NETWORK SECURITY PORTFOLIO

BS2940

Table of Contents

Introduction

Throughout this article we will explore the intricate world of Local Area Networks (LAN) and Wide Area Network (WAN). We will focus on analyzing the potential security threats that apply to either or both the network types. Subsequentially we will study the most practical and most used security frameworks and countermeasures.

Notoriously, WANs are attractive targets for attackers due to their centralized role in organizational operations. A single breach can disrupt multiple sites and services, significantly amplifying the impact of an attack. Furthermore, as businesses increasingly rely on virtual WANs for critical functions—such as hosting services on cloud servers—the consequences of a successful attack can be devastating, leading to operational downtime and financial losses.

A LAN connects devices within a limited area, like a home or office, enabling efficient communication and resource sharing. While typically private and secure, LANs are attractive targets for attackers due to their valuable data, ease of exploitation, and opportunities for lateral movement. The perception of LANs as "trusted" often leads to weaker security, making them vulnerable to external and insider threats. Securing LANs requires technical measures (e.g., encryption, segmentation) and user awareness to mitigate risks.

Security threats

Perhaps one of the most dangerous attacks in the contest of LANs is ARP spoofing, this along with DNS Chace poisoning, are not attacks in themselves, but they serve more as the foundation for other more destructive practices, compromising confidentiality, integrity and availability of network resources and data

Arp spoofing, as explained by Sithirasenan E. et al (2007), it the practice of exploiting how the Address resolution protocol (ARP) works, due to how computer devices map IP and MAC addresses within their ARP cache, and especially because ARP is stateless, meaning it will accept replies even if a request wasn't sent, an attacker is free to send fake ARP replies with a modified MAC address, in order to associate its MAC address with the victim's IP address inside the ARP cache.

Dynamic Host configuration Protocol (DHCP) servers have become more effective at detecting IP addresses making DNS spoofing harder to execute. Asaduzzaman J. et al (2023) have proposed a new strategy, which entails introducing a Rogue DHCP server into the network, with the intent of assigning malicious IP addresses and default gateway to the servers within the LAN, this is achieved because the rogue server typically responds faster than the default DHCP server. At this point any request made by the user is redirected to the attacker who is free to alter integrity or availability of data.

Man-in-the-Middle Attack (MitM)

A Man-in-the-Middle Attack (MitM) is one of the most dangerous cyber threats, often enabled by techniques like ARP spoofing and DNS spoofing. The attacker's goal, as explained by Mallik A. (2018), is to position themselves within the communication channel between two devices or networks, allowing them to intercept, decrypt, and potentially manipulate the data being exchanged.

The attack begins with the interception phase, where the attacker inserts themselves into the communication path using the techniques explained above.

Once the attacker has successfully intercepted the communication, they move to the decryption phase. Here, they use techniques like SSL hijacking (Sagar J., 2023) to bypass encryption. SSL hijacking involves forging authentication keys during the TCP handshake process, allowing the attacker to establish a seemingly secure connection with both the server and the client. This enables them to decrypt the data being transmitted without raising suspicion.

With access to decrypted communication, the attacker can monitor sensitive information, such as login credentials or financial data, or even alter the data being exchanged. This makes MitM attacks particularly devastating, as they undermine both the confidentiality and integrity of the communication.

DDoS attack

Denial of Service (DoS) attacks, another significant threat enabled by techniques like ARP and DNS spoofing, aim to overwhelm a victim's resources, rendering them unavailable by consuming the target's machine or network capacity. Through extensive research, Aws Naser J. (2015) provides a detailed analysis of Distributed Denial of Service (DDoS) attacks, shedding light on their mechanisms, impacts, and mitigation strategies.

A DDoS attack is essentially a more advanced form of a DoS attack. It is designed to disrupt entire systems or networks by leveraging multiple compromised devices to flood the target with traffic. This makes DDoS attacks particularly dangerous for WANs, where the interconnected nature of networks can amplify the scale and impact of the attack.

To execute this attack, the attacker must trick the user into running malware containing the payload, thereby turning their machine into part of a botnet—a network of hijacked devices. When the attacker decides to launch a DDoS attack, they send a command to the botnet through Command-and-Control servers (C&C), instructing the infected machines to launch the attack.

Security requirements

To build secure LANs and WANs, several security aspects must be addressed. Adefemi A. (2020) provides extensive research based on the CIA Triad (confidentiality, integrity, availability), offering a framework for robust network protection.

Confidentiality can be ensured through encryption, which renders data illegible to unauthorized parties. This is achieved using strong protocols like AES (Advanced Encryption Standard), paired with secure key generation, storage, and distribution mechanisms. Additionally, implementing role-based access control (RBAC) and adopting a zero-trust model ensures that only authenticated and authorized entities can access specific resources or network traffic.

To maintain integrity, practices like data validation and message authentication are essential. These methods verify that data has not been tampered with during transmission or storage. Abergos J. (2024) highlights the effectiveness of network segmentation in isolating critical components, safeguarding them in the event of a breach. Segmentation is a versatile technique, allowing administrators to control traffic flow based on type, source, destination, and other parameters, providing an additional layer of security.

