Campus: Midrand

Faculty: Information Technology

Code: Network Security

Group:5

Lecturer's Name: Grace Kangwa

Students Full Name: Thelumusa Mthethwa

Students Full Name: Tafara Wilfred

Students Full Name: Tanaka Nyabanga

Students Full Name: Tsietsi Kgwale;

Department/Area	Network Medium	Security Device	Hosts	Servers	Description
Lecture Room	• Router – The network requires access to An Internet service this device will accommodate the necessary transmissions for effective directing of data.	Firewall – This is a physical firewall that will manage and filter traffic based on their packet and protocols form both outside and inside the network	Desk Top Computer/ Laptop		This network implementation will work in conjunction with the afore mentioned components. The segment will have a router for dedication to lecture room that is also switched from the entire network

	• Bridge – lecturer rooms of the same faculty will benefit from being connected under the same subnet and gain improved communication	IPS/IDS – This will stand as a firewall feature that can allow well managed and monitored packets that traverse the network, preventing and detecting threats accessing the network.	Switch – this will provide a switched network for access to the server that's on campus to establish traffic control , and better links of transportation		to an on-premise server and thereafter a gateway that also routes that subnet.
	• Wireless Access Point – the device will have appropriate control to provide access to devices from lecture rooms	VPNs – The use of this implementation Is to have a secure communication on the network that is ultimately used by lecturers	Printer- Available to use when there's a need for any physical documentation		
IT Department	• Switch – Placing a switch here will promote multiple connections to IT staff having main resources received and	Email Security – to prevent any phishing and hijacking attacks this preventative measure will secure the IT Infrastructure	Printers – This is to be used for documents need to be presented on paper for reasonable purposes.		The IT department is essential to ensure main operations of the network therefore they require thorough access to the network infrastructure. This

	sent effectively that require immediate attention.	from malicious attacks and secure appropriate communication channels through email services.			area will be placed at the gateway of all communication to enable monitoring of any network problems.
	• Router – this will serve the purpose of access to a broadband network and enhance transmissions over wireless connections.	IPsec – Data integrity and confidentiality will be maintained for reassurance in packet sources and further authenticate a transmitted data packet through selected users.	LAPTOPS/Desk Top Computers		
		Firewall – A firewall at this portion of the network will hold out any unknown traffic. This will be stateful inspection firewall			

Labs	• Access Point – Provide access to the connected LAN devices	Antivirus/ Anti-malware software will prevent trojans and other threats from creating drawback in the system	Projectors – Provide wide screen displaying capabilities for numerous viewing for the entire lab		Given that labs are on multiple floors and different rooms there is a need to connect each floor and room to a bridge to form a single network and extend bandwidth, in a room hosts will connect to a physical switch with fibre optic/Ethernet cabling from the switch to the host moreover the switch will be cabled to a router/access point and the server on campus.
	• Routers – To provide routing of a all connectivity that is passed	Firewalls – a firewall added at this section of the network will allow reliable use of the available privileges and continue to stop what seems to cause harm and has not been listed for occupy the network.			
	• Bridge – this device will extend the network in separate settings and allow address filtering from dedicated hosts.	NAC – Only access allowed to by controlling hosts from which the system requirements and updates meet specifications			

		will have the approval to continue operations on the network.			
Main Administration	Router/Access point – This is to avail the administration department active access to the services of the internet and general router capabilities for access control	*Antimalware software – applying this mechanism into the security of the network will safeguard main operations and data from being lost as well as keeping the system from potential attacks*.			For clients running administrative operations this will be the main port of entry for proposed services to the network and should cover activities such as monitoring and controlling, troubleshooting, updating, and maintaining the network to work to the best of it's capabilities. The Administration department will regulate the protocols such ICMP, HTTP,OSPF,POP,FTP,
	Switch – Connect all hosts that are direct to this area and extend the link to other segments.	Application security – this is to ensure that the applications used on the network are legitimate and have no defective responses or are			

		not adequate for installation on the network.			
	Bridge – The bridge is useful here to join the main administrator to the network and gain holistic control for authentication and authorization	SEIMs – this feature can monitor traffic, data and log activity, suspicious activity, and policy violation (Basic Types Of Network Security Measures, 2022)			
		Website Security – websites that need not to be accessed will not be reachable by the end-user such as those with malware, and high fluctuation of data.			

		Firewall – this will prevent any threat intending to infiltrate the network and cause DDoS attack, or ransomware attack to be halted and keep administration data from unauthorized and unauthenticated clients.			

Other technologies to include on the network will be the use of DHCP to enable configuration of IP addresses in support of assigning hosts an effective communication mechanism.

NAT – addresses in the network will need to be mapped to a corresponding public address to enhance security and prevent network channels from being spoofed and attacked by hackers.

Data Loss Prevention will contain the necessary measures to prevent sensitive data from being lost, misused, and accessed by unauthorised users. These Technologies help identity, monitor, and protect data that is used at rest, and in transit.

