Networking Course Work

NETWORK UPGRADE AND PYTHON PACKET SNIFFER

AHMED F MAHMOUD – CU2000512

Introduction and expected learning outcomes

This coursework is divided into 2 tasks the first is to update an existing network. And the second task is to use python to create a packet sniffer. I believe after completing this course work, I will gain a deeper understanding of packet switching, learn how to configure networks, and apply network security protocols.

Tools

For the first part of the course work, the main network tool that I used in this coursework is GNS3. the reason I choose GNS 3 over other network simulation tools is gns3 virtualizes the network which means that every device on the network is using actual resources (RAM, Storage, CPU). However, other software like cisco packet tracer for example simulates the network which means that the network is not real hence the name simulation. The bellow figure shows all the main difference between the GNS3 and cisco packet tracer. For the second part of the coursework, I used python and imported a library called Sockets to create the program.

Features	GNS 3	Cisco Packet Tracer
Network type	Virtual networks	Simulated networks
Virtual machine integration	VMware or Virtual box	Not supported
Custom iso	Download any custom device (Fortinet, F5, Cisco)	Only cisco devices
Wireshark integration	supported	Not supported
Eases of use	Not very easy to setup and a lot of bugs	Very easy to setup runs smoothly with no bugs

As for the second part of the course work, I used python as it is a high-level programing language and very user friendly. I also Imported 2 libraries to help me create the packet sniffer the first is the sockets library and the second is the struct library.

Scenario

For the first part of the project, I assumed that I was working as a network administrator for a startup named MyFin Tech. After the spread of corona virus, I was asked by the CEO to upgrade the network to allow employees to work from home. I was also asked to implement security protocols that allow for confidentiality, integrity, and availability of the system.

MyFin Tech

Table of Contents

Task one

The next few pages are the proposal. As mentioned earlier, I assumed that I created this proposal while working for MyFin Tech

.

MyFin Tech

Date: 12/10/2021
Task 1

MyFin Tech

Network Upgrades Proposal

Prepared by: Ahmed.farouk@MyFin-Tech.com

MyFin Tech

Date: 12/10/2021
Task 1

Project outline

MyFinTech wishes to upgrade their facility located at fifth settlement, New Cairo, Cairo, Egypt. This upgrade will not only allow MyFin Techs' employees to gain uninterrupted remote access to the network, but also upgrade the current security protocols. To accomplish these goals, I propose the following.

Objectives	Network Upgrade	Network security	Allow for remote access
Tasks	. Redesign the network (2 tier design) . Enable STP protocol . Implement EtherChannel . Implement (Virtual local area networks) . Inter V-lan routing	. MAC address table attacks . VLAN Hopping Attacks . STP Attacks . ARP Attacks . Configuring the Firewall . Configuring the IPS . Configuring SSL . implement extra security recommendations	. Install VPN server . Update the firewall to allow certain traffic

Specifically, I recommend the installation of the following products which will meet My FinTech's current needs while also allowing for future expansion.

- FortiGate-6501F
- Cisco SG350-28P

Pricing

Name	Price	QTY	Subtotal
FortiGate-6501F	2,545.00	1	$2,545.00
Cisco SG350-28P	800	1	$800.00
Total			$3,345.00

Installation and Implementation

Phase	Duration
Hardware Positioning	7 days
Device Installation and configuration	2 days
Implementing network security	4 days
Implementing web application security	3 days

Acceptance

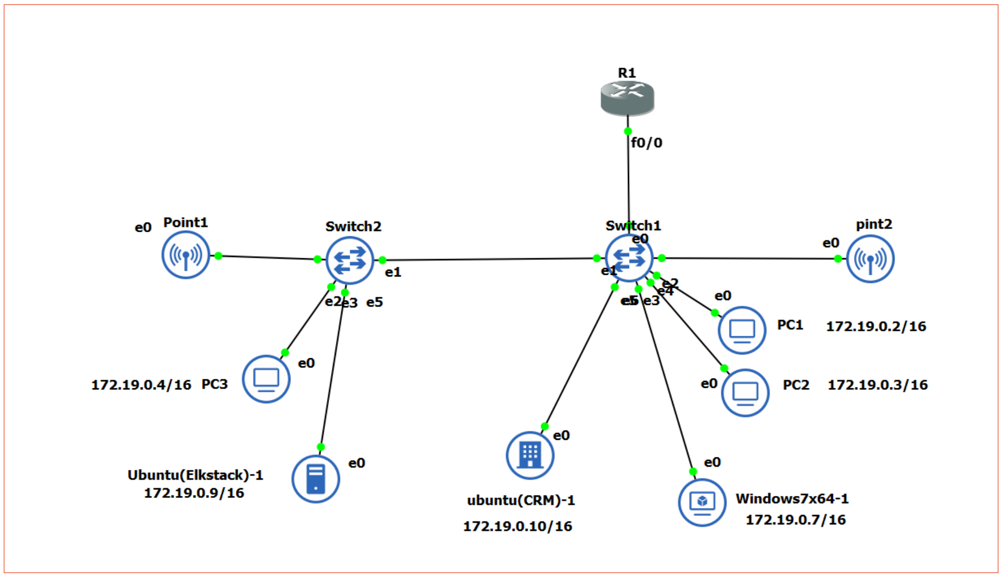
Please sign and date this proposal to indicate your acceptance of the **pricing**, and **Installation/ Implementation** indicated above.

