Corporate Infrastructure Final Proposal

Robert Minson

College of Science, Engineering, and Technology, Grand Canyon University

ITT-116 Platforms and Network Technologies

Kellen Reed

April 21, 2022

***Infrastructure and Technology Requirements***

In a corporate structure, a network needs to be developed with thought and care, especially one that requires a DMZ, demilitarized zone. For this company, Lopes Manufacturing, they required a network that could hold 240 devices and have a web app server and hybrid exchange server hosted in a DMZ.

When building a network, you want to work from the bottom up. Start by connecting all your devices to layer two switches, in total you should have about seven 48 port switches to accommodate for all the devices and have backups for if one or two go down. After that you connect the layer two switches to two layer three switches with 24 ports. The reason for having two layer three ports is simply just redundancy. From here, you connect the layer three switches into two eight port firewalls and those firewalls into two layer two switches to create your DMZ. We incorporate two firewalls and two layer two switches for redundancy reasons. Then, within the DMZ, you have two layer two switches each with 24 ports that are both connected to two servers, one that is for the web app server and one for the hybrid exchange server. Those 24 port layer two switches are also connected to two other eight port switches that are connected to the ISP, internet service provider. Finally, on each layer of the network, except for the bottom, you have the devices connected to each other. For example, all of the 48 port layer two switches are connected to each other in addition to everything they are connected to that was mentioned up above. This same thought can be applied to the layer three switches and both pairs of firewalls.

***Network Diagram***

See attached PDF(1).

***Final Switch and Router Configurations***

ACCESS SWITCH

Building configuration...

Current configuration : 2450 bytes

!

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname CORP-SW-02

!

!

!

no ip domain-lookup

!

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface FastEthernet0/1

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/2

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/3

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/4

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/5

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/6

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/7

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/8

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/9

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/10

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/11

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/12

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/13

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/14

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/15

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/16

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/17

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/18

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/19

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/20

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/21

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/22

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/23

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/24

switchport access vlan 2

switchport mode access

!

interface GigabitEthernet0/1

switchport trunk allowed vlan 2,4,6,96

switchport mode trunk

!

interface GigabitEthernet0/2

!

interface Vlan1

no ip address

shutdown

!

interface Vlan6

ip address 10.0.6.2 255.255.255.0

!

ip default-gateway 10.0.6.1

!

!

!

!

line con 0

!

line vty 0 4

login

line vty 5 15

login

!

!

!

!

end

CORE SWITCH

Building configuration...

Current configuration : 2005 bytes

!

version 16.3.2

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname CORP-CORE-01

!

!

!

!

!

!

!

no ip cef

ip routing

!

no ipv6 cef

!

!

!

!

!

!

!

!

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface GigabitEthernet1/0/1

!

interface GigabitEthernet1/0/2

switchport trunk allowed vlan 2,4,6,96

switchport mode trunk

!

interface GigabitEthernet1/0/3

switchport trunk allowed vlan 2,4,6,96

switchport mode trunk

!

interface GigabitEthernet1/0/4

switchport trunk allowed vlan 2,4,6,96

switchport mode trunk

!

interface GigabitEthernet1/0/5

switchport trunk allowed vlan 2,4,6,96

switchport mode trunk

!

interface GigabitEthernet1/0/6

switchport trunk allowed vlan 2,4,6,96

switchport mode trunk

!

interface GigabitEthernet1/0/7

!

interface GigabitEthernet1/0/8

!

interface GigabitEthernet1/0/9

!

interface GigabitEthernet1/0/10

!

interface GigabitEthernet1/0/11

!

interface GigabitEthernet1/0/12

!

interface GigabitEthernet1/0/13

!

interface GigabitEthernet1/0/14

!

interface GigabitEthernet1/0/15

!

interface GigabitEthernet1/0/16

!

interface GigabitEthernet1/0/17

!

interface GigabitEthernet1/0/18

!

