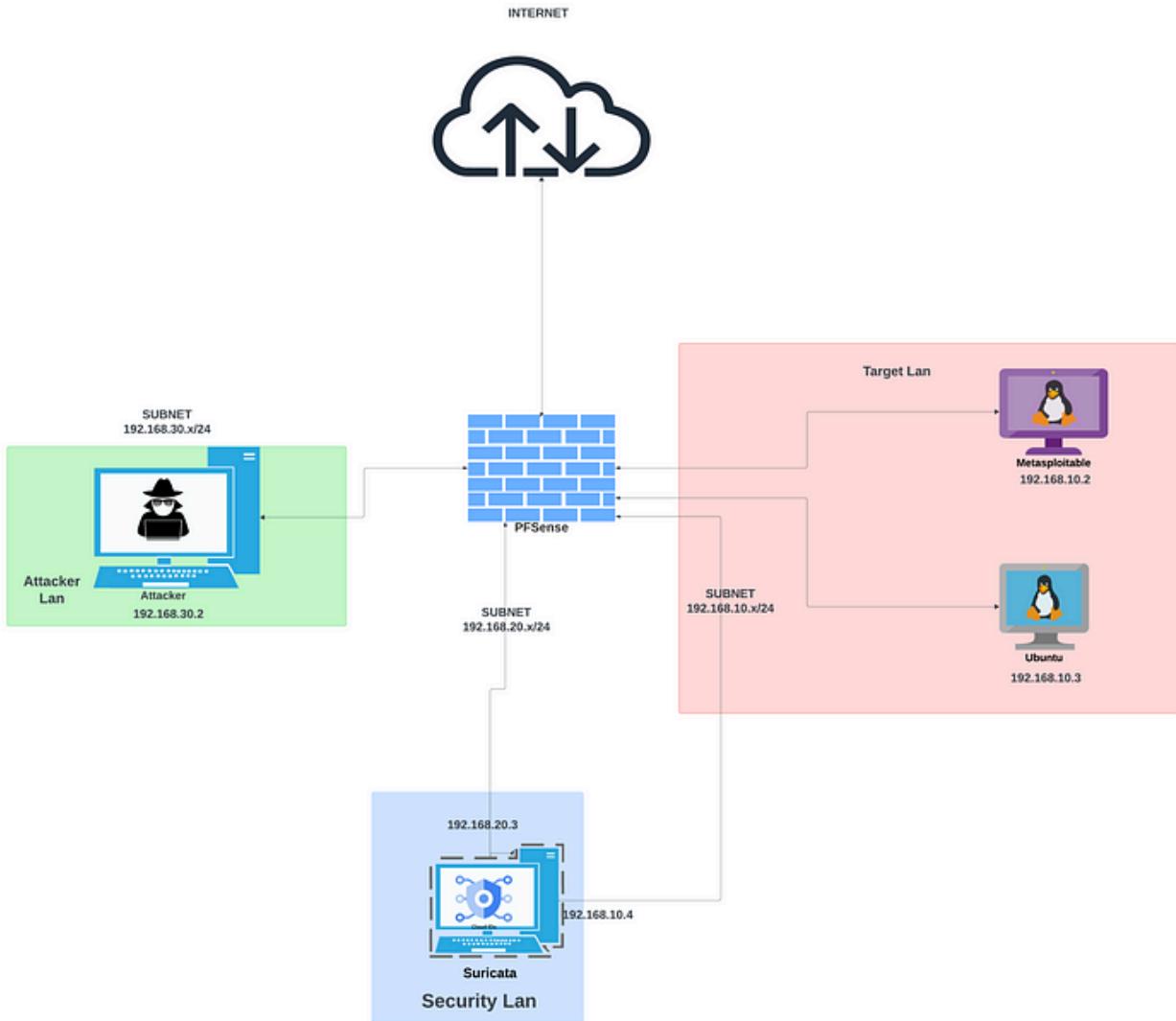


Creating this lab not only allowed me to refresh my networking and virtualization skills but also emphasized the importance of understanding your network to effectively secure and monitor for threats. It's a project I've been eager to share, detailing step-by-step configurations for each system in the simulated home network.

If you are familiar with computer networking, virtualization and basics of operating systems and build your own lab.

Lab Environment:

1. Having a network diagram helps while setting it up, to avoid confusion. Having a blueprint is indeed a good practice.
2. Below is the network diagram I came up with when building up my home network.



3. Networks:

a. Target Lan (192.168.10.x/24):

→ This would include the Metasploitable and Ubuntu Desktop machines.

→ Also, One of the interface of the monitoring device running suricata will be in target lan and configured to run in promisc mode, this helps the interface to capture all the traffic in the target lan.

b. Security Lan (192.168.20.x/24):

→ All the machines for monitoring traffic and threats will have their interface in this subnet, I will have a Ubuntu Machine running suricata and splunk, with one interface in this subnet and other in the target-lan for monitoring.

c. Attacker Lan (192.168.30.x/24):

→ I have kept a kali machine connected to this lan which will simulate the attacks on to my target lan.

Installation:

I assume, you understood the lab environment. I have given the resources on how to install ubuntu and kali linux in virtualbox. I will be demonstrating on how to setup pfSense and Splunk Cloud.

1. [Virtualbox](#).
2. [Ubuntu Desktop](#).
3. [Kali Linux](#).
4. [Pfsense](#) (Just install the file , the configurations for this are described in the below sections).
5. [Metasploitable](#).

Installation and configuring pfSense:

Create a new machine, I have named it PfSense gateway.

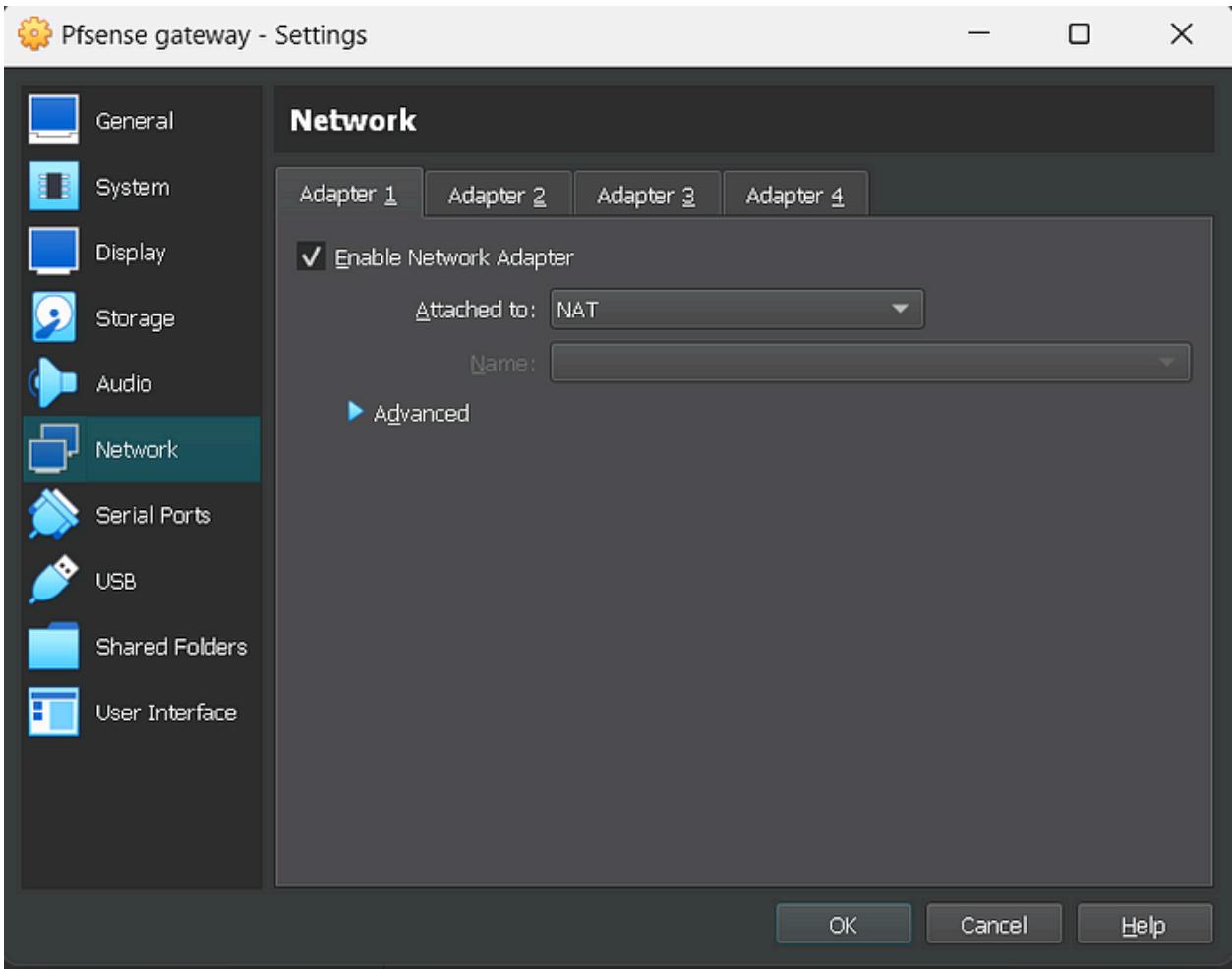
1. Ram:- 2 gb (recommended).
2. CPU- 2 (recommended).
3. Storage:- 20–25 (Default recommended).