Availability ensures that network resources remain accessible to authorized users when needed. As mentioned above A major threat to availability is Denial-of-Service (DoS) attacks, including jamming attacks, which aim to overwhelm network resources and disrupt access. To safeguard availability, several measures must be implemented.

Intrusion Detection Systems (IDS) play a critical role in monitoring and detecting malicious activities or unusual network traffic (Raza M. 2024), enabling timely responses to potential threats. Additionally, redundancy and failover mechanisms are essential for maintaining continuous operation, even in the event of component failures. Regular maintenance and updates, including the application of security patches, are necessary to protect systems against known vulnerabilities and ensure their resilience.

Having a well-defined incident response plan is crucial for effectively addressing and mitigating security incidents when they occur. For traffic management, SD-WANs can monitor and apply policing to inbound and outbound traffic, allowing organizations to enforce one-way traffic policies and reduce exposure to threats. Finally, implementing robust backup and recovery solutions ensures that data and system states can be restored quickly after an attack, minimizing downtime and maintaining operational continuity.

Countermeasures

There are several approaches to mitigating the risk of ARP spoofing. Booker D. (2023) emphasizes the importance of configuring strong encryption protocols while also monitoring the network using spoofing detection tools.

It is critically important to implement port security, which restricts the number of devices that can operate on any given port. This significantly limits the attacker's ability to exploit the network. Additionally, setting static ARP entries on critical devices ensures that their ARP tables remain fixed and immune to dynamic manipulation, further reducing the risk of spoofing attacks. These measures, when combined, create a robust defense against ARP spoofing threats.

Conti M et al. (2016) propose the use of ANAX, a system leveraging machine learning techniques, to detect DNS cache poisoning attacks in real time. The authors also highlight the effectiveness of "entropy-increasing mechanisms," which enhance the randomness of DNS packets. These mechanisms, such as Source Port Randomization, make it significantly more challenging for attackers to inject invalid DNS responses, thereby strengthening the security of DNS systems

As highlighted by Dr. A. Shaji G. (2023), one of the most important security measures against Man-in-the-middle attacks is the encryption of data. Encryption makes it significantly harder to compromise the integrity of the data. It is recommended to use standard cryptographic protocols, as they are well-vetted and thoroughly tested over time, unlike custom-made solutions. Additionally, establishing appropriate parameters—such as selecting the correct key length and cryptographic algorithm—is crucial. Strong access control mechanisms are also essential to monitor and restrict unauthorized access.

One of the most effective mitigation measures to use against DDoS attacks is the use of Bidirectional Stateful Firewalls. Any software installed on a virtual machine should incorporate such a firewall, as it can help mitigate accessibility risks, such as disabling sensitive services or reducing user permissions.

The key feature of bidirectional firewalls (also known as two-way firewalls) is their ability to monitor not only incoming traffic but also outgoing traffic. This dual monitoring can potentially detect DDoS attacks originating from within an infected machine.

Other techniques, as outlined by Richter B. (2015), include:

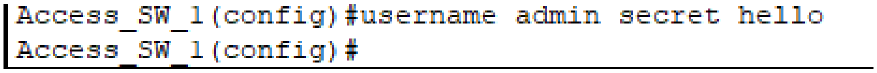
- Rate Limiting: This limits the amount of traffic that can be sent to the network, dropping or rerouting any excess traffic.
- Traffic Filtering: This involves filtering traffic based on source and destination IP addresses, as well as other characteristics that help identify malicious activity.
- Load Balancing: Some enterprises opt to run multiple servers to distribute the load, preventing any single server from being overwhelmed by an attack.

Packet Tracer Implementation: Security Configuration Overview

we will now dive into a practical implementation of a security configuration using the packet tracer platform. We will use this time to document and discuss the reasoning behind the chosen configuration as well as the practices and methods used to implement the various security measures.

Basic Security (Part one)

I began by implementing basic access controls on the switches and router to establish a foundational layer of security. A user account was created with the username **admin** and password **hello** for login access (figure 1)



```
Access_SW_1(config)#username admin secret hello
Access_SW_1(config)#
```

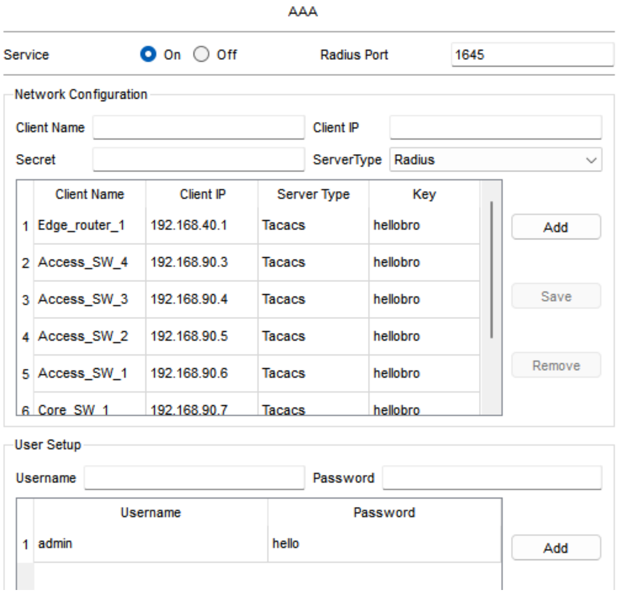
Figure 1: account set up

To further secure the devices, I added a password **bye** for privileged EXEC mode. This ensures that only authorized users can execute commands that modify the device's configuration, preventing unauthorized changes.

