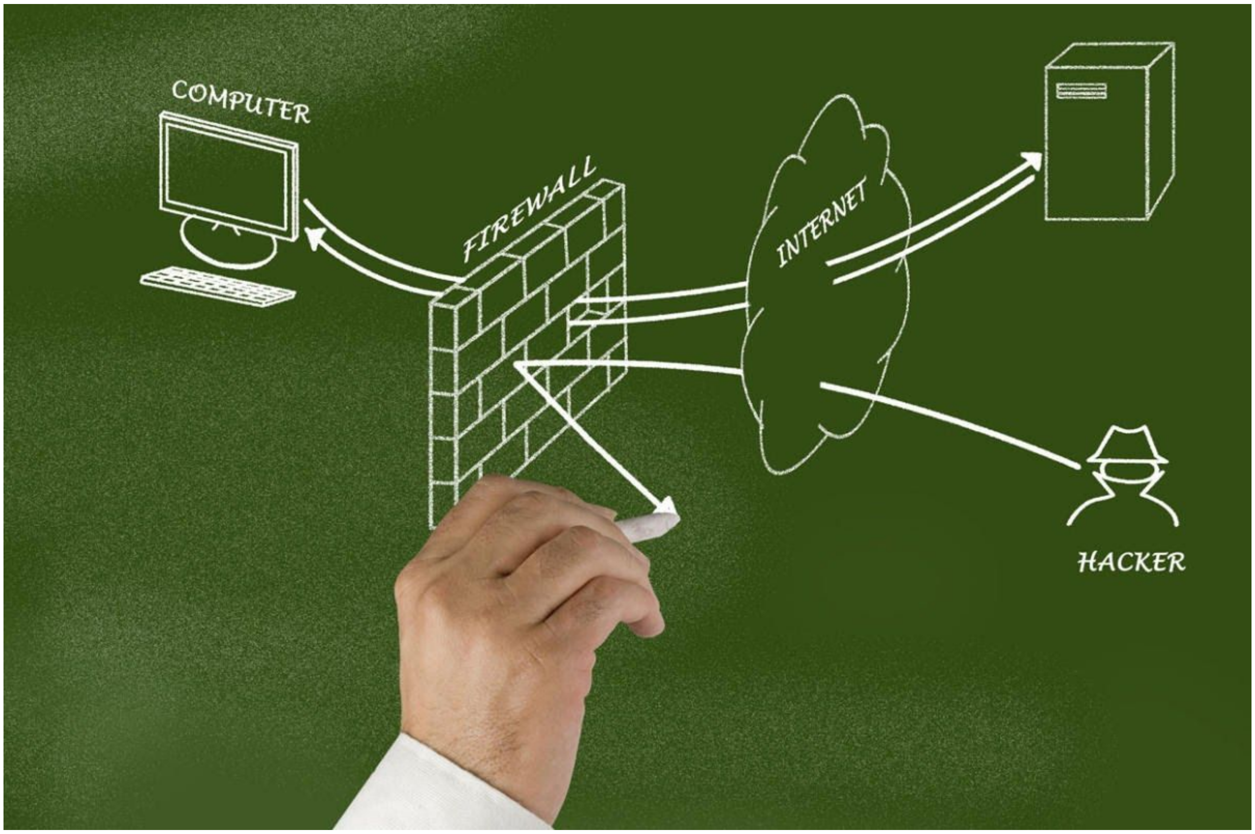
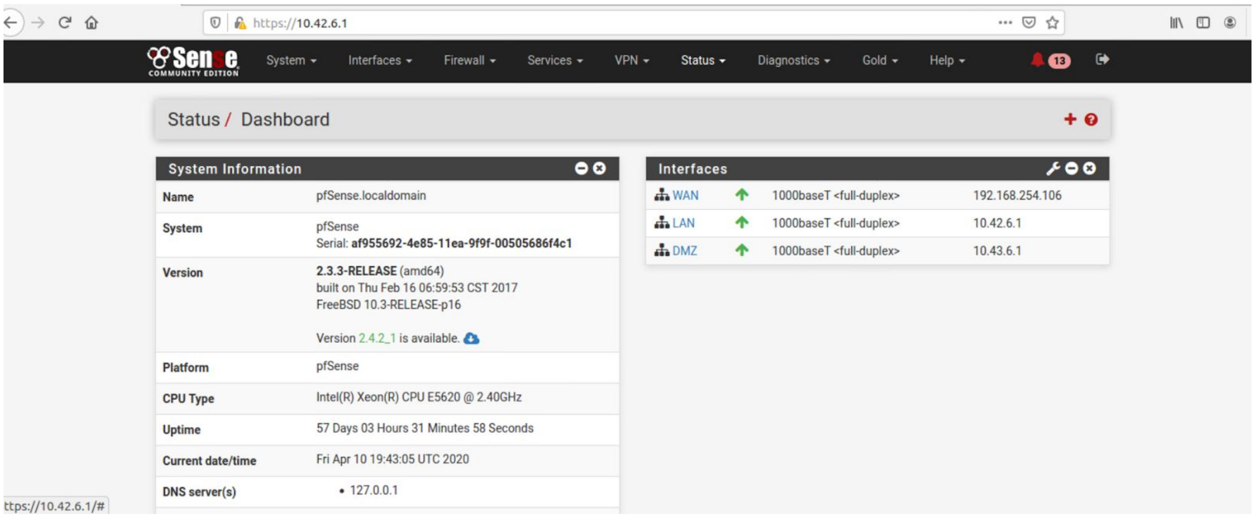
Firewall Homework



PfSense

Inside PfSense



System Information

Name	pfSense.localdomain
System	pfSense Serial: af955692-4e85-11ea-9f9f-00505686f4c1
Version	2.3.3-RELEASE (amd64) built on Thu Feb 16 06:59:53 CST 2017 FreeBSD 10.3-RELEASE-p16 Version 2.4.2_1 is available.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz
Uptime	57 Days 03 Hours 31 Minutes 58 Seconds
Current date/time	Fri Apr 10 19:43:05 UTC 2020
DNS server(s)	• 127.0.0.1

Interfaces

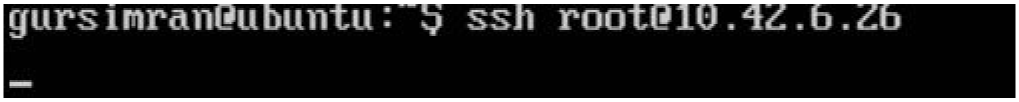
WAN	1000baseT <full-duplex>	192.168.254.106
LAN	1000baseT <full-duplex>	10.42.6.1
DMZ	1000baseT <full-duplex>	10.43.6.1

Why you might want to block ping responses in an infrastructure/internal network.

