

Process Guide

Computer Security and Investigations

Aditya Patel, Jaspreet Singh Saini, Tuan
Khanh Vu, Ranvijay Singh & Matt Bastian

2020/04/15

Contents:

Process Guide.....	1
Introduction and summary:	4
Purpose of this Document:	4
Configuring components:	5
1. Setting up Active Directory on Windows Server 2019:.....	5
1.1 Initial configurations:.....	5
1.2 Installing Services:	6
1.3 Active Directory configuration:	6
1.4 Conclusion:	6
2. Hardening endpoints via GPOs (Windows 10 Workstation):.....	7
2.1 Creating a security template:.....	7
2.2 Configuring Policy Settings:.....	8
2.3 Saving Templates:	9
2.4 Applying the Security Template:	10
Security Template in Detail:.....	11
1 Account policies:	11
2 Local policies	12
2.1 User Rights Assignment.....	12
2.2 Security options	14
3 Administrative template (Computer).....	15
3.1 System	15
3.1.1 Audit Process Creation	15
3.2 Windows Components	15
3.2.1 App Package Deployment.....	15
3.2.2 Windows Remote Management (WinRM)	16
3.2.3 Windows Remote Shell.....	17
4 Administrative Template (User).....	18
4.1 Windows Components	18
4.1.1 Attachment Manager	18
4.1.2 Windows Installer	18

Problems faced:	20
3. Steps taken to setup Active Directory Delegated Scheme:	23
3.1 OU Security Model:	23
3.2 How to add OU and groups:	24
4. Configuring IPSEC VPN using pfSense and other features:	25
4.1 Basic Network Architecture:	25
VMWare virtual machine setup:	25
4.2 pfSense initial installation:	26
4.2.1 Booting via USB:	26
4.2.2 pfSense Command Menu:	28
4.2.3 pfSense Web Console:	29
4.3 Setup OpenVPN:	32
4.3.1 Generating Certificates:	32
4.4 Setup Authentication Server:	35
4.5 Setup OpenVPN:	38
4.6 OpenVPN installation on remote machine:	42
4.7 Enhancing security and more:	43
5. QNAP's NAS Recommended Settings:	44
5.1 Encrypted Volumes:	44
5.2 Network Access Protection:	44
6. Setting up encrypted volumes using VeraCrypt for better key management:	48
7. General Endpoint Security Recommendations:	49
7.1 Definition:	49
7.2 Endpoint Security Management:	49
7.3 Recommendation:	49
Works Cited:	51

Introduction and summary:

Creating a secure data transfer model consisting of secure hosts and data stores suitable for small businesses or accounting office environment using standardized tools.

Major components can be classified as follows:

- Establishing a minimum hardened endpoint standard for the secure hosts.
- Creating hardened builds via Group policies that could be deployed by a client.
- Creating an encrypted volume for storage with an easy to manage user and key management system, e.g. VeraCrypt & EFS via AD on the target server.
- Setup IPSEC VPN or Secure SMB for the secure tunnel with the storage volumes, or other app options.
- Outline a basic nested delegation scheme in AD to which the GPO's outlined above would be applied.

Aim: To create security in a box type option that can be given to a small business without much adjustment at their end.

Purpose of this Document:

This document will act as a guide to replicate the process of creating an environment as described above. It includes details about steps taken to configure each component required to start, improve and maintain secure communications between hosts and data stores.

This step-by-step guide includes the following:

- How to setup Active Directory manually on Windows Server 2019.
- How to create a Nested delegation scheme for Administrative tasks.
- How to apply recommended GPOs and security recommendations for hardening endpoints.
- How to setup IPSEC VPN using pfSense.
- How to encrypt storage volumes and manage keys using VeraCrypt.
- How to configure the QNAP NAS data store and best practices.

Configuring components:

1. Setting up Active Directory on Windows Server 2019:

The following instructions include steps taken to create a New AD forest and installation of other essential services for Windows Server 2019 Active Directory. Moreover, security recommendations from Microsoft for new domain controllers are also referenced for the server's security hardening.

1.1 Initial configurations:

- 1) Change the hostname of the server.
- 2) Open **Control Panel > Network and Internet > Network connection**. From there, select the network adapter the machine is using and go to its properties to set a static IP address in the TCP/IPv4 settings.
- 3) Set the preferred DNS server to the address of the server used for Active directory.

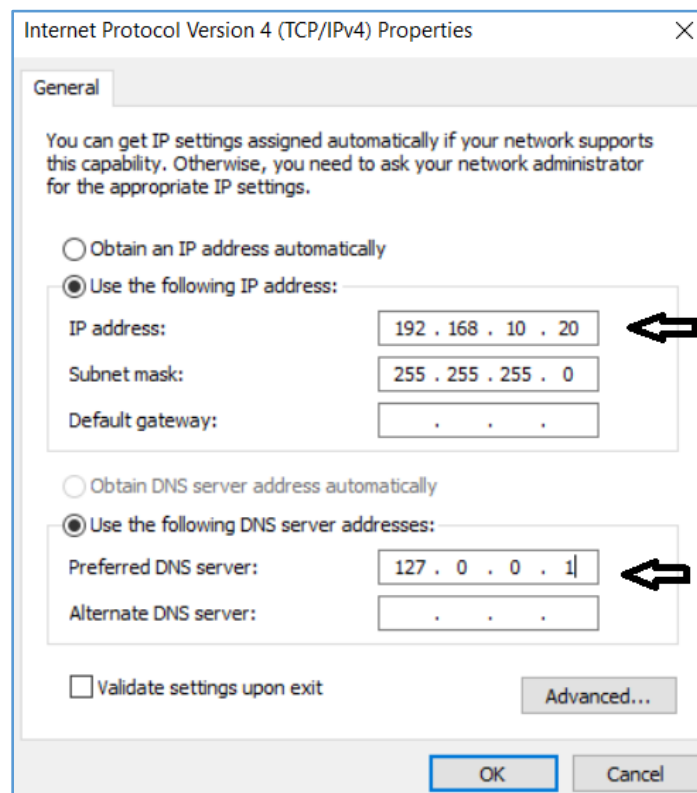


Figure 1. Setting static IP and preferred DNS server.

- 4) You can set any range of IPs for example 10.0.0.0 or 172.0.0.0 as well.
- 5) Fully patch both servers with the latest Windows updates from Microsoft.

1.2 Installing Services:

- 1) Open the Server Manager by hitting the “Windows” key on your keyboard.
- 2) In the Add Roles and Features Wizard, click next to the “Server Selection” tab and select your server.
- 3) Right-click on “Manage” add the following roles and features:
 - Active Directory Domain Services
 - DHCP Server
 - DNS Server
 - File and Storage Services

Features:

- File Server Resource Manager
- Web Server (IIS)
- .NET 4.5, .NET 3.5 (including ASP and ASP.NET)
- Simple TCP/IP
- Group Policy Management

You can add other features as well by following the “Add Roles and Features Wizard” depending on your work requirements.

- 4) At the end of the wizard confirm all selections and click “Install”. After installation succeeds, in the “Results” tab under Active Directory Domain Services select the option “Promote this server to a domain controller”. This will open a new wizard.

1.3 Active Directory configuration:

Once the Active Directory Domain Services Configuration Wizard is open follow these steps:

- 1) Under the “Deployment Configuration” choose the “Add a new forest” option and type in a non-routable DNS domain name. For example, “**abcd.local**” or “**54321.local**”.
- 2) On the Domain Controller options, select functional levels and set them both to “Windows Server 2016” if they are not already selected by default.
- 3) Also, leave the “Specify domain controller capabilities” as is.
- 4) Enter a password and click next at skip the DNS options and click next again.
- 5) Click next at all other tabs, you can check all the options you chose at the “Review Options” tab and at the “Prerequisites Check” screen click on “Install”.
- 6) After the installation is complete the system will reboot automatically and display the NEW domain login screen.

1.4 Conclusion:

Now you have Active Directory Domain Services installed and it can be managed using the Active Directory administrative tools.

2. Hardening endpoints via GPOs (Windows 10 Workstation):

2.1 Creating a security template:

- 1) Open Microsoft management console by either typing **"mmc"** in the windows search menu or pressing **"Windows Key + R"** then typing in **"MMC"**.
- 2) Open a console and add snap-ins. Snap-ins are entities in the Group policy management tool that allow a user to edit group policy objects, we can have selective snap-ins in our template.
- 3) Add security templates snap-ins to the console. Snap-ins added Security template, windows defender firewall, and local computer policy.

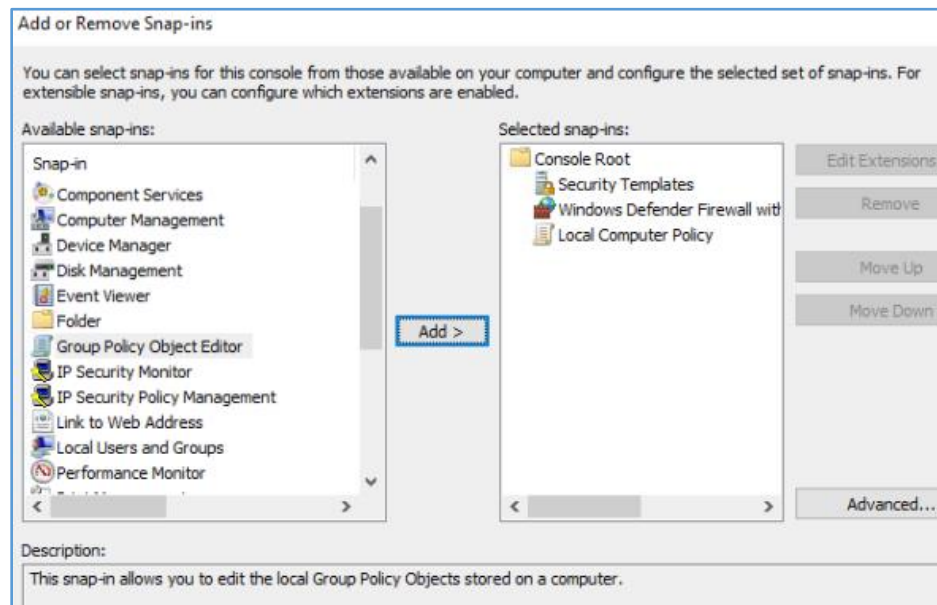


Figure 2. Add or Remove Snap-ins window.

- 4) Right-click and create a new template.

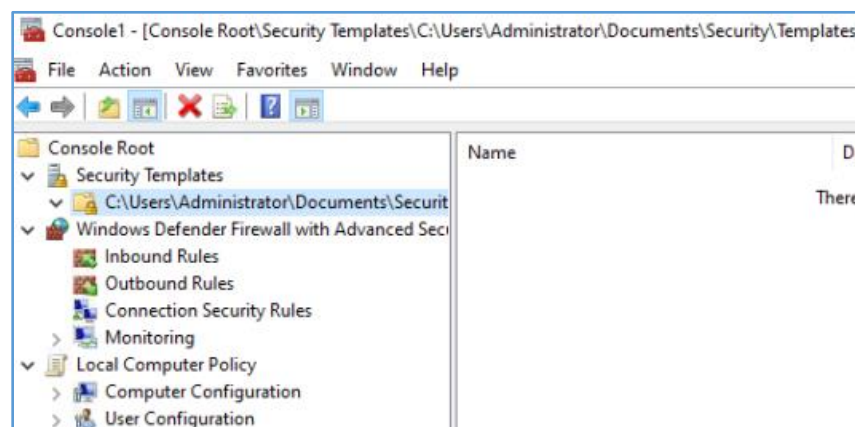


Figure 3. Creating a new security template.

- 5) Name the template. In our case – sever sec template. Click ok and continue. (Posey, 2018)

2.2 Configuring Policy Settings:

Steps for setting up policies are rather simple, all one needs to know is the path to the policy setting, the template tree is huge and complex.