AAA (Authentication, Authorization, and Accounting)

For a more robust authentication mechanism, I implemented AAA using the TACACS+ protocol. TACACS+ is ideal because it provides strong encryption and granular control over user access. On the AAA server (figure 2), I configured the IP addresses of the switches, set the authentication key to **hellobro**, and created user accounts for authentication. On the switches, I specified the server's IP address and the same authentication key to ensure secure communication between the devices and the server.

To handle potential server downtime, I configured the devices to fall back to local authentication. This means the same user accounts and passwords are stored locally, allowing users to log in even if the server is unavailable. This ensures continuity and prevents lockouts during network issues or maintenance.



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

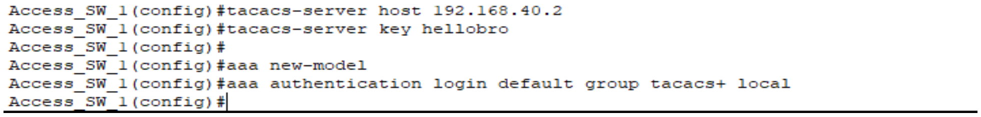
	Client Name	Client IP	Server Type	Key
1	Edge_router_1	192.168.40.1	Tacacs	hellobro
2	Access_SW_4	192.168.90.3	Tacacs	hellobro
3	Access_SW_3	192.168.90.4	Tacacs	hellobro
4	Access_SW_2	192.168.90.5	Tacacs	hellobro
5	Access_SW_1	192.168.90.6	Tacacs	hellobro
6	Core_SW_1	192.168.90.7	Tacacs	hellobro

User Setup

Username Password

	Username	Password
1	admin	hello

Figure 2: AAA server configuration

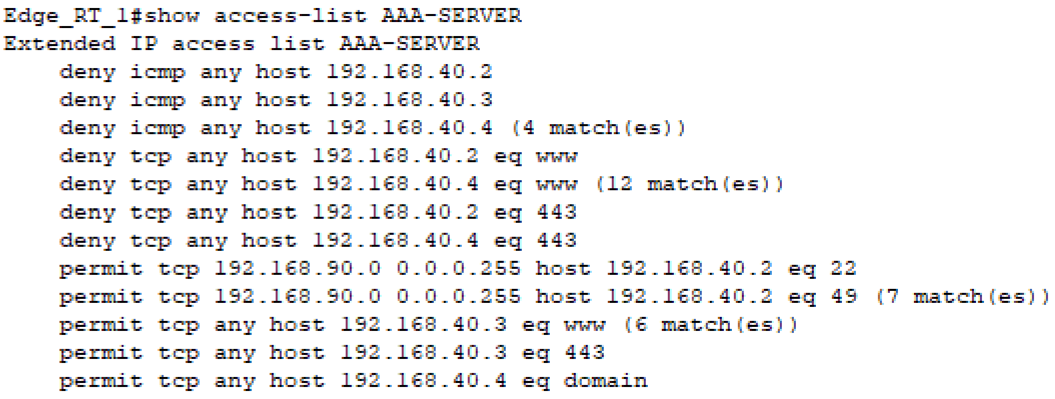


```
Access_SW_1(config)#tacacs-server host 192.168.40.2
Access_SW_1(config)#tacacs-server key hellobro
Access_SW_1(config)#
Access_SW_1(config)#aaa new-model
Access_SW_1(config)#aaa authentication login default group tacacs+ local
Access_SW_1(config)#
```