Signature _______________ Date _______________

Network Upgrades

- Since I used GNS3 I was able to configure everything in the proposal starting from the V-Lans to the VPN server.
- In general, the more devices you add the more redundancy you have in the network. However, In the proposal above I added 2 new devices only because as it is stated in the course work that the company's network is small (startup). and the budget would not allow for more devices to be added.
- The reason I choose FortiGate-6501F is that it is a very powerful firewall that has an intrusion prevention system (IPS) built in, allows for client to site VPN, has a graphical user interface (easier configuration), can do the router's job (routing), and is relatively not expensive.
- I also added a small layer 3 switch because I wanted to create a simple 2 tire architecture, and I also wanted to allow for Inter V-lan routing threw the multilayer switch

The Current Network



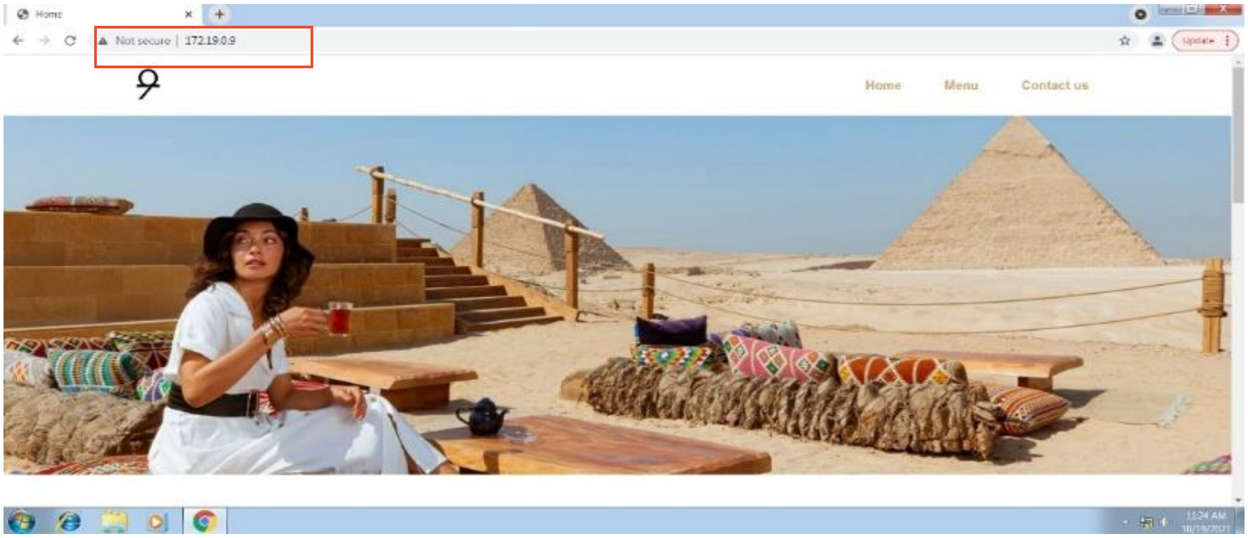
The current network contains the following devices

- 2 switches
- 1 router
- 2 access points
- 3 virtual PCs
- windows 7 virtual machine
- Ubuntu webserver (Hosting a website we built last year)
- Ubuntu server hosting the companies CRM

