AICTE - CISCO VIRTUAL INTERNSHIP PROJECT REPORT - 2024

CYBER SHIELD

Submitted by

ROHIT KANNA P R – 722821243048

AICTE ID: **STU662f41ea8a0ac1714373098**

Mentor: **Mr. J DHANASEKAR AP/ECE**

Domain: **CYBER SECURITY**

Department of Artificial Intelligence and Data Science

SRI ESHWAR COLLEGE OF ENGINEERING

(An Autonomous Institution - Affiliated to Anna University**)**

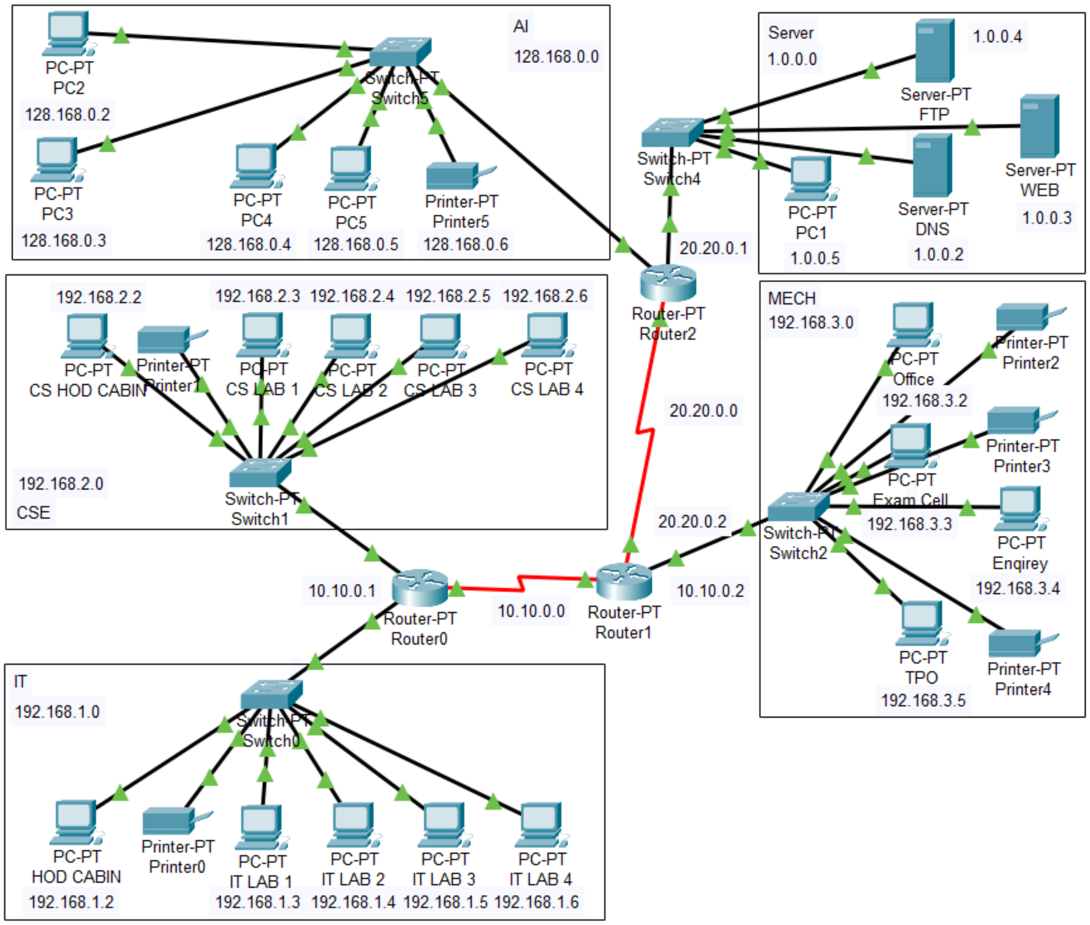
Coimbatore - 641 202

Introduction:

