7-2 Project Three: Restructuring Status Report

Joshua Merren

Southern New Hampshire University

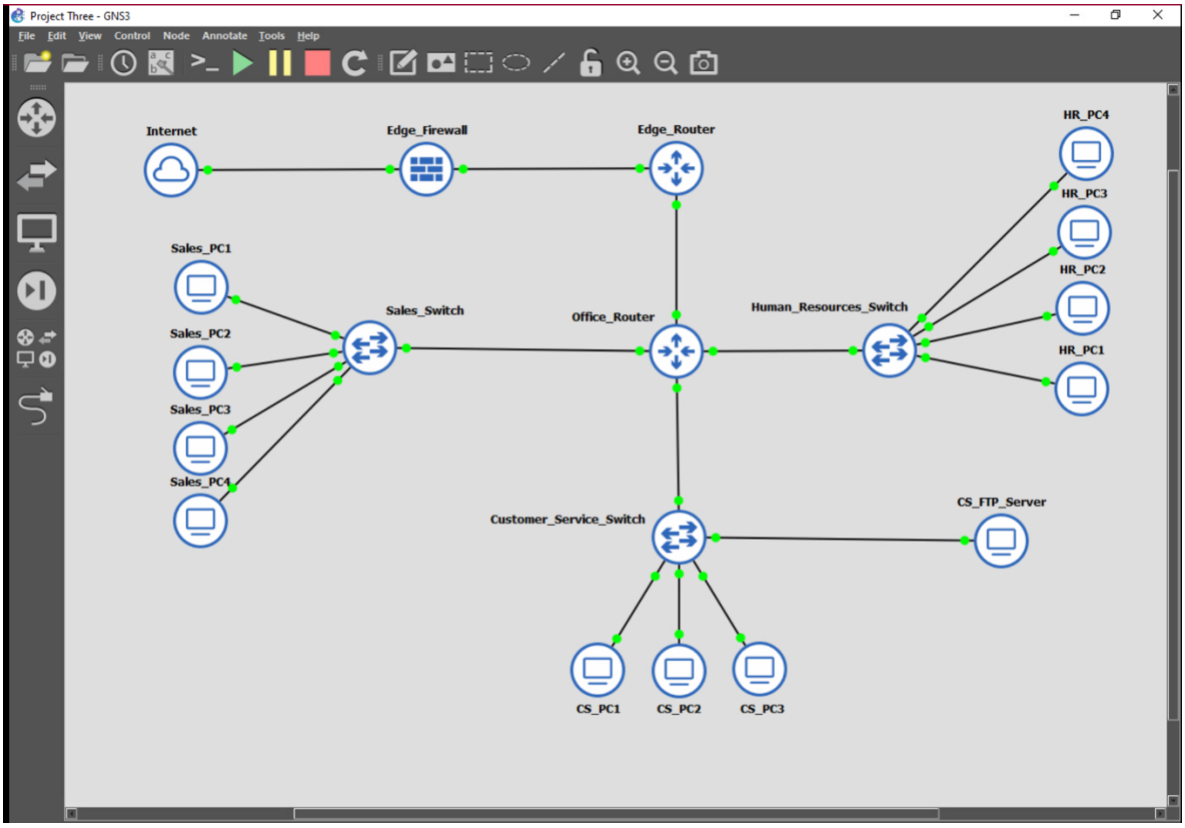
CYB-310-13414-M01 Network Defense

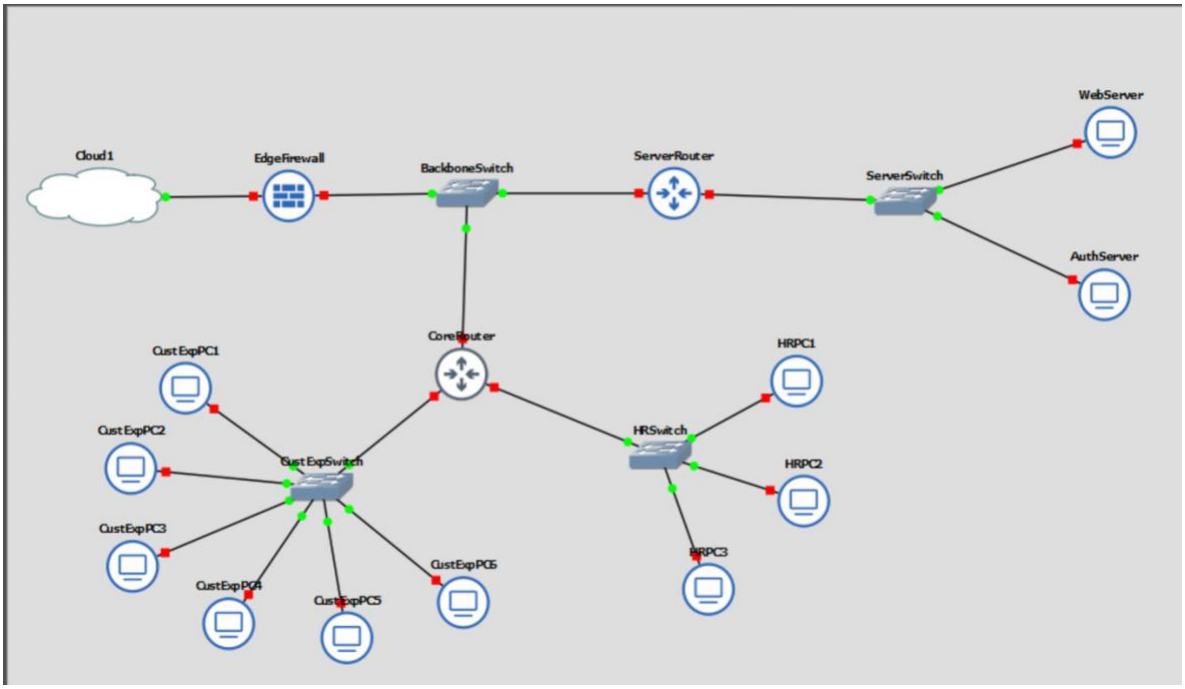
Professor Megan Buckner

15 October 2024

