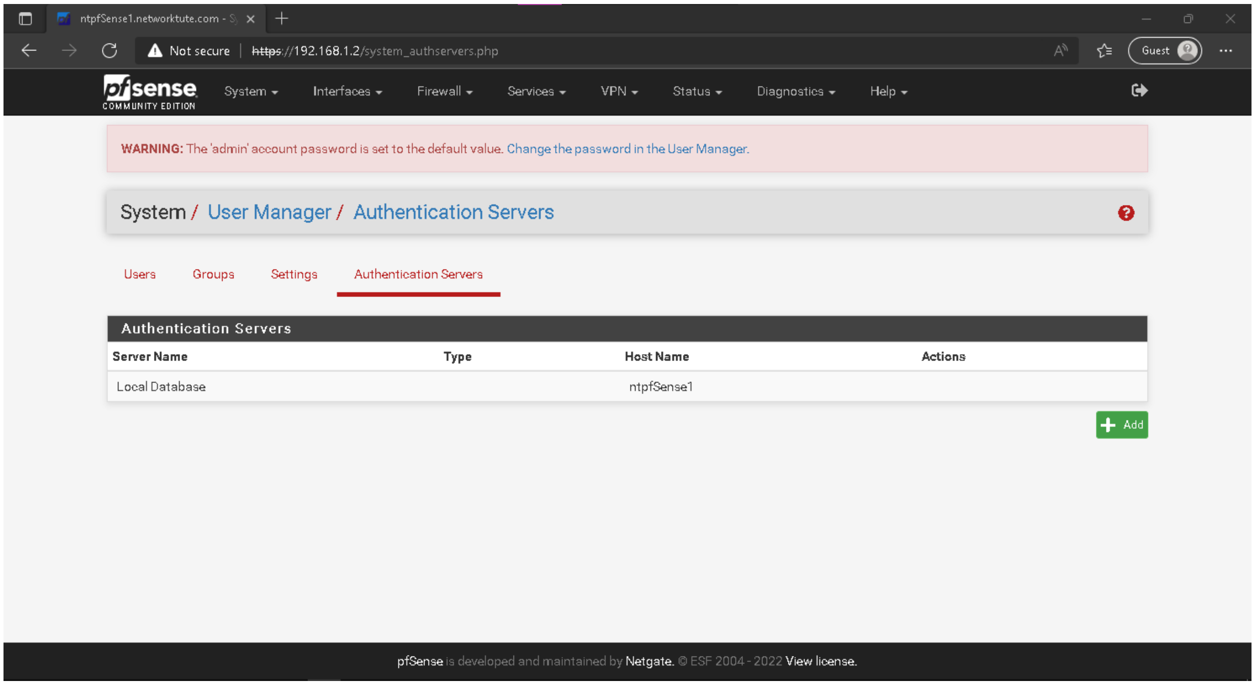
Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.8.105
LAN	↑	1000baseT <full-duplex>	192.168.1.2

Step 7:

On the **System** / **User Manager** / **Users** page, click on the **Authentication Servers** tab.

On the **System** / **User Manager** / **Authentication** Servers page, click + **Add**.


ntpfSense1.networktute.com - S
Not secure
https://192.168.1.2/system_authservers.php
Guest
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / User Manager / Authentication Servers

Authentication Servers

Server Name	Type	Host Name	Actions
Local Database		ntpfSense1	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

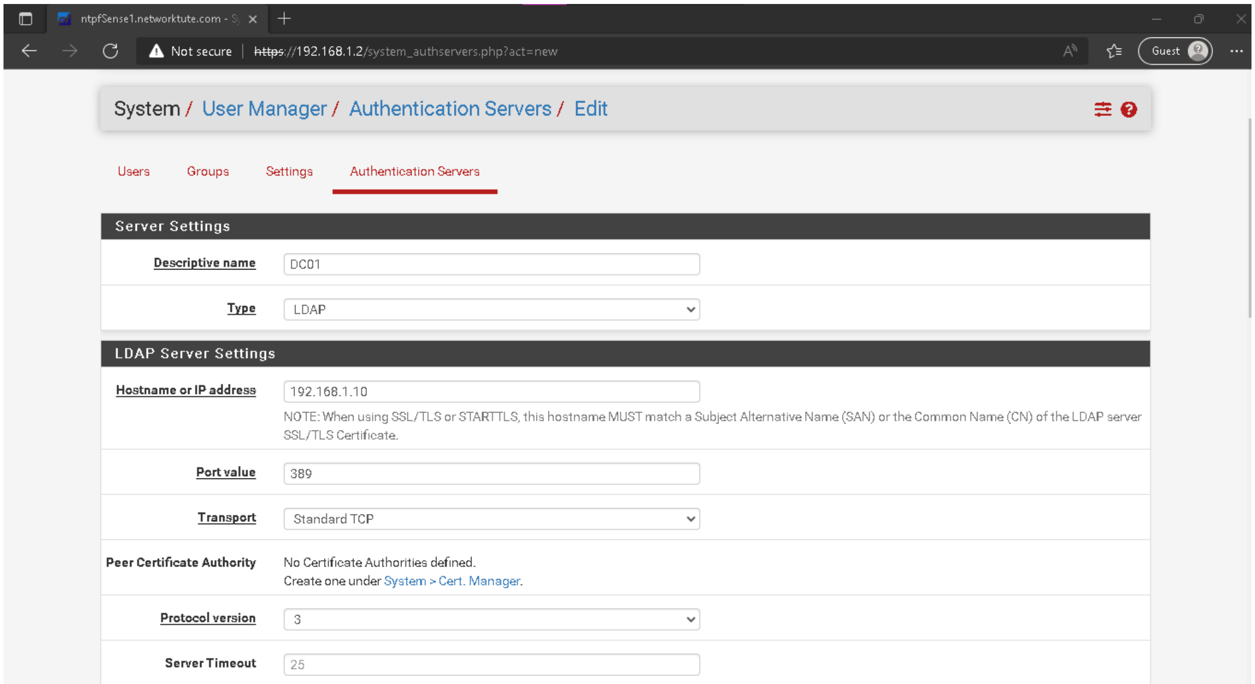
Step 8:

On the **System** / **User Manager** / **Authentication Servers** / **Edit** page, under the **Server Settings** section, type the following for the **Descriptive name** field:

DC01

Under the **LDAP Server Settings** section, type the following for the **Hostname** or **IP address** field:

192.168.1.10



ntpfSense1.networktute.com - S
Not secure
https://192.168.1.2/system_authservers.php?act=new
Guest

System / User Manager / Authentication Servers / Edit

Users | Groups | Settings | Authentication Servers

Server Settings

Descriptive name	DC01
Type	LDAP

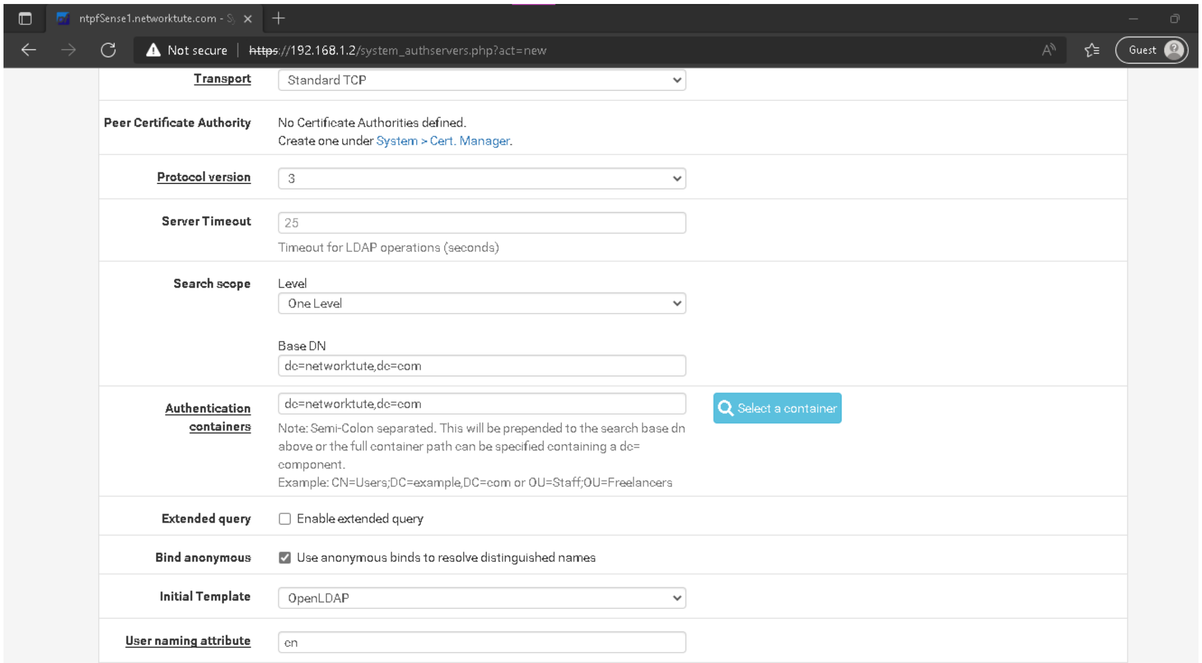
LDAP Server Settings

Hostname or IP address	192.168.1.10 NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.
Port value	389
Transport	Standard TCP
Peer Certificate Authority	No Certificate Authorities defined. Create one under System > Cert. Manager.
Protocol version	3
Server Timeout	25

Step 9:

