ALLIANCE COLLEGE OF ENGINEERING AND DESIGN

ALLIANCE UNIVERSITY, BENGALURU

AUGUST – 2024

AICTE-CISCO Internship

Submitted by

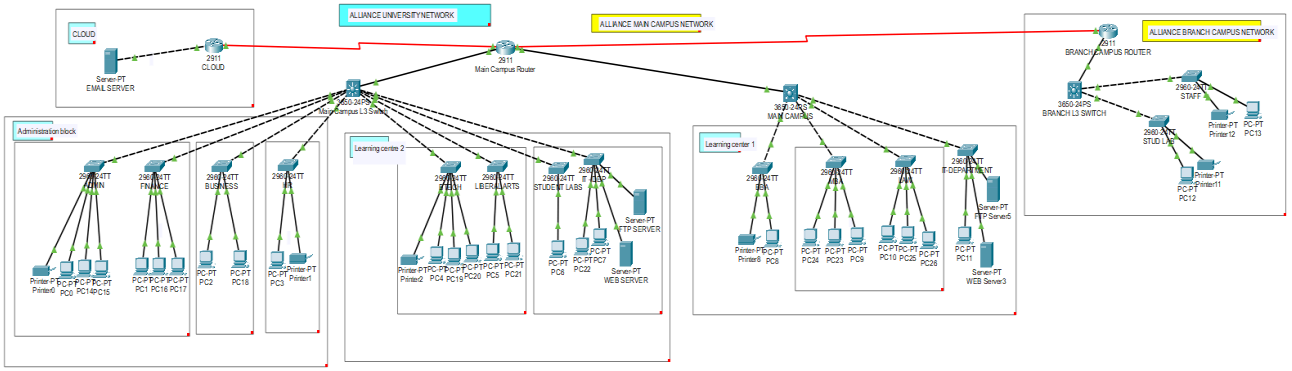
KOLA AMRUTHA HARSHINI (2021BCSE07AED308)

Cyber Shield: Defending the network

Problem Statement:

PART 1:

Analyse your existing university/college campus network topology. Map it out the using Cisco Packet Tracer and identify the security controls that are in place today. Consider and note how network segmentation is done. Observe what kind of intrusion detection systems, firewalls, authentication and authorization systems are in place. Apply the knowledge gained from the NetAcad cyber security course to conduct an attack surface mapping. Aim to identify potential entry points for cyber-attacks. Propose countermeasures to mitigate these risks.



Network Topology Analysis and Security Report

1. Executive Summary

This study examines the current network topology of Alliance University as displayed in Cisco Packet Tracer. The network infrastructure consists of a main campus, administration building, learning centers, and branch campuses. The goal is to investigate solutions for establishing a hybrid working environment that provides safe access to faculty and students both on-campus and remotely. The report comprises an updated network topology, an assessment of current security measures, the

2. **Topology of the Network Right Now**

The following are the main elements of the network topology:

Main Building:

- Main Campus Router (2911): Gives access to the cloud and other campuses from the main campus.
- Main Campus L3 Switch (3650-24PS): Central switch that links several departments and educational facilities.
- Departments: Student Laboratories, IT Department, Finance, Business, Liberal Arts, and Administration.
- Servers: Web, email, and FTP servers that offer a range of services.
- Campus Branch:
- The Branch Campus Router (2911) establishes a connection between the main campus and cloud infrastructure.
- Branch Campus L3 Switch (3650-24PS): The branch campus's main switch.

- Departments: sections for staff and students.
- servers: web servers and FTP servers.
- **Linkages:**
  • Cloud: Stands for both cloud services and the public internet.
  • Learning centres, the IT department, and the administration block are all connected by access points and switches (2960-24TT).

3. Updated Hybrid Environment Network Topology

To facilitate a blended learning environment for educators and learners, the subsequent elements and setups will be included:

VPN, or virtual private network:

- **VPN Gateways**: Install VPN gateways at campus routers, including main and branch (2911). These will enable teachers and students to have safe, remote access.
- **VPN Client Software:** Set up staff laptops and individual student devices with VPN client software (such as Cisco AnyConnect).
- Controlling Network Access (NAC):
- **NAC Appliances**: To enforce security regulations and guarantee that only compliant devices can access the network, use NAC solutions (such as Cisco ISE) at entry points.