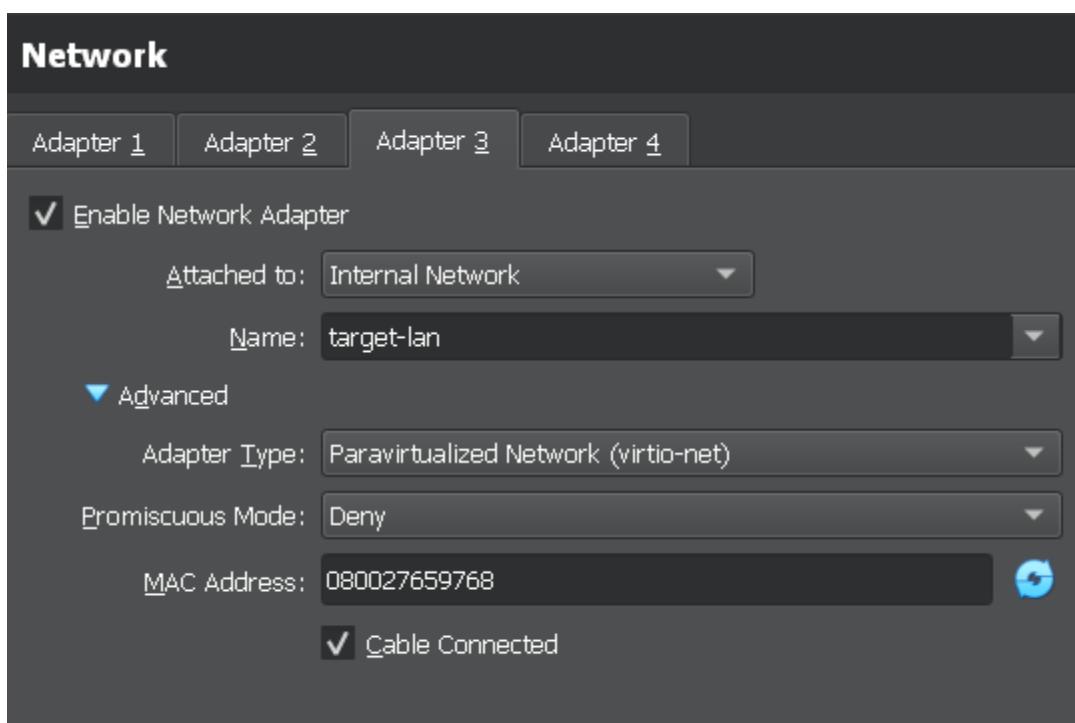
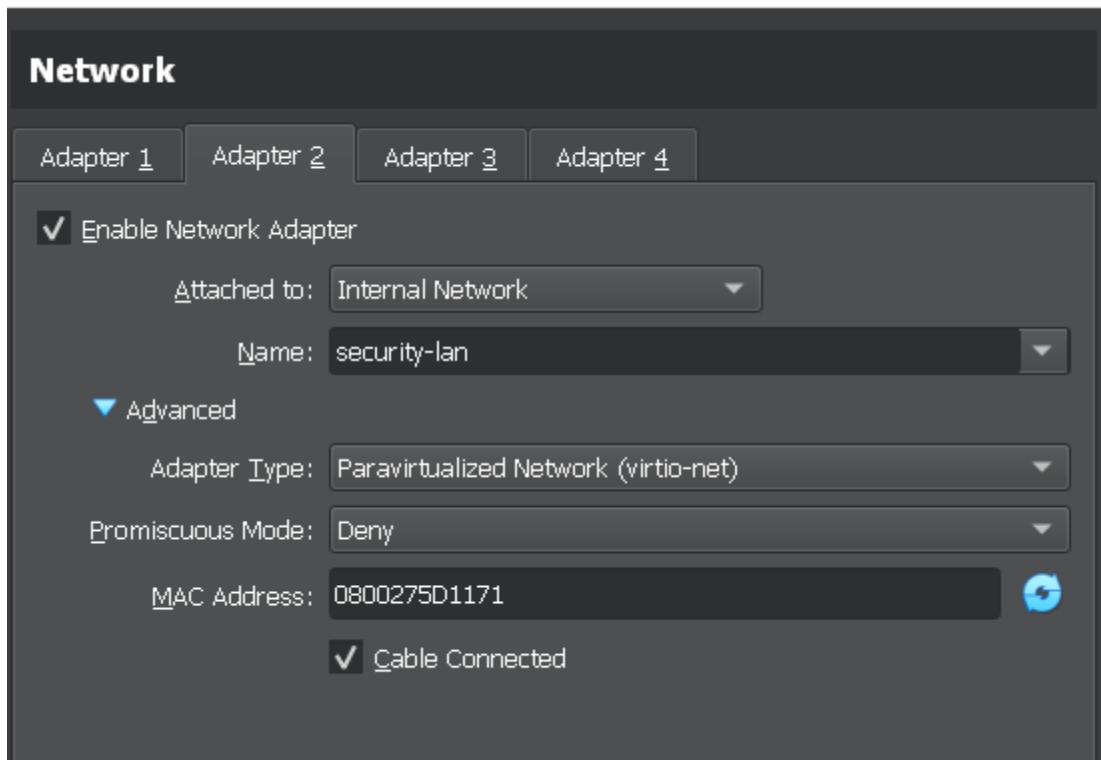
LAN setup:

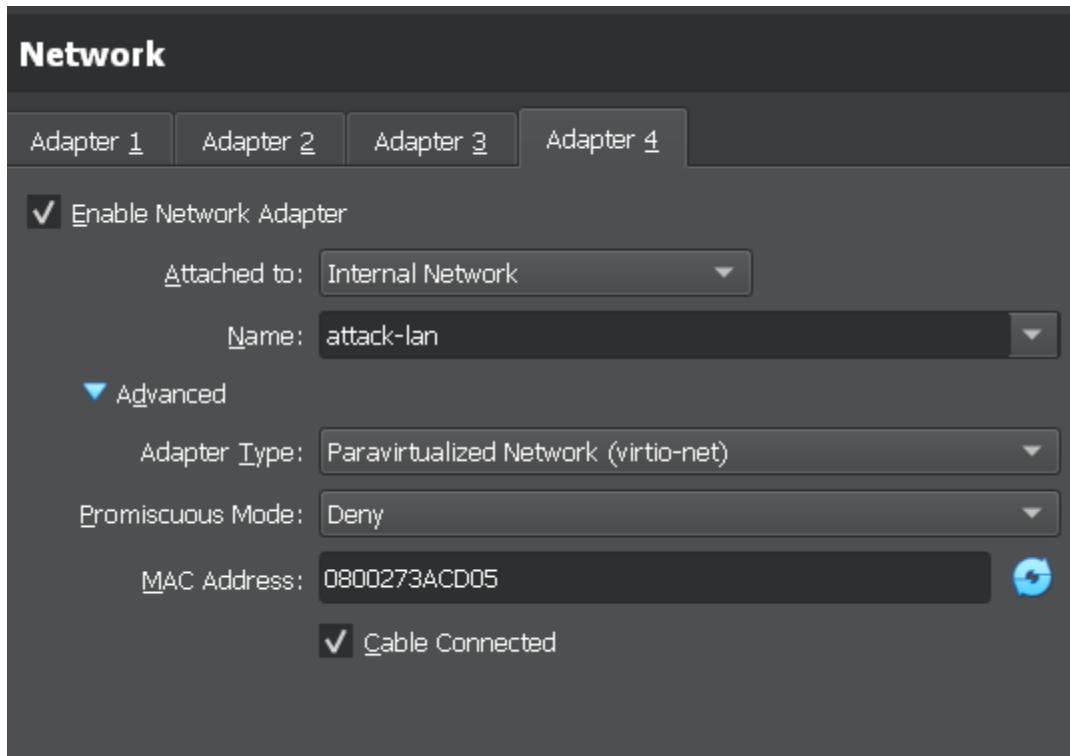
I have created 4 adapters on the machine running pfSense:

1. Adapter 1 — NAT.
2. Adapter 2 — Security Lan.
3. Adapter 3 — Target Lan.
4. Adapter 4 — Attacker Lan.

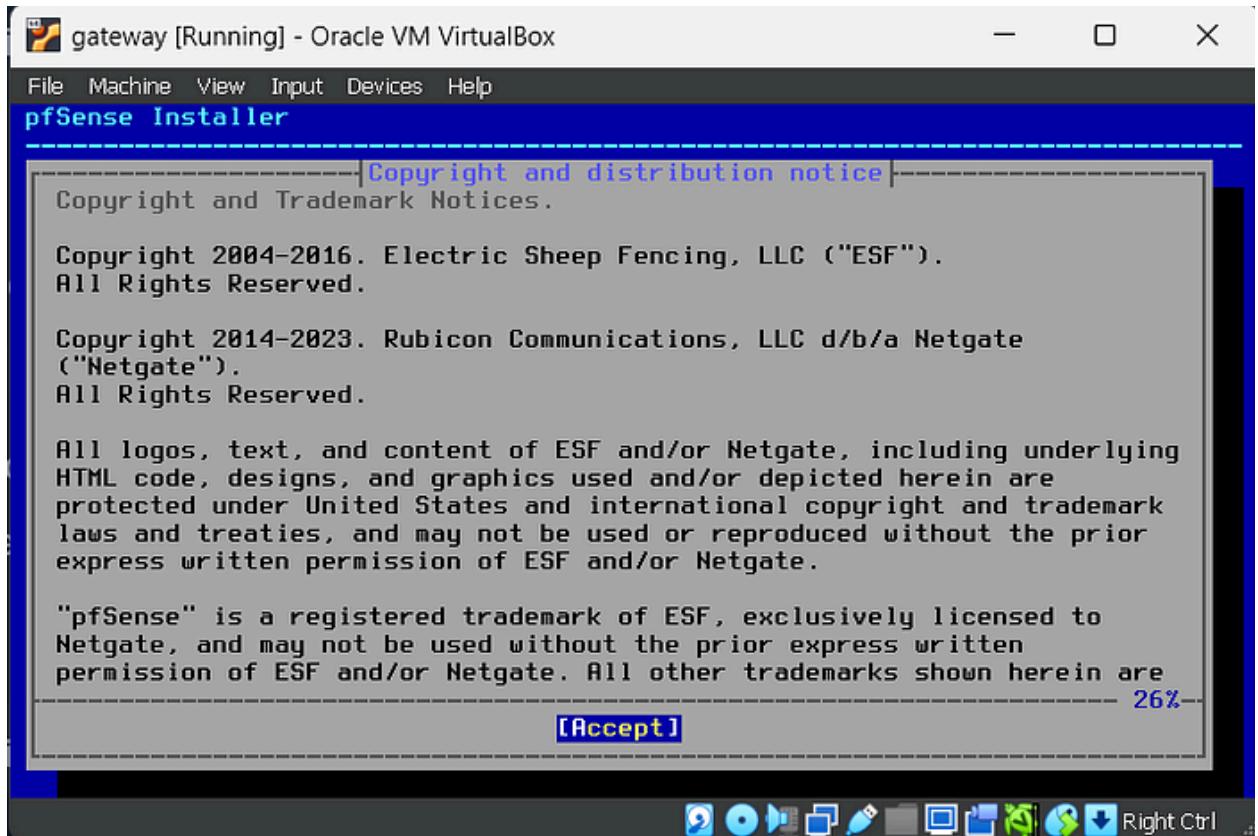
check the below screenshots:



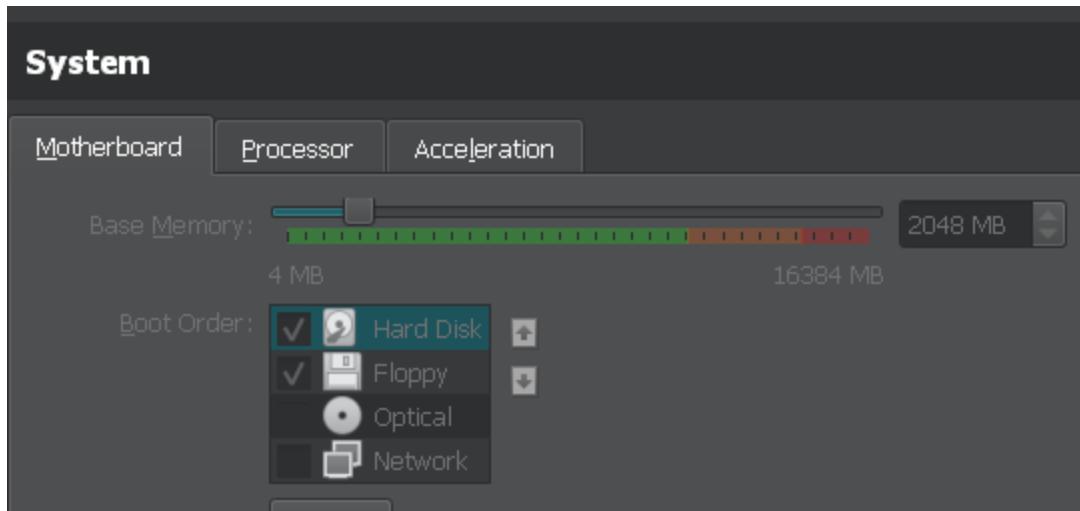




Now start the machine and wait for the copyright section to appear:



Select Install → Auto UFS → BR DOS Partition → Finish → Commit and wait for it to install and then reboot. After rebooting if it prompts for the Copyright page again like above, change the boot order of the virtual machine.



