

Network Security

Ensuring robust network security is essential for protecting an organization's data, infrastructure, and operations. One of the most effective ways to achieve this is by using hybrid-based Next Generation Firewalls (NGFWs). These firewalls are highly efficient, versatile, and can easily integrate with cloud environments. Unlike traditional firewalls, NGFWs can detect applications and perform deep packet inspection, which means they can analyse the contents of network traffic in detail. This ability allows them to identify and block advanced malware and other sophisticated threats. Additionally, NGFWs often come with built-in tools like Virtual Private Networks (VPNs), Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS), making them a comprehensive security solution (Patel, 2024).

Virtual Private Networks (VPNs) are crucial for securing data transmitted over public networks. VPNs create a secure, encrypted tunnel between the user's device and the network, ensuring that sensitive data remains confidential. Two types of VPNs are recommended: site-to-site VPNs and remote access VPNs. Site-to-site VPNs connect entire networks, such as linking a head office with branch offices, while remote access VPNs are used for individual remote workers connecting through devices like laptops. Full tunnelling is advised for remote access VPNs to ensure that all internet traffic passes through the encrypted connection, offering complete protection when accessing public networks (Akinsanya et al., 2024).

Another critical element of network security is the use of Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS). An IPS continuously monitors network traffic for potential threats and blocks them in real-time, actively preventing sophisticated cyberattacks. In contrast, an IDS passively detects and alerts administrators of any unusual activities or anomalies in the network. While an IPS focuses on immediate threat prevention, an IDS provides ongoing monitoring without interfering with network performance. For a robust security posture, both IPS and IDS should be implemented together (Alhasan & Surantha, 2021).

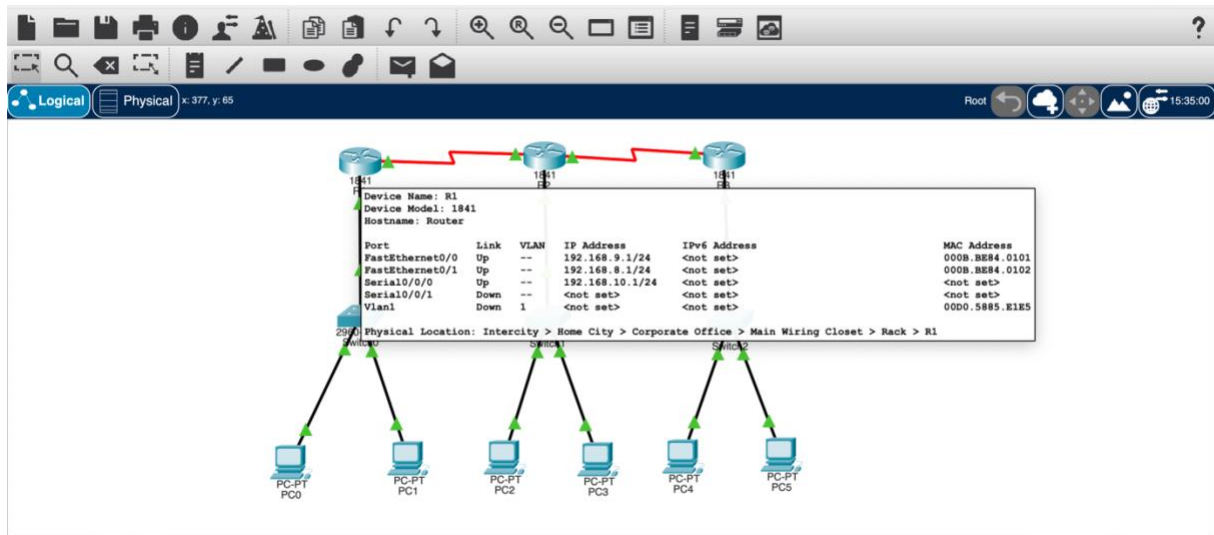
To further enhance security, network segmentation is recommended. Network segmentation divides the network into smaller subnetworks, each with its own access rules and policies. This approach limits the exposure of sensitive data, ensuring that users only have access to the information they need for their tasks. If a breach occurs, segmentation can help contain the threat, preventing it from spreading across the entire network (Islam et al., 2023).

