Network Project Documentation

Project Title: Enterprise Network Design and Security

Course:Network Security-NTI

Student Name: Alaa Mostafa Saeed

Table of Contents

Introduction 3

Network Design..... 3

Implementation..... 4

Testing & Verification..... 6

Conclusion..... 10

Introduction

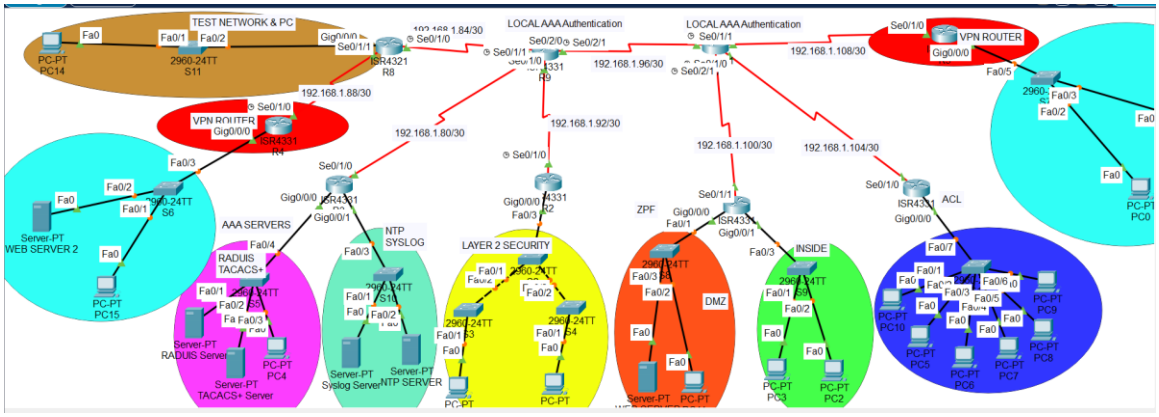
Project Objective: Applying Network Security concepts to an enterprise network topology

Scope: Subnetting, OSPF + Authentication, ACL, AAA, ZBF, VPN, SSH

Tools Used: Cisco Packet Tracer

Network Design

4.1 Topology:



4.2 IP Addressing & Subnetting:

Subnets	Network ID	Default gateway
192.168.1.0/28	192.168.1.0	192.168.1.1
192.168.1.16/29	192.168.1.16	192.168.1.17
192.168.1.24/29	192.168.1.24	192.168.1.25
192.168.1.32/29	192.168.1.32	192.168.1.33
192.168.1.40/29	192.168.1.40	192.168.1.41
192.168.1.48/29	192.168.1.48	192.168.1.49
192.168.1.56/29	192.168.1.56	192.168.1.57

192.168.1.64/29	192.168.1.64	192.168.1.65
192.168.1.72/29	192.168.1.72	192.168.1.73
192.168.1.80/30	192.168.1.80	192.168.1.81
192.168.1.84/30	192.168.1.84	192.168.1.85
192.168.1.88/30	192.168.1.88	192.168.1.89
192.168.1.92/30	192.168.1.92	192.168.1.93
192.168.1.96/30	192.168.1.96	192.168.1.97
192.168.1.100/30	192.168.1.100	192.168.1.101
192.168.1.104/30	192.168.1.104	192.168.1.105

4.3 Routing Protocol:

All routers were configured under OSPF process ID 1, and all networks were placed in Area 0 for simplicity.

We used MD5 as our authentication type and authentication was done on all interfaces.

Implementation

5.1 Subnetting:

The given block was 192.168.0.0/24. We divided it into multiple subnets to accommodate the LANs and WAN links. Each LAN required up to 14 hosts, so we used /28 subnets. WAN links were point-to-point, so /30 subnets were sufficient. The addressing scheme ensures efficient IP usage.

5.2 OSPF Configuration:

All routers were configured with OSPF process ID 1. Networks from LANs and WAN links were advertised under Area 0. To secure routing updates, OSPF MD5 authentication was applied on the WAN interfaces.

5.3 SSH Configuration:

SSH was configured on all routers and switches to secure remote access. Telnet was disabled, and only SSH connections are permitted. A local admin user with a strong password was created for authentication.

5.4 VPN Setup:

A site-to-site VPN was configured to provide secure communication between the R4 and R5 routers. The VPN ensures that data traveling over the public network is encrypted and authenticated. ISAKMP (IKE Phase 1) was used to establish the security association, while IPsec (Phase 2) handled encryption using AES. The VPN tunnel was verified by sending encrypted traffic between LAN hosts.

5.5 Zone-Based Firewall (ZBF):

A Zone-Based Firewall was implemented to enforce security policies between different network zones. Three zones were defined: INSIDE (LAN), OUTSIDE (WAN/Internet), and DMZ (public services). Class maps were created to identify traffic, policy maps to define actions, and zone-pair policies to permit or block traffic accordingly. This provided granular control compared to traditional ACLs.

5.6 Access Control Lists (ACLs):

“ACLs were configured to filter traffic and enforce security policies. Extended ACLs was used for controlled access to specific services. For example, HTTP traffic from the LAN was allowed to the Internet, while ping access was explicitly denied. ACLs also played a role in defining interesting traffic for the VPN.

5.7 Authentication, Authorization, Accounting (AAA):

AAA was implemented to secure device access. Local AAA provided basic username/password authentication, while server-based AAA (RADIUS/TACACS+) was simulated for centralized authentication. Authorization was configured to control user privilege levels, and accounting was set to log administrative access attempts.