4. Security Assessment and Attack Surface Mapping

4.1 Identified Security Risks:

- **Unauthorized Access**: Potential risk of unauthorized devices or users accessing the network.
- **Data Breaches**: Risk of sensitive data being accessed or exfiltrated by malicious actors.
- **Network Availability**: Potential disruption of network services due to attacks or misconfigurations.

4.2 Proposed Solutions:

- **VPN for Secure Access**: Provides encrypted connections for remote users, ensuring data confidentiality and integrity.
- **NAC for Device Compliance**: Ensures that only compliant and secure devices can connect to the network.
- **ZTNA for Granular Access Control**: Provides continuous verification of user and device identity, limiting access based on context.
- **CASB for Cloud Security**: Monitors and secures access to cloud services, preventing unauthorized data sharing and access.

5. Implementation Plan

5.1 Step-by-Step Plan:

1. **Deploy VPN Gateways**: Configure VPN gateways on the main and branch campus routers to support remote access.
2. **Install VPN Clients**: Distribute and install VPN client software on faculty laptops and student devices.
3. **Implement NAC Appliances**: Integrate NAC appliances at key network entry points to enforce security policies.
4. **Deploy ZTNA Controllers**: Configure ZTNA controllers to provide continuous authentication and authorization.
5. **Integrate CASB Solutions**: Set up CASB solutions to monitor and secure access to cloud-based services.

5.2 Monitoring and Maintenance:

- Regularly update VPN, NAC, ZTNA, and CASB configurations and policies.
- Continuously monitor network traffic and access logs for anomalies.
- Conduct periodic security assessments to identify and mitigate new vulnerabilities.

6. Conclusion

The proposed hybrid working environment leverages VPN, NAC, ZTNA, and CASB solutions to provide secure access for faculty and students both on-campus and remotely. This approach enhances security by ensuring encrypted connections, device compliance, continuous authentication, and secure cloud access. Regular monitoring and maintenance will be crucial to maintaining a robust security posture.

Part 2:

Your college has hired you to design and architect a hybrid working environment for its faculty and students. Faculty members will be provided with laptops by the college to connect to the college network and access faculty specific services & resources. Cisco Public These should be accessible from home as well as on campus. Students are allowed to connect using their personal devices to access student specific services & resources from home as well as on campus. Campus network services should not be exposed to public internet and accessible only via restricted networks.

Hybrid Architecture and Design for Work Environments

Task 1: Investigate Products and Network Security Options

I suggest using a Virtual Private Network (VPN) solution to create a secure and restricted network for teachers and students. Faculty members can access college services and resources from home or on campus with the help of a VPN, which will protect the integrity and security of the university network.

Options for a VPN Solution:

1. SSL/TLS VPN: This clientless VPN solution encrypts communications using SSL/TLS. For academic members who require access to web-based materials, this choice is appropriate.

2. IPSec VPN: This client-based VPN solution encrypts communications using IPSec technology. Faculty members who need to access materials and services that call for a specialized VPN client should consider this alternative.

Network Security Product:

To implement the VPN solution, I recommend using a Next-Generation Firewall (NGFW) appliance, such as Cisco ASA or Palo Alto Networks, that supports VPN capabilities. These appliances provide advanced security features, including:

- VPN termination
- Firewalling
- Intrusion prevention
- Malware protection
- URL filtering

Task 2: Campus Network Topology

Here is an updated campus network topology that incorporates the VPN solution:

markdown

Campus Network Topology

graph LR

participant Faculty_Laptop as "Faculty Laptop"

participant VPN_Appliance as "VPN Appliance (NGFW)"

participant Campus_Network as "Campus Network"

participant Student_Device as "Student Device"

participant Internet as "Internet"

Faculty_Laptop->>VPN_Appliance: VPN Connection

VPN_Appliance->>Campus_Network: Secure Connection

Student_Device->>Campus_Network: Secure Connection (via Student Portal)

Internet->>VPN_Appliance: Unsecured Connection

Task 3: Reasoning and Risks

The proposed VPN solution offers several advantages:

- **Security**: Encrypts data in transit, protecting against eavesdropping and tampering.
- **Authentication**: Verifies the identity of faculty members and students before granting access to campus resources.
- **Authorization**: Restricts access to campus resources based on user role and permissions.