Browse the directories and look for desirable and required policies fitting for your model.

Following are the steps to set or change any policy:

- 1) Select a policy, the policy I chose for this demonstration is: **'Access this computer from the network'** in the local security section.
- 2) The user interface path to the policy is - **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment****'Access this computer from the network'**

The default recommendation asks to set the policy to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only)

Description:

- This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).
- The recommended state for this setting is Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS.
- Accounts with the "Access this computer from the network" right may access resources on the system, and this right must be limited to those requiring it. If a user (without the right to access the server from the network) installs an application on their computer, and if the application requires the user to have the right to access the server, the application will not function properly.
- **Proposal** for a corporate environment (only selective users can access this computer from any network)
- Use the "Add User or Group" to add desired entities.

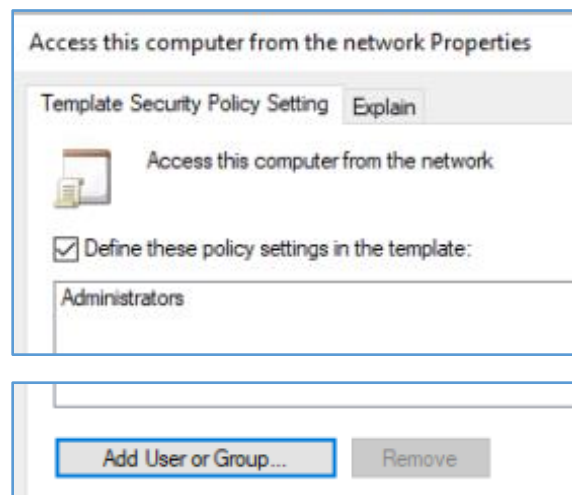


Figure 4. Add User or Group

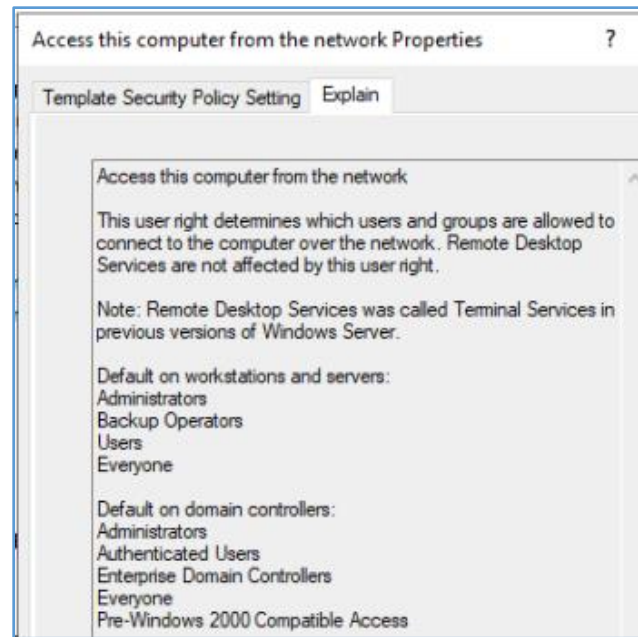


Figure 5. Policy explanation

Rationale:

Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the **Access this computer from the network** user right is required for users to connect to shared printers and folders. If this user right is assigned to the Everyone group, then anyone will be able to read the files in those shared folders. (Centre for Internet Security, 2020)

Purpose:

- To prevent users other than the Administrators from accessing the server machine.

2.3 Saving Templates:

- Once all the required policies are set. Save the console file (.msc). A .msc extension stands for Microsoft security compliance.
- This will be the location where the .inf file of the template will be saved. This file will be used to apply all the GPO settings.

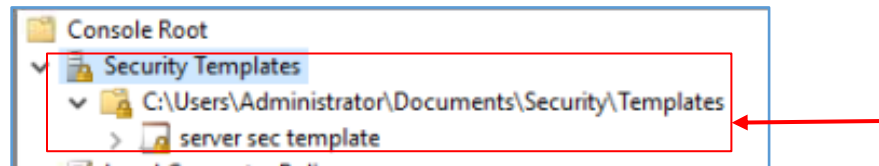
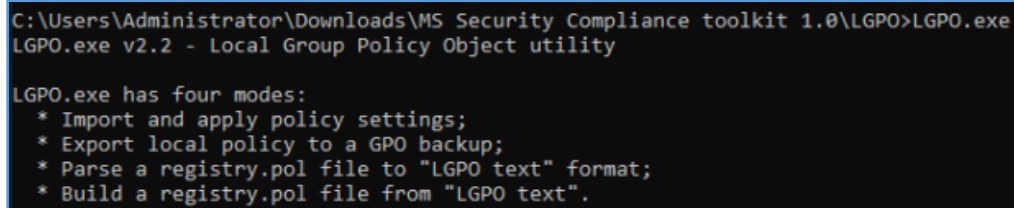


Figure 6. The saved template.

2.4 Applying the Security Template:

- We used a tool that comes with the Microsoft Security Compliance Toolkit 1.0 (available at the Microsoft website), to apply the above-made security template.
- The tool used was LGPO.exe to apply the security template.

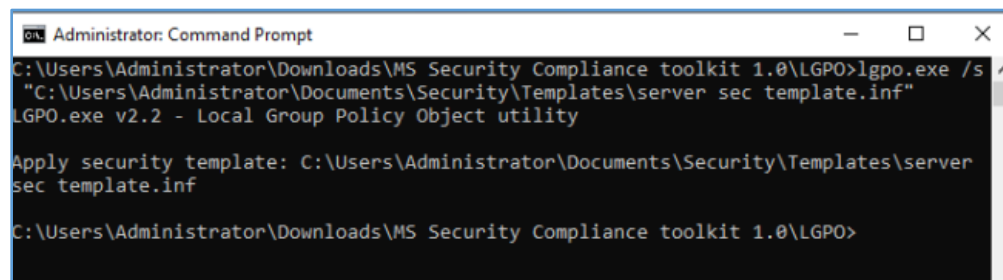


```
C:\Users\Administrator\Downloads\MS Security Compliance toolkit 1.0\LGPO>LGPO.exe
LGPO.exe v2.2 - Local Group Policy Object utility

LGPO.exe has four modes:
* Import and apply policy settings;
* Export local policy to a GPO backup;
* Parse a registry.pol file to "LGPO text" format;
* Build a registry.pol file from "LGPO text".
```

Figure 7. LGPO.exe

- The tool has extensive use, but here we used the command “lgpo.exe /s path\security_template.inf” to apply the above-made template.



```
Administrator: Command Prompt
C:\Users\Administrator\Downloads\MS Security Compliance toolkit 1.0\LGPO>lgpo.exe /s
"C:\Users\Administrator\Documents\Security\Templates\server sec template.inf"
LGPO.exe v2.2 - Local Group Policy Object utility

Apply security template: C:\Users\Administrator\Documents\Security\Templates\server
sec template.inf

C:\Users\Administrator\Downloads\MS Security Compliance toolkit 1.0\LGPO>
```

Figure 8. Applying the above-created template.

Security Template in Detail:

1 Account policies:

1.1 Password must meet complexity requirements:

Purpose:

- This policy setting is set to prevent users from creating weak passwords. Brute forcing attempts to become long and futile when dealing with more complex and long passwords.

Ensure 'Password must meet complexity requirements' is set to 'Enabled'

Description:

- This policy setting is used to maintain a minimum standard for new passwords' strength by ensuring that they meet the default requirements.
- When this policy is set to "Enabled", new passwords must meet the following requirements:
- Must not contain the account name of the user or parts of the user's full name that exceed two consecutive characters.
- Must be at least six characters in length.
- Should contain characters from three of the following categories:
 - English uppercase characters (A through Z) & English lowercase characters (a through z).
 - Base 10 digits (0 through 9).
 - Non-alphabetic characters (for example, !, \$, #, %).
 - "A catch-all category of any Unicode character that does not fall under the previous four categories. This fifth category can be regionally specific." (Centre for Internet Security, 2020)

The recommended state for this setting is: Enabled.

1.2 Minimum password length:

Purpose:

- This policy serves the same purpose as the one above, this policy setting is set to prevent users from creating weak passwords. Brute forcing attempts to become long and futile when dealing with more complex and long passwords.
- Ensure 'Minimum password length' is set to '14 or more character(s)'

Description:

This policy setting is used to maintain a minimum standard for a password's length for a user account by ensuring that they meet the minimum default requirements. There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is better than "password."

Rationale:

There are many different types of password attacks that would prove effective against weak passwords. For example, Dictionary attacks (using common words and phrases) & brute force attacks (Try every possible combination of characters.). Attackers try to obtain the account databases so they can use tools to discover the passwords for the accounts found in that database to get access.

2 Local policies

2.1 User Rights Assignment

To navigate to a policy, follow the UI path and look for the name of the desired policy in that directory.

UI PATH - Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\

2.1.1 Allow log on through Remote Desktop Services

Purpose:

- To block access to the server for everyone accepts entities conducting off-site maintenance.

Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators'

Description:

- This policy setting determines which users or groups have the right to log on as a Remote Desktop Services client.
- This user right should only be granted to the Administrators and the Remote Desktop Users group, to prevent unauthorized users from gaining access to computers on your network using Remote Assistance.

The recommended state for this setting is Administrators.

Rationale:

- Any account with this user right can log on to the remote console of the computer.
- If not configured properly this user right can give remote access to unauthorized users who can download and run malicious programs and possibly use it to elevate their privileges.

2.1.2 Create a token object

Purpose:

- To prevent any user from escalating privileges and obtain restricted information.
- Ensure 'Create a token object' is set to 'No One'

Description:

- This policy setting grants a process the permission to create an access token, that can give elevated rights to access sensitive data.

The recommended setting for this policy is No One.

Note: This user right is considered a "sensitive privilege" for auditing.

Rationale:

A user account with this right can gain complete control over the system, possibly compromising the system. It is highly recommended that this right should not be assigned to any user.

2.1.3 Debug programs

Purpose:

- This right can be exploited to capture hashed passwords or inject malicious code, to prevent that from happening only a select few people should have this right, for our testing only the administrator is given this right.

Ensure 'Debug programs' is set to 'Administrators'

Description:

- This policy setting allows users to attach a debugger to any process in the system or to the kernel, which grants complete access to sensitive and critical operating system components even the ones they don't own.

The recommended state for this setting is Administrators.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

This setting gives sensitive privileges to users which can be exploited to capture information from the system memory, access and modify kernel or application structures. Attack tools can be used to exploit this user's right to obtain hashed passwords and other private security information or to inject malicious code.

2.1.4 Generate Security Audit

Purpose:

- To have all the processes and services to generate security logs might look effective, but when investigating a security event, it will become difficult to find significant logs. To avoid that, selective processes and services are selected.

Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'

Description:

- This policy setting determines which users or processes have the privileges to generate audit records in the Security logs.

The recommended setting for this policy is LOCAL SERVICE, NETWORK SERVICE.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

An attacker could use this to flood the logs making it more difficult to locate any illicit activity. Also, if the event log is configured to overwrite events as needed, any evidence of unauthorized activities could be overwritten by many unrelated events.

2.2 Security options

UI Path - Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

2.2.1 Network access: Let Everyone permissions apply to anonymous users

Purpose:

- For a server running a service and anonymous user connecting to that service, this will let the users have additional permissions that the everyone group has on the domain, this right is to prevent such a scenario to take place.

Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'

Description:

- This policy, if set to “Enabled”; considers anonymous connections to the computer as a part of the network. Thus, the privileges that are set to “Everyone” will be applied to those anonymous connections as well.

The recommended state for this setting is **Disabled**.

Rationale:

An unauthorized user could anonymously gain access to sensitive information, giving rise to the possibility to perform social engineering attacks, or launch DoS attacks. (Centre for Internet Security, 2020)

3 Administrative template (Computer)

3.1 System

3.1.1 Audit Process Creation

3.1.1.1 *Include command line in process creation events*

UI PATH - Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events

Purpose:

- If multiple admins were to use this machine, log in through the command line is possible. If the command line input is being security audited, other admins with similar privileges can look for passwords and other information entered.