Testing & Verification

Connectivity (Ping/Traceroute):

Basic connectivity was verified using ICMP pings and traceroute between hosts across different subnets. Successful replies confirmed proper IP addressing and routing.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.89

Pinging 192.168.1.89 with 32 bytes of data:

Reply from 192.168.1.89: bytes=32 time=4ms TTL=251
Reply from 192.168.1.89: bytes=32 time=4ms TTL=251
Reply from 192.168.1.89: bytes=32 time=5ms TTL=251
Reply from 192.168.1.89: bytes=32 time=79ms TTL=251

Ping statistics for 192.168.1.89:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 79ms, Average = 23ms
```

OSPF Neighbors:

OSPF neighbor adjacencies were verified using the `show ip ospf neighbor` command. The output confirmed that all routers formed adjacencies and exchanged LSAs successfully.

```
R7#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.98      0   FULL/  -        00:00:31    192.168.1.98    Serial0/1/1
192.168.1.109     0   FULL/  -        00:00:37    192.168.1.109   Serial0/2/0
192.168.1.105     0   FULL/  -        00:00:30    192.168.1.105   Serial0/1/0
192.168.1.101     0   FULL/  -        00:00:30    192.168.1.101   Serial0/2/1
```

ACL Testing:

ACL functionality was tested by attempting allowed and denied traffic. For example, HTTP traffic from the LAN to the Internet was successful, while ICMP ping was blocked as intended

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

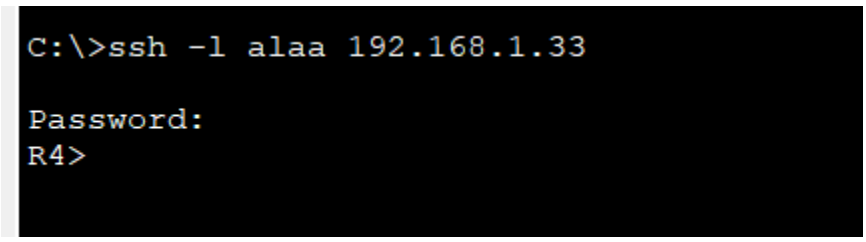
VPN Verification:

The VPN tunnel was verified by generating interesting traffic between LANs. The `show crypto map` and `show crypto ipsec sa` commands confirmed that encrypted packets were successfully exchanged.

```
R4#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: R4-R5_MAP, local addr 192.168.1.89

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.32/255.255.255.248/0/0)
   remote  ident (addr/mask/prot/port): (192.168.1.40/255.255.255.248/0/0)
   current_peer 192.168.1.109 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #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.: 192.168.1.89, remote crypto endpt.:192.168.1.109
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

R4#
R4#show crypto ?
  ipsec   Show IPSEC policy
  isakmp  Show ISAKMP
  key     Show long term public keys
  map     Crypto maps
R4#show crypto map
Crypto Map R4-R5_MAP 10 ipsec-isakmp
        Peer = 192.168.1.109
        Extended IP access list 103
            access-list 103 permit ip 192.168.1.32 0.0.0.7 192.168.1.40 0.0.0.7
        Current peer: 192.168.1.109
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): Y
        Transform sets={
                R4-R5,
        }
        Interfaces using crypto map R4-R5_MAP:
                Serial0/1/0
```

SSH Connection Test:

SSH access to routers was tested using an SSH client. Login with the configured admin user"alaa" was successful, confirming secure remote access.



AAA Login Verification:

AAA login was verified by attempting to access the router. Local credentials were accepted, and when simulated, the router also checked against the RADIUS server and TACACS+ server. Failed login attempts were denied.

ZBF Testing:

Zone-Based Firewall rules were verified by generating traffic between zones. Permitted traffic (HTTP, ICMP,HTTPS,SSH) passed successfully, while unauthorized traffic was dropped. Logs confirmed the firewall actions.

```
R6#show policy-map type inspect zone-pair sessions

policy exists on zp IN-OUT
 Zone-pair: IN-OUT

  Service-policy inspect : IN-OUT-pol

    Class-map: IN-to-OUT (match-any)
      Match: protocol http
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol https
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol ssh
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        0 packets, 0 bytes
        30 second rate 0 bps
      Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes

policy exists on zp OUT-DMZ
 Zone-pair: OUT-DMZ

  Service-policy inspect : OUT-DMZ-pol

    Class-map: OUT-to-DMZ (match-any)
      Match: protocol http
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol https
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol ssh
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
```

Conclusion

Summary of achievements:

In this project, we successfully designed and implemented a secure enterprise network. The network was divided into well-structured subnets with an efficient IP addressing scheme. Dynamic routing was achieved using OSPF with authentication, ensuring secure and reliable routing updates. Remote access was secured through SSH, and site-to-site VPN provided encrypted communication between sites. Security policies were enforced using ACLs and a Zone-Based Firewall, while AAA added centralized authentication and access control. Testing and verification confirmed that all objectives were met and that the network operated as intended.

Future improvements:

Although the project met all the required objectives, several enhancements can be considered for future work. These include adding redundancy with protocols such as HSRP/VRRP, implementing load balancing, integrating more advanced intrusion prevention systems (IPS/IDS), and extending the VPN setup to include remote access users. These improvements would help the network achieve higher resilience, scalability, and enterprise-level security.