Scroll down to the **Search scope** section, and type the following for the **BASE DN** field and on the **Authentication containers** field:

```
dc=networktute,dc=com
```



ntpfSense1.networktute.com - S
Not secure
https://192.168.1.2/system_authservers.php?act=new
Guest

Transport	Standard TCP
Peer Certificate Authority	No Certificate Authorities defined. Create one under System > Cert. Manager.
Protocol version	3
Server Timeout	25 Timeout for LDAP operations (seconds)
Search scope	Level One Level Base DN dc=networktute,dc=com
Authentication containers	dc=networktute,dc=com Select a container Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers
Extended query	□ Enable extended query
Bind anonymous	☑ Use anonymous binds to resolve distinguished names
Initial Template	OpenLDAP
User naming attribute	cn

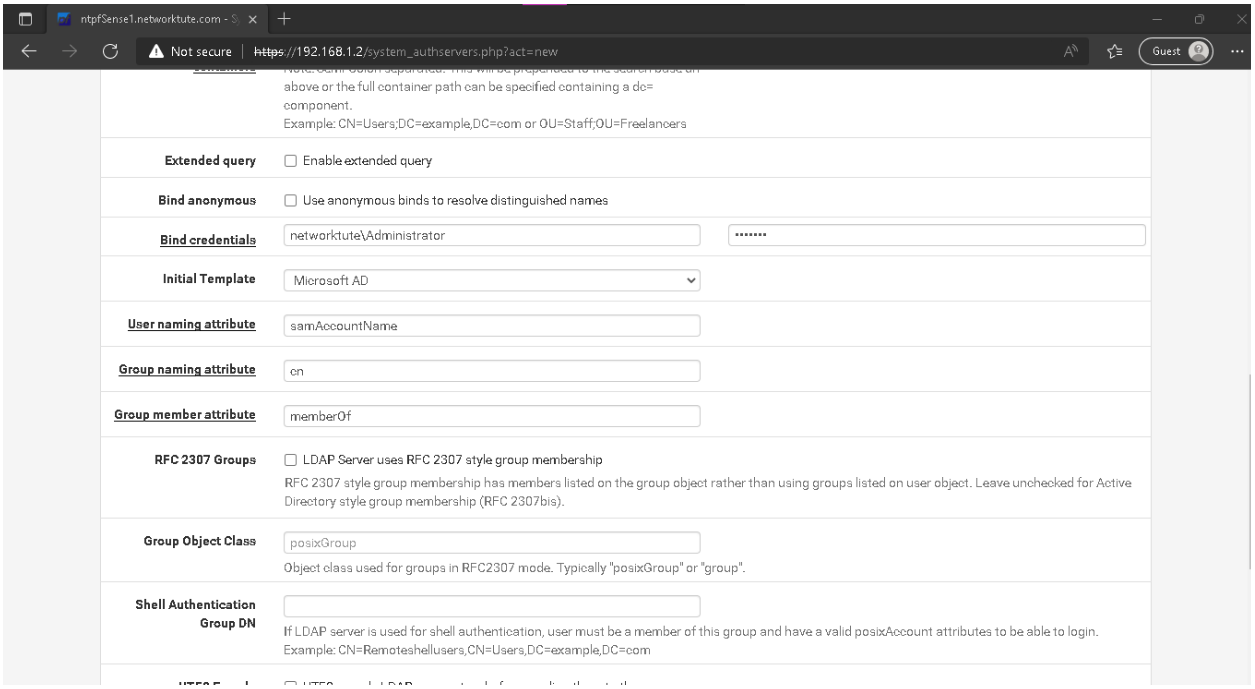
Step 10:

For the **Bind anonymous** field, uncheck **Use anonymous binds to resolve distinguished names**.

Type the following for the **Bind credentials** field:

```
User DN: networktute\Administrator
Password: Networktute@1
```

Select **Microsoft AD** from the **Initial Template** drop-down.



ntpfSense1.networktute.com

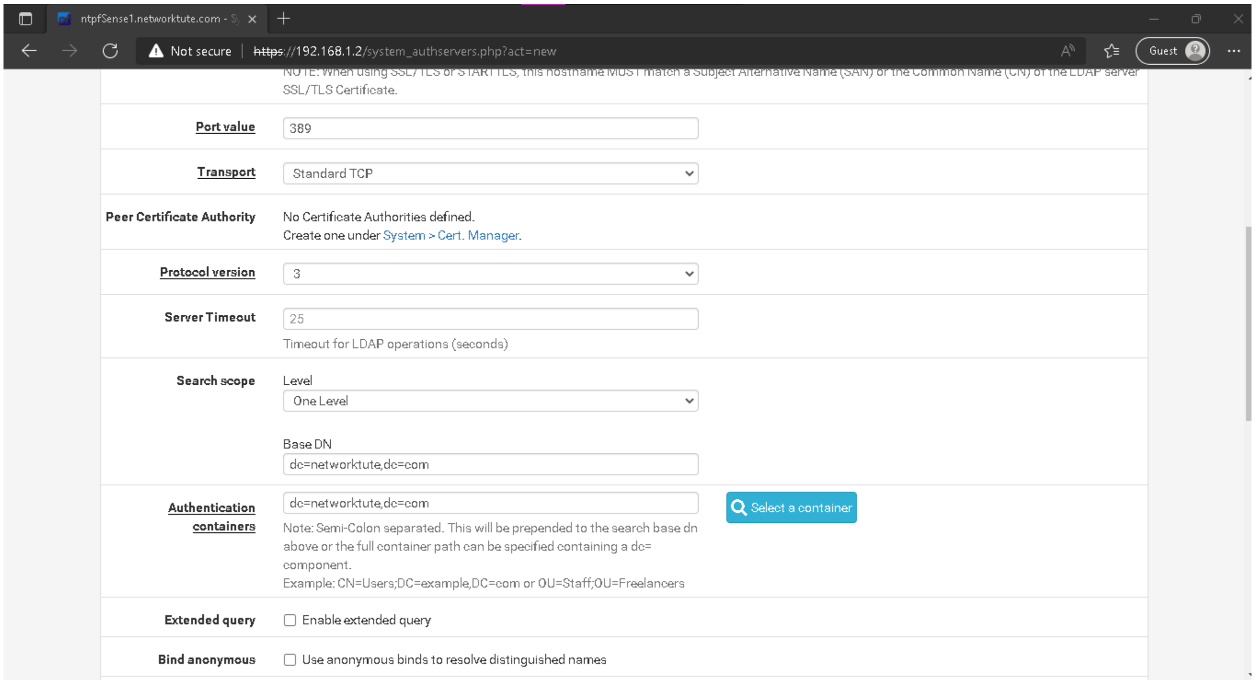
Not secure | https://192.168.1.2/system_authservers.php?act=new

above or the full container path can be specified containing a dc= component.
Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers

Extended query	☐ Enable extended query
Bind anonymous	☐ Use anonymous binds to resolve distinguished names
Bind credentials	networktute\Administrator •••••••
Initial Template	Microsoft AD
User naming attribute	samAccountName
Group naming attribute	cn
Group member attribute	memberOf
RFC 2307 Groups	☐ LDAP Server uses RFC 2307 style group membership RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).
Group Object Class	posixGroup Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".
Shell Authentication Group DN	If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login. Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

Step 11:

Scroll up and click **Select a container** next to the **Authentication containers** field.



https://192.168.1.2/system_authservers.php?act=new

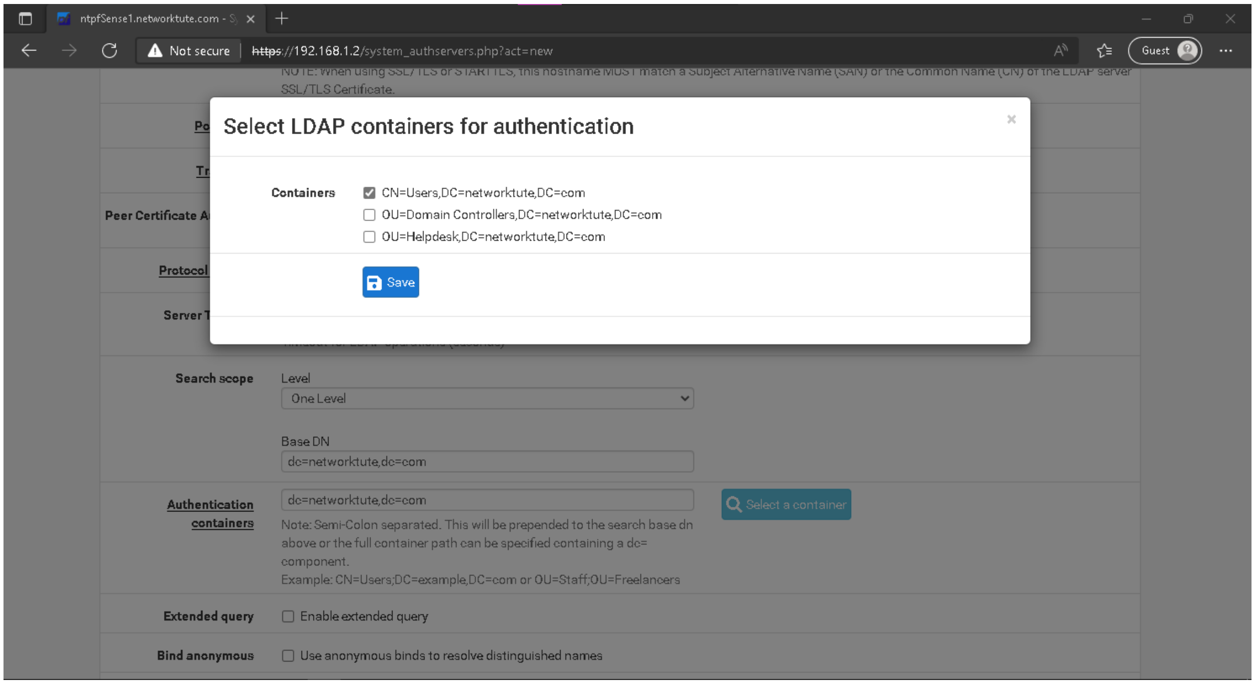
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.

