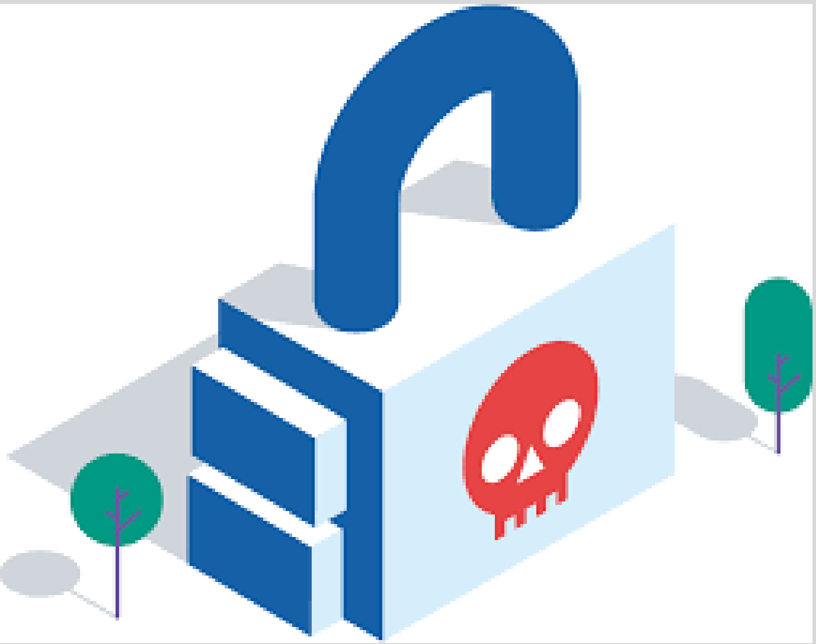
Basic knowledge



Student name: Le Viet An

Student number: 3466604

E-mail: lean1112014@gmail.com

Table of Contents

I. Introduction

This document is to show how I understand basic knowledge of network through the way I explain and apply it.

The 'basic knowledge' portfolio part of this semester is to learn about knowledge of IT Security that helps me improve my technical skills (especially networking and Linux). Moreover, I can understand how to design a secured network.

For me, everything is still new so I chose structured design to have good foundation 5s6

For the basic knowledge assignment, I will prove knowledge of the following subjects:

- 2 segregated networks and a public network (VLAN) with a firewall-router in between.
- (secured) server(s) for the public functionality/service in a DMZ network.
- (secured) server(s) for the internal functionality.
- External (from seclab) access to the public functionality/service.
- Strict firewall filtering for inbound, outbound and internal communications.
- vpn access to the network.
- basic monitoring for the most important servers/services in a SOC-like setup.
- IDS detections, also for SOC-like services

II. Company Chosen

ASML

In this portfolio, I am going to choose ASML as the company to analysis, design, and realization and test my demo environment.

ASML is a large company based in Velhoven, Netherlands. They give chip manufacturers everything they need (from hardware to software). With lithography system technology along with many advanced software, ASML technology is trusted by many leading chip manufacturers. With strong growth, ASML has now appeared in 16 countries with 19,000 employees worldwide.

III. Demo environment

3.1: Analysis

After going through the home website and with some information related to this company, I think some below attacks method can occur.

Threat	Description	Impact level	Probability
DDOS	Flooding the target resource	High	Medium
Malware Infection	stealing private information or spying on a computer by malicious software	High	Medium
SQL injection	Using SQL statements via webpage input to steal or destroy database	High	High
SciptKiddies	Downtime, Reputation damage	Medium	Low

ASML is a big company so all damages caused by the any attack greatly affects the company, while DDOS and malware are both attack methods that hackers use very often. Moreover, the competition between companies is now very large, so if attacked by malware infection, the company's data will be stolen or completely destroyed.

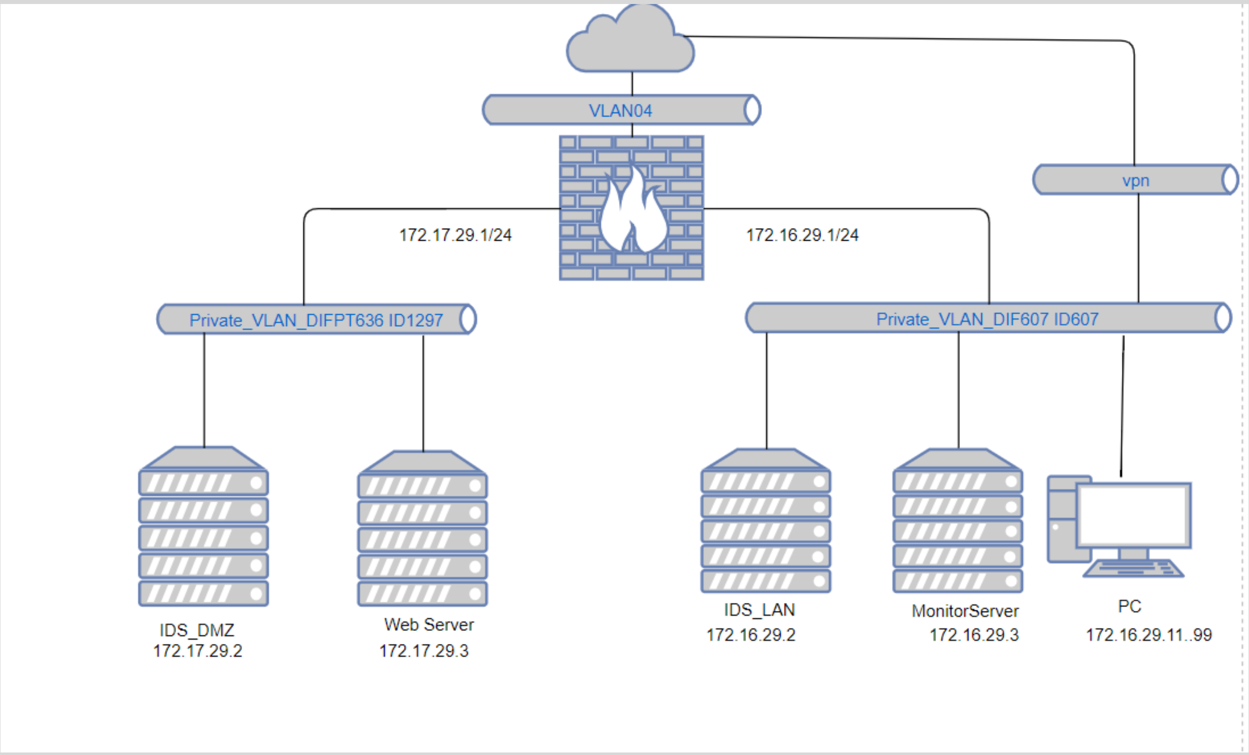
3.2: Network design

For network design, I use only one firewall for filtering all traffic data. There are 2 separate networks; the first one is the DMZ network with IDS inside to detect any risks attempt and a web server for public access. The other one is LAN network including IDS, Monitor, and WS. In the LAN network, IDS has the same role as IDS in DMZ. For the Monitor server, it will collect all data from IDS and firewall to make an overview of the system.

Design

In my network design, after research many examples of network design I make a decision to set up only one firewall which will filter all the data before passing them. According to the requirements, I also have 2 separate networks which are DMZ and private LAN network. In the DMZ, there is an IDS inside to watch and detect all risks. Moreover, the web server is also set up in DMZ for public access.

For the private LAN network, I also set up a monitor to gather information from the firewall and IDS to make an overview of the network.



IP configuration WAN and Firewall in DMZ			
DMZ LAN network	172.17.29.0/24		
WAN Firewall IP address	172.17.29.1/24 (static) - DMZ	192.168.4.11/24 (static) - WAN	172.16.29.1/24 (static) - LAN

IDS_DMZ	172.17.29.2/24 (static)
WebServer	172.17.29.3/24 (static)

Then, we configure LAN for the workstations of the company.

IP configuration LAN and firewall	
IP-range (subnet) LAN:	172.16.29.11 – 172.16.29.99 (netmask 255.255.255.0)
LAN ip-address firewall:	172.16.29.1/24
IDS_LAN	172.16.29.2/24
Monitor Server	172.16.29.3/24

The needed network segregation

A. Why is network segregation important?

Use the principles of minimum privileges and need - to know. If a system does not need to communicate with another system on the network, it is not allowed. If a system only needs to talk to another system on a specific port or protocol and nothing else, it should be limited like that.

Separate information and infrastructure based on your security requirements. This may include the use of different hardware or platforms based on security classification or different risk and risk environments in which each network system or segment operates.

Identify, authenticate and authorize access to entities based on your security requirements.

This includes users, systems and services that restrict their access to their intended function.

Make white list instead of blacklist. It is granting access to known goods, instead of denying access to known bad faces. This will also improve the organization's ability to analyze log files.

How to implement network segregation:

Apply technologies at over simply the network layer.

Each system and network ought to be metameric and segregated, wherever attainable, from the information link layer up to and as well as the applying layer.

It is not spare to implement a hardware-based firewall because the solely protecting security lives.

Use the principles of least privilege and need-to-know. If a system doesn't need to communicate with another system on the network, it should not be allowed to. If a system only needs to talk to another system on a specific port or protocol and nothing else, it should be restricted as such.

Separate info and infrastructure supported your security needs.

This may embrace victimization totally different hardware or platforms supported security classifications or different threat and risk environments within which every system or network phase operates.

Identify, authenticate and authorize access for entities based on your security requirements.

This includes users, systems and services that should have their access restricted to that required to perform their intended function.

Implement whitelisting instead of blacklisting.

That is grant access to the illustrious sensible, rather than denying access to the known bad.

This will conjointly improve Associate in nursing organization's capability to investigate log files

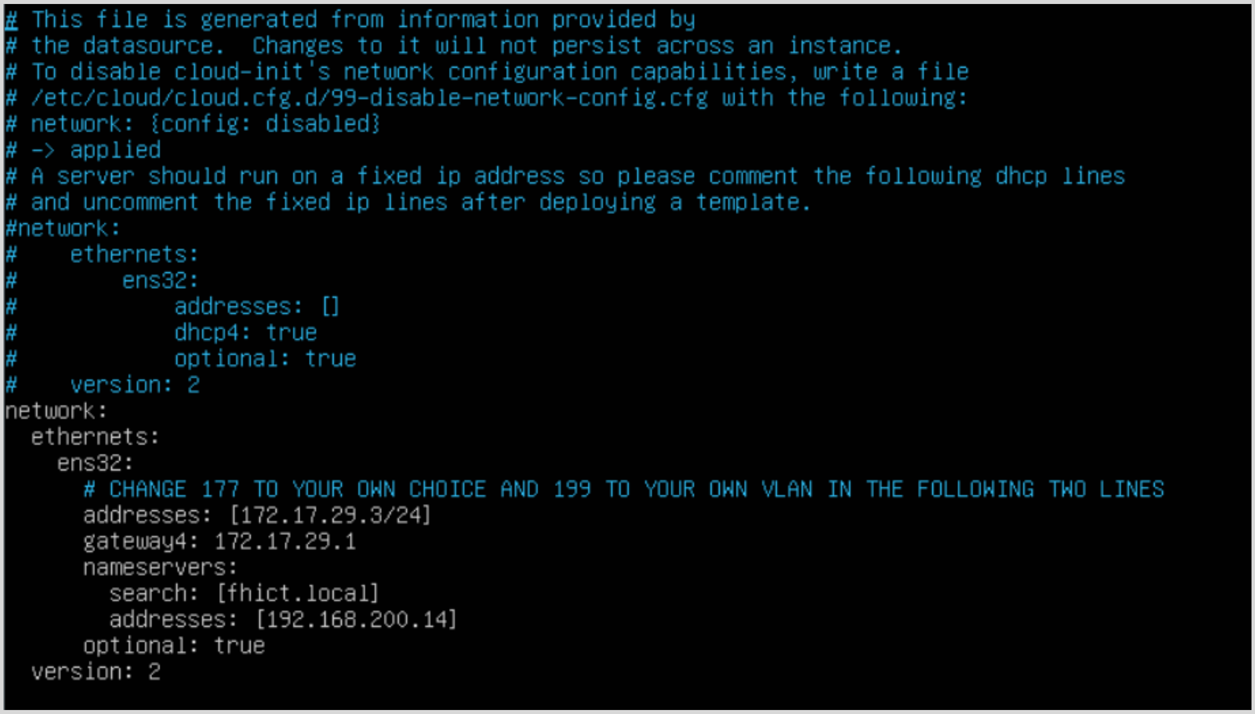
Webserver

I choose a template of Ubuntu 18.04 Server to set up my webserver.

First, Configure web server.

Follow the command on the screen, I open this file by :

$sudo nano /etc/netplan/seclab.yaml



```
# This file is generated from information provided by
# the datasource.  Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
# -> applied
# A server should run on a fixed ip address so please comment the following dhcp lines
# and uncomment the fixed ip lines after deploying a template.
#network:
#    ethernets:
#        ens32:
#            addresses: []
#            dhcp4: true
#            optional: true
#    version: 2
network:
  ethernets:
    ens32:
      # CHANGE 177 TO YOUR OWN CHOICE AND 199 TO YOUR OWN VLAN IN THE FOLLOWING TWO LINES
      addresses: [172.17.29.3/24]
      gateway4: 172.17.29.1
      nameservers:
        search: [fhict.local]
        addresses: [192.168.200.14]
      optional: true
  version: 2
```

Then I activated the websever

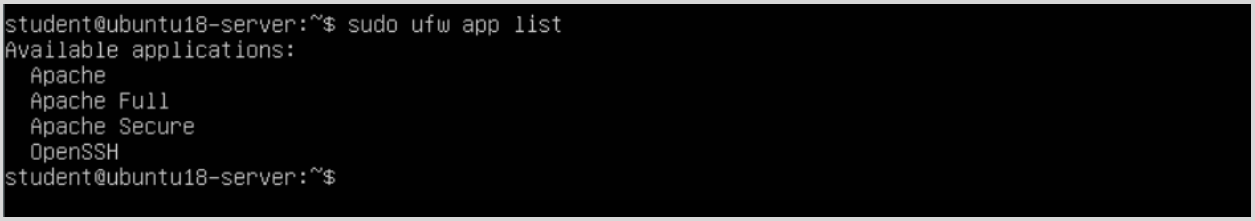
$sudo netplan apply

Next, I installed apache2 for webserver

$Sudo apt install apache2

And, I ajusted the firewall

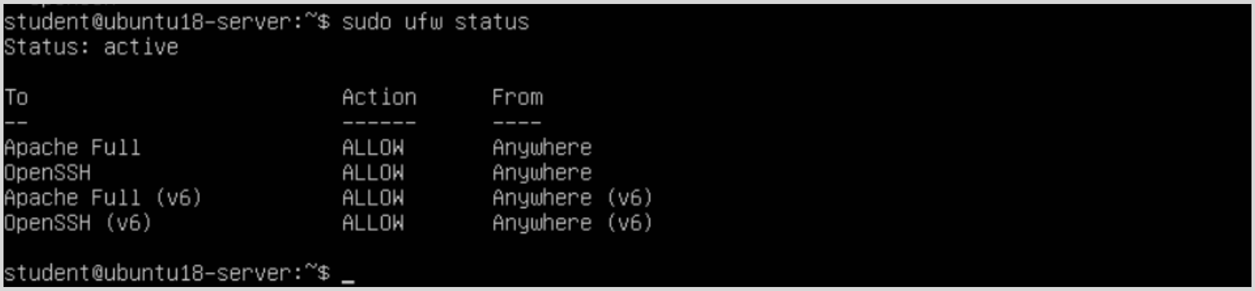
+)check ufw application: $sudo ufw app list



```
student@ubuntu18-server:~$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  OpenSSH
student@ubuntu18-server:~$
```

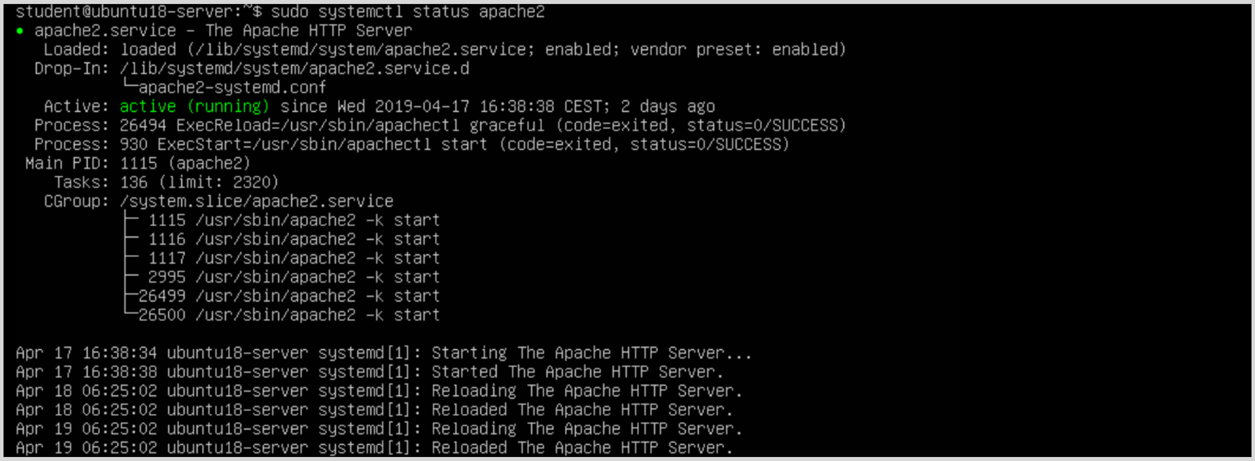
+) enable the most restrictive profile that will still allow the traffic you've configured, permitting traffic on port 80:$sudo ufw allow ‘Apache’

+)verify the change: $sudo ufw status



```
student@ubuntu18-server:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
Apache Full                ALLOW       Anywhere
OpenSSH                    ALLOW       Anywhere
Apache Full (v6)           ALLOW       Anywhere (v6)
OpenSSH (v6)               ALLOW       Anywhere (v6)

student@ubuntu18-server:~$ _
```

Next,Checking my webserver: $sudo systemctl status apache2



```
student@ubuntu18-server:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Wed 2019-04-17 16:38:38 CEST; 2 days ago
  Process: 26494 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
  Process: 930 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 1115 (apache2)
    Tasks: 136 (limit: 2320)
   CGroup: /system.slice/apache2.service
           ├─ 1115 /usr/sbin/apache2 -k start
           ├─ 1116 /usr/sbin/apache2 -k start
           ├─ 1117 /usr/sbin/apache2 -k start
           ├─ 2995 /usr/sbin/apache2 -k start
           ├─26499 /usr/sbin/apache2 -k start
           └─26500 /usr/sbin/apache2 -k start

Apr 17 16:38:34 ubuntu18-server systemd[1]: Starting The Apache HTTP Server...
Apr 17 16:38:38 ubuntu18-server systemd[1]: Started The Apache HTTP Server.
Apr 18 06:25:02 ubuntu18-server systemd[1]: Reloading The Apache HTTP Server.
Apr 18 06:25:02 ubuntu18-server systemd[1]: Reloaded The Apache HTTP Server.
Apr 19 06:25:02 ubuntu18-server systemd[1]: Reloading The Apache HTTP Server.
Apr 19 06:25:02 ubuntu18-server systemd[1]: Reloaded The Apache HTTP Server.
```

The needed firewall

A. Why Firewall Filtering is important:

The main purpose of using Firewall Filter is to check traffic packets and perform actions based on configured rules (such as Pass and Block). These rules are carefully designed based on the used applications, organization policies, or specific rules required for that network.