Ensure 'Include command line in process creation events' is set to 'Disabled'

Description:

- If this policy is set to “Enabled”, it will include command-line arguments and log that information under security audit events whenever a new process is created.

The recommended state for this setting is Disabled.

Rationale:

Command-line arguments often contain sensitive or private information like system info, usernames, and passwords. Enabling this policy will allow, any user who has read access to the security events permission to read the command-line arguments for any successfully created process. (Centre for Internet Security, 2020)

3.2 Windows Components

3.2.1 App Package Deployment

3.2.1.1 *Allow a Windows app to share application data between users*

UI PATH - Computer Configuration\Policies\Administrative Templates\Windows

Components\App Package Deployment\Allow a Windows app to share application data between users

Purpose:

- To isolate user data, if a user is compromised, app data shared by apps over an organization can also be compromised. To prevent information from being leaked.

Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'

Description:

- This policy allows a Windows app to share data between users on one system who have installed the app. Windows. Storage API contains a folder (SharedLocal) that holds all the data shared by users through an application.

The recommended state for this setting is Disabled.

Rationale:

Possibility of users accidentally sharing sensitive data with other instances of that app used by a different user.

3.2.2 Windows Remote Management (WinRM)

3.2.2.1 Allow remote server management through WinRM

UI PATH - Computer Configuration\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow remote server management through WinRM

Purpose:

- Although the network is trusted, all the management is done on a physical machine. For a larger enterprise, it is essential to set up remote server management, however, limiting the access to one or two personnel.

Ensure 'Allow remote server management through WinRM' is set to 'Disabled'

Description:

- This setting allows one to manage whether to allow windows remote management to accept HTTP requests automatically over the default HTTP port.

Recommended for this setting is: Disabled

Rationale:

Features that potentially enable inbound network connections are particularly risky. Only enable the use of the Windows Remote Management (WinRM) service on trusted networks, and where additional controls like IPsec can be implemented. (Centre for Internet Security, 2020)

3.2.3 Windows Remote Shell

3.2.3.1 Allow Remote Shell Access

UI PATH - Computer Configuration\Administrative Templates\Windows Components\Windows Remote Shell\Allow Remote Shell Access

Purpose:

- This policy is configured to stop the server from accepting new remote shell connections.

Ensure 'Allow Remote Shell Access' is set to 'Disabled'

Description:

- Enabling this policy will allow any new applications to gain remote access to the server and execute scripts and commands.
- Disabling this policy will stop any new remote shell to the server. However, pre-authorized users can gain remote shell access.

The recommended state for this setting is Disabled.

Rationale:

Enabling any inbound network connections to pose certain risks. We recommend enabling the policy on trusted networks only. (Centre for Internet Security, 2020)

4 Administrative Template (User)

4.1 Windows Components

4.1.1 Attachment Manager

4.1.1.1 Notify antivirus programs when opening attachments

UI PATH- User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments

Purpose:

- To catch illicit content when opening and attachment. In a scenario where mail servers don't catch a file containing any kind of malicious entity, this policy will call registered anti-viruses to scan the attachment.

Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'

Description:

- This policy setting notifies registered antivirus programs. Multiple programs can be notified, however, they ought to be registered.

The recommended state for this setting is Enabled.

Note: only updated antivirus programs will work with this policy.

Rationale:

Antivirus programs that do not scan downloaded files, this policy aids that avenue of risk. (Centre for Internet Security, 2020)

4.1.2 Windows Installer

4.1.2.1 Always install with elevated privileges

UI PATH - User Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges

Purpose:

- This policy is set to disable to prevent anything to be installed with escalated rights. If enabled, it will allow any user to install any program that requires access to files and directories restricted to that user.

Ensure 'Always install with elevated privileges' is set to 'Disabled'

Description:

- This policy determines whether any program on the system should be granted system permissions by Windows Installer when it installs.

- **Note:** To have this policy work effectively, you must configure it in both Computer Configuration and User Configuration folders.

The recommended state for this setting is Disabled.

Rationale:

Skilled individuals can take advantage of the permissions granted to the user by this setting, to change privileges and gain permanent access to restricted files. This can be done by a user adding their current account in local Admins groups by making a windows installer installation package that can make new local accounts that belong to the local built-in admin's group and have that account add the current account. And perform unauthorized activities by installing malicious software. (Centre for Internet Security, 2020)

Problems faced:

Administrative Templates (Computer)

MSS (Legacy)

UI PATH - **Computer Configuration\Policies\Administrative Templates\MSS (Legacy)**

Available when working with the Microsoft security compliance manager tool (SCM).

Below are the steps are taken to have MSS polices appear in the GPO manager. Since we were not working with SCM we regardless of that tried to install the toolkit. If you are required to work with SCM you will have to install a SQL server and its components to get it to fully work. SCM is a complex tool that requires additional downloads to work effectively, I decided to not proceed with it.

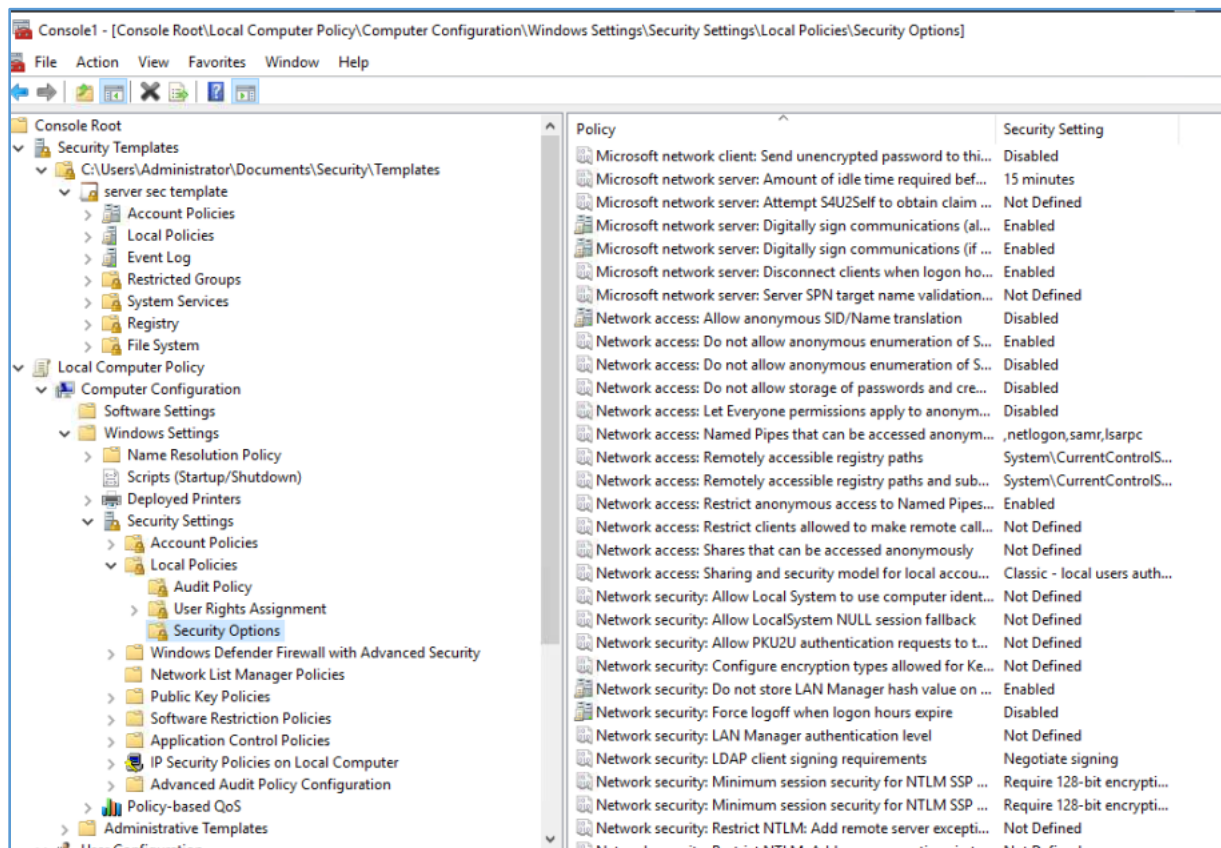
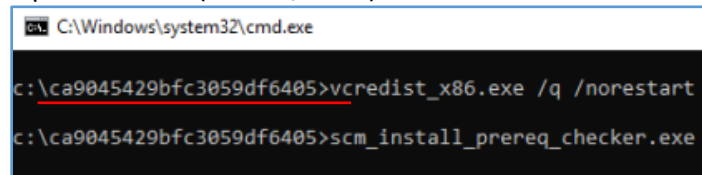


Figure 9. Console1.

While creating the group policy objects (GPOs) from these CIS benchmarks, we came across a problem of missing settings in our Group Policy Management console on Windows Server 2019. Use the following link to have MSS settings appear in your console.

<https://www.vmadmin.co.uk/microsoft/43-winserver2008/348-server2012mssgposettings>

The tool before starting installation prompts a command-line interface and creates a temporary folder (as shown in the illustration below.) This folder is supposed to have a LocalGPO.msi file that holds our desired network settings. But the problem was that for us the temporary folder did not have the LocalGPO.msi present in it. (Barnes, 2016)



```
C:\Windows\system32\cmd.exe

c:\ca9045429bfc3059df6405>vcredist_x86.exe /q /norestart
c:\ca9045429bfc3059df6405>scm_install_prereq_checker.exe
```

Figure 10. CLI to create a LocalGPO.msi file.

- The illustration below shows the contents of the temporary folder.

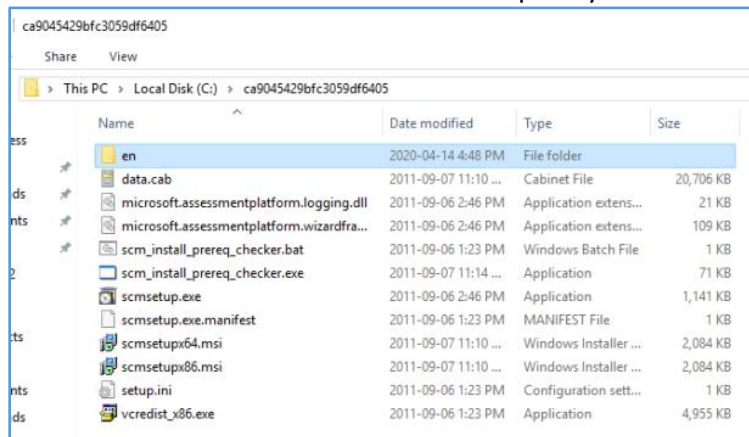


Figure 11. Contents of the temporary folder.

- Regardless we tried to proceed with the full installation again.
- The installation failed with an error.

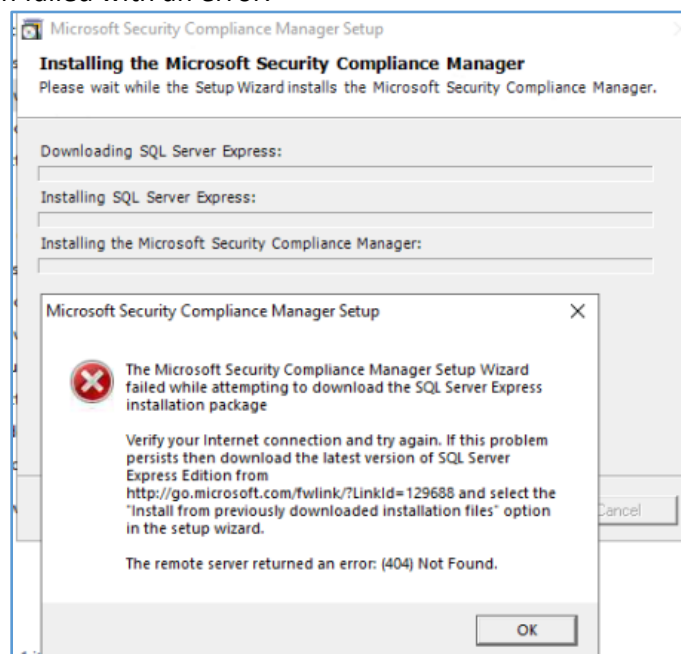


Figure 12. Error in installation.

