Configuring a Network with SIEM Detection and Monitoring

Description

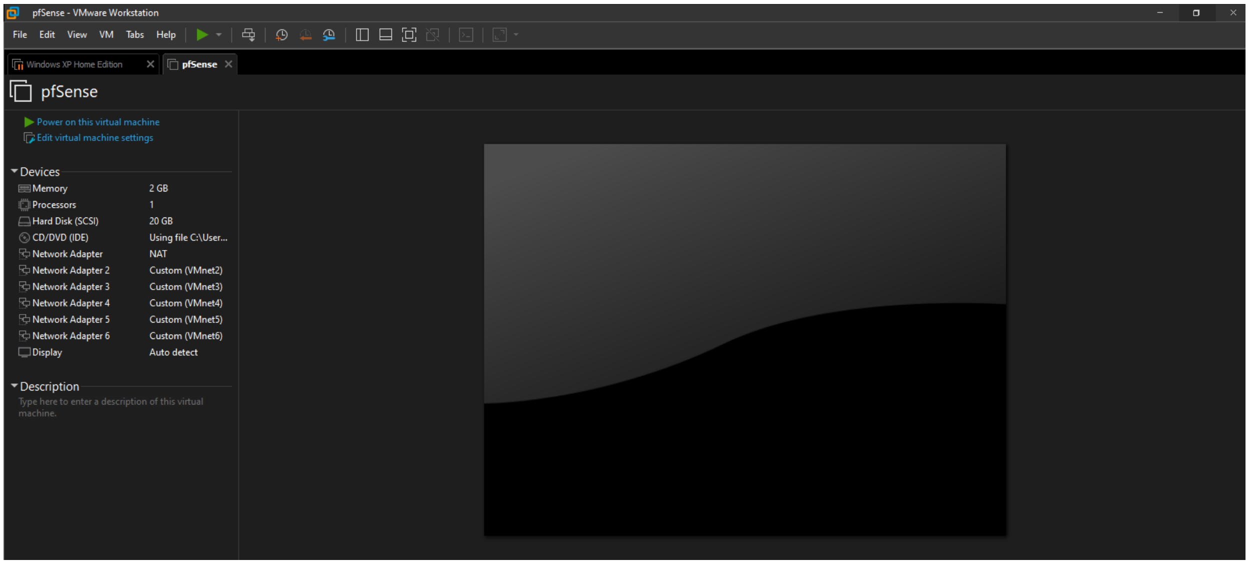
The main purpose of this lab is to gain hands-on experience with network configuration along with detecting and monitoring attacks within a controlled, virtual network by monitoring alerts and reading logs through a SIEM. The lab involves configuring a small network consisting of a victim network with one user and a Domain Controller, two SIEM tools connected separately to the victim network for security monitoring and log management of said network, a Kali Linux machine as the attacker machine, and a network firewall that will connect to all of the other virtual networks and acts as a default gateway, which will filter and segment the network.

Programs and Environments Used

- Hypervisor: VMWare Workstation 16 Pro
- Firewall: pfSense
- SIEM Tools: Security Onion, Splunk
- Servers: Windows Server 2016 (Domain Controller), Ubuntu Server
- Desktops: Windows 10 Enterprise, Ubuntu Desktop

pfSense Configuration

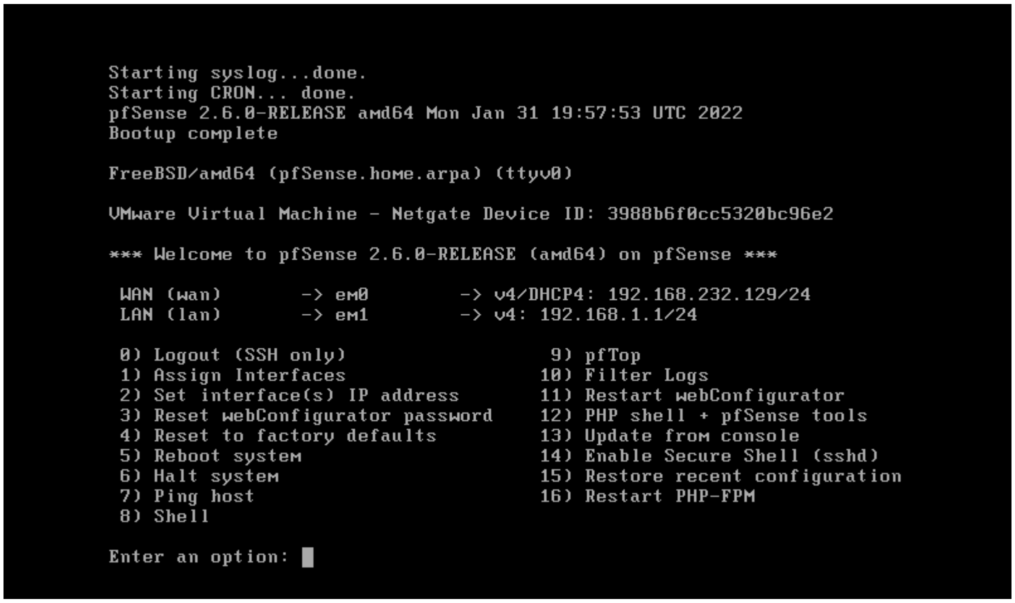
pfSense will be configured as a network firewall in order to segment the network, which can only be accessed from our Kali Linux machine for additional configuration.



pfSense - VMware Workstation
File
Edit
View
VM
Tabs
Help
Windows XP Home Edition
pfSense
pfSense
Power on this virtual machine
Edit virtual machine settings
Devices
Description
Type here to enter a description of this virtual machine.

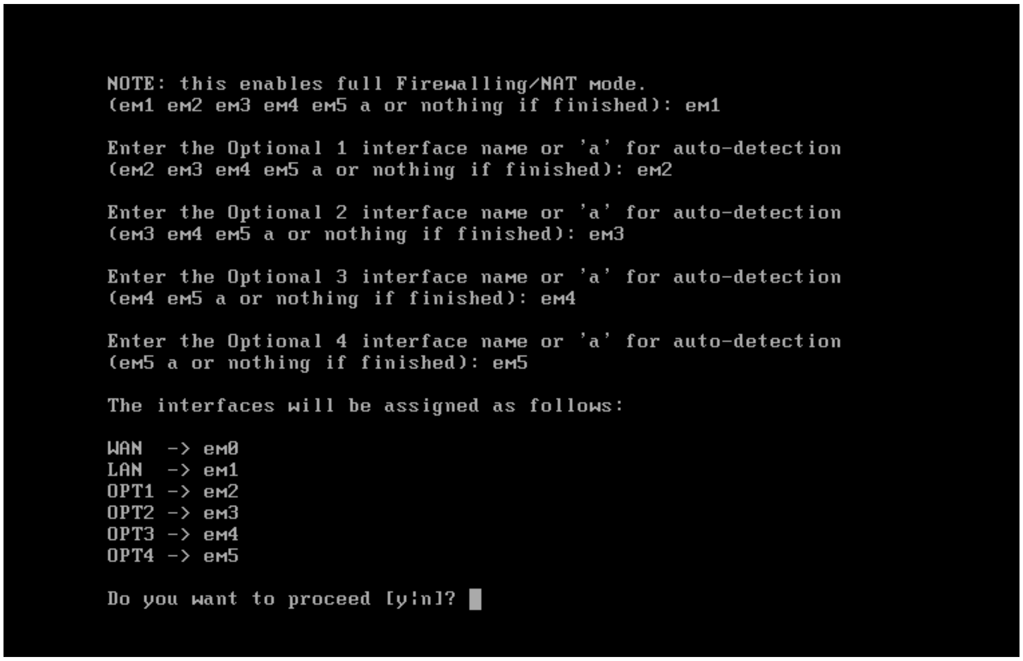
Memory	2 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file C:\User...
Network Adapter	NAT
Network Adapter 2	Custom (VMnet2)
Network Adapter 3	Custom (VMnet3)
Network Adapter 4	Custom (VMnet4)
Network Adapter 5	Custom (VMnet5)
Network Adapter 6	Custom (VMnet6)
Display	Auto detect

For this network, pfSense will require 6 network adapters in total to support the other machines/virtual networks created in the later portion of the lab as seen above.



```
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 3988b6f0cc5320bc96e2

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.232.129/24
 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       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

After accepting all of the default settings for the pfSense installation, pfSense will load this screen above. The LAN address will be the IP address for pfSense once we configure it. From here, we will assign the pfSense interfaces to the corresponding network interfaces for the other virtual networks as seen below:



```
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 em4 em5 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 em4 em5 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 em4 em5 a or nothing if finished): em3

Enter the Optional 3 interface name or 'a' for auto-detection
(em4 em5 a or nothing if finished): em4

Enter the Optional 4 interface name or 'a' for auto-detection
(em5 a or nothing if finished): em5

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2
OPT2 -> em3
OPT3 -> em4
OPT4 -> em5