In the ever-evolving landscape of cybersecurity, safeguarding network infrastructures is paramount, particularly within educational institutions. This report delves into a comprehensive analysis and enhancement of our college's network topology, emphasizing the critical aspects of security controls and attack surface mapping. By leveraging Cisco Packet Tracer, we provide a visual representation of the current network setup, identify potential vulnerabilities, and propose robust countermeasures. Additionally, we design a secure hybrid working environment for faculty and students, ensuring restricted access to campus resources and implementing content filtering to curb misuse, thus fortifying the network against cyber threats.

PART 1:

The campus network of a university comprises several core components that are fundamental to its operation. At the heart of the network are the routers, which are critical devices responsible for directing traffic across different networks. These routers form the backbone of the network, ensuring that data packets find their way from one segment of the network to another efficiently. Complementing the routers are the switches, which connect and manage multiple devices within the same network segment. Switches play a pivotal role in ensuring that devices such as computers, printers, and servers can communicate seamlessly within the network.



Firewalls are another essential component of the campus network, tasked with protecting the network by controlling incoming and outgoing traffic based on predefined security rules. These rules help in preventing unauthorized access and in mitigating potential threats. The servers within the network host various critical services such as the university's website, email systems, and databases. These servers are the workhorses of the network, handling data storage, processing, and serving up resources as requested by users across the campus.

Wireless connectivity across the campus is provided by access points strategically placed to ensure comprehensive coverage. These access points allow students, faculty, and visitors to connect to the network wirelessly, facilitating mobility and ease of access. The integration of these core components creates a robust and dynamic network capable of supporting the diverse needs of a university environment.

Security is a paramount concern in the design and operation of the campus network. One of the primary security measures implemented is network segmentation, which involves dividing the network into different VLANs (Virtual Local Area Networks). Each VLAN is tailored to specific user groups such as administration, faculty, students, and guests. This segmentation helps in containing and managing network traffic more effectively and provides an additional layer of security by isolating different user groups.

Firewalls are configured with detailed rules to control traffic flow between these different network segments. By setting up stringent policies, the firewalls ensure that only authorized traffic is allowed to pass between segments, thereby protecting sensitive information and maintaining the integrity of the network. Additionally, the network employs Intrusion Detection Systems (IDS) which continuously monitor network traffic for signs of suspicious activity. These systems are vital in identifying and responding to potential security breaches in real time.

The campus network also relies on robust authentication systems to verify the identity of users attempting to access the network. Systems such as RADIUS (Remote Authentication Dial-In User Service) or LDAP (Lightweight Directory Access Protocol) are employed to handle user authentication. These systems ensure that only authorized individuals can gain access to the network, thereby safeguarding sensitive data and resources. Once authenticated, users are subject to authorization systems that employ Role-Based Access Control (RBAC). This approach restricts access to resources based on user roles, ensuring that individuals can only access information and services relevant to their responsibilities.

To maintain and troubleshoot the network, Cisco Packet Tracer is used as a primary tool for network mapping. This powerful simulation tool allows network administrators to create detailed network topology diagrams that illustrate the placement and interconnectivity of routers, switches, firewalls, and other network components. By using Cisco Packet Tracer, administrators can visualize the network structure, simulate potential issues, and test changes before implementing them in the live network. This proactive approach helps in maintaining network reliability and performance.

The network diagram produced using Cisco Packet Tracer serves as a blueprint for understanding the campus network’s design and operation. It provides a clear representation of how data flows through the network, highlighting key components and their interconnections. Such diagrams are invaluable for network planning, troubleshooting, and optimizing network performance.