Technologies

Cisco 2600X Series Ethernet Managed Switch – this device

Is great for a more secure network as it contains a wide variety of options because it is a full managed switched. Characteristics to note include ACLs, VPNs, and port scanning. It is a more expense switch but could work well in an environment that need to keep their assets from being compromised (Bliss, 2015).

ERP (UNIT4 Business World) – this type of ERP has capabilities for customization meaning it can be customized to the college's needs according to the varying departments. UNIT4 has a functionality to manage complex financial operations (Davidson, 2024).

Local Sever – Lenovo ThinkSystem SR650 V3 has to be implemented as it is a cutting-edge created to perform enterprise level tasks at an affordable price. (Ahmad, 2023)

Cloud server – Truehost Africa 1 core processor, 1gb RAM, 25GB Disk Space, 2TB Bandwidth

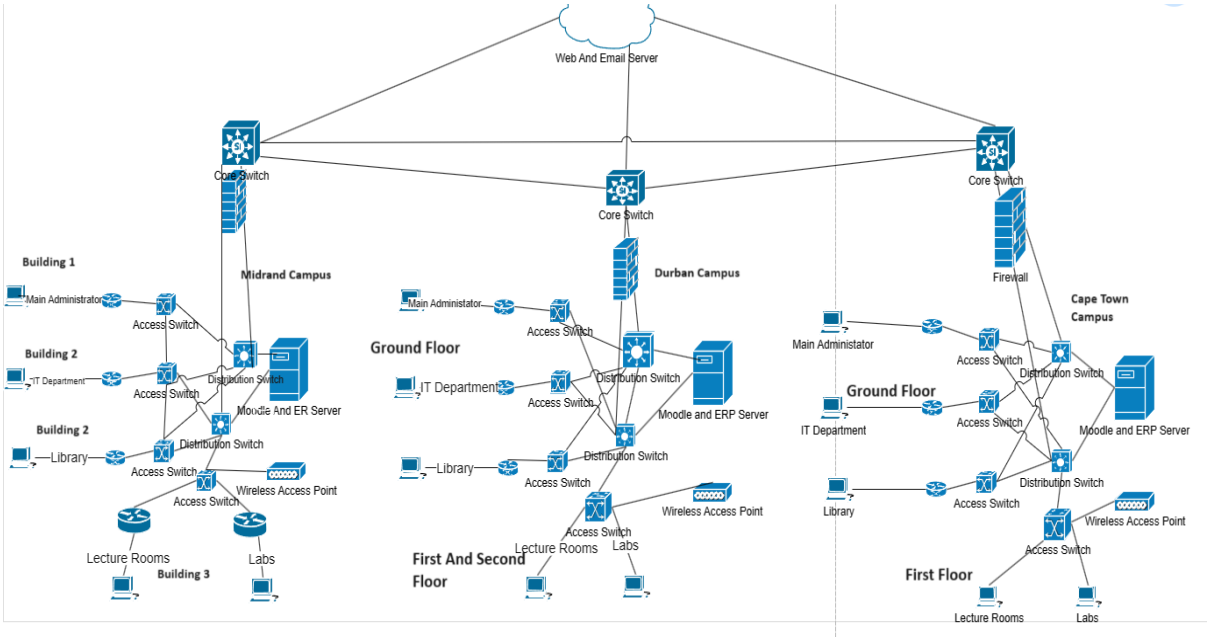
Printer – HP Officejet pro 9025e

VPN (NordVPN) – All internet traffic is secured by 256-bit AES encryption, which comes as standard. It's coupled with 2,048-bit SSL keys and DNS leak protection. Nord offers configuration enabling a connection depending on different requirements, such as downloading, P2P file sharing, video streaming, or anonymity (Husain, 2024).

Cisco Secure Firewall 4200 Series - Firewall throughput: 71 Gbps IPS throughput: 71 Gbps, IPSec VPN throughput: 51 Gbps, Maximum VPN peers: 20,000.

Connection Medium - Yutianhome500ft/150m OD-5mm Industrial TPU OS2 LC to LC Outdoor Armored Fiber Optic Cable, Duplex Single Mode Fiber Patch Cable, 9/125um Uniboot LC Fiber with Pulling Eye Kit Installed on one end. The cable features a strong tensile jacket high abrasion resistance, water proof, high and low-temperature resistance, uv-resistant, bending resistant.

1.1.



