Cisco Networking Academy – Project

Sravya Duvvuri

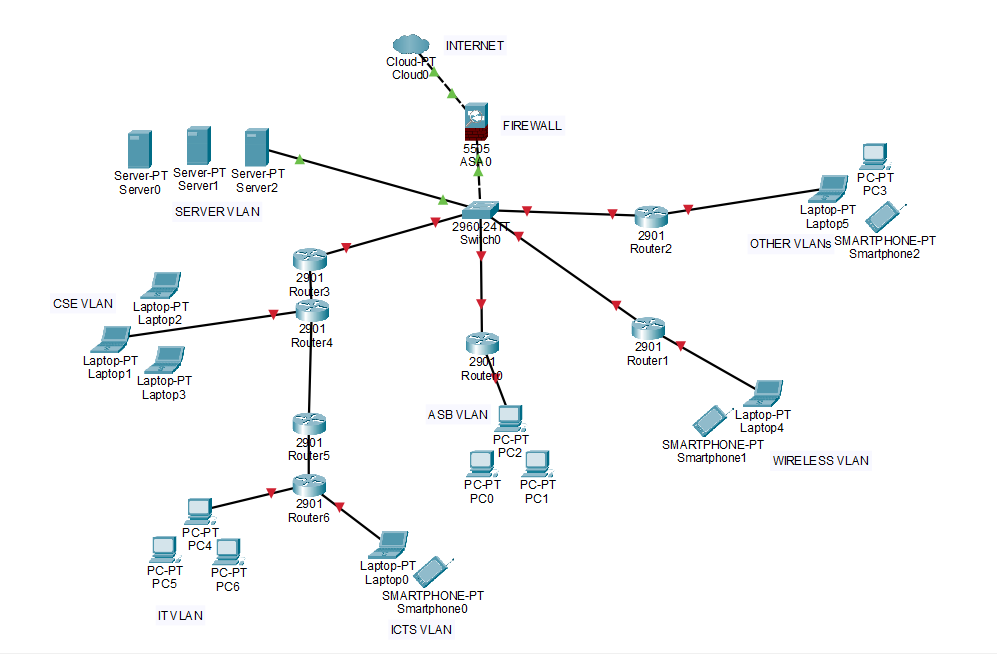
CB.EN.U4CSE22353

Problem Statement

Choose a university/college campus and analyse its network topology. Map the network using Cisco Packet Tracer and identify the security controls that are in place, such as network segmentation, intrusion detection systems, firewalls, and authentication and authorization systems. Apply the knowledge gained from the NetAcad cyber security course to conduct an attack surface mapping, aiming to identify potential entry points for cyber-attacks. Propose countermeasures to mitigate these risks.

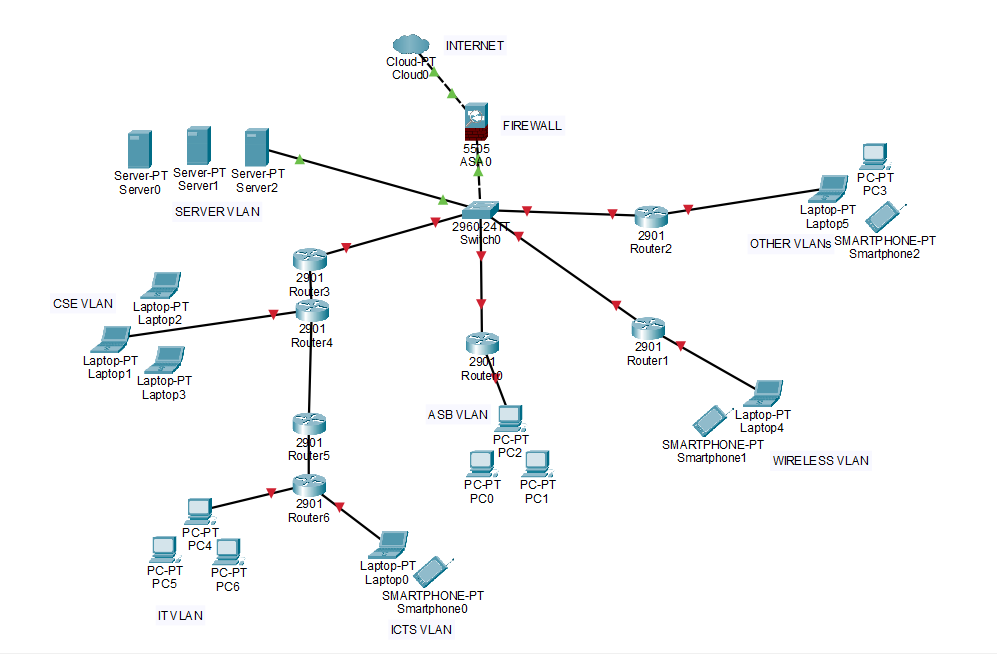
Introduction

To complete the given problem statement, to analyse and apply the knowledge I have gained about cybersecurity and networking, I have used the topology diagram of Amrita Vishwa Vidyapeetham, Coimbatore Campus as reference and its model has been created in Cisco’s packet tracer. The diagram reference is below.