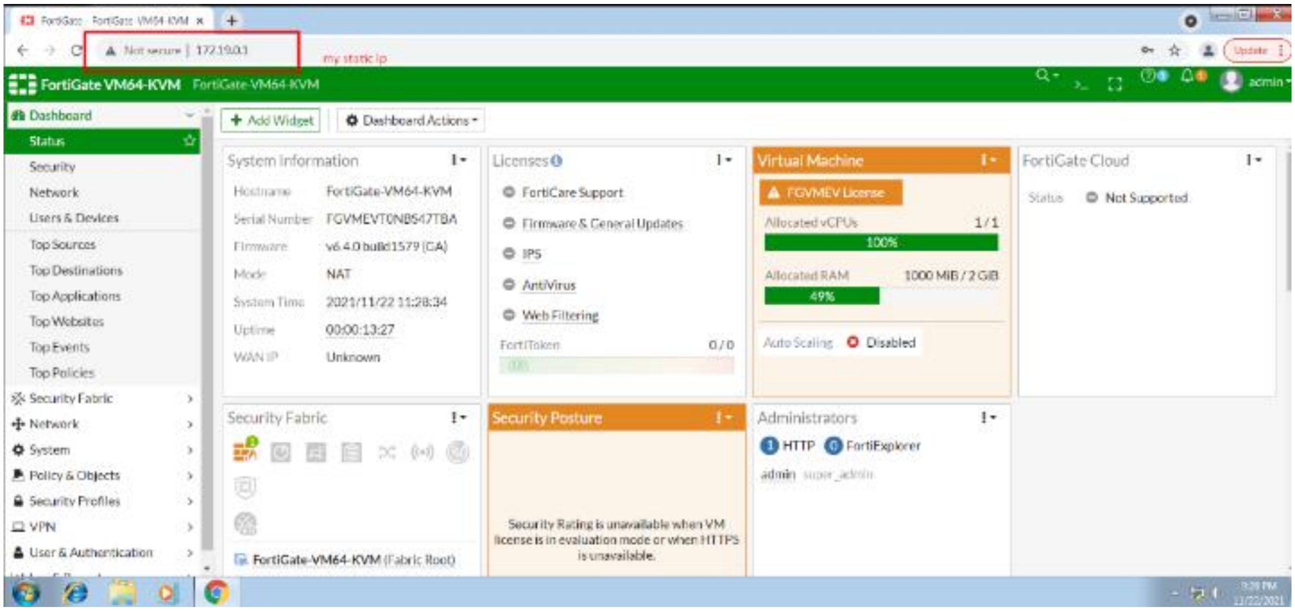
Testing the current network functionality

- The network has Ip address manually assigned starting from 172.19.0.2 to 172.19.0.9 and a default gateway of 172.19.0.1 all with a subnet mask of 255.255.0.0

- All devices can ping each other
- The webserver is hosting files from Apache and the webserver is accessible from any device on the network as shown below
- The firewall is configured and accessible from the windows 7 machine threw the IP 172.19.0.1
- The gate way for all the devices is the firewalls IP because FortiGate allows for routing



Not secure | 172.19.0.9



Not secure | 172.19.0.1

my static ip

FortiGate VM64-KVM FortiGate-VM64-KVM

System Information

Hostname FortiGate-VM64-KVM
Serial Number FGVMEVTONBS47TBA
Firmware v6.4.0 build1579 (GA)
Mode NAT
System Time 2021/11/22 11:28:34
Uptime 00:00:13:27
WAN IP Unknown

Licenses

FortiCare Support
Firmware & General Updates
IPS
AntiVirus
Web Filtering
FortiToken 0 / 0

Virtual Machine

FGVMEV License
Allocated vCPUs 1 / 1
100%
Allocated RAM 1000 MiB / 2 GiB
49%
Auto Scaling Disabled

FortiGate Cloud

Status Not Supported

Security Fabric

FortiGate-VM64-KVM (Fabric Root)

Security Posture

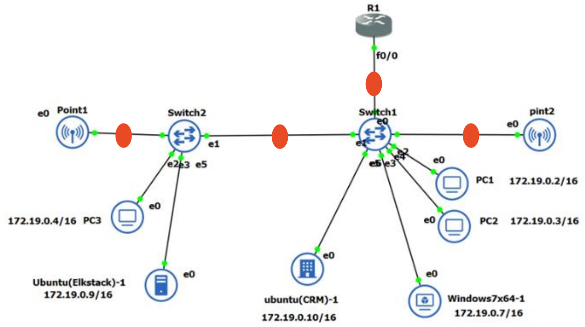
Security Rating is unavailable when VM license is in evaluation mode or when HTTPS is unavailable.