STAFF Network

1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1 0.0 0 0 0 0 0 0 0

AND = 192.168.0.0

1 1 0 0 0 0 0 0.1 0 1 0 0 0 1 0.0 0 0 0 0 0 0 0.0 0 0 0 0 0 0 0

Number of hosts = 2^9= 512 staff host IP addresses

MIDRAND Campus(Students)

1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 0 0 0.0 0 0 0 0 0 0 0

AND = 192.168.8.0

1 1 0 0 0 0 0 0.1 0 1 0 0 1 0 0.0 0 0 0 1 0 0 0.0 0 0 0 0 0 0 0

1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 0 0 0.0 0 0 0 0 0 0 0

AND = 192.168.8.0

1 1 0 0 0 0 0 0.1 0 1 0 0 1 0 0.0 0 0 0 1 0 0 1.0 0 0 0 0 0 0 0

1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 0 0 0.0 0 0 0 0 0 0 0

AND = 192.168.8.0

1 1 0 0 0 0 0 0.1 0 1 0 0 1 0 0.0 0 0 0 1 0 1 0.0 0 0 0 0 0 0 0

1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 0 0 0.0 0 0 0 0 0 0 0

AND = 192.168.8.0

1 1 0 0 0 0 0 0.1 0 1 0 0 1 0 0.0 0 0 0 1 0 1 1.0 0 0 0 0 0 0 0 0

Cape Town Campus(Students)

1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 0 0 0.0 0 0 0 0 0 0 0

AND = 192.168.8.0

1 1 0 0 0 0 0 0.1 0 1 0 0 1 0 0.0 0 0 0 1 1 0 0.0 0 0 0 0 0 0 0

1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 0 0 0.0 0 0 0 0 0 0 0

AND = 192.168.8.0

1 1 0 0 0 0 0 0.1 0 1 0 0 1 0 0.0 0 0 0 1 1 0 1.0 0 0 0 0 0 0 0

Durban Campus(Students)

1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 0 0 0.0 0 0 0 0 0 0 0

AND = 192.168.8.0

1 1 0 0 0 0 0 0.1 0 1 0 0 1 0 0.0 0 0 0 1 1 1 0.0 0 0 0 0 0 0 0

1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 0 0 0.0 0 0 0 0 0 0 0

AND = 192.168.8.0

1 1 0 0 0 0 0 0.1 0 1 0 0 1 0 0.0 0 0 0 1 1 1 1.0 0 0 0 0 0 0 0

Number of hosts = $2^{11} = 2048$ all three campuses Student IP Addresses

Campus	Subnet Allocation	Subnet Mask	Subnet ID	Network ID	IP Adress Range	Building Addresses	Broadcast Address

Midrand	Students	255.255.255.0	255.255.248.0 (/21)	192.168.8.0(/21)	192.168.8.1 – 192.168.11.254	Building B– 192.168.8.1 – 192.168.8.150 Building C- 192.168.9.150 – 192.168.9.254 LABa Building A(Library) – 192.168.8.151 – 192.168.8.201	192.168.11.255
	Staff	255.255.255.0	255.255.254.0 (/23)	192.168.0.0(/23)	192.168.0.1 - 192.168.0.74	Building A(Admin) – 192.168.0.1 – 192.168.0.15 IT Department – 192.168.0.16 – 192.168.0.30 Other – 192.168.0.31 – 192.168.0.74	192.168.0.255
Cape Town	Student	255.255.255.0	255.255.248.0(/21)	192.168.8.0(/21)	192.168.12.0 – 192.168.13.254 .	Floor 1 – 192.168.12.0 – 192.168.12.100 Ground(Library) – 192.168.12.101 – 192.168.12.175	192.168.13.255
	Staff	255.255.255.0	255.255.254.0 (/23)	192.168.0.0(/23)	192.168.0.75 - 192.168.0.149	Ground(Admin) – 192.168.0.75 - 192.168.0.89 IT department – 192.168.0.90 – 192.168.0.103 Other 192.168.0.140 – 192.168.0.149	192.168.0.255
Durban	Student	255.255.255.0	255.255.248.0 (/21)	192.168.8.0(/21)	192.168.14.0 – 192.168.15.254	Floor 1 – 192.168.14.0 - 192.168.14.120 Floor 2 – 192.168.14.121 – 192.168.14.241 Ground Floor(Library) – 192.168.15.0 - 192.168.15.75	192.168.15.255

