Student Name: Uzoma Uche

Student No: 22077181

Course: Network Security (LD7007)

Instructor: Dr Syed Raza &

Dr Nasr Abosata

Word Count: 3827

The Network Security Implementation using ACL, IPS,VPN & ASA Firewall.

**Table of Contents**

1. Executive Summary

**2. Architecture & Communication - BLOCK A**

2.1 Configuration of Internet Protocol Connectivity & Device Hardening

2.2 Configuration of Servers DHCP, DNS, WEB, & SYS-Log

2.3 Configuration of Dynamic Routing [OSPF] & Inter-VLAN Routing/Trunking

**3. Block B: Secure Operations and Service Delivery**

3.1 Implementation of ACL on Routing Device

3.2 Implementation of Site-To-Site IPSec VPN

3.3 Implementation of NIPS & Testing

3.4 Firewall configuration

**4. Research and Development**

4.1 Zero Trust Network Security Framework

4.2 Overview of VPN Reliability

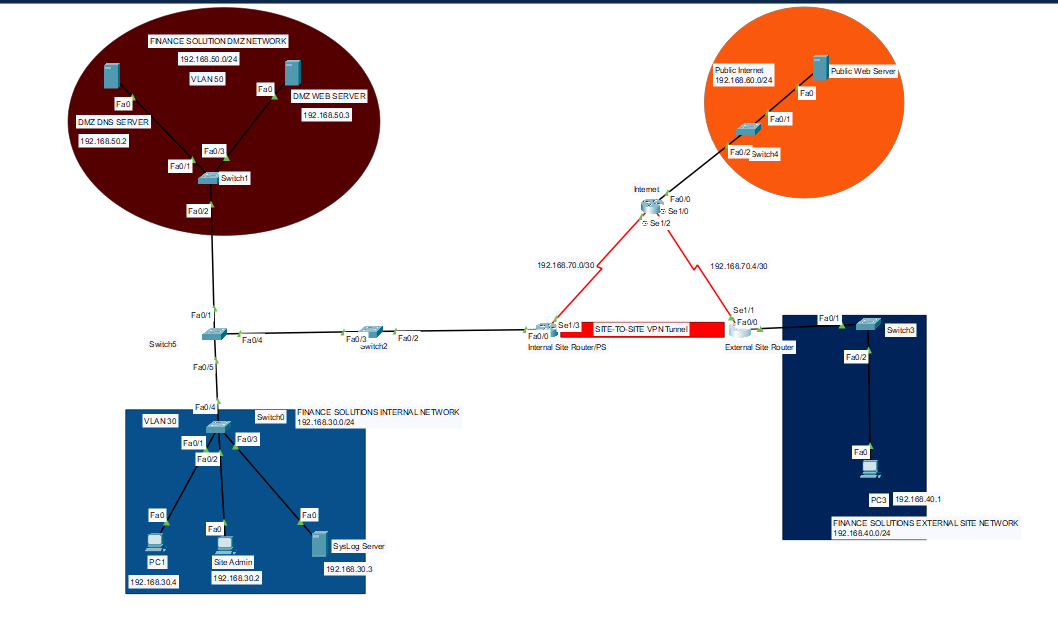
4.3 Cryptographic Mechanism of IPsec

5. Future Work

Conclusion

References

**NETWORK TOPOLOGY**



**Fig. 1**

**Executive Summary**

In the provided network topology, there is a direct connection between the DMZ (Demilitarized Zone) network and the internal network via a switch. Meanwhile, the other two networks are separated by routers, one connected through a serial DTE connection and the other through a Site-to-Site VPN tunnel. My objective is to bolster network security across the internetwork and the Wide Area Network (WAN). To achieve this, I intend to implement various security measures, including the establishment of a Site-to-Site VPN tunnel, the implementation of Access Control Lists (ACLs), and the deployment of an IOS-based Intrusion Prevention System (IPS).

Furthermore, I will undertake the essential process of device hardening to enhance the security of the organization's Local Area Network (LAN). To facilitate this endeavor, I will leverage an appropriate network simulation environment. Notably, the organizational network is already equipped with an integrated IPsec VPN solution, which ensures robust encryption to safeguard data confidentiality and integrity.

The comprehensive network design will be grounded in Cisco devices and realized using the Cisco Packet Tracer platform. The advantage of this simulation environment lies in its faithful replication of Cisco device components, enabling us to validate configurations in a true-to-life manner. The commands utilized within the simulation environment will directly translate to real-world device settings, streamlining the deployment process.

Through Cisco Packet Tracer, I will create a virtual network closely resembling the actual network setup. This will enable me to rigorously test the effectiveness of various security protocols before their application to live systems. My aim is to configure IP connectivity, DHCP, DNS, web services, SYS-Log, OSPF, trunking, and IPsec VPN protocols to bolster the security of the topology.

Subsequently, I will offer a comprehensive overview of the Zero Trust Network Security Framework, shedding light on its core principles and benefits. I will also examine the dependability of VPN systems and the IPsec's underlying cryptographic algorithms, giving you a thorough knowledge of these crucial elements.

The next stage of my project will include a thorough explanation of how to configure DHCP, DNS, web services, SYS-Log, RIPV2, trunking, and IPsec VPN, among other things. This detailed instruction manual will guarantee the efficient application of these security measures, nurturing a safe and dependable network architecture.