Do you want to proceed [y|n]?
```

The listed pfSense interfaces will correspond with the following virtual network:

WAN → WAN

LAN → Kali

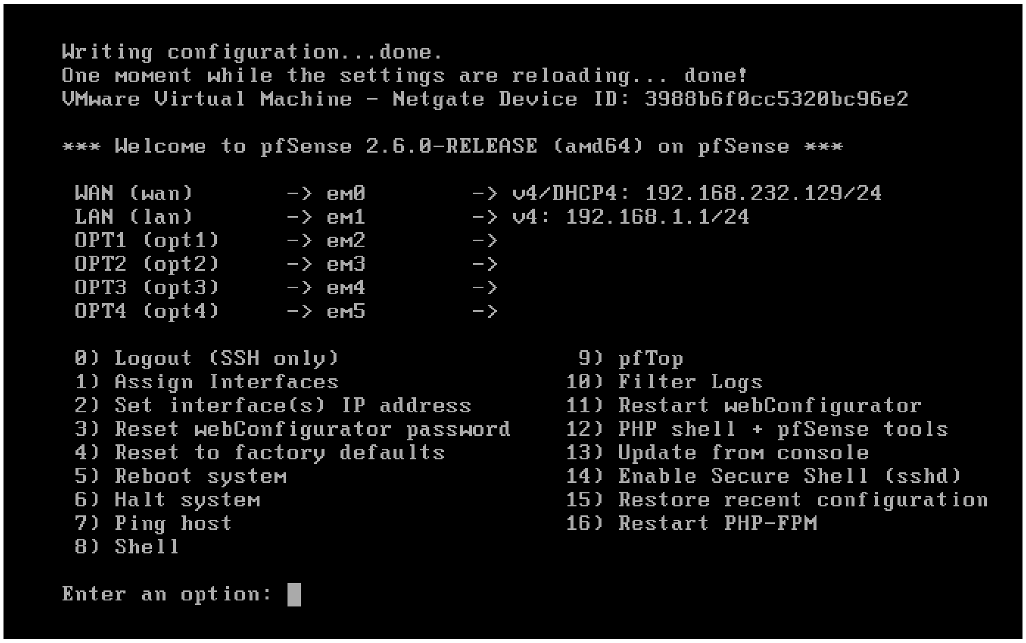
OPT1 → Victim Network

OPT2 → Security Onion

OPT3 → Span Port

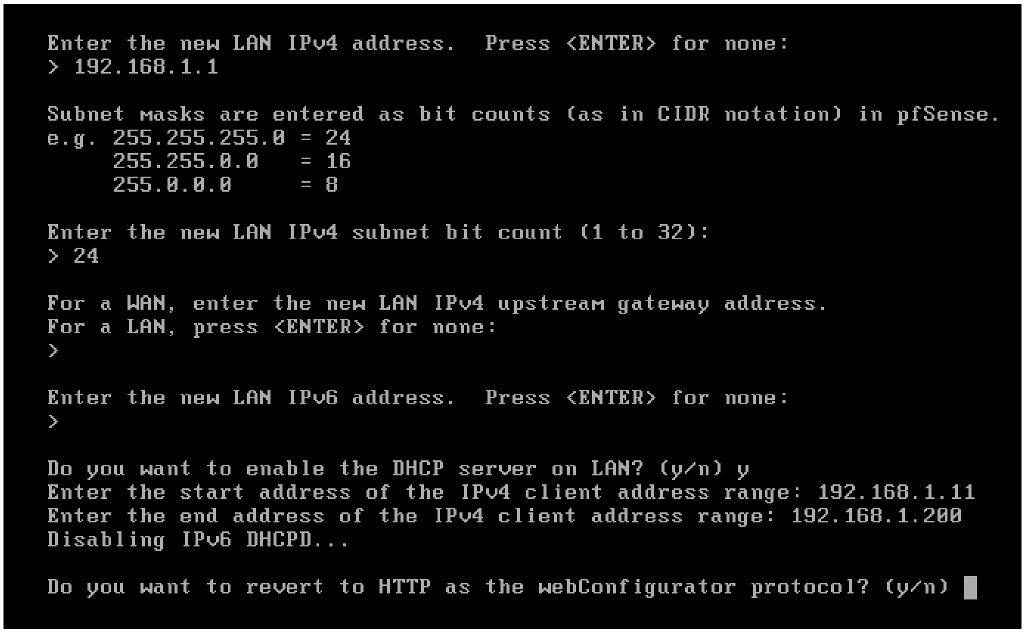
OPT4 → Splunk

After assigned the pfSense interfaces to the corresponding virtual networks, pfSense will load this screen below, which shows we need to assign IP addresses to the remaining interfaces:



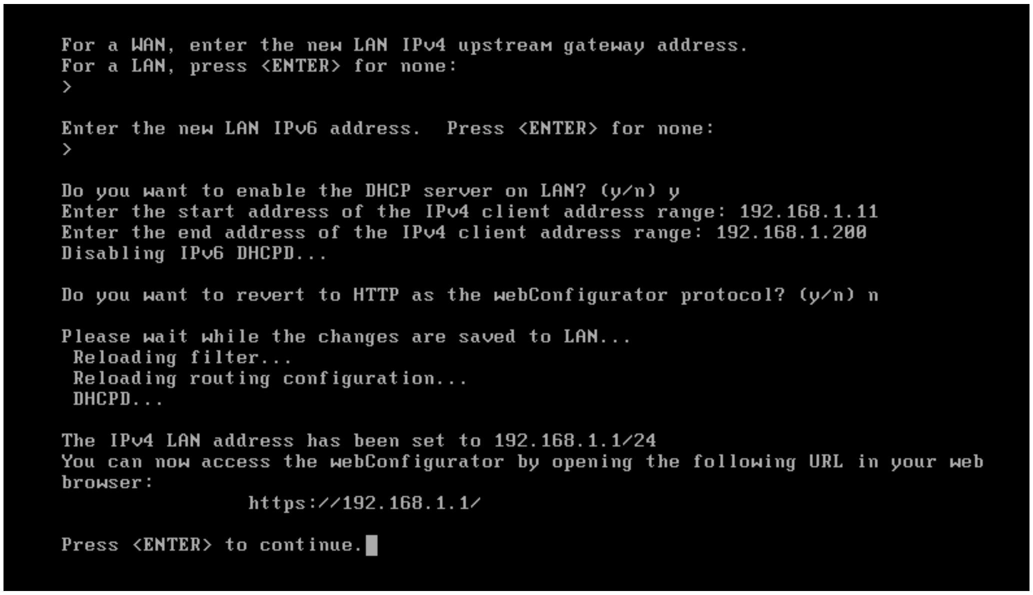
```
Writing configuration...done.
One moment while the settings are reloading... done!
VMware Virtual Machine - Netgate Device ID: 3988b6f0cc5320bc96e2

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.232.129/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
 OPT1 (opt1)     -> em2        ->
 OPT2 (opt2)     -> em3        ->
 OPT3 (opt3)     -> em4        ->
 OPT4 (opt4)     -> em5        ->

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

Enter an option:
```

To do so, we will enable DHCP server on the LAN network, and set a range of IP addresses for assignment to the other interfaces as shown below:



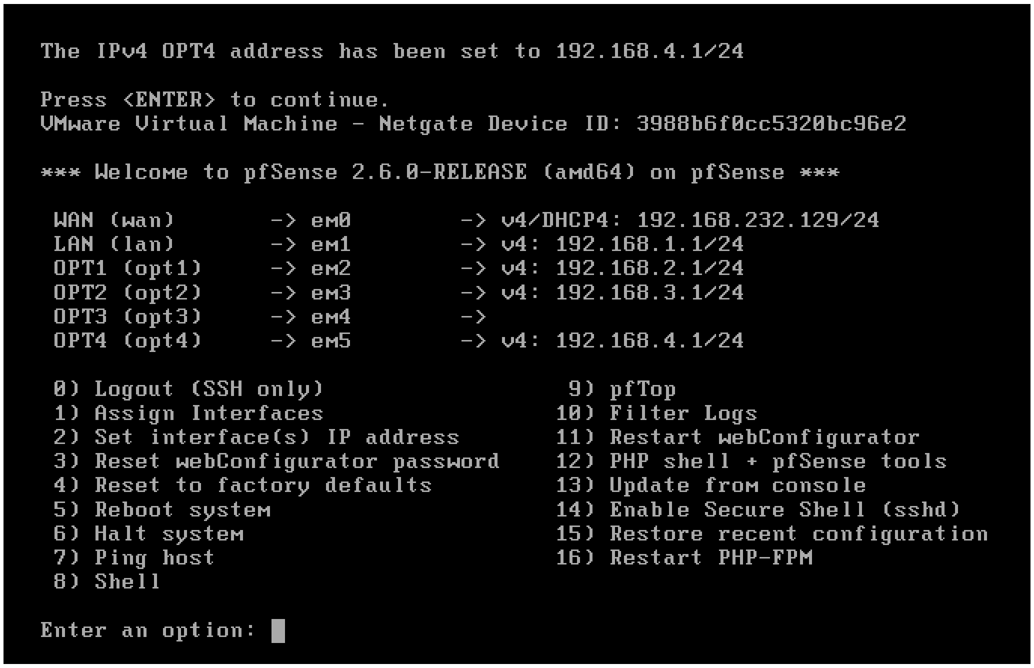
```
Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.1

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 32):
> 24

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:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.11
Enter the end address of the IPv4 client address range: 192.168.1.200
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n)
```

After finish configuring the DHCP server to the LAN network, pfSense can now be accessed to its assigned IP address 192.168.1.1 through a web browser, which we will see in the later part of the lab via Kali Linux. The finished setup can be seen below:



```
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:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.11
Enter the end address of the IPv4 client address range: 192.168.1.200
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

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

The IPv4 LAN address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.1.1/

Press <ENTER> to continue.
```

After configuring a DHCP pool of available IP addresses used for assignment, we will continue assigning IP addresses to the remaining interfaces on pfSense. OPT3 (Span Port) will be left unassigned as it is going to have Span Port with traffic that is monitored from the victim network by Security Onion. Therefore, the final pfSense configuration can be seen below:

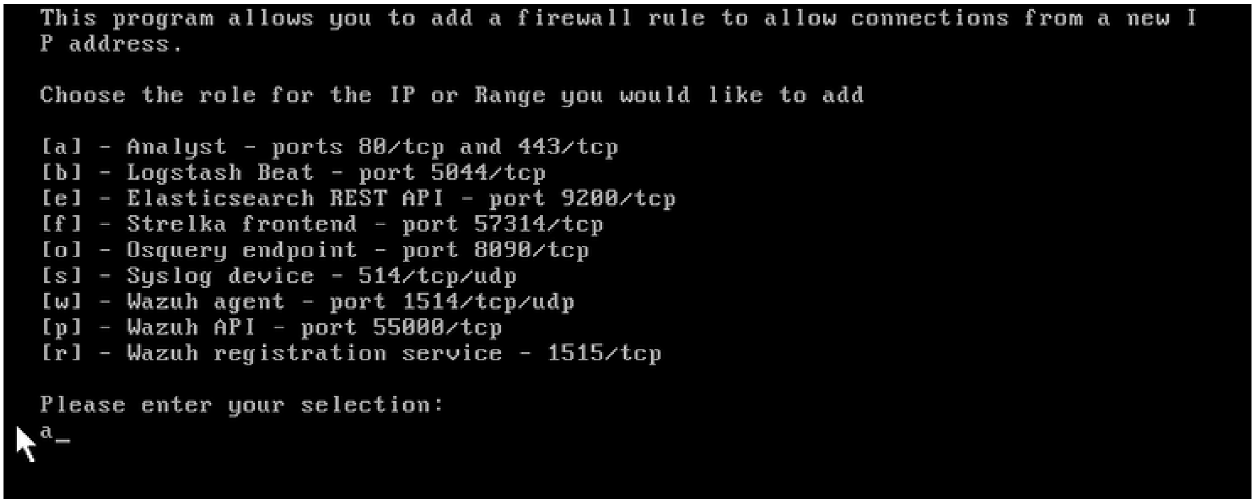