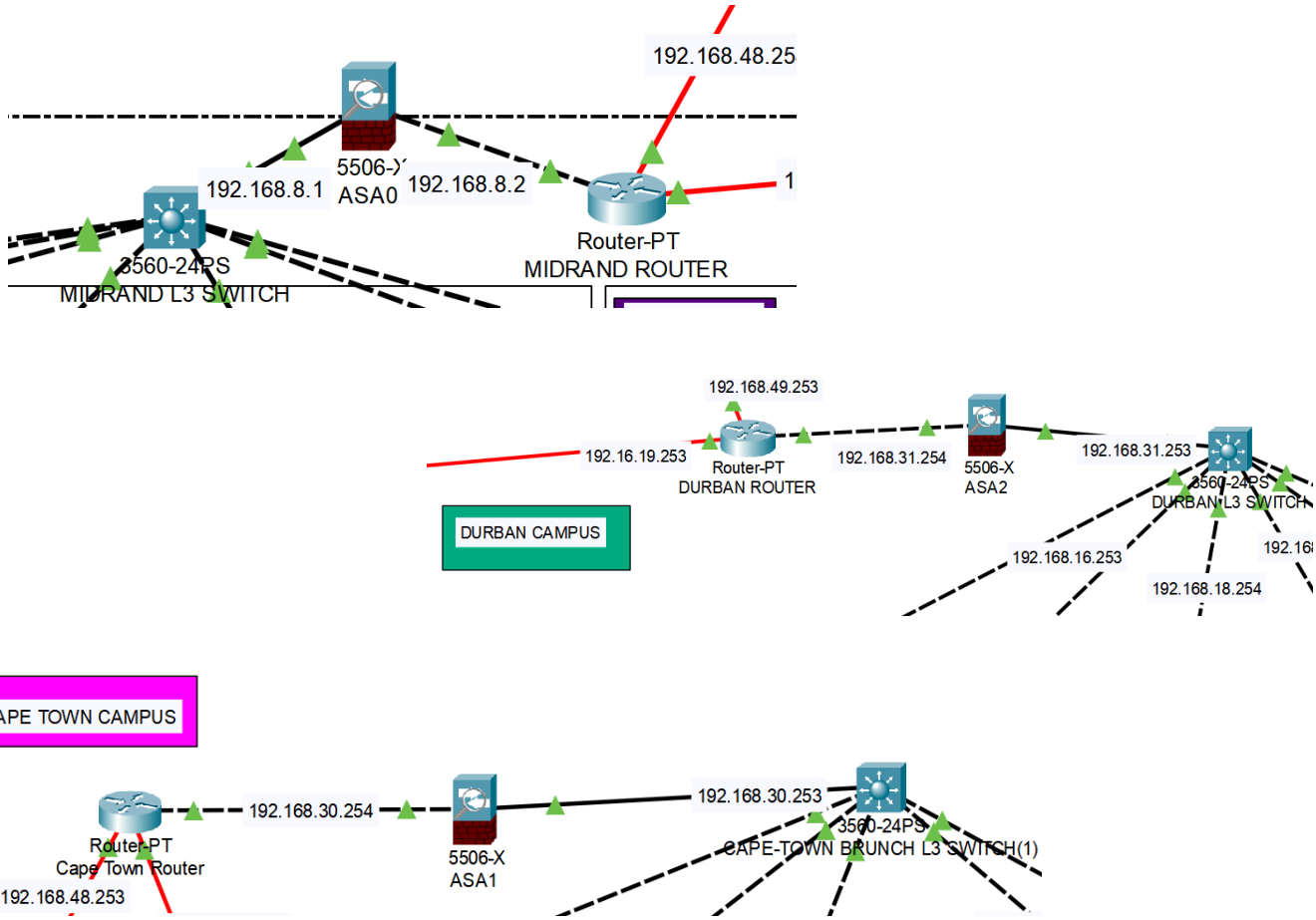
	Staff	255.255.255.0	255.255.254.0(/23) (Team, 2023)	192.168.0.0(/23)	192.168.0.151 - 192.168.0.254	Ground Floor(Admin) – 192.168.0.150 – 192.168.0.164 IT Department – 192.168.0.165 – 192.168.0.175 Other – 192.168.0.176 – 192.168.0.254	192.168.0.255

Deliverable 2

(Please see Packet Tracer file)

Deliverable 3

3.1. In order to ensure that the ingress and egress of traffic is monitored and filtered on the network we firstly would need to install three CISCO ASA 5506 firewalls with the first being installed in between the Midrand L3 Switch and the Midrand_router, the second between the Durban L3 switch and the Durban Router and the third would be between the Cape Town Branch L3 switch and the Cape Town Router. The first action in each configuration would be to open the command line interface and configure the firewalls. Enter the “conf t” command to enter privilege mode to change its hostname to BeMidrand. The subsequent hostnames will also be BeDurban and BeCapeTown respectively.



Then the second configuration executed on the CLI would be to create a password and configure the gig1/3 line to #no shut, opening up the network line for data flow. Then we'd configure to add ip addresses as well as setting the security level to 0 for untrusted areas and 100 for all trusted areas. Following the installation and configuration of the firewalls and switches, network traffic analysis's main objectives for network administrators are to intercept and analyse the network data (Hamdan, 2022) . The two main objectives for network administrators are incident reporting which allows them to detect and respond to any incident that may occur on the network and secondly to troubleshoot any network error that may also occur.

This is done to counter the actions of bad actors seeking to perform address resolution protocol (ARP) spoofing using net sniffing as means of hacking where they can even act as the man in the middle in-between data transfers. Net sniffing involves the use of pcap file enabled software like Wireshark (Usha Banerjee, 2010) that is able to view the packets that are on a network belonging to other users. (S. Ansari, 2003).