I. **Network Reconfiguration**: Include the following screenshots:

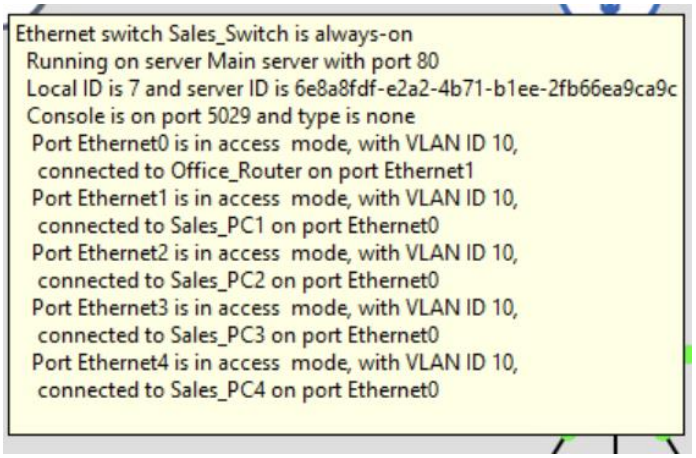
A. **Network diagram**

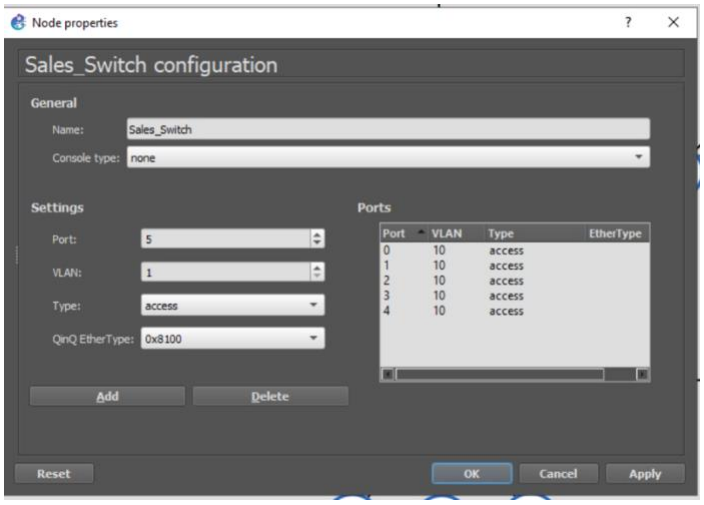




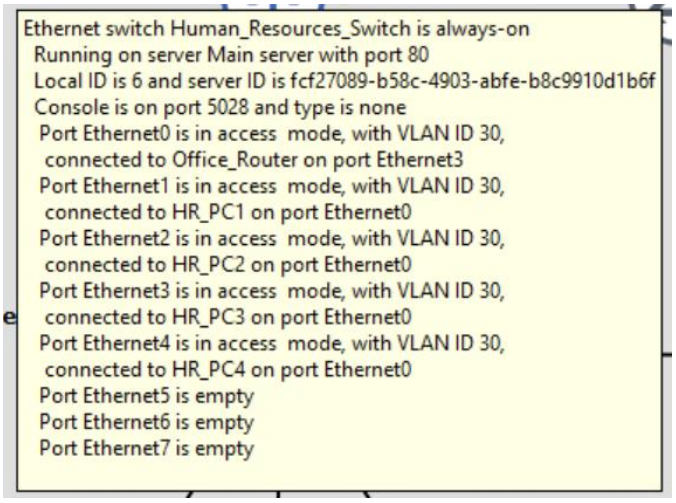
B. **Port assignment and VLAN assignment** for each switch