Benefits of deploying and using Firewall filtering is to protect the organization / company network from malicious packages, blocking attempts / hacks that are made on specific ports (by filtering or blocking port) and allow or deny specific actions.

B. How and where to implement Firewall Filtering:

In order to understand and determine the location and number of Firewalls that will be placed in your network, the organization / company will need to check their network infrastructure first, and then analyze the potential risks out or not. Most commonly, Firewalls are located on ports between the Internet and the local network and / or between subnets in the LAN. This way of deploying can help the Firewall perform the most powerful actions for every passed transaction.

However, the location of the Firewall may also depend on the needs or privacy requirements of the organization / company. The most important thing an organization / company will need to note is that the more established a firewall is, the lower the network will be able to do it. If, in any case, anywhere in our network has a firewall, then the transaction will actually slow down due to the testing time of each firewall. In short, it is important that the organization / company must learn and know how they should implement and set up a firewall.

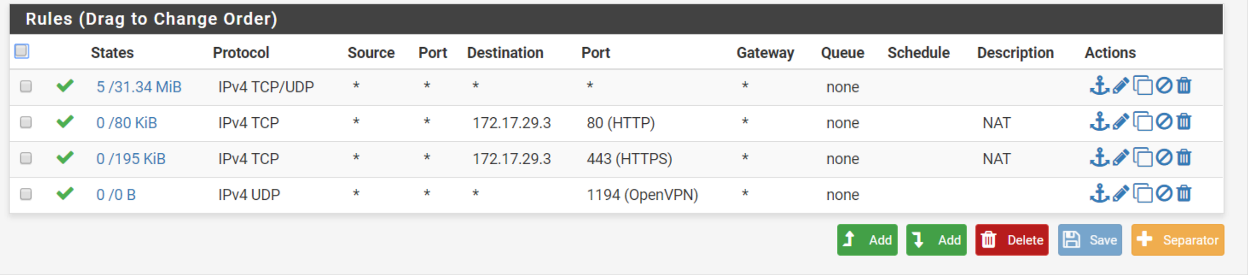
Firewall types:

- **Stateless firewall**
- **Stateful firewall**
- **Next Generation firewall**

How I design my firewall:

- Wan IP: 192.168.4.11(VLAN04)
- LAN IP: 172.16.29.1(VLANDIF607)
- DMZ IP: 172.17.29.1(VLANDIFPT ID1297)

Rules of WAN

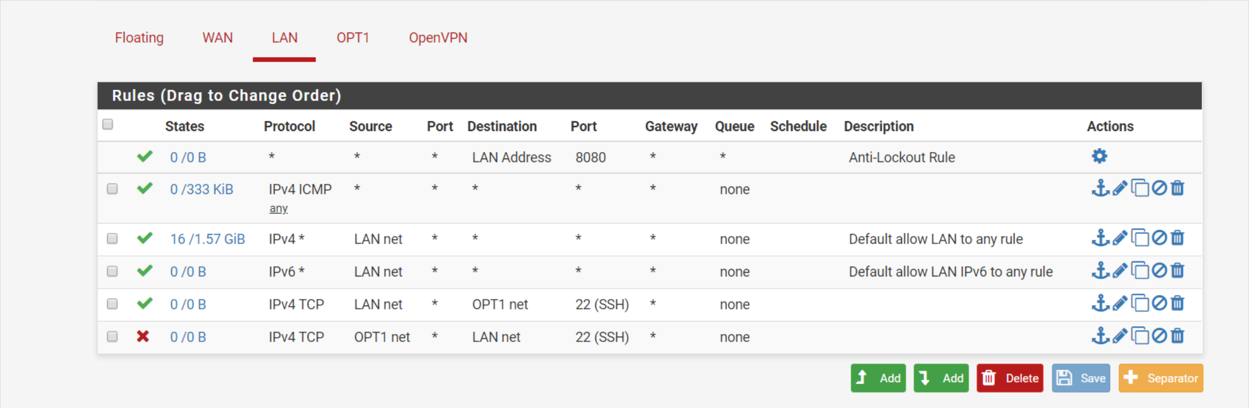


Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	5 /31.34 MiB	IPv4 TCP/UDP	*	*	*	*	*	none			
□	✓	0 /80 KiB	IPv4 TCP	*	*	172.17.29.3	80 (HTTP)	*	none		NAT	
□	✓	0 /195 KiB	IPv4 TCP	*	*	172.17.29.3	443 (HTTPS)	*	none		NAT	
□	✓	0 /0 B	IPv4 UDP	*	*	*	1194 (OpenVPN)	*	none			

Rules of LAN

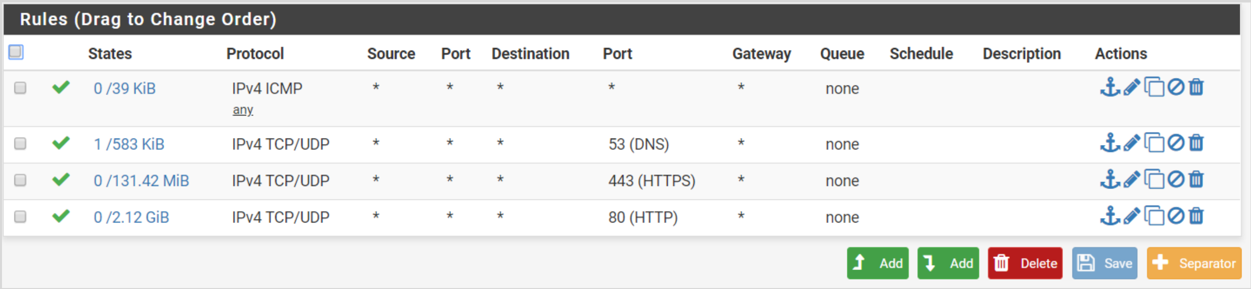
As you can see, I have 2 rules on LAN that have the same port. I have set up 1 to allow LAN access to the DMZ but I also have 1 to block from the DMZ to LA



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0 /0 B	*	*	*	LAN Address	8080	*	*		Anti-Lockout Rule	⚙
□	✓	0 /333 KiB	IPv4 ICMP any	*	*	*	*	*	none			
□	✓	16 /1.57 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	
□	✓	0 /0 B	IPv4 TCP	LAN net	*	OPT1 net	22 (SSH)	*	none			
□	✗	0 /0 B	IPv4 TCP	OPT1 net	*	LAN net	22 (SSH)	*	none			

DMZ rules



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /39 KiB	IPv4 ICMP any	*	*	*	*	*	none			
□	✓	1 /583 KiB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none			
□	✓	0 /131.42 MiB	IPv4 TCP/UDP	*	*	*	443 (HTTPS)	*	none			
□	✓	0 /2.12 GiB	IPv4 TCP/UDP	*	*	*	80 (HTTP)	*	none			

The design for vpn access

VPN, also known as Virtual Private Network, allows users to set up a virtual private network with another network on the Internet. VPN can be used to access websites that are restricted to geographic location, protect your browsing activity from "curiosity" on public Wifi networks by setting up a virtual private network.

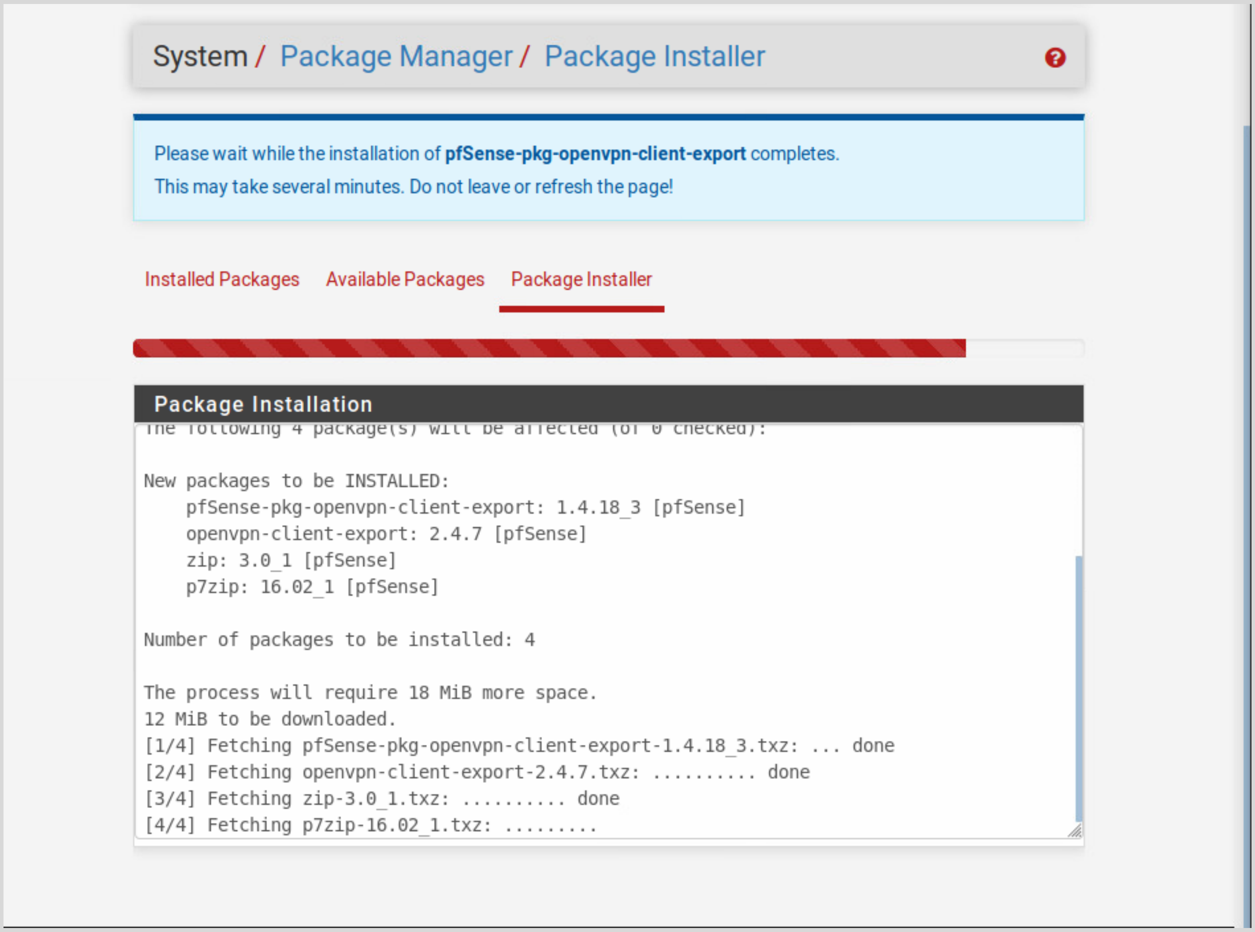
Basically, VPN forwards all of your network traffic traffic to the system - where it is possible to remotely access local network resources and bypass Internet censorship. Most operating systems have VPN support integrated

My design for VPN access is User Authentication-Remote Access with encryption algorithm AES-128-CBC and Digest algorithm:SHA256.

The VPN will then check the current machine that the user is using to see if it has the same certificate as the Certificate Authority on PFSense. If the certificates are appropriate, connecting users using VPN will be established. After successful connection, all communication between VPN and LAN users will be encrypted with AES-128-CBC.

How I design VPN:

Firstly, I did set up a package on pfSense

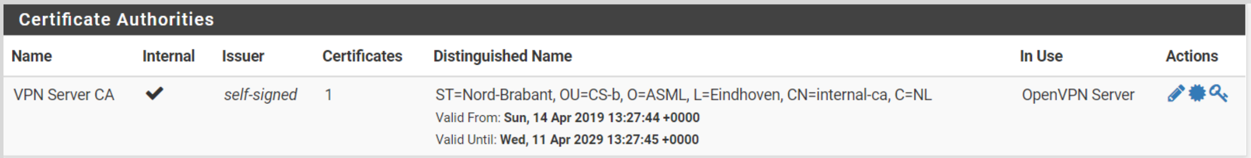


Please wait while the installation of **pfSense-pkg-openvpn-client-export** completes.
This may take several minutes. Do not leave or refresh the page!

Package Installation

```
The following 4 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
    pfSense-pkg-openvpn-client-export: 1.4.18_3 [pfSense]
    openvpn-client-export: 2.4.7 [pfSense]
    zip: 3.0_1 [pfSense]
    p7zip: 16.02_1 [pfSense]

Number of packages to be installed: 4

The process will require 18 MiB more space.
12 MiB to be downloaded.
[1/4] Fetching pfSense-pkg-openvpn-client-export-1.4.18_3.txz: ... done
[2/4] Fetching openvpn-client-export-2.4.7.txz: .......... done
[3/4] Fetching zip-3.0_1.txz: .......... done
[4/4] Fetching p7zip-16.02_1.txz: .........
```

Then, I created a server certificate authority



Certificate Authorities

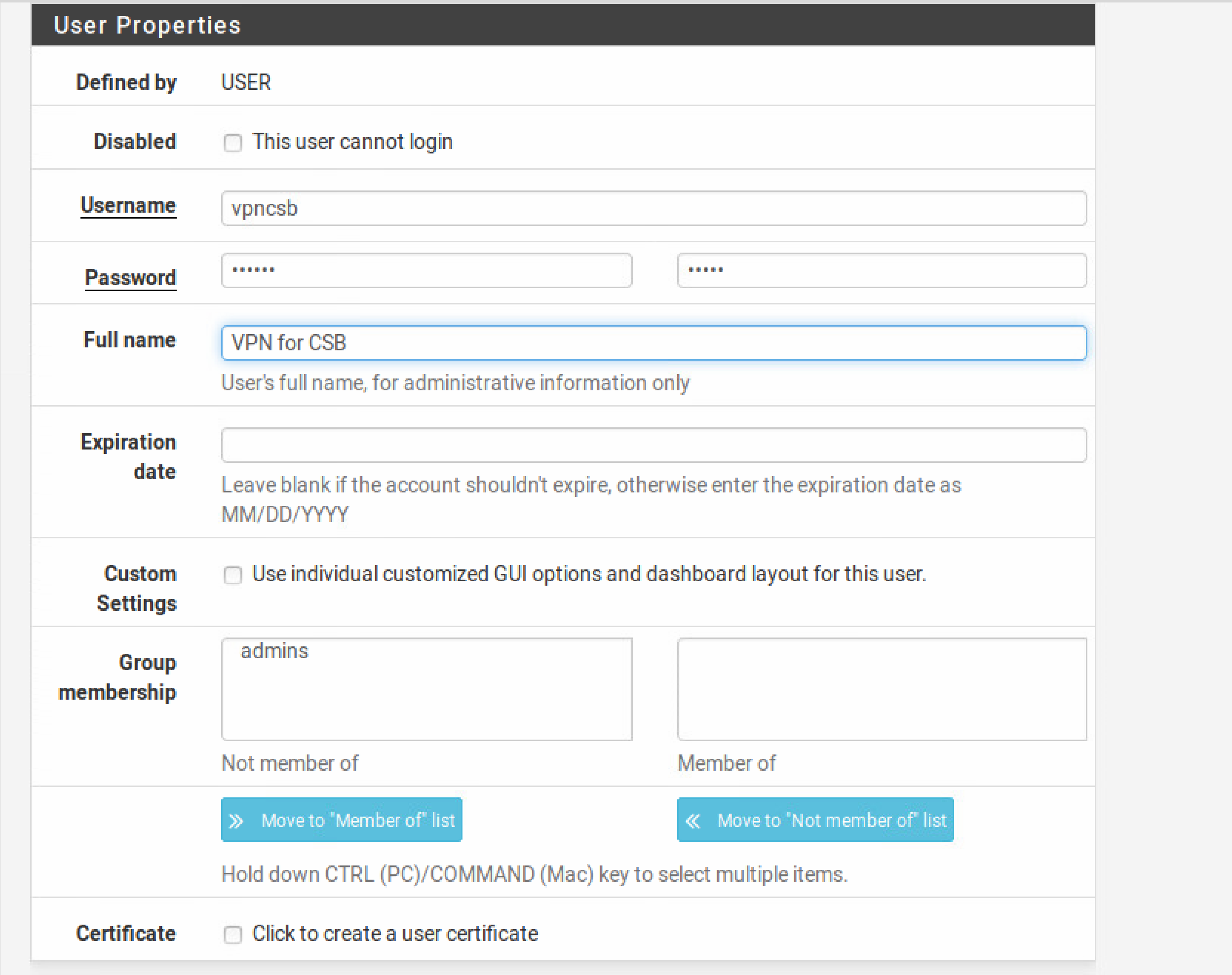
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
VPN Server CA	✓	*self-signed*	1	ST=Nord-Brabant, OU=CS-b, O=ASML, L=Eindhoven, CN=internal-ca, C=NL Valid From: **Sun, 14 Apr 2019 13:27:44 +0000** Valid Until: **Wed, 11 Apr 2029 13:27:45 +0000**	OpenVPN Server	

Next, I went to user setting and did set up for user here.