In conclusion, the goal of my endeavour is to build a strong and secure network environment by combining security mechanisms that have been tested and confirmed using Cisco Packet Tracer. This method not only strengthens network security but also makes it easier to fully comprehend key security ideas, enabling our firm to successfully mitigate possible risks.

**2. Block A: Architecture and Communication**

1. Block A: Network Architecture and Communication

In this section, I will undertake the initial configuration of essential devices. To accomplish this, I need to first identify the devices within the network topology. The routers utilized are Cisco 2811 integrated services routers, each capable of managing multiple WAN interfaces. These routers are equipped with four high-speed WAN slots, facilitating connections for various technologies like T1, xDSL, and others.

2. The network also incorporates six Cisco 2960-24TT switches, each furnished with 24 ports, ensuring rapid data transmission. Moving on to the server setup, there are a total of four servers strategically positioned across three distinct locations. Notably, two of these servers are situated within the DMZ Network location. Specifically, there is a DMZ DNS server and a DMZ web server present in this segment. This arrangement allows the DMZ to operate as a dedicated subnetwork, effectively linking hosts situated on the external network.

3. In this network setup, the DMZ Network plays a crucial role by directly interfacing with the internal network. It serves as the manager for all hosts within that network segment. The internal network encompasses a SysLog server for streamlined log management. Additionally, the system administrator is linked to this segment to access logs and take necessary actions based on them. This administrator connection serves as the entry point for other internal hosts to access the network.

4. The entire arrangement is connected through the internal Site Router, facilitating communication with other parts of the topology. On the opposite side of the topology, two distinct sections are present, each connected through its dedicated router.

5. The first section, the Public Internet Network, involves a Public Web Server functioning as the gateway for internet access. This server enables the organization to share their hosted web pages with the internet audience. A router connects this section to the broader internet, ensuring proper connectivity.

6. The second section, known as the External Site Network, serves as a segregated space for guest systems. An External Site Router isolates this segment, and an external host is linked to the router.

7. The overall topology relies on class C private IP addresses for configuration. The internal network operates within the IP address block 192.168.30.0, the DMZ network utilizes 192.168.50.0, the public internet employs 192.168.60.0, and the external site network uses 192.168.40.0. All four sections employ a subnet mask of 255.255.255.0.

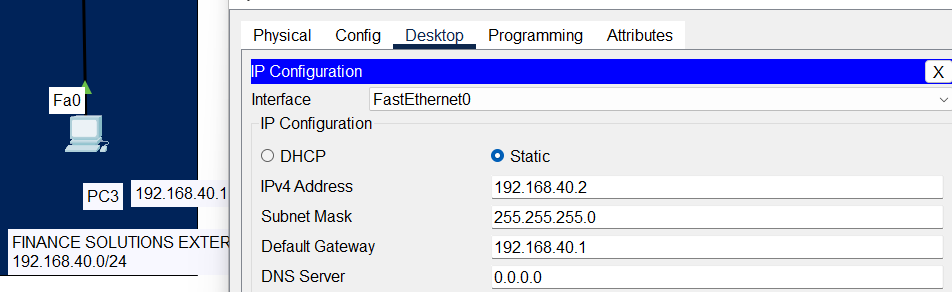
8. Notably, the routers are interconnected through serial DTE connections, with the IP address block 192.168.70.0. These connections are tailored for only two hosts, as defined by the subnet mask 255.255.255.252.

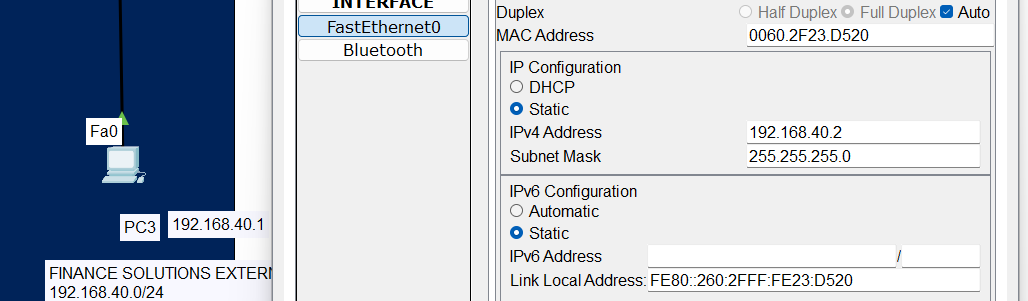
9. An interesting facet of the setup is the Site-to-Site VPN Tunnel, establishing a secure connection between the Internal Site Router and the External Site Router.

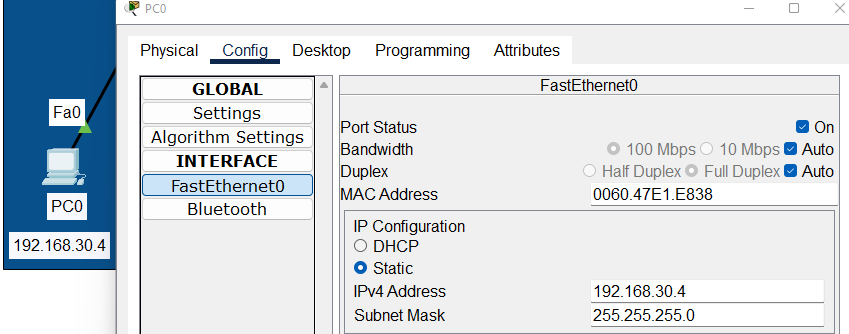
To enhance the security of the devices, a fundamental level of hardening has been implemented in the router configurations.