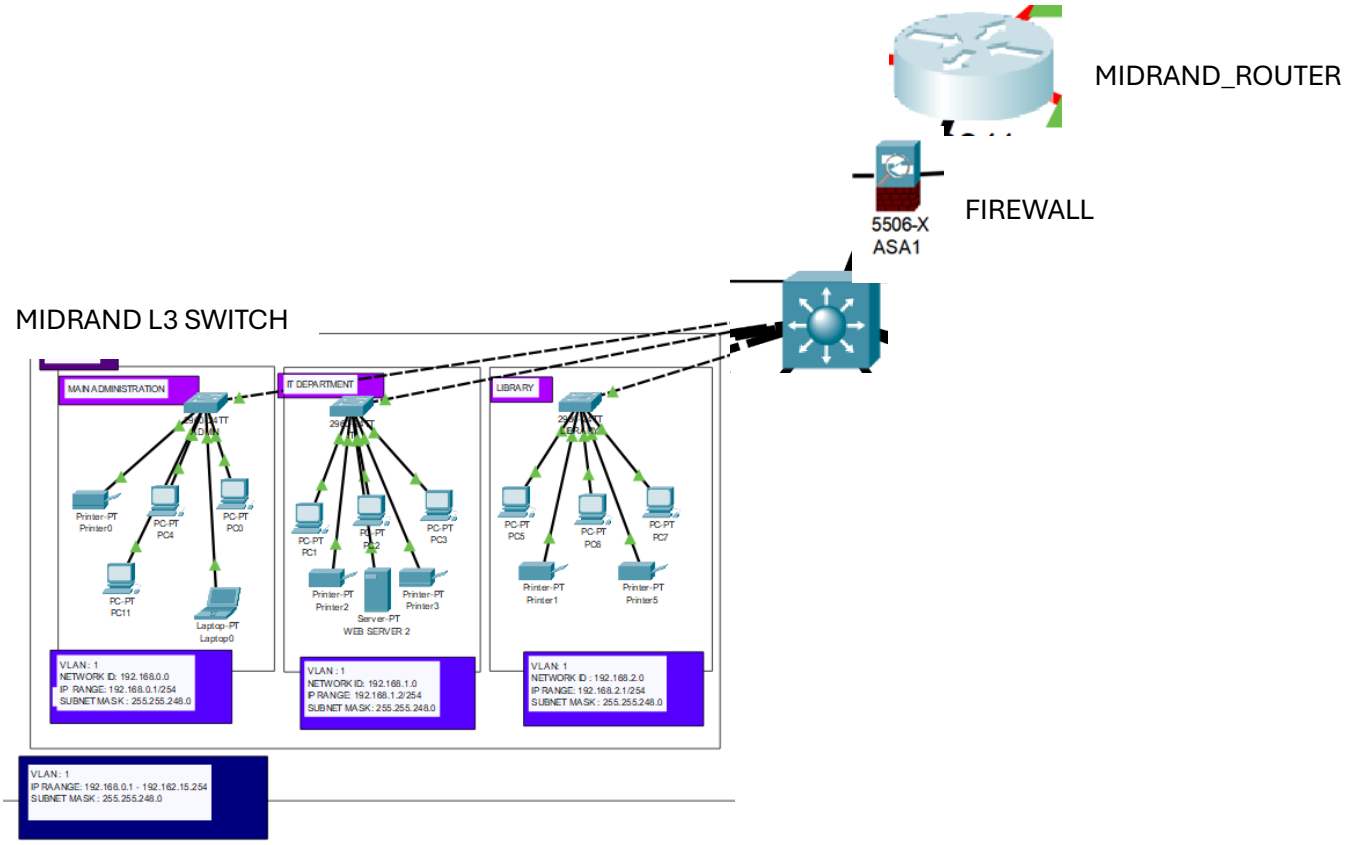
Network administrators are able to use these techniques to read the packets on the network layer of the TCP/IP protocol to validate and monitor the traffic on the network. PCAP or packet capture allows for the interception and analysis of packets on the network. (Anon., 2024) Packet analysis allows for network administrators to identify network security breeches and intrusions and even monitor certain brute force attacks where users use multiple login attempts to flood the network with unwanted traffic.

In the case of Belmand College, we would need to incorporate the use of firewalls as well as an intrusion detection system (IDS) that can be installed to analyse that traffic. We would then incorporate the use of the IPS which would greatly assist in the time delays that are experienced by users when only using IDS and firewalls (Chuanxi Cai, 2018) It is the interest of users seeking to access network data quickly that the optimal configuration of these systems be implemented. An IDS can generate alarms while an IPS can prevent users who generate alarms from accessing the network.

The use of access control lists allows for and denial of access to a network through rules that are agreed upon by stakeholders and network administrators. These routers can be installed in switches and routers which consist of ordered rules or access control entities which can define a packet classification scheme (Jiang Qian, 2001).

In the example below is how an IDS/IPS system would be implemented on a Cisco 2600X Series Ethernet Managed Switch and Cisco Secure Firewall 4200 Series

Example of How an effective IDS/IPS system would be implemented.