Then start the machine again:

```
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y/n]? 2024-07-20T12:16:11.428001+00:00 - php-fpm 388
-- /rc.linkup: Ignoring link event during boot sequence.
2024-07-20T12:16:15.757194+00:00 - php-fpm 388 -- /rc.linkup: Ignoring link event
during boot sequence.
2024-07-20T12:16:15.760246+00:00 - php-fpm 389 -- /rc.linkup: Ignoring link event
during boot sequence.
em0: link state changed to UP
2024-07-20T12:16:17.514097+00:00 - php-fpm 661 -- /rc.linkup: DHCP Client not running on wan (em0), reconfiguring dhclient.
2024-07-20T12:16:32.899874+00:00 - php-fpm 661 -- /rc.newwanip: rc.newwanip: Info: starting on em0.
2024-07-20T12:16:32.900235+00:00 - php-fpm 661 -- /rc.newwanip: rc.newwanip: ok (IP address: 10.0.2.15) (interface: WAN[wan]) (real interface: em0).
pflog0: promiscuous mode enabled

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 vtnet0 vtnet1 vtnet2 or a):
```

I have set the first adapter to NAT, hence the WAN interface is indeed em0 so enter em0 and then click [Enter].

Then you will be shown the below screen

```
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

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

KVM Guest - Netgate Device ID: 0180a05d7479a58c2827

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24

 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: █
```

Assigning Interfaces

Enter 1 → Should vlan be set up : y → Enter parent interface : [Click Enter] → then set the interface as below image → then proceed with “y”.

Adapter 1(NAT): – em0...(this will be facing the internet).

Adapter 2(Security-Lan):-vtnet0.

Adapter 3(Target-Lan):-vtnet1.

Adapter 4(Attacker Lan):- vtnet2.

```
VLAN Capable interfaces:
em0      08:00:27:2f:46:d5    (up)
vtnet0   08:00:27:66:5b:01    (up)
vtnet1   08:00:27:5b:ec:0a    (up)
vtnet2   08:00:27:2a:3d:f3    (up)

Enter the parent interface name for the new VLAN (or nothing if finished):
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 vtnet0 vtnet1 vtnet2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet0 vtnet1 vtnet2 a or nothing if finished): vtnet0

Enter the Optional 1 interface name or 'a' for auto-detection
(vtnet1 vtnet2 a or nothing if finished): vtnet1

Enter the Optional 2 interface name or 'a' for auto-detection
(vtnet2 a or nothing if finished): vtnet2
```

Configuring IP addresses

emo : Adapter 1 (NAT)

Enter 2 → Enter 1 (for wan interface) → DHCP (ipv4): “y” →
DHCP(ipv6):”n” → [Enter]

```
Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) y
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPCD...
Disabling IPv6 DHCPCD...
Please wait while the changes are saved to WAN...
```

vtneto : Adapter 2 (Security Lan)

Enter 2 → DHCP(v4):”n” → 192.168.20.1 → Subnet Mask : 24 →
[ENTER] → DHCP(v6):”n” → [Enter] → Enable DHCP on LAN:”y” →
Start:192.168.20.2 → End:192.168.20.254.

```
Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp)
2 - LAN (vtnet0 - dhcp)
3 - OPT1 (vtnet1)
4 - OPT2 (vtnet2)

Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.20.1

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:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n
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: 192.168.20.2
Enter the end address of the IPv4 client address range: 192.168.20.254
```

What the above configuration does is, it sets the ip 192.168.20.1 for the vtne0 interface and subnet 24 (255.255.255.0) which is associated with the Adapter 1 which we named it as Security-Lan in the internal network section in beginning. Then we tell that this interface will act

as dhcp through which our machines connected to this network will get the ip.

Since this is a /24 subnet it will consist of 254 usable address , one is used by the vtneto interface i.e 192.168.20.1 and remaining addresses will be leased by the connected machines later.

Repeat the above processes for:

vtnet1: Adapter 3(target-lan)

IPv4 address: 192.168.10.1.

subnet:/24.

dhcp range:192.168.10.2–254.

vtnet2: Adapter 4 (attacker-lan)

IPv4 address: 192.168.30.1

subnet:/24

dhcp range:192.168.30.2–254.

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vnet0    -> v4: 192.168.20.1/24
OPT1 (opt1)    -> vnet1    -> v4: 192.168.10.1/24
OPT2 (opt2)    -> vnet2    -> v4: 192.168.30.1/24

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: █
```

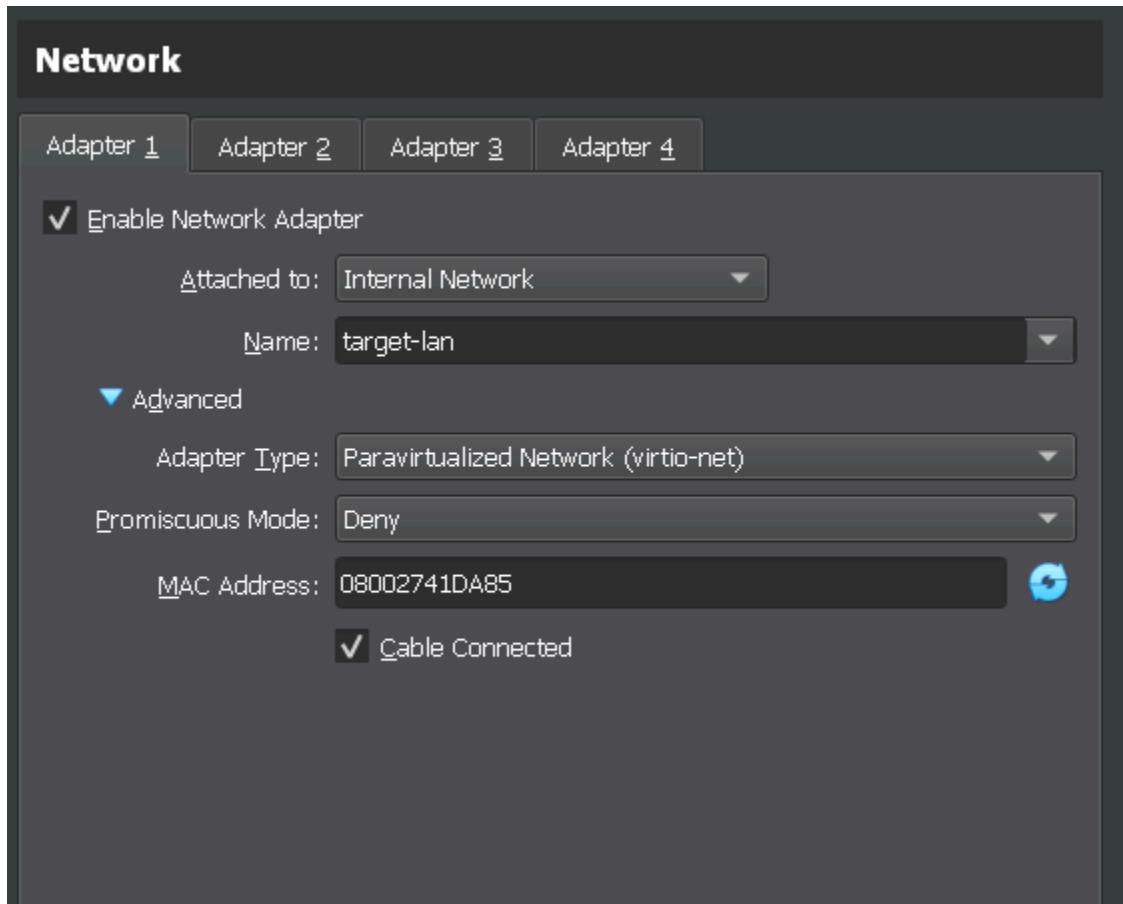
After setting up the ip addresses, the screen should display the interfaces with their ip address same as above.

Connect Machine to their respective LAN:

1. Connecting Ubuntu to the Target-Lan:

After installation → Go to machine settings → Set Adapter to Internal

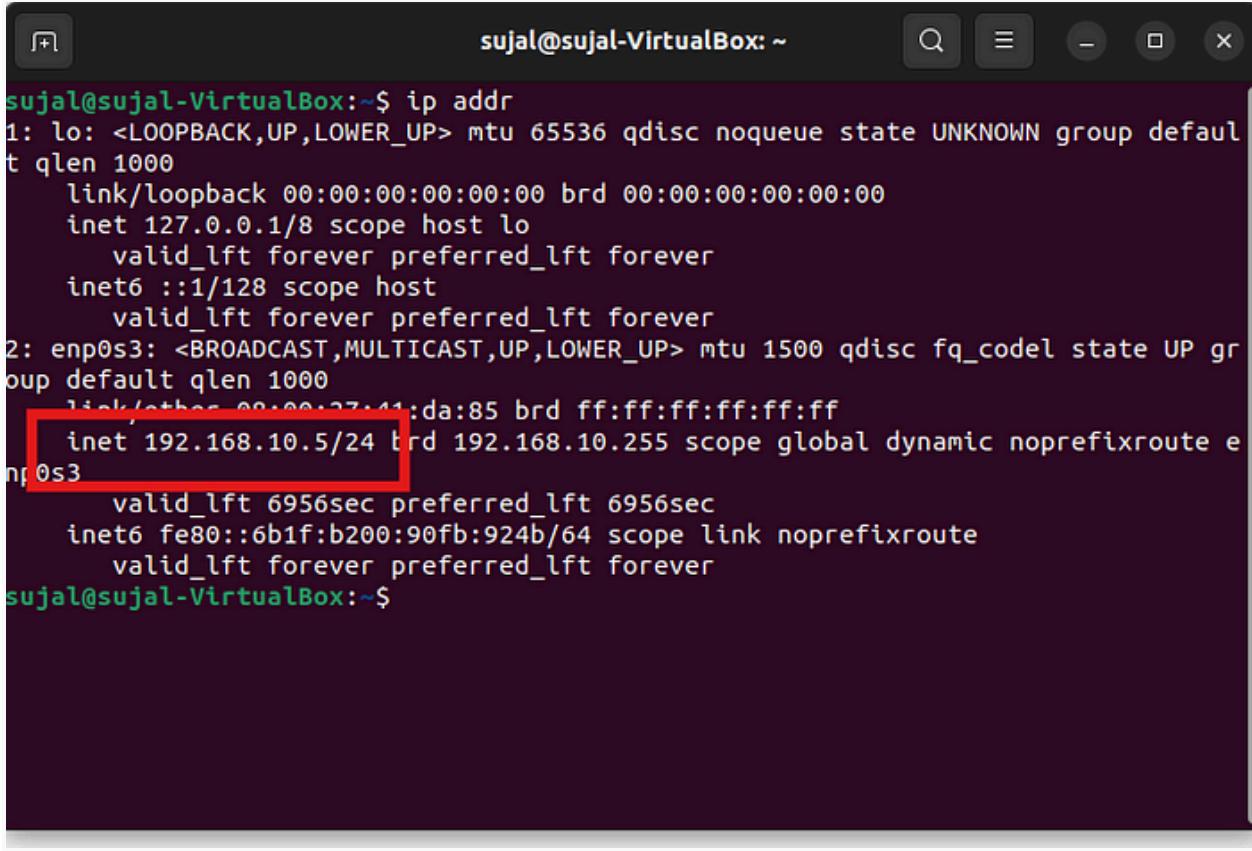
Network and target-lan → Save and restart the machine.



To verify if the machine got its ip address from the pfSense dhcp run

the below command:

```
ip addr
```



```
sujal@sujal-VirtualBox:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:00:27:41:da:85 brd ff:ff:ff:ff:ff:ff
   inet 192.168.10.5/24 brd 192.168.10.255 scope global dynamic noprefixroute enp0s3
        valid_lft 6956sec preferred_lft 6956sec
    inet6 fe80::6b1f:b200:90fb:924b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
sujal@sujal-VirtualBox:~$
```

We can see that the interface got its ip as the configured network range for target-lan.

NOTE:- Incase you don't see any ip address ,run “sudo dhclient [interface name]” from the terminal.

Similarly add the metasploitable machine to target lan and kali linux to attacker lan.