Port value	389
Transport	Standard TCP
Peer Certificate Authority	No Certificate Authorities defined. Create one under System > Cert. Manager.
Protocol version	3
Server Timeout	25 Timeout for LDAP operations (seconds)
Search scope	Level: One Level Base DN: dc=networktute,dc=com
Authentication containers	dc=networktute,dc=com Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers
Extended query	☐ Enable extended query
Bind anonymous	☐ Use anonymous binds to resolve distinguished names

Step 12:

On the **Select LDAP containers for authentication** pop-up box, enable the **CN=Users,DC=NETWORKTUTE,DC=COM** checkbox.

Click **Save**.



Select LDAP containers for authentication

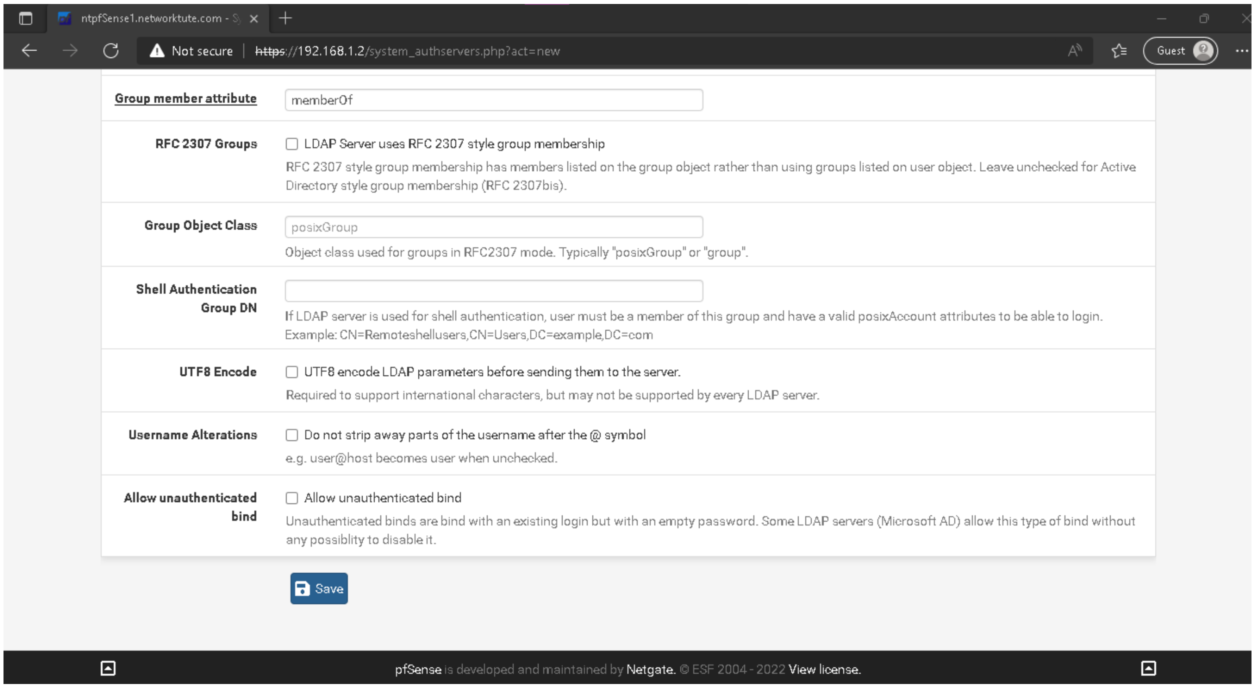
Containers
☑ CN=Users,DC=networktute,DC=com
☐ OU=Domain Controllers,DC=networktute,DC=com
☐ OU=Helpdesk,DC=networktute,DC=com

https://192.168.1.2/system_authservers.php?act=new

Search scope	Level: One Level Base DN: dc=networktute,dc=com
Authentication containers	dc=networktute,dc=com Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers
Extended query	☐ Enable extended query
Bind anonymous	☐ Use anonymous binds to resolve distinguished names

Step 13:

Scroll down and click **Save**.



Group member attribute: memberOf

RFC 2307 Groups: □ LDAP Server uses RFC 2307 style group membership

RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class: posixGroup

Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

Shell Authentication Group DN:

If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login. Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

UTF8 Encode: □ UTF8 encode LDAP parameters before sending them to the server.

Required to support international characters, but may not be supported by every LDAP server.

Username Alterations: □ Do not strip away parts of the username after the @ symbol

e.g. user@host becomes user when unchecked.

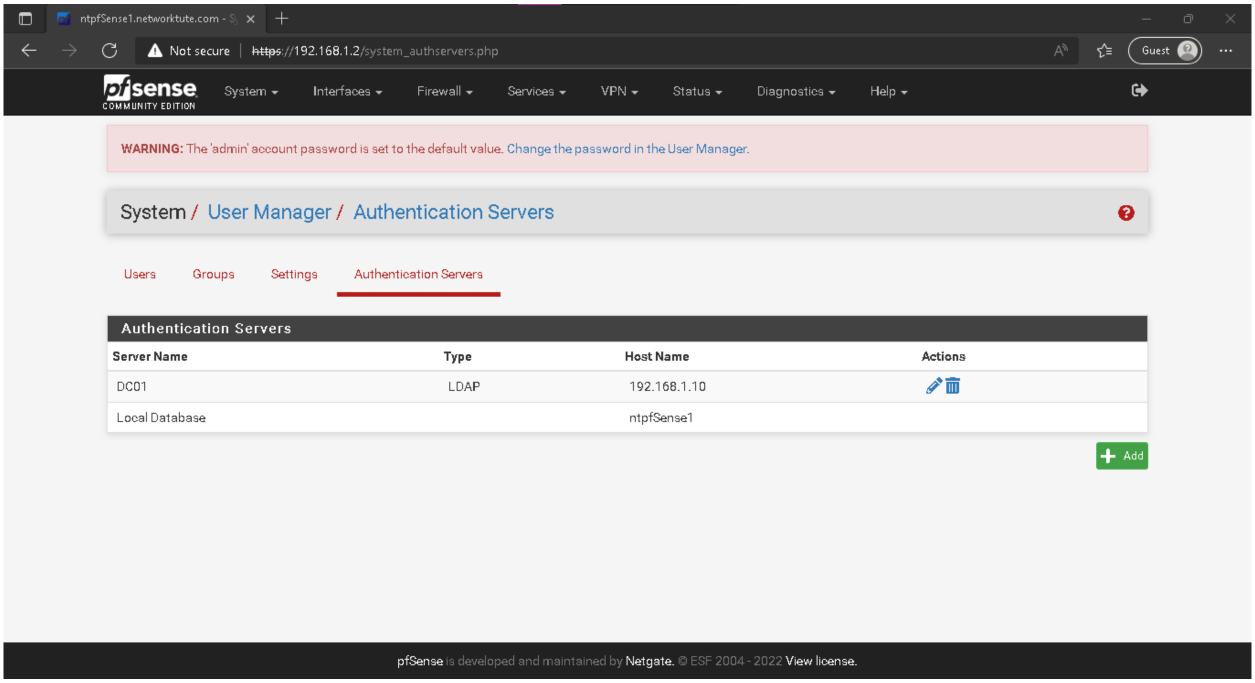
Allow unauthenticated bind: □ Allow unauthenticated bind

Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possiblity to disable it.

Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

Step 14:

On the **System / User Manager / Authentication Servers** page, the configured authentication server now appears



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / User Manager / Authentication Servers

Authentication Servers

Server Name	Type	Host Name	Actions
DC01	LDAP	192.168.1.10	
Local Database		ntpfSense1	