Additionally, implementing Network Access Control (NAC) and Multifactor Authentication (MFA) helps ensure that only authorized users can access the network. NAC verifies devices before granting network access, while MFA requires users to provide two or more forms of verification (such as a password and a code sent to their

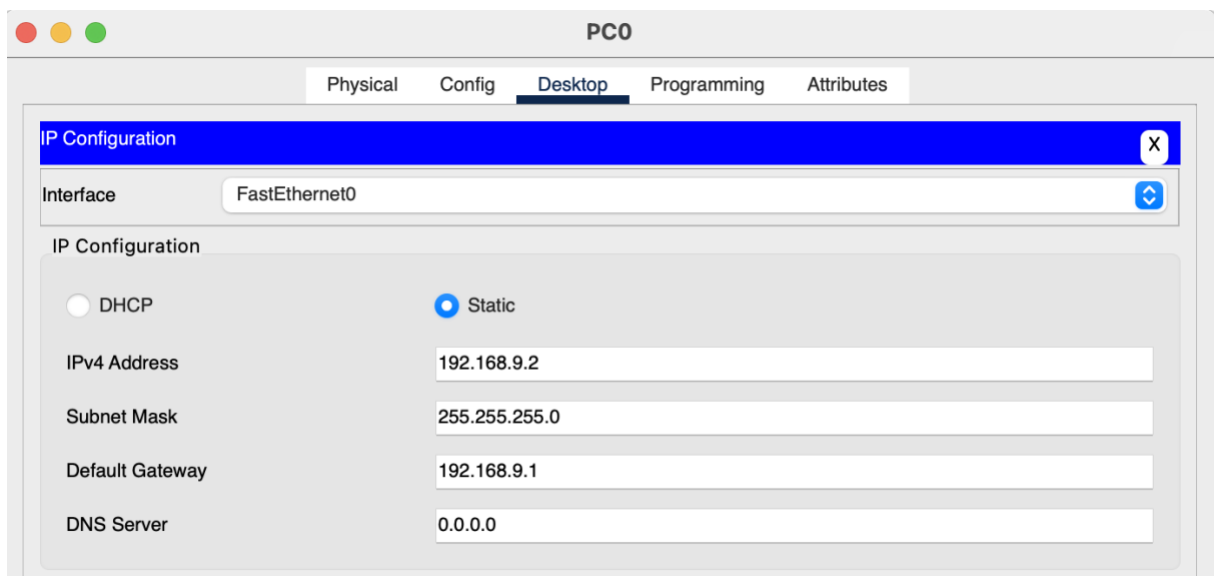
phone) to log in. These measures significantly reduce the risk of unauthorized access. Keeping network devices up to date with regular security patches is also crucial. Outdated software can be vulnerable to attacks, so maintaining the latest updates ensures that security tools remain effective (Ranaweera et al., 2021).