```
(kali㉿kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e:c2:80 brd ff:ff:ff:ff:ff:ff
        inet 192.168.30.2/24 brd 192.168.30.255 scope global dynamic noprefixroute
            valid_lft 6921sec preferred_lft 6921sec
        inet6 fe80::7629:bdbd:5afa:8923/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

Kali Linux Ip

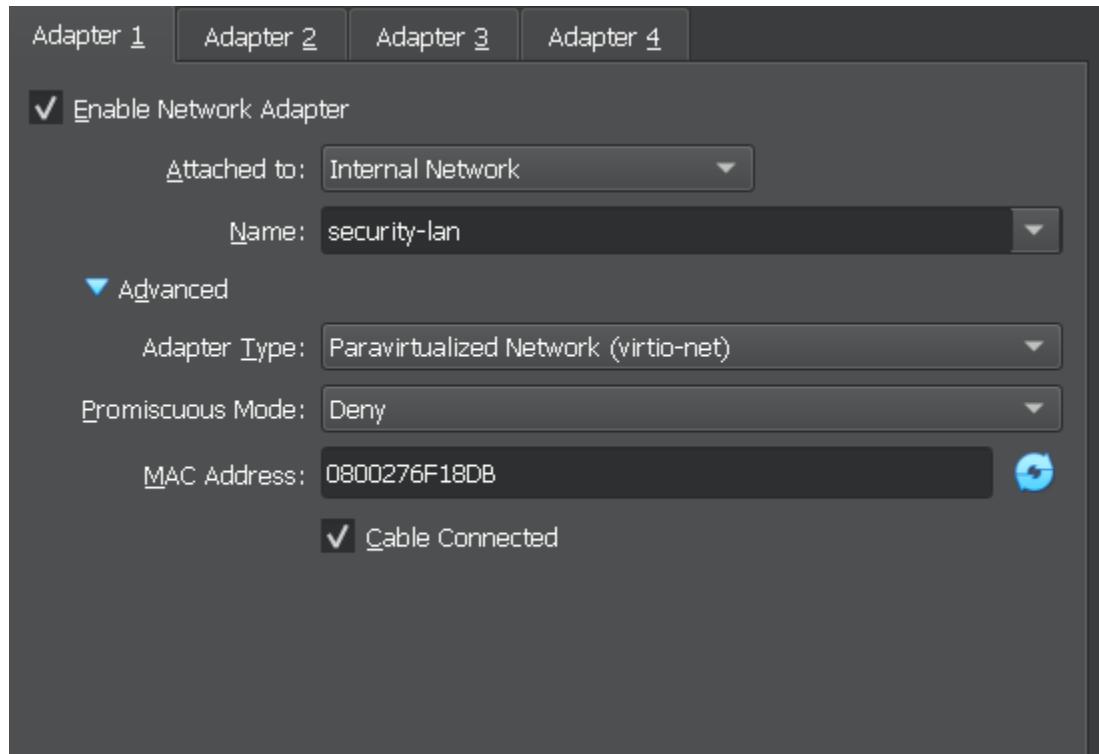
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:2c:d1:b2
          inet addr:192.168.10.6 Bcast:192.168.10.255 Mask:255.255.255.0
            inet6 addr: fe80::a00:27ff:fe2c:d1b2/64 Scope:Link
                      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                      RX packets:3 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                      RX bytes:756 (756.0 B) TX bytes:6066 (5.9 KB)
                      Base address:0xd020 Memory:f0200000-f0220000

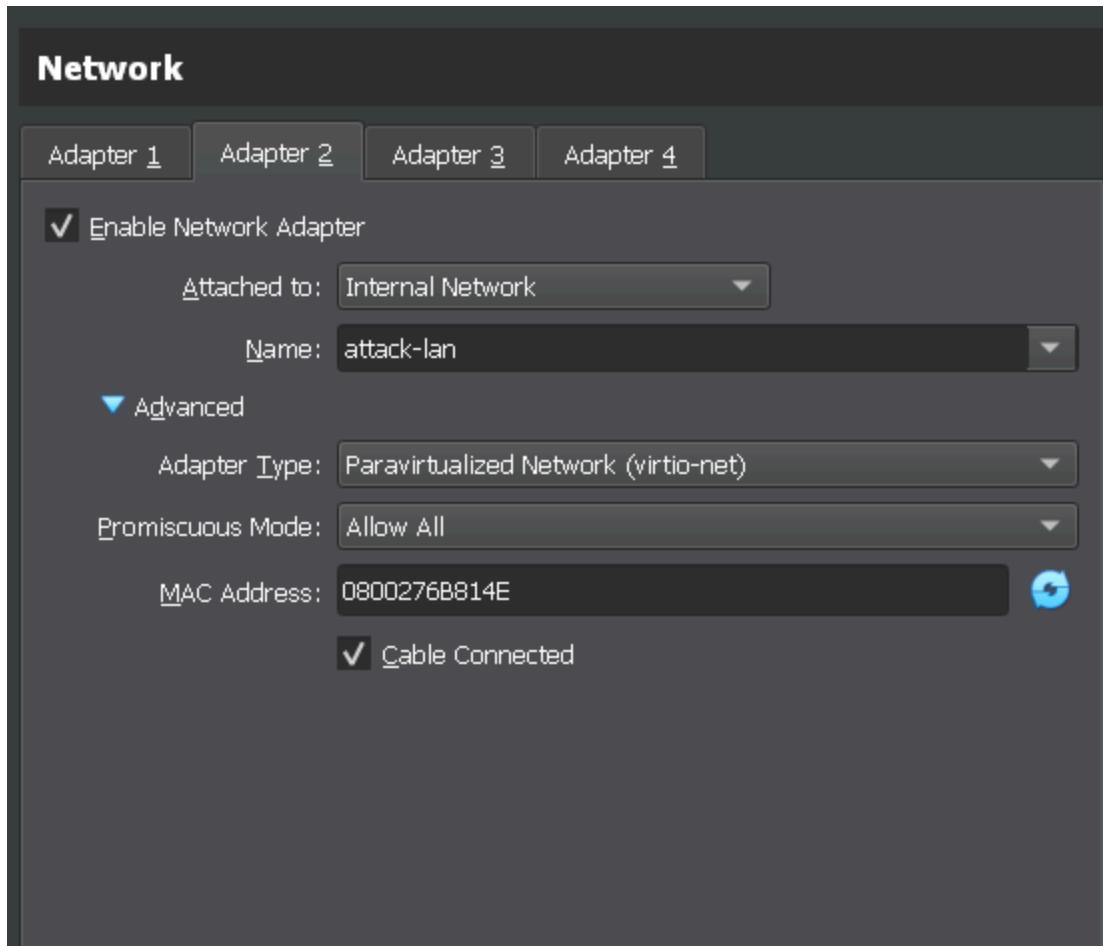
lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
                      UP LOOPBACK RUNNING MTU:16436 Metric:1
                      RX packets:106 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:0
                      RX bytes:25709 (25.1 KB) TX bytes:25709 (25.1 KB)
```

metasploitable ip

Configuring Ubuntu Server running suricata and splunk:

I have named it SOC ANALYST, set 1 adapter of the this machine to the security-lan and other in the target lan in promisc mode.





```
sujal@sujal-VirtualBox: ~ $ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.20.5  netmask 255.255.255.0  broadcast 192.168.20.255
                ether 08:00:27:6b:88:14  txqueuelen 1000  (Ethernet)
                RX packets 52  bytes 5121 (5.1 KB)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 103  bytes 11717 (11.7 KB)
                TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

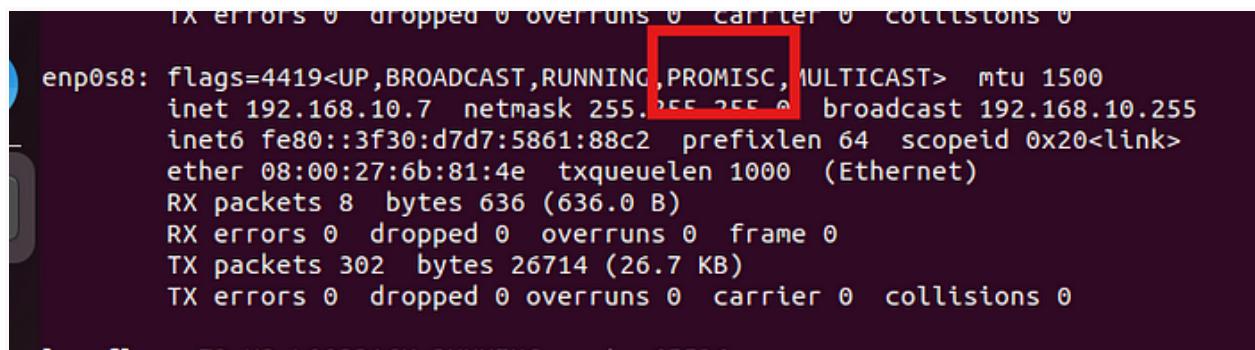
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.7  netmask 255.255.255.0  broadcast 192.168.10.255
                ether 08:00:27:6b:81:4e  txqueuelen 1000  (Ethernet)
                RX packets 2  bytes 384 (384.0 B)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 80  bytes 9343 (9.3 KB)
                TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
                loop  txqueuelen 1000  (Local Loopback)
                RX packets 188  bytes 16003 (16.0 KB)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 188  bytes 16003 (16.0 KB)
                TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

sujal@sujal-VirtualBox: ~ $
```

We need to keep the interface enp0s8 which has the ip 192.168.10.7 in promisc mode, run the below command :

```
sudo ip link set enp0s8 promisc on
```



```
rx errors 0 dropped 0 overruns 0 carrier 0 collisions 0
enp0s8: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500
inet 192.168.10.7 netmask 255.255.255.0 broadcast 192.168.10.255
inet6 fe80::3f30:d7d7:5861:88c2 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:6b:81:4e txqueuelen 1000 (Ethernet)
RX packets 8 bytes 636 (636.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 302 bytes 26714 (26.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
1: eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.10.6 netmask 255.255.255.0 broadcast 192.168.10.255
inet6 fe80::4101:27ff:fe00:214e prefixlen 64 scopeid 0x20<link>
ether 08:00:27:01:00:21 txqueuelen 1000 (Ethernet)
RX packets 10 bytes 1000 (1.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10 bytes 1000 (1.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Phew ! We are done with connecting the machines to the local network.