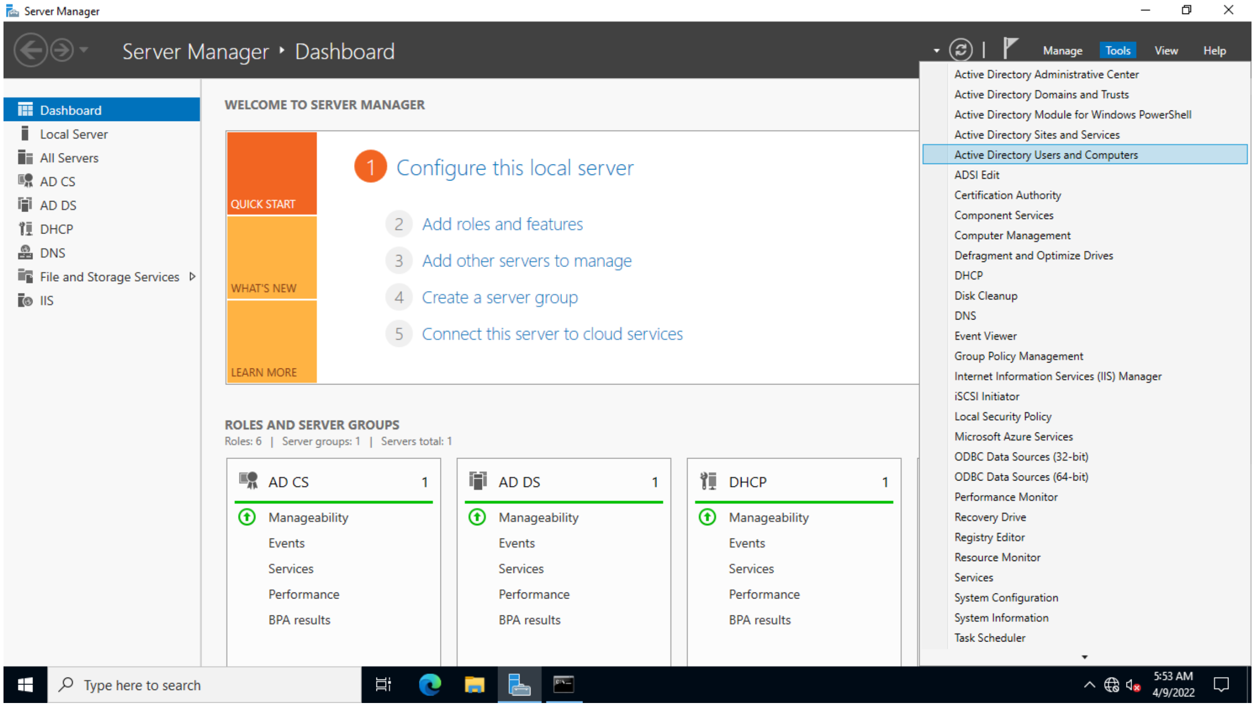
Add
pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

Step 15:

You will now create a new user in Active Directory.

Open **Server Manager** from the taskbar.

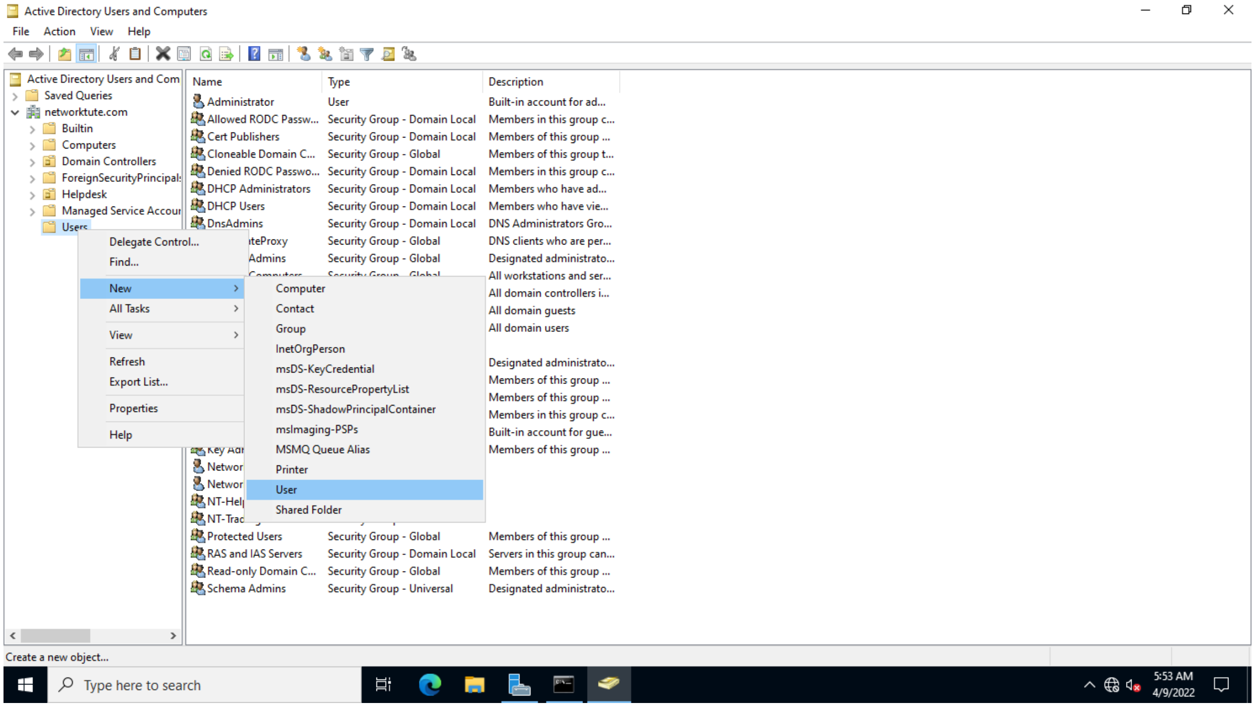
On the **Server Manager** window, click the **Tools** menu and select **Active Directory Users and Computers**



Step 16:

On the **Active Directory Users and Computers** window, expand **NETWORKTUTE.COM** if it's not already

Select and right-click on Users and select **New** > **User**.



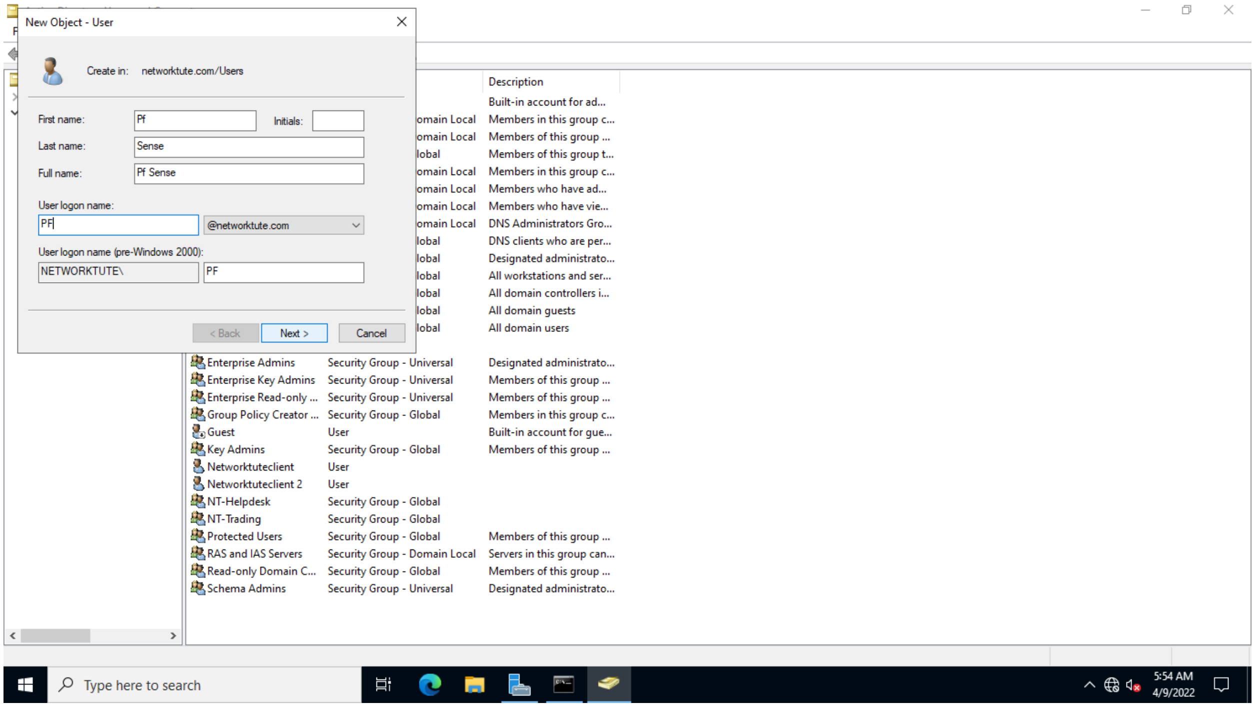
Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RODC Passw...	Security Group - Domain Local	Members in this group c...
Cert Publishers	Security Group - Domain Local	Members of this group ...
Cloneable Domain C...	Security Group - Global	Members of this group t...
Denied RODC Passwo...	Security Group - Domain Local	Members in this group c...
DHCP Administrators	Security Group - Domain Local	Members who have ad...
DHCP Users	Security Group - Domain Local	Members who have vie...
DnsAdmins	Security Group - Domain Local	DNS Administrators Gro...
teProxy	Security Group - Global	DNS clients who are per...
Admins	Security Group - Global	Designated administrato...
		All workstations and ser...
		All domain controllers i...
		All domain guests
		All domain users
		Designated administrato...
		Members of this group ...
		Members of this group ...
		Members in this group c...
		Built-in account for gue...
Key Ad		Members of this group ...
Networ		
Networ		
NT-Hel		
NT-Trac		
Protected Users	Security Group - Global	Members of this group ...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can...
Read-only Domain C...	Security Group - Global	Members of this group ...
Schema Admins	Security Group - Universal	Designated administrato...

Step 17:

On the **New Object** - **User** dialog box, enter the following:

First name: PF
Last name: Sense
User logon name: pf

Click **Next**.