-username: vncsb

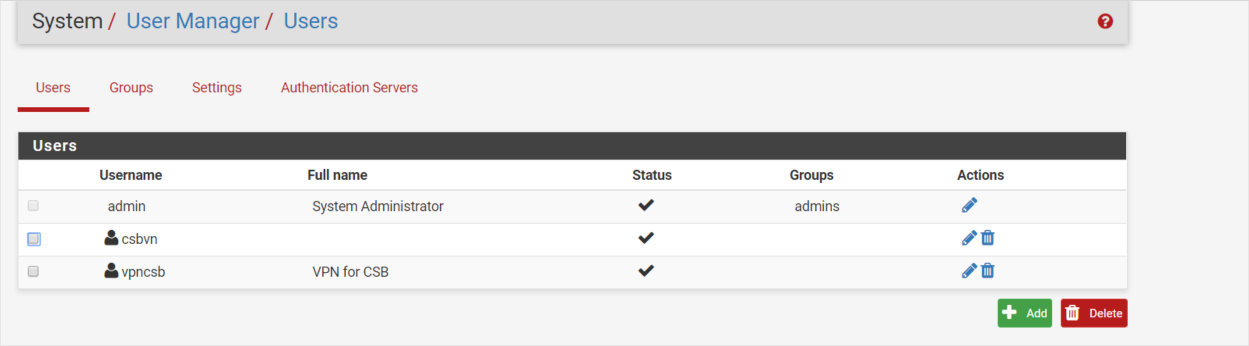
-password: admin

-Group membership: NOT member of admins



User Properties

Defined by	USER
Disabled	□ This user cannot login
Username	vpncsb
Password	•••••• •••••
Full name	VPN for CSB User's full name, for administrative information only
Expiration date	 Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	□ Use individual customized GUI options and dashboard layout for this user.
Group membership	Not member of: admins Member of:
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.
Certificate	□ Click to create a user certificate



Users

	Username	Full name	Status	Groups	Actions
□	admin	System Administrator	✓	admins	✎
□	csbvn		✓		✎ 🗑
□	vpncsb	VPN for CSB	✓		✎ 🗑

After that, I continued doing set up openVPN

-Server mode: Remote Access (User Auth)

-Backend for Authentication: Local Database

-Protocol: UDP

-Interface: WAN

-Local port:1194

- TLS authentication with key: Check – Match with my Certificate Authority

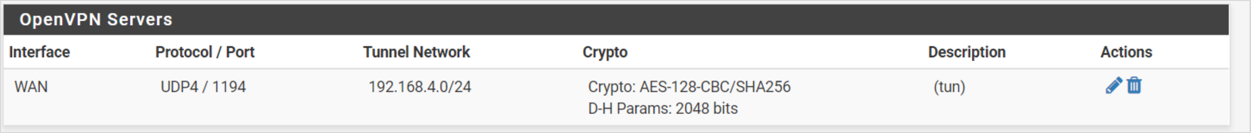
-Key length: 2048

-Encryption Algorithm: AES-128-CBC

-Auth digests Algorithm: SHA256 (160-bit)

-IPV4 Tunnel Network: 192.168.4.0/24

-IPV4 Local networks: 172.16.29.0/24



OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	192.168.4.0/24	Crypto: AES-128-CBC/SHA256 D-H Params: 2048 bits	(tun)	✎ 🗑

Other secure connections used

a. HTTPS

I did implement the webserver with HTTPS which is located in DMZ area. With HTTPS, the communication protocol will be encrypted by TLS .

Although not perfect, HTTPS is also a measure against phishing scams. If you are using a public Wi-Fi network (in cafes, airports ...) to access your bank account, look for the lock icon, HTTPS text on the address and address box. Only accurate of this online banking page. This is the most effective way to verify that you are accessing the correct address, instead of going to another phishing or phishing site. If you don't see HTTPS, make sure your access network is not secure.

Step 1:Enable the SSL Module

Enable Apache SSL module

```
-$ sudo a2enmod ssl
```

Activate the default website

```
-$ sudo a2ensite default-ssl
```

Restart apache

```
-$ sudo service apache2 reload
```

Step 2:Create a SSL Certificate

Create a new directory

```
-$ sudo mkdir /etc/apache2/ssl
```

Generate a new Certificate and Private Key

```
-$ sudo openssl req –x509 –nodes –days 365 –newkey rsa:2048 –keyout /etc/apache2/ssl/apache.key –out /etc/apache2/ssl/apache.crt
```

Fill out all fields and set the file permissions to protect my private key and certificate.

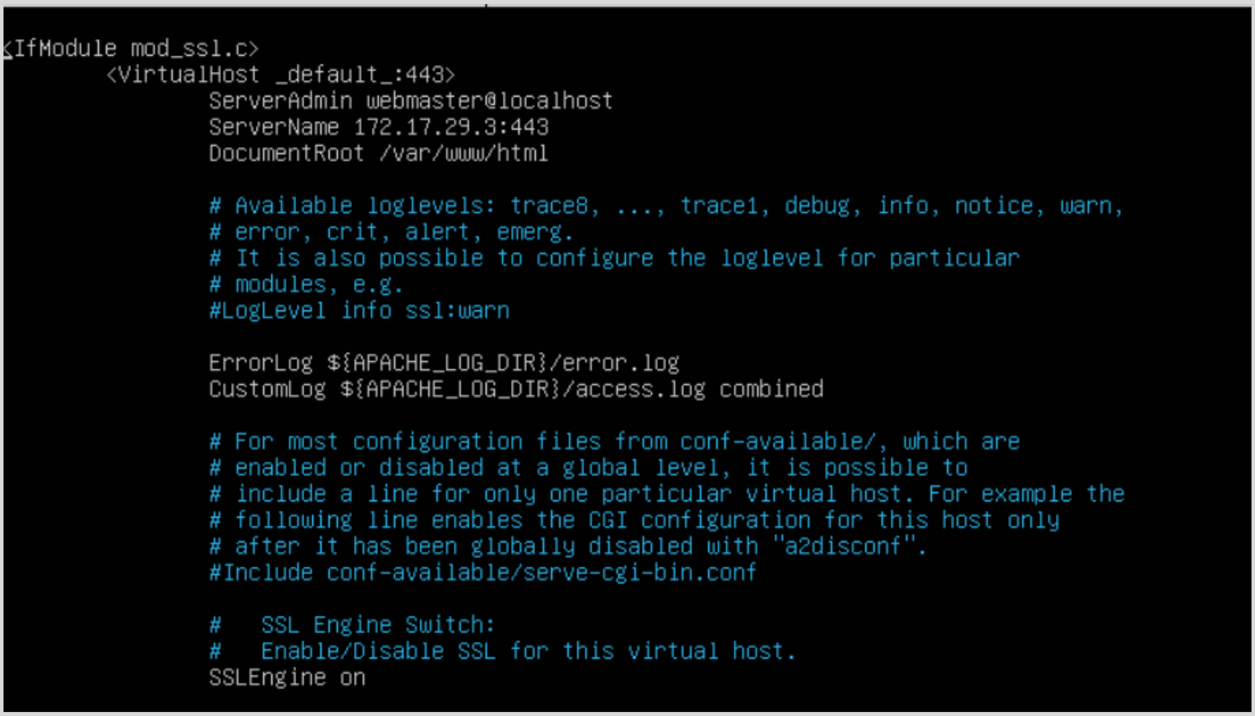
```
-$ sudo chmod 600 /etc/apache2/ssl/*
```

Step 3: Configure Apache to Use SSL

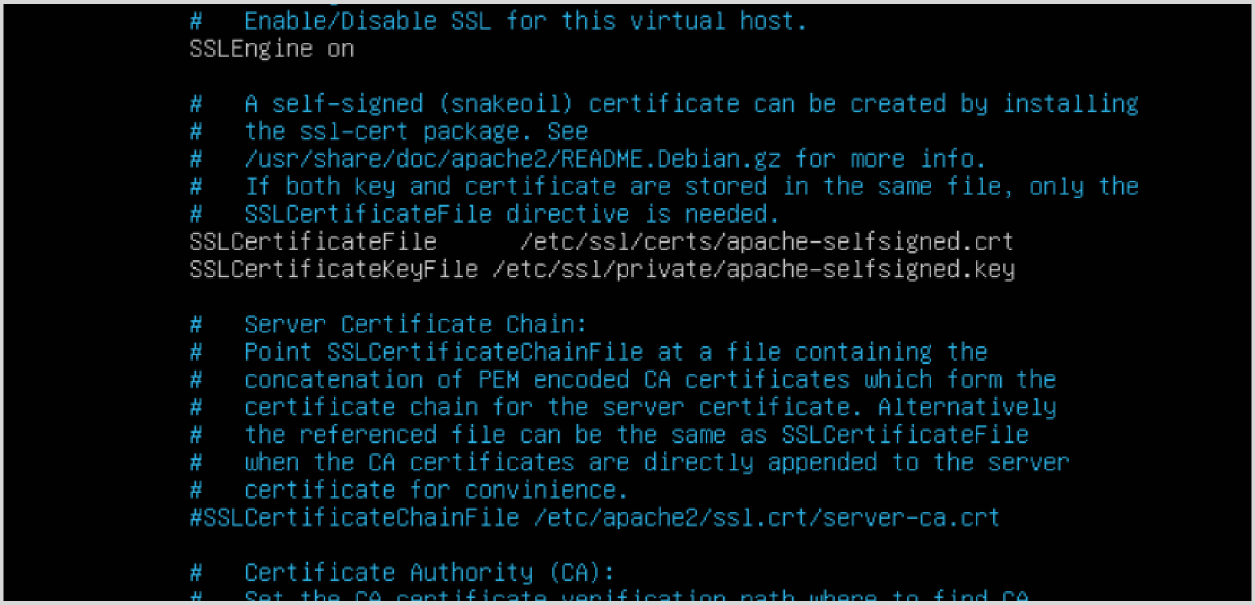
Open the server configuration by:

```
-sudo nano /etc/apache2/sites-enable/default-ssl.conf
```

Then I changed some lines in the configuration file



```
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost
                ServerName 172.17.29.3:443
                DocumentRoot /var/www/html

                # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
                # error, crit, alert, emerg.
                # It is also possible to configure the loglevel for particular
                # modules, e.g.
                #LogLevel info ssl:warn

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined

                # For most configuration files from conf-available/, which are
                # enabled or disabled at a global level, it is possible to
                # include a line for only one particular virtual host. For example the
                # following line enables the CGI configuration for this host only
                # after it has been globally disabled with "a2disconf".
                #Include conf-available/serve-cgi-bin.conf

                #   SSL Engine Switch:
                #   Enable/Disable SSL for this virtual host.
                SSLEngine on
```



```
                #   Enable/Disable SSL for this virtual host.
                SSLEngine on

                #   A self-signed (snakeoil) certificate can be created by installing
                #   the ssl-cert package. See
                #   /usr/share/doc/apache2/README.Debian.gz for more info.
                #   If both key and certificate are stored in the same file, only the
                #   SSLCertificateFile directive is needed.
                SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.crt
                SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

                #   Server Certificate Chain:
                #   Point SSLCertificateChainFile at a file containing the
                #   concatenation of PEM encoded CA certificates which form the
                #   certificate chain for the server certificate. Alternatively
                #   the referenced file can be the same as SSLCertificateFile
                #   when the CA certificates are directly appended to the server
                #   certificate for convinience.
                #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

                #   Certificate Authority (CA):
                #   Set the CA certificate verification path where to find CA
```

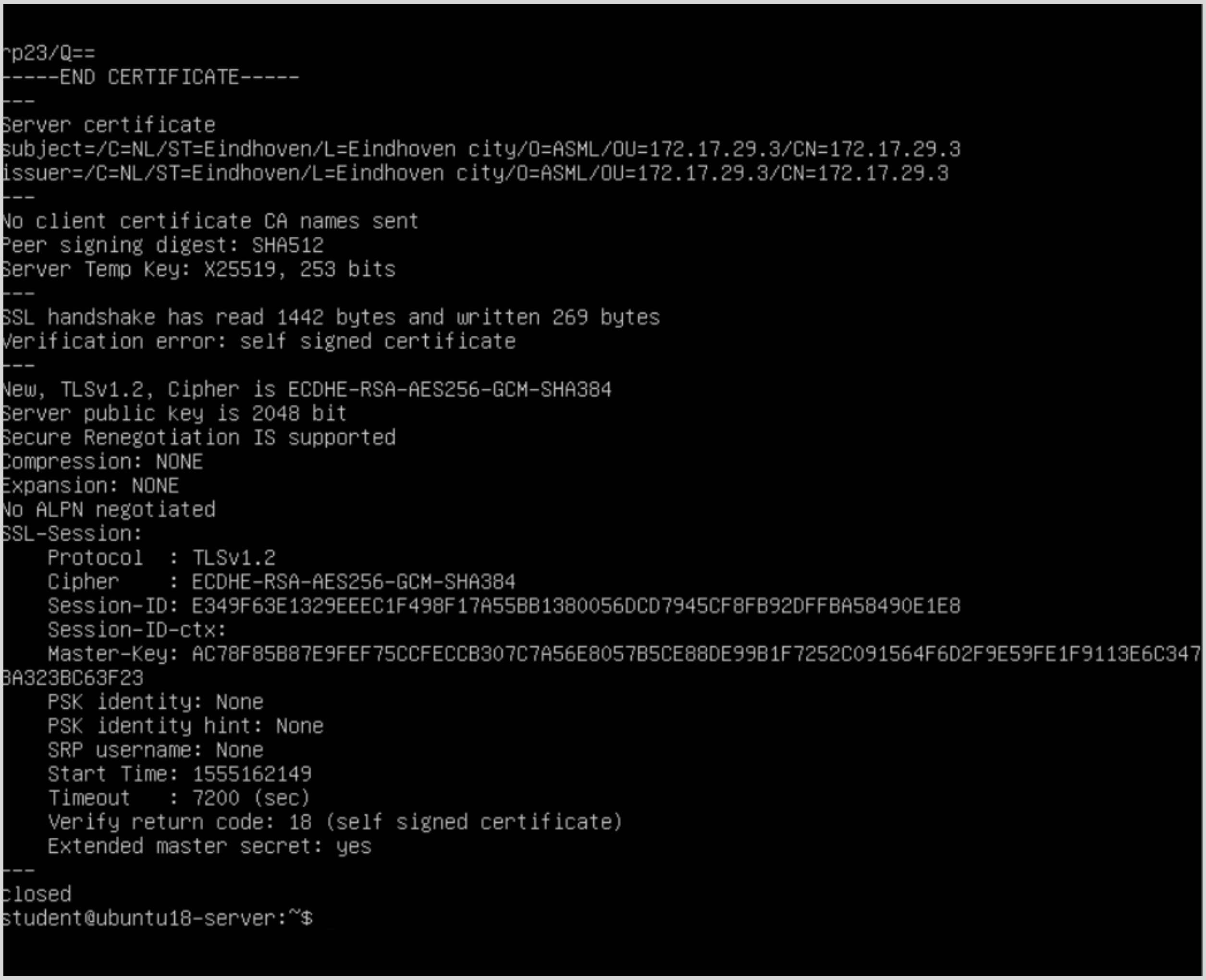
And reload the service

-$ sudo service apache reload

Step 4: Test

Run the command

```
-$ openssl s_client -showconvert -connect 172.17.29.3:443
```

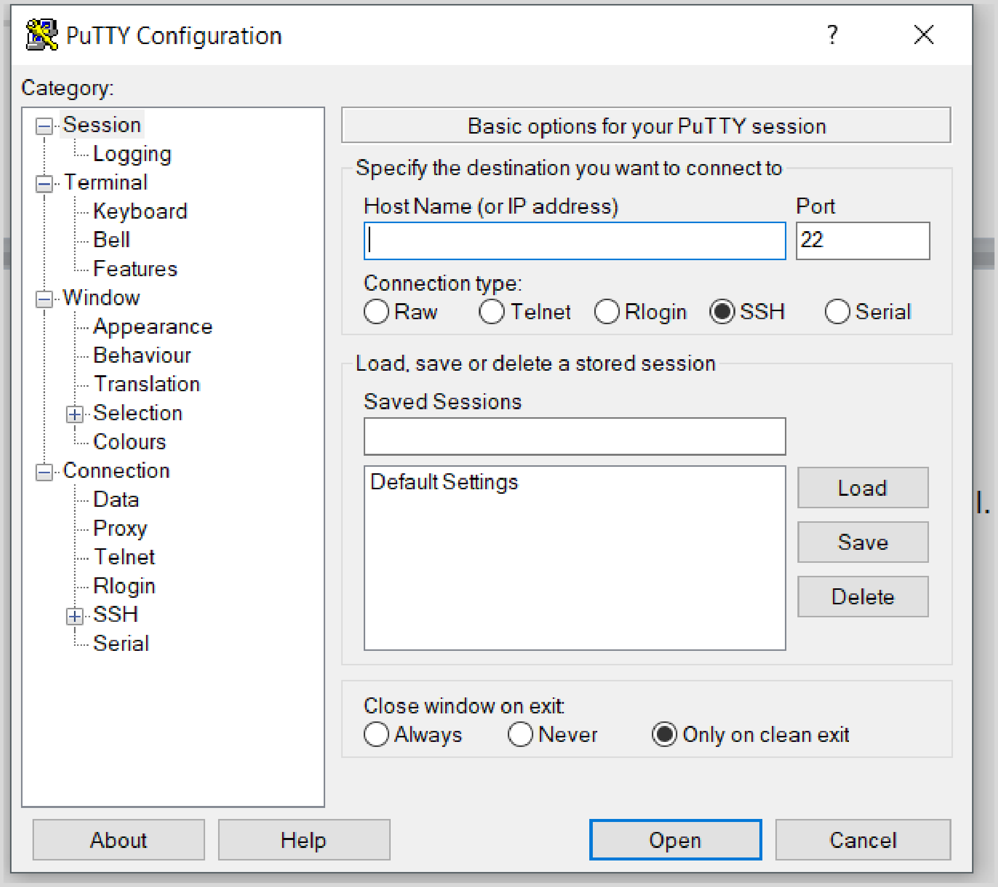


```
rp23/Q==
-----END CERTIFICATE-----
---
Server certificate
subject=/C=NL/ST=Eindhoven/L=Eindhoven city/O=ASML/OU=172.17.29.3/CN=172.17.29.3
issuer=/C=NL/ST=Eindhoven/L=Eindhoven city/O=ASML/OU=172.17.29.3/CN=172.17.29.3
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1442 bytes and written 269 bytes
Verification error: self signed certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: E349F63E1329EEEC1F498F17A55BB1380056DCD7945CF8FB92DFFBA58490E1E8
    Session-ID-ctx:
    Master-Key: AC78F85B87E9FEF75CCFECCB307C7A56E8057B5CE88DE99B1F7252C091564F6D2F9E59FE1F9113E6C347
3A323BC63F23
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1555162149
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: yes
---
closed
student@ubuntu18-server:~$
```

b. SSH

SSH, or called Secure Shell, is a remote control protocol that allows users to control and modify servers remotely over the Internet. The service was created to replace the unencrypted Telnet and use cryptographic techniques to ensure that all incoming and outgoing communications from the remote server take place in encrypted state. It provides an algorithm to authenticate remote users, transfer input from the client to the host, and relay the results back to the customer.

For setting up ssh, first I need open port 22 on pfsense , then doing install. For window, I download Putty software instead of using command on Linux.



Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions:

Default Settings

Close window on exit:
○ Always ○ Never ● Only on clean exit

IDS(Intrusion Detection System)

IDS (Intrusion Detection Systems) is a device or software that monitors network traffic, suspicious behaviors and alerts for system administrators. The purpose of IDS is to detect and prevent actions that damage system security, or actions in the attack process such as port detection and scanning. IDS can also distinguish between internal attacks (from employees or customers in the organization) and external attacks (from hackers). In some cases, IDS can react to unusual / malicious traffic by blocking users or network access source IP addresses.