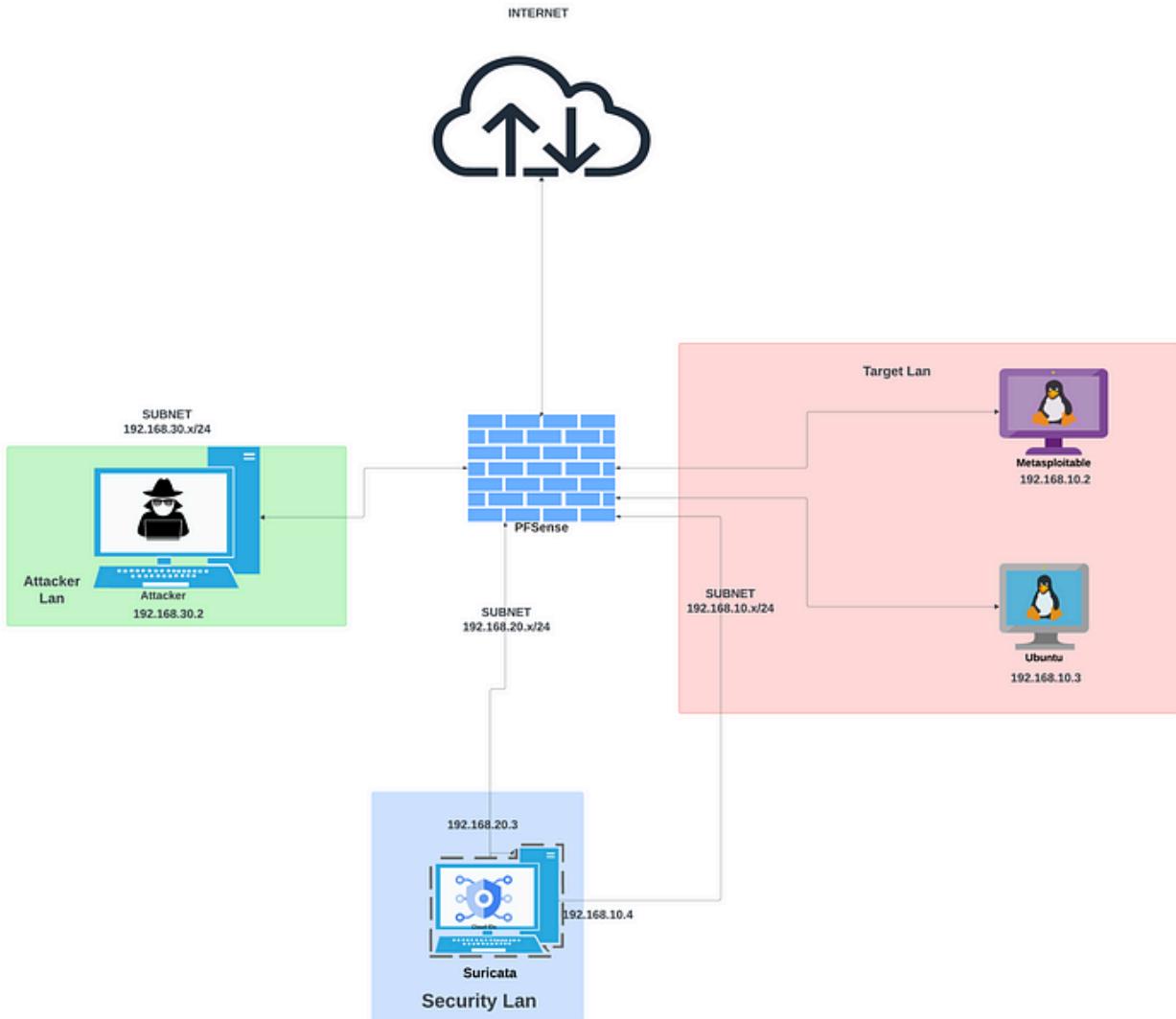
Summary:

1. Ubuntu → Lan: Target , Ip:192.168.10.5 .
2. Metasploitable → Lan:Target , Ip:192.168.10.6
3. Kali Linux → Lan:Attacker , Ip:192.168.30.2
4. SOC Analyst→ Lan:Security , Ip:192.168.20.5

5. Pfsense Wan → Lan:NAT , Ip:10.0.2.15/24
6. PFsense vtnet1 → Lan:Security , Ip:192.168.20.1
7. Pfsense vtnet2 → Lan:Target , Ip:192.168.10.1
8. Pfsense vtnet3 → Lan:Attacker, Ip:192.168.30.1

Next we have to give some of the machines the internet access by configuring firewall rules on pfsense and spin up suricata on the ubuntu machine in the security lan

I will setup the necessary firewall rules to give the internet access to certain machines and spin up suricata on SOC Analyst machine to work as an IDS.

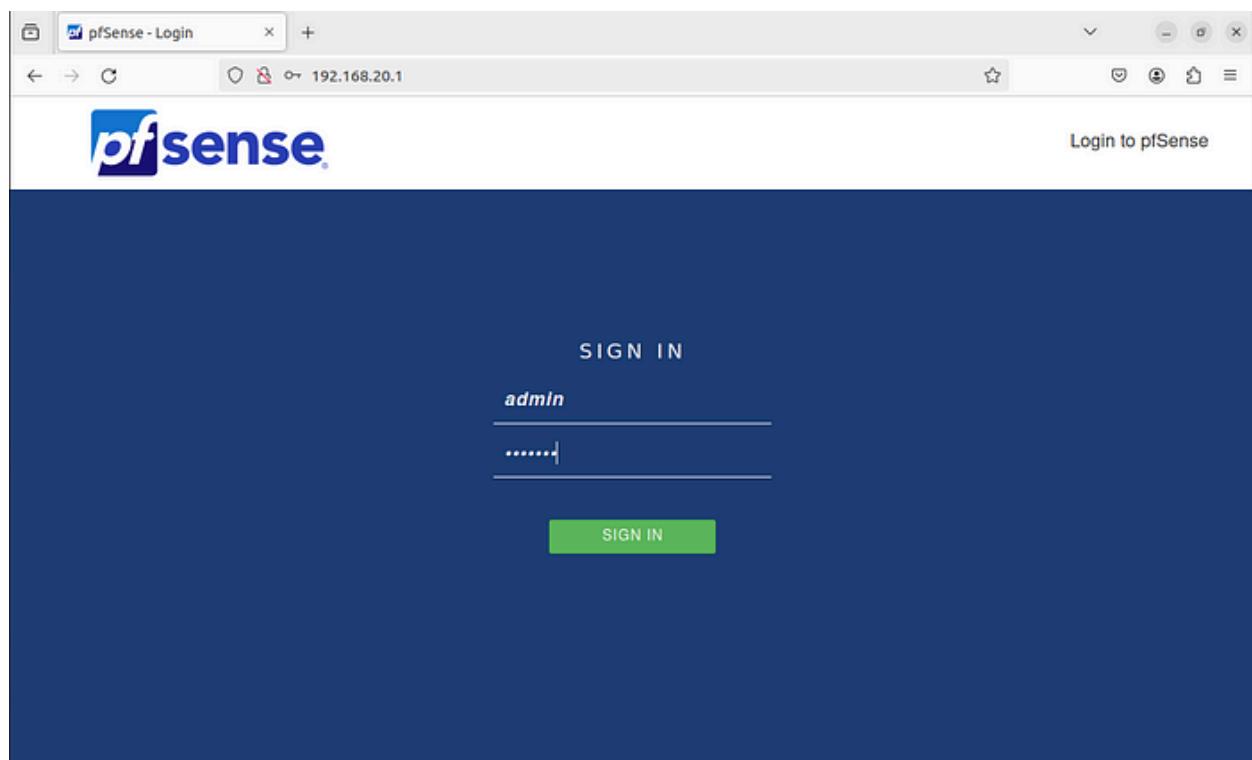


Accessing Pfsense Web GUI

First we need to access the web interface of the pfsense which is by default accessible only by the devices connected to the LAN network, devices connected to WAN / OPT1 / OPT2 are not allowed. That's the

reason, the ubuntu machine in the security lan is connected to LAN network of the pfSense.

To access the web GUI : Open Browser → Enter pfSense IP of the security LAN interface (192.168.20.1) → Username:-admin & Password:- pfSense.



pfSense.home.arpa - Wiz. x Server Not Found

192.168.20.1/wizard.php?xml=setup_wizard.xml

On this screen the general pfSense parameters will be set.

Hostname	pfSense
Name of the firewall host, without domain part.	
Examples: pfsense, firewall, edgefw	
Domain	homelab.com
Domain name for the firewall.	
Examples: home.arpa, example.com	
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.	
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	9.9.9.9
Override DNS	<input checked="" type="checkbox"/>
Allow DNS servers to be overridden by DHCP/PPP on WAN	

>> Next

I have set the hostname as default and domain to homelab.com,

primary dns : – 8.8.8.8 and secondary:9.9.9.9

Time Server Information

Please enter the time, date and time zone.

Time server hostname	2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.	
Timezone	Etc/UTC

>> Next

Set the time server to default

Screenshot of the pfSense web interface showing the configuration for the WAN interface (em0).

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	WAN
Enter a description (name) for the interface here.	
IPv4 Configuration Type	DHCP
IPv6 Configuration Type	None
MAC Address	XX:XX:XX:XX:XX:XX
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: XX:XX:XX:XX:XX or leave blank.	
MTU	1500
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.	
MSS	1460
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.	
Speed and Duplex	Default (no preference, typically autoselect)

Reserved Networks

Block private networks and loopback addresses	<input checked="" type="checkbox"/>	Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input checked="" type="checkbox"/>	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Save

Only set the above sections for the wan interface.

The two options above block private networks:- This will block any incoming packets from the RFC 1918 reserved addresses (private addresses) towards wan interface,because packets to and from the internet with source address set to private ip address is something which should not be allowed since we are using [nat](#).

Change admin credentials:

Click on the change admin password poping up at the top of the screen.

The screenshot shows the pfSense User Manager interface. The URL in the browser is 192.168.20.1/system_usermanager.php?act=edit&userid=0. The page title is "System / User Manager / Users / Edit". The navigation tabs at the top are "Users" (selected), "Groups", "Settings", and "Authentication Servers".

User Properties

Defined by	SYSTEM			
Disabled	<input type="checkbox"/> This user cannot login			
Username	admin			
Password	*****			
Full name	System Administrator User's full name, for administrative information only			
Expiration date	08/21/2024 Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY			
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.			
Group membership	<table border="1"><tr><td>Not member of</td><td>admins</td><td>Member of</td></tr></table>	Not member of	admins	Member of
Not member of	admins	Member of		

To get the details of the pfSense server go to the dashboard after saving changes. The dashboard shows the status of the pfSense firewall such as CPU type, memory usage, last configuration etc.

Assign Interface Names:-

The screenshot shows the pfSense Status/Dashboard page. At the top, there's a navigation bar with links for System, Interfaces, Firewall, Services, and VPN. A red box highlights the 'Interfaces' link. Below the navigation, there's a 'System Information' section with the following details:

Name	pfSense.hcse)
User	admin@192.168.1.1
System	KVM Guest Netgate Device ID: 0a5ae7b13702e7315e38
BIOS	Vendor: innoteck GmbH

On the right side of the dashboard, there's a sidebar with icons for WAN, LAN, OPT1, and OPT2. Below the sidebar, there's a small status bar showing 'CPU: 0% | RAM: 0% | Swap: 0%'.

The screenshot shows the pfSense Interfaces/Interface Assignments page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation, the title is 'Interfaces / Interface Assignments'. There are tabs for Interface Assignments, Interface Groups, Wireless, VLANs, QinQs, PPPs, GREs, GIFs, Bridges, and LAGGs. The 'Interface Assignments' tab is selected and highlighted with a red underline.

The main content area displays a table of network interfaces and their assigned ports:

Interface	Network port
WAN	em0 (08:00:27:be:bc:22)
LAN	vtnet0 (08:00:27:54:21:65)
OPT1	vtnet1 (08:00:27:a3:9f:70)
OPT2	vtnet2 (08:00:27:8d:d6:6f)

Each row in the table has a 'Delete' button to its right. At the bottom left, there's a blue 'Save' button. A note at the bottom of the table states: 'Interfaces that are configured as members of a lagg(4) interface will not be shown.'

Lets change the name of the LAN interface

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	Security Lan Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	XX:XX:XX:XX:XX:XX This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx or leave blank.
MTU	1500 If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	1460 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

I have only changed the name of the Interface to security lan for ease, every other configuration such as ipv4 address, dhcp has been configured at the beginning of setting up pfSense, change the name of other interfaces to their respective LAN name. Uncheck the last two options

Reserved Networks

Block private networks and loopback addresses	<input type="checkbox"/>	Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input type="checkbox"/>	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

This is a LAN interface so traffic from private ip addresses towards this interfaces should be allowed. Once done click Save and then click Apply changes.