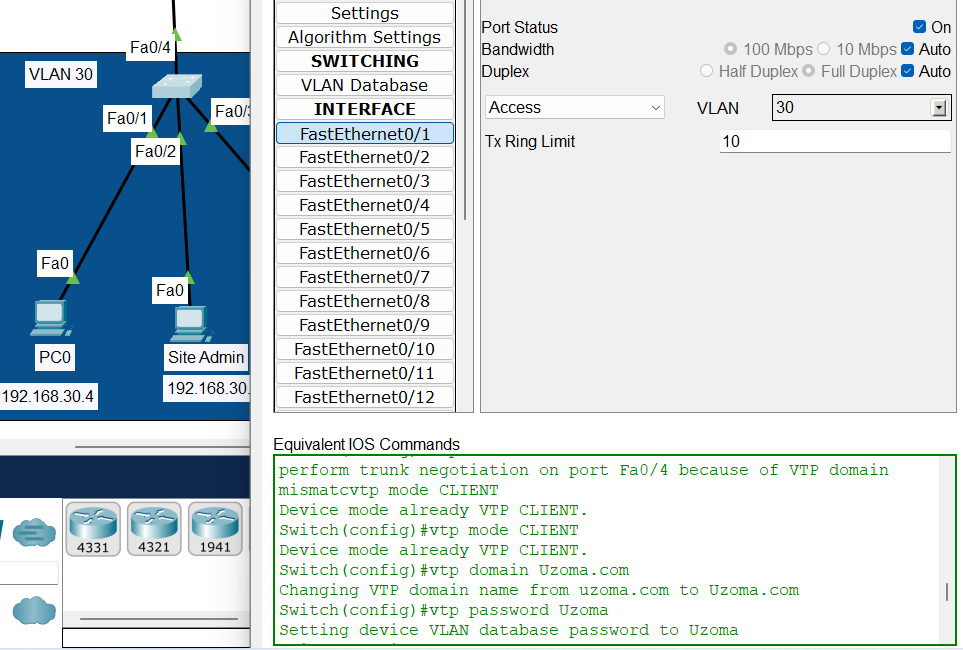
As part of the initial steps in device hardening, the routers have been set up with specific configurations. To establish clear identification, the routers have been assigned distinct names: "InternalNetwork" for the Internal Site Route, "ExternalNetwork" for the External Site Route, and "Internet" for the internet connection.

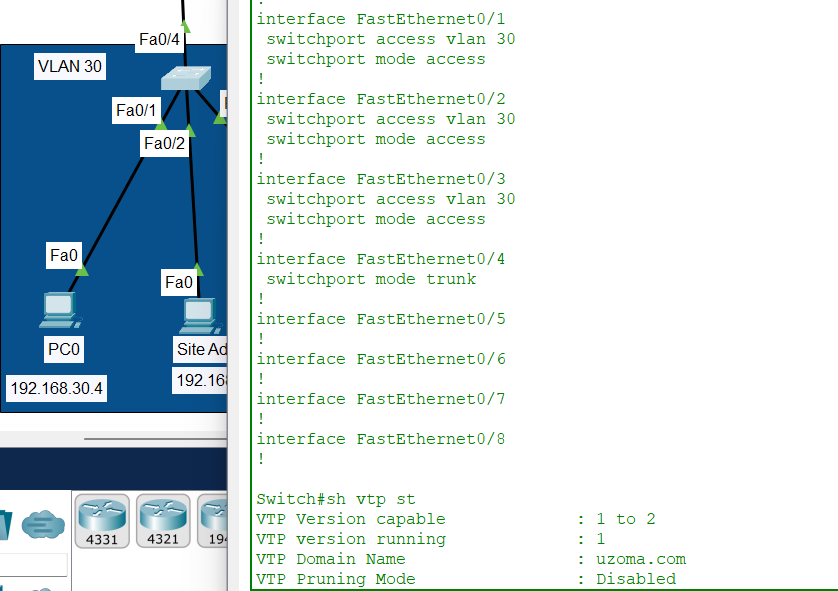
Regarding the router ports, a systematic approach has been taken. The serial ports serve the purpose of interconnecting the routers, while the primary ethernet port is utilized for linking with the switches. Notably, the interconnection between switches is facilitated by fast ethernet connections, and thanks to the serial connection, there is no requirement for separate configuration. This setup effectively replicates the configuration of preceding switches. To summarize, the configuration can be outlined as follows:

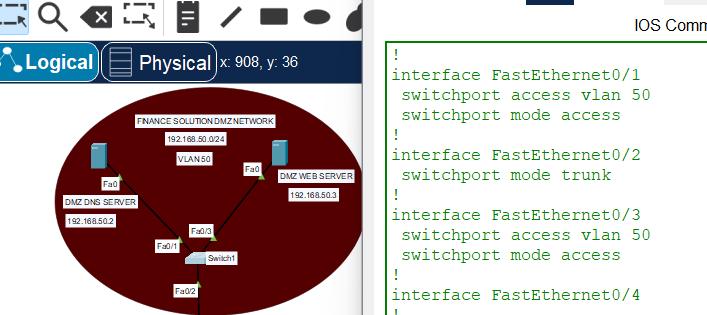


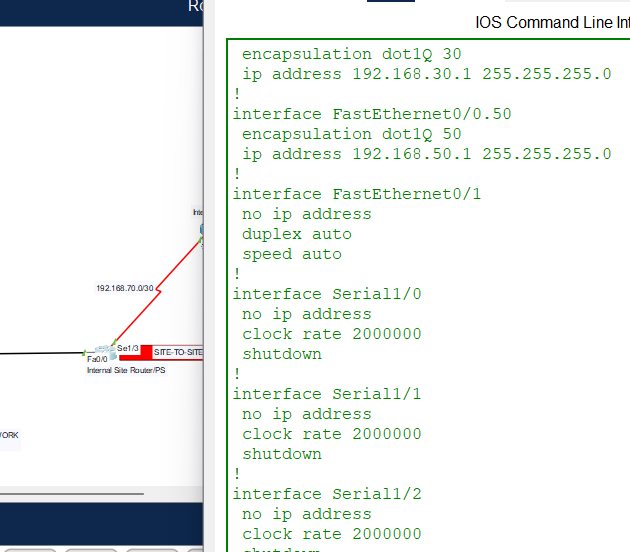


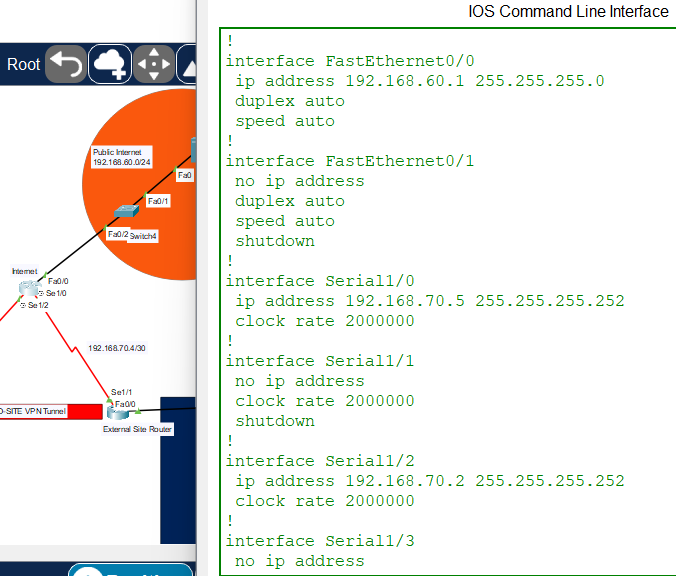




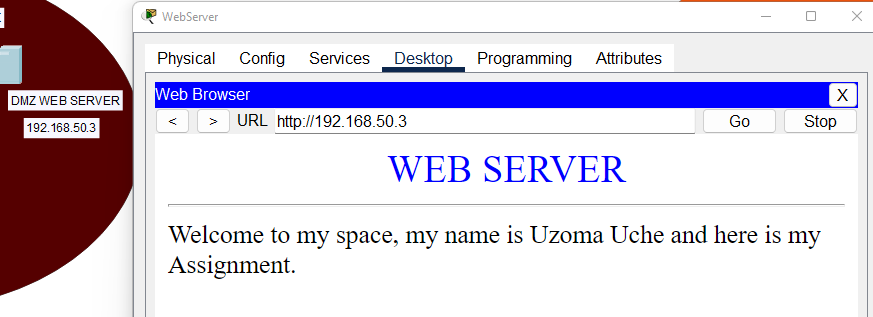


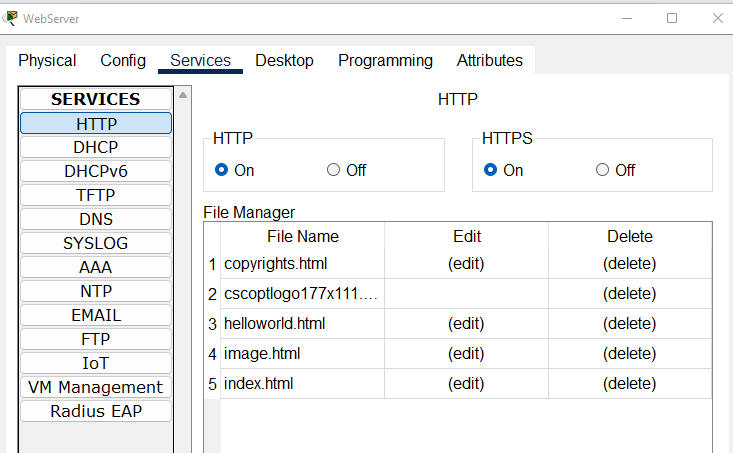




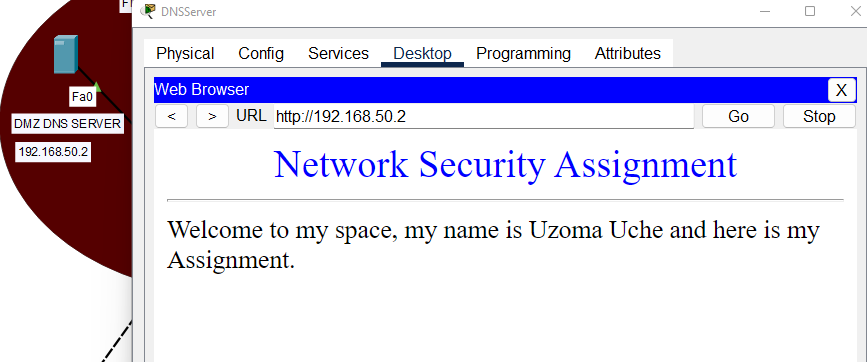


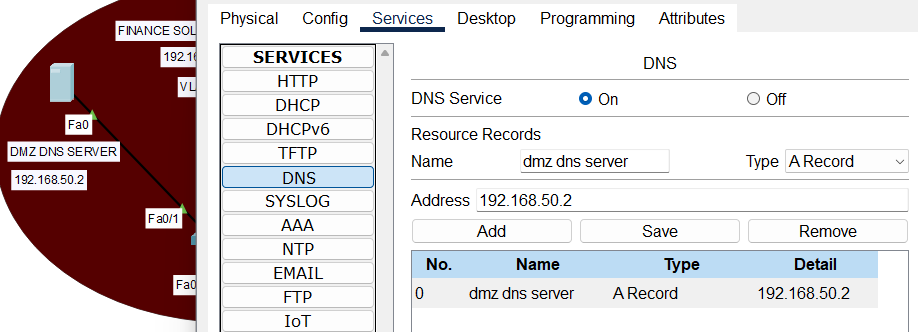
By taking care with HTTP, Web Server provides operators and programmes with a dependable interface. Software-based Cisco IOS devices. In addition to providing a thorough explanation for HTTP services to and from Cisco devices, the connected HTTP server application programme interface (API) wires server application interfaces.