```
The IPv4 OPT4 address has been set to 192.168.4.1/24

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 3988b6f0cc5320bc96e2

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.232.129/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
 OPT1 (opt1)     -> em2        -> v4: 192.168.2.1/24
 OPT2 (opt2)     -> em3        -> v4: 192.168.3.1/24
 OPT3 (opt3)     -> em4        ->
 OPT4 (opt4)     -> em5        -> v4: 192.168.4.1/24

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

Enter an option:
```

Security Onion Configuration

For this section, I was not able to complete it after waiting for Security Onion to finish its installation due to how much memory it requires, and my host machine is not capable of allocating a high amount of RAM for both Security Onion and an Ubuntu desktop virtual machine running at the same time (Ubuntu desktop is used to access the SIEM web interface of Security Onion once its installation is complete). Instead, I had a friend who also worked on this lab with me and provided some screenshots of the Security Onion configuration.

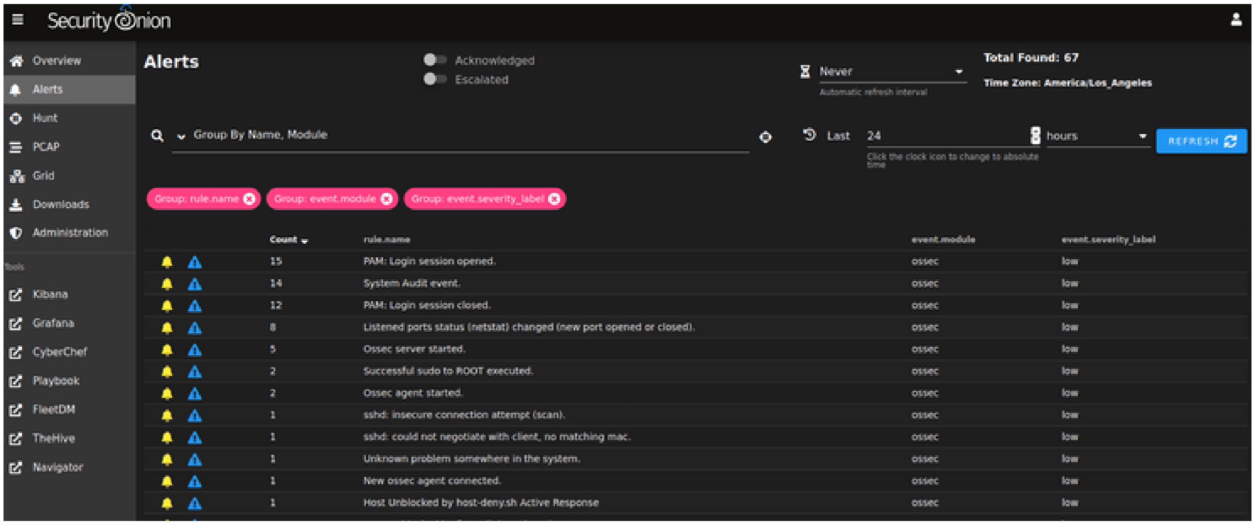
Once the installation of Security Onion is fully complete, run the “sudo so-allow” command and select option [a] once this menu shows up as seen below:



```
This program allows you to add a firewall rule to allow connections from a new I
P address.

Choose the role for the IP or Range you would like to add

[a] - Analyst - ports 80/tcp and 443/tcp
[b] - Logstash Beat - port 5044/tcp
[e] - Elasticsearch REST API - port 9200/tcp
[f] - Strelka frontend - port 57314/tcp
[o] - Osquery endpoint - port 8090/tcp
[s] - Syslog device - 514/tcp/udp
[w] - Wazuh agent - port 1514/tcp/udp
[p] - Wazuh API - port 55000/tcp
[r] - Wazuh registration service - 1515/tcp