IDS/IPS System		
No.	**PC NAME & IP ADDRESS**	**Violation**
1	192.168.0.2 (PC4)	Corporate Policy Violation
2	192.168.0.5 (PC11)	P2P_Usage
3	192.168.0.3 (PC0)	Social Media Usage
4	192.168.1.2 (PC2)	Multiple Login Attempts
5	192.168.1.3 (PC3)	Suspicious ARP Behaviour
6	192.168.2.2 (PC5)	Bad Traffic Protocol
7	192.168.2.3 (PC6)	Protocol Other
8	192.168.2.4 (PC7)	Metasploit Traffic

In the example above is how an effective IDS/IPS system would be able to respond to threats. Should the above computers with their respective IP addresses be found in the following violations, the use of an IDS/IPS filter table would analyse and then flag that specific IP address and then the destination ports would be blocked to stop the college server getting compromised. If PC (7) 192.168.2.4 appears on the traffic analyser, it would then be added to the network filter.

Then after restarting the network traffic the volition should no longer appear in the traffic analyser then the network administrator would be able to conduct an investigation based on these findings, documenting the incident in case of future troubleshooting, prevention and reporting

3.2 A network topology on cisco packet tracer for a campus known as Belmand College has multiple campuses and multiple buildings on each campus. In its Main campus is the Midrand Campus which has three buildings.

BUILDING A has VLAN:1 IP RANGE: 192.168.0.1 – 192.162.15.254, SUBNET MASK: 255.255.248.0 has 3 LAN's the first one is the MAIN ADMINISTRATION LAN which has VLAN 1 with a NETWORK ID: 192.168.0.0, IP RANGE: 192.168.0.1/254, SUBNET MASK: 225.225.246.0 . This LAN has a 2960 27TT ADMIN Switch connecting a Printer PT Printer0, PC-PT PC4, PC-PT PC0, PC-PT PC11 Laptop-PT Laptop0.

The second LAN in Building A is the IT DEPARTMENT which has VLAN:1, NETWORK ID: 192.168.1.0, IP RANGE: 192.168.1.2/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT switch connecting PC-PT PC1, PC-PT PC2, PC-PT PC3, Printer-PT Printer2, Server-PT WEB SERVER2, Printer-PT Printer3

The third LAN in BUILDING A is the LIBRARY which has VLAN:1, NETWORK ID: 192.168.2.0, IP RANGE: 192.168.2.1/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT switch connecting PC-PT PC5, PC-PT PC6, PC-PT PC7, Printer-PT Printer1, Server-PT WEB SERVER2, Printer-PT Printer5

The second building is BUILDING B which has its first LAN named LAB which has VLAN:1, NETWORK ID: 192.168.4.0, IP RANGE: 192.168.4.1/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LAB(01) switch connecting PC-PT PC8, PC-PT PC9, PC-PT PC10, PC-PT PC16, PC-PT PC15.

The second LAN in BUILDING B is LECTURER ROOMS which has VLAN:1, NETWORK ID: 192.168.5.0, IP RANGE: 192.168.5.1/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LECTURE ROOM switch connecting PC-PT PC12, PC-PT PC20, PC-PT PC21, PC-PT PC14.

The third building is BUILDING C which has its first LAN named LABS which has VLAN:1, NETWORK ID: 192.168.6.0, IP RANGE: 192.168.6.1/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LAB(02) switch connecting PC-PT PC18, PC-PT PC13, PC-PT PC17, PC-PT PC19.

The second LAN in BUILDING C is LECTURER ROOMS which has VLAN:1, NETWORK ID: 192.168.7.0, IP RANGE: 192.168.7.1/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LECTURE ROOMS switch connecting PC-PT PC25, PC-PT PC24, PC-PT PC23, PC-PT PC22.

All these Main campus buildings' switches are connected to the 3560-24PS MIDRAND L3 SWITCH which is connected to MIDRAND_ROUTER which has an IPv4 Address: 192.168.19.253, SUBNET MASK 255.255.248.0

The second Campus is the Durban Campus which has VLAN: 3 (Durban-Network) IP RANGE: 192.168.16.1 – 1.192.162.31.254 SUBNET MASK: 255.255.248.0 and has 3 different floors with different LANs on each floor.

The GROUND FLOOR has its first LAN named LIBRARY and has VLAN:3, NETWORK ID: 192.168.16.0, IP RANGE: 192.168.16.1/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LIBRARY(D) switch connecting PC-PT PC26, PC-PT PC28, PC-PT PC27, Printer-PT Printer7.

The second LAN in GROUND FLOOR is IT SUPPORT which has VLAN:3, NETWORK ID: 192.168.17.0, IP RANGE: 192.168.17.1/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT IT SUPPORT(D) switch connecting PC-PT PC29, PC-PT PC31, PC-PT PC30, Server-PT WEB SERVER

The FIRST FLOOR also has two LANS the first one named LECTRURE ROOM which has VLAN:3, NETWORK ID: 192.168.18.0, IP RANGE: 192.168.18.1/254, SUBNET MASK: 255.255.248.0 with a 2960- LECTRURE ROOMS(D) switch connecting PC-PT PC32, PC-PT PC33, Printer-PT Printer8

The second LAN in FIRST FLOOR is LAB which has VLAN:3, NETWORK ID: 192.168.19.0, IP RANGE: 192.168.19.1/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LABS(D) switch connecting PC-PT PC35, PC-PT PC45, PC-PT PC34