Figure 3: AAA switch configuration

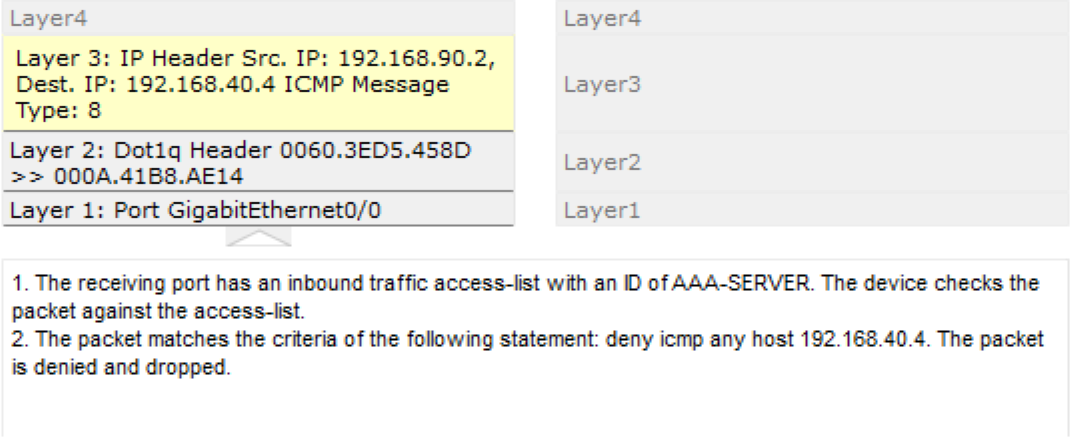
Servers access control

When securing the network's servers, to minimize the attack surface, I restricted unnecessary services. Leaving For the AAA_SERVER and DNS_SERVER, I denied protocols like ICMP (ping) and http/https resolved around specific tasks (AAA authentication and DNS). However, for the WEB_SERVER, I kept http and https on while still denying ICPM. Picture 4 shows the access control list implemented in EDGE_ROUTER, and for demonstrational purposes picture 5 shows a ICPM packet direct to one of the servers being dropped



```
Edge_RT_1#show access-list AAA-SERVER
Extended IP access list AAA-SERVER
    deny icmp any host 192.168.40.2
    deny icmp any host 192.168.40.3
    deny icmp any host 192.168.40.4 (4 match(es))
    deny tcp any host 192.168.40.2 eq www
    deny tcp any host 192.168.40.4 eq www (12 match(es))
    deny tcp any host 192.168.40.2 eq 443
    deny tcp any host 192.168.40.4 eq 443
    permit tcp 192.168.90.0 0.0.0.255 host 192.168.40.2 eq 22
    permit tcp 192.168.90.0 0.0.0.255 host 192.168.40.2 eq 49 (7 match(es))
    permit tcp any host 192.168.40.3 eq www (6 match(es))
    permit tcp any host 192.168.40.3 eq 443
    permit tcp any host 192.168.40.4 eq domain
```

Figure 4: server's access control list



Layer4

Layer 3: IP Header Src. IP: 192.168.90.2, Dest. IP: 192.168.40.4 ICMP Message Type: 8

Layer 2: Dot1q Header 0060.3ED5.458D >> 000A.41B8.AE14

Layer 1: Port GigabitEthernet0/0

Layer4

Layer3

Layer2

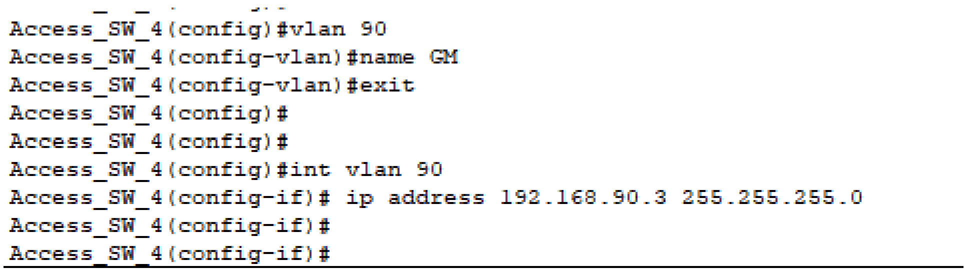
Layer1

1. The receiving port has an inbound traffic access-list with an ID of AAA-SERVER. The device checks the packet against the access-list.
2. The packet matches the criteria of the following statement: deny icmp any host 192.168.40.4. The packet is denied and dropped.

Figure 5: ICMP packet being dropped

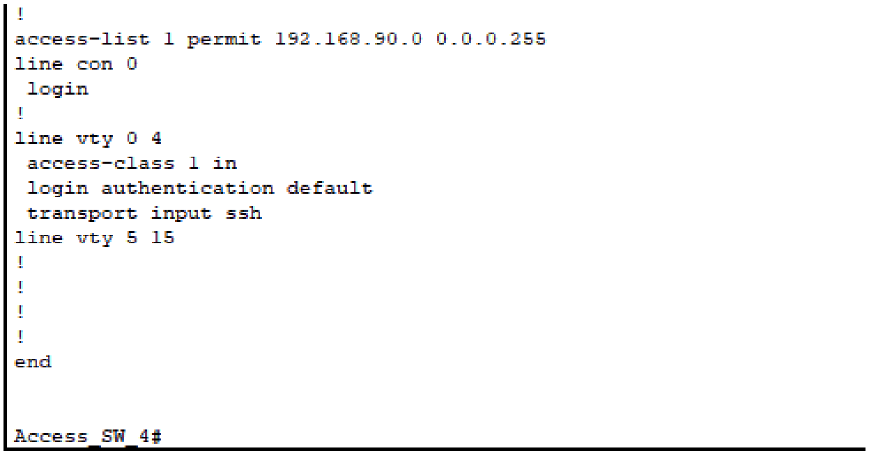
Basic security (part 2)