In the presence of requests with a spoofed source address, they can make a target machine send relatively large packets to another host.

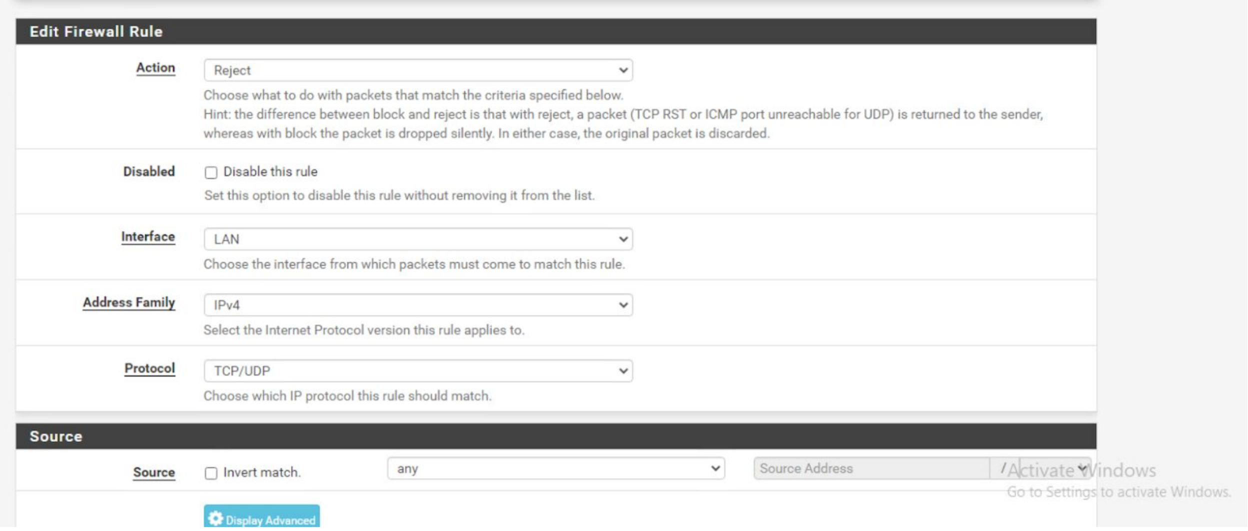
Block all SSH traffic coming into the LAN network

Result



```
gursimran@ubuntu:~$ ssh root@10.42.6.26
_
```

Steps



Edit Firewall Rule

Action — Reject

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 — LAN

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

Address Family — IPv4

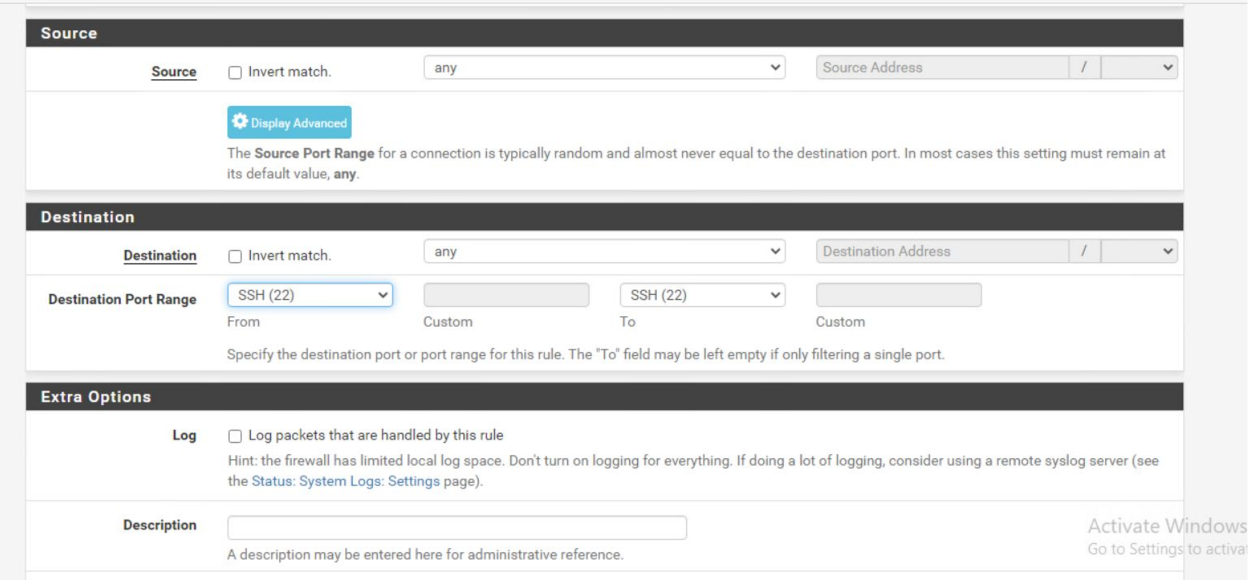
Select the Internet Protocol version this rule applies to.

Protocol — TCP/UDP

Choose which IP protocol this rule should match.

Source

Source — □ Invert match. any Source Address /



Source

Source — □ Invert match. any Source Address /

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**.

Destination

Destination — □ Invert match. any Destination Address /

Destination Port Range — From: SSH (22) Custom: — To: SSH (22) Custom: —

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

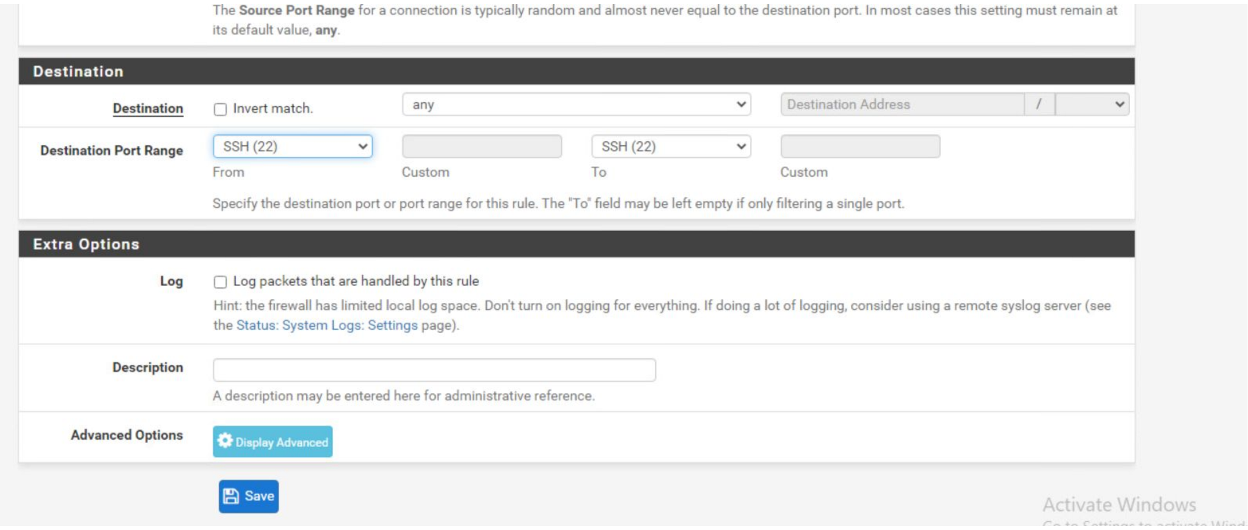
Extra Options

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 —

A description may be entered here for administrative reference.