The following are the MSS policies that were intended to implement.

- Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'.
- Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'.
- Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'.
- Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'.

(Centre for Internet Security, 2020)

3. Steps-taken to set up Active Directory Delegated Scheme:

Once Active Directory is set up and all the necessary features are installed; you can use the Active Directory Users and Computers to add OUs, Users, groups and assign different permissions to them.

For a small to medium scale businesses, it is recommended to not have too many roles as some might not be useful whereas having very few roles will result in no role separation.

Our recommended roles and permissions:

Service Administrators:

- Domain Admins - Highest service admin role across the domain. Only a few trusted administrators should have this level of authority. Has permissions to manage essential services as well as acts as an escalation role for admins with lower authority.

Data administrators:

- Tier 3 Admins – Authorized to manage all data admins and has granted permission to create new objects under the assigned OU. Acts as an escalation point for lower-level admins and manages them as well.
- Tier 2 Admins – Authorized to selectively create and delete users, computer accounts & groups that fall under their jurisdiction.
- Tier 1 Admins – Authorized to manage directory objects and perform tasks like password resets, updating user account properties or privileges, etc. (Michael, 2018)

You can add roles and separate some of these permissions to have a 4th Tier data admin or more service admin roles according to the organization's needs and structure.

3.1 OU Security Model:

Once the roles have been defined for the Organization, it is time to define your own OU security model.

The highest level of OU needs to be placed right under the Domain to manage and house all objects. It will be managed by service admins and acts as a topmost level of management over all other OUs. From here on, authority over directory services can start at the OU level instead of across the domain.

Below that OU, sub-OUs can be created to represent different offices, locations or headquarters, etc. These will be managed by data admin teams. Each of these OUs should have a common, inextensible ranking for ease of directory object management.

Lastly, to avoid privilege escalation you need to create groups for data admins in each sub-OU and then add an adequate number of admins to them. This helps us to restrict the admin accounts' jurisdiction to their designated level of management or lower. (Michael, 2018)

3.2 How to add OU and groups:

In order to create the OU model discussed above, we need to add groups for admins under each of the said OUs, add objects that will be controlled by the admins and then assigning administrative tasks to that group. Repeat this process for each OU and modify permissions when going a level up or down.

- 1) Open Active Directory Users and Computers.
- 2) Right-click on one of the OUs. Click “Delegate control” and hit the Next button.
- 3) On the Users or Groups page, click the “Add” button and add the users as well as admin groups that you want to delegate the controls to.
- 4) Here, you can select users, computers or groups to add and name them as well. If you are adding a new group, you can click the “Check Names” to double-check if the name is correct and then click OK.
- 5) Select the tasks you want to delegate to these users or groups. You can select common tasks or create custom tasks to delegate.

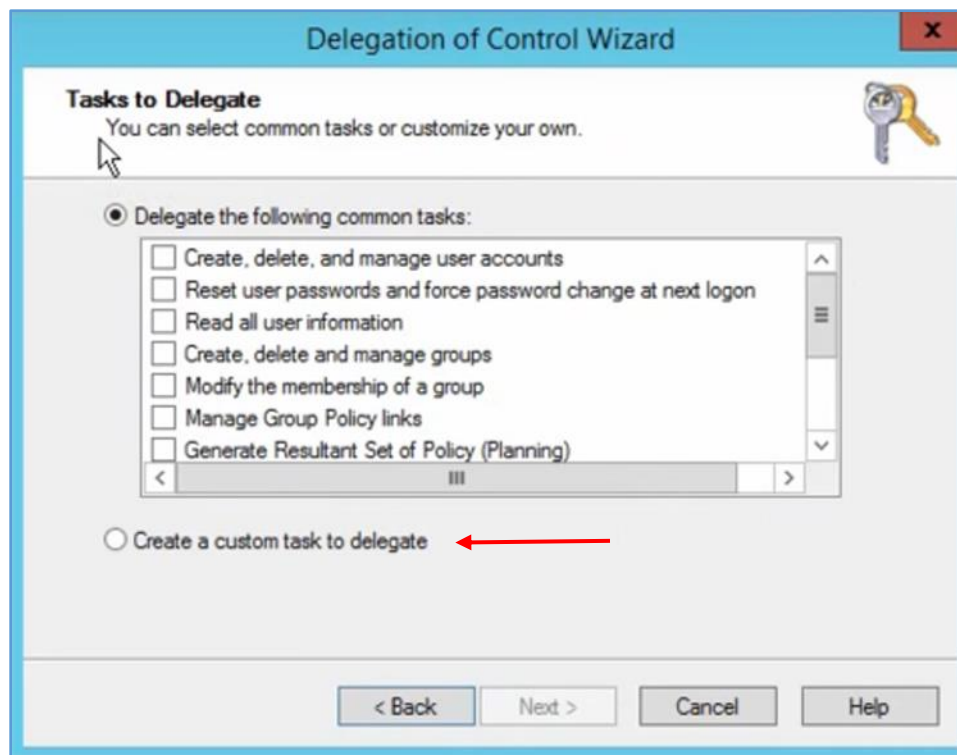


Figure 13. Tasks to Delegate.

- 6) Finally, verify the info on the final page of the wizard and click Finish.

4. Configuring IPSEC VPN using pfSense and other features:

4.1 Basic Network Architecture:

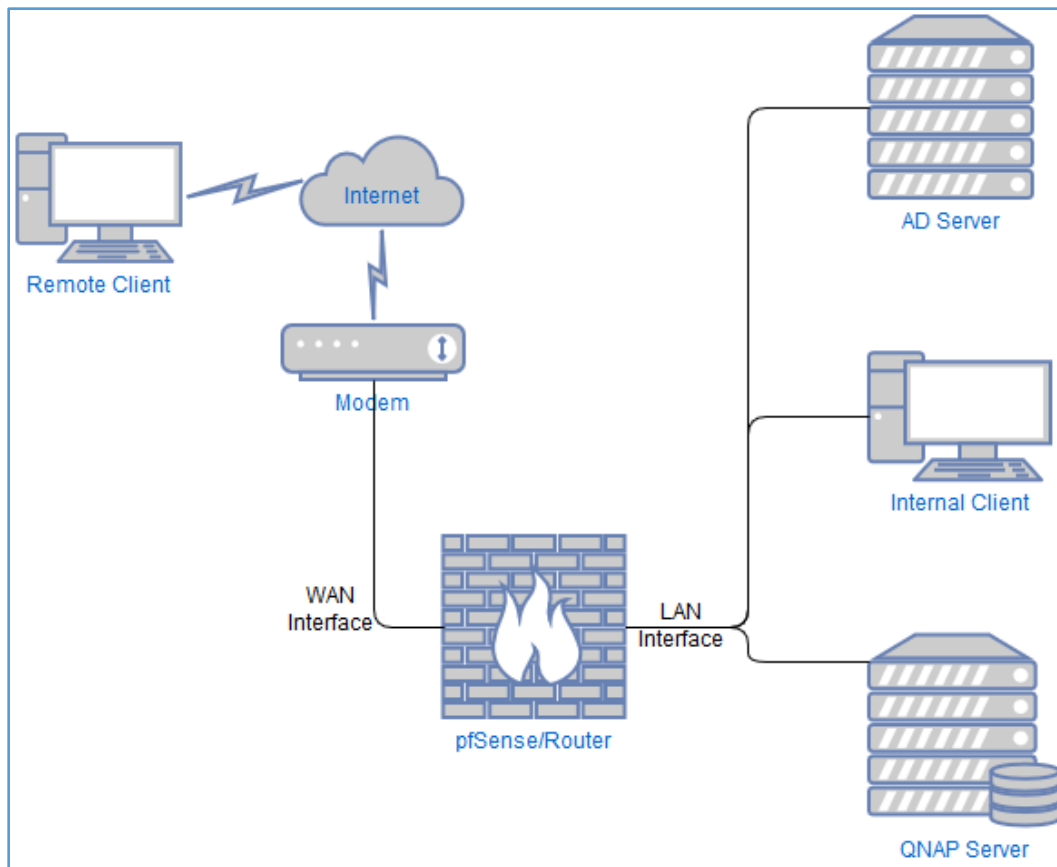


Figure 14. Basic architecture module.

For the demonstration part of the guide, we had set up a basic network infrastructure as shown above. The pfSense will act as a router with 2 interfaces: 1 WAN interface, and 1 LAN interface. However, in real life, you could set up multiple LAN interfaces, each attached to a specific subnet so that the network could be more secure.

VMWare virtual machine setup:

For demonstrating purpose, we are going to set up 3 Virtual Machines:

- Windows Server: 1 Adapter connected to the Custom VMnet3
- pfSense Virtual Machine: 2 Adapter (1 connected to the Custom VMnet3 and one is using NAT or Bridged)
- Client machine: 1 Adapter using NAT or Bridged (must be the same as the second adapter connected to the pfSense virtual machine)

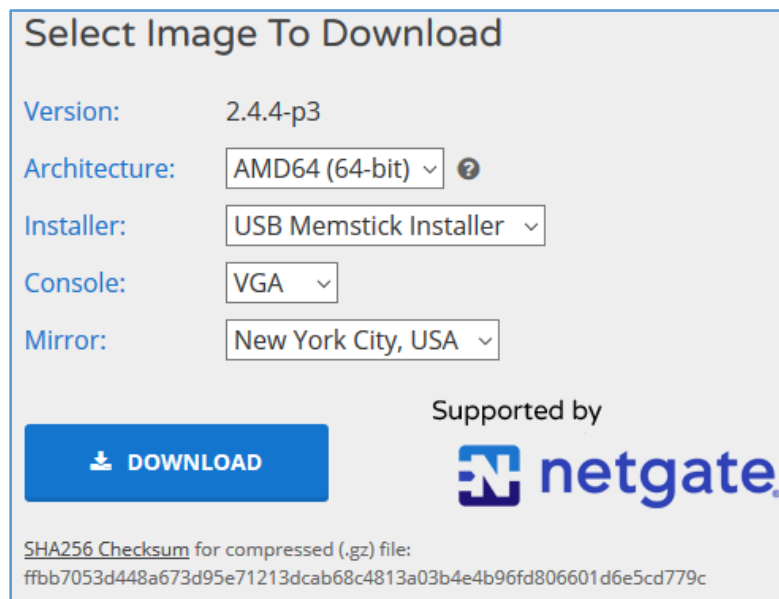
The Custom VMnet3 will act as the internal network, and the NAT or Bridged will act as the WAN network. You can choose to use the pfSense server as your DHCP server (we are going to show you how to do it below in this demonstration) or using another DHCP sources as well. However, you have to set up the default gateway of the internal network machines to the pfSense IP for this to work.

4.2 pfSense initial installation:

You can find the pfSense version of your choice from the website and download it using the link below.

pfSense: <https://www.pfsense.org/download/>

The most common way to install pfSense on your router is to use a bootable USB, you could also choose the console type as well as the region to download the image from. The version we are using for this environment is the community version, but the installation process is similar to the commercial version.



Select Image To Download

Version: 2.4.4-p3

Architecture: AMD64 (64-bit) ?

Installer: USB Memstick Installer

Console: VGA

Mirror: New York City, USA

Supported by

netgate

SHA256 Checksum for compressed (.gz) file:
ffbb7053d448a673d95e71213dcab68c4813a03b4e4b96fd806601d6e5cd779c

Figure 15. Download the pfSense image.