The SECOND FLOOR also has two LANS the first one named LAB which has VLAN:3, NETWORK ID: 192.168.20.0, IP RANGE: 192.168.20.1/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LAB(D) switch connecting PC-PT PC40, Printer-PT Printer9, PC-PT PC39, PC-PT PC38

The second LAN in SECOND FLOOR is LECTRURE ROOMS which has VLAN:3, NETWORK ID: 192.168.21.0, IP RANGE: 192.168.21.1/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LECTRURE ROOM(D) switch connecting PC-PT PC36, PC-PT PC46, PC-PT PC37

All these DURBAN CAMPUS floor switches are connected to the 3560-24PS DURBAN BRANCH L3 SWITCH which is connected to DURBAN BRANCH ROUTER which has an IPv4 Address: 192.168.31.254, SUBNET MASK 255.255.248.0 which is connected to MIDRAND_ROUTER from the MAIN Campus which has an IPv4 Address: 192.168.19.253, SUBNET MASK 255.255.248.0.

The Third Campus is the CAPE TOWN Campus which has VLAN: 4 (Cape Town-Network) IP RANGE: 192.168.32.1 – 1.192.162.31.254 SUBNET MASK: 255.255.248.0 and has 2 different floors with different LANs on each floor.

The GROUND FLOOR has its first LAN named ADMIN and has VLAN:4, NETWORK ID: 192.168.32.0, IP RANGE: 192.168.32.2/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT ADMIN(CPT) switch connecting PC-PT PC41, PC-PT PC42, PC-PT PC43, Printer-PT Printer6.

The second LAN in GROUND FLOOR is LIBRARY which has VLAN:4, NETWORK ID: 192.168.33.0, IP RANGE: 192.168.33.2/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LIBRARY(CPT) switch connecting PC-PT PC26(1), PC-PT PC28(1), PC-PT PC27(1)

The Third LAN in GROUND FLOOR is IT SUPPORT which has VLAN:4, NETWORK ID: 192.168.34.0, IP RANGE: 192.168.34.2/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LIBRARY(CPT) switch connecting PC-PT PC29(1), PC-PT PC36(1), PC-PT PC30(1), Server-PT WEB SERVER0

The FIRST FLOOR also has two LANS the first one named LECTRURE ROOMS which has VLAN:4, NETWORK ID: 192.168.35.0, IP RANGE: 192.168.35.2/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LECTRURE ROOMS(CPT) switch connecting PC-PT PC36(1), PC-PT PC44, Printer-PT Printer10, PC-PT PC37(1)

The second LAN in FIRST FLOOR is LABS which has VLAN:4, NETWORK ID: 192.168.36.0, IP RANGE: 192.168.36.2/254, SUBNET MASK: 255.255.248.0 with a 2960-24TT LABS(CPT) switch connecting PC-PT PC38(1), PC-PT PC39(1), PC-PT PC40(1)

All these CAPETOWN CAMPUS floor switches are connected to the 3560-24PS CAPETOWN BRANCH L3 SWITCH which is connected to CAPETOWN BRANCH ROUTER which has an IPv4 Address: 192.168.42.254, SUBNET MASK 255.255.248.0 which is connected to MIDRAND_ROUTER from the MAIN Campus which has an IPv4 Address: 192.168.19.253, SUBNET MASK 255.255.248.0.

To configure standard and extended access control lists (ACLs) in the Midrand_router CLI to control access to the finance and student management system or network segments, the following will need to be implemented.

Access Midrand_router CLI: Access the command-line interface (CLI) of MIDRAND_ROUTER.

Click on the Midrand_router PT and to the command line interface.

Create Standard ACL for Finance System:

Midrand_router(config)# access-list 1 permit 192.168.2.0 0.0.7.255 # Allow access from Belmand College main campus VLAN for Library

Midrand_router(config)# access-list 1 permit 192.168.33.0 0.0.7.255 # Allow access from Cape Town Campus VLAN for Library

Midrand_router(config)# access-list 1 deny any # Deny all other traffic

Create Standard ACL for Student Management System:

Midrand_router(config)# access-list 2 permit 192.168.0.0 0.0.7.255 # Allow access from Belmand College main campus VLAN for Main Administration

Midrand_router(config)# access-list 2 permit 192.168.1.0 0.0.7.255 # Allow access from Belmand College main campus VLAN for IT Department

Midrand_router(config)# access-list 2 permit 192.168.4.0 0.0.7.255 # Allow access from Building B (Belmand College main campus) VLAN for Lab

Midrand_router(config)# access-list 2 permit 192.168.16.0 0.0.7.255 # Allow access from Durban Campus VLAN for Library

Midrand_router(config)# access-list 2 deny any # Deny all other traffic

Create Extended ACL for Both Systems:

Midrand_router(config)# access-list 100 permit tcp any 192.168.2.0 0.0.7.255 eq <finance_system_ports> # Allow finance system traffic from Belmand College main campus Library VLAN