I have some test cases to check if IDS works or not:

Intrusion Test Case	Test description
Ping	Detect which IP is doing contact to my network
Network Scanning	To determine which protocols are used for network scanning, FP or FN?
Ddos	Detect who is trying to ddos my webserver

I used Snort on Ubuntu as an IDS and put them in Private Lan and DMZ.

Firstly, I did set up and change their ip to static ip(IP of the workstation where I put IDS in).

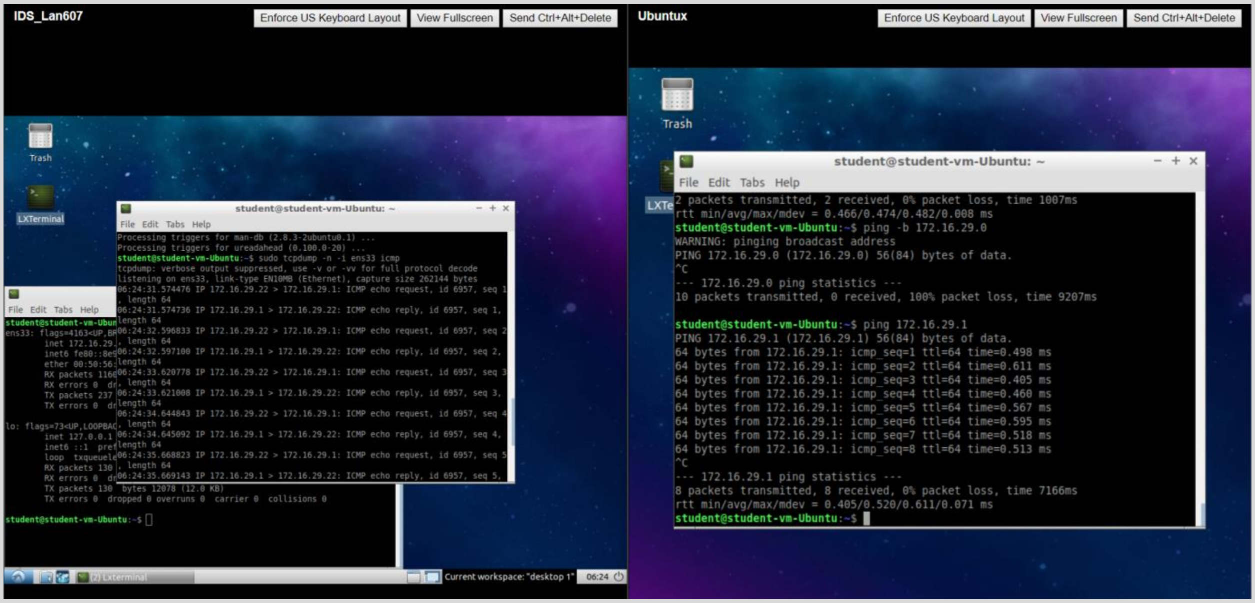
-Deploy Sort with command: $sudo apt install snort

+) Interface: ens32 (for IDS in DMZ) and ens33(for IDS in LAN)

+) Ip : 172.17.29.0/24(for DMZ) and 172.16.29.0(for LAN)

So I started the command line network sniffer tcpdump to listen for network traffic with interface ens33:

-$ sudo tcpdump –n –i ens33 icmp

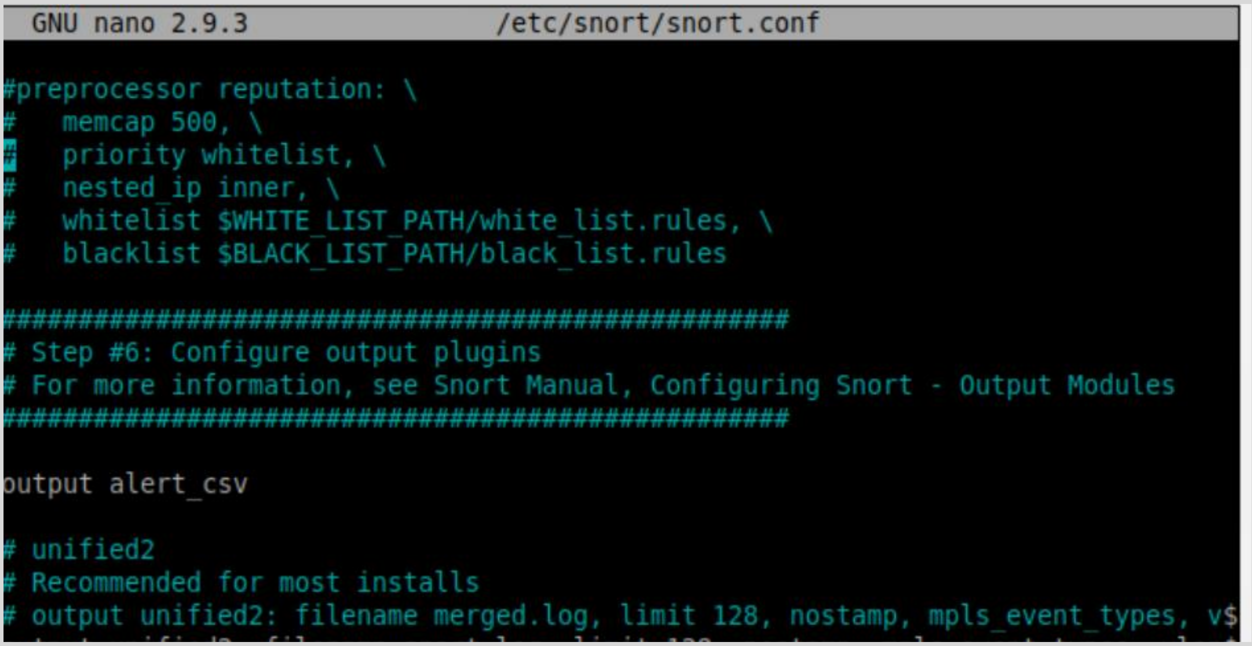


```
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-20) ...
student@student-vm-Ubuntu:~$ sudo tcpdump -n -i ens33 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
06:24:31.574476 IP 172.16.29.22 > 172.16.29.1: ICMP echo request, id 6957, seq 1
, length 64
06:24:31.574736 IP 172.16.29.1 > 172.16.29.22: ICMP echo reply, id 6957, seq 1,
length 64
06:24:32.596833 IP 172.16.29.22 > 172.16.29.1: ICMP echo request, id 6957, seq 2
, length 64
06:24:32.597100 IP 172.16.29.1 > 172.16.29.22: ICMP echo reply, id 6957, seq 2,
length 64
06:24:33.620778 IP 172.16.29.22 > 172.16.29.1: ICMP echo request, id 6957, seq 3
, length 64
06:24:33.621008 IP 172.16.29.1 > 172.16.29.22: ICMP echo reply, id 6957, seq 3,
length 64
06:24:34.644843 IP 172.16.29.22 > 172.16.29.1: ICMP echo request, id 6957, seq 4
, length 64
06:24:34.645092 IP 172.16.29.1 > 172.16.29.22: ICMP echo reply, id 6957, seq 4,
length 64
06:24:35.668823 IP 172.16.29.22 > 172.16.29.1: ICMP echo request, id 6957, seq 5
, length 64
06:24:35.669143 IP 172.16.29.1 > 172.16.29.22: ICMP echo reply, id 6957, seq 5,
```

```
student@student-vm-Ubun
ens33: flags=4163<UP,BR
        inet 172.16.29.
        inet6 fe80::8e9
        ether 00:50:56:
        RX packets 116
        RX errors 0  dr
        TX packets 237
        TX errors 0  dr

lo: flags=73<UP,LOOPBAC
        inet 127.0.0.1
        inet6 ::1  pref
        loop  txqueuele
        RX packets 130
        RX errors 0  dr
        TX packets 130  bytes 12078 (12.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

student@student-vm-Ubuntu:~$ 
```

```
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.466/0.474/0.482/0.008 ms
student@student-vm-Ubuntu:~$ ping -b 172.16.29.0
WARNING: pinging broadcast address
PING 172.16.29.0 (172.16.29.0) 56(84) bytes of data.
^C
--- 172.16.29.0 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9207ms

student@student-vm-Ubuntu:~$ ping 172.16.29.1
PING 172.16.29.1 (172.16.29.1) 56(84) bytes of data.
64 bytes from 172.16.29.1: icmp_seq=1 ttl=64 time=0.498 ms
64 bytes from 172.16.29.1: icmp_seq=2 ttl=64 time=0.611 ms
64 bytes from 172.16.29.1: icmp_seq=3 ttl=64 time=0.405 ms
64 bytes from 172.16.29.1: icmp_seq=4 ttl=64 time=0.460 ms
64 bytes from 172.16.29.1: icmp_seq=5 ttl=64 time=0.567 ms
64 bytes from 172.16.29.1: icmp_seq=6 ttl=64 time=0.595 ms
64 bytes from 172.16.29.1: icmp_seq=7 ttl=64 time=0.518 ms
64 bytes from 172.16.29.1: icmp_seq=8 ttl=64 time=0.513 ms
^C
--- 172.16.29.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7166ms
rtt min/avg/max/mdev = 0.405/0.520/0.611/0.071 ms
student@student-vm-Ubuntu:~$ 
```

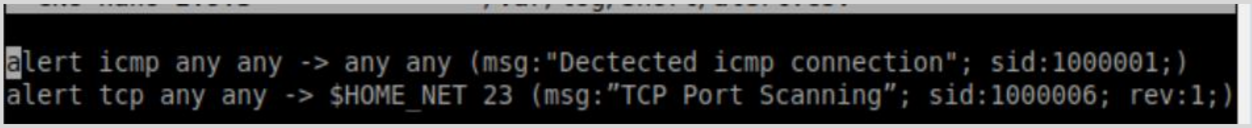
Next, I tried to configure snort with command: $sudo nano /etc/snort to save logging in a CSV (Comma Separated Values) text format.(when I add line output alert_csv)



```
 GNU nano 2.9.3                    /etc/snort/snort.conf

#preprocessor reputation: \
#    memcap 500, \
#    priority whitelist, \
#    nested_ip inner, \
#    whitelist $WHITE_LIST_PATH/white_list.rules, \
#    blacklist $BLACK_LIST_PATH/black_list.rules

###################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
###################################################

output alert_csv

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, v$
```

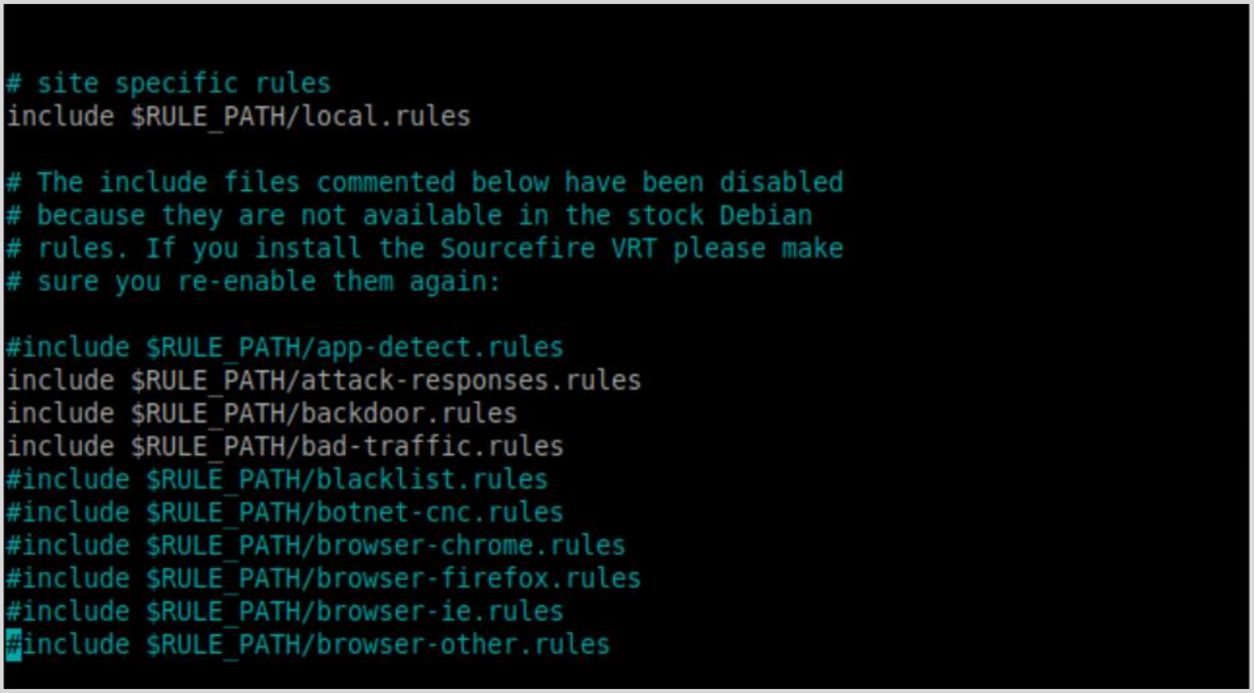
Then I did run this command to restart snort serivce: $sudo service snort restart

I checked directory the file /var/log/snort/alert.csv exists . Add the following test rule in the local.rules file that can recognize ping packets within the network as well as scanning action.

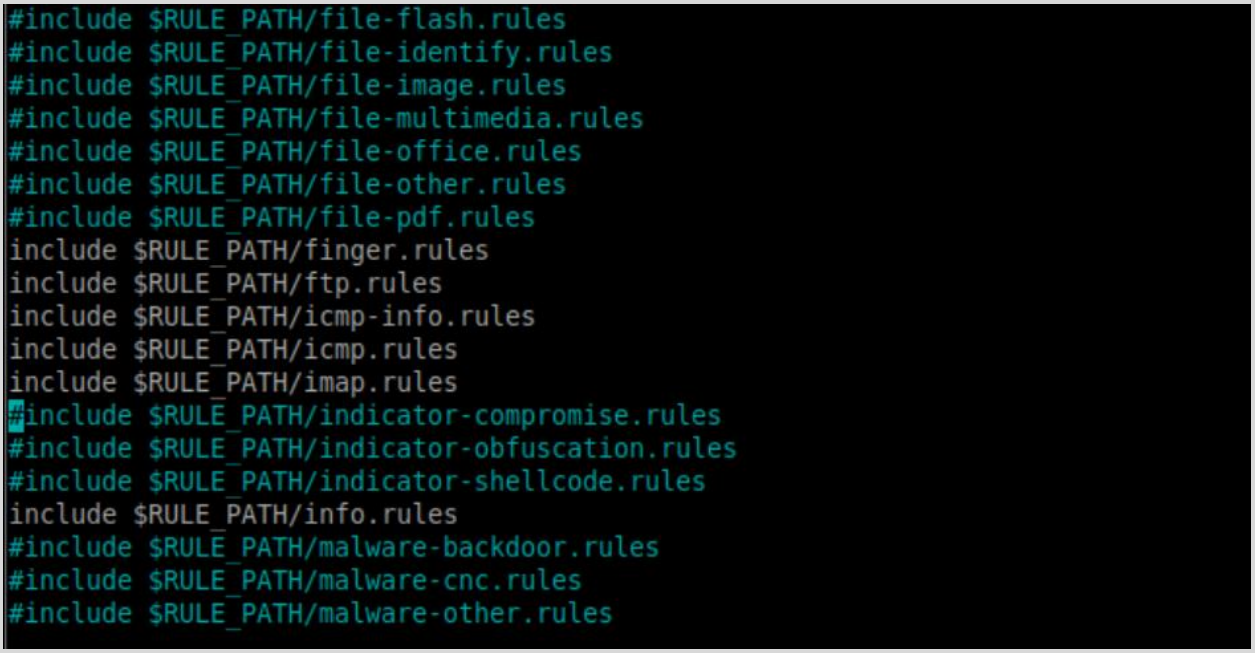


```
alert icmp any any -> any any (msg:"Dectected icmp connection"; sid:1000001;)
alert tcp any any -> $HOME_NET 23 (msg:”TCP Port Scanning”; sid:1000006; rev:1;)
```

For IDS, I did not change about rules of IDS because I think it is enough for my demo and I don’t want to change if I don’t have deep knowledge about it to avoid breaking the system.



```
# site specific rules
include $RULE_PATH/local.rules

# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:

#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
```



```
#include $RULE_PATH/file-flash.rules
#include $RULE_PATH/file-identify.rules
#include $RULE_PATH/file-image.rules
#include $RULE_PATH/file-multimedia.rules
#include $RULE_PATH/file-office.rules
#include $RULE_PATH/file-other.rules
#include $RULE_PATH/file-pdf.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/icmp-info.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/imap.rules
#include $RULE_PATH/indicator-compromise.rules
#include $RULE_PATH/indicator-obfuscation.rules
#include $RULE_PATH/indicator-shellcode.rules
include $RULE_PATH/info.rules
#include $RULE_PATH/malware-backdoor.rules
#include $RULE_PATH/malware-cnc.rules
#include $RULE_PATH/malware-other.rules
```

IT monitoring generally focuses on usability or performance monitoring: everything is still working, or not etc. This is somewhat easier to identify than whether everything is safe or not. But it is also very important in every business environment.

In this network design, I will set up a IT Monitoring machine in private LAN network so that administrators can have a secure look at their system's performance and capacity.
I set up IT monitoring with ip:172.16.29.3/24(static) and follow all the steps from the guideline on Canvas.