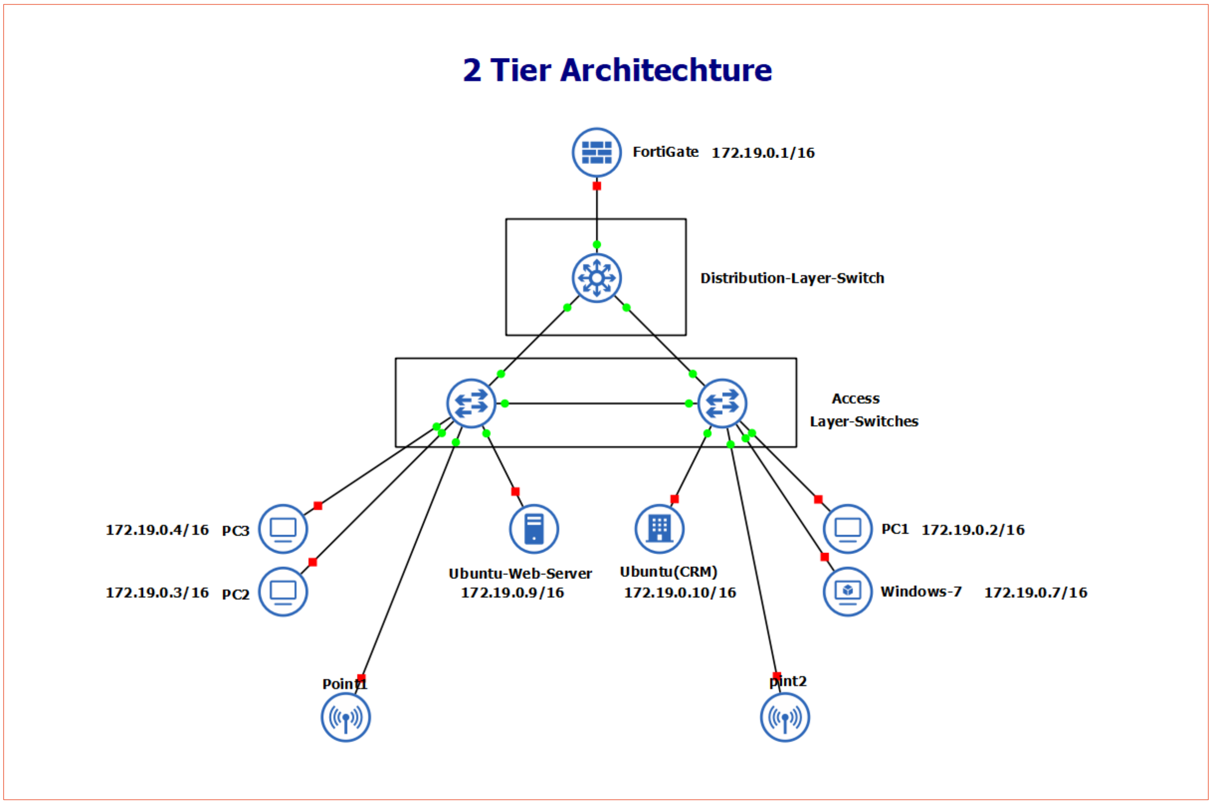
Administrators

1 HTTP 0 FortiExplorer
admin super_admin

Network Redesign (2 Tier Architecture)

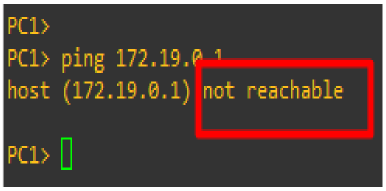
A big flow in this network is that there are multiple "single point of failures" which means if one of the wires shown in red go down the entire network will collapse. To fix this I added another switch and added a few more links. So, if one of the links is corrupted there are alternatives paths to pass the network traffic.





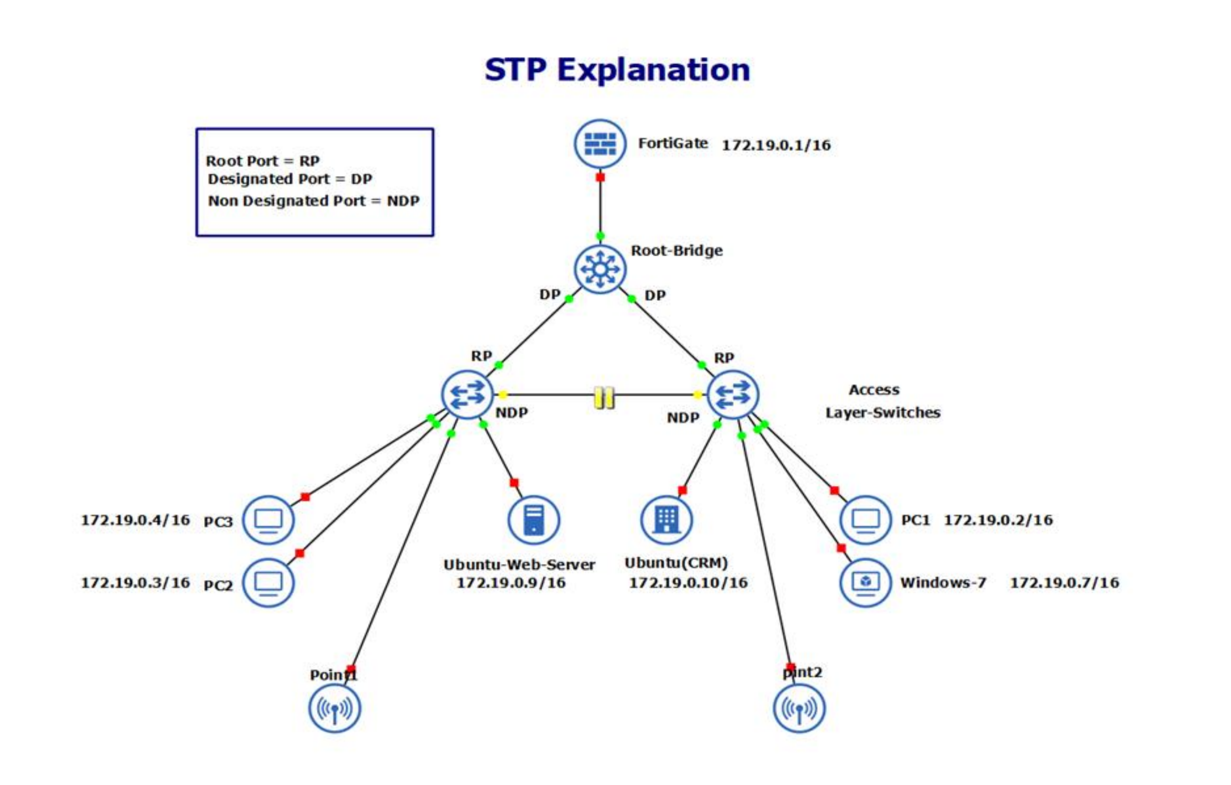
The new design is called a 2-tier architecture. Where there are 2 main layers of switches. The access layer which connects end devices to the network, and the distribution layer. As seen above now there are no single point of failures except one (from the distribution layer to the fire wall). To fix this I implemented ether channels explained below.