Cisco Packet Tracer Simulation

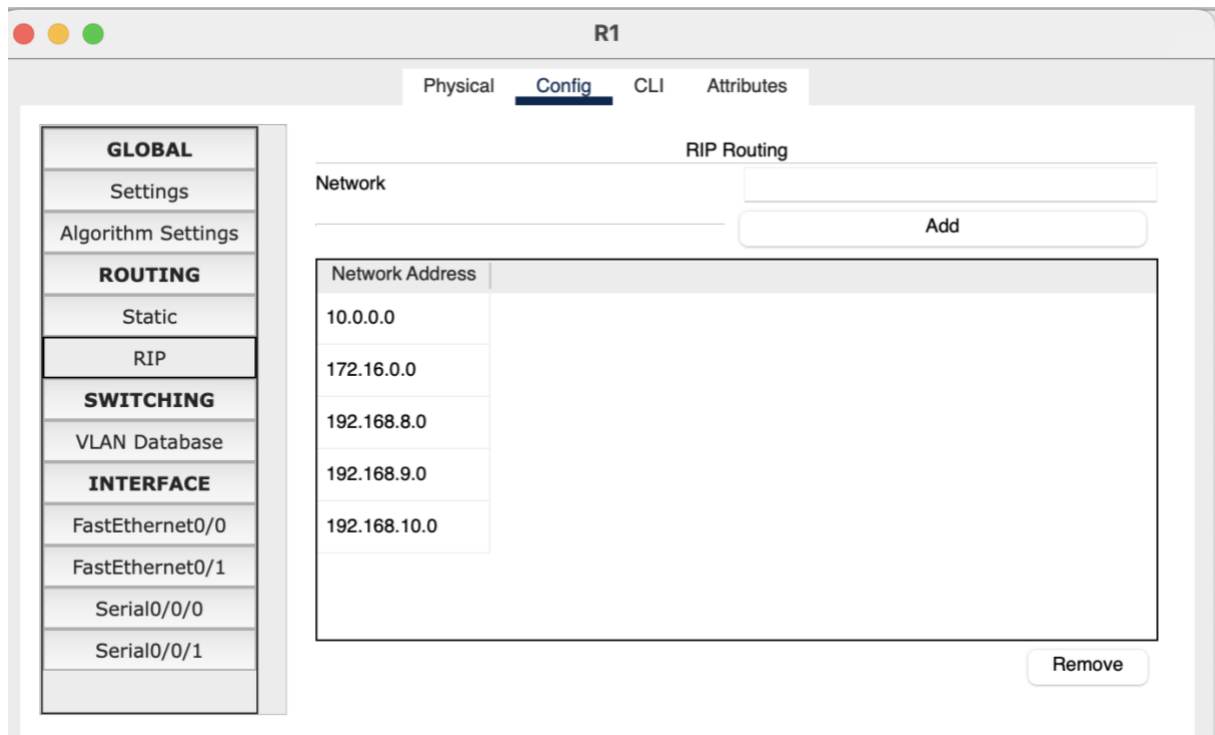
I began by adding three 1841 routers (R1, R2, and R3) and connected them using serial interfaces to ensure communication between different network segments. Each router was assigned specific IP addresses to establish clear pathways for data transmission. For example, Router R1's serial interface was given the IP address **192.168.10.1**, while R2's corresponding interface received **192.168.10.2**. This setup allowed the routers to communicate seamlessly and ensured proper routing of information.



Next, I connected multiple end devices (PCs) to the routers through three 2960-24TT switches. Each router had a Fast Ethernet interface for connecting these devices through the switches. I assigned IP addresses to the PCs based on the subnets configured on the routers. For instance, PC0 connected to Router R1 had the IP address **192.168.9.2**, while PC1 connected to R2 used **172.16.10.2**. These IP assignments ensured that each device could communicate within its network segment.



To ensure that data could travel between different parts of the network, I configured the Routing Information Protocol (RIP) on all three routers. RIP is a simple routing protocol that helps routers exchange information about the networks they can reach. This configuration allowed data to move smoothly between devices connected to different routers.