Please enter your selection:
a_
```

From here, type in the IP address associated with the Ubuntu Desktop. This will create a firewall rule on Security Onion that will allow the Ubuntu Desktop access to the SIEM web interface straight from the desktop.

Afterwards, navigate to the Security Onion's IP address on the Ubuntu Desktop's web browser, and you will have access to the SIEM web interface of Security Onion as seen below:



Alerts

○ Acknowledged
○ Escalated

Never
Automatic refresh interval

Total Found: 67
Time Zone: America/Los_Angeles

Group By Name, Module

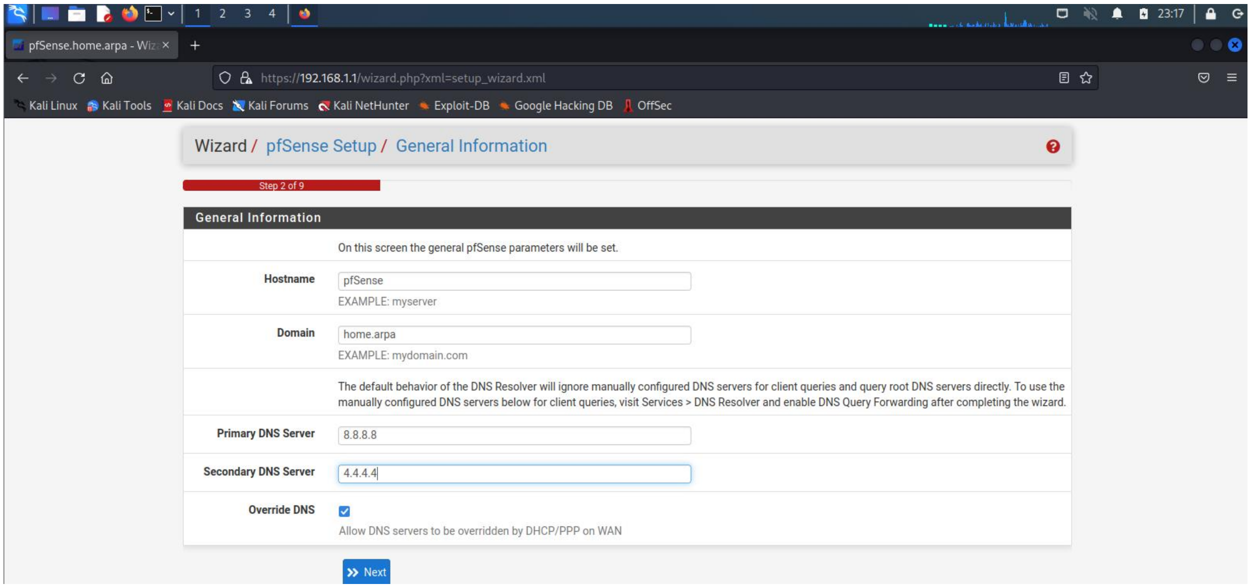
Last 24 hours
Click the clock icon to change to absolute time

Group: rule.name ⊗ Group: event.module ⊗ Group: event.severity_label ⊗

Count	rule.name	event.module	event.severity_label
15	PAM: Login session opened.	ossec	low
14	System Audit event.	ossec	low
12	PAM: Login session closed.	ossec	low
8	Listened ports status (netstat) changed (new port opened or closed).	ossec	low
5	Ossec server started.	ossec	low
2	Successful sudo to ROOT executed.	ossec	low
2	Ossec agent started.	ossec	low
1	sshd: insecure connection attempt (scan).	ossec	low
1	sshd: could not negotiate with client, no matching mac.	ossec	low
1	Unknown problem somewhere in the system.	ossec	low
1	New ossec agent connected.	ossec	low
1	Host Unblocked by host-deny.sh Active Response	ossec	low

Configuring pfSense Interfaces and Rules Through Kali Linux

With pfSense configured earlier, one can access the pfSense WebConfigurator through a web browser in order to make changes to pfSense interface and firewall rules. To do so, we will search for pfSense's IP address (192.168.1.1) in Firefox. After login into pfSense, we will receive this webpage for initial setup as seen below:



https://192.168.1.1/wizard.php?xml=setup_wizard.xml

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSense
EXAMPLE: myserver

Domain: home.arpa
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

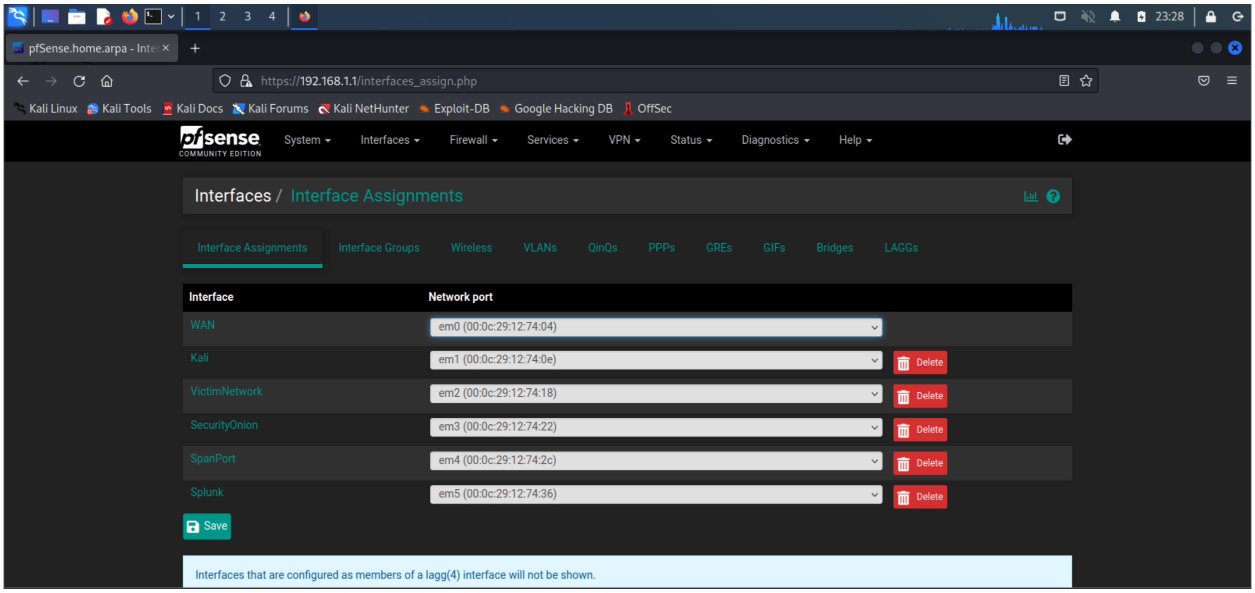
Primary DNS Server: 8.8.8.8

Secondary DNS Server: 4.4.4.4

Override DNS: ☑
Allow DNS servers to be overridden by DHCP/PPP on WAN

From here, we will assign pfSense's primary and secondary DNS servers as shown above. 8.8.8.8 and 4.4.4.4 are Google's DNS servers.

Afterwards, once we finish the initial setup, we will go to interfaces assignments to view all of our assigned interfaces from earlier. From here, we will change the pfSense default interface names to the ones that corresponds to their virtual network in our lab (listed previously in pfSense Configuration) as seen below:

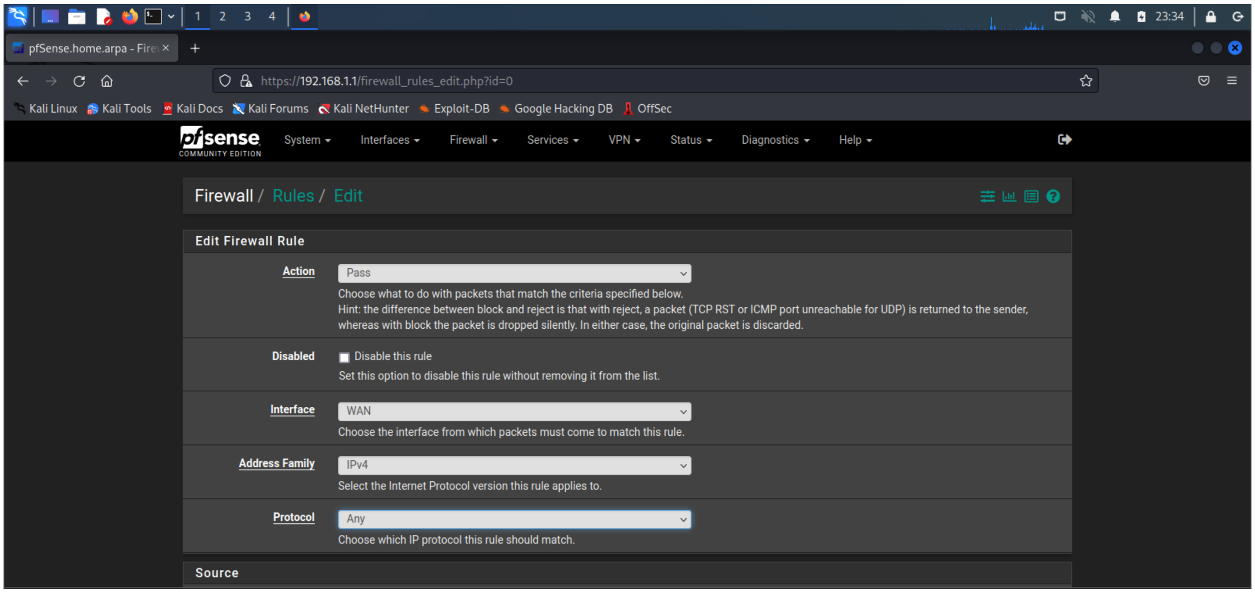


Interfaces / Interface Assignments

Interface	Network port
WAN	em0 (00:0c:29:12:74:04)
Kali	em1 (00:0c:29:12:74:0e) Delete
VictimNetwork	em2 (00:0c:29:12:74:18) Delete
SecurityOnion	em3 (00:0c:29:12:74:22) Delete
SpanPort	em4 (00:0c:29:12:74:2c) Delete
Splunk	em5 (00:0c:29:12:74:36) Delete

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Next, we will create a firewall rule where the pfSense will accept any protocols pass through the firewall as shown below. This will allow for interesting types of security alerts and logs to view when we conduct an attack and monitor/detect it:



Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: □ Disable this rule
Set this option to disable this rule without removing it from the list.

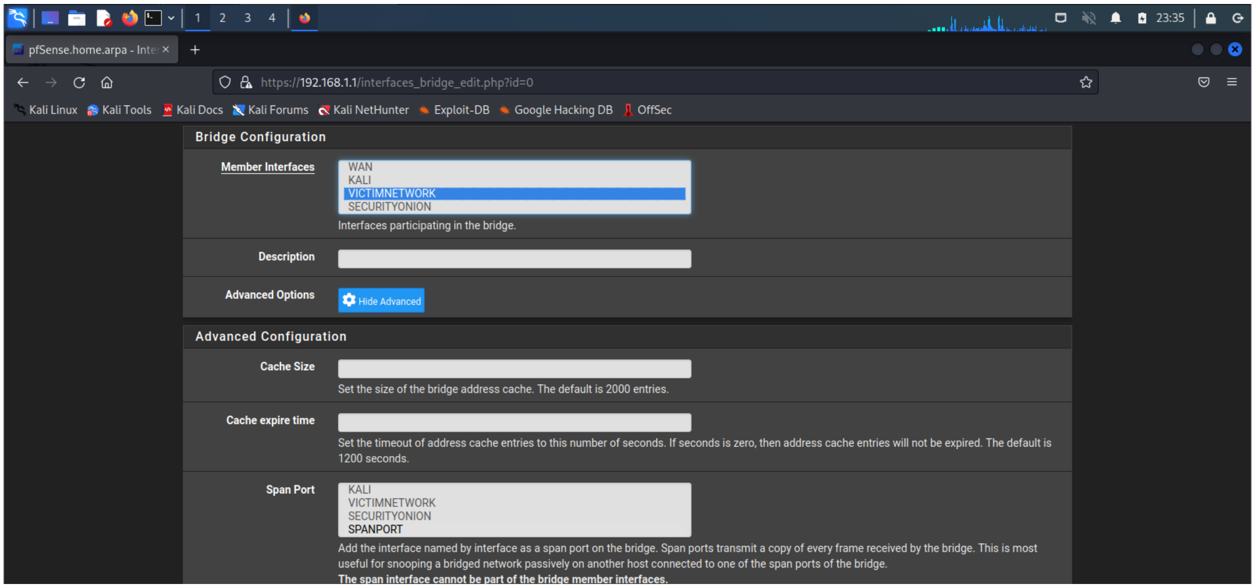
Interface: WAN
Choose the interface from which packets must come to match this rule.

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

Protocol: Any
Choose which IP protocol this rule should match.

Source

We will also want to create a bridge where the member interface is the victim network with the Span Port set as shown below:



Bridge Configuration

Member Interfaces: WAN, KALI, VICTIMNETWORK (selected), SECURITYONION

Interfaces participating in the bridge.

Description:

Advanced Options: Hide Advanced

Advanced Configuration

Cache Size:

Set the size of the bridge address cache. The default is 2000 entries.

Cache expire time:

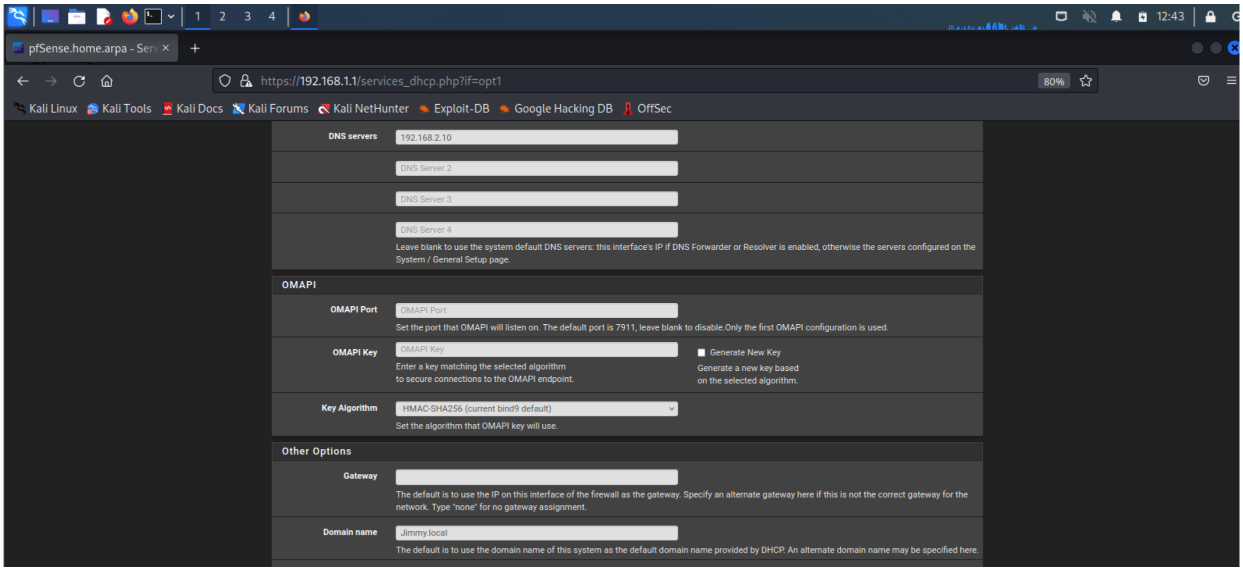
Set the timeout of address cache entries to this number of seconds. If seconds is zero, then address cache entries will not be expired. The default is 1200 seconds.

Span Port: KALI, VICTIMNETWORK, SECURITYONION, SPANPORT

Add the interface named by interface as a span port on the bridge. Span ports transmit a copy of every frame received by the bridge. This is most useful for snooping a bridged network passively on another host connected to one of the span ports of the bridge.

The span interface cannot be part of the bridge member interfaces.

Lastly, we will need to add the DNS server to the DHCP server for the victim network. In addition, we will also add the domain name “Jimmy.local” as shown below. This DNS server IP address and domain name will be from the Domain Controller that will be set up in the next section of this lab. These settings are necessary in order for the Windows User to join the local Active Directory domain in the later section of the lab:



DNS servers: 192.168.2.10

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.

OMAPI

OMAPI Port: OMAPI Port

Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable.Only the first OMAPI configuration is used.

OMAPI Key: OMAPI Key

Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.

□ Generate New Key

Generate a new key based on the selected algorithm.

Key Algorithm: HMAC-SHA256 (current bind9 default)

Set the algorithm that OMAPI key will use.

Other Options

Gateway:

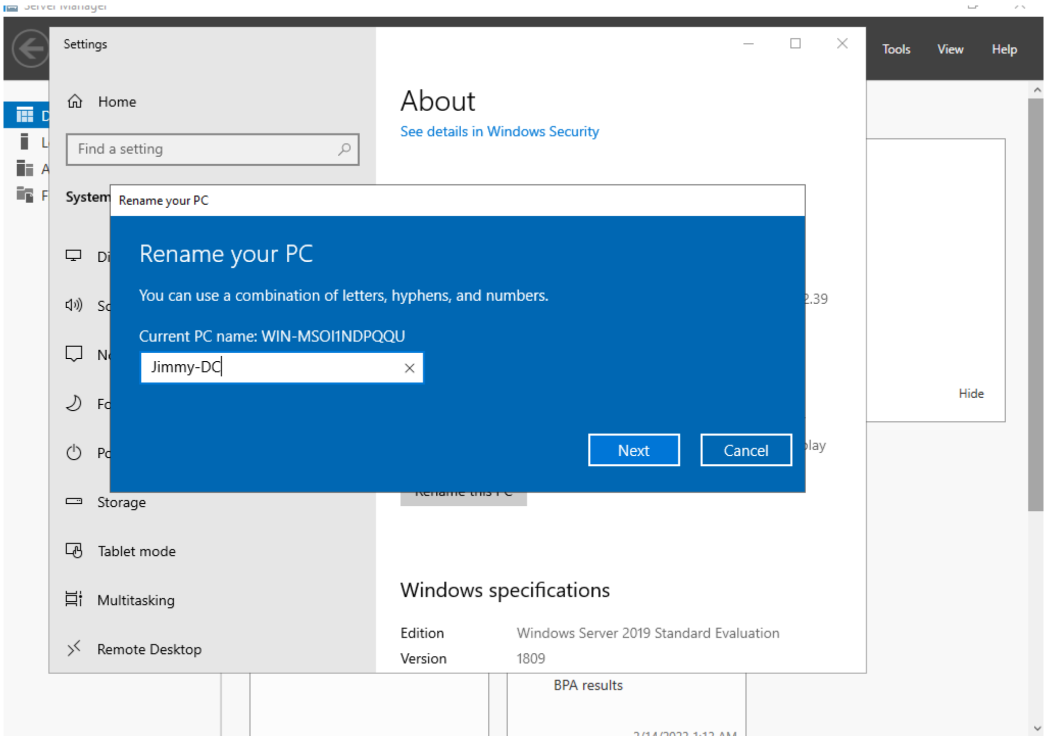
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

Domain name: Jimmy.local

The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.

Windows Server Domain Controller Configuration

In this section, we will be setting an local Active Directory domain with a Windows 2016 Server as the Domain Controller with one Windows 10 user. Once we are finished with configuring the initial setup of making an Administrator account, we will change the PC name of the Windows Server to something that we can resemble it is a Domain Controller as shown below:



About

Rename your PC

You can use a combination of letters, hyphens, and numbers.

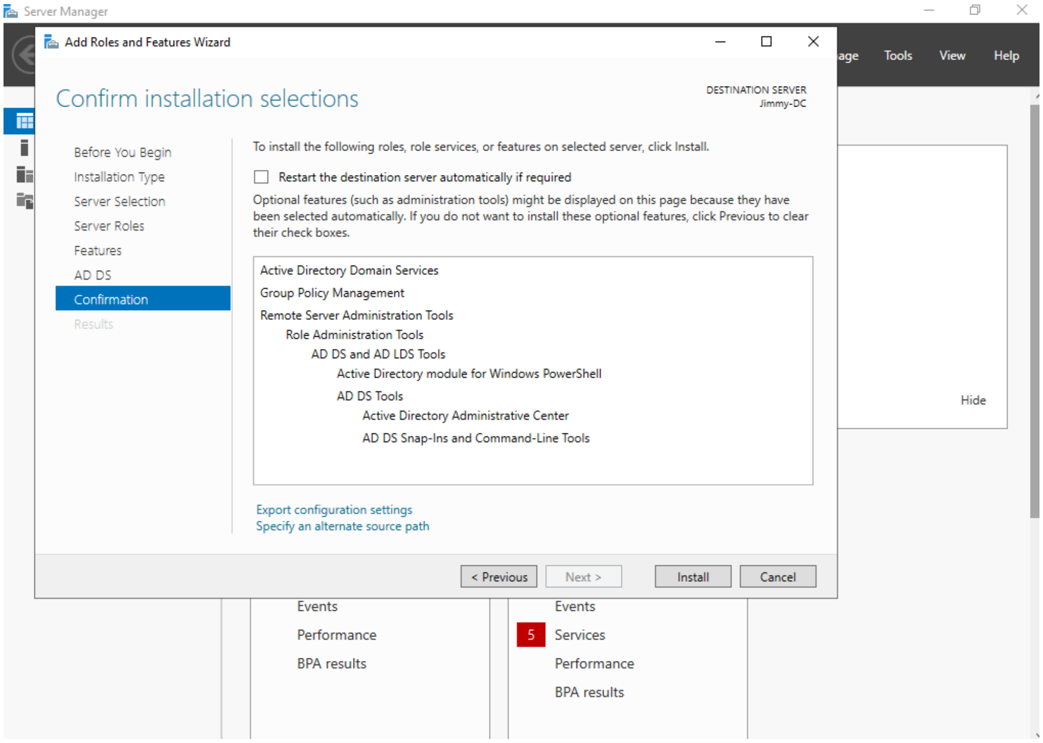
Current PC name: WIN-MSOI1NDPQQU

Jimmy-DC

Windows specifications

Edition	Windows Server 2019 Standard Evaluation
Version	1809

Next, we will want to add the Active Directory Domain Services (AD DS) server role with the default features as shown below:



Confirm installation selections

DESTINATION SERVER
Jimmy-DC

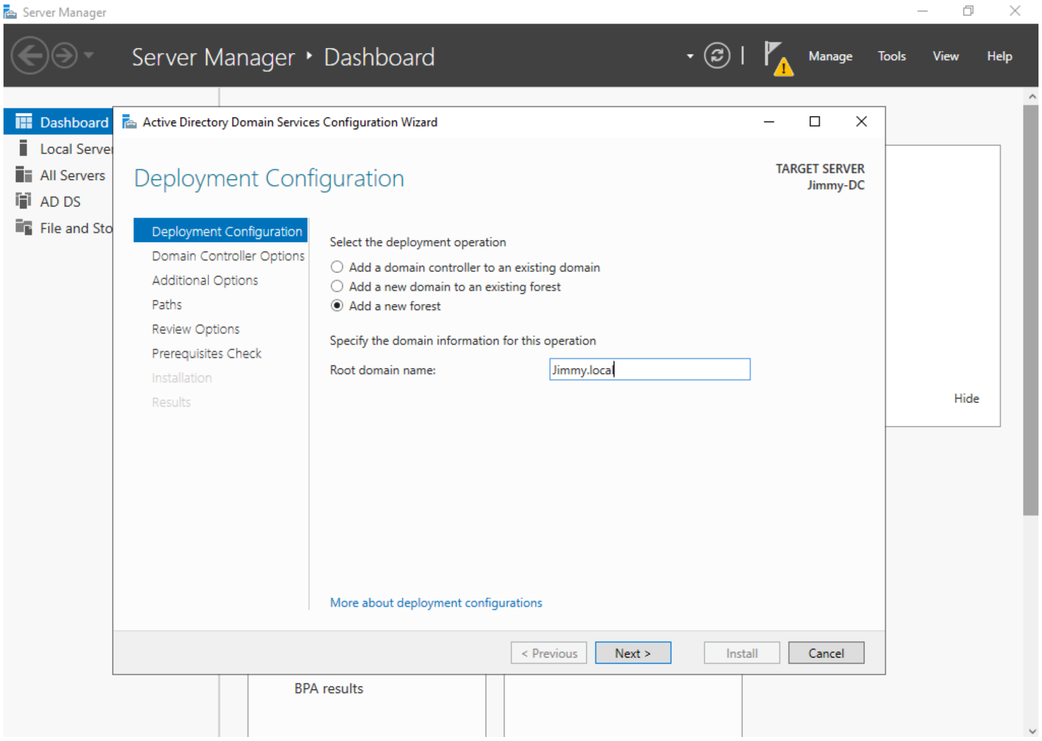
To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- Active Directory Domain Services
- Group Policy Management
- Remote Server Administration Tools
    - Role Administration Tools
        - AD DS and AD LDS Tools
            - Active Directory module for Windows PowerShell
            - AD DS Tools
                - Active Directory Administrative Center
                - AD DS Snap-Ins and Command-Line Tools

After the server role installation is complete, we would want to promote the Windows server to a Domain Controller. Since this is our first Domain Controller, we will create a new forest with a root domain name as “Jimmy.local” as our local Active Directory domain as shown below:



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
Jimmy-DC

Select the deployment operation

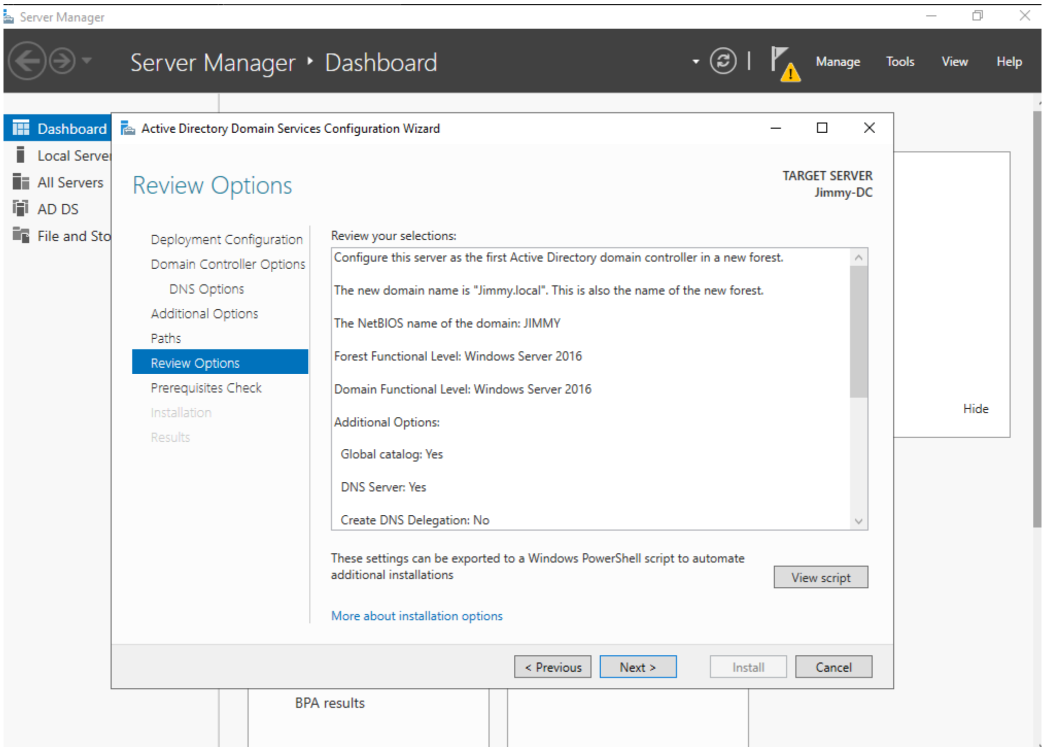
○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: Jimmy.local

More about deployment configurations