To streamline network management, I created VLAN 90 as the Management VLAN (figure 4). This allows me to remotely access and manage all switches from a centralized location, simplifying administration and enhancing security. I configured the Core switch and Edge router to allow communication with other VLANs while ensuring that only devices within VLAN 90 can access the switches remotely.
To enforce this, I set up an access list on the Edge router that permits traffic only from IP addresses belonging to VLAN 90. This ensures that unauthorized devices outside the management VLAN cannot remotely access the network devices (figure 5).



```
Access_SW_4(config)#vlan 90
Access_SW_4(config-vlan)#name GM
Access_SW_4(config-vlan)#exit
Access_SW_4(config)#
Access_SW_4(config)#
Access_SW_4(config)#int vlan 90
Access_SW_4(config-if)# ip address 192.168.90.3 255.255.255.0
Access_SW_4(config-if)#
Access_SW_4(config-if)#
```

Figure 6: Vlan 90 configuration

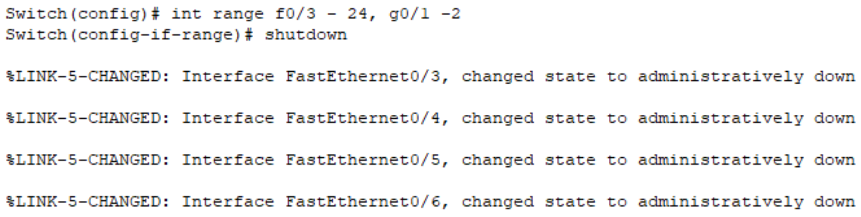


```
!
access-list 1 permit 192.168.90.0 0.0.0.255
line con 0
 login
!
line vty 0 4
 access-class 1 in
 login authentication default
 transport input ssh
line vty 5 15
!
!
!
!
end


Access_SW_4#
```

Figure 7 remote ssh configuration

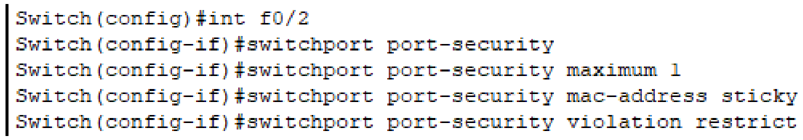
Port Security

Next, I focused on securing the physical ports on the switches. I disabled all unused ports to prevent attackers from exploiting them to gain access to the network (figure 6) . For active ports, I implemented port security with MAC address restrictions (figure 7). Using the sticky MAC feature, the switch dynamically learns and stores the MAC addresses of connected devices. After the first successful ping, the switch locks down the port to only allow traffic from that specific MAC address (figure 8). This prevents unauthorized devices from connecting to the network, even if they gain physical access to a port.



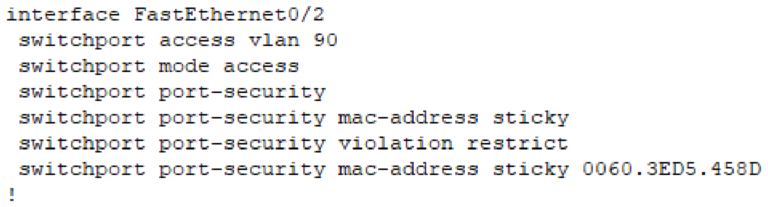
```
Switch(config)# int range f0/3 - 24, g0/1 -2
Switch(config-if-range)# shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
```

Figure 8: unused port shutdown



```
Switch(config)#int f0/2
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation restrict
```

Figure 9: MAC address restriction configuration commands



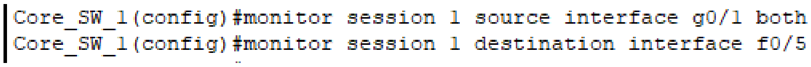
```
interface FastEthernet0/2
 switchport access vlan 90
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.3ED5.458D
!
```

Figure 10: interface f0/2 running configuration showing the stored MAC address

Local Span and Sniffer

To enhance network visibility and monitoring, I deployed a network sniffer. This tool captures and analyzes traffic, which is essential for troubleshooting and detecting potential security threats. On the Core switch, I configured a SPAN (Switched Port Analyzer) session to mirror traffic from the port connected to the Edge router (source port) to the port where the sniffer is connected (destination port) (figure 9). This setup allows the sniffer to monitor all internal traffic routed through the Core switch.

However, I realized that traffic from external networks to the server wasn't being captured by the sniffer on the Core switch. To address this, I added a second sniffer on the server switch. This ensures that all traffic, whether internal or external, is monitored, leaving no blind spots in the network.



```
Core_SW_1(config)#monitor session 1 source interface g0/1 both
Core_SW_1(config)#monitor session 1 destination interface f0/5
```

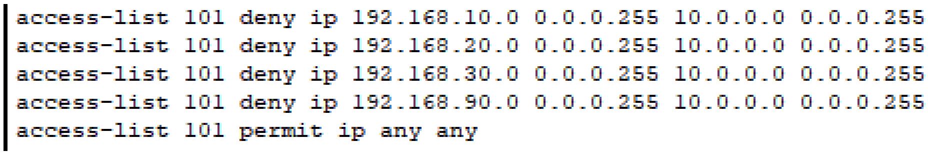
Figure 11: sniffer configuration

Site-to-Site VPN

To secure communication between the HQ and Remote Site, I configured a site-to-site VPN using IPsec and ISAKMP. IPsec provides strong encryption, ensuring that all data transmitted between the two locations is secure and unreadable to outsiders (figure 15). ISAKMP (Internet Security Association and Key Management Protocol) is used to establish the secure tunnel and manage encryption keys (figure14).