Implementing the Spanning tree protocol

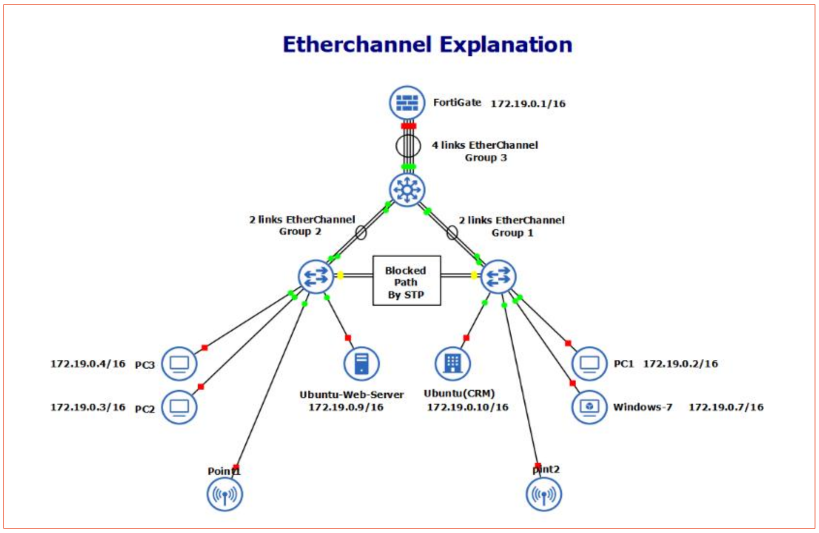


```
PC1>
PC1> ping 172.19.0.1
host (172.19.0.1) not reachable

PC1>
```

After I added the new switch and redesigned the entire network, the network was not working. This is because of redundant links causing loops. To fix this I needed to enable STP. STP is a loop prevention networking protocol that allows for redundancy while creating a loop free layer 2 topology. STP works by logically blocking physical links to prevent frames from circling around the network for ever. It works by electing a root switch and then other switches on the network find the best path to the root switch and disables other paths to stop the looping from accruing. In the diagram below I specified the root bridge, the root ports, designated ports, and non-designated ports.



EtherChannel



An EtherChannel allows grouping of several physical links to create one logical ethernet link for the purpose of providing redundancy and high-speed links. In the network I added a total of 6 new physical links. One extra link for all the switch-to-switch connections and grouped 4 physical links to connect the distribution switch to the firewall. This is because all the network traffic outside the network will pass through that link, and it needed high bandwidth and to provide redundancy. There are 2 protocols alliable that allow for EtherChannel PAGP and LACP I used and configured LACP because PAGP is only available for cisco devices and since I am connecting a cisco device to another vendor devise, I had to use LACP. There are 3 modes for the Ports to choose from while configuring the EtherChannels On, Active, and Passive.

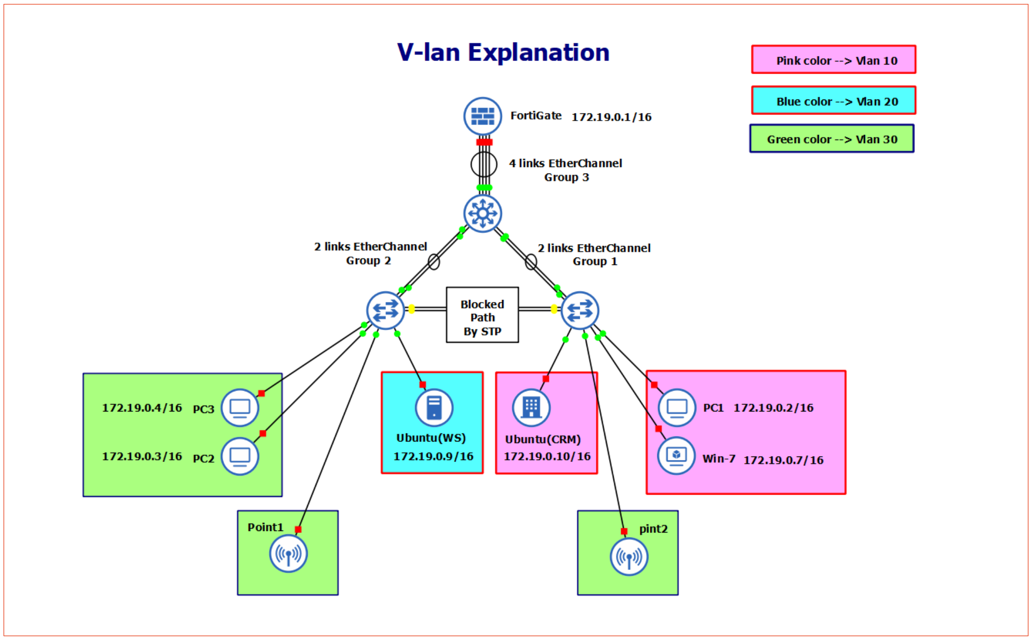
Switch one	Switch two	Channel Establishment
On	On	Yes
On	Active, Passive	No
Active	Active	Yes
Active	Passive	yes
Passive	Passive	no

