

Network Security Architecture with Zero Trust Implementation

Contents

Executive Summary:	4
Block A: Architecture and Communication	5
2.1 Configure IP connectivity and device hardening	6
2.1.1 Login to CISCO ASA 5505 Firewall and Configure the Separate VLAN 3 interfaces for Finance LAN	7
2.1.2 Now Assign the VLAN to the Physical port Ethernet0/1 to ASA Firewall	7
2.1.3 Configure VLAN in Finance LAN Switch which is connected to CISCO ASA 5505	7
2.1.4 Moving Towards the Finance DMZ Zone Configuration section	8
2.1.5 Configure the VLAN 2 In the DMZ switch	8
2.1.6 Login to ASA 5505 and Configure the VLAN 2 and Ethernet0/2 Address	8
2.1.7 Now testing to End to End Connectivity from LAN IP 192.168.30.40 to DMZ Webserver	9
2.1.8 ASA 5505 to Internal Router Network Configuration	9
2.1.9 Configure VLAN Interface 6 in the switch	10
2.1.10 Logged in the internal router and Configure the subinterface and encapsulation for inter-VLAN routing	10
2.1.11 Connectivity from Firewall to router Established	11
2.2 Configure servers DHCP, DNS, WEB, SYS-Log	12
2.2.1 Configure the Dynamic host configuration Protocol [DHCP] in CISCO ASA 5505	12
2.2.2 Configure the DNS server in DMZ environment	13
2.2.3 Configure the Web server in the DMZ	14
2.2.4 Configure the Syslog server in finance LAN	14
2.2.5 Configure IP address on finance Interface Vlan 3	15
2.2.6 Execute the Command to Set the Login username and password on the finance Switch	15
2.2.7 Login from site Admin machine with user id and password	16
2.2.8 Logs are generated and sent to Syslog server	16
2.3 Configure Dynamic Routing (RIPV2) and Inter-Vlan Routing/Trunking	17
2.3.1 Configuring the Internal Router with Sub-interface	17
2.3.2 Now moving towards the Internet Router and Configure serial Interface 0/1/0 and 0/1/1 with relevant IP Address	17
2.3.3 Execute the below mention configuration in the External router	18
2.4 Routing Information Protocol Configuration for Exchanging Networks Information	19
2.4.1 Internal Router	19
2.4.2 Internet Router	19
2.4.3 External Router	19
Block B: Secure Operations and Service Delivery	21
3.1 Implement ACL and Firewall on ASA device	21

3.2	Implement Site-To-Site IPsec VPN	22
3.2.1	Internal Router VPN Configuration	22
3.2.2	External Router Configuration	24
3.3	NIPS implementation and testing	28
Research & Development		30
4.1	Zero Trust Network Security Framework.....	30
4.2	Overview of VPN reliability	31
4.3	Cryptographic mechanism of IPsec.....	32
Conclusion and Future Work		33

1 Executive Summary:

An integrated high performance, extremely consistent, scalable, and protected network communication is crucial for every organization, which can safeguard, sensitive digital information. Hence the implementor need to explore every aspect about the security threats which can be leveraged by the hacker to gain access to those critical assets

The goal to implement network security to develop security posture around the digital workflow and process. which ensure safe and reliable business continuity, without any information leakage or any unfavourable factors, and also make sure that the all the digital assets which connected through networks have some security measure applied such as firewall, antivirus, encryption and access list. And so on.

This paper explores various security assessment while developing core network architecture and it also emphasizes to deliver a highly secure environment in which only legitimate key person who is dealing with core Infrastructure system, only have access to the critical applications such as DNS server web server, Syslog server or any other service which can require the optimum security from internal as well as the outer world

2 Block A: Architecture and Communication

As networks grow, its complexity will also increase, and so it poses greater (Varadharajan et al., 2019) administrative and execution challenges. However, there are certain protocol and policy-driven mechanism offer a promising solution to overcome some of those challenges. Network Security is a multi-dimension approach it cannot be fulfilled by only one single methodology hence Implementor needs to apply certain control (Wang et al., 2007) on the network topology such as VLAN.IDS IPS, VPN and Access list, which can further strengthen the security posture of the Networks In the BLOCK A demonstrates how the end to end connectivity configured according to figure [figure 1.1]

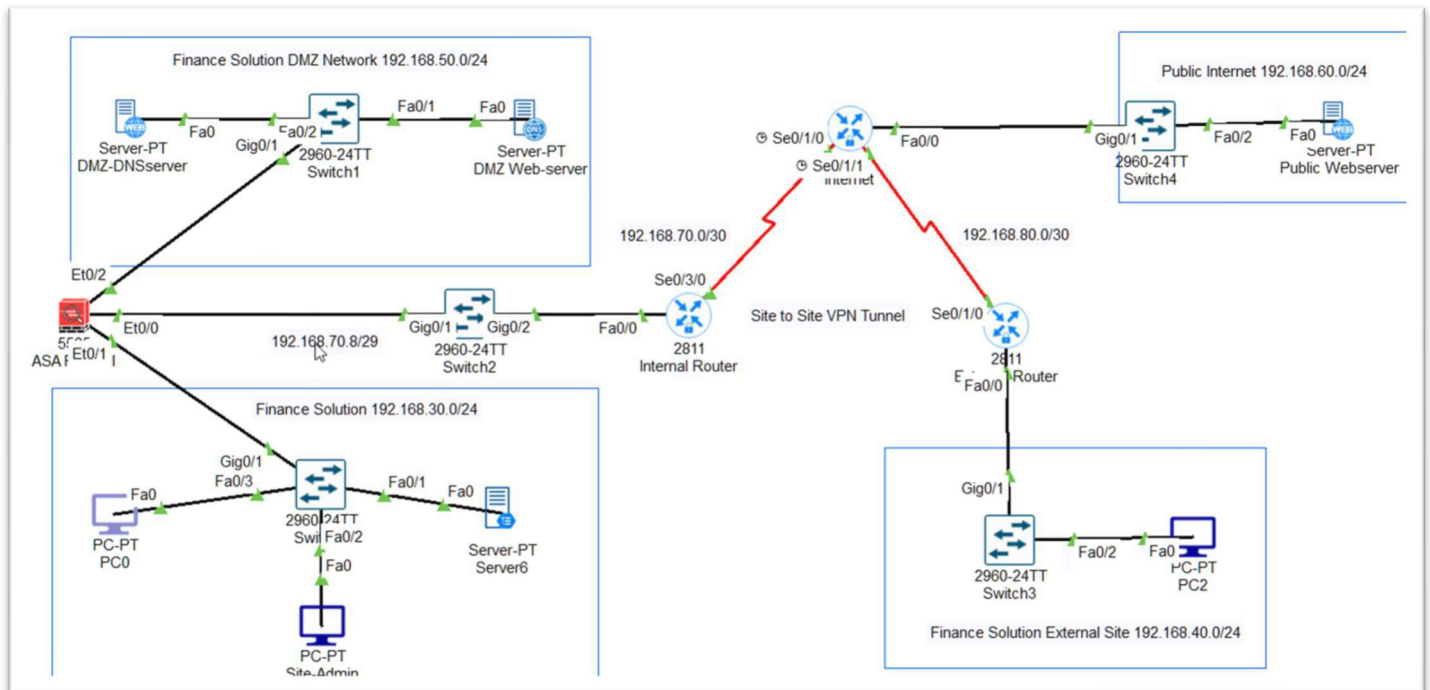


Figure 1.1 [Network Infrastructure Diagram with DHCP , DNS, Web, Syslog server with Site to site VPN connectivity]