Interface	Network port
WAN	em0 (08:00:27:be:bc:22)
SecurityLan	vtnet0 (08:00:27:54:21:65)
TargetLan	vtnet1 (08:00:27:a3:9f:70)
AttackerLan	vtnet2 (08:00:27:8d:d6:6f)

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

Adding firewall rules through GUI

Click Firewall → Rules → Interface → Add

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾

Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs

Interfaces / Interface Assignment

Interface Assignments Interface Groups

Interface Network

WAN em0 (08:00:27:be:bc:22)

SecurityLan vtnet0 (08:00:27:54:21:65)

Firewall / Rules / WAN

Floating WAN SECURITYLAN TARGETLAN ATTACKERLAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
0/0 B	*	Reserved	*	*	*	*	*		Block bogon networks	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Up Add Down Add Delete Toggle Copy Save Separator

Before adding rules let us first understand the default rules of the pfSense firewall:

1. Any requests made from outside the LAN to our internal network is blocked, this is ingress filtering. pfSense will block all the incoming requests towards our network by default.
2. Any requests made from our internal network (that is the requests made from our LAN network (renamed to security lan) to the internet will be allowed and the corresponding responses into the lan will be allowed as well, because pfSense runs as a stateful firewall which keeps track of the states of network connections made from our network, this is egress filtering i.e filtering outgoing packets.
3. Any other requests to/from our OPT1 and OPT2 LAN are blocked by default until any explicit rule is configured to allow the outgoing traffic from these LAN's.
4. Learn more about pfSense filtering through [here](#).

I will add a rule to allow connections made from our security-lan to destination port listening on port 443.

The screenshot shows a web-based configuration interface for a pfSense firewall. The URL in the address bar is `192.168.20.1/firewall_rules_edit.php?if=lan&after=-1`. The main title is "Edit Firewall Rule".

Action: Pass (selected)

Disabled: Disable this rule

Interface: SECURITYLAN

Address Family: IPv4

Protocol: TCP

Source:

- Source:** Invert match, Any, Source Address /
- Display Advanced:** (button)
- A note: "The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any."

Source

Source Invert match SECURITYLAN subnets Source Address /

Source Port Range (other) From Custom (other) To Custom
Specify the source port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Destination

Destination Invert match Any Destination Address /

Destination Port Range HTTPS (443) From Custom HTTPS (443) To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

The description below at each setting, is enough to understand what each setting would help us to achieve.

Firewall / Rules / SECURITYLAN											
Floating WAN SECURITYLAN TARGETLAN ATTACKERLAN											
Rules (Drag to Change Order)											
#	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3/2.63 Mib	*	*	*	SECURITYLAN Address	80	*	*		Anti-Lockout Rule	 
<input type="checkbox"/>	✓ 2/12 KiB	IPv4 TCP	SECURITYLAN subnets	*	*	80 (HTTP)	*	none			 
<input type="checkbox"/>	✓ 21/2.59 Mib	IPv4 TCP	SECURITYLAN subnets	*	*	443 (HTTPS)	*	none			 
<input type="checkbox"/>	✓ 7/118 KiB	IPv4 TCP/ UDP	SECURITYLAN subnets	*	*	53 (DNS)	*	none			 

 Add  Add  Delete  Toggle  Copy  Save  Separator

Lets understand the above rules in short:

Rule 1: This rule is by default and it allows us to access the web interface of the pfSense.

Rule 2: This rule will allow http request from our security-lan from any port to any destination listening on port 80.

Rule 3: This rule will allow https connections initiated from our security lan to any destination listening on port 443.

Rule 4: This rule will allow any dns queries made from our security lan to any destination listening on port53 for dns queries.

We need to set the name servers in etc/resolv.conf in the machines who needs to surf the internet through browser, open the [/etc/resolv.conf](#) file.

```
sudo nano /etc/resolv.conf
```

and then add the nameserver 8.8.8.8 at the bottom of the file, then save your file.

```
GNU nano 6.2                                     /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search home.arpa
nameserver 8.8.8.8
```

Now let us try to reach the internet through our browser from our
ubuntu machine.

pfSense.home.arpa - Fire × goku vs vegeta - Google × +

C https://www.google.com/search?channel=fs&client=ubuntu-sn&q=goku+vs+vegeta ☆

Google goku vs vegeta × | 🔍

All Images Videos Shopping News Maps Books More Tools

Full fight Who would win Manga Photo Game Drawing Stats Video download GIF

Videos : See results about

Goku and Vegeta's FINAL BATTLE

YouTube · SeeReax 45.42 26 Feb 2024

A Hot, Unbound Dragon Ball Z episode 30)

That's great ! It gave us the results.

Lets determine the traffic flows

Traffic rules for Inter-Lan communication:

1. Security Lan:- Internet access for outgoing allowed, traffic from attacker-lan is blocked and traffic from target lan (except for certain traffic such splunk forwarders to send data to any siem tool for data ingestion if configured in future) to security-lan is blocked.

2. Target Lan: Traffic from security-lan and attacker lan allowed to the target lan, traffic from target-lan to attacker lan should be allowed, traffic from target-lan to the internet is allowed.
3. Attacker-Lan: Traffic to internet is allowed (this is necessary to install tools and stuff).
4. WAN:- All the incoming traffic from the internet should be blocked by default, if certain traffic is necessary will be allowed based on requirements.

I hope you can configure the above rules, I have put up the screenshots for every firewall rule configured on each interface with their description:

Security-Lan:

Floating	WAN	SECURITYLAN	TARGETLAN	ATTACKERLAN	Rules (Drag to Change Order)							
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	✓ 0/3.72 MiB	*	*	*	SECURITYLAN Address	80	*	*		Anti-Lockout Rule		
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	SECURITYLAN subnets	*	TARGETLAN subnets	*	*	*	none	all the traffic towards target-lan is allowed		
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	ATTACKERLAN subnets	*	SECURITYLAN subnets	*	*	*	none	All the traffic from attacker lan is blocked		
<input type="checkbox"/>	✓ 0/21 KiB	IPv4 TCP	SECURITYLAN subnets	*	*	80 (HTTP)	*	*	none	http traffic allowed to the Internet		
<input type="checkbox"/>	✓ 0/168.54 MiB	IPv4 TCP	SECURITYLAN subnets	*	*	443 (HTTPS)	*	*	none	https traffic allowed to the Internet		
<input type="checkbox"/>	✓ 3/283 KiB	IPv4 TCP/UDP	SECURITYLAN subnets	*	*	53 (DNS)	*	*	none	Dns queries allowed to the Internet		
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	TARGETLAN subnets	*	SECURITYLAN subnets	*	*	*	none	all the traffic from target lan is blocked		

Add Add Delete Toggle Copy Save Separator

Target-Lan

Floating	WAN	SECURITYLAN	TARGETLAN	ATTACKERLAN	Rules (Drag to Change Order)							
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	✗ 0/0 B	IPv4 TCP	*	*	TARGETLAN address	80 (HTTP)	*	*	none	access to the pfsense portal is locked on this address		
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	192.168.10.6	*	WAN address	*	*	*	none	all the traffic from metasploitable is blocked to the internet		
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	TARGETLAN subnets	*	ATTACKERLAN subnets	*	*	*	none	all the traffic towards attacker lan is allowed		
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	ATTACKERLAN subnets	*	TARGETLAN subnets	*	*	*	none	All the traffic from attacker lan is allowed		
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	SECURITYLAN subnets	*	TARGETLAN subnets	*	*	*	none	All the traffic from security-lan is allowed		
<input type="checkbox"/>	✓ 0/1.64 MiB	IPv4 TCP/UDP	TARGETLAN subnets	*	*	53 (DNS)	*	*	none	Dns queries allowed to the internet		
<input type="checkbox"/>	✓ 0/14.33 MiB	IPv4 TCP	TARGETLAN subnets	*	*	443 (HTTPS)	*	*	none	https traffic allowed to the internet		
<input type="checkbox"/>	✓ 0/68 KiB	IPv4 TCP	TARGETLAN subnets	*	*	80 (HTTP)	*	*	none	http traffic allowed to the internet		

Add Add Delete Toggle Copy Save Separator

Attacker-lan:

Floating	WAN	SECURITYLAN	TARGETLAN	ATTACKERLAN				
Rules (Drag to Change Order)								
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue
<input type="checkbox"/>	X 0/2 KIB	IPv4 TCP	*	*	ATTACKERLAN address	80 (HTTP)	*	none
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	TARGETLAN subnets	*	ATTACKERLAN subnets	*	*	none
<input type="checkbox"/>	✓ 0/336 B	IPv4 *	ATTACKERLAN subnets	*	TARGETLAN subnets	*	*	none
<input type="checkbox"/>	✓ 0/76 KIB	IPv4 TCP/ UDP	ATTACKERLAN subnets	*	*	53 (DNS)	*	none
<input type="checkbox"/>	✓ 0/216 KIB	IPv4 TCP	ATTACKERLAN subnets	*	*	80 (HTTP)	*	none
<input type="checkbox"/>	✓ 0/14 KIB	IPv4 TCP	ATTACKERLAN subnets	*	*	443 (HTTPS)	*	none

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

Do test the firewall rules, I have tested the rules and all worked according to the way I expected, if there are any mistakes or you face any issues you can reach me out at my [linkedIn](#).

Setting up suricata:

Open up your SOC Analyst Machine and run:

```
sudo apt-get update && sudo apt-get install suricata
```

Once suricata is installed first we need to check few things:

1. The other interface in the target lan which we are going to monitor is in promiscous mode.
2. No communication takes place on that interface.

To put the interface into promisc mode run :

```
sudo ifconfig [interface] promisc
```

```
sujal@sujal-VirtualBox:~$ sudo ifconfig enp0s8 promisc
sujal@sujal-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.20.5 netmask 255.255.255.0 broadcast 192.168.20.255
        inet6 fe80::9f7d:c9f5:ff78:ec58 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:6f:18:db txqueuelen 1000 (Ethernet)
            RX packets 209774 bytes 229060997 (229.0 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 72782 bytes 8773658 (8.7 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500
        inet 192.168.10.8 netmask 255.255.255.0 broadcast 192.168.10.255
        inet6 fe80::7778:321b:993b:be12 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:6b:81:4e txqueuelen 1000 (Ethernet)
            RX packets 9191 bytes 1157442 (1.1 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 18553 bytes 1593205 (1.5 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 42848 bytes 3471335 (3.4 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 42848 bytes 3471335 (3.4 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

To stop communication on promiscous interface:

we will flush the ip it got from dhcp and block all the communications using iptables rule, run:

```
sudo ip addr flush dev [interface]  
sudo iptables -A INPUT -i [interface] -j DROP  
sudo iptables -A OUTPUT -o [interface] -j DROP  
sudo iptables-save
```

```
sujal@sujal-VirtualBox:~$ sudo ip addr flush dev enp0s8  
sujal@sujal-VirtualBox:~$ sudo iptables -A INPUT -i enp0s8 -j DROP  
sujal@sujal-VirtualBox:~$ sudo iptables -A OUTPUT -o enp0s8 -j DROP  
sujal@sujal-VirtualBox:~$ iptables-save  
iptables-save v1.8.7 (nf_tables): Could not fetch rule set generation id: Permission denied (you must be root)  
  
sujal@sujal-VirtualBox:~$ sudo iptables-save  
# Generated by iptables-save v1.8.7 on Sun Jul 21 20:12:07 2024  
*filter  
:INPUT ACCEPT [0:0]  
:FORWARD ACCEPT [0:0]  
:OUTPUT ACCEPT [0:0]  
-A INPUT -i enp0s8 -j DROP  
-A INPUT -i enp0s8 -j DROP  
-A OUTPUT -o enp0s8 -j DROP  
-A OUTPUT -o enp0s8 -j DROP  
COMMIT  
# Completed on Sun Jul 21 20:12:07 2024  
sujal@sujal-VirtualBox:~$ █
```

```
sujal@sujal-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
DROP       all  --  anywhere        anywhere
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
DROP       all  --  anywhere        anywhere
sujal@sujal-VirtualBox:~$
```

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet6 fe80::7a15:5287:c1ca:8357  prefixlen 64  scopeid 0x20<link>
          ether 08:00:27:6b:81:4e  txqueuelen 1000  (Ethernet)
            RX packets 9207  bytes 1160783 (1.1 MB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 18566  bytes 1595330 (1.5 MB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Now to confirm whether we can capture traffic from target-lan from this interface, run tcpdump on the interface in promisc mode.