Midrand_router(config)# access-list 100 permit tcp any 192.168.33.0 0.0.7.255 eq <finance_system_ports> # Allow finance system traffic from Cape Town Campus Library VLAN

Midrand_router(config)# access-list 100 permit tcp any 192.168.0.0 0.0.7.255 eq <student_mgmt_system_ports> # Allow student management system traffic from Belmand College main campus Main Administration VLAN

Midrand_router(config)# access-list 100 permit tcp any 192.168.1.0 0.0.7.255 eq <student_mgmt_system_ports> # Allow student management system traffic from Belmand College main campus IT Department VLAN

Midrand_router(config)# access-list 100 permit tcp any 192.168.4.0 0.0.7.255 eq <student_mgmt_system_ports> # Allow student management system traffic from Building B (Belmand College main campus) Lab VLAN

Midrand_router(config)# access-list 100 permit tcp any 192.168.16.0 0.0.7.255 eq <student_mgmt_system_ports> # Allow student management system traffic from Durban Campus Library VLAN

Midrand_router(config)# access-list 100 deny ip any any # Deny all other traffic

Apply ACLs to Router Interfaces:

Apply ACL 1 to the incoming interface for traffic to the finance system:

Midrand_router(config)# interface <finance_system_ports>

Midrand_router(config-if)# ip access-group 1 in

Apply ACL 2 to the incoming interface for traffic to the student management system:

Midrand_router(config)# interface <student_mgmt_system_ports>

Midrand_router(config-if)# ip access-group 2 in

Deliverable 4

Please see Presentation PowerPoint file

Deliverable 5

BELMAND COLLEGE NETWORK CONFIGURATION & SECURITY GUIDE

Summary

This manual offers a simplified method for building up and protecting Belmand College's network infrastructure, assuring secure, effective operations on all campuses and in distant work settings.

Important Elements

Configuring a Network

High-speed connections: gigabit Ethernet inside campuses, fibre optics for intercampus communication.
VLANs: Separate VLANs for guest, academic, and managerial traffic.
Safety Protocols
Installed at important intersections, firewalls are set up with strong access restrictions.
IPS: immediate threat identification and mitigation.

Observation and Administration

SIEM System: Log management and unified monitoring for unusual behaviour.
Patch management includes both routine updates and essential patching procedures.

Gaining Access and Control

Cisco ISE: Role-based access controls combined with centralised authentication.
Vulnerability checks involve constant scanning and quick corrective action plans.

Updates & Communication

Automated Alerts: For upgrades to the system and security incidents.
Engaging Stakeholders: Providing regular updates on the security posture and network condition.

Method of Implementation

Phased deployment will begin with crucial security and infrastructure configurations, with each step being carefully verified and documented before moving further.

Bibliography

Anon., 2024. *What is Packet Capture (PCAP)?*. [Online]
Available at: https://www.solarwinds.com/resources/it-glossary/pcap
[Accessed 20 March 2024].

Chuanxi Cai, S. M. W. Z., 2018. Confguration of intrusion prevention systems based on a legal user:. *Information Technology and Management,* 20(2), pp. 55-71.

Hamdan, M., 2022. *Youtube*. [Online]
Available at: https://www.youtube.com/watch?v=o-QNMSPbOGY
[Accessed 20 March 2024].

Jiang Qian, S. H. K. N., 2001. ACLA: A Framework for Access Control List (ACL) Analysis and Optimization. *Communications and Multimedia Security Issues of the New Century,* Volume 64.

S. Ansari, S. R. H. C., 2003. Packet sniffing: a brief introduction. *IEEE Potentials,* 21(5), pp. 17-19.

Usha Banerjee, A. V. M. S., 2010. Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of Computer Applications,* 6(7), pp. 1- 5.

Ahmad, N. (2023, May 12). *7 Best Rack Servers of 2023*. Retrieved from ServerWatch: https://www.serverwatch.com/hardware/top-rack-servers/

Basic Types Of Network Security Measures. (2022, June 9). Retrieved from Dot Security: https://dotsecurity.com/insights/blog-types-of-network-security-measures

Bliss, E. (2015, July 31). *Network Switch 101*. Retrieved from tom's Hardware: https://www.tomshardware.com/reviews/network-switch-basics,4123-3.html#:~:text=For%20the%20sake%20of%20simplicity%2C%20there%20are%20three,to%20this%20topic%3A%20unmanaged%2C%20intelligent%2Fsmart%20and%20fully%20managed.

Davidson, R. (2024, February 6). *The Higher Education ERP System*. Retrieved from SoftwareConnect: https://softwareconnect.com/roundups/best-higher-education-erp-software/

Husain, O. (2024, March 2024). *Best VPNs for South Africa in 2024 and some to avoid*. Retrieved from compaitech: https://www.comparitech.com/blog/vpn-privacy/best-vpn-south-africa/

Team, E. (2023, August 9). *Network infrastructure Desn - Planning a Campus Network*. Retrieved from NETWORK ENCYCLOPEDIA: https://networkencyclopedisa.com/network-infrastructure-design/