The Domain Controller will have DNS Server and Global catalog options checked by default as they are necessary for it to operate properly. The full configuration of the Domain Controller can be seen below:



Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "Jimmy.local". This is also the name of the new forest.

The NetBIOS name of the domain: JIMMY

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

Additional Options:

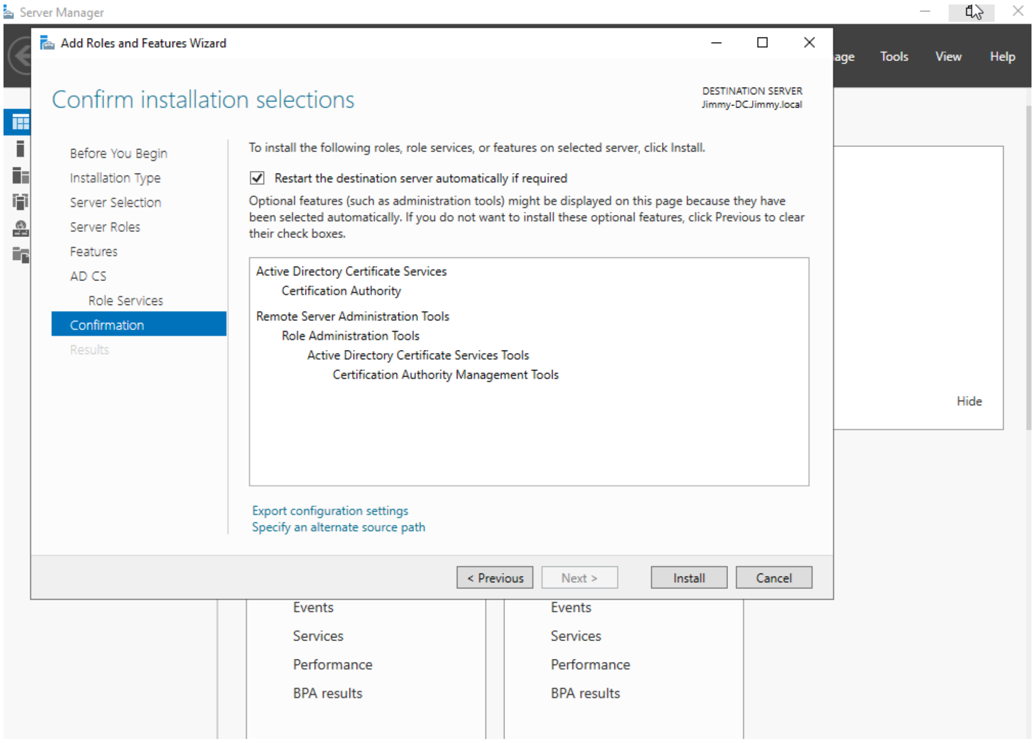
Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations

Next, we would want to go through the same process for setting up the Active Directory Certificate Services (AD CS). In the installation, we would want to check the box for Certificate Authority (CA) as that would allow the Domain Controller to act as a CA to validate certificates. The screenshots of settings that up can be seen below:



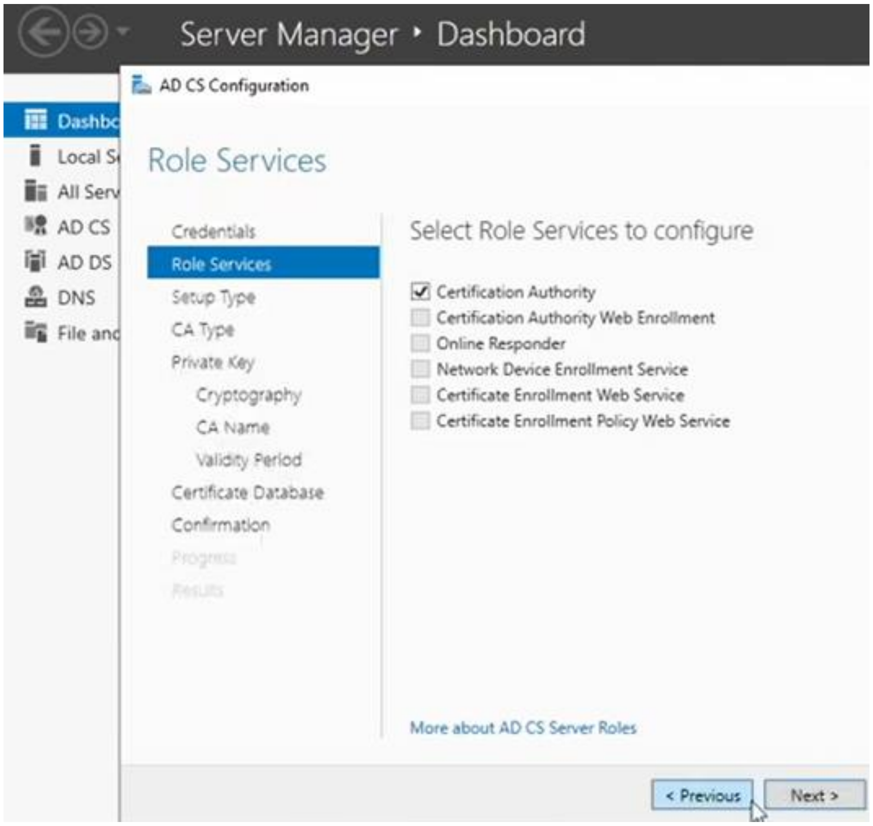
To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Certificate Services
- Certification Authority

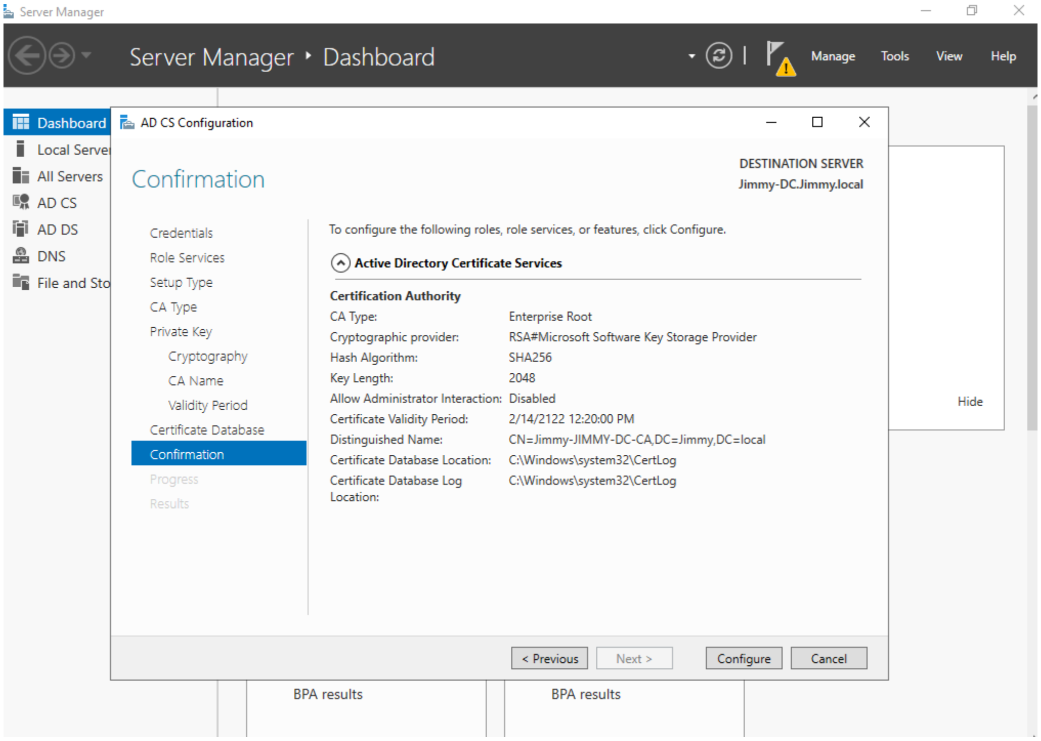
Remote Server Administration Tools
- Role Administration Tools
  - Active Directory Certificate Services Tools
    - Certification Authority Management Tools



Role Services

Select Role Services to configure

☑ Certification Authority
□ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service



Confirmation

DESTINATION SERVER
Jimmy-DC.Jimmy.local

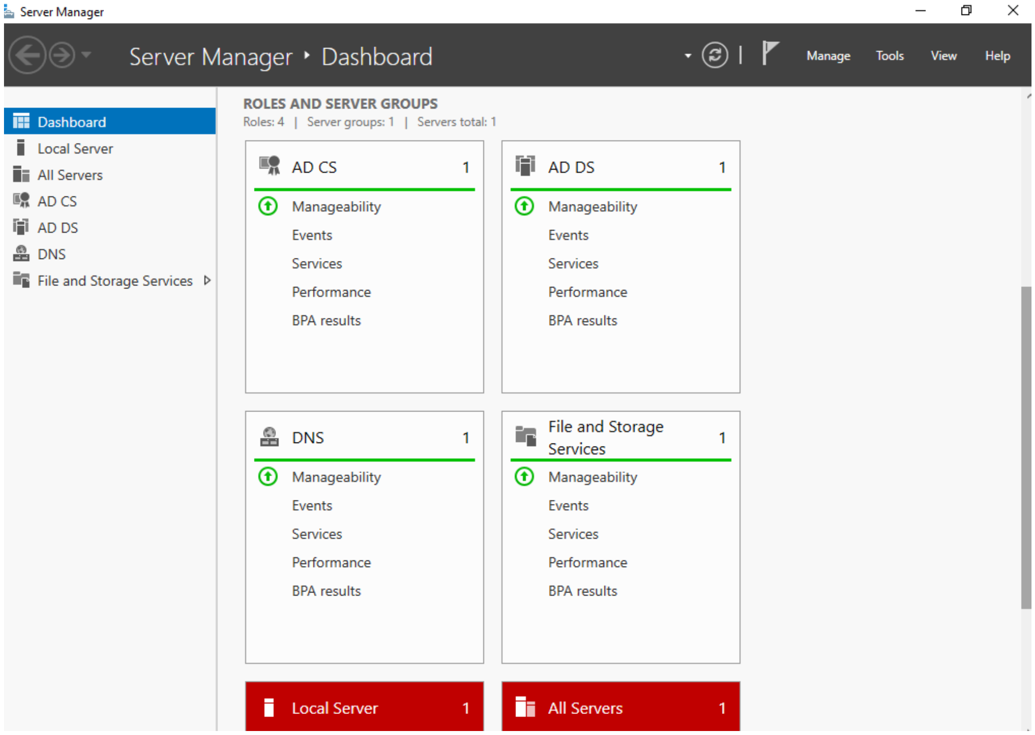
To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

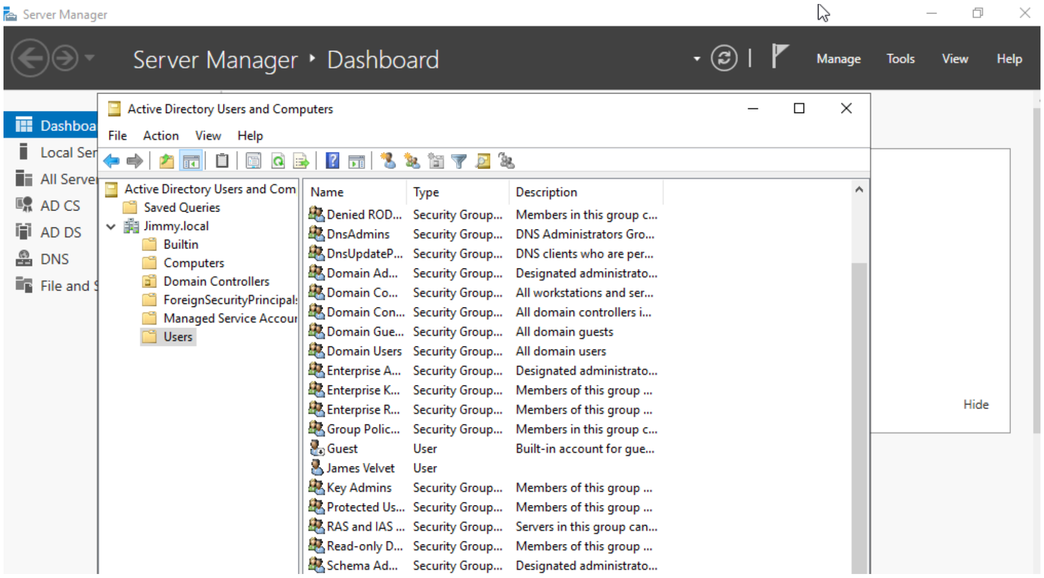
Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	2/14/2122 12:20:00 PM
Distinguished Name:	CN=Jimmy-JIMMY-DC-CA,DC=Jimmy,DC=local
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Once both AD DS and AD CS are properly installed and assigned to the now Windows Server Domain Controller, we should see this screenshot in our main dashboard below:

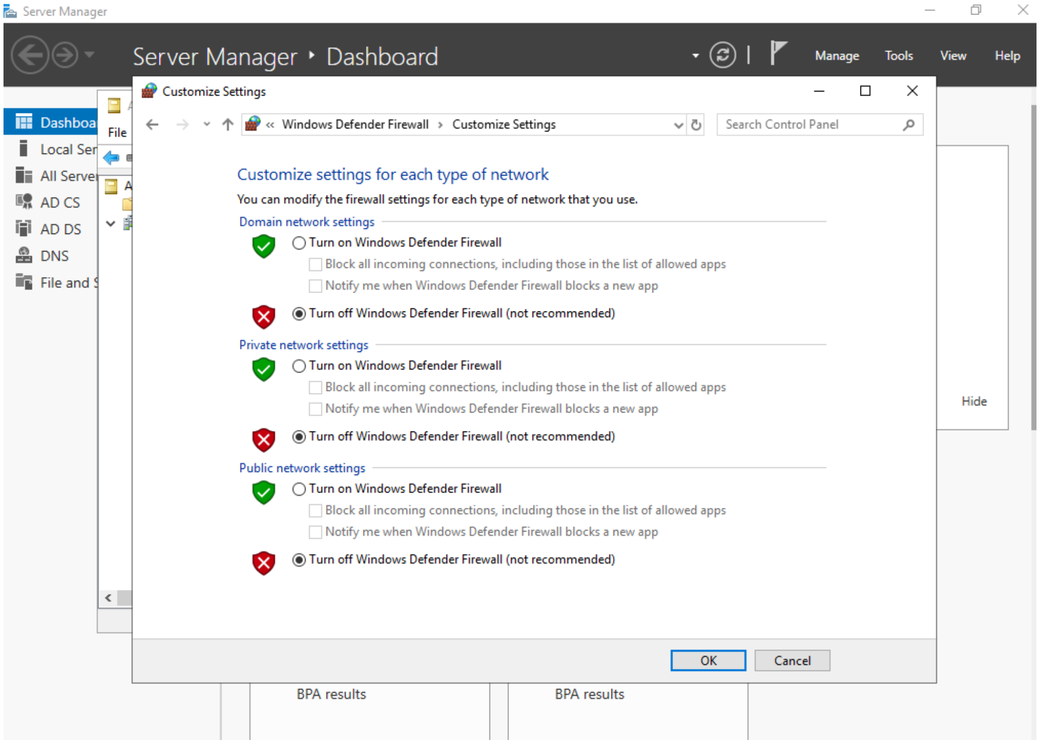


Next, we would want to create a new Windows user (named James Velvet) within the Users folder for our Active Directory as shown below:



Name	Type	Description
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
James Velvet	User	
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...

Afterwards, we will disable all of the default Window’s firewall settings in order to maximize the amount of vulnerabilities we can generate from alerts and logs once we start detecting and monitoring them. The disabling of the Windows firewall can be seen below:



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