```
sudo tcpdump -i enp0s8
```

```
sujal@sujal-VirtualBox:~$ sudo tcpdump -i enp0s8
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
20:14:42.538854 IP6 fe80::7a15:5287%enp0s8 > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
```

Use one of the machines in target lan to communicate with other hosts or access internet.

```
sujal@sujal-VirtualBox:~$ nslookup google.com
Server:          8.8.8.8
Address:         8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.182.110
Name:   google.com
Address: 2404:6800:4007:80f::200e
```

```
sujal@sujal-VirtualBox:~$
```

Go back to your SOC Analyst machine, and see if the interface captured any traffic

```
sujal@sujal-VirtualBox:~$ sudo tcpdump -i enp0s8
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
20:14:42.538854 IP6 fe80::7a15:5287:clca:8357 > ff02::16: Hbh ICMP6, multicast listener report v2, 2 group record(s), length 48
20:15:40.114363 IP6 fe80::7a15:5287:clca:8357.mdns > ff02::fb.mdns: 0 [9q] PTR (QM)? _nfs._tcp.local. PTR (QM)? _ipp._tcp.local. PTR (QM)? _tpp._tcp.local. PTR (QM)? _ftp._tcp.local. PTR (QM)? _webdav._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _smb._tcp.local. PTR (QM)? _afpovertcp._tcp.local. (141)
20:16:04.579924 IP 192.168.10.5.35251 > dns.google.domain: 8616+ A? google.com. (28)
20:16:04.677968 IP dns.google.domain > 192.168.10.5.35251: 8616 1/0/0 A 142.250.182.110 (44)
20:16:04.679311 IP 192.168.10.5.37679 > dns.google.domain: 51759+ AAAA? google.com. (28)
20:16:04.722524 IP dns.google.domain > 192.168.10.5.37679: 51759 1/0/0 AAAA 2404:6800:4007:80f::200e (56)
20:16:09.747289 ARP, Request who-has 192.168.10.1 tell 192.168.10.5, length 28
20:16:09.747902 ARP, Reply 192.168.10.1 is-at 08:00:27:a3:9f:70 (oui Unknown), length 28
```

Yahoo! The interface can capture the traffic from the target-lan.

Testing Suricata

I would like you to clone the rules for nmap scans from this [repo](#).

Once cloned copy the path to the local.rules file and put in the

rule-files section of the suricata.yaml file

```
sudo nano /etc/suricata/suricata.yaml
```

```

GNU nano 6.2                               /etc/suricata/suricata.yaml

# When auto-config is enabled the hashmode specifies the algorithm for
# determining to which stream a given packet is to be delivered.
# This can be any valid Napatech NTPL hashmode command.
#
# The most common hashmode commands are: hash2tuple, hash2tuplesorted,
# hash5tuple, hash5tuplesorted and roundrobin.
#
# See Napatech NTPL documentation other hashmodes and details on their use.
#
# This parameter has no effect if auto-config is disabled.
#
hashmode: hash5tuplesorted

## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /etc/suricata/rules

rule-files:
# - suricata.rules
- /home/sujal/opnsense-suricata-nmaps/local.rules

##
## Auxiliary configuration files.
##
classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
# threshold-file: /etc/suricata/threshold.config

##
## Include other configs
##

# Includes: Files included here will be handled as if they were in-lined
# in this configuration file. Files with relative pathnames will be
# searched for in the same directory as this configuration file. You may
# use absolute pathnames too.

```

Save it and then spin up suricata on the interface enp0s8.

```
sudo suricata -c /etc/suricata/suricata.yaml -i enp0s8 -k none -l .
```

The above command runs suricata with the specified configuration file i.e suricata.yaml (which is made by default on installation) and the

interface (enp0s8) will monitor -k none does the checksum validation and -l . sets the logging to the current directory.

```
sujal@sujal-VirtualBox:~$ sudo suricata -c /etc/suricata/suricata.yaml -i enp0s8 -k none -l .
21/7/2024 -- 21:08:42 - <Notice> - This is Suricata version 6.0.4 RELEASE running in SYSTEM mode
21/7/2024 -- 21:08:42 - <Notice> - all 2 packet processing threads, 4 management threads initialized, engine started.
```

Suricata is monitoring, run nmap from kali linux and then open fast.log to see if it detected any nmap scanning techniques.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.10.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-21 16:24 EDT
Nmap scan report for 192.168.10.5
Host is up (0.0026s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

```
sujal@sujal-VirtualBox:~$ cat fast.log
07/21/2024-21:09:01:858487 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:111
07/21/2024-21:09:01:858487 [**] [1:3400001:1] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:139
07/21/2024-21:09:01:868074 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:1114
07/21/2024-21:09:01:868084 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:2020
07/21/2024-21:09:01:868635 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:301
07/21/2024-21:09:01:873465 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:3404
07/21/2024-21:09:01:873435 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:3527
07/21/2024-21:09:01:873473 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:2068
07/21/2024-21:09:01:878350 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:9593
07/21/2024-21:09:01:878642 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:1123
07/21/2024-21:09:01:878642 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:8193
07/21/2024-21:09:01:879689 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:9666
07/21/2024-21:09:01:879784 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:48080
07/21/2024-21:09:01:891191 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:34572
07/21/2024-21:09:01:893190 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:2602
07/21/2024-21:09:01:893209 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:70
07/21/2024-21:09:01:893210 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:3007
07/21/2024-21:09:01:893950 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:10025
07/21/2024-21:09:01:893288 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:555
07/21/2024-21:09:01:893939 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:9575
07/21/2024-21:09:01:897839 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
TCP] 192.168.30.2:40977 -> 192.168.10.5:7512
07/21/2024-21:09:01:898266 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {
```

Open the fast.log file, it indeed logged nmap SYN scanning, hence our suricata server is running as an IDS

I will be demonstrating on how to setup splunk server on the SOC

Analyst machine and data ingestion into the splunk indexer. To learn more about splunk check [here](#).

Installing Splunk

Install splunk from [splunk website](#), after installation run the below command in the directory which the splunk installation file was saved.

```
sudo tar xvzf [splunk tar file] -C /opt/
```

```
root@sujal-VirtualBox:/opt# tar xvcf /home/sujal/Downloads/splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz -C /opt/
```

Then start the splunk server with the below command, it will ask for setting admin account and password on initial start of the server.

```
cd /opt/splunk/bin && sudo ./splunk start --accept-license
```

```
root@sujal-VirtualBox:/opt/splunk/bin# sudo ./splunk start --accept-license
This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise,
you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: dataadmin
Password must contain at least:
    * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password: 
```

Once done, it will show the uri on which the splunk gui can be accessed, login with the username and password you configured above.

The Splunk web interface is at <http://sujal-VirtualBox:8000>

The screenshot shows the Splunk Enterprise dashboard. At the top, it says "Hello, Administrator". Below this, there's a "Quick links" section with links to "Dashboard", "Recently viewed", "Created by you", and "Shared with you". The main area is titled "Common tasks" and contains six cards: "Add data" (Add data from a variety of common sources), "Search your data" (Turn data into doing with Splunk search), "Visualize your data" (Create dashboards that work for your data), "Add team members" (Add your team members to Splunk platform), "Manage permissions" (Control who has access with roles), and "Configure mobile devices" (Login or manage mobile devices using Splunk Secure Gateway). Below this, there's a "Learning and resources" section with "Product tours" (New to Splunk? Take a tour to help you on) and "Learn more with Splunk Docs" (Deploy, manage, and use Splunk software).

The installation of splunk is successful

Ingesting data to Splunk

Click Settings → Add Data → [Method]

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Q Find

Hello, Administrator

Apps Manage

Search apps by name...

Quick links Dashboard Recently

Common tasks

- Add data** Add data from a variety of common sources.
- Visualize your data** Create dashboards that work for you.
- Manage permissions** Control who has access with roles.

Add Data

Explore Data

Monitoring Console

KNOWLEDGE

- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

DATA

- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Virtual indexes
- Source types
- Ingest actions

DISTRIBUTED ENVIRONMENT

- Indexer clustering
- Forwarder management
- Federated search
- Distributed search

SYSTEM

- Server settings
- Server controls
- Health report manager
- RapidDiag
- Instrumentation
- Licensing
- Workload management
- Mobile settings

USERS AND AUTHENTICATION

- Roles
- Users
- Tokens
- Password management
- Authentication methods

Find more apps

Learning and resources

Product tour Learn more with Splunk Docs

Thank You for Download! > Add Data | Splunk 9.2.2 +

sujal-virtualbox:8000/en-US/manager/search/adddata

Cloud computing Networking Operating System Security

Get your cloud computing data in to the Splunk platform. Get your networking data in to the Splunk platform. Get your operating system data in to the Splunk platform. Get your security data in to the Splunk platform.

10 data sources 2 data sources 1 data source 3 data sources

4 data sources in total

Or get data in with the following methods

Upload files from my computer Local log files Local structured files (e.g. CSV) Tutorial for adding data!

Monitor files and ports on this Splunk platform instance Files - HTTP - WMI - TCP/UDP - Scripts Modular inputs for external data sources

Forward data from a Splunk forwarder Files - TCP/UDP - Scripts

There are guides on the data sources and method types. To learn more about ingestion in splunk check this [documentaion](#).

I will be demonstrating Monitor and Forward method, for the demonstration purpose for monitoring method I will be monitoring the log file generated by suricata on the machine running splunk. I created a directory suricata in my user directory, then spinned up suricata to log the alerts in that directory.

