

Network Changes SOP (pfSense):

Purpose:

Process to make hardware or software changes and how to implement pfSense to configure organizations network topology.

Scope:

This SOP covers the steps for any changes to hardware or software in the organization's network infrastructure

Pfsense will be used to create subnets, DHCP ranges, and to assign roles and IP addresses for all important devices within the organization's network infrastructure.

Responsibilities:

Information Technology (IT) department has sole responsibility for configuring the organization's network and overseeing hardware & software changes.

IT Department is required to create and update subnets, DHCP ranges, and IP addresses for important shared resources.

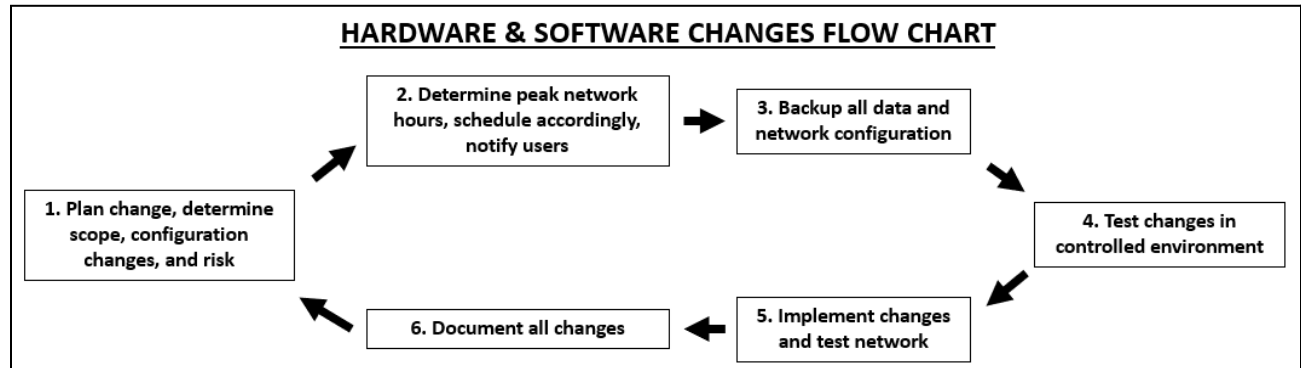
Prerequisites:

[pfSense](#) - world's most trusted open source network security solution.

pfSense GUI should be run as an administrator for full functionality.

Procedures:

Hardware & Software Changes:



1. Plan change, determine scope, configuration changes, and risk

- Plan change well in advance
- Determine how many devices in the networks infrastructure the change will affect (scope)
- Identify any risks associated, and have a contingency plan and mitigation strategy in place in the event something goes wrong

2. Determine peak network hours, schedule accordingly, notify users

- Schedule changes during times with low network traffic
- Notify all users of changes and how they may affect access

3. Backup all data and network configuration

- Ensure all data and the network configuration are backed up locally and to an offline device.

4. Test changes in controlled environment

- Recreate the organization's network environment to the best of your ability
- Test new hardware within the confines of this environment prior to deployment

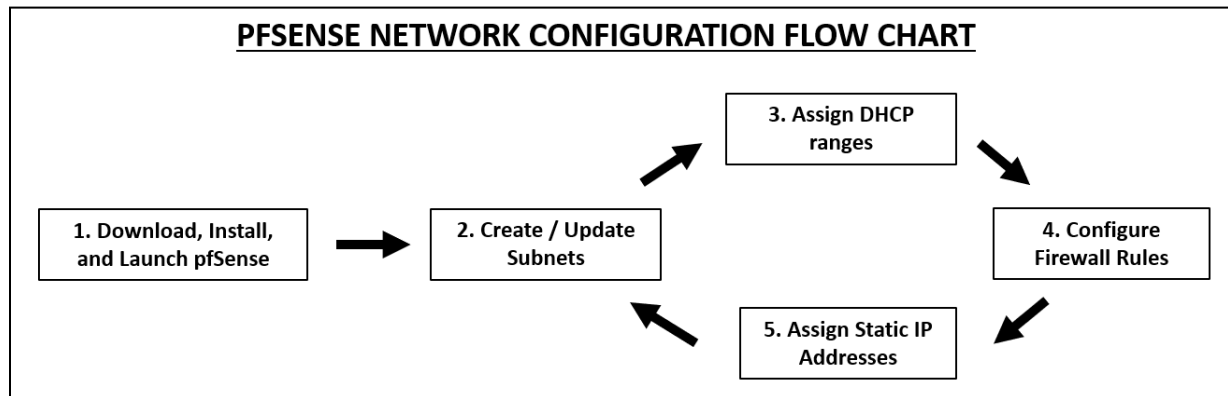
5. Implement changes and test network

- Implement changes and compare previous network baseline to current condition to identify any changes resulting from change