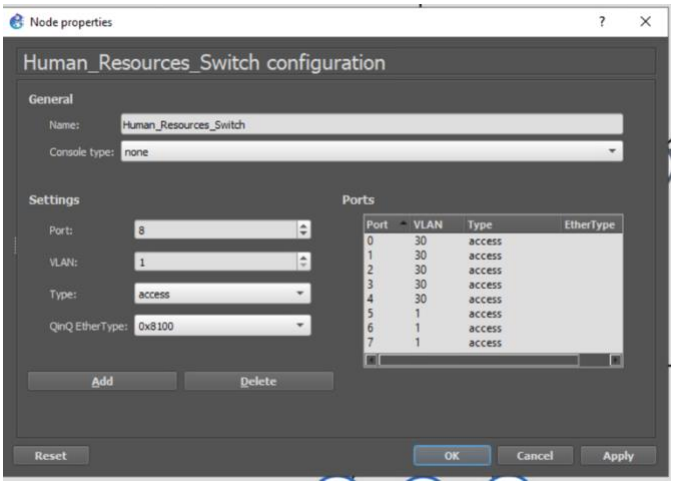
Sales Switch:



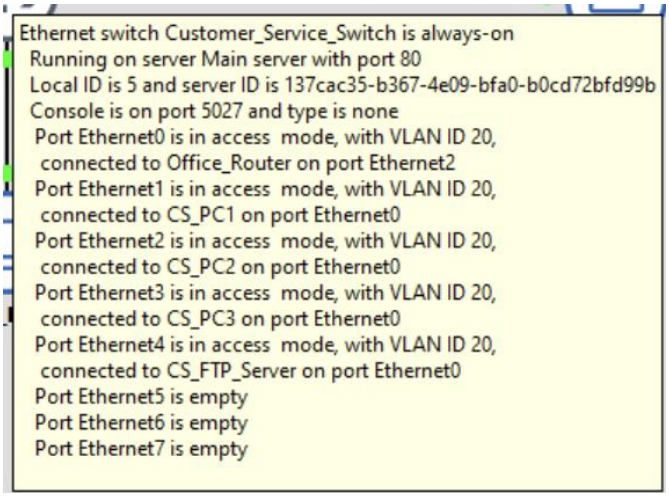


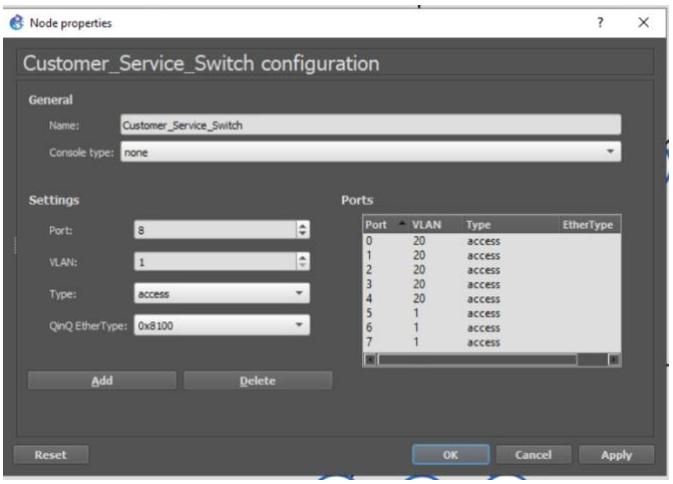
HR Switch:





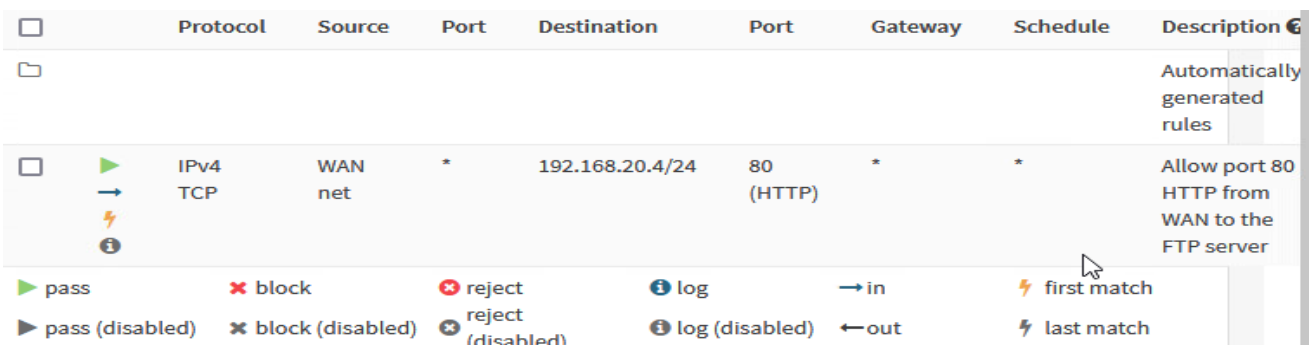
Customer Service Switch:





II. **Traffic Flow Configuration**: Include screenshots of the following:

A. Configure a firewall rule to **allow port 80** HTTP from the WAN to the FTP server.



	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
	IPv4 TCP	WAN net	*	192.168.20.4/24	80 (HTTP)	*	*	Allow port 80 HTTP from WAN to the FTP server

pass | block | reject | log | in | first match
pass (disabled) | block (disabled) | reject (disabled) | log (disabled) | out | last match

B. Configure a firewall rule to **allow port 443** HTTPS from the WAN to the FTP server.

	IPv4 TCP	WAN net	*	192.168.20.4/24	80 (HTTP)	*	*		Allow port 80 HTTP from WAN to the FTP server
	IPv4 TCP	WAN net	*	192.168.20.4/24	443 (HTTPS)	*	*		Allow Port 443 HTTPS from the WAN to the FTP server

pass | block | reject | log | in | first match
pass (disabled) | block (disabled) | reject (disabled) | log (disabled) | out | last match

C. Configure a firewall rule to **block port 80** HTTP from the WAN to any other system.

	IPv4 TCP	WAN net	*	*	80 (HTTP)	*	*		Block port 80 HTTP from WAN to any other system

pass | block | reject | log | in | first match

D. Configure a firewall rule to **block port 443** HTTPS from the WAN to any other system.

	IPv4 TCP	WAN net	*	*	80 (HTTP)	*	*		Block port 80 HTTP from WAN to any other system
	IPv4 TCP	*	*	*	443 (HTTPS)	*	*		Block port 443 HTTPS from WAN to any other system

III. Organizational Security Strategy

A. Explain how the **security posture** of the organization has been improved by the restructuring.

Restructuring our network has significantly improved our security posture by improving the protective measures across the organization. By redesigning the network layout and tightening firewall rules, we have significantly reduced vulnerabilities that attackers could

exploit. We deploy advanced detection technologies to monitor and alert us to suspicious activities, enhancing our proactive response to threats. Network segmentation improvements have isolated critical assets to prevent unauthorized access and potential breaches. We have also strengthened data security by implementing robust encryption protocols for data at rest and in transit, ensuring that intercepted data remains unreadable. Moreover, comprehensive logging and monitoring have increased our visibility into network activities, enabling us to identify and address potential security incidents better. We have updated access controls to ensure that only authorized personnel can access sensitive network segments, effectively reducing the risk of data leaks. We have enhanced compliance with industry standards, maintaining trust with our clients and partners. We also intensified our cybersecurity awareness training, educating employees about security practices and their role in maintaining our cybersecurity defenses. These strategic improvements have fortified our network against external threats and positioned us as a resilient organization facing evolving cyber challenges.

B. Describe how the tenets of the **CIA triad** (confidentiality, integrity, and availability) are affected by the restructuring.

Confidentiality: The network restructuring has significantly boosted the confidentiality of organizational data by incorporating advanced security measures. Confidentiality in cybersecurity refers to the protection of information from unauthorized access. We have accomplished this by implementing encryption for data at rest and in transit, ensuring that intercepted data remains secure. Additionally, we have enforced multi-factor authentication and robust access controls, which help verify and limit access based solely on user permissions.

These steps are crucial for preventing unauthorized data breaches and safeguarding sensitive information within the organization (University of Tulsa, 2024).

Integrity: Integrity in the context of cybersecurity is about maintaining the accuracy and completeness of data. Our restructuring has reinforced data integrity by deploying intrusion detection systems that monitor and block potential threats in real-time, thus preventing unauthorized data modifications. Furthermore, we utilize regular data backups and validation techniques to ensure that data can be restored to its original state and is entered correctly into our systems. These steps protect against common threats like malware, ransomware, and SQL injection attacks, which could otherwise compromise the integrity of our data (University of Tulsa, 2024).

Availability: Ensuring data availability means keeping our systems accessible for legitimate use at all times, which is essential for operational continuity. The restructuring has enhanced this by using redundant systems and load balancers that distribute incoming network traffic across multiple servers. This setup minimizes downtime and mitigates the impact of distributed denial-of-service (DDoS) attacks. Regular system maintenance and continuous monitoring are also part of our strategy to promptly address and resolve any issues that could disrupt service availability. These efforts ensure users can access the data and systems they need without delay (University of Tulsa, 2024).

Reference:

University of Tulsa. (2024, January 4). *What is the CIA triad?* The University of Tulsa. Retrieved October 15, 2024, from https://online.utulsa.edu/blog/what-is-the-cia-triad/