Configuration:

```
# Interface range fa 0/1 -2 → specified the physical interfaces that I wanted to group together

# Channel-group 1 mode active → group them together

# Exit → to go back to the terminal configuration

# Interface port-channel 1 → specify the new port to edit

# Switch port mode trunk → witch to trunk port
```

Configuring Virtual local area networks

On the switch level (Data link layer) there is one main conflict that consumes the network resources which is the broadcast storm. this occurs when a pc on the network sends a broad cast message, and all the devices replay to that message. In big networks this will make the network slow or even collapse. To fix this issue I used virtual local area networks (V-Lans). V Lan is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. The figure below shows the 3 Vlans I configured in the network.



Another great feature in V-Lans is that it allows for better security. For example, in my network I only want 2 devices on the network to access the CRM machine because it contains valuable information. So, I configured a V-Lan for both resulting in only pc 1 and the windows 7 machine to communicate with the CRM machine. I also created a separate V-Lan for the ubuntu Web server machine. This adds one more layer of security to the network because it means that if the web server was compromised the attacker does not have access to other devises on the network (isolated in a separate V-lan).

Trunk links

After creating the above network, I was faced with a problem that devises on different switches cannot connect to each other even if they are on the same V-Lan. To fix this I had to configure trunk links between the switches to allow for the devises to communicate.

Configuration:

```
Switch 1 (config) # vlan 10

Switch 1 (config-vlan) # name LAN10

Switch 1 (config-vlan) exit

Switch 1 (config) # interface range fa 0/4

Switch 1 (config-inter) # switch port mode access vlan 10
```

Network Security Upgrades

To understand the security threats and mitigation in detail I broke down all the attacks and security upgrades into their respected layers from the OSI model.

Data Link Layer 2

Layer Two Security Upgrades

When it comes network security most network administrators outlook the layer two attacks the reason being they generally trust users on the local area network. However, not taking the right approaches to secure this layer can result in multiple attacks on the network.

MAC address table attacks

Attacks like MAC address flooding and MAC address Man in the middle are all very easy to occur if there are no proper security protocols to mitigate them. To mitigate such attack, I had to

1. Shutdown all unused ports

```
S1(config-inter) # shutdown
```

2. Enabled port security (allowed only authorized mac addresses)

```
S1(config-inter) # switchport port-security → enabled and configured to only one MAC
```

VLAN Hopping Attacks

Vlan hopping allows for an attacker to communicate to different vlans without the assistance of a router. This is possible if the attacker configures his/her device as a switch and take advantage of the auto trunking feature that is enabled on all switches by default. If successful, the attacker's device can jump from one vlan to another hence the name vlan hopping. To mitigate such attack, I had to

1. Disable trunking on all access ports
2. Disable auto trunking and manually configure all the trunk links

```
S1(config-inter) # switchport mode trunk
```

STP Attacks

An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. To mitigate such attack, I had to

1. Enable PortFast
2. Enable BPDU guard, Root guard, and Loop guard

Layer Three Security Upgrades

layer 3 is the network layer and this layer all the mitigations are related to IPs and ports. Witch means in this layer I was able allow certain protocols like ping and SSH and block other protocols like FTP. In this layer I also could block certain websites, monitor all the traffic, and filter any unwanted packets on the network. This is all possible threw the use of firewalls and an IPSs or IDSs.

ARP Attacks

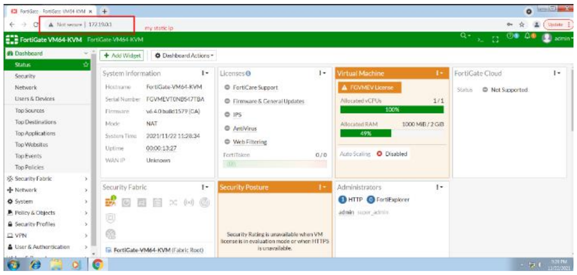
The Address Resolution Protocol is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given IP address. Attacker can take advantage of ARP and launch a wide range of attacks for example a man in the middle attack. To mitigate such attacks, I had to

1. Implemented Dynamic ARP Inspection

```
S1(config) # IP ARP inspection vlan 20
```

Configuring the Firewall

I choose FortiGate 6501F which is a firewall that comes with an IPS built in. it is relatively not expensive and has a graphical user interface. To start configuring the fire wall with the graphical interface I had to first set an IP to any of the ports then access it with one of the VMs in the virtual network. Now I had a graphical interface for the rest of the configuration.