New Object - User

Create in: networktute.com/Users

First name: Pf

Initials:

Last name: Sense

Full name: Pf Sense

User logon name:

PF @networktute.com

User logon name (pre-Windows 2000):

NETWORKTUTE\ PF

		Description
		Built-in account for ad...
	omain Local	Members in this group c...
	omain Local	Members of this group ...
	lobal	Members of this group t...
	omain Local	Members in this group c...
	omain Local	Members who have ad...
	omain Local	Members who have vie...
	omain Local	DNS Administrators Gro...
	lobal	DNS clients who are per...
	lobal	Designated administrato...
	lobal	All workstations and ser...
	lobal	All domain controllers i...
	lobal	All domain guests
	lobal	All domain users
Enterprise Admins	Security Group - Universal	Designated administrato...
Enterprise Key Admins	Security Group - Universal	Members of this group ...
Enterprise Read-only ...	Security Group - Universal	Members of this group ...
Group Policy Creator ...	Security Group - Global	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group - Global	Members of this group ...
Networktuteclient	User	
Networktuteclient 2	User	
NT-Helpdesk	Security Group - Global	
NT-Trading	Security Group - Global	
Protected Users	Security Group - Global	Members of this group ...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can...
Read-only Domain C...	Security Group - Global	Members of this group ...
Schema Admins	Security Group - Universal	Designated administrato...

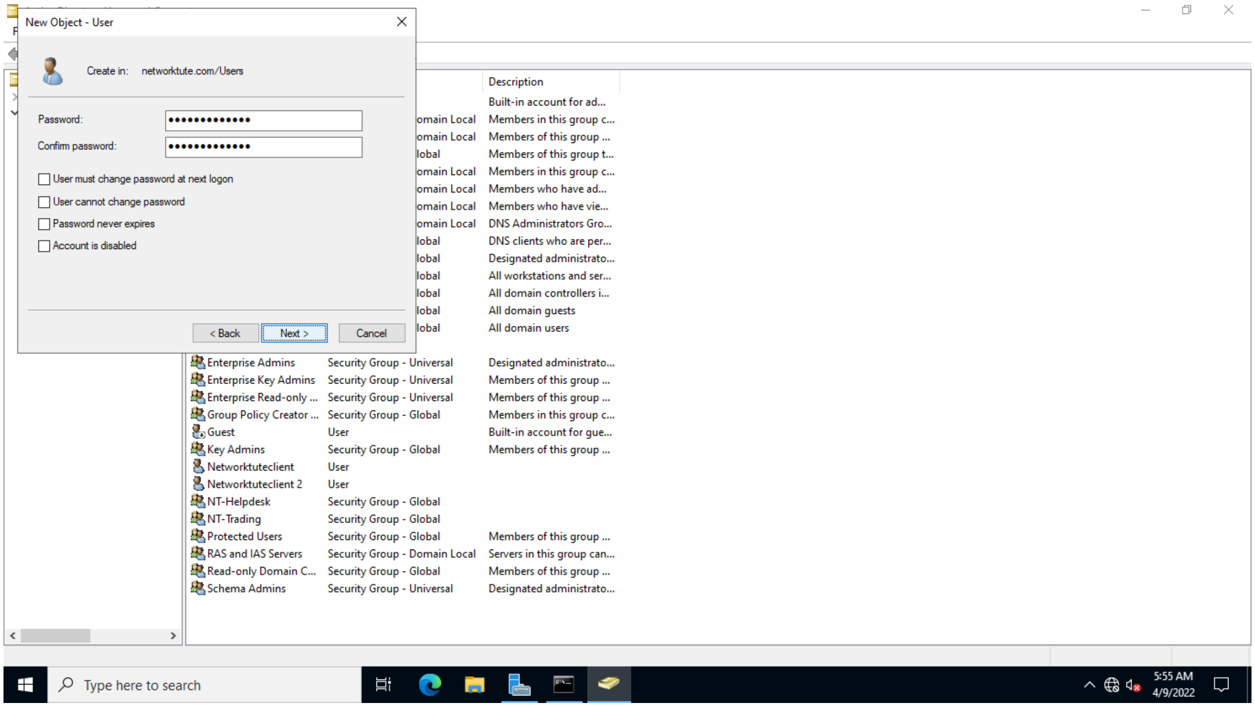
Step 18:

Type the following for the **Password** and **Confirm password** field:

Networktute@1

Uncheck the **User must change password at next logon** option.

Click **Next**.



New Object - User

Create in: networktute.com/Users

Password: •••••••••••••

Confirm password: •••••••••••••

□ User must change password at next logon

□ User cannot change password

□ Password never expires

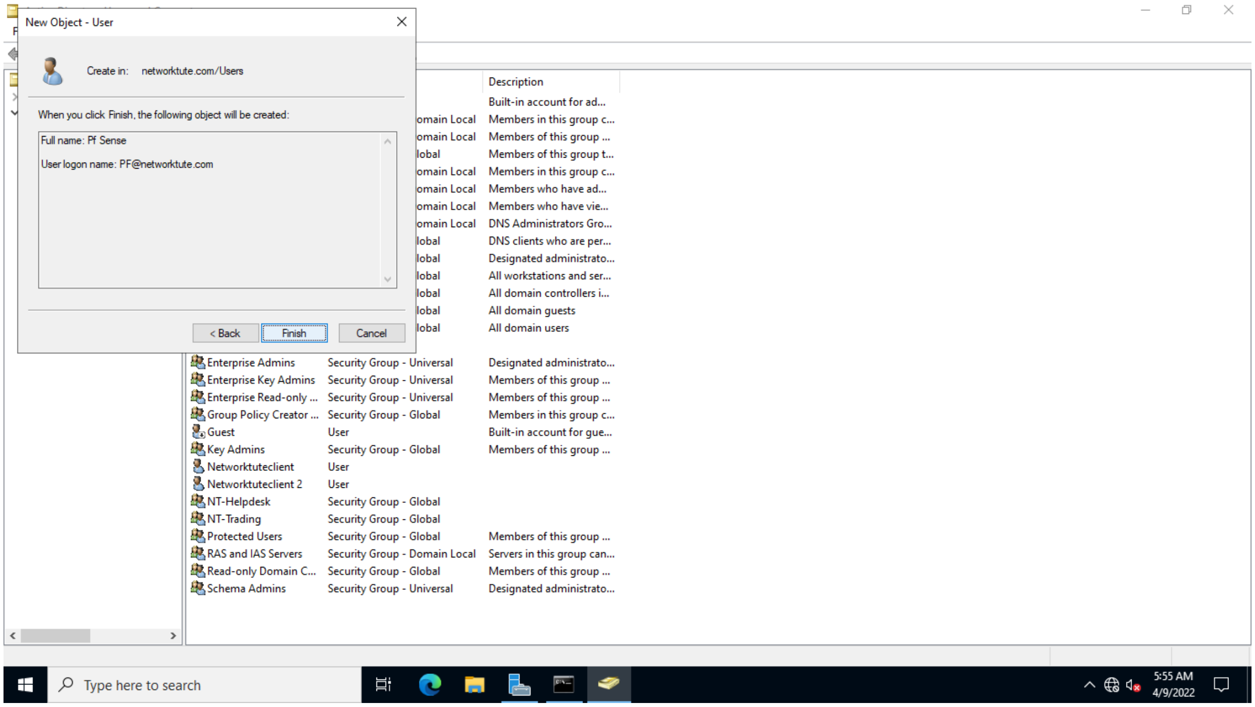
□ Account is disabled

< Back | Next > | Cancel

		Description
		Built-in account for ad...
	omain Local	Members in this group c...
	omain Local	Members of this group ...
	lobal	Members of this group t...
	omain Local	Members in this group c...
	omain Local	Members who have ad...
	omain Local	Members who have vie...
	omain Local	DNS Administrators Gro...
	lobal	DNS clients who are per...
	lobal	Designated administrato...
	lobal	All workstations and ser...
	lobal	All domain controllers i...
	lobal	All domain guests
	lobal	All domain users
Enterprise Admins	Security Group - Universal	Designated administrato...
Enterprise Key Admins	Security Group - Universal	Members of this group ...
Enterprise Read-only ...	Security Group - Universal	Members of this group ...
Group Policy Creator ...	Security Group - Global	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group - Global	Members of this group ...
Networktuteclient	User	
Networktuteclient 2	User	
NT-Helpdesk	Security Group - Global	
NT-Trading	Security Group - Global	
Protected Users	Security Group - Global	Members of this group ...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can...
Read-only Domain C...	Security Group - Global	Members of this group ...
Schema Admins	Security Group - Universal	Designated administrato...

Step 19:

Click **Finish**.