```
sujal@sujal-VirtualBox:~$ mkdir suricata
sujal@sujal-VirtualBox:~$ cd suricata/
sujal@sujal-VirtualBox:~/suricata$ ls
sujal@sujal-VirtualBox:~/suricata$ sudo suricata -c /etc/suricata/suricata.yaml
-i enp0s8 -k none -l .
[sudo] password for sujal:
Sorry, try again.
[sudo] password for sujal:
22/7/2024 -- 17:07:54 - <Notice> - This is Suricata version 6.0.4 RELEASE runnin
g in SYSTEM mode
22/7/2024 -- 17:07:54 - <Notice> - all 2 packet processing threads, 4 management
threads initialized, engine started.
```

Next spin up your kali machine and perform a SYN Scan with nmap on any one of the machine this will add the logs to the directory specified.

Select Monitoring files and directories.

The screenshot shows the Splunk Enterprise interface for adding new data sources. The top navigation bar includes 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation is a progress bar with five steps: 'Select Source' (green dot), 'Set Source Type' (white circle), 'Input Settings' (white circle), 'Review' (white circle), and 'Done' (white circle). The current step is 'Select Source'. A 'Next >' button is located at the top right of the progress bar. The main content area has a left sidebar with links to 'Files & Directories', 'HTTP Event Collector', 'TCP / UDP', 'Scripts', 'Splunk Assist Instance Identifier', 'Systemd Journald Input for Splunk', 'Logd Input for the Splunk platform', and 'Splunk Secure Gateway'. The main panel displays instructions for monitoring files and directories, including a note about selecting a directory which might cause problems if objects have different source types. It shows a 'File or Directory' input field containing '/home/sujal/suricata/fast.log' with a 'Browse' button, and two buttons for monitoring: 'Continuously Monitor' (selected) and 'Index Once'. Below these are 'Includelist' and 'Excludelist' fields. At the bottom of the main panel is a 'FAQ' section with links to common questions.

Select continuously monitor option, so that if new data is logged then splunk will index it for us to monitor simultaneously.

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add Data Set Source Type Input Settings Review Done < Back Next >

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: /home/sujal/suricata/fast.log

View Event Summary

Source type: default ▾ Save As

List ▾ Format 20 Per Page ▾ 1 2 3 4 5 6 7 8 Next >

	Time	Event
1	7/22/24 5:20:43.879 PM	07/22/2024-17:20:43.879300 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:4 2837 -> 192.168.10.5:199
2	7/22/24 5:20:43.887 PM	07/22/2024-17:20:43.887943 [**] [1:3400001:1] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:4 2837 -> 192.168.10.5:80
3	7/22/24 5:20:43.907 PM	07/22/2024-17:20:43.907763 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:4 2837 -> 192.168.10.5:1096
4	7/22/24 5:20:43.911 PM	07/22/2024-17:20:43.911852 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:4 2837 -> 192.168.10.5:1059
5	7/22/24 5:20:43.922 PM	07/22/2024-17:20:43.922916 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:4 2837 -> 192.168.10.5:3878

Review if the logs added are in the correct format.

Save Source Type

Name

Description

Category

App

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More ↗](#)

Constant value
 Regular expression on path
 Segment in path

Host field value

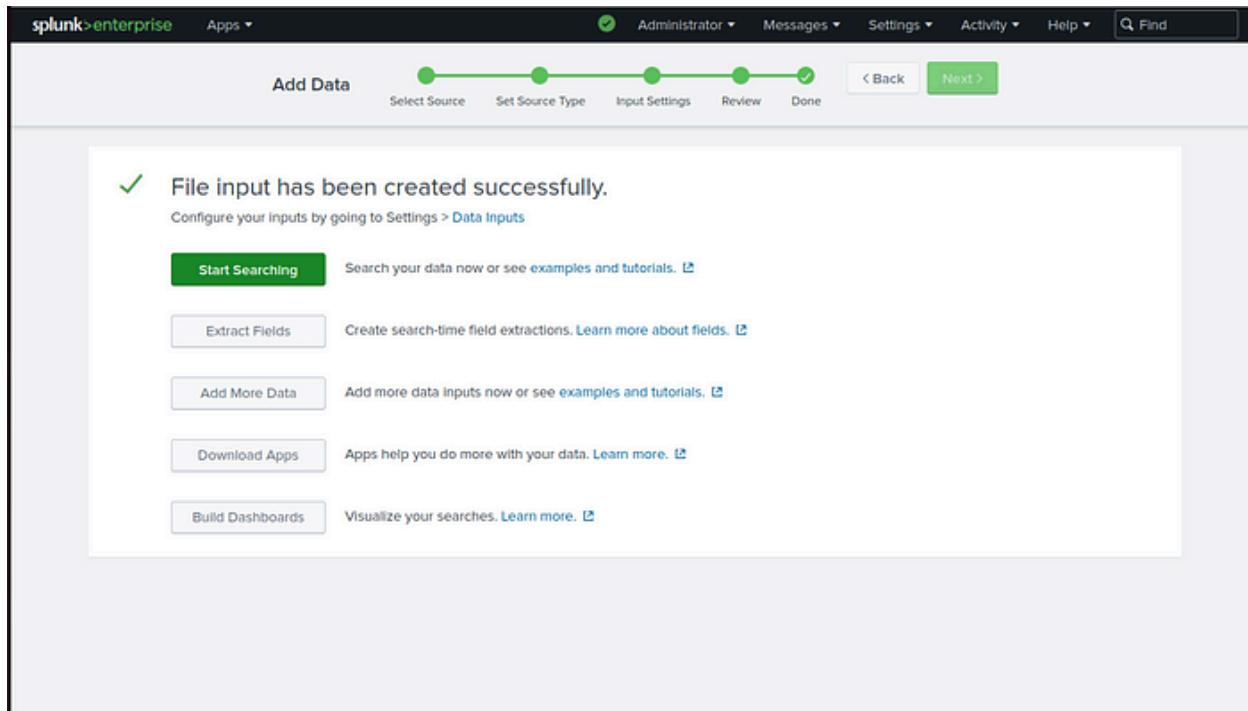
Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More ↗](#)

Index [Create a new index](#)

FAQ

- › How do indexes work?
- › How do I know when to create or use multiple indexes?

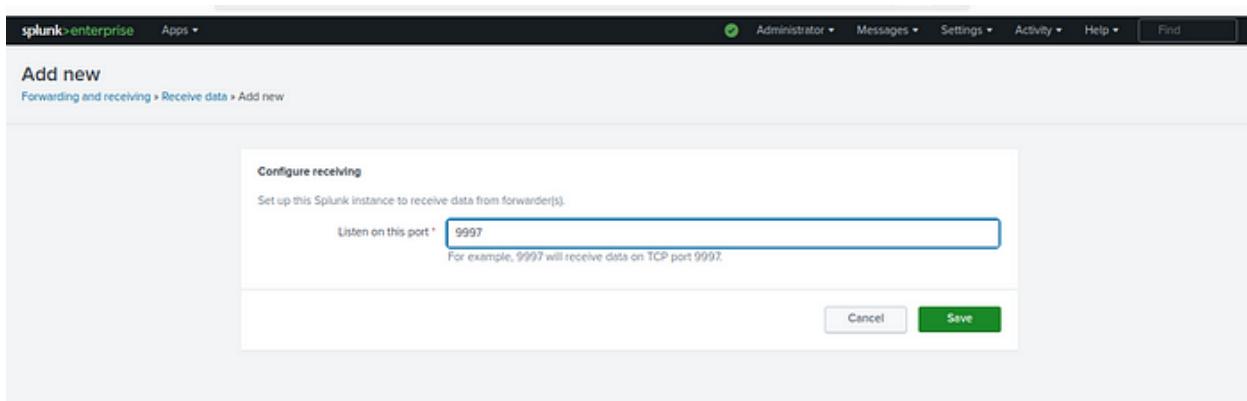


The screenshot shows the search results page in Splunk Enterprise. The search bar contains the query: 'source="/home/sujal/suricata/fast.log" host="sujal-VirtualBox" index="main" sourcetype="Suricata IDS logs"'. The results show 141 events found before 7/22/24 5:30:26.000 PM. The interface includes a timeline visualization at the top, event filtering options, and a detailed list of log entries below. The list view shows columns for Time and Event. The first few events are listed as follows:

Time	Event
07/22/24 5:20:46.060 PM	07/22/2024-17:20:46.060122 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] (TCP) 192.168.30.2:42837 -> 192.168.10.5:4444 host = sujal-VirtualBox : source = /home/sujal/suricata/fast.log : sourcetype = Suricata IDS logs
07/22/24 5:20:46.060 PM	07/22/2024-17:20:46.060122 [**] [1:3400002:2] POSSBL SCAN SHELL M-SPLOIT TCP [*] [Classification: A Network Trojan was detected] [Priority: 1] (TCP) 192.168.30.2:42837 -> 192.168.10.5:4444 host = sujal-VirtualBox : source = /home/sujal/suricata/fast.log : sourcetype = Suricata IDS logs
07/22/24 5:20:46.060 PM	07/22/2024-17:20:46.060121 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] (TCP) 192.168.30.2:42837 -> 192.168.10.5:8290 host = sujal-VirtualBox : source = /home/sujal/suricata/fast.log : sourcetype = Suricata IDS logs
07/22/24 5:20:46.060 PM	07/22/2024-17:20:46.060072 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] (TCP) 192.168.30.2:42837 -> 192.168.10.5:37 host = sujal-VirtualBox : source = /home/sujal/suricata/fast.log : sourcetype = Suricata IDS logs
07/22/24 5:20:46.051 PM	07/22/2024-17:20:46.051918 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] (TCP) 192.168.30.2:42837 -> 192.168.10.5:416 host = sujal-VirtualBox : source = /home/sujal/suricata/fast.log : sourcetype = Suricata IDS logs

Setting up Universal forwarders.

Click Settings → Forwarding and Receiving → Configure Receiving → New Receiving Port → Add port [9997 default].



I will set up a forwarder on ubuntu machine in target lan to forward the data to the splunk server in security lan. Need to add a rule to allow this traffic to security lan through pfsense.

Floating	WAN	SECURITYLAN	TARGETLAN	ATTACKERLAN				
Rules (Drag to Change Order)								
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue
<input checked="" type="checkbox"/>	0/384 KIB	*	*	*	SECURITYLAN Address	80	*	*
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	TARGETLAN subnets	*	192.168.20.5	9997	*	none

Floating	WAN	SECURITYLAN	TARGETLAN	ATTACKERLAN				
Rules (Drag to Change Order)								
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue
<input type="checkbox"/>	<input checked="" type="checkbox"/> 2/5.62 MIB	IPv4 TCP	TARGETLAN subnets	*	192.168.20.5	9997	*	none

Install the universal forwarder on the target lan machines from [here](#).

Move to the directory where splunk forwarder is downloaded and extract it to the /opt directory.

```
sudo tar xzvf [forwarder file] -C /opt/
cd /opt/splunkforwarder/bin && sudo ./splunk start --accept-license (start the forwarder)
sudo ./splunk enable boot-start (to automatically start the splunk service on boot)
sudo ./splunk add forward-server [SOC Analyst IP]:[Receiving Port] (Add a forward server)
```

Run the below command to tell the forwarder what data to send.

```
sudo ./splunk add monitor /var/log/auth.log
```

To verify if the data is being forwarded

Click Search & Reporting → Data Summary.

The screenshot shows the Splunk Enterprise interface with the 'Data Summary' window open. The window title is 'Data Summary'. Below it, there are three tabs: 'Hosts (1)', 'Sources (2)', and 'Sourcetypes (2)'. The 'Hosts (1)' tab is selected. A search bar labeled 'Filter' is present. The main table displays one host entry:

Host	Count	Last Update
sujal-VirtualBox	368	7/23/24 11:46:30.000 AM

On the left side of the interface, there is a sidebar with 'Search' and 'Analytics' tabs, and a search bar. On the right side, there is a 'Search & Reporting' panel with a 'Smart Mode' dropdown and a search bar.

Time	Event
7/22/24 5:20:46.060 PM	07/22/2024-17:20:46.060122 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:42837 -> 192.168.10.5:4444 host = sujal-VirtualBox source = /home/sujal/suricata/fast.log sourcetype = Suricata IDS logs
7/22/24 5:20:46.060 PM	07/22/2024-17:20:46.060122 [**] [1:3400020:2] POSSBL SCAN SHELL M-SPLOIT TOP [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.30.2:42837 -> 192.168.10.5:4444 host = sujal-VirtualBox source = /home/sujal/suricata/fast.log sourcetype = Suricata IDS logs
7/22/24 5:20:46.060 PM	07/22/2024-17:20:46.060121 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:42837 -> 192.168.10.5:8290 host = sujal-VirtualBox source = /home/sujal/suricata/fast.log sourcetype = Suricata IDS logs
7/22/24 5:20:46.060 PM	07/22/2024-17:20:46.060072 [**] [1:3400002:2] POSSBL PORT SCAN (NMAP -sS) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.30.2:42837 -> 192.168.10.5:37 host = sujal-VirtualBox source = /home/sujal/suricata/fast.log sourcetype = Suricata IDS logs

The forwarder is working fine and we can get the data into splunk .

Note : To save resources and avoid storage consumption delete the logs manually or through scripts .

Do add more forwarders to get all the necessary data into your splunk server for monitoring.