4.2.1 Booting via USB:

After you have installed the pfSense on your bootable USB boot up the router and select your USB as your boot source. Then, pfSense will prompt you with its' EULA. Select "Accept" to continue.

- Select the "Install" option to start installing pfSense.

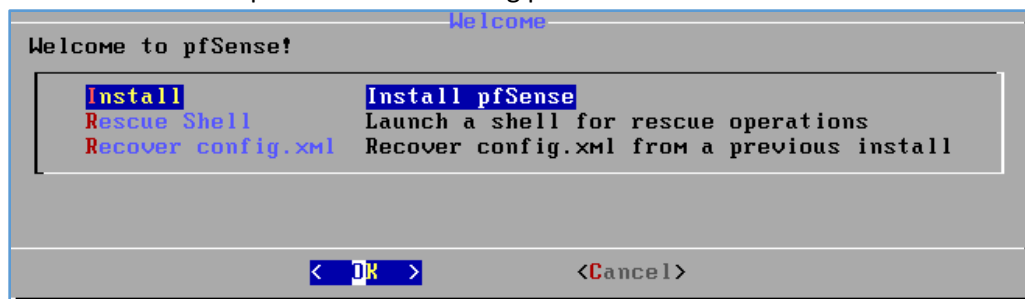


Figure 16. Start installing pfSense.

- Next, it will ask for what keyboard driver you are using, here, select one or use the default.

- Finally, it will ask you to partition your disk, here let the pfSense installer setup the disk partition for me using “Auto (UFS)” option.



Figure 17. Setup disk partition.

- After you have finished all the initial setup, it will ask if you want to access the shell first or just reboot the system. Here, we are going to finish the process and reboot the system.

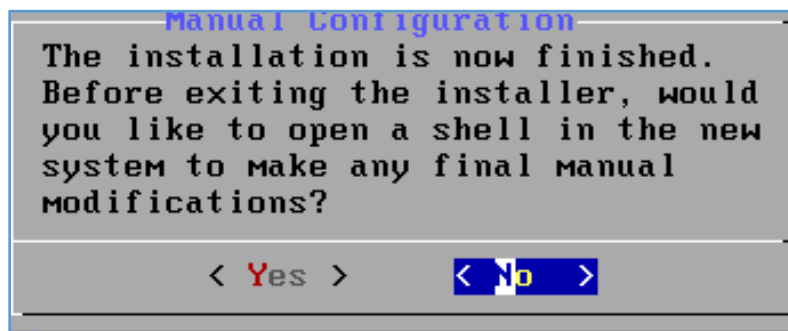


Figure 18. Finishing installation (1).

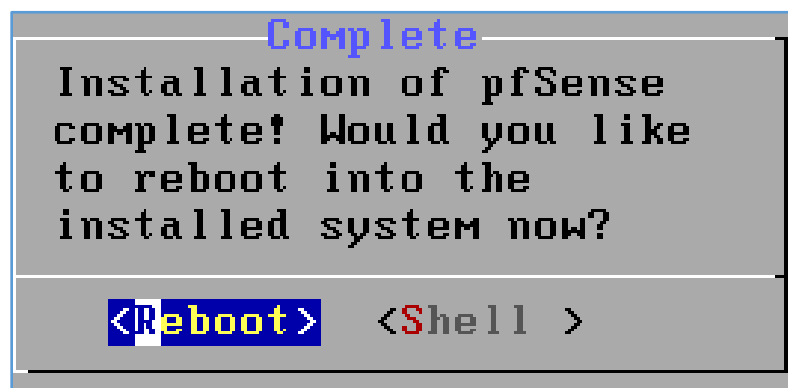


Figure19. Finishing installation (2).

4.2.2 pfSense Command Menu:

After the system is rebooted, you will be prompted with the pfSense command menu. As you can see, pfSense is going to have 2 interfaces: 1 WAN and 1 LAN. The WAN interface's IP is usually your public IP provided to you by the ISP. The LAN interface's IP is going to be a static IP you need to setup.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.4-RELEASE (Patch 3) amd64 Wed May 15 18:53:44 EDT 2019
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 81ded13cf3cd0b484046

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.2.57/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address ←
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults    12) PHP shell + pfSense tools
5) Reboot system              13) Update from console
6) Halt system                14) Enable Secure Shell (sshd)
7) Ping host                  15) Restore recent configuration
8) Shell                      16) Restart PHP-FPM

Enter an option: █
```

Figure 20. The pfSense command menu.

To change the LAN's IP, choose option "2" which is "Set interface(s) IP address", and choose option "2" which is the LAN interface. Here I am going to set it to 192.168.31.1 which is also going to be the router IP. I also need to give it a subnet mask because this is just for demonstration purpose only, I will set it to 24.

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.31.1 █
```

Figure 21. Setup LAN interface IP.

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24 █
```

Figure 22. Set up a LAN interface netmask.

- The next two options could be skipped since we are not going to use IPv6.

```

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

```

Figure 23. Setup LAN IPv6

- Finally, we need to set up the DHCP server on the pfSense so that it could distributing IPs to the machines that are connected to the LAN interface.

```

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.31.10
Enter the end address of the IPv4 client address range: 192.168.31.100
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