New Object - User

Create in: networktute.com/Users

When you click Finish, the following object will be created:

Full name: Pf Sense

User logon name: PF@networktute.com

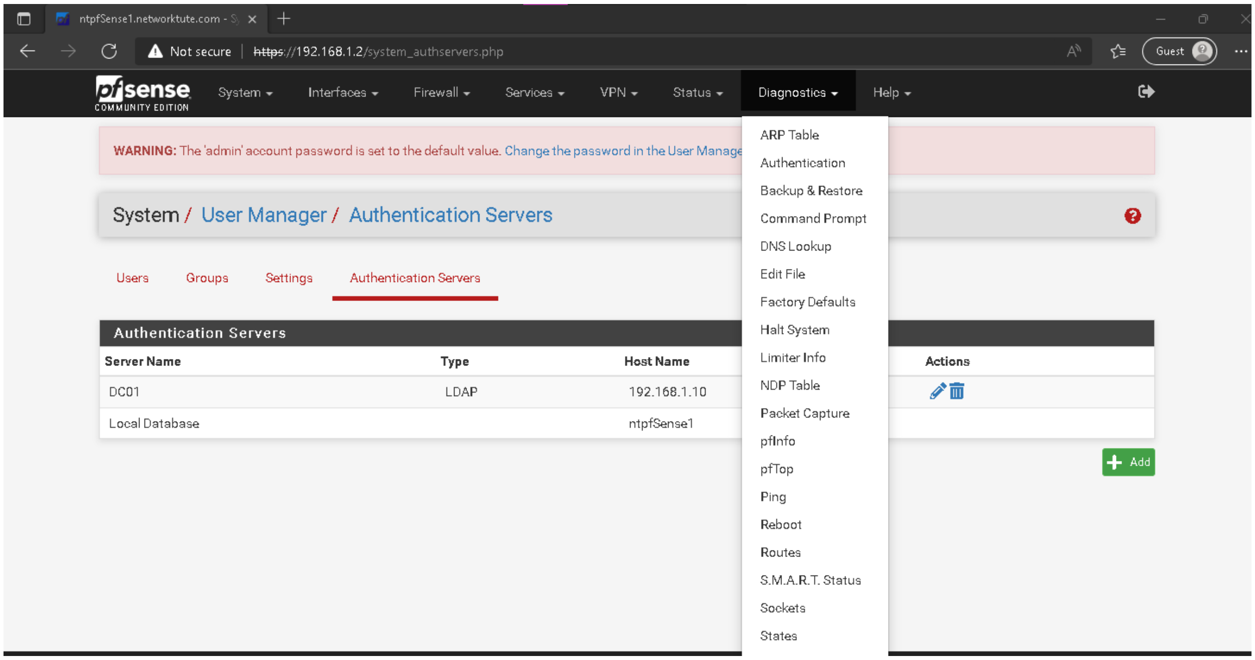
< Back | Finish | Cancel

		Description
		Built-in account for ad...
	omain Local	Members in this group c...
	omain Local	Members of this group ...
	lobal	Members of this group t...
	omain Local	Members in this group c...
	omain Local	Members who have ad...
	omain Local	Members who have vie...
	omain Local	DNS Administrators Gro...
	lobal	DNS clients who are per...
	lobal	Designated administrato...
	lobal	All workstations and ser...
	lobal	All domain controllers i...
	lobal	All domain guests
	lobal	All domain users
Enterprise Admins	Security Group - Universal	Designated administrato...
Enterprise Key Admins	Security Group - Universal	Members of this group ...
Enterprise Read-only ...	Security Group - Universal	Members of this group ...
Group Policy Creator ...	Security Group - Global	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group - Global	Members of this group ...
Networktuteclient	User	
Networktuteclient 2	User	
NT-Helpdesk	Security Group - Global	
NT-Trading	Security Group - Global	
Protected Users	Security Group - Global	Members of this group ...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can...
Read-only Domain C...	Security Group - Global	Members of this group ...
Schema Admins	Security Group - Universal	Designated administrato...

Step 20:

Restore **Microsoft Edge** browser from the taskbar. You will be on the **pfsense** web page.

Click the **Diagnostics** menu drop-down and select **Authentication**.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manage

System / User Manager / Authentication Servers

Authentication Servers

Server Name	Type	Host Name	Actions
DC01	LDAP	192.168.1.10	
Local Database		ntpfSense1	

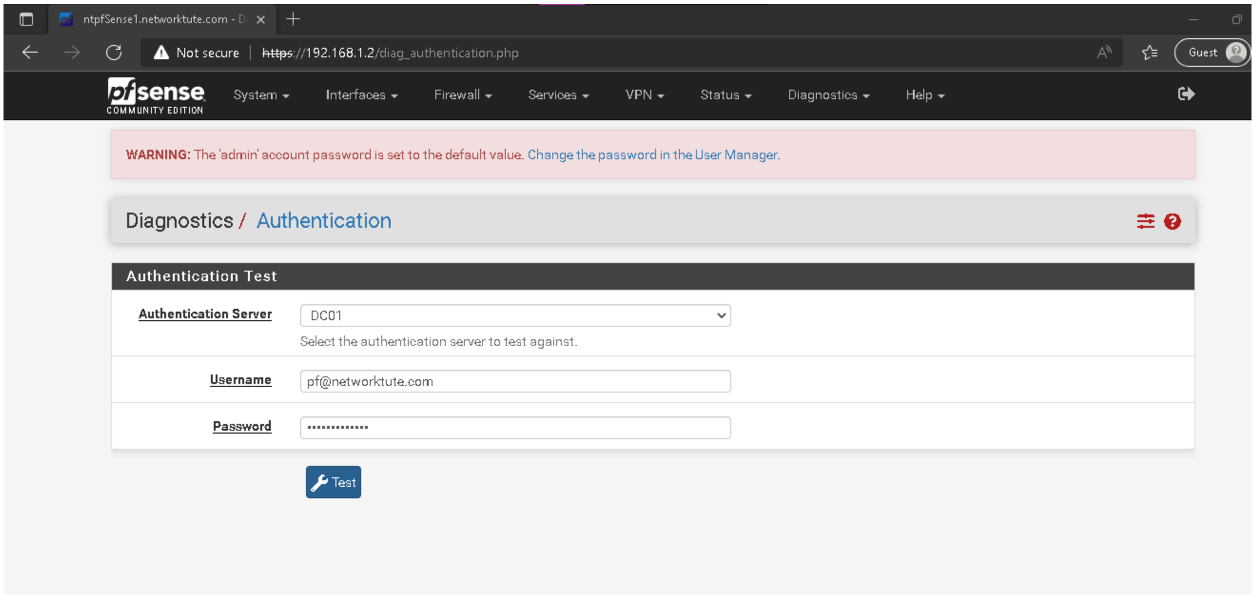
Step 21:

From the **Diagnostics** / **Authentication** page, select **DC01** as the **Authentication Server**.

Enter the following credentials:

Username: pf@networktute.com
Password: Networktute@1

Click **Test.**



ntpfSense1.networktute.com - D
Not secure | https://192.168.1.2/diag_authentication.php
Guest
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

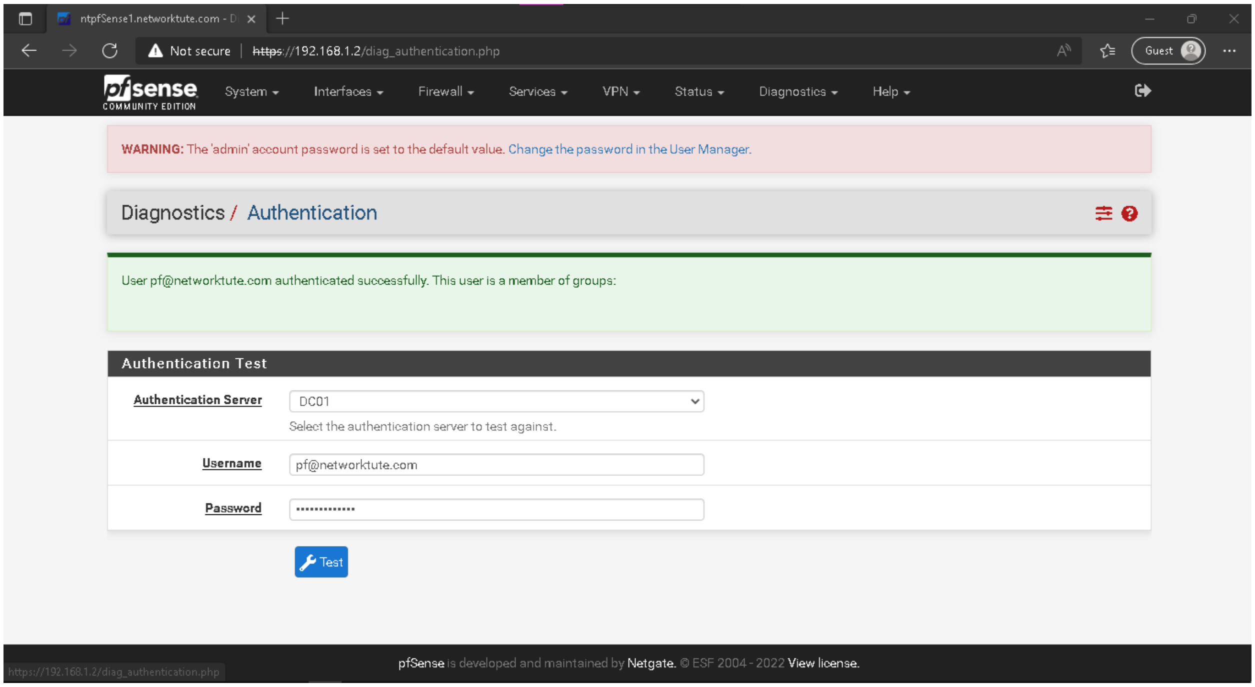
Diagnostics / Authentication

Authentication Test

Authentication Server	DC01 Select the authentication server to test against.
Username	pf@networktute.com
Password	••••••••••••••

Step 22:

You will get a successful authentication message in green once the test completes.



ntpfSense1.networktute.com - D
Not secure | https://192.168.1.2/diag_authentication.php
Guest
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Diagnostics / Authentication

User pf@networktute.com authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server	DC01 Select the authentication server to test against.
Username	pf@networktute.com
Password	••••••••••••••

Test
https://192.168.1.2/diag_authentication.php

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

Note: You can utilize the active directory for pfsense authentication now that you've connected your firewall with the active directory using the LDAP protocol. To accomplish this, go to System > User Manager Settings and activate AD authentication.

Close **Microsoft Edge** browser and **Active Directory Users and Computers** window.