Nagios XI will be used as Monitoring application in this network demo

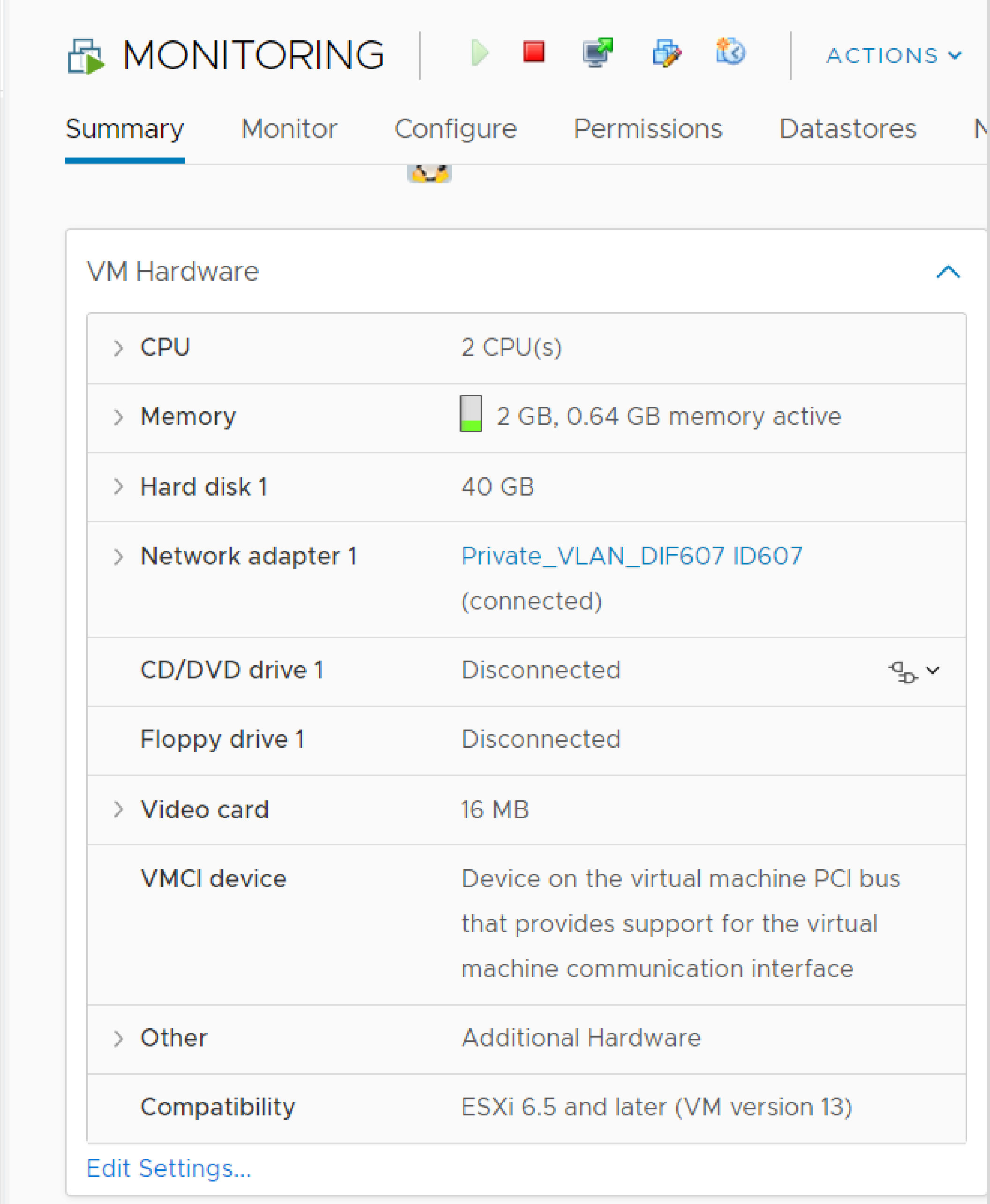
IP address of Nagios: 172.16.29.3

- Login credentials web configuration: username: nagiosadmin / password: nagiosadmin
- Machines will be monitored: IDS (DMZ), Webserver, PFSense

To set up IT monitoring, I follow all steps on Canvas.

1. Deploy the template "Templ_nagiosxi-5.2.9" from Templates -> Courses – ICS

2. In vcenter, change the network adapter from dummyport to private_VLAN DIF607 ID607

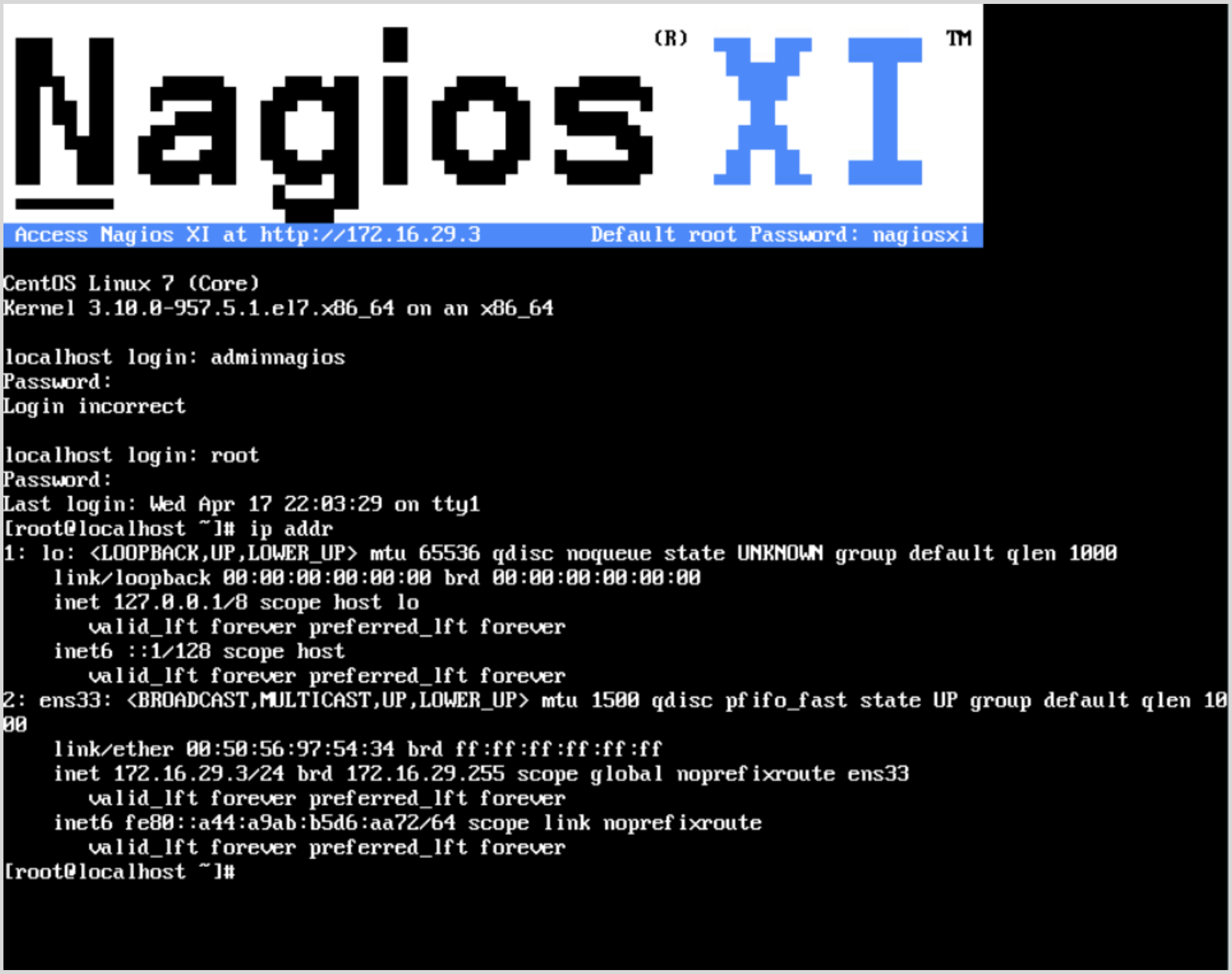


VM Hardware

CPU	2 CPU(s)
Memory	2 GB, 0.64 GB memory active
Hard disk 1	40 GB
Network adapter 1	Private_VLAN_DIF607 ID607 (connected)
CD/DVD drive 1	Disconnected
Floppy drive 1	Disconnected
Video card	16 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 6.5 and later (VM version 13)

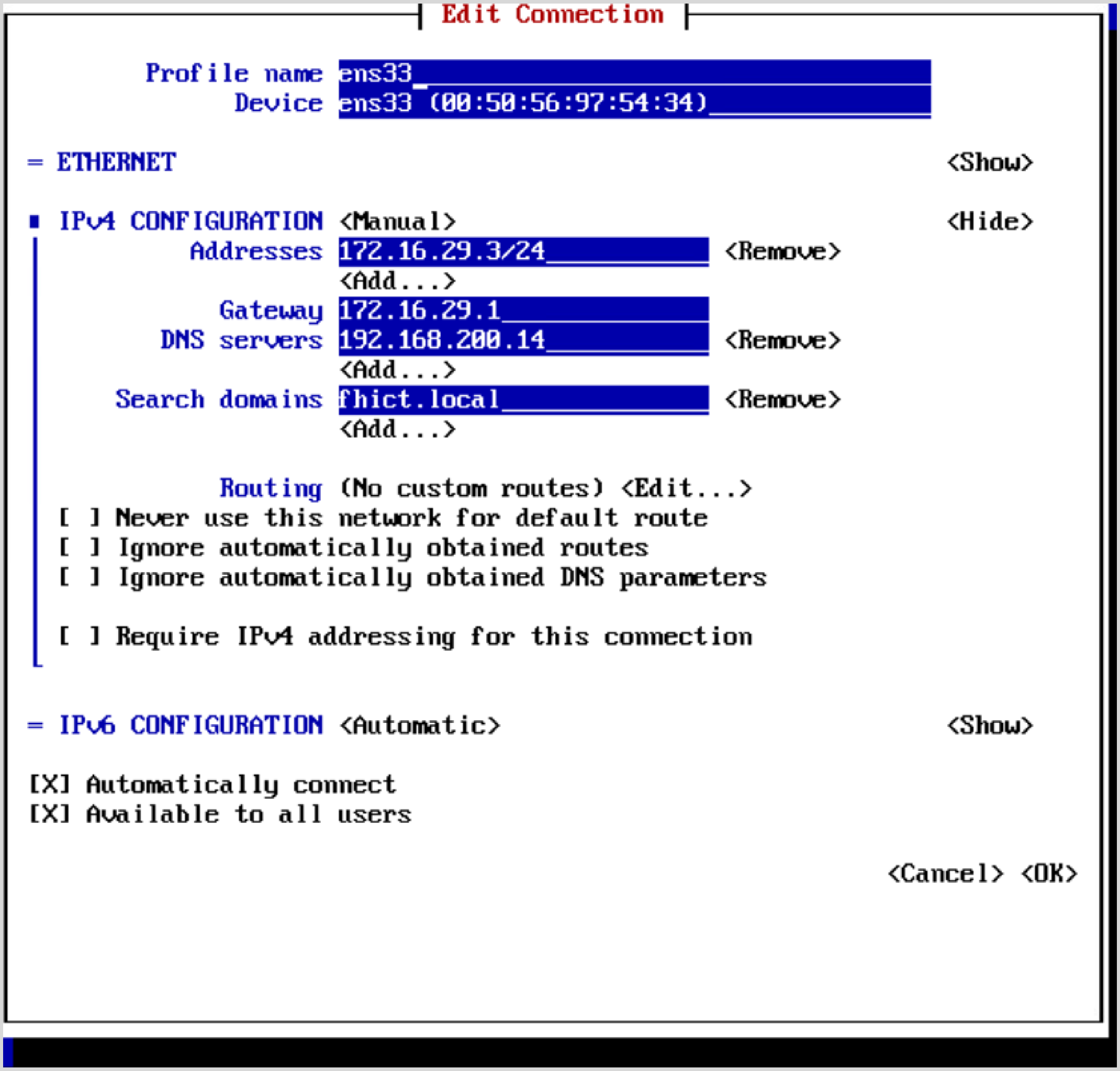
Edit Settings...

3. I started my vm and you will see the IP-address appear in the welcome screen as soon as it has booted. It uses DHCP by default, so I did set it to static by command.:$nmtui edit ens33



```
 Access Nagios XI at http://172.16.29.3         Default root Password: nagiosxi

CentOS Linux 7 (Core)
Kernel 3.10.0-957.5.1.el7.x86_64 on an x86_64

localhost login: adminnagios
Password:
Login incorrect

localhost login: root
Password:
Last login: Wed Apr 17 22:03:29 on tty1
[root@localhost ~]# 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:50:56:97:54:34 brd ff:ff:ff:ff:ff:ff
    inet 172.16.29.3/24 brd 172.16.29.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::a44:a9ab:b5d6:aa72/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@localhost ~]#
```

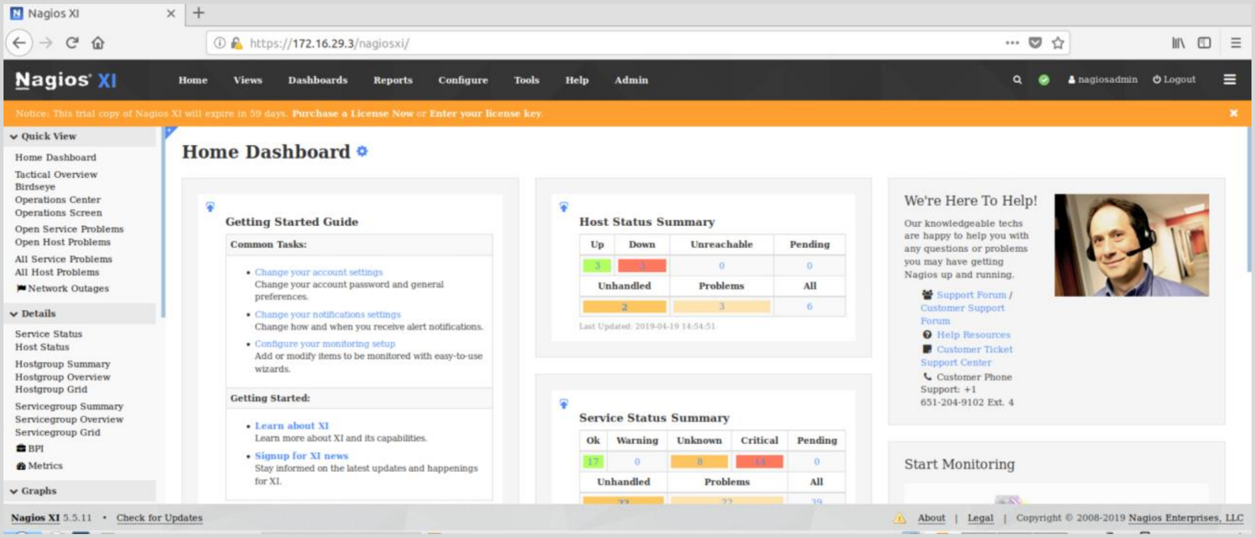
.



```
                     ┤ Edit Connection ├

        Profile name ens33_
              Device ens33 (00:50:56:97:54:34)

= ETHERNET                                              <Show>

■ IPv4 CONFIGURATION <Manual>                            <Hide>
│          Addresses 172.16.29.3/24         <Remove>
│                    <Add...>
│            Gateway 172.16.29.1
│        DNS servers 192.168.200.14         <Remove>
│                    <Add...>
│     Search domains fhict.local            <Remove>
│                    <Add...>
│
│            Routing (No custom routes) <Edit...>
│ [ ] Never use this network for default route
│ [ ] Ignore automatically obtained routes
│ [ ] Ignore automatically obtained DNS parameters
│
│ [ ] Require IPv4 addressing for this connection
└

= IPv6 CONFIGURATION <Automatic>                         <Show>

[X] Automatically connect
[X] Available to all users

                                                   <Cancel> <OK>
```

4. Follow the configuration steps on the web site 172.16.29.3

5. Write down your admin login and password with user name: nagiosxiadmin/password:nagiosxiadmin



Notice: This trial copy of Nagios XI will expire in 59 days. **Purchase a License Now** or **Enter your license key.**

Home Dashboard

Getting Started Guide

Common Tasks:

- Change your account settings
  Change your account password and general preferences.
- Change your notifications settings
  Change how and when you receive alert notifications.
- Configure your monitoring setup
  Add or modify items to be monitored with easy-to-use wizards.

Getting Started:

- **Learn about XI**
  Learn more about XI and its capabilities.
- **Signup for XI news**
  Stay informed on the latest updates and happenings for XI.

Host Status Summary

Up	Down	Unreachable	Pending
3	3	0	0
Unhandled		Problems	All
2		3	6

Last Updated: 2019-04-19 14:54:51

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
17	0	8	14	0
Unhandled		Problems		All
22		22		39

We're Here To Help!

Our knowledgeable techs are happy to help you with any questions or problems you may have getting Nagios up and running.

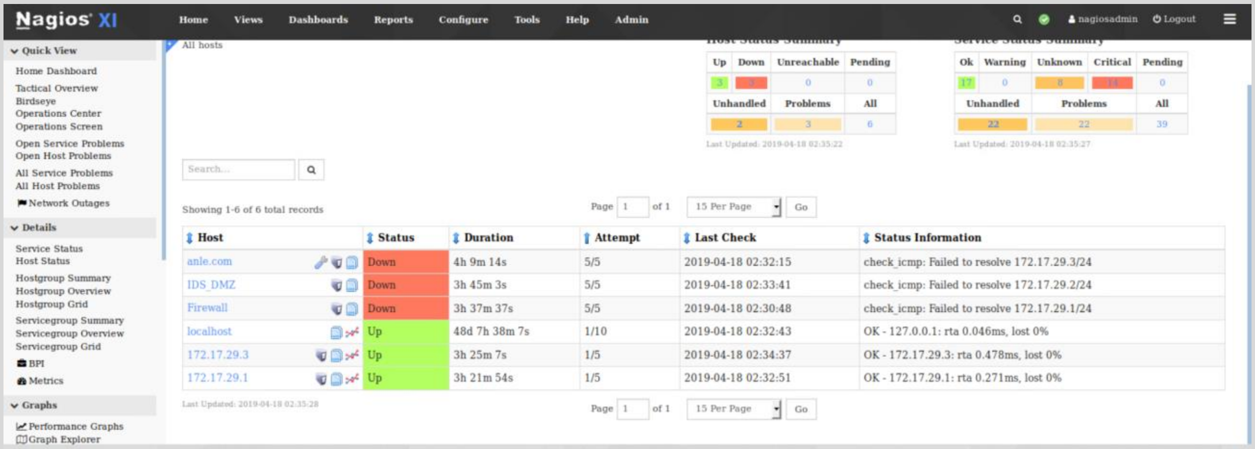
Support Forum / Customer Support Forum
Help Resources
Customer Ticket Support Center
Customer Phone Support: +1 651-204-9102 Ext. 4

Start Monitoring

Nagios XI 5.5.11 • Check for Updates

About | Legal | Copyright © 2008-2019 Nagios Enterprises, LLC

Here is overview of Monitoring after being set up using nagiosXi.



