رواد مصر الرقمية

Implementing network security with ACLs and NAT

Team Members:

1- Ezz Eldin Ayman
2- Kareem Hamdy
3- Poula Amged
4- Reham Adel
5- Youssef Khalil
6- Mohamed Badawy

2024

Table of Contents

Introduction:-

In today's digital age, securing network infrastructure is paramount to protect sensitive data and ensure the integrity and availability of network resources. Two critical components in achieving robust network security are Access Control Lists (ACLs) and Network Address Translation (NAT).

Access Control Lists (ACLs) are essential tools for network administrators, allowing them to define and enforce security policies by controlling the flow of traffic based on predefined rules. These rules can filter traffic based on various criteria such as IP addresses, protocol types, and ports, thereby preventing unauthorized access and mitigating potential threats.

Network Address Translation (NAT), on the other hand, plays a crucial role in conserving public IP addresses and enhancing security by masking internal IP addresses from external networks. NAT can be implemented in different forms, including Static NAT, which maps a private IP address to a fixed public IP address, and Port Address Translation (PAT), which allows multiple devices on a local network to be mapped to a single public IP address using different ports.

This project for ***Hospital consists of four floors*** delves into the implementation of network security using ACLs and NAT, exploring their configurations, benefits, and best practices. By understanding and applying these technologies, organizations can significantly enhance their network security posture, ensuring a safer and more reliable network environment.

Project's components:-

	Name	Model	QTY.
1	Cloud1	Cloud-PT	1
2	Router	ISR4331	1
3	Multi Switch	3650-24PS	3
4	Switch	2960-24TT	4
5	PC	PC-PT	8
6	Printer	Printer-PT	1
7	Server	Server-PT	1
8	IP Phone	7960	4

Configuration commands:-

The most important configuration commands we used:-

1. **Access:** Access is the process of enabling devices to connect to the network. Access ports are configured to allow end devices to connect to the network.
2. **Trunk:** A trunk is a link between network switches that carries traffic from multiple VLANs. Trunk ports are configured to allow traffic from all VLANs to pass through.
3. **Port Security (MAC-Sticky / Protected):** Port security is a feature that prevents unauthorized access to the network. Ports can be configured as MAC-Sticky, where the MAC addresses connected to the ports are saved, or Protected, where the ports are protected from threats.
4. **STP Port Fast (End Devices):** The STP PortFast feature is used to speed up the connection process to end devices by bypassing some steps of the Spanning Tree Protocol (STP).
5. **STP Port Fast BPDU Guard (Default):** The BPDU Guard feature is used to protect the network from incorrect configurations by disabling ports that receive unexpected BPDU messages.
6. **STP Rapid-PVST (All):** Rapid-PVST is a fast spanning tree protocol that provides faster network convergence and is used on all ports.
7. **VLANs:** Virtual Local Area Networks (VLANs) are used to segment the network into logical parts, improving performance and security.
8. **VLANs Root:** The VLAN root is the switch selected to be the root in the Spanning Tree Protocol (STP) for each VLAN.
9. **VTP Transparent:** The VTP Transparent mode is used to allow the switch to pass VTP information without participating in VLAN management.
10. **VLANs Routing:** VLAN routing is used to allow communication between different VLANs through a router or a multilayer switch.

11. **Network Routing:** Network routing is the process of selecting the best paths to transfer data across the network.
12. **ACL Standard:** Standard Access Control Lists (ACLs) are used to filter traffic based on source IP addresses.
13. **NAT Static:** Static Network Address Translation (NAT) is used to map a private IP address to a fixed public IP address.
14. **NAT PAT:** Port Address Translation (PAT) is used to map multiple private IP addresses to a single public IP address using port numbers.

Departments:-

- IT
- Reception
- Radiology
- Laboratory
- Doctors
- Clinics
- Pharmacy

VLANs:-

- v10 - 10.0.0.0
- v20 - 20.0.0.0
- v30 - 30.0.0.0
- v40 - 40.0.0.0
- v50 - 50.0.0.0
- v60 - 60.0.0.0
- v70 - 70.0.0.0
- v75 - 75.0.0.0
- v90 - 90.0.0.0

The project on Cisco Packet tracer software:-