MSSQL, Oracle and MySQL

Relational database servers include MSSQL, Oracle, and MySQL, to name a few. A database server is a client/server application that delivers database services to clients, which might be other programs or computers.

SQL (Structured Query Language) is a programming language that can be used to store, manage, and retrieve data from a database. The SQL database is a Microsoft software (database) that is commonly referred to as MSSQL. It's a relational database, which implies it's a collection of data items with pre-defined relationships. MSSQL is a database engine that runs on both Windows and Linux computers. The database engine is in charge of executing queries and keeping track of database files, pages, and indexes, among other things. Database objects (stored procedures, views, and triggers) are also created. Clients connect to an MSSQL database engine using TCP port 1433 by default, and the SQL Management studio connects to the database engine using the same port.

Oracle database is an RDMS (Relational Database Management System) developed by Oracle that is similar to MSSQL in many ways. It also functions in client/server mode, with clients connecting to the server via the SQLnet service on TCP port 1521.

Oracle and SQL both utilize SQL, however MSSQL uses T-SQL (Transact SQL) while Oracle uses PL/SQL (Procedure Language/SQL). The fundamental difference between these two languages is how they handle variables and stored procedures. T-SQL is simpler and easier to use than PL/SQL, which is more powerful and sophisticated.

Oracle owns MySQL, a widely used open-source database. It may run on a variety of operating systems, including Windows, Linux, and Unix. By default, clients connect to the MySQL port using TCP port 3306. MySQL also employs SQL for updating, querying, and managing data.

Task 4: Use RDP for Remote Connection

RDP (Remote Desktop Protocol) is a Microsoft protocol for gaining remote access to a computer running Windows. RDP is mostly used to connect to virtual machines (Windows servers) or for troubleshooting. The transport protocol is TCP, and the port number is 3389.

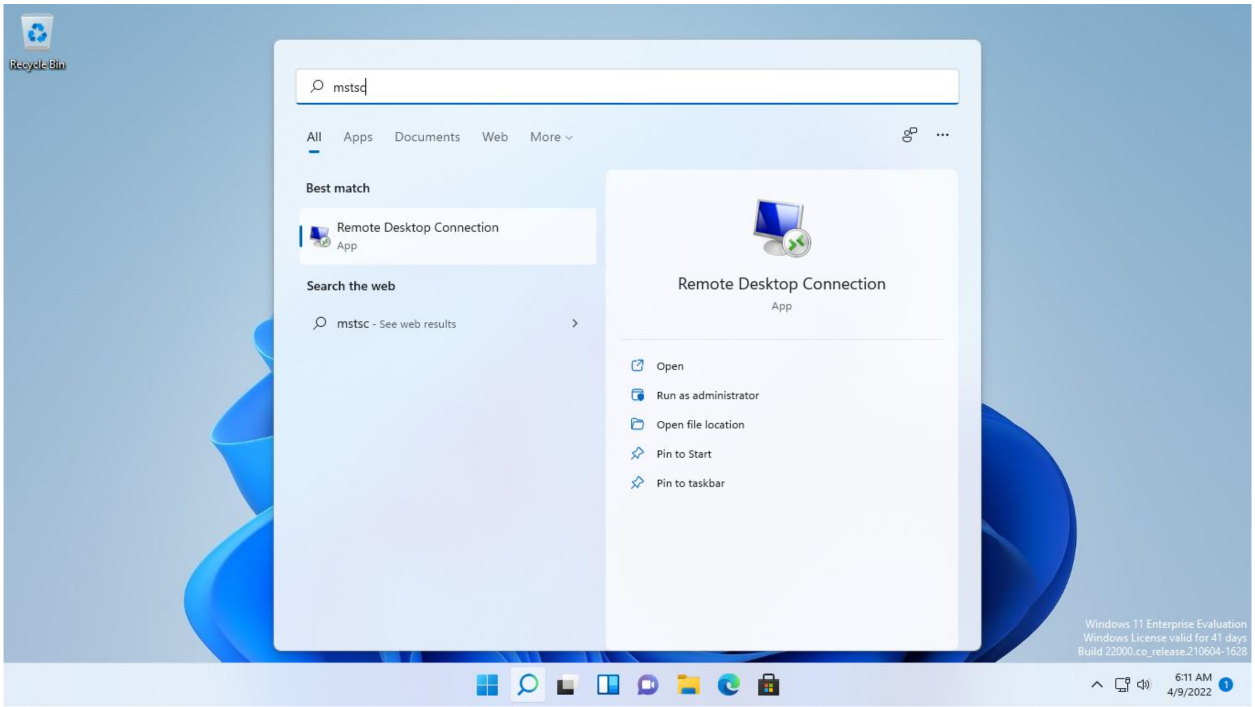
In this task, RDP will be used to access the **NTSER22VM1** server from the **NTWIN11VM1** machine.

Step 1:

Connect to **NTWIN11VM1**.

Click the **Start** menu and type: ***mstsc***

Select **Remote Desktop Connection**.

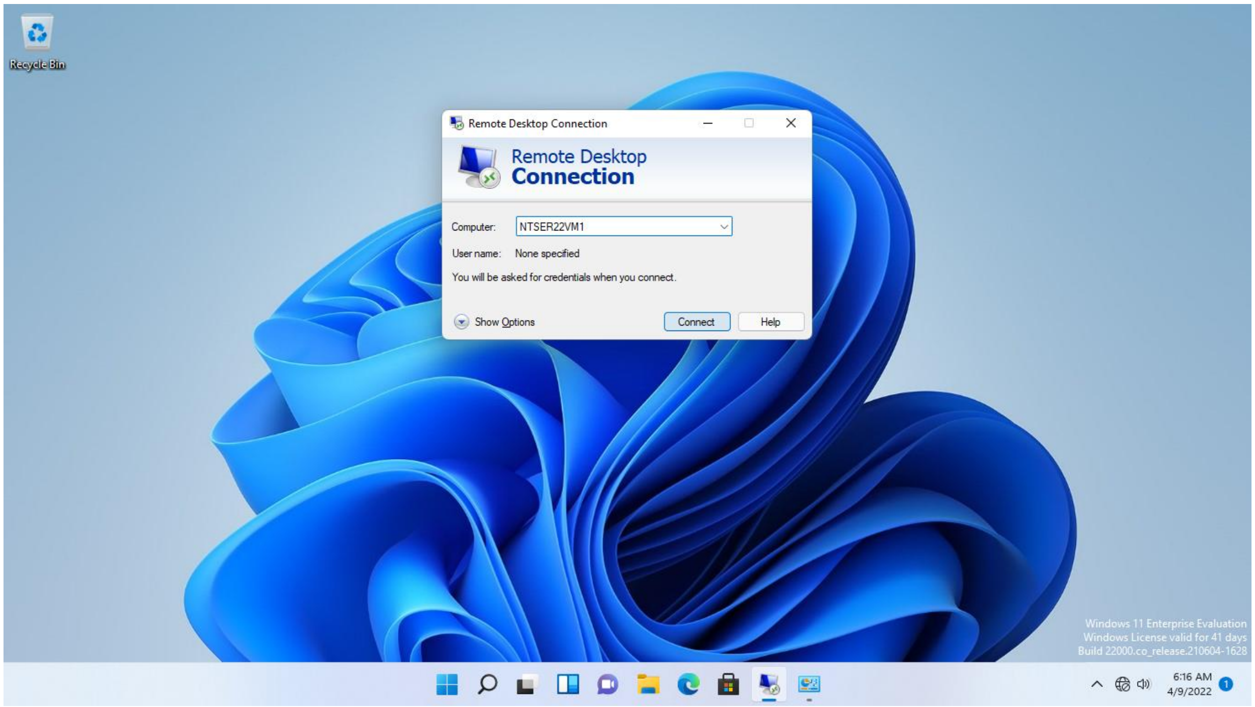


Step 2:

On the **Remote Desktop Connection** window, type the following for the **Computer** field:

NTSER22VM1

Click **Connect**.


Recycle Bin
Remote Desktop Connection
Remote Desktop
Connection

Computer: NTSER22VM1

User name: None specified

You will be asked for credentials when you connect.