Up	Down	Unreachable	Pending
3	3	0	0
Unhandled		Problems	All
2		3	6

Last Updated: 2019-04-18 02:35:22

Ok	Warning	Unknown	Critical	Pending
17	0	8	14	0
Unhandled		Problems		All
22		22		39

Last Updated: 2019-04-18 02:35:27

Showing 1-6 of 6 total records

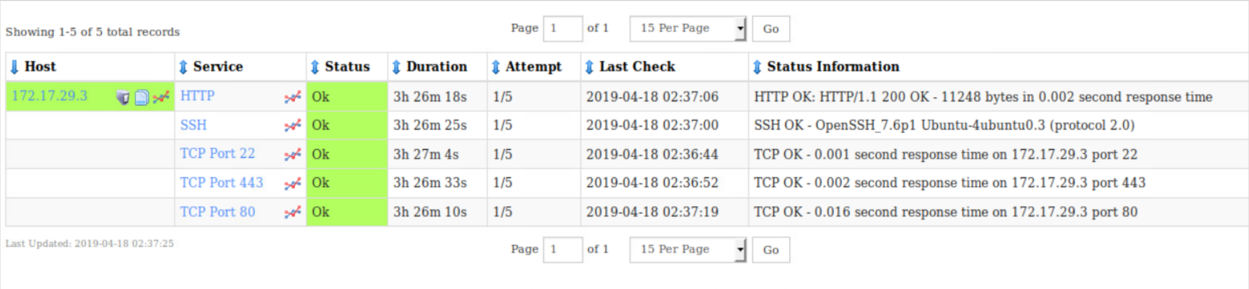
Page 1 of 1 15 Per Page Go

Host	Status	Duration	Attempt	Last Check	Status Information
anle.com	Down	4h 9m 14s	5/5	2019-04-18 02:32:15	check_icmp: Failed to resolve 172.17.29.3/24
IDS_DMZ	Down	3h 45m 3s	5/5	2019-04-18 02:33:41	check_icmp: Failed to resolve 172.17.29.2/24
Firewall	Down	3h 37m 37s	5/5	2019-04-18 02:30:48	check_icmp: Failed to resolve 172.17.29.1/24
localhost	Up	48d 7h 38m 7s	1/10	2019-04-18 02:32:43	OK - 127.0.0.1: rta 0.046ms, lost 0%
172.17.29.3	Up	3h 25m 7s	1/5	2019-04-18 02:34:37	OK - 172.17.29.3: rta 0.478ms, lost 0%
172.17.29.1	Up	3h 21m 54s	1/5	2019-04-18 02:32:51	OK - 172.17.29.1: rta 0.271ms, lost 0%

Last Updated: 2019-04-18 02:35:28

Page 1 of 1 15 Per Page Go

We also can select one of the hosts to see more detail.



Showing 1-5 of 5 total records

Page 1 of 1 15 Per Page Go

Host	Service	Status	Duration	Attempt	Last Check	Status Information
172.17.29.3	HTTP	Ok	3h 26m 18s	1/5	2019-04-18 02:37:06	HTTP OK: HTTP/1.1 200 OK - 11248 bytes in 0.002 second response time
	SSH	Ok	3h 26m 25s	1/5	2019-04-18 02:37:00	SSH OK - OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 (protocol 2.0)
	TCP Port 22	Ok	3h 27m 4s	1/5	2019-04-18 02:36:44	TCP OK - 0.001 second response time on 172.17.29.3 port 22
	TCP Port 443	Ok	3h 26m 33s	1/5	2019-04-18 02:36:52	TCP OK - 0.002 second response time on 172.17.29.3 port 443
	TCP Port 80	Ok	3h 26m 10s	1/5	2019-04-18 02:37:19	TCP OK - 0.016 second response time on 172.17.29.3 port 80

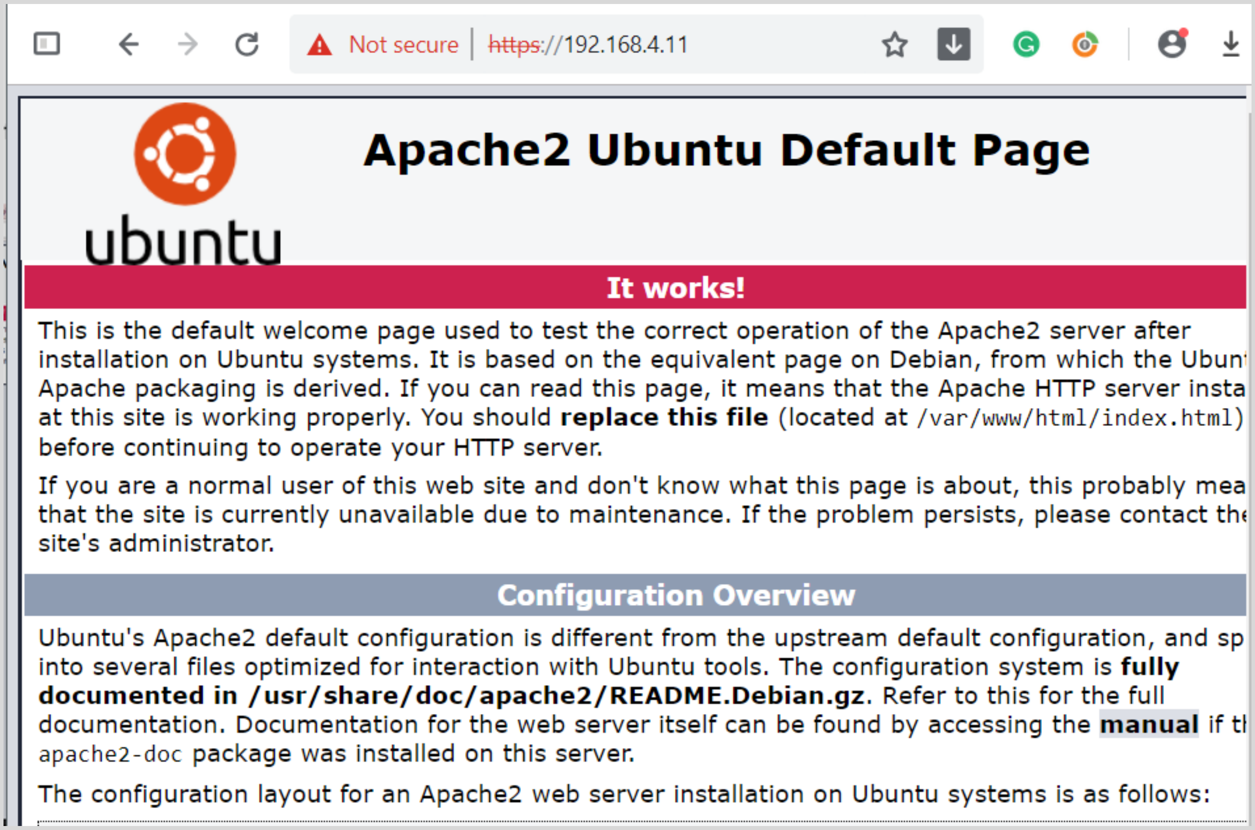
Last Updated: 2019-04-18 02:37:25

Page 1 of 1 15 Per Page Go

IV. Test results

1. Basic function of internal and public functionality/services.

-webserver can be reached from outside.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubun Apache packaging is derived. If you can read this page, it means that the Apache HTTP server insta at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably mea that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

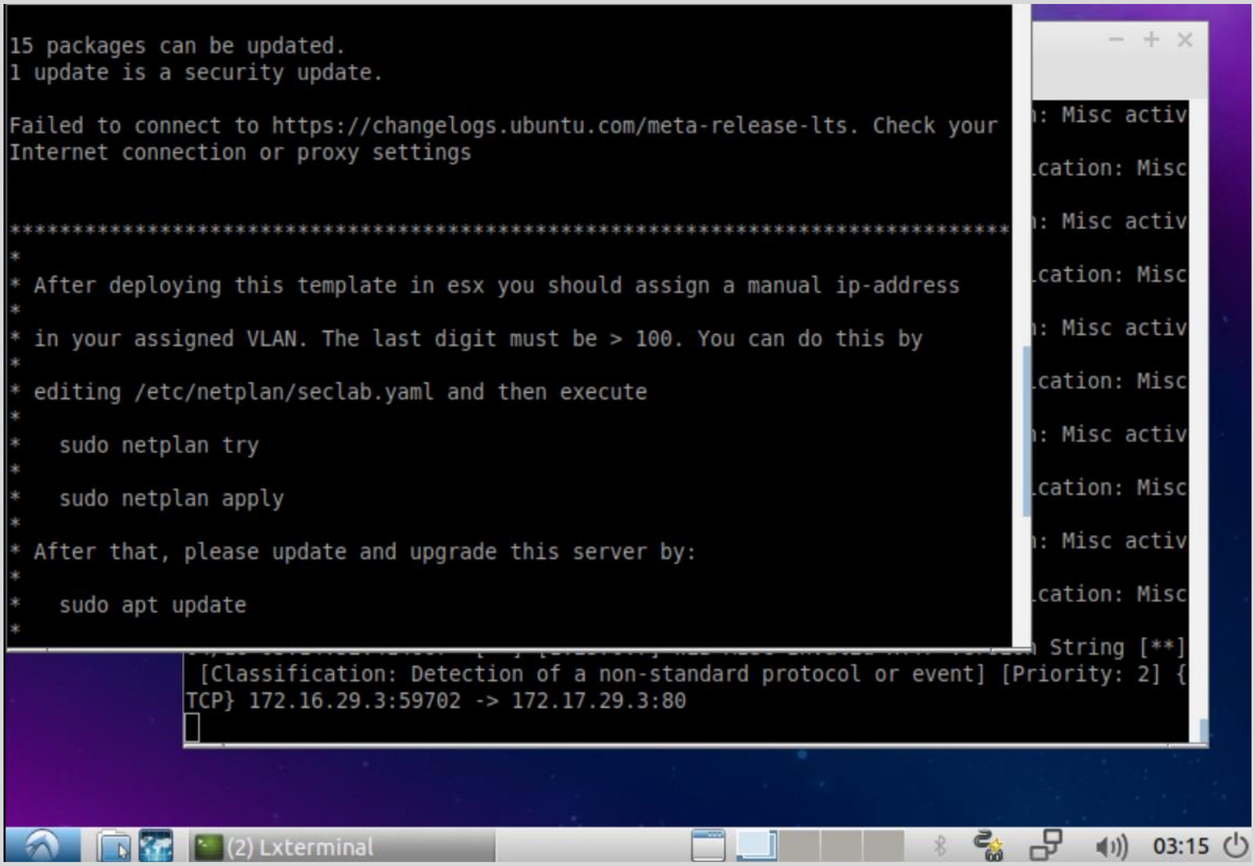
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and sp into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if th `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

2. **SSH Connection Test On Ubuntu WS:**

SSH from LAN to DMZ: ssh 172.17.29.3

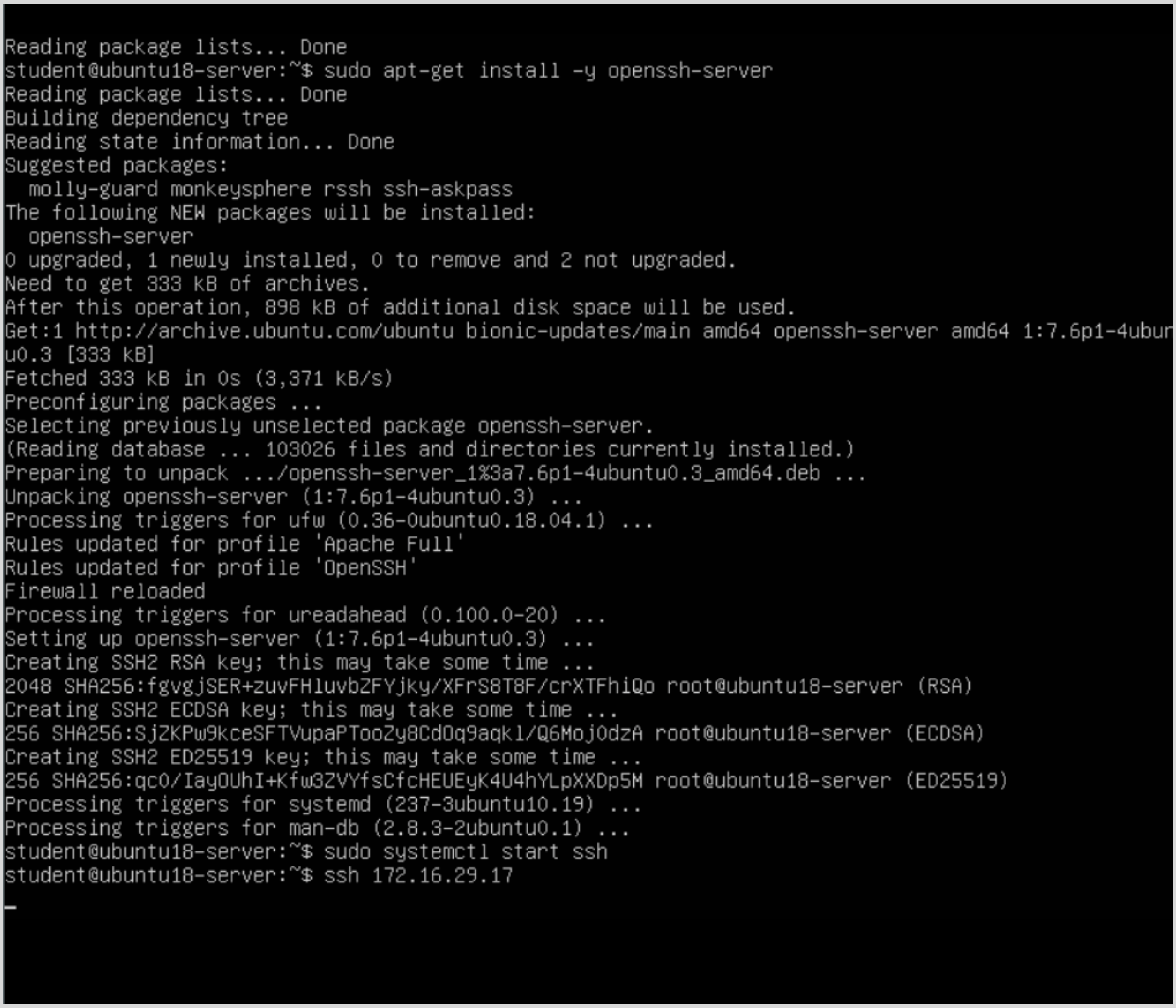
-SSH connection was successfully established with credentials



```
15 packages can be updated.
1 update is a security update.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings


*******************************************************************************
*
* After deploying this template in esx you should assign a manual ip-address
*
* in your assigned VLAN. The last digit must be > 100. You can do this by
*
* editing /etc/netplan/seclab.yaml and then execute
*
*   sudo netplan try
*
*   sudo netplan apply
*
* After that, please update and upgrade this server by:
*
*   sudo apt update
*
```

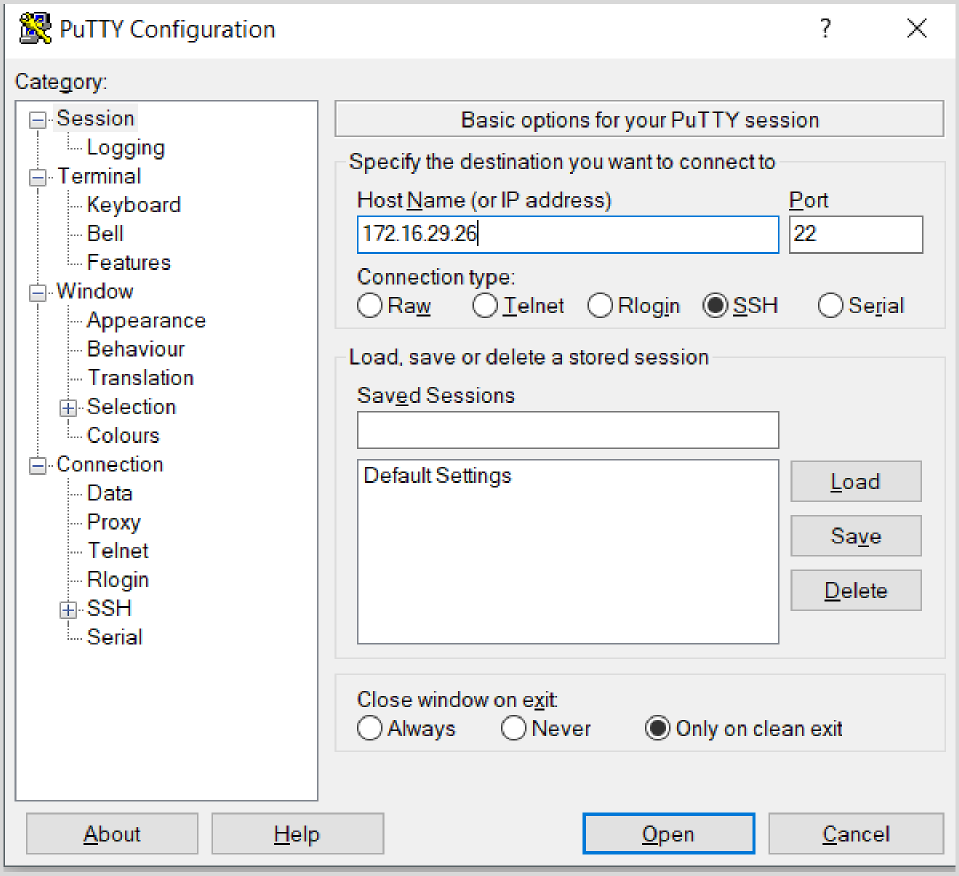
```
: Misc activ
.cation: Misc
: Misc activ
.cation: Misc
: Misc activ
.cation: Misc
: Misc activ
.cation: Misc
: Misc activ
.cation: Misc
 String [**]
 [Classification: Detection of a non-standard protocol or event] [Priority: 2] {
TCP} 172.16.29.3:59702 -> 172.17.29.3:80
```

SSH connection was block by PFSense, as a result, there was no reply from LAN workstation or any connection was established.



```
Reading package lists... Done
student@ubuntu18-server:~$ sudo apt-get install -y openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass
The following NEW packages will be installed:
  openssh-server
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 333 kB of archives.
After this operation, 898 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-server amd64 1:7.6p1-4ubun
u0.3 [333 kB]
Fetched 333 kB in 0s (3,371 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openssh-server.
(Reading database ... 103026 files and directories currently installed.)
Preparing to unpack .../openssh-server_1%3a7.6p1-4ubuntu0.3_amd64.deb ...
Unpacking openssh-server (1:7.6p1-4ubuntu0.3) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.1) ...
Rules updated for profile 'Apache Full'
Rules updated for profile 'OpenSSH'
Firewall reloaded
Processing triggers for ureadahead (0.100.0-20) ...
Setting up openssh-server (1:7.6p1-4ubuntu0.3) ...
Creating SSH2 RSA key; this may take some time ...
2048 SHA256:fgvgjSER+zuvFHluvbZFYjky/XFrS8T8F/crXTFhiQo root@ubuntu18-server (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:SjZKPw9kceSFTVupaPTooZy8CdOq9aqkl/Q6MojOdzA root@ubuntu18-server (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:qcO/IayOUhI+Kfw3ZVYfsCfcHEUEyK4U4hYLpXXDp5M root@ubuntu18-server (ED25519)
Processing triggers for systemd (237-3ubuntu10.19) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
student@ubuntu18-server:~$ sudo systemctl start ssh
student@ubuntu18-server:~$ ssh 172.16.29.17
_
```