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**.

Destination

Destination — □ Invert match. any Destination Address /

Destination Port Range — From: SSH (22) Custom: — To: SSH (22) 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 —

A description may be entered here for administrative reference.

Advanced Options

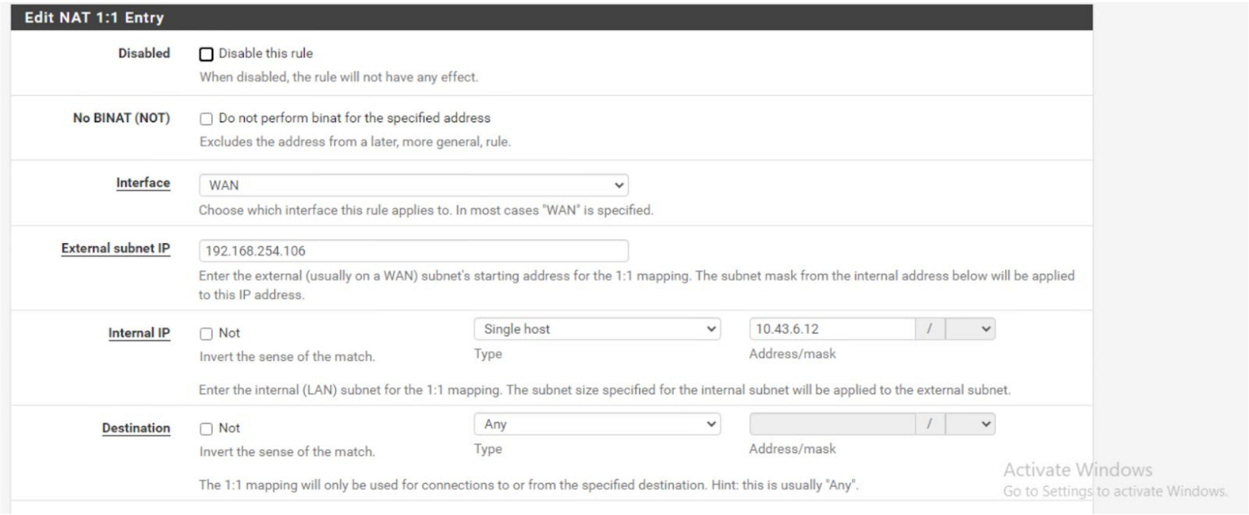
Brief summary as to how you could use logging to your advantage in a real world scenario.

From a security point of view, the purpose of a log is to act as a red flag when something bad is happening. Reviewing logs regularly could help identify malicious attacks on your system. It can be done in a robust way using log management tools.

What could be utilized to better organize and digest logs? Why are these useful?

Splunk Enterprise Security - This tool for Windows and Linux is a world leader because it combines network analysis with log management together with an excellent analysis tool.

Set up a 1:1 NAT for Web Server



Edit NAT 1:1 Entry

Disabled: □ Disable this rule
When disabled, the rule will not have any effect.

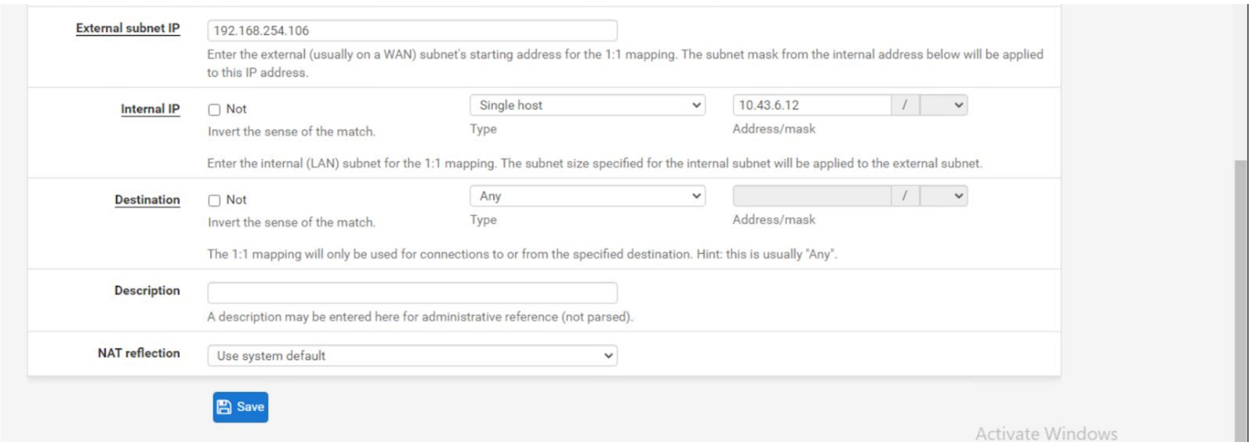
No BINAT (NOT): □ Do not perform binat for the specified address
Excludes the address from a later, more general, rule.

Interface: WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

External subnet IP: 192.168.254.106
Enter the external (usually on a WAN) subnet's starting address for the 1:1 mapping. The subnet mask from the internal address below will be applied to this IP address.

Internal IP: □ Not — Invert the sense of the match. | Type: Single host | Address/mask: 10.43.6.12 /
Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.

Destination: □ Not — Invert the sense of the match. | Type: Any | Address/mask: /
The 1:1 mapping will only be used for connections to or from the specified destination. Hint: this is usually "Any".



External subnet IP: 192.168.254.106
Enter the external (usually on a WAN) subnet's starting address for the 1:1 mapping. The subnet mask from the internal address below will be applied to this IP address.

Internal IP: □ Not — Invert the sense of the match. | Type: Single host | Address/mask: 10.43.6.12 /
Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.

Destination: □ Not — Invert the sense of the match. | Type: Any | Address/mask: /
The 1:1 mapping will only be used for connections to or from the specified destination. Hint: this is usually "Any".