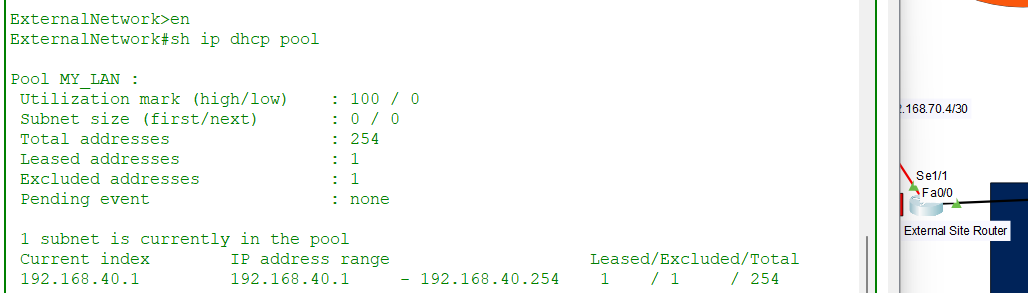




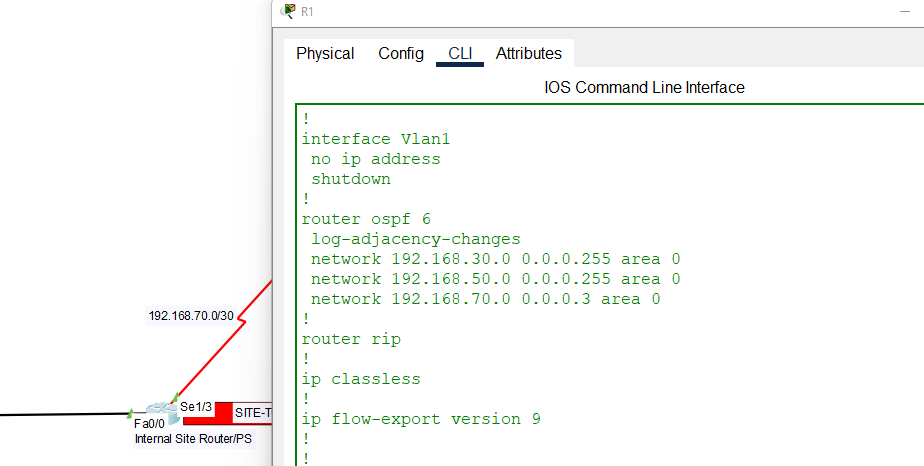
I've established a DHCP pool to facilitate automatic IP assignment for all hosts, with the exception of the DMZ servers which will be configured manually.



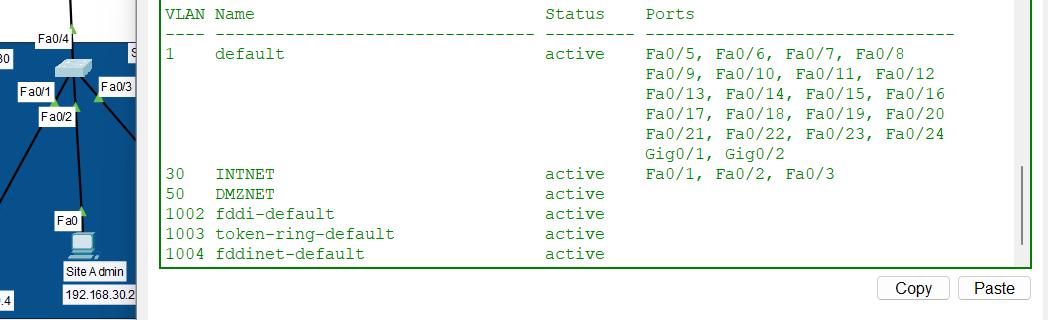




The upcoming setup involves the implementation of the OSPF protocol for Dynamic Routing. The overall network structure is built upon numerous subnets, all falling under a unified IP network labeled as 192.168.70.0. The OSPF protocol will be assigned the identifier 192.168.40.0 and will be extended across all routers within the network.