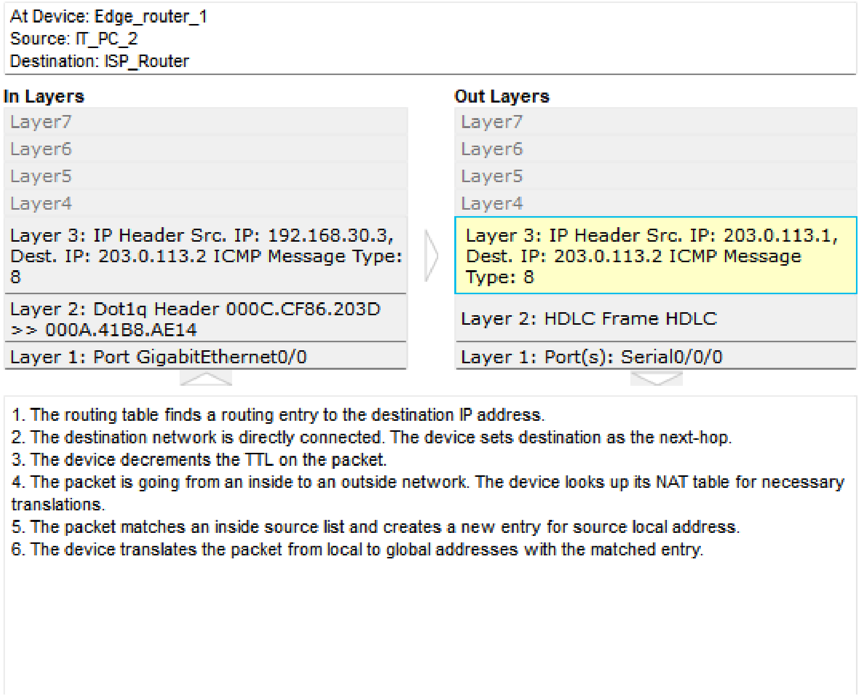
One challenge I encountered was NAT (Network Address Translation) interfering with the VPN. NAT modifies the IP headers of packets, which can disrupt the VPN's ability to encrypt traffic properly. To resolve this, I excluded the VPN traffic from NAT using an access list (figure 10). This ensures that traffic between the HQ and Remote Site is not altered by NAT and can be encrypted correctly by the VPN.

Figures 11 and 12 show a demonstration of NAT being active and inactive, according to whether traffic is directed to the VPN or not.



```
access-list 101 deny ip 192.168.10.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 101 deny ip 192.168.20.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 101 deny ip 192.168.30.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 101 deny ip 192.168.90.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 101 permit ip any any
```

Figure 12: NAT access control list

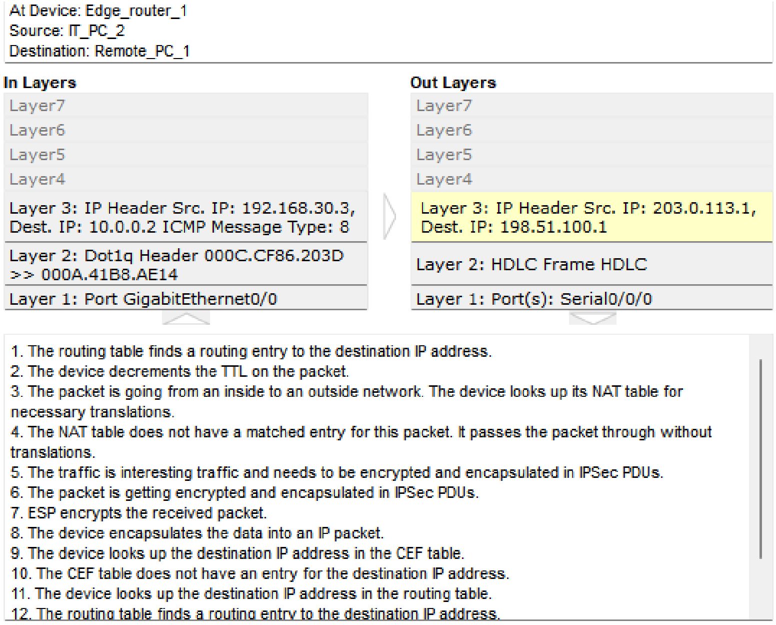


At Device: Edge_router_1
Source: IT_PC_2
Destination: ISP_Router

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.30.3, Dest. IP: 203.0.113.2 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 203.0.113.1, Dest. IP: 203.0.113.2 ICMP Message Type: 8
Layer 2: Dot1q Header 000C.CF86.203D >> 000A.41B8.AE14	Layer 2: HDLC Frame HDLC
Layer 1: Port GigabitEthernet0/0	Layer 1: Port(s): Serial0/0/0

1. The routing table finds a routing entry to the destination IP address.
2. The destination network is directly connected. The device sets destination as the next-hop.
3. The device decrements the TTL on the packet.
4. The packet is going from an inside to an outside network. The device looks up its NAT table for necessary translations.
5. The packet matches an inside source list and creates a new entry for source local address.
6. The device translates the packet from local to global addresses with the matched entry.