6. Document all changes

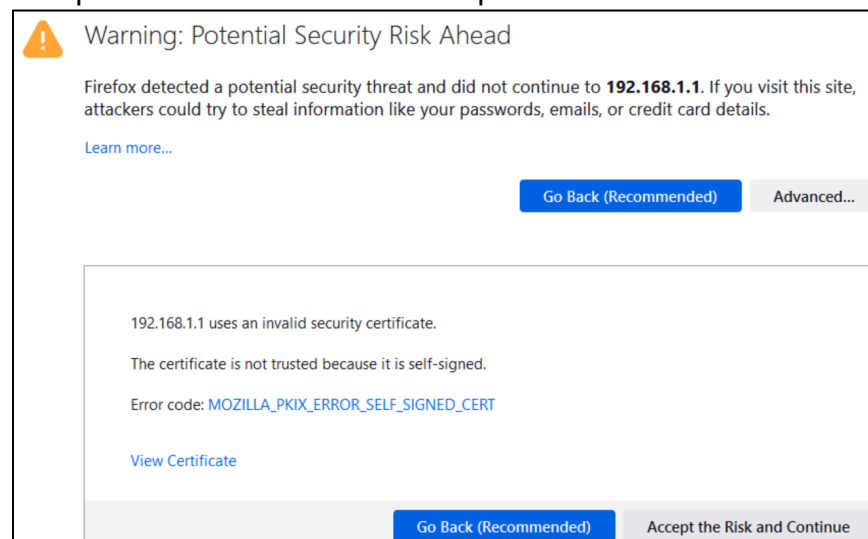
- Develop detailed documentation regarding changes
- Ensure proper secure storage of all network configuration and network device information

Configuration Changes:



1. Download, Install, and Launch pfSense GUI

- Download pfSense from official website ([pfSense](https://www.pfsense.org/))
 - Ensure you select the correct install file for your Operating System (OS)
 - Select all defaults during installation wizard
- To launch pfSense GUI ensure your computer is connected to the LAN interface of the connected device
 - Open a web browser and navigate to the default pfSense IP address (192.168.1.1).
 - You will likely be provided with a warning similar to the one below, accept the risk to continue to the pfSense GUI



- Login to the pfSense GUI with the default username and password
 - User: admin
 - Password: pfsense

2. Create / Update Subnets (Repeat steps 2 & 3 to create additional subnets)

- Navigate to Interfaces > LAN > Configure interface IP and subnet mask
 - **IPv4 Configuration Type:** Static IPv4

IPv4 Configuration Type	Static IPv4
--------------------------------	-------------

- **IPv4 Address:** Enter first IP of subnet you want to create / update and the appropriate subnet mask

Static IPv4 Configuration	
IPv4 Address	192.168.x.x / 24

3. Assign DHCP ranges

- Navigate to Services > DHCP Server > Select the subnet you created
 - Check the “Enable DHCP server on LAN interface”
 - **Range:** Enter the range of IP addresses for the subnet DHCP pool

Range	192.168.x.x	192.168.x.x
	From	To

4. Configure Firewall Rules

- Navigate to Firewall > Rules > Select tab for created subnet > Add
 - Create rule to allow traffic between subnets

■ Action: Pass

Action	Pass
---------------	------

■ Interface: Subnet_1 name

Interface	LAN
Choose the interface from which packets must come to match this rule.	

■ Address Family: IPv4

Address Family	IPv4
Select the Internet Protocol version this rule applies to.	

■ Protocol: Any

Protocol	Any
Choose which IP protocol this rule should match.	

■ Source: Subnet_2 name

Source	<input type="checkbox"/> Invert match	LAN address
---------------	---------------------------------------	-------------




■ Destination: Any

Destination	<input type="checkbox"/> Invert match	any
--------------------	---------------------------------------	-----

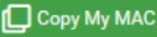
- Save and select Apply Changes

5. Assign Static IP Addresses

- Navigate to Services > DHCP Server > Select the tab of the interface where the device you would like to statically map resides
 - At bottom of page under “DCHP” Static Mappings for this Interface”
 - Select Add

DHCP Static Mappings for this Interface (total: 1)				
Static ARP	MAC address	IP address	Hostname	Description
✓	08:00:27:4e:54:87	192.168.1.250	Win19_Server	 
 Add				

- Configure the following:
 - **MAC Address:** MAC of device

MAC Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/>	
MAC address (6 hex octets separated by colons)		

- **IP Address:** IP of device

IP Address	<input type="text"/>
If an IPv4 address is entered, the address must be outside of the pool. If no IPv4 address is given, one will be dynamically allocated from the pool.	
The same IP address may be assigned to multiple mappings.	

- **Description:** Description of device (ex. office_printer)

Description	<input type="text"/>
A description may be entered here for administrative reference (not parsed).	

- Save and Apply Changes

References:

- [So, You Want to Write an SOP?](#)
- [37 Best Standard Operating Procedure \(SOP\) Templates](#)
- [Standard Operating Procedures](#)
- [Protect home network using subnets with pfSense](#)
- [ChatGPT](#)
- [What is a subnet? | How subnetting works](#)
- [Dynamic Host Configuration Protocol \(DHCP\)](#)
- [What is a Firewall?](#)
- [Static IP address](#)

Definitions:

- **Subnet** - smaller network inside a large network
- **DHCP** - client/server protocol, automatically provides IP)host with its IP and other related configuration information such as subnet mask and default gateway
- **Firewall** - network security device, monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies
- **Static IP** - unique identifier for a device that connects to the internet

Revision History:

4/4/2023 -- "Network Configuration SOP" created by Rob Gregor

4/5/2023 – "Network Changes SOP" updated by Rob Gregor