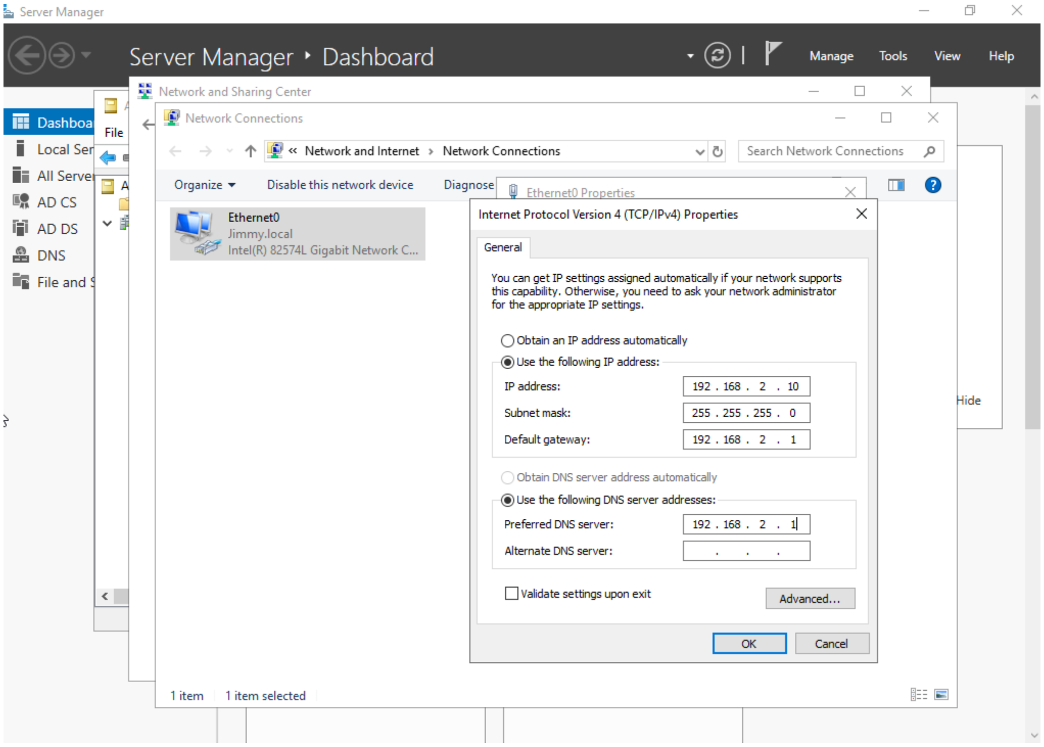
○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Lastly, we will assign the Domain Controller its network adapter configurations with 192.168.2.10 as its IP address, pfSense firewall as its default gateway and DNS server as seen below:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

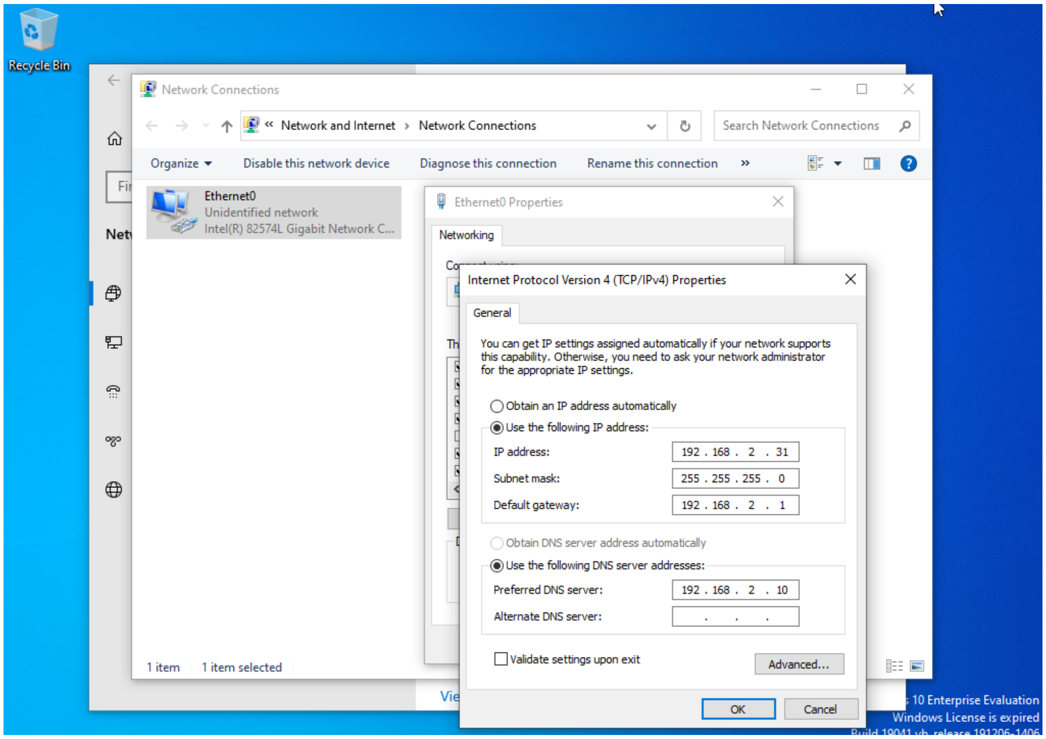
Preferred DNS server: 192 . 168 . 2 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

Adding the User to the Local Active Directory Domain

Once the virtual machine for the Windows user (James Velvet) is set and we have changed the PC name for that respective Windows user, we would want to first configure its network adapter settings with 192.168.2.31 as its IP address, pfSense as its default gateway, and the Domain Controller as its DNS server as seen below:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

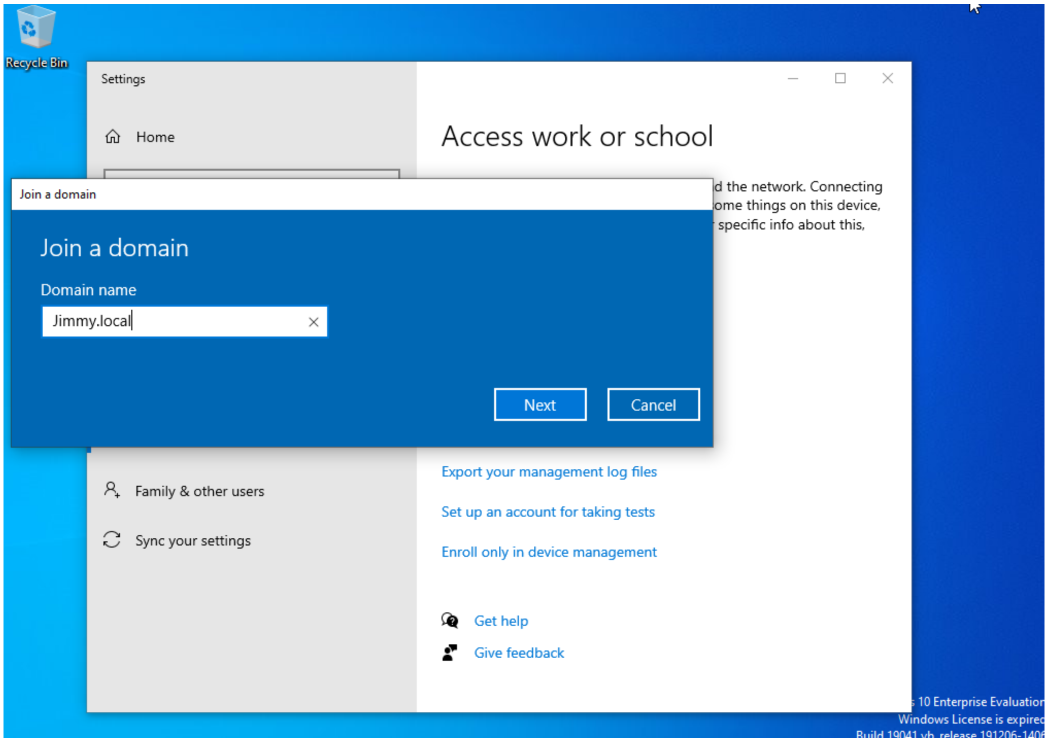
IP address: 192 . 168 . 2 . 31
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 2 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 2 . 10
Alternate DNS server: . . .

□ Validate settings upon exit

Afterwards, we will let the user join the local Active Directory domain (Jimmy.local) as seen below. The domain account used to verify is the Administrator account set up within the Windows Server at the very beginning of that section:


Recycle Bin
Settings
Home
Family & other users
Sync your settings
Export your management log files
Set up an account for taking tests
Enroll only in device management
Get help
Give feedback
Next
Cancel
10 Enterprise Evaluation
Windows License is expired
Build 19041.vb_release.191206-1406

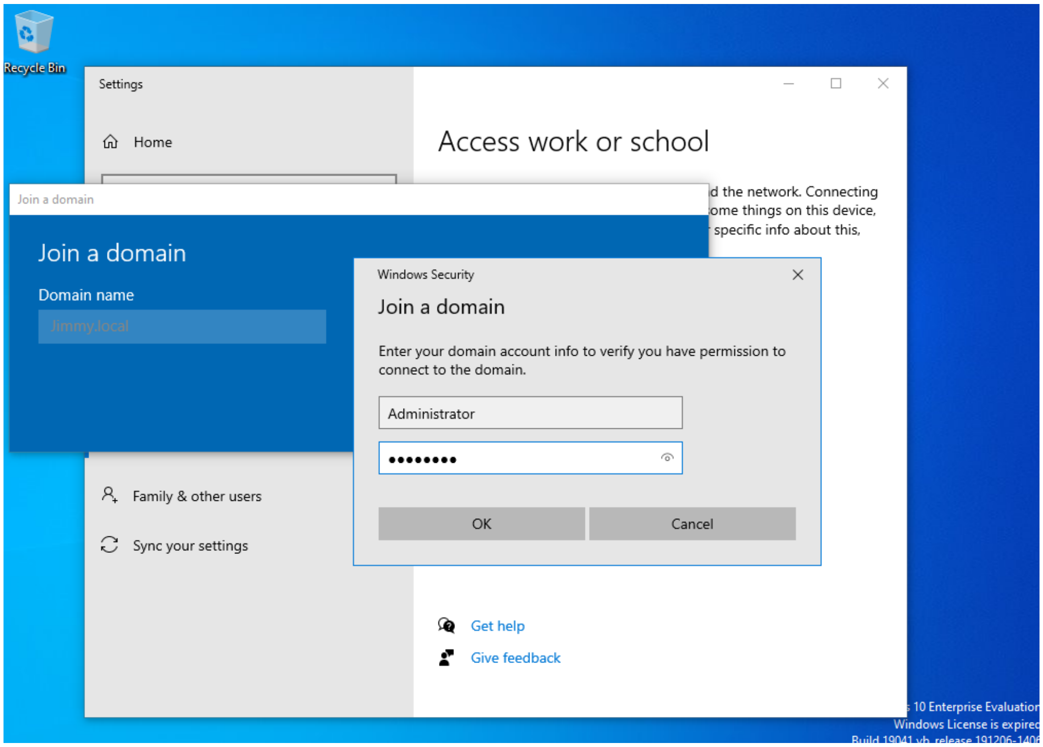
Access work or school

d the network. Connecting
ome things on this device,
specific info about this,

Join a domain

Join a domain

Domain name: Jimmy.local



Access work or school

d the network. Connecting
ome things on this device,
specific info about this,

Join a domain

Join a domain

Domain name: Jimmy.local

Windows Security

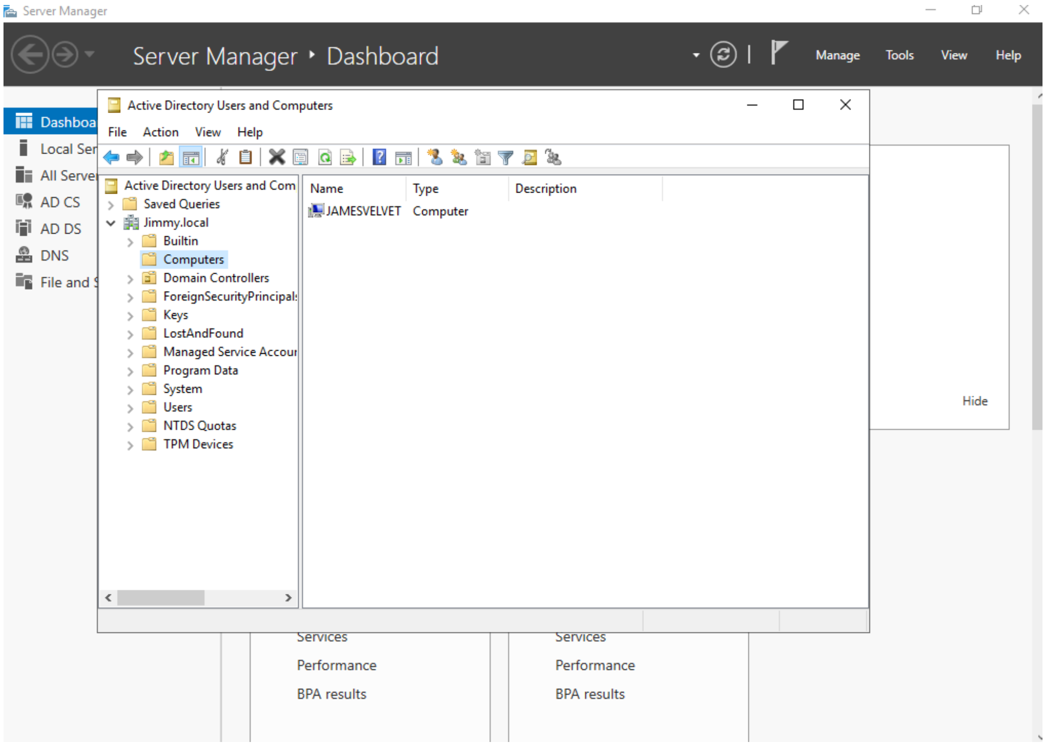
Join a domain

Enter your domain account info to verify you have permission to connect to the domain.

Administrator

••••••••

We can confirm that the Windows user (James Velvet) was able to join the local Active Directory domain by checking the Windows Server’s Active Directory Computers folder as seen below:



Name	Type	Description
JAMESVELVET	Computer	

Ubuntu Server and Splunk Configuration

TBA

Installing Universal Forwarder on Windows Server

TBA