**Cisco ASA 5506-X Firewall Configuration on a 3-Tier Campus LAN Architecture**

**Created by: Antonio Scotland**

**Table of Contents**

[Abstract 3](#_Toc129170616)

[Introduction 5](#_Toc129170617)

[Method and Equipment 5](#_Toc129170618)

[Update Static Routes on SP1 5](#_Toc129170619)

[Hostname Configuration on ASA1 5](#_Toc129170620)

[Ip Subnetting on ASA1, R1 and R2 6](#_Toc129170621)

[Update OSPF configuration and default route on R1 and R2 7](#_Toc129170622)

[Configure OSPF and default route on ASA1 7](#_Toc129170623)

[Create Object Network and Configure Address Translation using PAT on ASA1 8](#_Toc129170624)

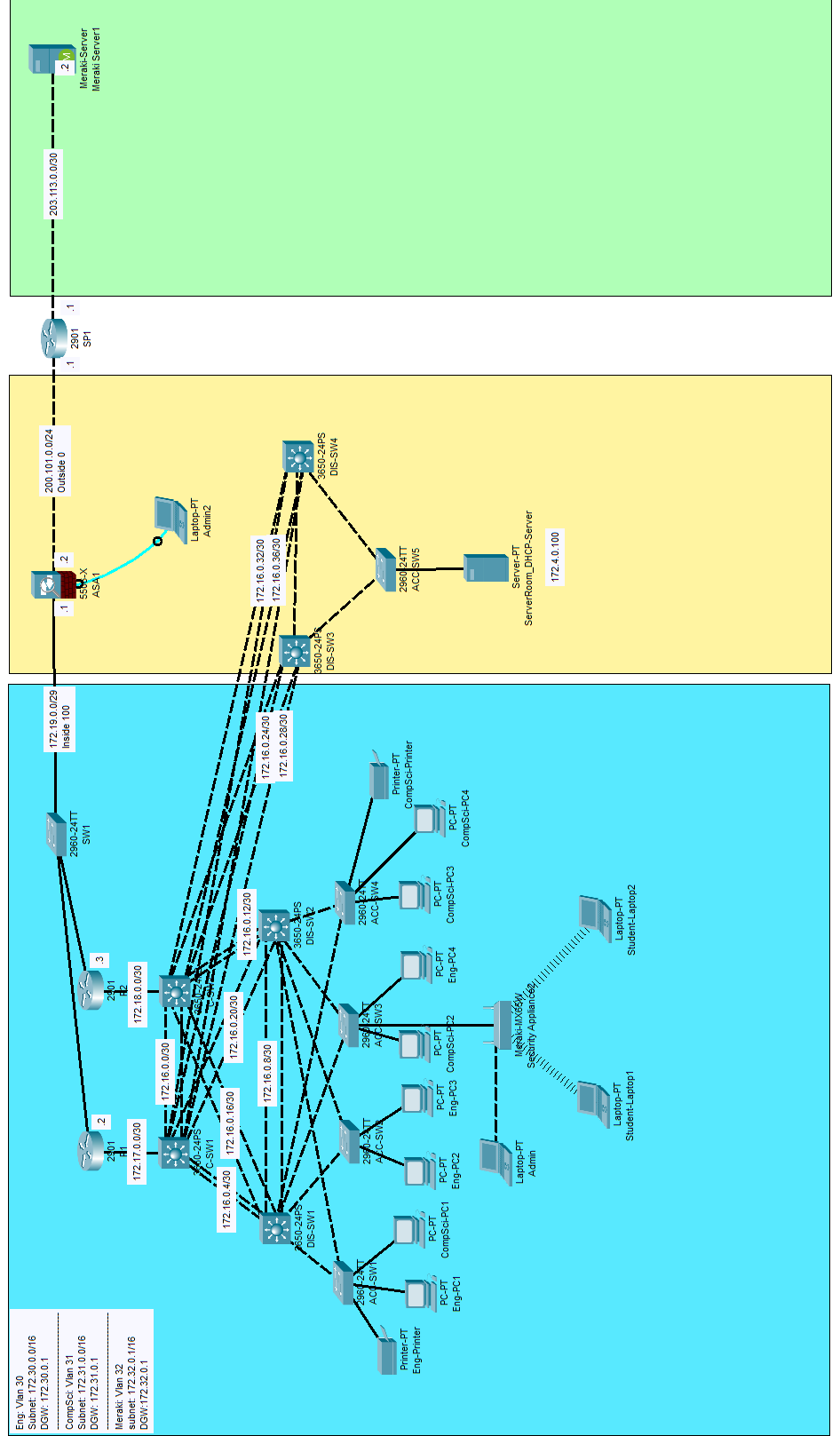
[Create ACL on ASA1 8](#_Toc129170625)