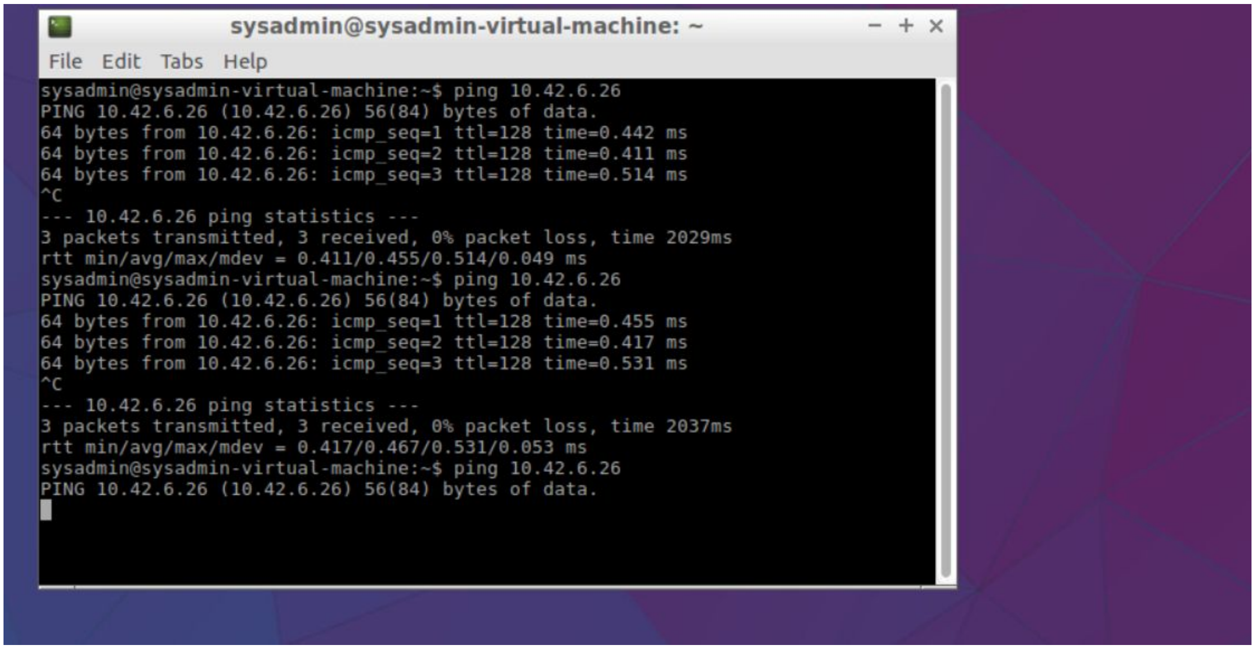
Description:
A description may be entered here for administrative reference (not parsed).

NAT reflection: Use system default

Setting up the firewall rule for NAT 1:1 from internal IP 10.43.6.12 and open to any system to connect.

Windows

Linux clients inability to ping Windows Client

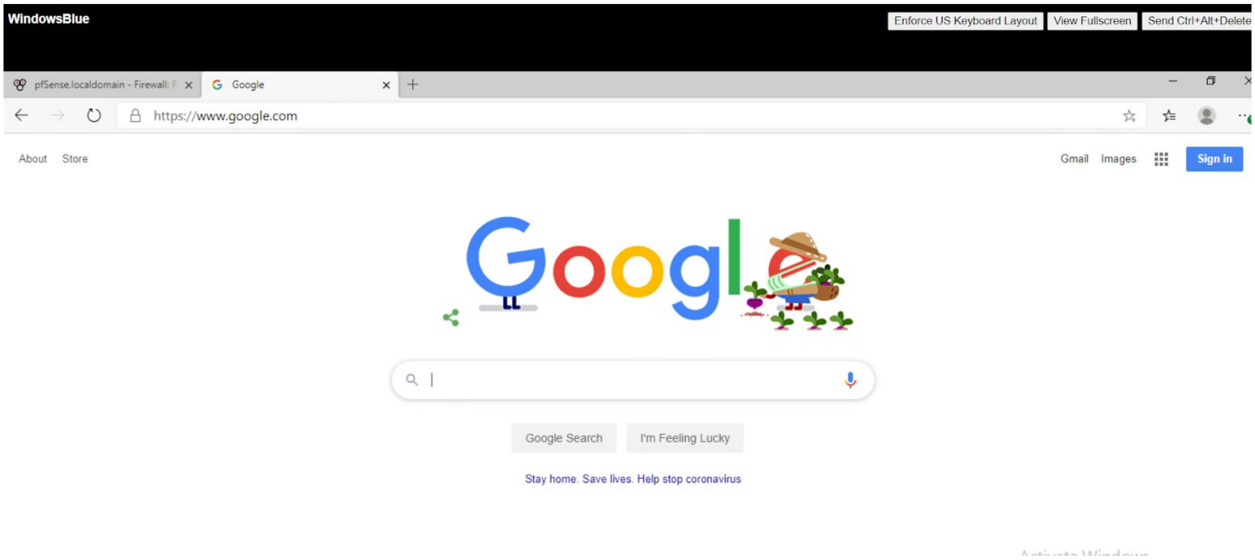


```
sysadmin@sysadmin-virtual-machine:~$ ping 10.42.6.26
PING 10.42.6.26 (10.42.6.26) 56(84) bytes of data.
64 bytes from 10.42.6.26: icmp_seq=1 ttl=128 time=0.442 ms
64 bytes from 10.42.6.26: icmp_seq=2 ttl=128 time=0.411 ms
64 bytes from 10.42.6.26: icmp_seq=3 ttl=128 time=0.514 ms
^C
--- 10.42.6.26 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 0.411/0.455/0.514/0.049 ms
sysadmin@sysadmin-virtual-machine:~$ ping 10.42.6.26
PING 10.42.6.26 (10.42.6.26) 56(84) bytes of data.
64 bytes from 10.42.6.26: icmp_seq=1 ttl=128 time=0.455 ms
64 bytes from 10.42.6.26: icmp_seq=2 ttl=128 time=0.417 ms
64 bytes from 10.42.6.26: icmp_seq=3 ttl=128 time=0.531 ms
^C
--- 10.42.6.26 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2037ms
rtt min/avg/max/mdev = 0.417/0.467/0.531/0.053 ms
sysadmin@sysadmin-virtual-machine:~$ ping 10.42.6.26
PING 10.42.6.26 (10.42.6.26) 56(84) bytes of data.
```