SSH Connection Test On my window laptop:



Specify the destination you want to connect to

Host Name (or IP address): 172.16.29.26

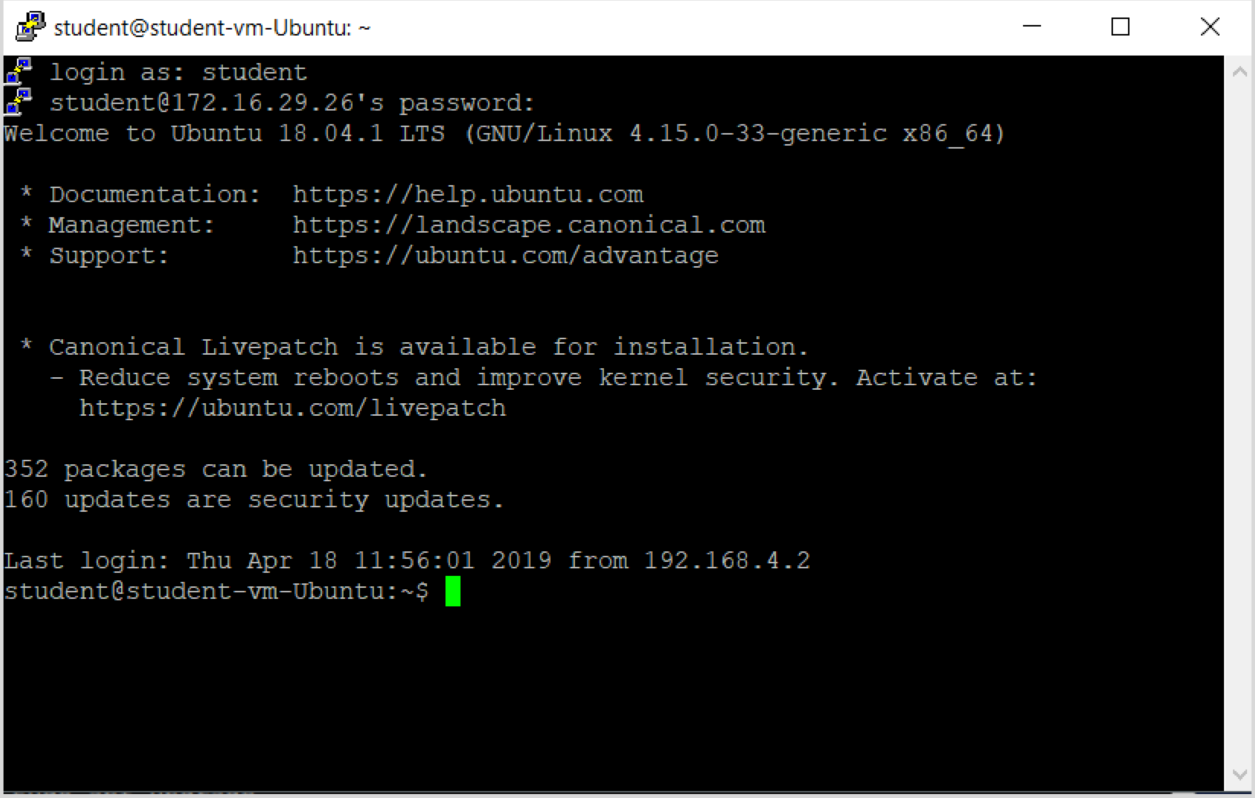
Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions:

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

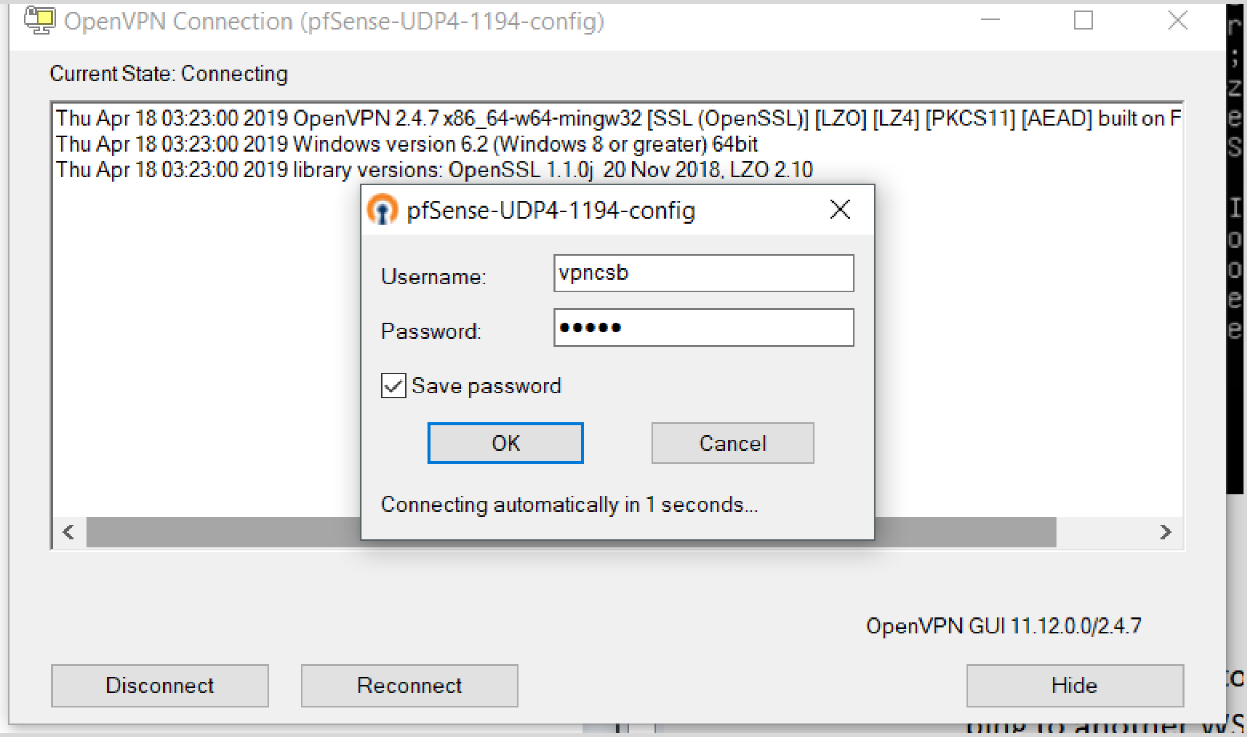


```
  login as: student
  student@172.16.29.26's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-33-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

352 packages can be updated.
160 updates are security updates.

Last login: Thu Apr 18 11:56:01 2019 from 192.168.4.2
student@student-vm-Ubuntu:~$
```

3. VPN access

I use my own laptop to test. The goal of this test is to check If a successfully VPN client can ping to another WS after log in with SSH.

-Connected VPN user with username:vpncsb/pass:admin



Current State: Connecting

```
Thu Apr 18 03:23:00 2019 OpenVPN 2.4.7 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] [AEAD] built on F
Thu Apr 18 03:23:00 2019 Windows version 6.2 (Windows 8 or greater) 64bit
Thu Apr 18 03:23:00 2019 library versions: OpenSSL 1.1.0j  20 Nov 2018, LZO 2.10
```

Username: vpncsb

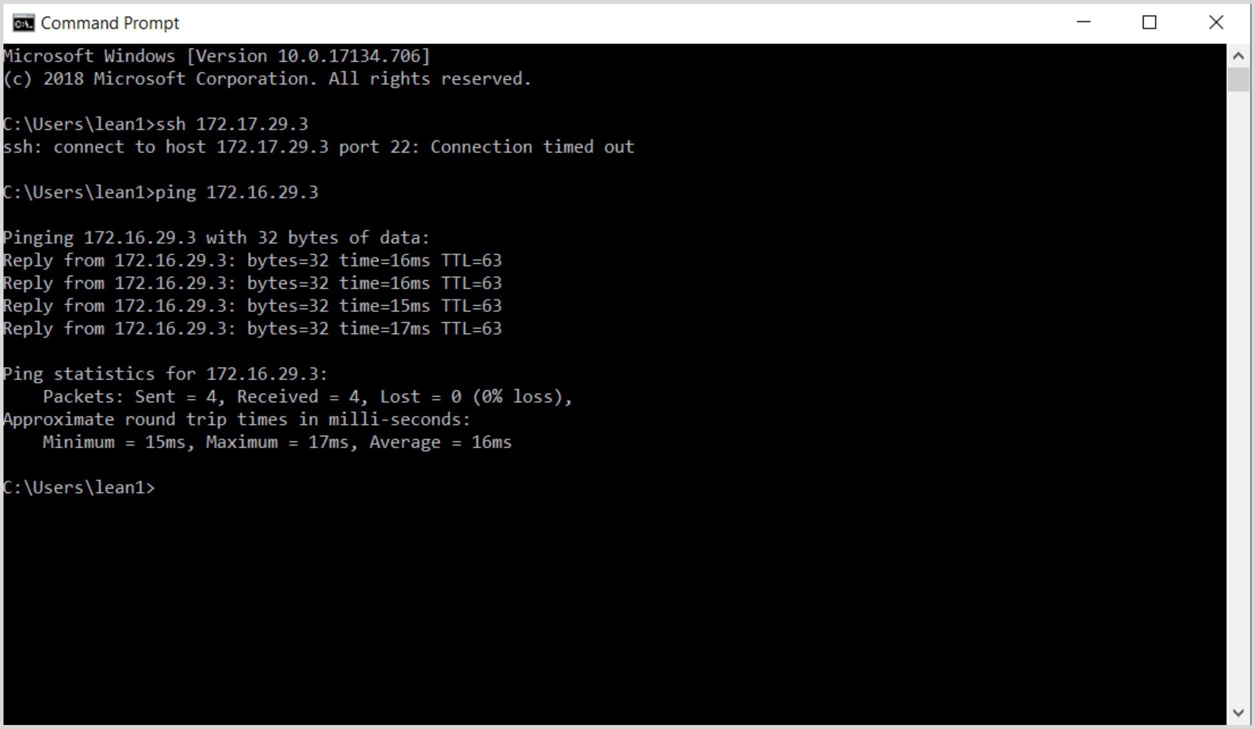
Password: •••••

☑ Save password

Connecting automatically in 1 seconds...

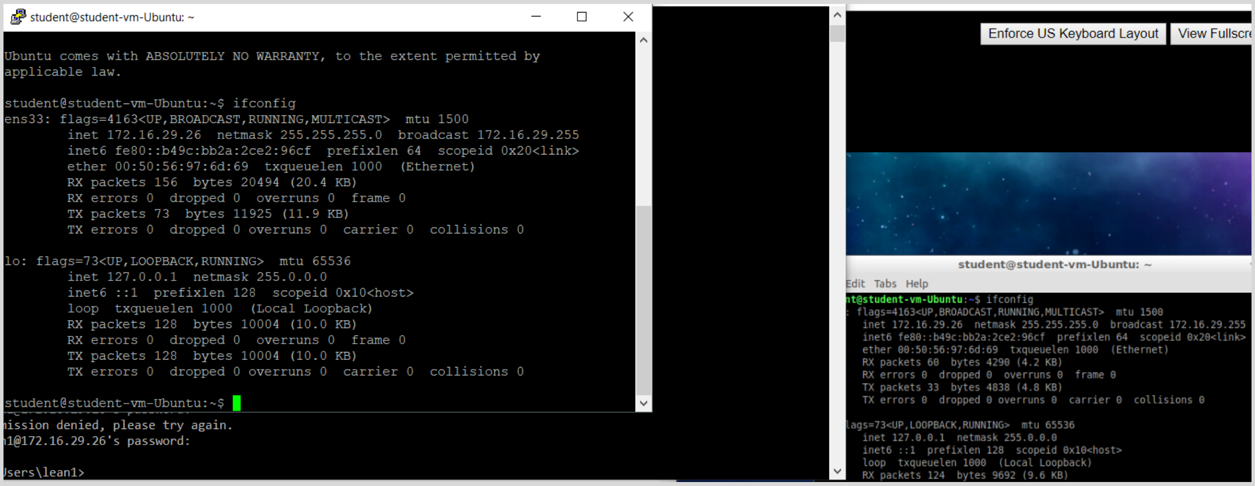
OpenVPN GUI 11.12.0.0/2.4.7

-Ping ws machine



```
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\lean1>ssh 172.17.29.3
ssh: connect to host 172.17.29.3 port 22: Connection timed out

C:\Users\lean1>ping 172.16.29.3

Pinging 172.16.29.3 with 32 bytes of data:
Reply from 172.16.29.3: bytes=32 time=16ms TTL=63
Reply from 172.16.29.3: bytes=32 time=16ms TTL=63
Reply from 172.16.29.3: bytes=32 time=15ms TTL=63
Reply from 172.16.29.3: bytes=32 time=17ms TTL=63

Ping statistics for 172.16.29.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 17ms, Average = 16ms

C:\Users\lean1>
```

-SSH work station from my computer by Putty


student@student-vm-Ubuntu: ~
Enforce US Keyboard Layout
View Fullscre
student@student-vm-Ubuntu: ~
Edit
Tabs
Help

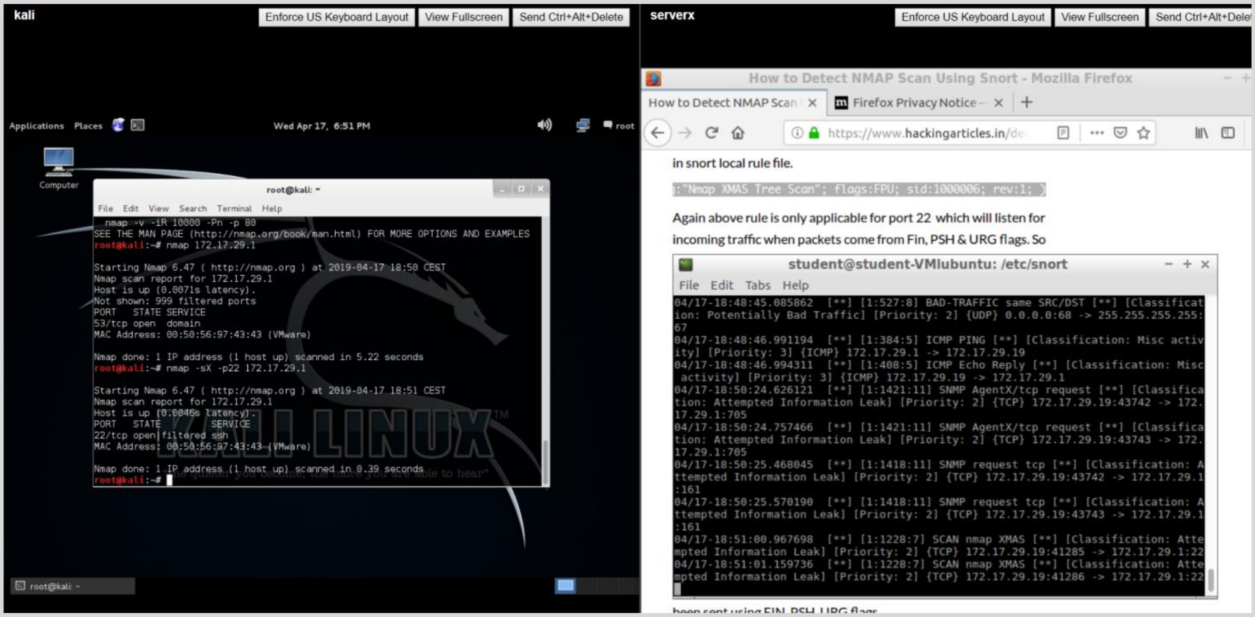
```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

student@student-vm-Ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.29.26  netmask 255.255.255.0  broadcast 172.16.29.255
        inet6 fe80::b49c:bb2a:2ce2:96cf  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:97:6d:69  txqueuelen 1000  (Ethernet)
        RX packets 156  bytes 20494 (20.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 73  bytes 11925 (11.9 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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 128  bytes 10004 (10.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 128  bytes 10004 (10.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

student@student-vm-Ubuntu:~$
```

```
nission denied, please try again.
n1@172.16.29.26's password:

Jsers\lean1>
```

```
nt@student-vm-Ubuntu:~$ ifconfig
: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
   inet 172.16.29.26  netmask 255.255.255.0  broadcast 172.16.29.255
   inet6 fe80::b49c:bb2a:2ce2:96cf  prefixlen 64  scopeid 0x20<link>
   ether 00:50:56:97:6d:69  txqueuelen 1000  (Ethernet)
   RX packets 60  bytes 4290 (4.2 KB)
   RX errors 0  dropped 0  overruns 0  frame 0
   TX packets 33  bytes 4838 (4.8 KB)
   TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lags=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 124  bytes 9692 (9.6 KB)
```

4. IDS Functioning

IDS detected that this attacker is trying to scan all available ports from any active machine in my network.



```
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap 172.17.29.1

Starting Nmap 6.47 ( http://nmap.org ) at 2019-04-17 18:50 CEST
Nmap scan report for 172.17.29.1
Host is up (0.0071s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:97:43:43 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.22 seconds
root@kali:~# nmap -sX -p22 172.17.29.1

Starting Nmap 6.47 ( http://nmap.org ) at 2019-04-17 18:51 CEST
Nmap scan report for 172.17.29.1
Host is up (0.0046s latency).
PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 00:50:56:97:43:43 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
root@kali:~#
```

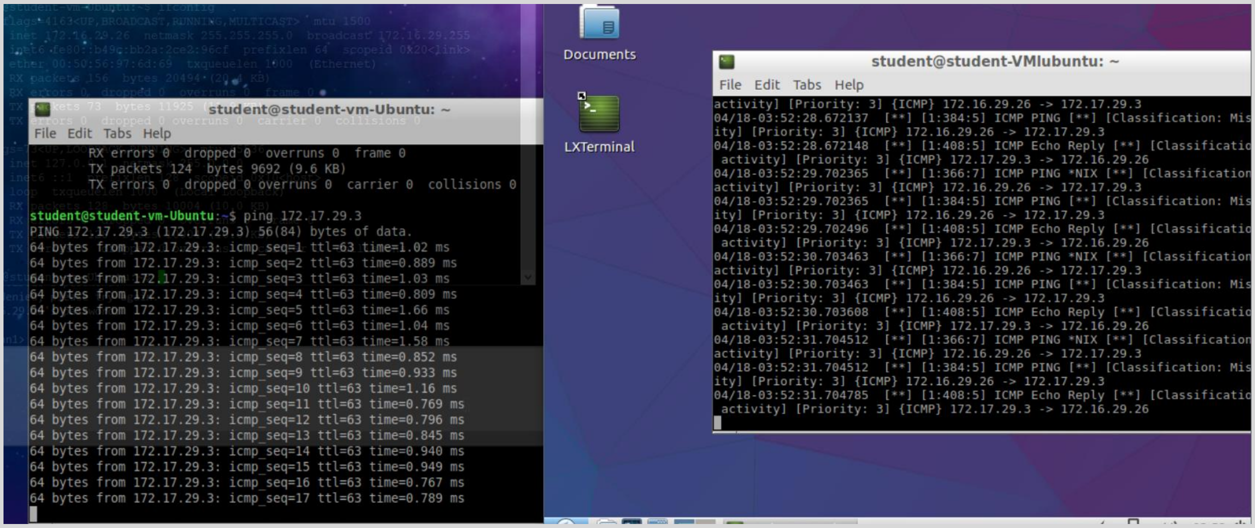
in snort local rule file.

```
:"Nmap XMAS Tree Scan"; flags:FPU; sid:1000006; rev:1; )
```