Identified Security Risks with their Proposed Solutions

The network topology picture has been labelled with the identified risks which are described below



**(6)**

**(5)**

**(4)**

**(3)**

**(2)**

**(1)**

Following are the identified security risks and the proposed solutions to mitigate those risks:

1. Proxy server – it must be placed between Internet and the Firewall in the topology as it helps in preventing the user’s identity from being traced.
2. VPN – On a need basis, the end devices or the laptops, PCs etc must be enabled with a VPN.   
   (In the diagram above, any one of the areas to be implemented has been highlighted)
3. IDS /IPS must be enabled in the Firewall (if the functionality exists within the firewall, else implement) to prevent unauthorized / malicious traffic from Internet.
4. Communication Redundancy - instead of a single link, it is better to have a Primary and a Secondary internet link, in case the Primary link goes down then traffic can be routed via secondary link.
5. Firewalls – There needs to be a secondary firewall in case the primary firewall goes down to prevent any downtime for the internet access.
6. Inter VLAN communication – inter VLAN communication must be disabled between CSE VLAN, IT VLAN, ICTS VLAN, ASB VLAN, Wireless VLAN and Other VLAN’s so that unauthorized access can be restricted.

(In the diagram above, any one of the areas to be implemented has been highlighted)

Countermeasures to mitigate attack surface risks

1. Vulnerability Assessment – A vulnerability assessment needs to be done for the Firewall, Switch, Routers, Servers, Wi-Fi controllers at regular intervals.
2. MFA needs to be enforced for accessing the Network devices and making configuration changes. These changes must be carefully logged for any future investigation.
3. Strong Passwords must be enforced for the end users who will be accessing the infrastructure.
4. To prevent DoS and DDoS attacks, ensure patches and upgrades are current, distribute the workload across server systems, and block external Internet Control Message Protocol (ICMP) packets at the border.
5. Implement WPA2 standard for wireless security.
6. Hardening of the devices per standard and regular checks of its workings.
7. All data stored must be encrypted.
8. All the network infrastructure devices should be enabled with backup devices, for example we need to have primary Firewall and backup to ensure high availability.
9. Firewall Policies or ACL (Access control lists) must be reviewed on a periodic basis.

Terms

**VLAN** stands for Virtual Local Area Network. Its main purpose is to enhance network security, performance, and manageability. By separating devices into different VLANs, we can control which devices can communicate with each other, reducing the scope of traffic and potential security risks.

**IDS** stands for Intrusion Detection System. It is a security technology used to monitor and analyse network traffic for signs of malicious activity, policy violations, or unusual behaviour that could indicate a potential security breach or cyberattack.

**IPS** stands for Intrusion Prevention System. It is a security technology designed to complement and enhance the capabilities of an above-mentioned IDS. While the IDS detects and alerts on suspicious or malicious activity, an IPS takes it a step further by blocking or preventing those threats from reaching their targets.

**VPN** stands for Virtual Private Network. It enables secure and encrypted communication over a public network, such as the internet, between two or more devices by creating private and secure "tunnel" through which data can travel, protecting the data from interception and ensuring privacy and confidentiality.

**Firewalls** act as a barrier between a trusted internal network and an untrusted external network. The main purpose of a firewall is to control and monitor incoming and outgoing network traffic based on predetermined security rules. By doing so, firewalls help prevent unauthorized access, protect against cyber threats, and enforce security policies.

**Passwords** must be strong and unique, using a password manager which is a secure and convenient way to handle passwords. These accounts with strong passwords must be further secured using **MFA** or Multi-factor authentication.

**Vulnerability assessment** is the process of identifying, analysing, and evaluating security vulnerabilities in a network. The main goal is to discover potential weaknesses that could be exploited by attackers to compromise the confidentiality, integrity, or availability of the target.

**Access controls** includes – Encryption, Smart cards, Passwords, Biometrics, ACLs, Protocols, Firewalls, Routers, IDS, Clipping level thresholds, procedures, background checks, data classification etc.