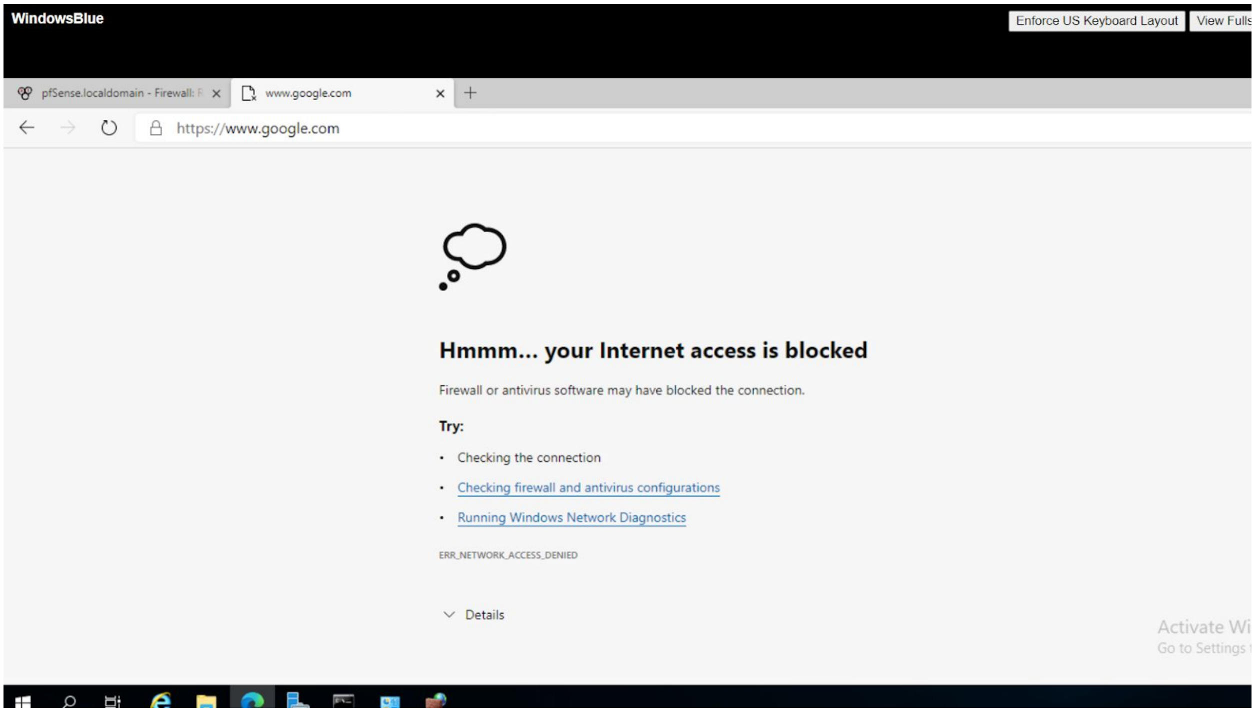
Brief description of why it could be important to block inbound connections between LAN clients.
It is important for two reasons. First to protect attack from any spoofed IP addresses and second is if one of the client is compromised, other are not directly affected by it.

Block Microsoft Edge from accessing the internet.

Before



After



Hmmm... your Internet access is blocked

Firewall or antivirus software may have blocked the connection.

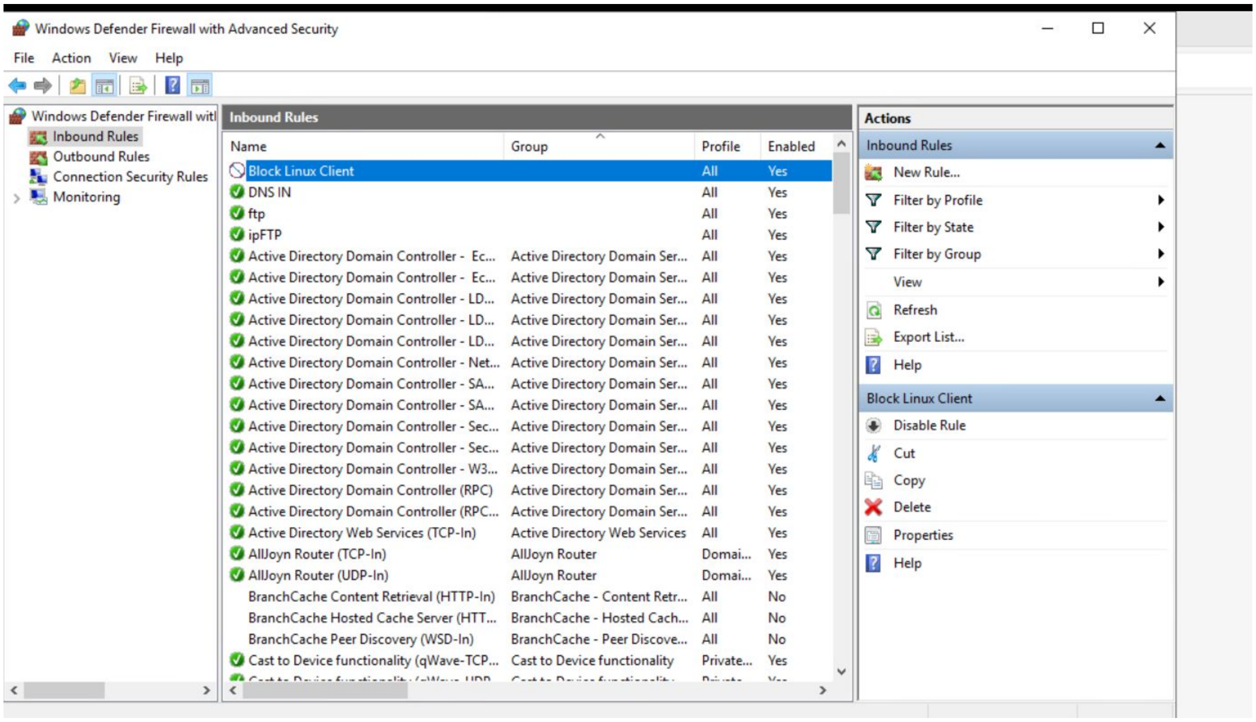
Try:

- Checking the connection
- Checking firewall and antivirus configurations
- Running Windows Network Diagnostics