Again above rule is only applicable for port 22 which will listen for incoming traffic when packets come from Fin, PSH & URG flags. So

```
04/17-18:48:45.085862  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
04/17-18:48:46.991194  [**] [1:384:5] ICMP PING [**] [Classification: Misc activ
ity] [Priority: 3] {ICMP} 172.17.29.1 -> 172.17.29.19
04/17-18:48:46.994311  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc
 activity] [Priority: 3] {ICMP} 172.17.29.19 -> 172.17.29.1
04/17-18:50:24.626121  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 172.17.29.19:43742 -> 172.
17.29.1:705
04/17-18:50:24.757466  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 172.17.29.19:43743 -> 172.
17.29.1:705
04/17-18:50:25.468045  [**] [1:1418:11] SNMP request tcp [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 172.17.29.19:43742 -> 172.17.29.1
:161
04/17-18:50:25.570190  [**] [1:1418:11] SNMP request tcp [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 172.17.29.19:43743 -> 172.17.29.1
:161
04/17-18:51:00.967698  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 172.17.29.19:41285 -> 172.17.29.1:22
04/17-18:51:01.159736  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 172.17.29.19:41286 -> 172.17.29.1:22
```

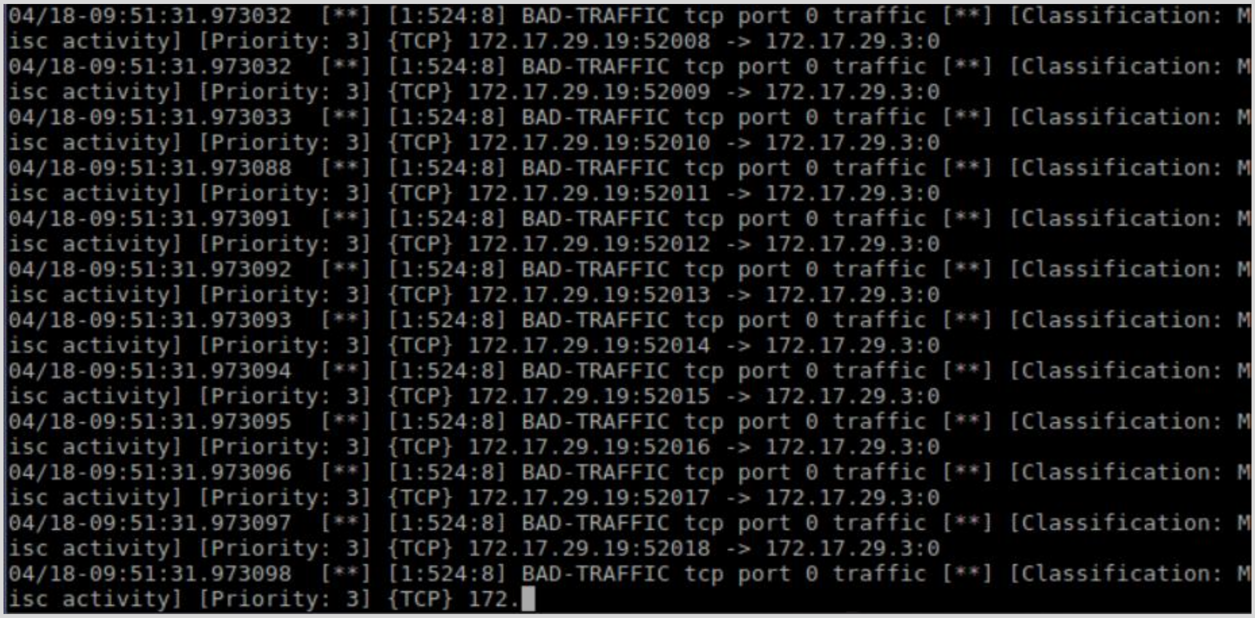
When I try to ping from LAN to DMZ, IDS also detected it.



```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 124  bytes 9692 (9.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

student@student-vm-Ubuntu:~$ ping 172.17.29.3
PING 172.17.29.3 (172.17.29.3) 56(84) bytes of data.
64 bytes from 172.17.29.3: icmp_seq=1 ttl=63 time=1.02 ms
64 bytes from 172.17.29.3: icmp_seq=2 ttl=63 time=0.889 ms
64 bytes from 172.17.29.3: icmp_seq=3 ttl=63 time=1.03 ms
64 bytes from 172.17.29.3: icmp_seq=4 ttl=63 time=0.809 ms
64 bytes from 172.17.29.3: icmp_seq=5 ttl=63 time=1.66 ms
64 bytes from 172.17.29.3: icmp_seq=6 ttl=63 time=1.04 ms
64 bytes from 172.17.29.3: icmp_seq=7 ttl=63 time=1.58 ms
64 bytes from 172.17.29.3: icmp_seq=8 ttl=63 time=0.852 ms
64 bytes from 172.17.29.3: icmp_seq=9 ttl=63 time=0.933 ms
64 bytes from 172.17.29.3: icmp_seq=10 ttl=63 time=1.16 ms
64 bytes from 172.17.29.3: icmp_seq=11 ttl=63 time=0.769 ms
64 bytes from 172.17.29.3: icmp_seq=12 ttl=63 time=0.796 ms
64 bytes from 172.17.29.3: icmp_seq=13 ttl=63 time=0.845 ms
64 bytes from 172.17.29.3: icmp_seq=14 ttl=63 time=0.940 ms
64 bytes from 172.17.29.3: icmp_seq=15 ttl=63 time=0.949 ms
64 bytes from 172.17.29.3: icmp_seq=16 ttl=63 time=0.767 ms
64 bytes from 172.17.29.3: icmp_seq=17 ttl=63 time=0.789 ms
```

```
activity] [Priority: 3] {ICMP} 172.16.29.26 -> 172.17.29.3
04/18-03:52:28.672137  [**] [1:384:5] ICMP PING [**] [Classification: Mis
ity] [Priority: 3] {ICMP} 172.16.29.26 -> 172.17.29.3
04/18-03:52:28.672148  [**] [1:408:5] ICMP Echo Reply [**] [Classificatio
 activity] [Priority: 3] {ICMP} 172.17.29.3 -> 172.16.29.26
04/18-03:52:29.702365  [**] [1:366:7] ICMP PING *NIX [**] [Classification
activity] [Priority: 3] {ICMP} 172.16.29.26 -> 172.17.29.3
04/18-03:52:29.702365  [**] [1:384:5] ICMP PING [**] [Classification: Mis
ity] [Priority: 3] {ICMP} 172.16.29.26 -> 172.17.29.3
04/18-03:52:29.702496  [**] [1:408:5] ICMP Echo Reply [**] [Classificatio
 activity] [Priority: 3] {ICMP} 172.17.29.3 -> 172.16.29.26
04/18-03:52:30.703463  [**] [1:366:7] ICMP PING *NIX [**] [Classification
activity] [Priority: 3] {ICMP} 172.16.29.26 -> 172.17.29.3
04/18-03:52:30.703463  [**] [1:384:5] ICMP PING [**] [Classification: Mis
ity] [Priority: 3] {ICMP} 172.16.29.26 -> 172.17.29.3
04/18-03:52:30.703608  [**] [1:408:5] ICMP Echo Reply [**] [Classificatio
 activity] [Priority: 3] {ICMP} 172.17.29.3 -> 172.16.29.26
04/18-03:52:31.704512  [**] [1:366:7] ICMP PING *NIX [**] [Classification
activity] [Priority: 3] {ICMP} 172.16.29.26 -> 172.17.29.3
04/18-03:52:31.704512  [**] [1:384:5] ICMP PING [**] [Classification: Mis
ity] [Priority: 3] {ICMP} 172.16.29.26 -> 172.17.29.3
04/18-03:52:31.704785  [**] [1:408:5] ICMP Echo Reply [**] [Classificatio
 activity] [Priority: 3] {ICMP} 172.17.29.3 -> 172.16.29.26
```

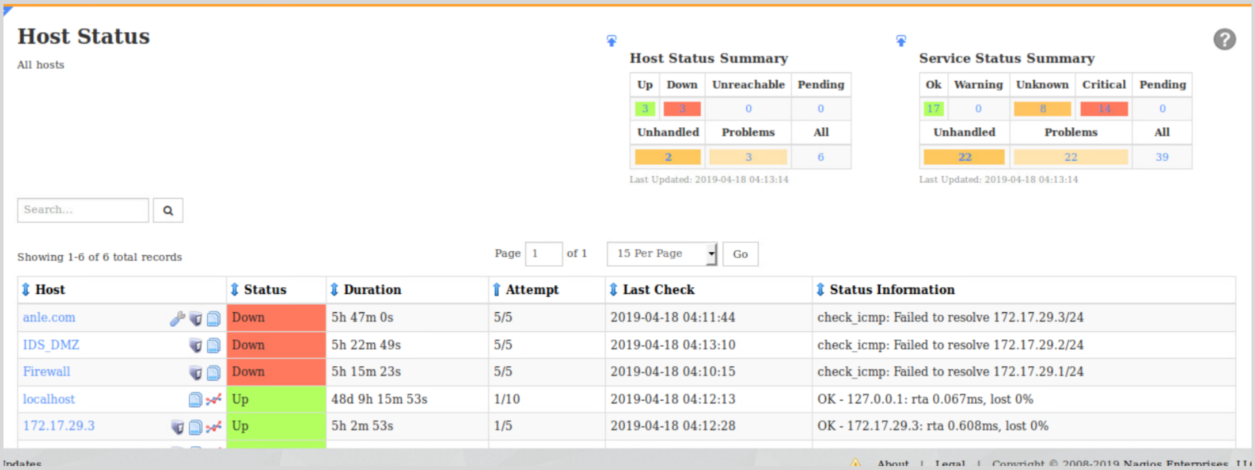
IDS also can detect Ddos attack from another workstation.



```
04/18-09:51:31.973032  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.17.29.19:52008 -> 172.17.29.3:0
04/18-09:51:31.973032  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.17.29.19:52009 -> 172.17.29.3:0
04/18-09:51:31.973033  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.17.29.19:52010 -> 172.17.29.3:0
04/18-09:51:31.973088  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.17.29.19:52011 -> 172.17.29.3:0
04/18-09:51:31.973091  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.17.29.19:52012 -> 172.17.29.3:0
04/18-09:51:31.973092  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.17.29.19:52013 -> 172.17.29.3:0
04/18-09:51:31.973093  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.17.29.19:52014 -> 172.17.29.3:0
04/18-09:51:31.973094  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.17.29.19:52015 -> 172.17.29.3:0
04/18-09:51:31.973095  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.17.29.19:52016 -> 172.17.29.3:0
04/18-09:51:31.973096  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.17.29.19:52017 -> 172.17.29.3:0
04/18-09:51:31.973097  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.17.29.19:52018 -> 172.17.29.3:0
04/18-09:51:31.973098  [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: M
isc activity] [Priority: 3] {TCP} 172.
```

5. IT Monitoring

- Host status



Host Status

All hosts

Host Status Summary

Up	Down	Unreachable	Pending
3	3	0	0

Unhandled	Problems	All
2	3	6

Last Updated: 2019-04-18 04:13:14

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
17	0	8	14	0

Unhandled	Problems	All
22	22	39

Last Updated: 2019-04-18 04:13:14

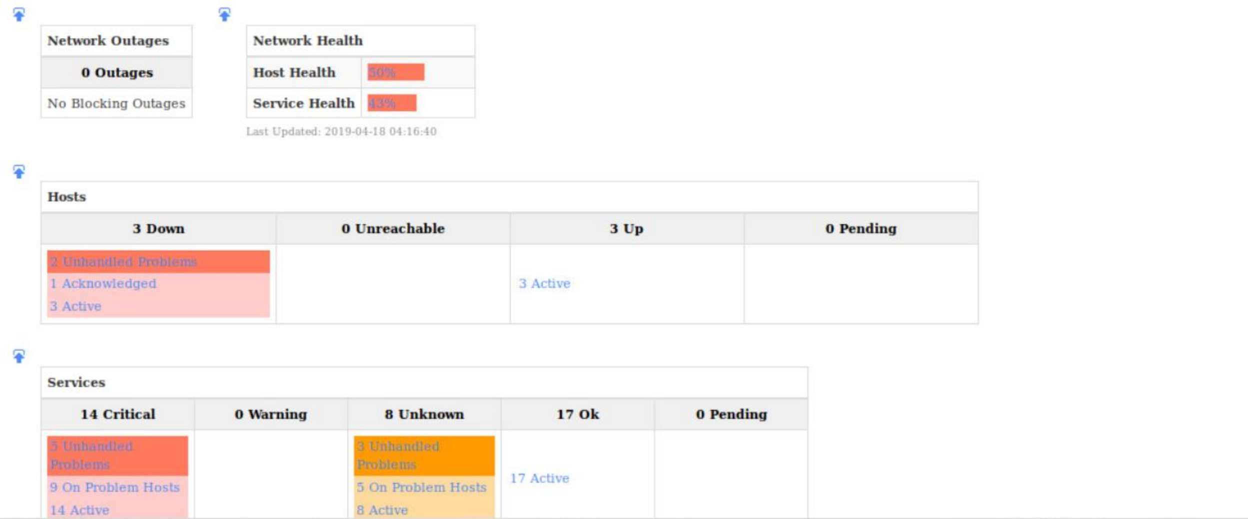
Showing 1-6 of 6 total records

Host	Status	Duration	Attempt	Last Check	Status Information
anle.com	Down	5h 47m 0s	5/5	2019-04-18 04:11:44	check_icmp: Failed to resolve 172.17.29.3/24
IDS_DMZ	Down	5h 22m 49s	5/5	2019-04-18 04:13:10	check_icmp: Failed to resolve 172.17.29.2/24
Firewall	Down	5h 15m 23s	5/5	2019-04-18 04:10:15	check_icmp: Failed to resolve 172.17.29.1/24
localhost	Up	48d 9h 15m 53s	1/10	2019-04-18 04:12:13	OK - 127.0.0.1: rta 0.067ms, lost 0%
172.17.29.3	Up	5h 2m 53s	1/5	2019-04-18 04:12:28	OK - 172.17.29.3: rta 0.608ms, lost 0%

Updates
About | Legal | Copyright © 2008-2019 Nagios Enterprises, LL

From here, you can see all the report of each host (status, duration, and attempt).

- View



Network Outages
0 Outages
No Blocking Outages

Network Health	
Host Health	50%
Service Health	43%

Last Updated: 2019-04-18 04:16:40

Hosts

3 Down	0 Unreachable	3 Up	0 Pending
2 Unhandled Problems 1 Acknowledged 3 Active		3 Active	

Services

14 Critical	0 Warning	8 Unknown	17 Ok	0 Pending
5 Unhandled Problems 9 On Problem Hosts 14 Active		3 Unhandled Problems 5 On Problem Hosts 8 Active	17 Active	

In this page, it shows an overview of what problems for the system.

V. Overall Conclusion

1. Level of security for the company

In fact, I have to admit that my design is not strong enough to be applied to big companies but that is all I can do with my knowledge. I think that to help increase security, I will design 2 firewalls instead of 1 firewall and apply more encryption methods.

2. The help of system against the analyzed risks

I designed a system with 2 separated networks that contains one DMZ network which has a webserver. IDS in DMZ as well as in Private are always running to notify security breaches immediately. Furthermore, the Webserver is always up and working completely separated with private LAN network.

My private LAN is designed to be reached only via WS (from private LAN network) or users from home using VPN connections. However, the main thing of security in my network is firewall which is configured to block all traffic from DMZ to LAN that makes sure LAN network is private.

3. Advice for remaining improvement of the security for the company

As I have analyzed the possible cases with the company's system. Currently DDOS, SQL injection though are old methods but they are still used by hackers to steal information so I want to give advice to the company

- Always update the highest security mode.

- Always scan for viruses with files downloaded from outside to the company.

VI. Reflection

Overview

This is really a huge challenge for me. All new and quite complicated for a freshman, I had to really try to be able to complete my portfolio. But I myself realized that what I learned was worthwhile, it gave me a better overview of cybersecurity and also helped me to orient my career.

Difficulties

The first difficulty was that I was completely overwhelmed because there were so many documents to read, there were so many things to find out that made everything ambiguous. During the practice, I encountered a lot of errors about the system such as unable to install static ip, vpn installation error or firewall that did not work. These things take me a lot of time to fix.

Conclusion

I have completed my portfolio based on my friends' help through classroom practice, and teacher advice as well as my mentor. Extremely enthusiastic teachers and mentors answer my questions via email as well as in class, which saves me a lot of time.

Reference

https://www.owasp.org/index.php/Intrusion_Detection

https://www.cyber.gov.au/publications/network-segmentation-and-segregation

https://portal.fhict.nl/Studentenplein/LMC/1819vj/Cyber%20Security/CSB/01_Network-Separation-and-filtering/Workshop01-%20firewall%20practical%202018%20v1.1.pdf

http://www.ciscopress.com/articles/article.asp?p=1218144&seqNum=4

https://www.simplified.guide/ubuntu/install-ssh-server

https://portal.fhict.nl/Studentenplein/LMC/1819vj/Cyber%20Security/CSB/02_Secure-Connections-and-VPN/Assignment%201.pdf

https://portal.fhict.nl/Studentenplein/LMC/1819vj/Cyber%20Security/CSB/02_Secure-Connections-and-VPN/Assignment%202.pdf

https://portal.fhict.nl/Studentenplein/LMC/1819vj/Cyber%20Security/CSB/02_Secure-Connections-and-VPN/Assignment%203.pdf

https://portal.fhict.nl/Studentenplein/LMC/1819vj/Cyber%20Security/CSB/03_Intrusion-Detection/IDS%20basic%20setup%202018.pdf

https://portal.fhict.nl/Studentenplein/LMC/1819vj/Cyber%20Security/CSB/04_IT-Monitoring/Easy%20Start%20with%20Nagios%20XI%202019.pdf

https://www.compuquip.com/blog/the-different-types-of-firewall-architectures