The IPv4 LAN address has been set to 192.168.31.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.31.1/
Press <ENTER> to continue.

```

Figure 24. Setup the LAN interface DHCP server

4.2.3 pfSense Web Console:

Now, the machines on the Local network could access pfSense web console using the IP on the LAN interface which is 192.168.31.1. The default username for the pfSense is “admin” and the password is “pfsense”

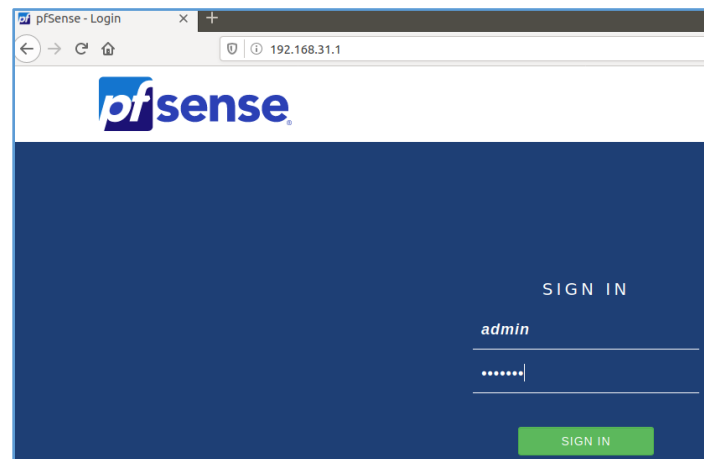


Figure 25. pfSense web console.

- After login, you will have to go through the pfSense setup wizard on the web GUI.

For the General Information, we will have to enter the Hostname and the domain that you want pfSense to use, this could be used as an alternative method for using the IP address if you have a centralized DNS server since we do not set up the DNS server and use google public DNS server, this process could be omitted.

The screenshot shows the 'General Information' step of the pfSense setup wizard. The breadcrumb trail at the top is 'Wizard / pfSense Setup / General Information'. A progress bar indicates 'Step 2 of 9'. The title is 'General Information'. Below the title, a message states: 'On this screen the general pfSense parameters will be set.' The form contains the following fields: 'Hostname' with the value 'pfSense' and an example 'EXAMPLE: myserver'; 'Domain' with the value 'Project.com' and an example 'EXAMPLE: mydomain.com'; 'Primary DNS Server' (empty); 'Secondary DNS Server' (empty); and 'Override DNS' which is checked with a red checkbox. Below the checkbox, it says 'Allow DNS servers to be overridden by DHCP/PPP on WAN'. At the bottom right is a blue button labeled '>> Next'.

Figure 26. Setup pfSense general information.

- Next, we need to set up the time zone that you want the pfSense system to be run on. For security and auditing purposes we are going to use the universal UTC.
- Next, we need to configure the WAN and LAN interface(s). However, we have already configured them in the earlier command menu, we could press “next” to continue with the next process.

The screenshot shows the 'Configure LAN Interface' step of the pfSense setup wizard. The breadcrumb trail at the top is 'Wizard / pfSense Setup / Configure LAN Interface'. A progress bar indicates 'Step 5 of 9'. The title is 'Configure LAN Interface'. Below the title, a message states: 'On this screen the Local Area Network information will be configured.' The form contains the following fields: 'LAN IP Address' with the value '192.168.31.1' and a note 'Type dhcp if this interface uses DHCP to obtain its IP address.'; and 'Subnet Mask' with the value '24' and a dropdown arrow. At the bottom left is a blue button labeled '>> Next'.

Figure 27. Setup LAN interface

NOTE:

Since we set up our virtual machine WAN interface to use Bridge or NAT which will be in private subnet such as (192.168.0.0/24). Therefore, we need to disable the “Block RFC1918 Private Networks” and “Block bogon networks” option under the WAN interface setup. This only relevant for testing purposes since we will not want to have private IPs entering our WAN interface in real life, so note that these two options should only be disabled for testing purposes.

RFC1918 Networks

Block RFC1918 Private Networks ☐ Block private networks from entering via WAN
 When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks ☐ Block non-Internet routed networks from entering via WAN
 When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

» Next

Figure 28. Allowing Private Network's IPs entering our WAN interface.

- The final part of setting up the pfSense is to change the default admin password. The more complex the password is, the better.

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

» Next

Figure 29. Change the admin default password.

- Now that all the installation process is finished, pfSense will ask you to reload.

Wizard completed.

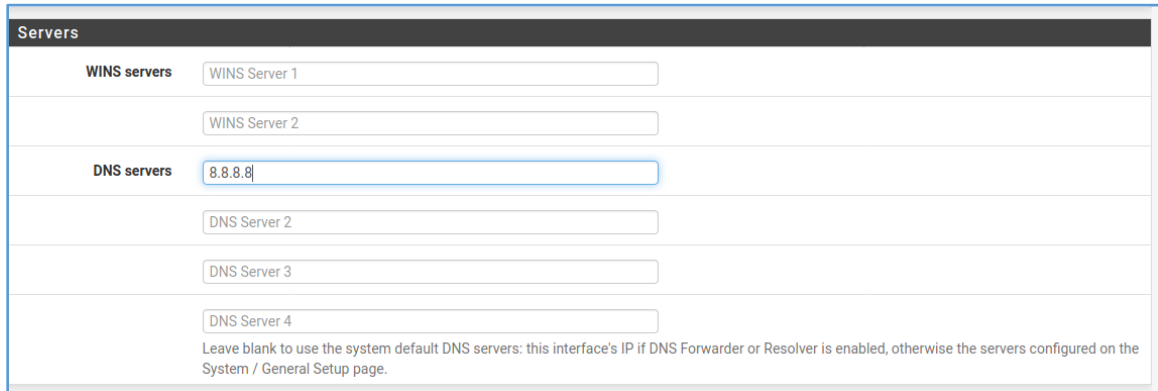
Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Figure 30. Finish up the pfSense initial configuration.

- Finally, we need to DHCP client of pfSense to have a DNS server. To do that on the top menu bar, choose “Services/DHCP Server”, scroll down to the Servers option, enter the IP of 8.8.8.8 which is the google DNS server IP address. If you have a DNS server set up already, you could use the IP of that server here.



Servers	
WINS servers	WINS Server 1
	WINS Server 2
DNS servers	8.8.8.8
	DNS Server 2
	DNS Server 3
	DNS Server 4

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

Figure 31. Setup a DNS server for DHCP clients.

4.3 Setup OpenVPN:

4.3.1 Generating Certificates:

- We will set up the OpenVPN tunnel for the remote client using the pfSense firewall application which will be installed on the Router. There will be 2 interfaces: WAN interface which will be connected to the Internet and has a public IP address, and LAN interface which will be connected to the internal network.
- The pfSense Firewall could be accessed using the IP address of the LAN interface. First, for security purposes, the default password to login to the web console of pfSense needs to be changed, this could be done under the “System/Users Manager”.
- After editing the default admin login privilege of pfSense web console, we will need to create a root Certificate Authority which will later be used to sign the certificate for OpenVPN. Under “System”, choose “Cert. Manager”
- First, I need to create a Certificate Authority under the CA tab. Here, I use sha256 with the key length of 2048 for the CA

Create / Edit CA

Descriptive name

Method

Create an internal Certificate Authority

Internal Certificate Authority

Key length (bits)

2048

Digest Algorithm

sha256

NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days)

3650

Common Name

The following certificate authority subject components are optional and may be left blank.

Country Code

CA

State or Province

City

Organization

Organizational Unit

Save

Figure 32. Create a root CA.






Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Root_CA	✓	self-signed	0	ST=Ontario, OU=CSI, O=Fleming College, L=Peterborough, CN=internal-ca Valid From: Wed, 18 Mar 2020 21:43:00 +0000 Valid Until: Sat, 16 Mar 2030 21:43:00 +0000		   
						 Add

Figure 33. Newly created root CA.

- Now that the root CA is created, we could use it to sign the server certificate. Click on “Certificates” tab, there will also be a default certificate there. Since we will not be using it, we are just going to delete it and create a new one. Here, we choose the “Root_CA” created earlier as the Certificate authority

Add/Sign a New Certificate	
Method	Create an internal Certificate
Descriptive name	Server_Cert
Internal Certificate	
Certificate authority	Root_CA
Key length	2048
Digest Algorithm	sha256
	NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.
Lifetime (days)	3650
Common Name	ServerCert
The following certificate subject components are optional and may be left blank.	
Country Code	None
State or Province	Ontario
City	Peterborough
Organization	Fleming College
Organizational Unit	CSI

Figure 34. Sign a new server certificate (1).

Certificate Attributes							
Attribute Notes	<p>The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.</p> <p>For Internal Certificates, these attributes are added directly to the certificate as shown.</p>						
Certificate Type	Server Certificate Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.						
Alternative Names	<table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>FQDN or Hostname</td> <td></td> <td>Delete</td> </tr> </tbody> </table> <p>Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.</p>	Type	Value		FQDN or Hostname		Delete
Type	Value						
FQDN or Hostname		Delete					
Add	+ Add						
Save							

Figure 35. Sign a new server certificate (2).

Certificates		
Name	Issuer	Distinguished Name
Server_Cert Server Certificate	Root_CA	ST=Ontario, OU=CSI, O=Fleming College, L=Peterborough, CN=ServerCert
CA: No		Valid From: Wed, 18 Mar 2020 21:44:52 +0000
Server: Yes		Valid Until: Sat, 16 Mar 2030 21:44:52 +0000

Figure 36. The new server certificates.

4.4 Setup Authentication Server:

- Now that the certification has been created to encrypt the traffic, we will need an authentication method to authenticate users. There are three options provided by the pfSense OpenVPN setup which are: Local Database (pfSense users' pool), LDAP, and RADIUS. Since we already have an Active Directory setup, we are going to use it as our authenticated server.
- On the AD we create a new OU for VPN authentication called "VPN_Users", inside is 2 users: "user1" and "users2" as well as a group called "VPN". We add the 2 new users to the "VPN" group for future managing purposes.

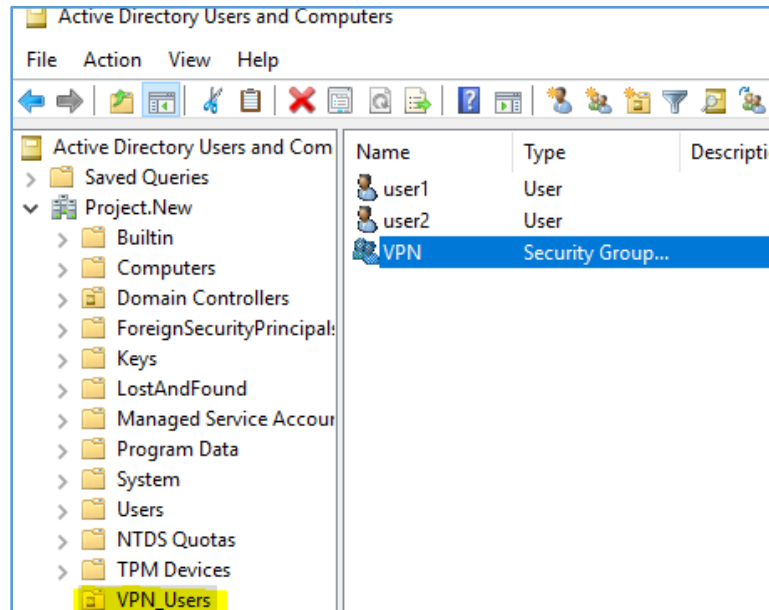


Figure 37. Setup users' pool for VPN authentication.

- In order to add the AD as an authentication server, under "System/User Manager" click on the "Authentication Servers" tab, click on "Add". Here, we need to enter the information of our AD and the specific OU that our users' pool is located.

Server Settings	
Descriptive name	<input type="text" value="ADServer"/>
Type	<input type="text" value="LDAP"/>
LDAP Server Settings	
Hostname or IP address	<input type="text" value="192.168.31.150"/> <small>NOTE: When using SSL or STARTTLS, this hostname MUST match the Common Name (CN) of the LDAP server's SSL Certificate.</small>
Port value	<input type="text" value="389"/>
Transport	<input type="text" value="TCP - Standard"/>
Peer Certificate Authority	<input type="text" value="Root_CA"/> <small>This option is used if 'SSL Encrypted' or 'TCP - STARTTLS' options are chosen. It must match with the CA in the AD otherwise problems will arise.</small>
Protocol version	<input type="text" value="3"/>
Server Timeout	<input type="text" value="25"/> <small>Timeout for LDAP operations (seconds)</small>
Search scope	<input type="text" value="Level"/> <input type="text" value="One Level"/>
	Base DN <input type="text" value="DC=Project;DC=New"/>
Authentication containers	<input type="text" value="OU=VPN_Users"/> <input type="button" value="Select a container"/> <small>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.</small>

Figure 38. Setup an Authentication server (1).

- Moreover, in order to get information about the AD our pfSense needs to bind to a user on the server. Here, we choose user1 as our bonded user.

Authentication containers	<input type="text" value="OU=VPN_Users"/> <input type="button" value="Select a container"/>
	<p>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</p>
Extended query	<input type="checkbox"/> Enable extended query
Bind anonymous	<input type="checkbox"/> Use anonymous binds to resolve distinguished names
Bind credentials	<input type="text" value="user1"/> <input type="password" value="....."/>
Initial Template	<input type="text" value="OpenLDAP"/> <input type="button" value="v"/>
User naming attribute	<input type="text" value="cn"/>
Group naming attribute	<input type="text" value="cn"/>
Group member attribute	<input type="text" value="member"/>
RFC 2307 Groups	<input type="checkbox"/> LDAP Server uses RFC 2307 style group membership RFC 2307 style group membership has members listed on the group object rather than using groups list Directory style group membership (RFC 2307bis).
Group Object Class	<input type="text" value="posixGroup"/> Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".
UTF8 Encode	<input type="checkbox"/> 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	<input type="checkbox"/> Do not strip away parts of the username after the @ symbol e.g. user@host becomes user when unchecked.
<input type="button" value="Save"/>	

Figure 39. Setup an Authentication server (2).

- After finished the configuration, the connection to the AD server could be tested on the "Settings" tab.

Users	Groups	Settings	Authentication Servers
Settings			
Session timeout	<input type="text" value="240"/>		
	Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk!		
Authentication Server	<input type="text" value="ADServer"/> <input type="button" value="v"/>		
Auth Refresh Time	<input type="text" value="30"/>		
	Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers.		
<input type="button" value="Save"/> <input type="button" value="Save & Test"/>			

Figure 40. Test AD connection (1).

LDAP settings		
Test results	Attempting connection to	192.168.31.150 OK
	Attempting bind to	192.168.31.150 OK
	Attempting to fetch Organizational Units from	192.168.31.150 OK
	Organization units found	
	OU=Domain Controllers,DC=Project,DC=New	
	OU=VPN_Users,DC=Project,DC=New	
	CN=Users,DC=Project,DC=New	

Figure 41. Test AD connection (2).

4.5 Setup OpenVPN:

- To setup, the OpenVPN goes to “VPN/OpenVPN”.
- Click on the “Wizards” tab and start configuring.
- Choose LDAP as the Authentication Backend Server Type, for the LDAP server we choose the “ADServer” that we have set up earlier, the certificate authority will be “Root_CA” and the certificate will be “Server_Cert”.
- Next, we will need to select the Interface where OpenVPN is going to receive the incoming traffic from, here it is the WAN interface. For the protocol, we use “UDP on IPv4 only” which is the popular configuration.

General OpenVPN Server Information	
Interface	<div>WAN</div> <div>The interface where OpenVPN will listen for incoming connections (typically WAN.)</div>
Protocol	<div>UDP on IPv4 only</div> <div>Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.</div>
Local Port	<div>1194</div> <div>Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.</div>
Description	<div>RemoteAccess</div> <div>A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.</div>

Figure 42. Setup OpenVPN general information.

- For the Cryptographic settings, we choose the AES-256-CBC as the Encryption Algorithm and SHA256 as the Authentication Digest Algorithm.

Cryptographic Settings	
TLS Authentication	<input checked="" type="checkbox"/> Enable authentication of TLS packets.
Generate TLS Key	<input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
TLS Shared Key	<div style="border: 1px solid #ccc; height: 60px; width: 100%;"></div> <p>Paste in a shared TLS key if one has already been generated.</p>
DH Parameters Length	<div>2048 bit</div> <p>Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.</p>
Encryption Algorithm	<div>AES-256-CBC (256 bit key, 128 bit block)</div> <p>The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.</p>
Auth Digest Algorithm	<div>SHA256 (256-bit)</div> <p>The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.</p>
Hardware Crypto	<div>No Hardware Crypto Acceleration</div> <p>The hardware cryptographic accelerator to use for this VPN connection, if any.</p>

Figure 43. Setup OpenVPN Encryption.

- For the tunnel settings, we need an IP pool which does not conflict with the current IP pool. Since the remote machine will need access to the QNAP storage, for the Local Network (Network that can be accessed from the remote endpoint), we will enter the network in which the QNAP is located.

Tunnel Settings	
Tunnel Network	<input type="text" value="192.168.24.0/24"/> <small>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.</small>
Redirect Gateway	<input type="checkbox"/> <small>Force all client generated traffic through the tunnel.</small>
Local Network	<input type="text" value="192.168.31.0/24"/> <small>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
Concurrent Connections	<input type="text"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>
Compression	<input type="text" value="Omit Preference (Use OpenVPN Default)"/> <small>Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.</small>
Type-of-Service	<input type="checkbox"/> <small>Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.</small>
Inter-Client Communication	<input type="checkbox"/> <small>Allow communication between clients connected to this server.</small>
Duplicate Connections	<input type="checkbox"/> <small>Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.</small>

Figure 44. Setup OpenVPN Tunnel.

- For the Client Settings, we will enable the “Dynamic IP” option and set the DNS Default Domain to Google DNS server on “8.8.8.8” so that the client could still access other websites.

Client Settings

Dynamic IP

☒

Allow connected clients to retain their connections if their IP address changes.

Topology

Subnet -- One IP address per client in a common subnet

Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

DNS Default Domain

8.8.8.8

Provide a default domain name to clients.

DNS Server 1

DNS server IP to provide to connecting clients.

DNS Server 2

DNS server IP to provide to connecting clients.

DNS Server 3

DNS server IP to provide to connecting clients.

DNS Server 4

DNS server IP to provide to connecting clients.

NTP Server

Network Time Protocol server to provide to connecting clients.

NTP Server 2

Network Time Protocol server to provide to connecting clients.

Figure 45. Setup OpenVPN client

- Finally, we need to allow firewall rules to be added automatically to allow client connection to the OpenVPN.

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule

☒

Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule

☒

Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

Figure 46. Allow firewall rules.

4.6 OpenVPN installation on the remote machine:

- In order to export the OpenVPN client, we need to install the OpenVPN-Client-Export packet under “System/Package Manager”.
- Now that the Client export has been installed on pfSense, we could download the OpenVPN client installer and install it on the remote machine.
- The installation package will come with the certificate ready to encrypt the traffic between the client and server using SSL/TLS handshake.
- To connect to the OpenVPN server, we will need to enter the credentials of the user inside the “VPN_Users” OU we created earlier, I use “user2” here.

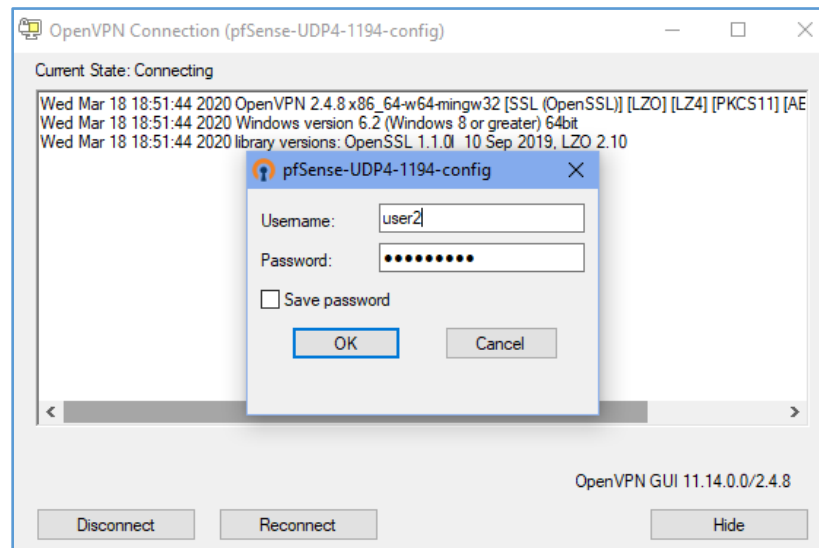


Figure 47. Authenticate against the OpenVPN server.

- Now, we can access the QNAP server remotely using a secure OpenVPN tunnel, where the traffic will be encrypted using OpenSSL.
- One of the benefits that pfSense provides us is the ability to monitor the OpenVPN connection to know what time what IPs connect and using what user credentials.
- To check the remote client IP goes to “Status/OpenVPN”.

Status / OpenVPN

RemoteAccess UDP4:1194 Client Connections

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent/Received	
user2	192.168.2.18:1194	192.168.24.3	Wed Mar 18 22:56:45 2020	4 KiB / 8 KiB	
user2					

Status: Actions:

RemoteAccess UDP4:1194 Routing Table

Common Name	Real Address	Target Network	Last Used
user2	192.168.2.18:1194	192.168.24.3	Wed Mar 18 22:56:46 2020

An IP address followed by C indicates a host currently connected through the VPN.

Figure 48. Check remote client's IP

- We can also check the OpenVPN logs under “Status/System Logs”, then choose the OpenVPN tab.

Last 50 OpenVPN Log Entries. (Maximum 50)			
Time	Process	PID	Message
Mar 18 22:55:18	openvpn	76802	192.168.2.18:1194 peer info: IV_LZ4v2=1
Mar 18 22:55:18	openvpn	76802	192.168.2.18:1194 peer info: IV_LZO=1
Mar 18 22:55:18	openvpn	76802	192.168.2.18:1194 peer info: IV_COMP_STUB=1
Mar 18 22:55:18	openvpn	76802	192.168.2.18:1194 peer info: IV_COMP_STUBv2=1
Mar 18 22:55:18	openvpn	76802	192.168.2.18:1194 peer info: IV_TCPNL=1
Mar 18 22:55:18	openvpn	76802	192.168.2.18:1194 peer info: IV_GUI_VER=OpenVPN_GUI_11
Mar 18 22:55:18	openvpn	76802	192.168.2.18:1194 [user2] Peer Connection Initiated with [AF_INET]192.168.2.18:1194
Mar 18 22:55:18	openvpn		user 'user2' could not authenticate.

Figure 49. Checking OpenVPN logs.

4.7 Enhancing security and more:

- To enhance the security of the pfSense, we need to restrict access to the pfSense web console by adding firewall rules.
- To block all OpenVPN clients from accessing the pfSense, under “Firewall/Rules” select the OpenVPN tab then add a new rule on top that will block TCP traffic that has the pfSense firewall port 80 and 443 as its destination.

Floating

WAN

LAN

OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<div><div>✗</div><div>0 / 2 KiB</div></div>	IPv4 TCP	*	*	This Firewall	80 - 443	*	none		Block OpenVPN Client	<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>0 / 1.39 MiB</div></div>	IPv4 *	*	*	*	*	*	none		OpenVPN RemoteAccess wizard	<div><div></div><div></div><div></div><div></div><div></div></div>

↑

Add

↓

Add

Delete

Save

+

Separator

Figure 50. Block web traffic trying to access the firewall console.

- This can also be done on the LAN network to only allow specific IPs to access the pfSense Firewall, and block others.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1 / 248 KiB	IPv4 TCP	192.168.31.150	*	This Firewall	80 - 443	*	none		Allow AD admin	Anchor Edit Copy Delete
<input type="checkbox"/>	✗ 0 / 107 KiB	IPv4 TCP	*	*	This Firewall	80 - 443	*	none		Block other users	Anchor Edit Copy Delete
<input type="checkbox"/>	✓ 7 / 89 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	Anchor Edit Copy Delete
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	Anchor Edit Copy Delete
↑ Add ↓ Add Delete Save + Separator											

Figure 50. Firewall rules to restrict access to pfSense web console.

5. QNAP's NAS Recommended Settings:

Network Attached Storage is a simple centralized storage device use to store and access data over local area network (LAN) via multiple user devices.

5.1 Encrypted Volumes:

You can create encrypted disk volumes to limit access over data and only certain users' s/devices are permitted.

To create volumes, take the following steps;

- Go to **"Control Panel > Storage Manager > Storage Space"**, and then click **"New Volume"** to create a new volume.
- In the next step, you will be provided with 3 options to create volume type select any one of those options. moving forward with selecting the type of disk you want along with the raid type.
- Now set the **"Snapshot Protection Setting"**. Note, this is asked if had selected either thick Multiple Volume or Thin Multiple volumes.
- Now select **'Encryption'**. In this step, you will be setting up a password for the volume.
- Now click on **"Finish"** and your volume is been encrypted. Verify this by checking your storage space in the control panel, you will see the status column with a lock symbol.

(Qnap Support, 2013)

5.2 Network Access Protection:

- This feature is considered one of the best security implementations since it blocks the communication protocols for decided time of time.
- This includes SSH, FTP, HTTPS, SAMBA, TELNET, etc.
- To enable Network access protection, go to **"Control Panel > System Settings > Security > Network Access Protection"** and Click **"Enable Network Access Protection"**

General Settings
Storage Manager
Network
Security
 Hardware
 Power
 Notification
 Firmware Update
 Backup / Restore
 External Device
 System Status
 System Logs
 Privilege Settings
 Network Services
 Applications

☒ **Enable Network Access Protection**

The network access protection enhances system security and prevents unwanted intrusion. You can block an IP period of time or forever if the IP fails to login the NAS from a particular connection method. Check the blocked IP [Level](#).

☒ **SSH:**
 In 1 minute , after unsuccessful attempts for 5 times , block the IP for 1 day .

☐ **Telnet:**
 In 1 minute , after unsuccessful attempts for 5 times , block the IP for 5 minute .

☒ **HTTP(S):**
 In 1 minute , after unsuccessful attempts for 5 times , block the IP for 30 minut .

☐ **FTP:**
 In 1 minute , after unsuccessful attempts for 5 times , block the IP for 5 minute .

☒ **SAMBA:**
 In 1 minute , after unsuccessful attempts for 5 times , block the IP for 5 minute .

☐ **AFP:**
 In 1 minute , after unsuccessful attempts for 5 times , block the IP for 5 minute .

Apply

Figure 51. QNAP Settings.