ERR_NETWORK_ACCESS_DENIED

Rules

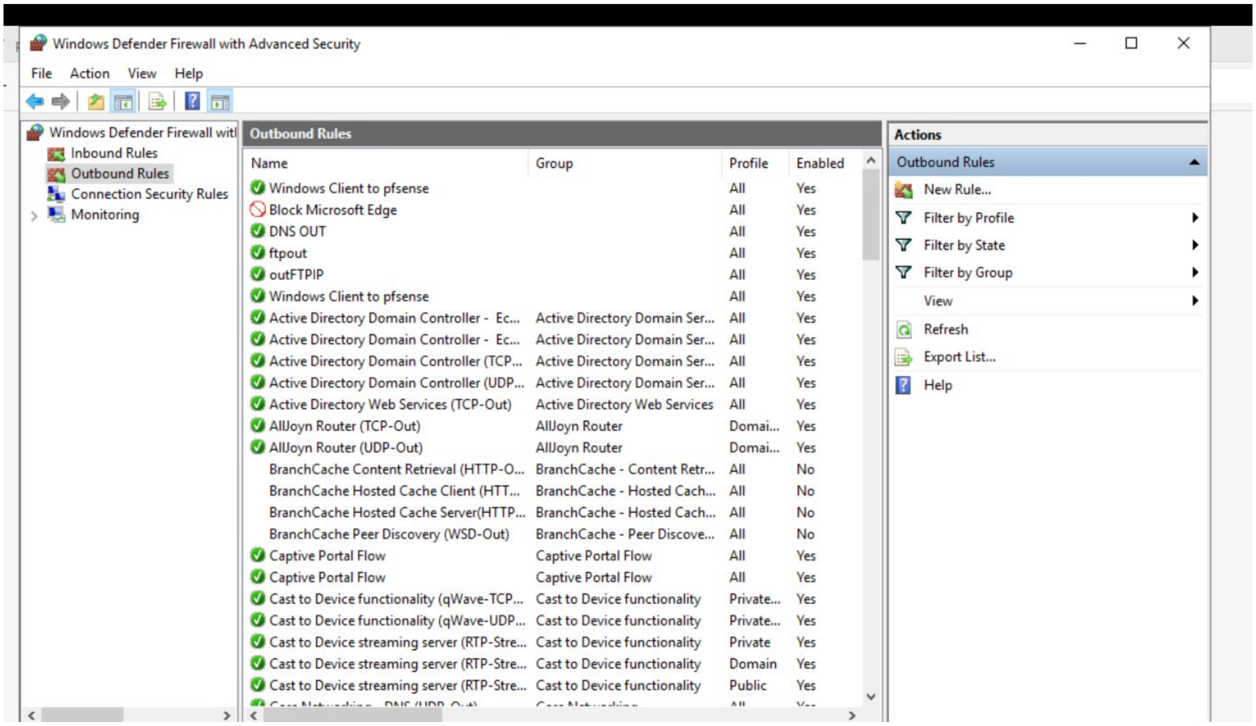
Inbound



Inbound Rules

Name	Group	Profile	Enabled
Block Linux Client		All	Yes
DNS IN		All	Yes
ftp		All	Yes
ipFTP		All	Yes
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller - Net...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller - SA...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller - SA...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller - Sec...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller - Sec...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller - W3...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller (RPC)	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller (RPC...	Active Directory Domain Ser...	All	Yes
Active Directory Web Services (TCP-In)	Active Directory Web Services	All	Yes
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes

Outbound

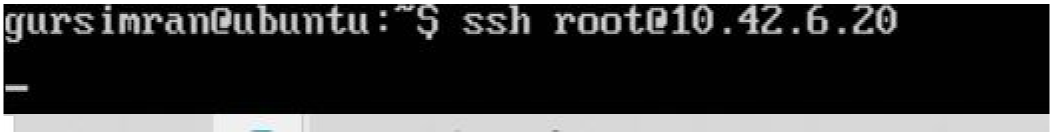


Outbound Rules

Name	Group	Profile	Enabled
Windows Client to pfsense		All	Yes
Block Microsoft Edge		All	Yes
DNS OUT		All	Yes
ftpout		All	Yes
outFTPIP		All	Yes
Windows Client to pfsense		All	Yes
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller (TCP...	Active Directory Domain Ser...	All	Yes
Active Directory Domain Controller (UDP...	Active Directory Domain Ser...	All	Yes
Active Directory Web Services (TCP-Out)	Active Directory Web Services	All	Yes
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All	No
BranchCache Hosted Cache Client (HTT...	BranchCache - Hosted Cach...	All	No
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No
Captive Portal Flow	Captive Portal Flow	All	Yes
Captive Portal Flow	Captive Portal Flow	All	Yes
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes

Linux

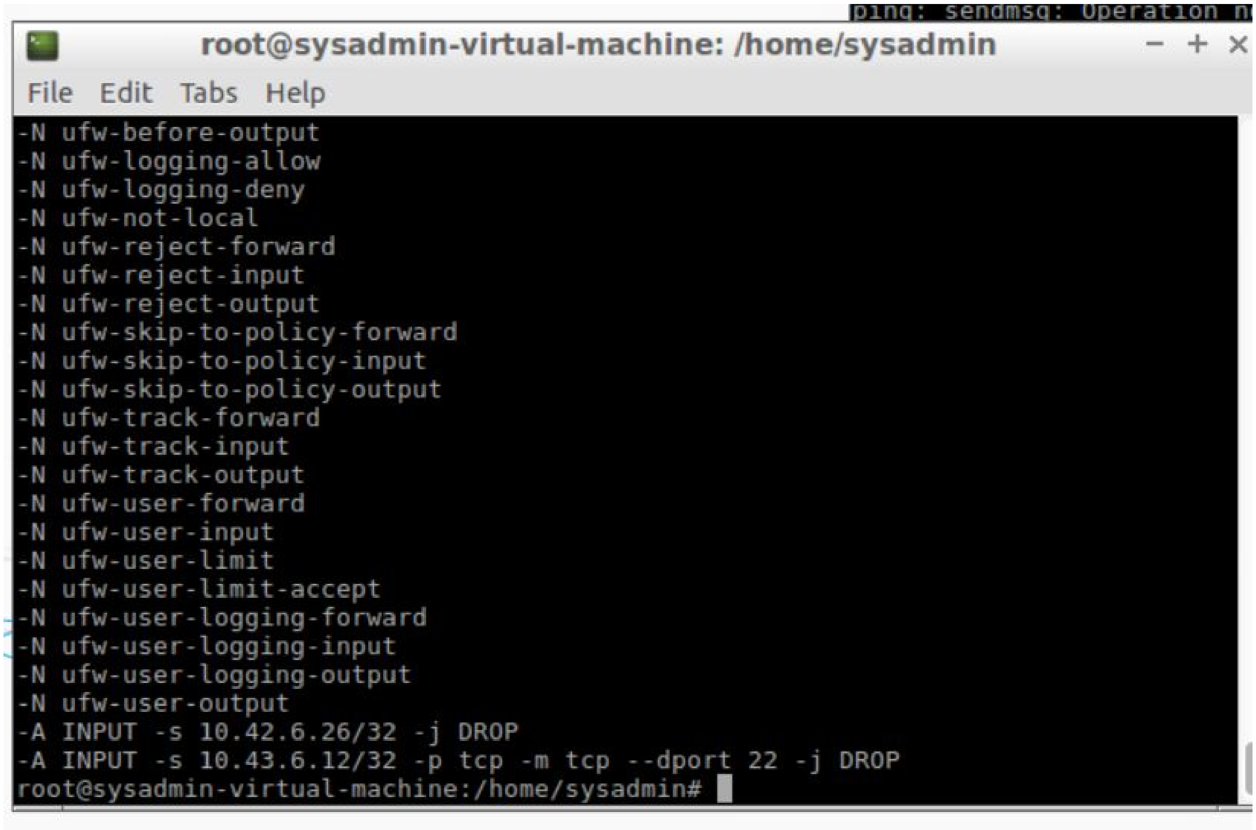
Refused SSH connection



```
gursimran@ubuntu:~$ ssh root@10.42.6.20
_
```