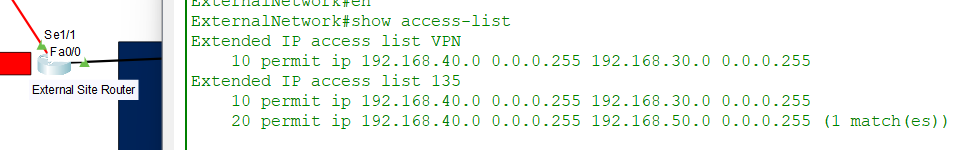
When pinging occurs between routers, acknowledgements are typically received in response. However, if pinging is initiated from a host, the expected responses might not be received. To enable successful communication in this scenario, it's necessary to establish trunk connections on switches. These trunk connections facilitate effective communication between the switches and the router, which are interconnected via fast ethernet ports. As a preliminary step, I will associate VLAN names with their respective VLAN numbers.



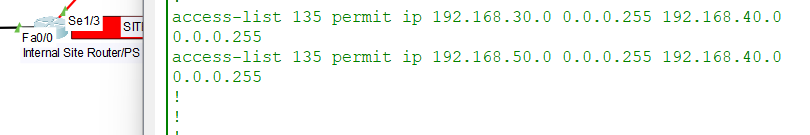
**Block B: Secure Operations and Service Delivery**

In this section, I've successfully established, activated, and set up a Standard Access Control List within the routers. The primary objective of implementing this ACL is to manage and regulate undesired network traffic that traverses through the router.

To illustrate, let's consider a scenario where a host within the External Site Network possesses the IP address 192.168.40.1. My intention is to exert control over this host's ability to connect with the internal site network. Hence, I will be implementing a command to achieve this restriction.

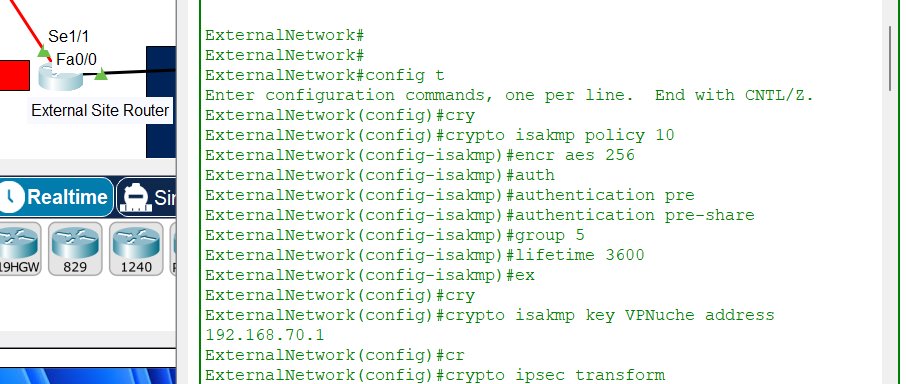


This configuration will effectively prevent any incoming data transmissions from the host situated within the External Site Network. Likewise, when considering the opposite scenario of permitting communication from hosts within the internal Site Network, let's assume that the site admin's IP address is 192.168.30.2, and the PC0's IP address is 192.168.30.3.

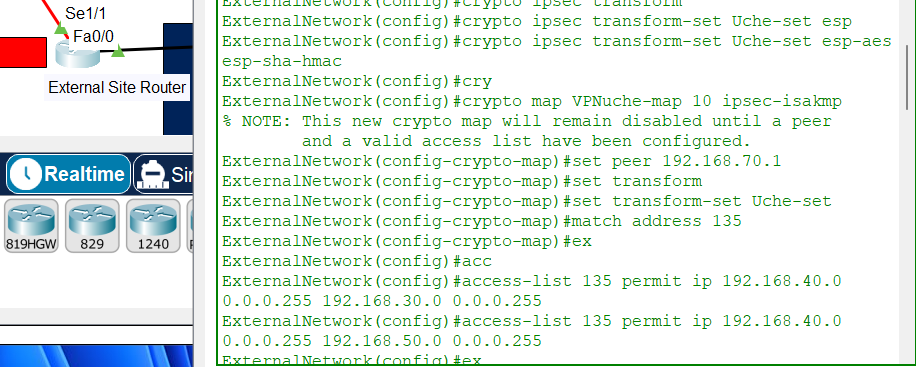


The next step involves the setup and configuration of a Site-to-Site IPsec VPN connecting RouterIPS and ExternalNetwork. This VPN will serve the purpose of thoroughly encrypting the network traffic that traverses the WAN network between these two routers.

For VPN configuration



Finally, applying crypto-map into the interface of WAN.



Through the implementation of Internet Protocol Security (IPSec) between the two routers, we've successfully activated several essential Cisco IOS VPN features. These encompass antireplay protection, assurance of data integrity, preservation of data confidentiality, and the verification of data origin authenticity.

To visually inspect the established VPN connections, the command "sh crypto ipsec sa" can be executed on both RouterIPS and ExternalNetwork.

Concluding the setup, the remaining task involves the application of an IOS-based Intrusion Prevention System (IPS) or Network Intrusion Prevention System (NIPS). Subsequently, I proceeded to assess the efficacy of the IPS. Worth noting is that I've exclusively implemented IOS IPS solely on InternalNetwork.

To initiate this process, I first enabled the IOS IPS functionality.

**Firewall on ASA device**

The internal network's security in this project is strengthened by an ASA device that includes a firewall. In order to operate as a security measure against unauthorized users, this firewall actively monitors all incoming and outgoing network traffic. To protect the network, it makes use of packet filtering methods. Only authorized users are allowed access, and these filters intercept and prevent messages that correspond to known dangers. For the purposes of this project, the firewall serves as a bridge connecting the DMZ network and the internal network of the company.