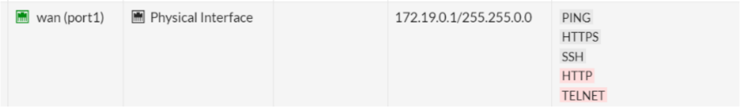


System Information

Hostname	FortiGate-VM64-KVM
Serial Number	FGVMEVT0NB547TBA
Firmware	v6.4.0 build1579 (GA)
Mode	NAT
System Time	2021/11/22 11:28:34
Uptime	00:00:13:27
WAN IP	Unknown

Allocated vCPUs 1/1 100%
Allocated RAM 1000 MiB / 2 GiB 49%
Auto Scaling Disabled
Status Not Supported
Security Rating is unavailable when VM license is in evaluation mode or when HTTPS is unavailable.

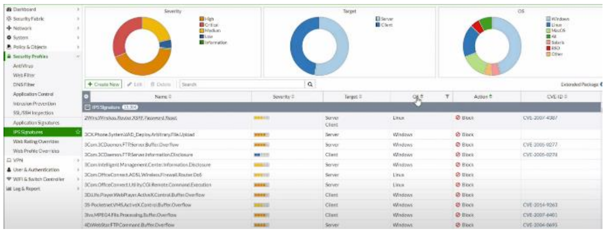
As shown below you can see all the allowed services on the network. Anything else will be blocked by the firewall.



wan (port1)	Physical Interface	172.19.0.1/255.255.0.0	PING HTTPS SSH HTTP TELNET

Configuring the IPS

An intrusion prevention system (IPS) is a form of network security that works to detect and prevent identified threats. In FortiGate I was able to configure the default IPS which monitored all the traffic and compares all the traffic to a database of malicious packets and if it finds any malicious packets it will automatically drop the packet.



Name	Severity	Target	OS	Action	CVE-ID
IPS Signatures 13,304					
2Wire.Wireless.Router.XSRF.Password.Reset		Server Client	Linux	Block	CVE-2007-4387
3CX.Phone.System.WID_Deploy.Arbitrary.File.Upload		Server	Windows	Block	
3Com.3CDaemon.FTP.Server.Buffer.Overflow		Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Disclosure		Client	Windows	Block	CVE-2005-0278
3Com.Intelligent.Management.Center.Information.Disclosure		Server	Windows	Block	
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS		Server	Linux	Block	
3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution		Server	Linux	Block	
3D.Life.Player.WebPlayer.ActiveX.Control.Buffer.Overflow		Client	Windows	Block	
3S-Pocketnet.VMS.ActiveX.Control.Buffer.Overflow		Client	Windows	Block	CVE-2014-9263
3ivx.MPEG4.File.Processing.Buffer.Overflow		Client	Windows	Block	CVE-2007-6401
4D.WebStar.FTP.Command.Buffer.Overflow		Server	Windows	Block	CVE-2004-0695

Transport Layer | 4

Layer Four Security Upgrades

Layer 4 is the transport layer, which enables network communication by utilizing standard transport protocols. The Transport Control Protocol (TCP) and the User Datagram Protocol (UDP) are also part of this layer.

Configuring Secure Sockets Layer (SSL)

Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network. I had to configure it by downloading a free certificate and enabling it on the website.

Application Layer | 5 6 7

Layer Five, Six, And Seven Security Upgrades

Layer five, six, and seven attacks all have to do with the end devices (the application). Most attacks occur on theses layers since it is the layers open to the internet. To limit the number of attacks on theses layers I recommend the following.

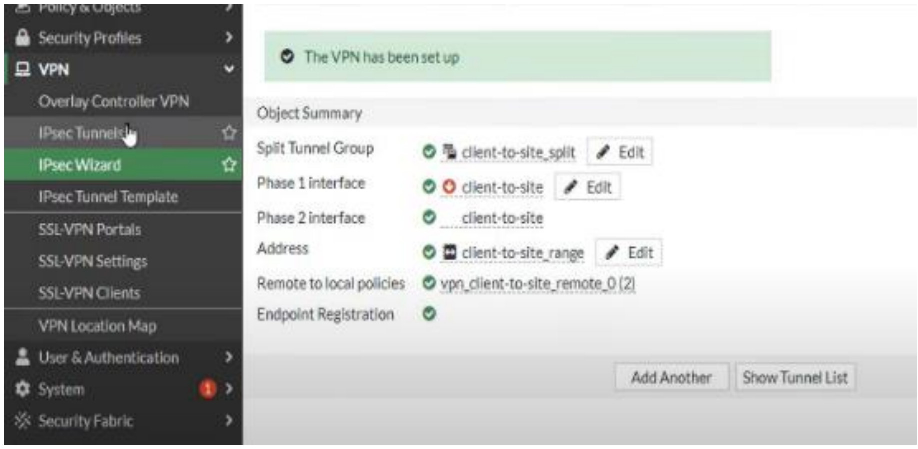
- Web application security
- Install the latest versions of the operating systems
- Install an antivirus on all end devices on the network
- Change the location of the computers to make sure only authorized users get access.
- All computers should never be unattended.
- All computers must auto lock after 10 minutes maximum.
- All computers must have the latest version of the operating system.
- All computers must have the latest versions of antiviruses.
- No external devises should be allowed (e.g., no USBs).
- All the valuable assets in the database must be encrypted.
- To access the data base, you should have a special username and password (a second layer of security after the normal computer password).
- All passwords must be updated every 3 months.
- All passwords must be at least 8 characters with at least one symbol and one number.
- All the information in the local server must be backed up (a good example is amazon cloud).
- All the waste material must be disposed properly (papers should be shredded).
- courses must be given to staff members about basics of computer security.