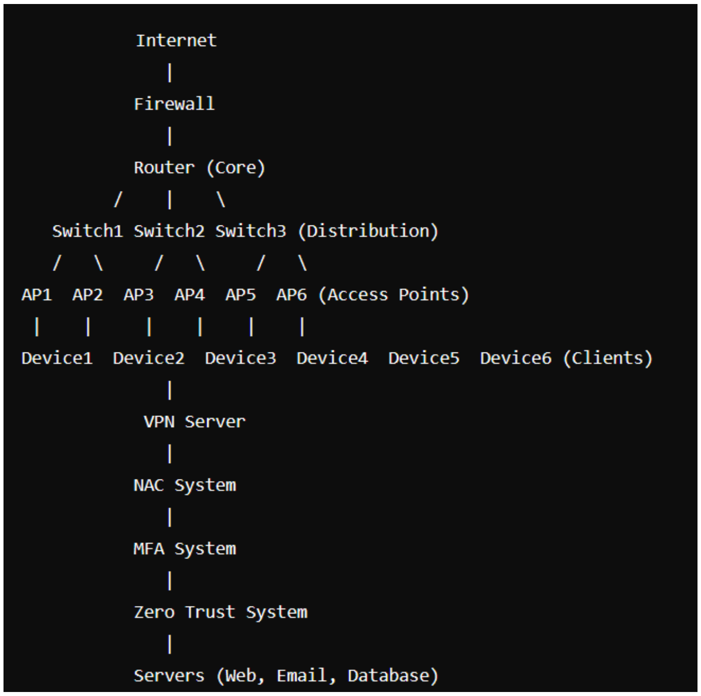
In essence, the campus network of a university is a complex and dynamic entity designed to support a wide range of activities and services. The core components – routers, switches, firewalls, servers, and access points – work in tandem to provide a reliable and secure network infrastructure. The implementation of security controls such as network segmentation, firewalls, IDS, authentication systems, and RBAC ensures that the network remains secure and resilient against potential threats. Tools like Cisco Packet Tracer aid in the effective management and maintenance of the network, ensuring that it can adapt to the evolving needs of the university community. Through meticulous planning, implementation, and monitoring, the campus network can provide a robust foundation for academic and administrative activities, fostering an environment of connectivity and collaboration.

Part 2:

The university’s campus network must meet the evolving needs of its faculty and students, ensuring secure access to resources both on-campus and remotely. Faculty members require secure access to academic databases, administrative tools, and communication platforms. Similarly, students need secure access to learning management systems, online libraries, and student portals from any location. Additionally, campus network services should be restricted from public internet access to protect sensitive data. These requirements demand robust security measures to prevent unauthorized access and cyber threats.

To address these requirements, the proposed solution integrates several key components into the existing network infrastructure. The first component is a Virtual Private Network (VPN), which will provide secure remote access to campus resources. VPNs establish encrypted tunnels, ensuring data transmitted between remote users and the campus network is protected from interception and tampering, allowing faculty and students to access resources securely from any location.

Multi-Factor Authentication (MFA) adds an extra layer of security for remote access by requiring users to provide two or more verification factors. This significantly reduces the likelihood of unauthorized access by making it harder for attackers to compromise user accounts.



```
             Internet
                |
             Firewall
                |
             Router (Core)
           /    |    \
     Switch1 Switch2 Switch3 (Distribution)
     /   \     /   \     /   \
  AP1  AP2  AP3  AP4  AP5  AP6 (Access Points)
   |    |     |    |    |    |
  Device1  Device2  Device3  Device4  Device5  Device6 (Clients)
                |
              VPN Server
                |
             NAC System
                |
             MFA System
                |
             Zero Trust System
                |
             Servers (Web, Email, Database)
```

Network Access Control (NAC) ensures that only authorized devices can connect to the network. NAC systems assess the security posture of devices attempting to connect and enforce policies to ensure compliance, preventing potentially compromised or non-compliant devices from accessing the network.

Incorporating a Zero Trust Architecture (ZTA) is another essential component. Zero Trust assumes threats can exist both inside and outside the network perimeter, enforcing strict access controls and continuous monitoring. ZTA principles ensure that all devices, whether inside or outside the network, are continuously authenticated and authorized.