Figure 13: packet being set to outer network is being translated (point 4)

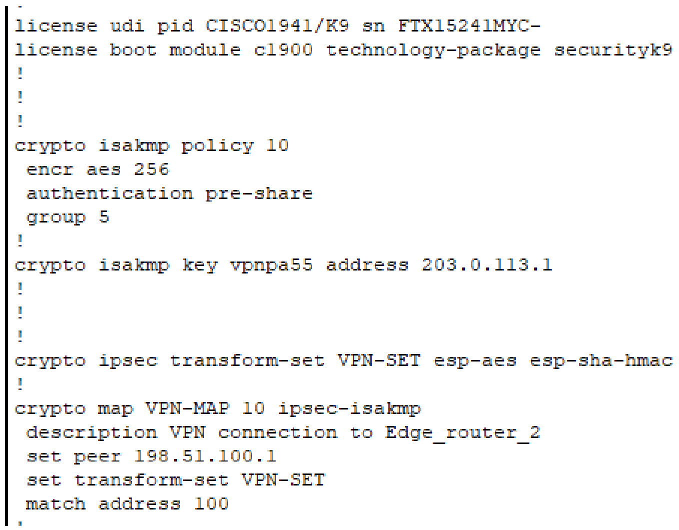


At Device: Edge_router_1
Source: IT_PC_2
Destination: Remote_PC_1

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.30.3, Dest. IP: 10.0.0.2 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 203.0.113.1, Dest. IP: 198.51.100.1
Layer 2: Dot1q Header 000C.CF86.203D >> 000A.41B8.AE14	Layer 2: HDLC Frame HDLC
Layer 1: Port GigabitEthernet0/0	Layer 1: Port(s): Serial0/0/0

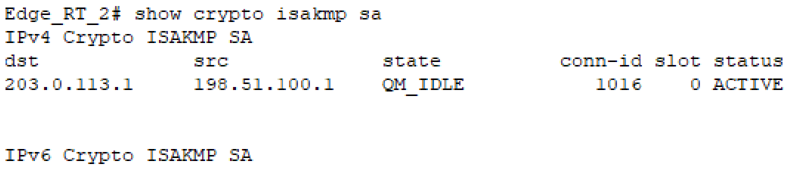
1. The routing table finds a routing entry to the destination IP address.
2. The device decrements the TTL on the packet.
3. The packet is going from an inside to an outside network. The device looks up its NAT table for necessary translations.
4. The NAT table does not have a matched entry for this packet. It passes the packet through without translations.
5. The traffic is interesting traffic and needs to be encrypted and encapsulated in IPSec PDUs.
6. The packet is getting encrypted and encapsulated in IPSec PDUs.
7. ESP encrypts the received packet.
8. The device encapsulates the data into an IP packet.
9. The device looks up the destination IP address in the CEF table.
10. The CEF table does not have an entry for the destination IP address.
11. The device looks up the destination IP address in the routing table.
12. The routing table finds a routing entry to the destination IP address.

Figure 14: packet being sent through VPN is not translated (point 4)



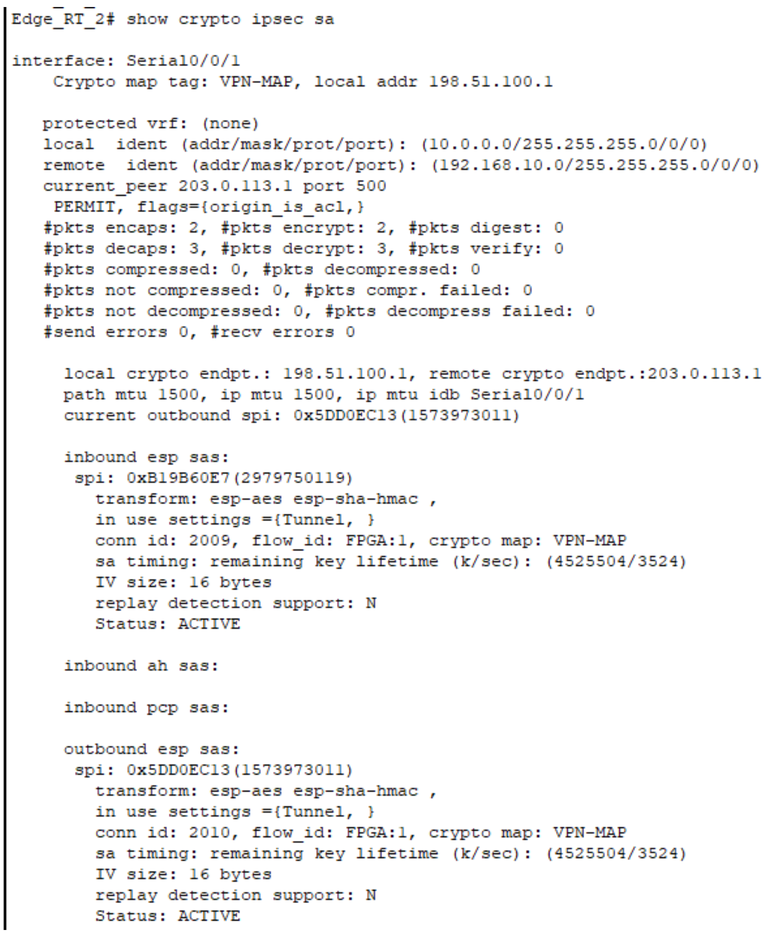
```
license udi pid CISCO1941/K9 sn FTX15241MYC-
license boot module c1900 technology-package securityk9
!
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key vpnpa55 address 203.0.113.1
!
!
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN connection to Edge_router_2
 set peer 198.51.100.1
 set transform-set VPN-SET
 match address 100
```