Allowing users to gain remote access

The main task here was to give a few users the ability to access the Ubuntu CRM machine from home. I found 2 ways to do that. Host the machine Online or create a client to site VPN.

	Host the machine Online	Client to site VPN
Advantages	Ease of use and flexibility	Is very secure since it creates and encrypted channel to the internal network
Disadvantages	An easy target for hackers since the entire machine is on the web	More technical and not that easy to use

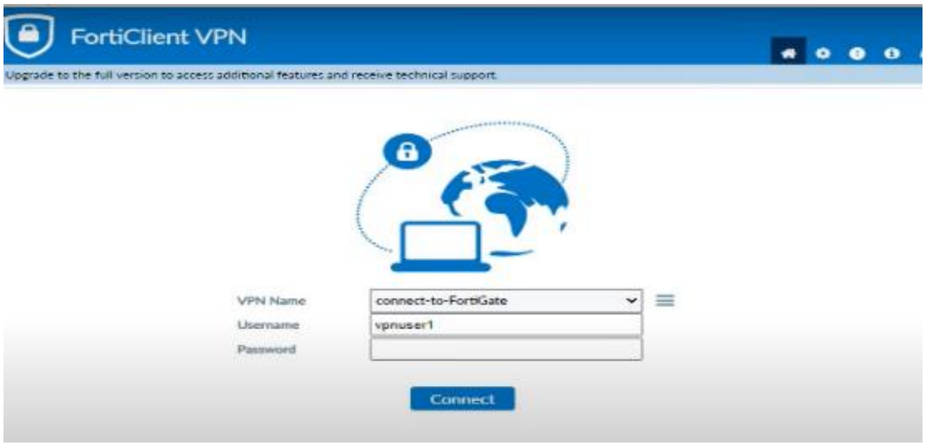
After inspecting the table above, I choose to go for the VPN options since it is more secure, and the company's CRM is very valuable. To create my VPN, I used the FortiGate IPsec wizard tab in the firewall to allow me to create a VPN with a username and a password for a few employees that need access to the CRM machine. And to access the VPN from the devises outside the network I use FortiGate client VPN for windows which is free.



✓ The VPN has been set up

Object Summary

Split Tunnel Group	✓ client-to-site_split
Phase 1 interface	✓ client-to-site
Phase 2 interface	✓ client-to-site
Address	✓ client-to-site_range
Remote to local policies	✓ vpn_client-to-site_remote_0 (2)
Endpoint Registration	✓



Upgrade to the full version to access additional features and receive technical support.

VPN Name	connect-to-FortiGate
Username	vpnuser1
Password	

How the network upgrades effected CIA

All the network upgrades discussed above ensure confidentiality, integrity, or availability. In some form or another the table below lists all the network upgrades and it effect on CIA.

Network Upgrade	Confidentiality	Integrity	Availability
Network Redesign			✓
STP			✓
EtherChannels			✓
Vlans + Trunk links	✓		✓
MAC address table attacks mitigation	✓	✓	✓
VLAN Hopping Attacks mitigation	✓	✓	
STP Attacks			✓
ARP Attacks			✓
Configuring the Firewall	✓	✓	
Configuring the IPS	✓	✓	
Configuring SSL	✓	✓	
Layer 5,6, and 7 security recommendations	✓	✓	✓

Network Redesign, STP, EtherChannels, mitigating STP and ARP attacks all ensure the availability of the network as they all help the network to not collapse. Vlans also ensures availability in the case of reducing broadcast storms and helps in confidentiality because it allows for grouping of the network end devices based on end devices' rolls. Mitigating MAC address table attacks establishes availability, integrity, and confidentiality. Mitigating Vlan hopping attacks, Configuring the Firewall, Configuring the IPS, Configuring SSL, and upper layer security recommendations all help in ensuring confidentiality and integrity. They all help in making sure the data is not exposed to unauthorized users and makes sure that the data is not tapered with before arriving to the destination.