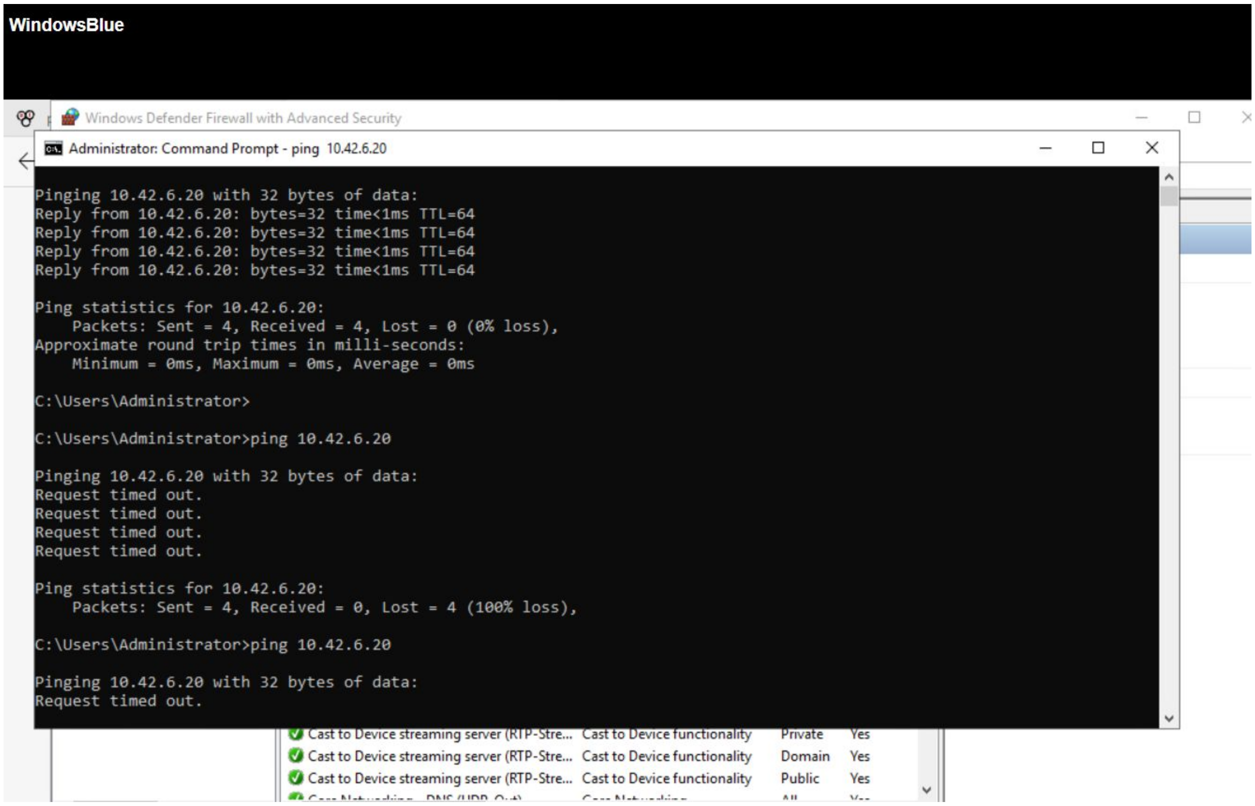
Block all incoming traffic from Windows Client to Linux Client.

Rules



```
                                                          ping: sendmsg: Operation n
-N ufw-before-output
-N ufw-logging-allow
-N ufw-logging-deny
-N ufw-not-local
-N ufw-reject-forward
-N ufw-reject-input
-N ufw-reject-output
-N ufw-skip-to-policy-forward
-N ufw-skip-to-policy-input
-N ufw-skip-to-policy-output
-N ufw-track-forward
-N ufw-track-input
-N ufw-track-output
-N ufw-user-forward
-N ufw-user-input
-N ufw-user-limit
-N ufw-user-limit-accept
-N ufw-user-logging-forward
-N ufw-user-logging-input
-N ufw-user-logging-output
-N ufw-user-output
-A INPUT -s 10.42.6.26/32 -j DROP
-A INPUT -s 10.43.6.12/32 -p tcp -m tcp --dport 22 -j DROP
root@sysadmin-virtual-machine:/home/sysadmin# 
```

Result


WindowsBlue
Windows Defender Firewall with Advanced Security
Administrator: Command Prompt - ping 10.42.6.20

```
Pinging 10.42.6.20 with 32 bytes of data:
Reply from 10.42.6.20: bytes=32 time<1ms TTL=64
Reply from 10.42.6.20: bytes=32 time<1ms TTL=64
Reply from 10.42.6.20: bytes=32 time<1ms TTL=64
Reply from 10.42.6.20: bytes=32 time<1ms TTL=64

Ping statistics for 10.42.6.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>

C:\Users\Administrator>ping 10.42.6.20

Pinging 10.42.6.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.42.6.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 10.42.6.20

Pinging 10.42.6.20 with 32 bytes of data:
Request timed out.
```