The updated network diagram integrates these new components into the existing topology. VPN servers are added for secure remote access, NAC systems for device compliance, and MFA components to enhance authentication security. This comprehensive update ensures the network meets the evolving security and access requirements of the university community.

The proposed solution addresses several key risks and offers significant advantages. One primary risk addressed is unauthorized access. Implementing VPN and MFA ensures only authenticated and authorized users can access campus resources, significantly reducing the likelihood of unauthorized access. VPNs provide encrypted tunnels for data transmission, protecting sensitive information from being intercepted or tampered with during transit, preventing data breaches.

Device security is another critical risk addressed. NAC ensures only compliant devices are allowed to connect to the network by enforcing security policies and assessing the security posture of devices. This prevents compromised or insecure devices from accessing network resources, reducing the risk of malware infections and other security threats.

The proposed solution offers several advantages, enhancing the security and accessibility of campus resources. Secure remote access enables faculty and students to access necessary resources from any location, promoting flexibility and continuity in academic and administrative activities. MFA and Zero Trust Architecture significantly enhance security measures, providing robust protection against a wide range of cyber threats. MFA adds an extra layer of verification, making it more challenging for attackers to compromise user accounts, while Zero Trust principles ensure continuous authentication and strict access controls.

Moreover, the proposed solution is scalable, capable of growing with the university's needs. As the university expands and the number of users and devices increases, the solution can be scaled to accommodate growth without compromising security. This scalability ensures the network remains robust and secure, supporting the evolving needs of the university community.

```
Router> enable
Router# configure terminal

! Interface Configuration
Router(config)# interface g0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# interface g0/1
Router(config-if)# ip address 192.168.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

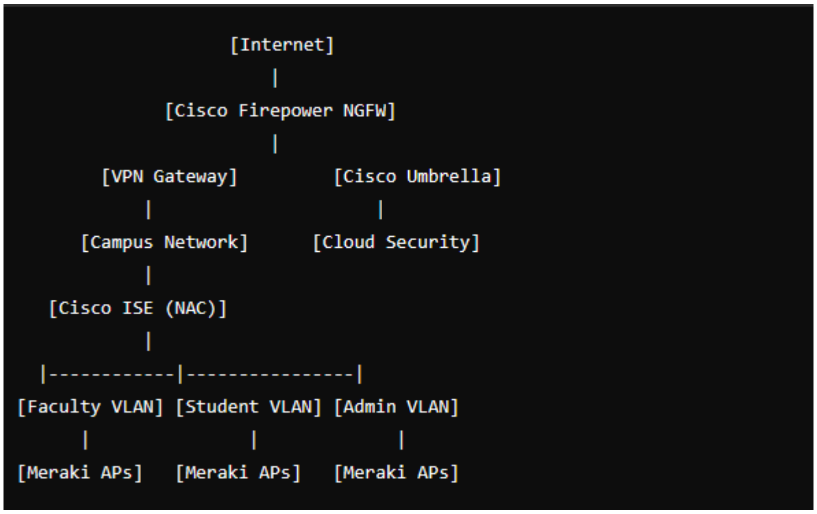
```
! Static Routing and NAT
Router(config)# ip route 0.0.0.0 0.0.0.0 g0/0
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 1 permit 192.168.2.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface g0/0 overload
Router(config)# interface g0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface g0/1
Router(config-if)# ip nat outside
Router(config-if)# exit

! Firewall Configuration
Router(config)# access-list 101 permit ip any any
Router(config)# access-list 102 deny ip any any
Router(config)# interface g0/0
Router(config-if)# ip access-group 101 in
Router(config-if)# exit


Switch> enable
Switch# configure terminal

! VLAN Configuration
Switch(config)# vlan 10
Switch(config-vlan)# name Faculty
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name Students
Switch(config-vlan)# exit