Figure 15: VPN configuration



```
Edge_RT_2# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
203.0.113.1     198.51.100.1    QM_IDLE           1016    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Figure 16: ISAKMP shows active channel



```
Edge_RT_2# show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: VPN-MAP, local addr 198.51.100.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 203.0.113.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 198.51.100.1, remote crypto endpt.:203.0.113.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
     current outbound spi: 0x5DD0EC13(1573973011)

     inbound esp sas:
      spi: 0xB19B60E7(2979750119)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3524)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x5DD0EC13(1573973011)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2010, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3524)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

Figure 17 IPsec SA show the packet being encrypted while travelling through the tunnels

Conclusion

This terminates my security configuration for the subject typology.

While the process was challenging at times, it provided an invaluable learning experience. I thoroughly enjoyed diving into the intricacies of network security, troubleshooting issues, and applying best practices to create a secure and efficient network. This project has significantly deepened my understanding of network security, and I look forward to applying these skills in future endeavors.

References

- Avijit Mallik, “MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS”, 2018, available at: MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS | Mallik | Cyberspace: Jurnal Pendidikan Teknologi Informasi , V 2 pp 109-134, [accessed: 25 November 2024]
- Aws Naser Jaber, Mohamad Fadli Bin Zolkipli, Mazlina Binti Abdul Majid, “Security Everywhere Cloud: An Intensive Review of DoS and DDoS Attacks in Cloud Computing”, 2015, available at: Aws Naser Jaber et al. / Journal of Advanced & Applied Sciences (JAAS), 3 (5): 152-158, 2015 , V 03, Issue 05, pp 152-158, [accessed: 25 November 2024]
- Asaduzzaman Jony; Muhammad Nazrul Islam; Iqbal H. Sarker, 2023, “Unveiling DNS Spoofing Vulnerabilities: An Ethical Examination Within Local Area Networks”, available at: 10.1109/ICCIT60459.2023.10441649 , [accessed: 5 December 2024]
- Dr.A.Shaji George, A.S.Hovan George, Dr.T.Baskar, 2023, “SD-WAN Security Threats, Bandwidth Issues, SLA, and Flaws: An In-Depth Analysis of FTTH, 4G, 5G, and Broadband Technologies”, available at: https://doi.org/10.5281/zenodo.8057014 , [accessed: 4 January 2025]
- Davis Booker, 2023, “ARP Spoofing: Threats and Countermeasures”, 2023, available at: ARP Spoofing: Threats and Countermeasures | by Davis Booker (ISC)^2 | SEC + | Medium , [accessed: 4 January 2025]
- Elankayer Sithirasenan; Vallipuram Muthukkumarasamy, “Detecting Security Threats in Wireless LANs Using Timing and Behavioral Anomalies”, 2007, available at: 10.1109/ICON.2007.4444063 , [accessed: 5 December 2024]
- Kuburat Oyeranti Adefemi Alimi,Khmaies Ouahada ,Adnan M. Abu-Mahfouz, andSuvendi Rimer, 2020, available at: **https://doi.org/10.3390/s20205800** , [accessed: 6 January 2025]
- Leonardo Richter Bays, Rodrigo Ruas Oliveira, Marinho Pilla Barcellos, Luciano Paschoal Gaspary & Edmundo Roberto Mauro Madeira, “Virtual network security: threats, countermeasures, and challenges”, 2015, available at: Virtual network security: threats, countermeasures, and challenges | Journal of Internet Services and Applications , [accessed: 25 November 2024]
- Mauro Conti; Nicola Dragoni; Viktor Lesyk, 2016, “A Survey of Man In The Middle Attacks”, available at: 10.1109/COMST.2016.2548426 , V 18, Issue 3, pp 2027- 2051, [accessed: 6 January 2025]
- Muhammad Raza, Splunk, 2024, “Intrusion Detection Systems (IDS): Definition, Types, Purpose”, available at: Intrusion Detection Systems (IDS): Definition, Types, Purpose | Splunk , [accessed: 6 January 2025]