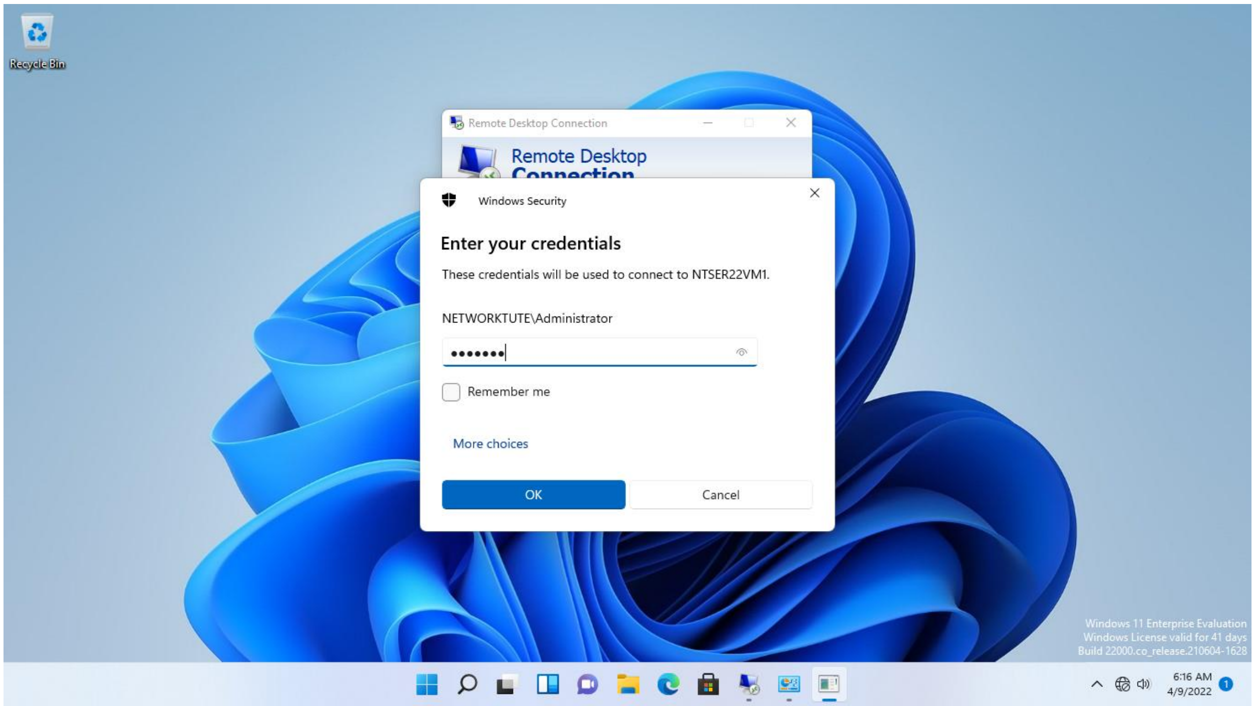
Show Options
Connect
Help
Windows 11 Enterprise Evaluation
Windows License valid for 41 days
Build 22000.co_release.210604-1628
6:16 AM
4/9/2022

Step 3:

On the **Windows Security - Enter your credentials** dialog box, type the following password:

Networktute@1

Click **OK**.



Windows Security

Enter your credentials

These credentials will be used to connect to NTSER22VM1.

NETWORKTUTE\Administrator

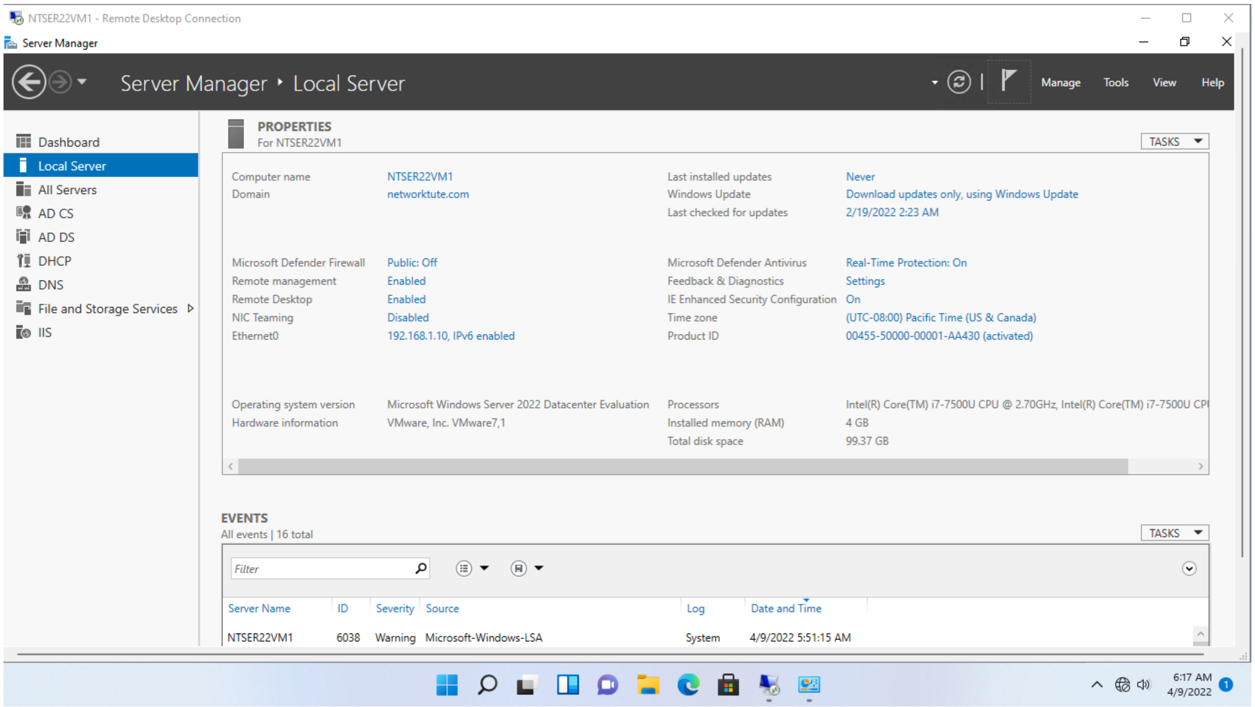
•••••••

□ Remember me

Recycle Bin
Remote Desktop Connection
Remote Desktop Connection
More choices
OK
Cancel
Windows 11 Enterprise Evaluation
Windows License valid for 41 days
Build 22000.co_release.210604-1628
6:16 AM
4/9/2022

Step 4:

You are now connected to **NTSER22VM1** over RDP protocol.



PROPERTIES
For NTSER22VM1

Computer name NTSER22VM1
Domain networktute.com

Last installed updates Never
Windows Update Download updates only, using Windows Update
Last checked for updates 2/19/2022 2:23 AM

Microsoft Defender Firewall Public: Off
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet0 192.168.1.10, IPv6 enabled

Microsoft Defender Antivirus Real-Time Protection: On
Feedback & Diagnostics Settings
IE Enhanced Security Configuration On
Time zone (UTC-08:00) Pacific Time (US & Canada)
Product ID 00455-50000-00001-AA430 (activated)

Operating system version Microsoft Windows Server 2022 Datacenter Evaluation
Hardware information VMware, Inc. VMware7,1

Processors Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz, Intel(R) Core(TM) i7-7500U CP
Installed memory (RAM) 4 GB
Total disk space 99.37 GB

EVENTS
All events | 16 total

Server Name	ID	Severity	Source	Log	Date and Time
NTSER22VM1	6038	Warning	Microsoft-Windows-LSA	System	4/9/2022 5:51:15 AM

Click (**X**) on the connection bar to disconnect the RDP session.

Click **OK** on the **Your remote session will be disconnected** message box.

Session Initiation Protocol (SIP)

Instead of traditional public switched telephone systems, most businesses now employ VoIP (Voice over IP) telephony services. Other multimedia services such as fax, SMS, video calls, and similar will also be transmitted over the Internet. VoIP is an acronym for Voice over Internet Protocol. Session Initiation Protocol (SIP), Real Time Transport Protocol (RTTP), and others RTP (Real-Time Transport Protocol), Secure RTP (SRTP), and others.

The SIP protocol is responsible for starting, regulating, and terminating multimedia sessions such as audio and video sessions, as well as messaging application sessions, in a multimedia context. SIP uses UDP as a transport protocol, and SIP clients connect to the server and other endpoints in the VoIP network via port 5060 or 5061. Unencrypted traffic is routed through port 5060, whereas encrypted traffic is routed through port 5061.

Unlike SIP, which is a signaling protocol, RTP and SRTP protocols are used for payload transmission (audio and video). These are voice and video transport protocols that use UDP as the transport protocol. They don't utilize a single port number, but rather a range of numbers beginning with 5004.

Internet Control Message Protocol (ICMP)

A network layer protocol is the Internet Control Messaging Protocol. It is the most extensively used protocol for debugging network device and host connectivity and availability. When the ping or traceroute, commands are entered into the command prompt, the ICMP protocol is used. ICMP isn't a transport protocol like TCP or UDP, and it's not used to send data. It's a network-layer diagnostic program.

IPSec, AH and ESP, GRE Tunnels

A virtual private network (VPN) secures and protects data traveling over a public network, such as the Internet. IPSec (Internet Protocol Security) is the primary protocol used in a VPN network, and it enables data authentication and encryption. You VPN and IPSec can be used to safeguard data between two hosts (computer to computer), for user remote access (computer to computer) or between two sites (router to router). router/firewall).

IPSec provides many functions and uses the following protocols:

- Authentication Header (AH) - Only data authentication is provided by IP protocol 51. (data integrity, data origin authentication, and replay protection)
- Encapsulating Security Payload (ESP) - Data confidentiality (encryption) and data authentication are provided via IP protocol number 50. (data integrity, data origin authentication, and replay protection)

Data authentication algorithms such as HMAC MD5, HMAC SHA1, HMAC SHA256, and HMAC SHA512 must be selected when configuring VPN. An encryption algorithm such as DES, 3DES, AES CBC Key Length 128, or AES CBC Key Length 256 must be used for the encryption section. For a VPN connection to be created, both sides must be setup with the same algorithm.

IPSec can be implemented in two modes:

- Transport mode - In this mode, only the IP payload is encrypted or authenticated. The header remains unchanged.
- Tunnel mode - In this mode, all IP packets are encrypted or authenticated, including the header.

One disadvantage of IPSec VPN tunnels is that they only support unicast, not multicast. If you need to use a routing protocol over IPSec, you'll need to employ GRE tunnels. The IP protocol number 47 is used by GRE.

GRE is a tunneling encapsulation obligation and does not offer loan money, but in alliance accompanying IPSec, you will have a secure resolution that supports multicast, broadcast and non-IP pacts in the way that Novell Internetwork Packet Exchange (IPX) and AppleTalk.