! Port Assignment to VLANs
Switch(config)# interface range fa0/1 - 2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit

Switch(config)# interface range fa0/3 - 4
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit
```

```
Access Point> enable
Access Point# configure terminal

! Faculty SSID
Access Point(config)# interface dot11radio 0
Access Point(config-if)# ssid FacultySSID
Access Point(config-ssid)# vlan 10
Access Point(config-ssid)# authentication open
Access Point(config-ssid)# end

! Student SSID
Access Point(config)# interface dot11radio 0
Access Point(config-if)# ssid StudentSSID
Access Point(config-ssid)# vlan 20
Access Point(config-ssid)# authentication open
Access Point(config-ssid)# end
```

Part 3:

The university needs to restrict students from accessing irrelevant or harmful websites using campus resources. This is essential to ensure that students focus on educational content and are protected from potentially harmful online material. Effective measures are required to monitor and control internet usage, ensuring that the network is used appropriately and efficiently.

To address this requirement, the proposed solution incorporates several key components into the existing network infrastructure. One primary component is Web Content Filtering. This involves using devices or software that categorize and filter web traffic based on predefined policies. By categorizing websites and applying filters, the system can block access to non-educational and potentially harmful websites, ensuring that students only access relevant content.



```
                    [Internet]
                        |
              [Cisco Firepower NGFW]
                        |
        [VPN Gateway]         [Cisco Umbrella]
            |                     |
      [Campus Network]      [Cloud Security]
            |
   [Cisco ISE (NAC)]
            |
  |------------|----------------|
[Faculty VLAN] [Student VLAN] [Admin VLAN]
      |               |             |
[Meraki APs]   [Meraki APs]   [Meraki APs]
```

Additionally, Firewall Rules will be updated to include additional restrictions on accessing certain categories of websites. Firewalls, already an integral part of network security, can be configured with specific rules to block access to websites that fall under unwanted categories. These rules enhance the existing security measures by adding another layer of control over internet usage.

The updated network diagram will incorporate web content filtering devices and updated firewall rules. These components will work together to create a secure and focused online environment for students, ensuring that they have access to necessary educational resources while being protected from irrelevant or harmful content.

The proposed solution addresses several key risks and offers significant advantages. One primary risk addressed is the misuse of resources. By implementing web content filtering and updating firewall rules, the network restricts access to non-educational and potentially harmful websites. This ensures that students focus on educational content and are not distracted by irrelevant online material.

Another critical risk addressed is network congestion. Blocking unnecessary content reduces bandwidth usage, ensuring that network resources are used efficiently. This helps in maintaining optimal network performance, especially during peak usage times, and prevents slowdowns caused by high bandwidth consumption from non-educational content.

The proposed solution offers several advantages. Improved productivity is a significant benefit, as restricting access to non-educational websites ensures that students remain focused on their studies and educational resources. By limiting distractions, students can make better use of their time and resources, leading to enhanced learning outcomes.

Enhanced security is another crucial advantage. Preventing access to malicious websites reduces the risk of malware infections and other cyber threats. This protection ensures that the network remains secure and that students' personal information and campus resources are safeguarded.

```
Router> enable
Router# configure terminal
Router(config)# ip dns server
Router(config)# ip domain lookup
Router(config)# ip name-server 208.67.222.222
Router(config)# ip name-server 208.67.220.220
Router(config)# exit
```

To implement the proposed solution effectively, several policies will be established:

1. Allow Educational Sites: Permit access to educational and research websites to ensure students have the resources they need for their studies.
2. Block Social-Media: Restrict access to social media platforms during school hours to minimize distractions and encourage students to focus on educational content.
3. Block Explicit Content: Prevent access to adult content and other inappropriate websites to protect students from harmful material.
4. Allow Campus Resources: Ensure that all campus resources, such as the university website, email, and online libraries, are always accessible.