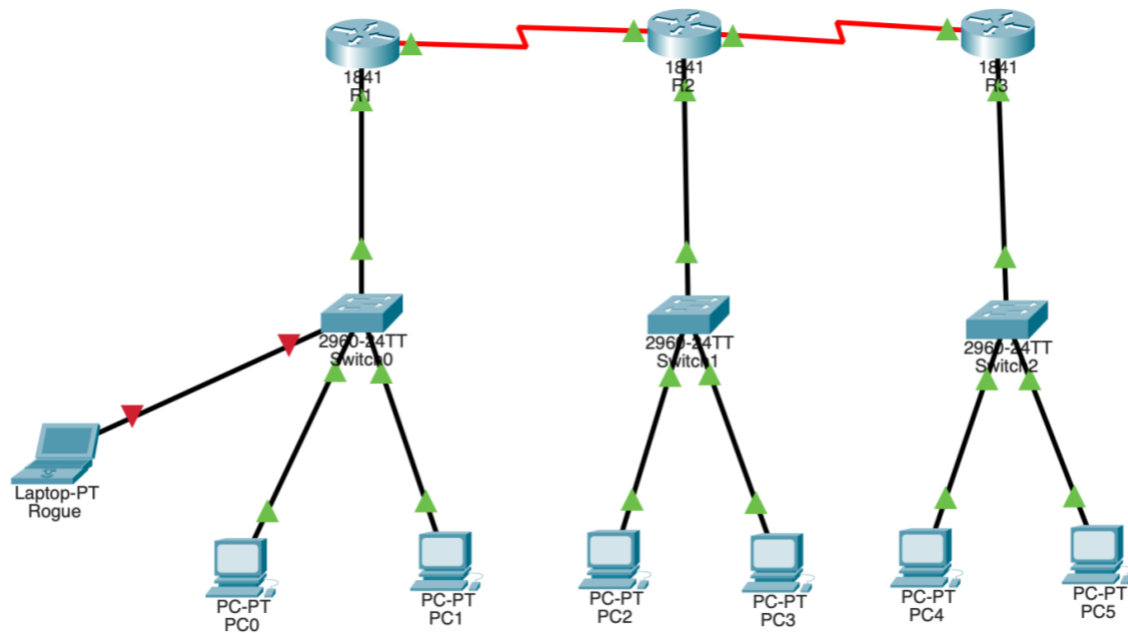
I then added password protection to each router to prevent unauthorized access. For example, I set passwords for the console and privileged access modes, ensuring that only authorized users could configure the routers. This step is crucial to protect the network's core infrastructure from potential attackers.

```
Router#enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret nds44l
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show running-config
Building configuration...

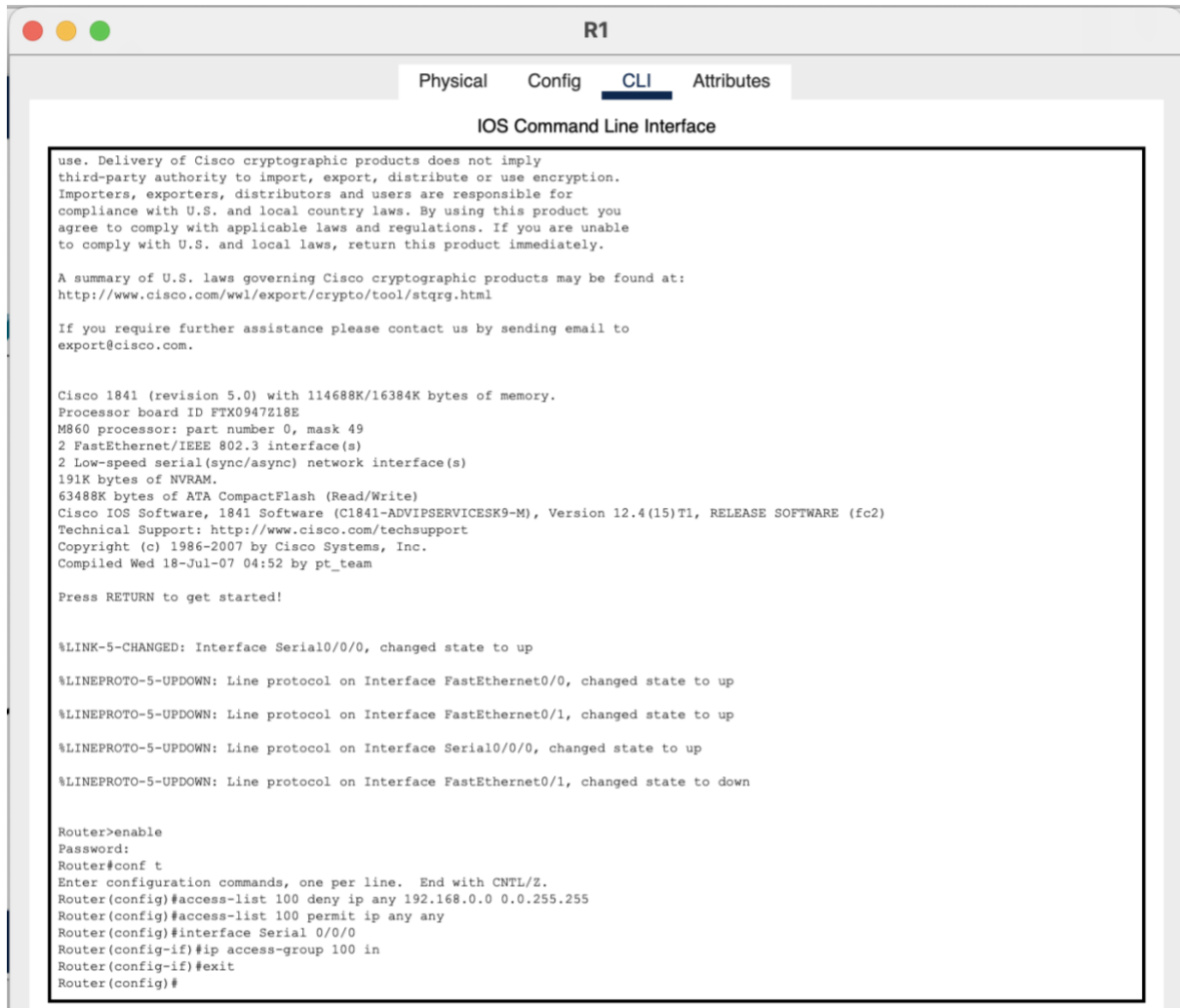
Current configuration : 878 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
enable secret 5 $1$mERr$3sWgkiNoj9Ma8P9QsIeMo.
!
!
!
!
!
no ip cef
no ipv6 cef
Router#
```