**4. BLOCK C: RESEARCH & DEVELOPMENT**

4.1 The Zero Trust cybersecurity model has gained significant popularity as a novel approach to preventing data breaches effectively. This tactical framework revolves around the central idea of eliminating the notion of trust from network architecture. The fundamental principle of Zero Trust is "never trust, always verify." This model is meticulously crafted to enhance the security of modern digital environments by thwarting lateral movement, employing network segmentation, implementing stringent user-access controls, and providing advanced threat prevention at Layer 7 (Palo Alto, 2020).

A Zero Trust Architecture employs a concept known as the "protected surface," which is customized for each organization. This surface serves as a safeguard for the organization's most valuable and crucial assets, including data, applications, services, and resources, collectively referred to as DAAS (Cser, 2018). The specific configuration of this protected surface is determined by the critical operations conducted by the organization, making it inherently unique. Unlike the expansive attack surface, the dimensions of the protected surface are significantly smaller, and it remains consistently discernible. This enables the organization to monitor the flow of network traffic within the organization, aligning it with the established protected surface.

Analyzing the users engaging with an organization's systems, along with the applications they employ and the manner in which they connect, constitutes a fundamental process in delineating the protected surface. This safeguarded zone is fortified through the implementation of an enforcement policy aimed at ensuring secure access to the entirety of the organizational data.

By deeply comprehending the intricate relationships between DAAS, services, users, and infrastructure, the organization aims to position controls as close as possible to this protected surface. This practice effectively establishes a sort of micro-perimeter around the data, which is flexible and adjusts its boundaries to match the movements of the safeguarded area.

To create this dynamic micro-perimeter, the organization can deploy a segmented gateway, often referred to as a next-generation firewall. This gateway functions to exclusively authorize identified and sanctioned network traffic, thereby permitting only legitimate applications with approved access to the protected surface.

In essence, this strategy constructs a robust security framework by taking a comprehensive view of the user-application-infrastructure landscape and strategically reinforcing it with precise controls situated in immediate proximity to the critical data.

In a recent instance, an extensive analysis was conducted on a prominent chemical industrial entity, revealing vulnerabilities within its Industrial Control Systems (ICS) across crucial facilities (Macias & Correia de Sousa, 2021). To address these concerns, a comprehensive security enhancement strategy was implemented, encompassing Zero Trust access management for both internal and remote interactions, fortified network security, and vigilant security monitoring. This proactive approach significantly elevated the organization's overall security maturity.

Notably, Deloitte devised a tailored Zero Trust reference architecture, meticulously tailored to the unique demands of their client's industry and critical facility requirements. This robust framework enveloped both Information Technology (IT) and Operational Technology (OT) systems, incorporating cloud services across multiple sites and industrial installations. This initiative prompted a transformative shift within the organization, effectively utilizing the novel security architecture to modernize the existing infrastructure while simultaneously establishing a blueprint for forthcoming deployments in other industrial settings.

The implementation of the Zero Trust reference architecture has become imperative due to the escalating threats and attacks on Industrial Control Systems (ICS). As organizations increasingly integrate various components of their Operational Technology (OT) infrastructure with IT networks and the Internet of Things (IoT), the security of their data becomes increasingly vulnerable. This convergence of OT and IT environments expands the attack surface of organizations, rendering them more susceptible to compromises.

Furthermore, considering that certain organizational facilities deal with hazardous chemicals, stringent control and surveillance measures are essential. Any cyber threats targeting the critical control systems could lead to catastrophic consequences, endangering human lives. The ramifications of a major incident in a critical industrial establishment extend beyond immediate safety concerns. Such incidents could jeopardize the organization's competitive edge, harm the environment, and even threaten its survival.

**4.2 Overview of VPN Reliability**

In the realm of security solutions, Virtual Private Networks (VPNs) have been relied upon for ensuring connectivity and safeguarding data. However, there are several factors that contribute to concerns about the reliability of VPNs, as outlined by Salamone in 2002. Questions arise about their effectiveness and the provision of redundancy measures.

The setup of a VPN is relatively straightforward. It begins with a server or VPN gateway strategically located within the organization's premises. Remote users establish connections either through their Internet Service Provider or by utilizing cable/DSL modem services. Remote sites connect via their respective servers or gateways, which are privately owned by those users.

In the face of mounting threats and the intricate integration of OT and IT networks, the Zero Trust architecture emerges as a crucial framework to mitigate risks and fortify overall security posture. This approach advocates for a comprehensive reassessment of traditional security practices and calls for continuous verification and strict access controls, regardless of the user's location or network source. By adopting a Zero Trust model, organizations can proactively address the challenges posed by ICS threats, better protect their data, and safeguard critical industrial operations.

The current issue revolves around the performance of a VPN under specific circumstances. The VPN is situated in a particular location as per the organization's choice. To enhance its reliability, the organization intends to set up a more robust VPN gateway at the same location. This process involves acquiring extra powerful fans and power supplies, advanced tools for remote network management, easily replaceable hot plug modules, and the ability to monitor various parameters such as cabinet temperature and fan speed.

A notable concern is maintaining consistent VPN services across the organization's devices. The challenge is to ensure uninterrupted VPN operation even if a device at a specific location within the organization fails. To address this, multiple vendors offer solutions such as load-balancing and clustering technologies. These approaches allow VPN users to seamlessly switch to an alternative device if the primary one encounters a failure. However, the level of understanding of these failover features varies significantly among organizations.