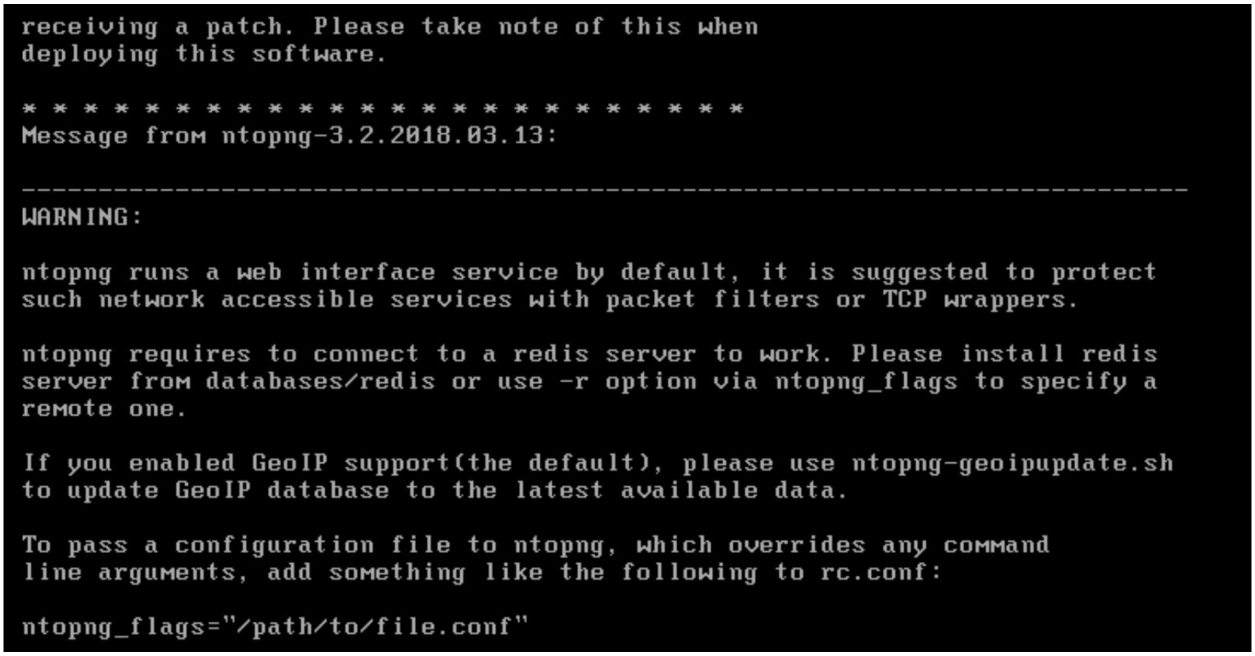
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes

Explain the importance of blocking incoming and outgoing traffic. What possible cases would require you to block either?

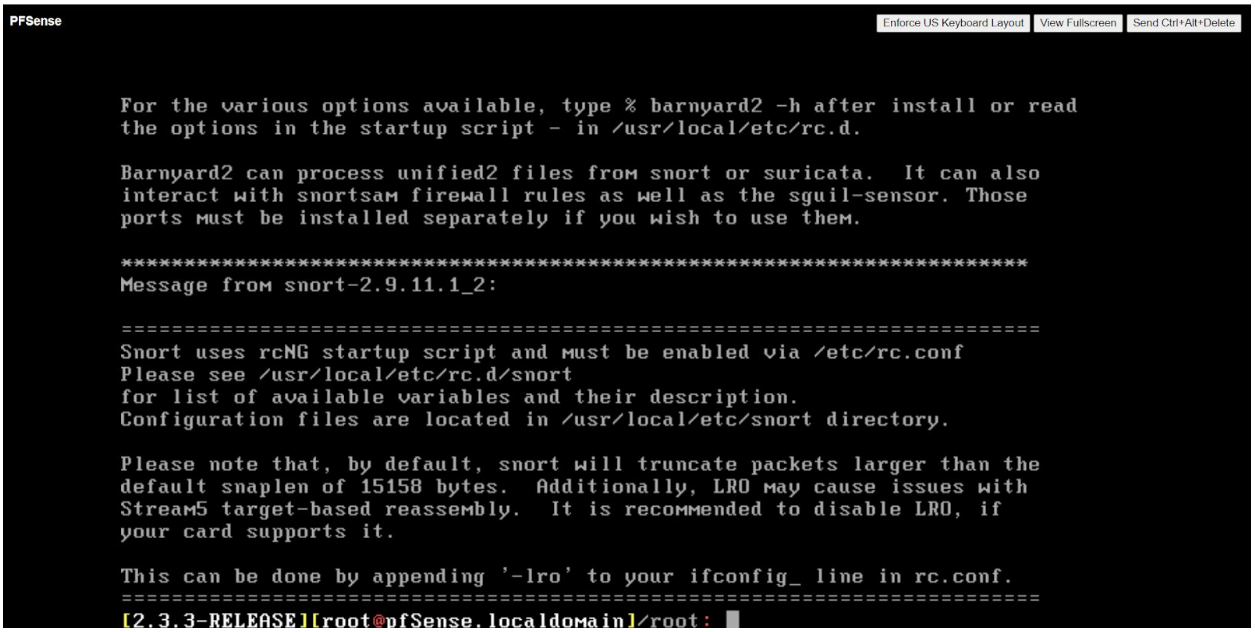
Blocking incoming traffic is important so that no outside user can exploit any services in use by the system/network. Blocking of outbound rules is important so that a user is not lured to connect to a malicious service (for example using phishing).

Extra Credit

Installation



```
receiving a patch. Please take note of this when
deploying this software.

* * * * * * * * * * * * * * * * * * * * * * * *
Message from ntopng-3.2.2018.03.13:

---------------------------------------------------------------------------
WARNING:

ntopng runs a web interface service by default, it is suggested to protect
such network accessible services with packet filters or TCP wrappers.

ntopng requires to connect to a redis server to work. Please install redis
server from databases/redis or use -r option via ntopng_flags to specify a
remote one.

If you enabled GeoIP support(the default), please use ntopng-geoipupdate.sh
to update GeoIP database to the latest available data.

To pass a configuration file to ntopng, which overrides any command
line arguments, add something like the following to rc.conf:

ntopng_flags="/path/to/file.conf"
```



```
For the various options available, type % barnyard2 -h after install or read
the options in the startup script - in /usr/local/etc/rc.d.

Barnyard2 can process unified2 files from snort or suricata.  It can also
interact with snortsam firewall rules as well as the sguil-sensor. Those
ports must be installed separately if you wish to use them.

**************************************************************************
Message from snort-2.9.11.1_2:

===========================================================================
Snort uses rcNG startup script and must be enabled via /etc/rc.conf
Please see /usr/local/etc/rc.d/snort
for list of available variables and their description.
Configuration files are located in /usr/local/etc/snort directory.

Please note that, by default, snort will truncate packets larger than the
default snaplen of 15158 bytes.  Additionally, LRO may cause issues with
Stream5 target-based reassembly.  It is recommended to disable LRO, if
your card supports it.

This can be done by appending '-lro' to your ifconfig_ line in rc.conf.
===========================================================================
[2.3.3-RELEASE][root@pfSense.localdomain]/root: 
```

Pfsense stopped working after upgrade, can’t proceed. GUI was not accessible.

Note - I was not thorough with this homework and found a lot of things that I didn’t fully understand specially from implementation point of view and failed to do good implementation specially for pfsense. I wanted to ask how can I improve on this or are there any resources on this. Thanks ;)