- If you only want certain IPs to connect to our storage devices, NAS also has a security feature that allows us to control the connections by either blocking a set of IPs' or allowing them to connect.
- You will find this setting under **“Control Panel > System Settings > Security > Security Level”**.

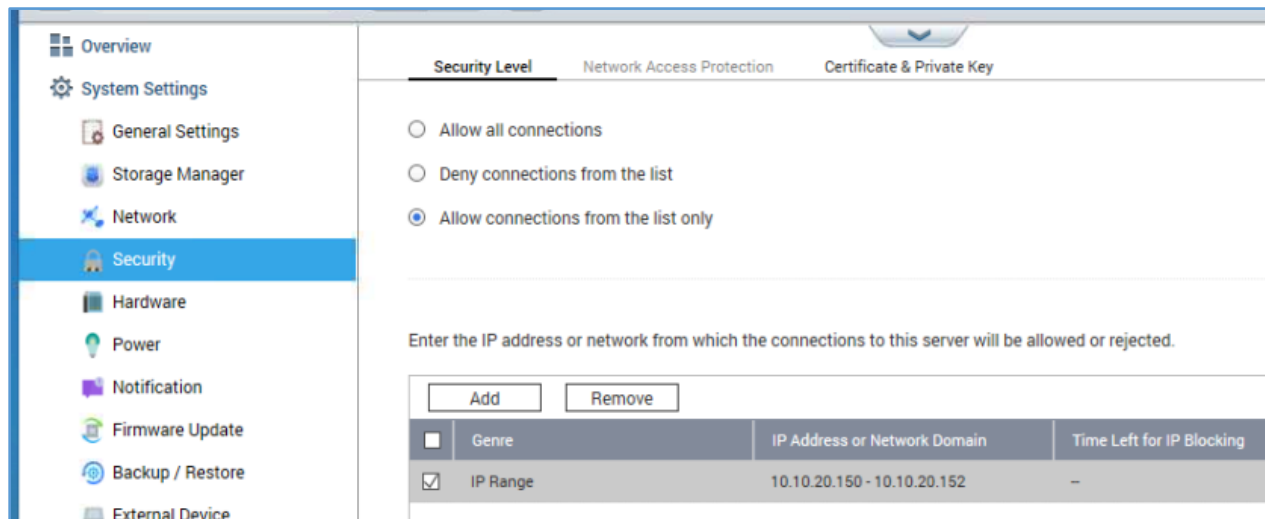


Figure 52. Whitelisting.

- We recommend whitelisting the IP's of the workstations you want to be able to access the QNAP NAS.
- The collecting system log is another feature you can add to the configurations. This security feature allows us to monitor system connections, for instance, one can view all the access attempts made by devices to retrieve data.
- This also gives the option to monitor all the communication protocols or only certain of them and save the file in a folder.
- To start System Connection Logging go to **“Control Panel > System Settings > System Connection Logs > Start Logging”**. You can view the connections logs under System event logs.

System Event Logs System Connection Logs Online Users Syslog Client Management						
All events ▼		Clear All	Save	Content Search		
Type	Date	Time	Users	Source IP	Computer name	Content
ⓘ	2020/03/11	16:16:02	p1	10.10.20.152	—	[Telnet / SSH] SSH service disabled.
ⓘ	2020/03/11	15:47:03	p1	10.10.20.152	—	[Security] System security level changed from [AllowSome] to [AllowAllWithSec].
ⓘ	2020/03/11	15:38:01	p1	10.10.20.150	—	[Security] System security level changed from [AllowAllWithSec] to [AllowSome].
ⓘ	2020/03/11	15:20:15	p1	10.10.20.150	—	[Share Folders] New share folder [CSIAP1] created.
ⓘ	2020/03/10	15:48:10	p1	172.16.0.206	—	[Users] User [p1]'s shared folder access rights changed.
ⓘ	2020/03/10	15:40:16	admin	172.16.0.206	—	[Users] User [p1]'s account information was changed.
ⓘ	2020/03/10	15:39:36	admin	172.16.0.206	—	[Users] New user [p1] added.
ⓘ	2020/03/10	15:38:21	admin	172.16.0.206	—	[Users] New user [dhannah] deleted.
⚠	2019/11/01	07:12:15	System	127.0.0.1	localhost	Failed to synchronize the time with NTP server.
⚠	2019/11/01	06:26:14	System	127.0.0.1	localhost	[Strip Disk Volume: Drive 1 2 3 4] The file system is not clean. It is suggested that you go to [Storage Manager] to run "Check File System".
<div> <div>⏪ ⏩</div> <div>Page 1 /16</div> <div>⏴ ⏵</div> <div>⌂</div> </div> <div>Display item: 1-50, Total: 782 Show 50 Item(s)</div>						

Figure 53. Monitoring logs.

- If you want to transfer files and data through the public network, it is strictly recommended to secure connection with SSL. SSL creates a secure tunnel and encrypted files are transferred.
- To enable SSL, go to **“Control Panel > System Settings > General Settings > System Administration”** and Click **“Enable secure connection”**.

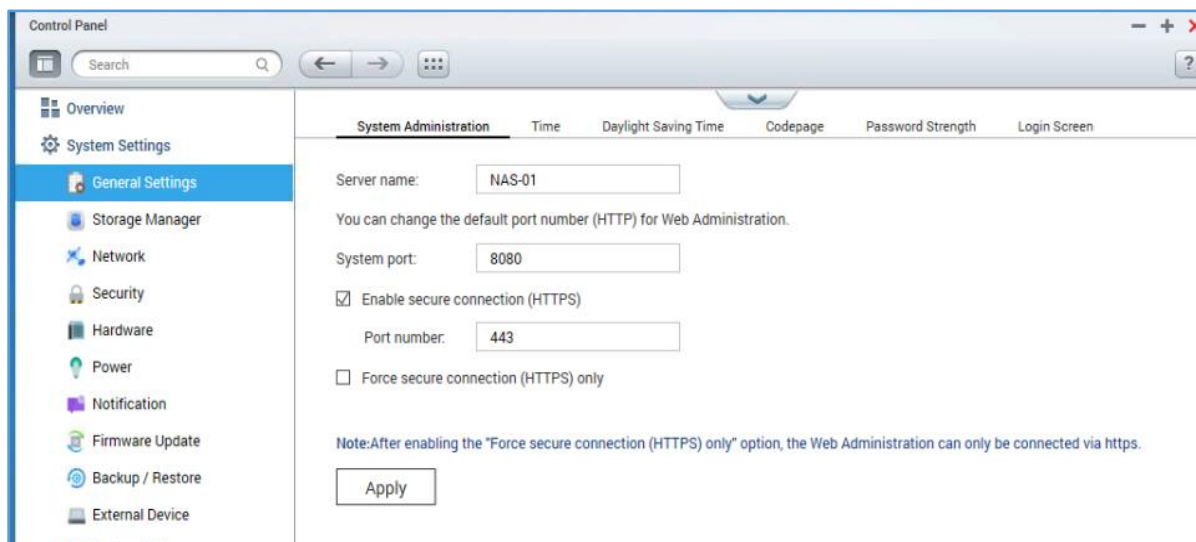


Figure 54. Enabling SSL.

- Sometimes on our assets, we have unnecessary services ON which leads to vulnerability and possible threat. By disabling these services, we reduce the likelihood of being attacked.
- Therefore, it is recommended that you disable SSH, TELNET and FTP service when not in use. These services can be disabled/enable in the **“Control Panel > System Settings > System Status > System Service”**. (QNAP , 2014)
















System Information	Network Status	System Service	Hardware Information	Resource Monitor
Antivirus			File Station	
Enabled			Enabled 	
Apple Networking			Surveillance Station	
Enabled			Enabled 	
DDNS Service			Qsync	
Enabled			Enabled 	
DLNA Media Server			RADIUS Server	
Enabled			Enabled 	
Disk Management			RTRR Server	
Enable iSCSI target service			Enabled 	
Port		3260	Rsync Server	
Download Station			Enabled 	
Enabled			SNMP	
FTP Service			Enabled 	
Enabled			Port	
Port		21	Service Binding	
Maximum connections		30	Enabled 	

Figure 55. Running Services.

6. Setting up encrypted volumes using VeraCrypt for better key management:

- Download the VeraCrypt installation package from the VeraCrypt project website.
- Once VeraCrypt is installed, launch it and click on “Create Volume” from the main window.
- Next, you choose whether to create an encrypted container or, encrypt the entire disk. Choose an encrypted container for the demonstration.
- After that, it will prompt whether you create a standard volume or a hidden volume. The hidden volume allows you to have a sort of “decoy” volume so that if you are required to enter your password under duress, only the contents of the outer volume will be revealed. The idea is to have all your confidential files in the inner Hidden container. For this demonstration, choose Standard VeraCrypt Volume.
- Now it will prompt for the location to save the container. The container is a regular file with whatever extension you would like. Ideally would name it something unassuming like dog.jpg, and then hide it in plain sight. Choose the location and in the box name it “container.hc” for the demonstration.
- Next, it will prompt for an encryption algorithm to use for encrypting the contents of the container. The default AES algorithm is enough, and the default Hash algorithm SHA-512 is as well.
- On the next screen, it will prompt for the size of the container. Make sure it is large enough to fit all the files you want to put in there. Choose between Kilobytes, Megabytes, Gigabytes, and Terabytes, then type in the value for the size you want. For demonstration purposes, select Megabytes and type 500 in the box for a 500MB container.
- When that is done, it will prompt you for a password to use in order to mount the volume. Following the onscreen password, the complexity guide is a good practice. Make sure it is a password you will remember, otherwise you will not be able to mount the volume anymore.
- Following that, choose the filesystem for the container (NTFS or FAT) If your disk is already NTFS it’s a good idea to make the container NTFS. Leave cluster size as default. After that is set up, you need to move your mouse within the window as random as possible to use as a seed for encryption of the volume.
- When that is done, test the volume. To do that, return to the main screen and click “select file”. Locate where the volume file was saved, then select a drive letter in the main screen and click “mount”. It will prompt for a password. Enter the one you used when you created the volume. Once it is mounted, you can copy files into the mounted virtual disk, then when you are done unmount it. Make sure to unmount it when finished, otherwise, it will not encrypt the data.

7. General Endpoint Security Recommendations:

7.1 Definition:

- Endpoints are devices connected to the network. It includes devices like Servers, laptops, desktop computers, tablets, printers or other specialized hardware such as Storage Devices and POS terminals. This can be either on-site or remote-connections gadgets.
- So, when we talk about implementing Network Security these endpoints should comply with certain criteria before they access the network.

7.2 Endpoint Security Management:

Authorize and monitor the access rights of endpoint devices and applying security policies that prevent any external or internal threats posed by those access rights.

The typical requirements of management are:

- Only allowing authorized endpoint devices and its users to access companies' assets, either on-premises or over a broader network (e.g., Wide area network (WAN) or the internet using VPN services).
- Monitoring endpoints using third party software like Zabbix, etc. Such tools provide a lot of analytical information about the endpoint's user activities and discrepancies in normal behavior. For which, you can also set "Alerts" for each type of event.
- Allowing the different administrative tiers to manage these devices and processes from one central console or application. (Mcafee, n.d.)

7.3 Recommendation:

The preliminary requirement of endpoint security doesn't involve much of technical configurations but simple user authentication. Certain policies suggest Two-factor authentication. This reduces frauds like credential theft, etc.

The organization contains a different type of work-levels. Each work level has access/restrictions to certain resources. The common practice is to restrict user control over these resources. Securing the user is also part of securing endpoint devices.

The basic recommendation is to never turn off the default firewall settings on these devices.

For instance, windows provide firewall security features. They can be used as follows.

- On desktop computers make sure these windows firewall settings are ON. You will find these under **“Start Menu < Control Panel < System and Security < Windows Defender Setting”**
- Windows also have advanced firewall settings. Using these options, we can block any incoming and outgoing connection rules. They simply allow/block your ports. You will find these under **“Start Menu < Control Panel < System and Security < Windows Defender Setting < Advance Setting”**.

You can also install 3rd party software such as Anti-virus, Antispyware, Host intrusion prevention, and intrusion detection system. These systems help to detect threats that are been neglected/unseen by default firewalls. These tools also help to maintain log records for future advancement in management policies.

The organization should not have a “Bring Your Own Device” (BYOD) policy. Because an outside device connected to the network servers is a simple invitation for threat and exposure for assets.

Most importantly UPDATE the devices when needed.

Works Cited:

- Barnes, A. (2016). *Missing MSS Settings in Security Options of Group Policy (GPO)*. Retrieved from [www.vmadmin.co.uk: https://www.vmadmin.co.uk/microsoft/43-winserver2008/348-server2012mssgposettings](https://www.vmadmin.co.uk/microsoft/43-winserver2008/348-server2012mssgposettings)
- Centre for Internet Security. (2020, 01 14). *CIS Benchmarks*. Retrieved from [www.cisecurity.org: https://www.cisecurity.org/cis-benchmarks/](https://www.cisecurity.org/cis-benchmarks/)
- Eguibar Information Technology. (n.d.). *AD Delegation Model*. Retrieved from [DelegationModel.com: http://www.delegationmodel.com/](http://www.delegationmodel.com/)
- Hoffman, C. (2017, JULY 12). *Why You Shouldn't Enable "FIPS-compliant" Encryption on Windows*. Retrieved from [howtogeek.com: https://www.howtogeek.com/245859/why-you-shouldnt-enable-fips-compliant-encryption-on-windows/](https://www.howtogeek.com/245859/why-you-shouldnt-enable-fips-compliant-encryption-on-windows/)
- Mcafee. (n.d.). *What Is Endpoint Security Management?* Retrieved from [Endpoint Security Managemen: https://www.mcafee.com/enterprise/en-ca/security-awareness/endpoint/what-is-endpoint-security-management.html](https://www.mcafee.com/enterprise/en-ca/security-awareness/endpoint/what-is-endpoint-security-management.html)
- Michael. (2018, 04 20). *How to: Active Directory Delegated Permissions Best Practices*. Retrieved from [spiceworks.com: https://community.spiceworks.com/how_to/146669-active-directory-delegated-permissions-best-practices](https://community.spiceworks.com/how_to/146669-active-directory-delegated-permissions-best-practices)
- Posey, B. (2018, 03 20). *Security templates for Windows: Configure your PCs and lock down your OS*. Retrieved from [http://techgenix.com: http://techgenix.com/security-templates/](http://techgenix.com)
- QNAP. (2014, 10 23). *QNAP: How to make your Turbo NAS more secure?* Retrieved from <https://www.qnap.com/en/how-to/faq/article/how-to-make-your-turbo-nas-more-secure/>
- Qnap Support. (2013, 05 17). *QNap*. Retrieved from <https://www.qnap.com/en/how-to/tutorial/article/how-do-i-encrypt-the-data-on-a-qnap-nas/>
- Security, C. C. (2019, 05 01). *Guidance for Hardening Microsoft Windows 10 Enterprise (ITSP.70.012)*. Retrieved from [Canadian Centre for Cyber Security: https://cyber.gc.ca/en/guidance/guidance-hardening-microsoft-windows-10-enterprise-itsp70012](https://cyber.gc.ca/en/guidance/guidance-hardening-microsoft-windows-10-enterprise-itsp70012)