Certain vendors provide a continuous cutover mechanism that automatically shifts active VPN sessions to a backup server if the primary VPN server fails. It's important to emphasize that this process is mainly manual rather than automated. Consequently, when a VPN server failure is detected, ongoing sessions are terminated, requiring users to restart their VPN client software. This leads to the initiation of a new session on a secondary VPN server.

**4.3 Cryptographic Mechanism of IPsec**

IPSec operates within the network layer of the TCP/IP protocol stack, furnishing a robust cryptographic mechanism for security purposes. This protocol employs two distinct categories of algorithms: authentication and encryption. By safeguarding complete IP packets, it ensures a comprehensive level of security, irrespective of the upper-layer protocol encapsulated within the packet's payload.

One of the noteworthy features of IPSec is its ability to provide security without necessitating alterations to existing applications. This means that the protective benefits of IPSec can be harnessed without requiring a complete overhaul of applications. Consequently, IPSec plays a pivotal role in various Virtual Private Networking (VPN) solutions, where its transparent security mechanisms cater to the end-user experience.

In the realm of networking, IPSec emerges as a key enabler of security over untrusted communication channels, notably the Internet. It operates as a shield that fortifies communication across such vulnerable networks. It's important to recognize that the progression of IPSec represents an evolutionary step in cryptography rather than a revolutionary upheaval.

The Zero Trust framework has gained widespread acceptance across industries, with notable endorsements from Gartner's CARTA, Forrester eXtended, NIST 800-207, and others. This approach is hailed as the most effective means of tackling modern security challenges, particularly in cloud environments. Zero Trust is of paramount importance due to its multifaceted benefits, including behavioral analysis, least privilege controls, robust identity verification, endpoint security, micro-segmentation, and more. Unlike relying solely on packet analysis or firewall rules, Zero Trust recognizes that threats cannot be thwarted through traditional means.

The conventional authentication model, which relies on session-based protocols, exposes vulnerabilities to potential intrusions between sessions. Zero Trust technology, however, excels at distinguishing normal from anomalous behavior within an organization. While VPNs offer a degree of protection, they are surpassed by the comprehensive approach of Zero Trust. As organizations continually expand their endpoint infrastructure, the task of consistently adding security layers becomes increasingly daunting. This challenge is exacerbated by the presence of servers and clouds, elevating the urgency of secure perimeter maintenance.

Local, virtual machine, and SaaS-hosted microsites further complicate the endeavor of monitoring and safeguarding perimeters. For organizations with geographically dispersed workforces, a borderless security strategy is imperative. Zero Trust security emerges as a stalwart defense against breaches, minimizing potential damages by segmenting networks based on functions, user groups, identities, and access controls.

**5. CONCLUSION AND FUTURE WORK**

This assignment focuses on enhancing network security within a given topology. A robust network security system is essential for organizations to mitigate the risks of data breaches and cyber-attacks. It safeguards against malicious spyware and ensures the confidentiality of shared information. As our reliance on technology grows, securing online data has become paramount. With the expansion of the internet and computer networks, maintaining data integrity is a critical consideration for any organization. This escalating need has led to a high demand for information security analysts.

Among the stringent security models we've explored, the Zero Trust network security model stands out. Its principle of continuous verification and distrust of assumed trustworthiness has proven highly effective in countering cyber threats. This approach has gained widespread popularity across organizations as a reliable defense strategy. Looking ahead, we anticipate the emergence of more security models that can provide similar safeguards for our data and information. IPsec, a key player in network layer security, has found extensive utility in the realm of cryptography. The inherent nature of IPsec paves the way for the evolution of cybersecurity. As the landscape evolves, the demand for additional security features becomes evident. Our responsibility involves vigilant threat monitoring, continuous learning, and adapting existing security measures to fortify data and information against theft and malicious cyber activities.

**REFERENCES**

1. Hauser, F., Haberle, M., Schmidt, M. & Menth, M., 2020. P4-ipsec: Site-to-site and host-to-host VPN with IPSec in P4-based SDN. IEEE Access, 8, pp. 139567-139586.

2. Rajput, A., Tewani, R. & Dubey, A., 2016. The helping protocol "DHCP". In: Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIAcom), pp. 634-637.

3. Khormali, A. et al., 2021. Domain name system security and privacy: A contemporary survey. Computer Networks, 185, p. 107699.

4. Lopez-Millan, G., Marin-Lopez, R. & Pereniguez-Garcia, F., 2019. Towards a standard SDN-based IPSec management framework. Computer Standards & Interfaces, 66, p. 103357.

5. Odi, A., Nwogbaga, N. & Chukwuka, N., 2015. The Proposed roles of VLAN and inter-VLAN routing in effective distribution of network services in Ebonyi State University. International Journal of Sciences and Research, 7, pp. 2608-2615.

6. Sarkar, P., 2010. A simple and generic construction of authenticated encryption with associated data. ACM Transactions on Information and System Security (TISSEC), 13(4), pp. 1-16.

7. Buck, C. et al., 2021. Never trust, always verify: A motivational literature review on current knowledge and research gaps of zero-trust. Computers & Security, 110, p. 102436.

8. Kent, S., 2005. IP authentication header (No. rfc 4302).

9. Khormali, A. et al., 2021. Domain name system security and privacy: A contemporary survey. Computer Networks, 185, p. 107699.

10. Srisuresh, P., 1999. Security model with tunnel-mode IPSec for NAT domains (No. rfc2709).