I also implemented switch port security on the 2960 switch to prevent unauthorized devices from connecting to the network. By configuring port security, I ensured that each switch port only allowed one specific device to connect. If a rogue device attempted to connect, the port would automatically block the connection. This security measure helps protect the network from internal threats and unauthorized access.



I then added an ASA 5505 firewall for further network security. The firewall acts as a barrier between the internal network and external threats, filtering traffic to ensure that only authorized data can pass through. I configured the firewall with basic rules to allow internal traffic while blocking any suspicious activity from the outside. This step helps protect the network from malware, hackers, and other external threats.

I also configured an Access Control List (ACL) on Router R1 to block unauthorized traffic. The ACL denied any data packets from networks that were not connected to R2 and R3. By applying this filter, I ensured that only trusted devices could communicate with the network, providing an additional layer of security against external attacks.



```
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

Router>enable
Password:
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 100 deny ip any 192.168.0.0 0.0.255.255
Router(config)#access-list 100 permit ip any any
Router(config)#interface Serial 0/0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#
```

Finally, I tested the network to ensure everything was working as expected. I used the ping command to verify connectivity between the routers and PCs. I also tested the firewall and port security configurations by attempting to connect unauthorized devices and ensuring they were blocked.

In summary, this project demonstrated how to design and secure a network using Cisco Packet Tracer. I established proper connections between routers, switches, and end devices, ensuring efficient communication. By implementing security measures like passwords, port security, firewalls, and ACLs, I protected the network from potential cyber threats. This setup helps prevent unauthorized access, malware infections, and data breaches, creating a more secure and reliable network for users.

References

- Alhasan, A. J., & Surantha, N. (2021). Evaluation of Data Center Network Security based on Next-Generation Firewall. *International Journal of Advanced Computer Science and Applications*, 12(9).
- Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. (2024). Virtual private networks (vpn): a conceptual review of security protocols and their application in modern networks. *Engineering Science & Technology Journal*, 5(4), 1452–1472.
- Islam, M. S., Uddin, M. A., Hossain, D. M. D., Ahmed, D. M. S., & Moazzam, D. M. G. (2023). Analysis and evaluation of network and application security based on next generation firewall. *International Journal of Computing and Digital Systems*, 13(1), 193–202.
- Patel, U. (2024). THE ROLE OF NEXT-GENERATION FIREWALLS IN MODERN NETWORK SECURITY: A COMPREHENSIVE ANALYSIS. *INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND TECHNOLOGY (IJARET)*, 15(4), 135–154.
- Ranaweera, P., Jurcut, A. D., & Liyanage, M. (2021). Survey on multi-access edge computing security and privacy. *IEEE Communications Surveys & Tutorials*, 23(2), 1078–1124.