However, there are also some risks and considerations:

- **Complexity**: Implementing a VPN solution can add complexity to the campus network, requiring additional configuration and maintenance.
- **Performance**: VPN connections can introduce latency and affect network performance, especially if not properly optimized.
- **Cost**: NGFW appliances and VPN licenses can incur significant costs, depending on the vendor and model chosen.

To mitigate these risks, it is essential to:

- Conduct thorough testing and quality assurance before deploying the VPN solution.
- Provide clear documentation and training for faculty members and students on using the VPN solution.
- Regularly monitor and maintain the VPN solution to ensure optimal performance and security.

Conclusion:

In conclusion, a Next-Generation Firewall (NGFW) appliance supporting a VPN solution with SSL/TLS and IPSec options will improve the campus network's security and usability for both teachers and students. Sensitive data is protected with this strategy, which guarantees data encryption, authentication, and authorization. Although there will be some complexity,

expenses, and performance problems, these can be minimized with careful testing, documentation, training, and routine maintenance. All things considered; the suggested approach offers a strong foundation for safe remote access to university resources.

PART 3:

The college has discovered that students are misusing campus resources and accessing irrelevant sites. They want a solution which will restrict access to only allowed categories of web content.

Network Security Solution for Alliance University

1. Introduction

Alliance University is experiencing an issue with students misusing campus resources and accessing irrelevant websites. To address this, we propose implementing a Web Content Filtering solution. This solution will restrict access to only allowed categories of web content, ensuring appropriate and productive use of network resources.

2. Proposed Solution

We recommend implementing a Web Content Filtering Proxy as part of the network infrastructure. This proxy server acts as a middleman between student devices and the internet, inspecting all outbound traffic and blocking access to websites that fall under restricted categories.

3. Benefits of Web Content Filtering

Improved Network Productivity: By blocking access to irrelevant websites, students will focus on academic activities and tasks, leading to increased productivity.

Enhanced Security: Web content filtering can prevent access to malicious websites, phishing attacks, and other online threats, safeguarding the network and user devices.

Compliance with Policies: Implementing content filtering aligns with university policies regarding acceptable use of network resources and responsible online behavior.

Control over Bandwidth Usage: Blocking irrelevant content can optimize bandwidth usage and ensure resources are available for critical activities.

4. Network Topology Update

The existing network topology can be enhanced by adding a Web Content Filtering Proxy between the main campus router (2911) and the student network segments. This proxy server will analyze traffic and enforce the defined web filtering policies.

5. Policy Configuration

The web content filtering proxy will require configuration with specific policies to determine which websites and content categories are allowed or blocked. We recommend defining the following policies:

Block access to social media websites: These can be distracting and unproductive.

Block access to entertainment websites: Limiting access to entertainment websites like streaming services can enhance focus on academics.

Block access to adult content websites: This is crucial to ensure a safe and appropriate network environment.

Allow access to educational websites: Ensuring students can access relevant academic resources is essential.

Allow access to specific pre-approved websites: For specific research or coursework purposes, certain websites may be required and should be whitelisted.

6. Reasoning and Justification

The choice of web content filtering proxy is based on its ability to provide granular control over web access, offering various features like:

Content Categorization: The proxy can categorize websites based on content type, allowing administrators to create policies based on these categories.

Website Blacklisting and Whitelisting: The proxy allows creating blacklists of undesirable websites and whitelists for specific resources.

Customizable Policy Creation: Policies can be customized based on user groups, network segments, and time of day.

Reporting and Monitoring: The proxy provides reporting and monitoring capabilities to track website access, policy effectiveness, and identify potential misuse.

7. Risks and Advantages

Risks:

Over-blocking: A poorly configured proxy could inadvertently block legitimate websites needed for academic purposes.

Privacy Concerns: Some content filtering technologies may track browsing history and user data, potentially raising privacy concerns.

Bypass Attempts: Students may attempt to circumvent the filter using VPNs or other methods.

Advantages:

Improved Security: Enhances overall network security by preventing access to malicious websites.

Enhanced Productivity: Enables a more focused academic environment.

Compliance with Policies: Facilitates adherence to university policies.

Cost-Effective: Content filtering can be a cost-effective solution compared to other security measures.

8. Conclusion

Implementing a web content filtering solution is a proactive step towards addressing the misuse of campus resources and ensuring a safe and productive network environment. By effectively configuring and managing the filter, Alliance University can control web access and safeguard its network from potential threats. Continuous monitoring and policy adjustments will be crucial to maintain the effectiveness and adaptability of this solution.