interface GigabitEthernet1/0/19

!

interface GigabitEthernet1/0/20

!

interface GigabitEthernet1/0/21

!

interface GigabitEthernet1/0/22

!

interface GigabitEthernet1/0/23

!

interface GigabitEthernet1/0/24

!

interface GigabitEthernet1/1/1

!

interface GigabitEthernet1/1/2

!

interface GigabitEthernet1/1/3

!

interface GigabitEthernet1/1/4

!

interface Vlan1

no ip address

shutdown

!

interface Vlan2

mac-address 000c.cf39.9101

ip address 10.0.2.1 255.255.255.0

!

interface Vlan4

mac-address 000c.cf39.9102

ip address 10.0.4.1 255.255.255.0

!

interface Vlan6

mac-address 000c.cf39.9103

ip address 10.0.6.1 255.255.255.0

!

interface Vlan96

mac-address 000c.cf39.9104

ip address 10.0.96.1 255.255.255.0

!

ip classless

!

ip flow-export version 9

!

!

!

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

!

!

end

***Cost Analysis***

There will be nine 48 port layer 2 switches, two 24 port layer 3 switches, five eight port firewalls, four 24 port layer 3 switches.

One 48 port layer 2 switch = $1,189.99

One 24 port layer 3 switch = $1,522.99

One 24 port layer 2 switch = $ 805.99

One 8 port firewall = $ 4,494.99

Total Equipment Cost = $ 39,454.8

The time requirement to do the job will be about 54.61 hours and will cost $50 an hour.

Total labor cost = $2,730.50

Total project cost = $42,185.30

***Work Structure Breakdown***

See attached PDF(2)

***Risk Analysis***

Risk can come in multiple forms for the network, but they all come back to hacking in some way or another. Not having a VPN, virtual protective network, applied opens your network up to be more easily hacked. Employees who are not selective with who or what they share company information with are also another major risk. Especially if the security for your network is a username and predetermined password that are handed out to employees.

***Security Threats Mitigation Approaches***

The best ways to mitigate the security threats to your system are to educate your employees and to use a cyber security organization. Your employees are always your weakest link in any network. Educating them on scam emails and general ways that hackers use them in order to get into their network are a must. In addition to training your staff, the use of a cyber security organization is a huge step in the right direction. You can get companies like SANS, Norton, or use the VPN from the company you purchased your firewall from for this. All of which can be used to help do the same things, protect your network from hackers via encryptions and other methods.

References

CDW. (n.d) *WatchGuard Compet Firebox M270 Network Firewall Appliance - 3-Year*

<https://www.cdw.com/product/cisco-550x-series-sg550x-24-switch-24-ports-managed->

[rack-mountable/4586961?pfm=srh](https://www.cdw.com/product/cisco-550x-series-sg550x-24-switch-24-ports-managed-rack-mountable/4586961?pfm=srh)

CDW. (n.d) *Cisco 550X Series SG550X-24 - switch - 24 ports - managed - rack-mountable*

<https://www.cdw.com/product/watchguard-compet-firebox-m270-network-firewall->

[appliance-3-year/5210697?pfm=srh](https://www.cdw.com/product/watchguard-compet-firebox-m270-network-firewall-appliance-3-year/5210697?pfm=srh)

CDW. (n.d)*Ubiquiti UniFi Switch USW-PRO-48-POE - 48 Port - Managed*

<https://www.cdw.com/product/ubiquiti-unifi-switch-usw-pro-48-poe-48-port->

[managed/5821012?pfm=srh](https://www.cdw.com/product/ubiquiti-unifi-switch-usw-pro-48-poe-48-port-managed/5821012?pfm=srh)

CDW. (n.d). *Ubiquiti UniFi Switch USW-Pro-24-POE - 24 Ports – Managed* <https://www.cdw.com/product/ubiquiti-unifi-switch-usw-pro-24-poe-24-ports-> managed/5823900?pfm=srh