[Verification & Discussion 9](#_Toc129170626)

[Reference 13](#_Toc129170627)

# Abstract

In this packet tracer project, I was able to implement a firewall using the Cisco ASA 5506-X appliance. This is a continuation from a previous project titled as “[Cisco Meraki Centralized WLC on a 3-Tier Campus LAN Architecture](https://github.com/ascotlan/Cisco-Meraki-Centralized-WLC-on-a-3-Tier-Campus-LAN-Architecture)”. Security levels were configured on the inside and outside interface on the firewall. I then successfully configured dynamic routes to/from the inside interface on the firewall using the OSPF routing protocol. A static default route to the outside was configured on the firewall. An object network was implemented to represent the inside network. That object was used to create address translation to the outside interface using PAT. ACLs were implemented to manage the flow of key traffic.



# Introduction

The goal is to secure the LAN implemented in the previous project titled as “[Cisco Meraki Centralized WLC on a 3-Tier Campus LAN Architecture](https://github.com/ascotlan/Cisco-Meraki-Centralized-WLC-on-a-3-Tier-Campus-LAN-Architecture) “, using the Cisco ASA 5506-X firewall. After configuring a hostname on the Cisco ASA appliance, names, service-levels, and IP addresses will be assigned to the outside and inside interfaces on the Cisco ASA appliance. I will update the static routes on the service provider router so that traffic from the service provider router has a route to the LAN with the firewall outside interface IP address as the next hop address. The interfaces on routers R1 and R2 facing the inside interface of the firewall will be added to the same subnet as the firewall inside interface using static IP assignment. Default routes to the inside interface on the firewall will also be configured on routers R1 and R2. The OSPF configuration will be updated to reflect the changes on R1 and R2. OSPF will also be configured on the inside interface of the ASA appliance and a default route outside the LAN will be implemented. An object network will be used to translate the LAN network to the outside interface using Port Address Translation (PAT).

# Method and Equipment

## Update Static Routes on SP1

### SP1

SP1>en

SP1#show run | include ip route

!

ip route 172.0.0.0 255.0.0.0 200.101.0.2

ip route 172.0.0.0 255.0.0.0 200.101.0.3

!

SP1#config t

Enter configuration commands, one per line. End with CNTL/Z.

SP1(config)#no ip route 172.0.0.0 255.0.0.0 200.101.0.3

SP1(config)#do show run | include ip route

!

ip route 172.0.0.0 255.0.0.0 200.101.0.2

## Hostname Configuration on ASA1

ciscoasa>en

Password:

ciscoasa#config t

ciscoasa(config)#hostname ASA1

ASA1(config)#exit

ASA1#copy run start

Source filename [running-config]?

Cryptochecksum: 3242414f 76390dfd 4d1b3eb0 56931cb5

1102 bytes copied in 1.422 secs (774 bytes/sec)

ASA1#

## Ip Subnetting on ASA1, R1 and R2

### ASA1

ASA1#config t

ASA1(config)#int g1/1

ASA1(config-if)#ip address 200.101.0.2 255.255.255.0

ASA1(config-if)#no shutdown

ASA1(config-if)#nameif outside

INFO: Security level for "outside" set to 0 by default.

ASA1(config-if)#security-level 0

ASA1(config-if)#int g1/2

ASA1(config-if)#ip address 172.19.0.1 255.255.255.248

ASA1(config-if)#nameif inside

INFO: Security level for "inside" set to 100 by default.

ASA1(config-if)#security-level 100

ASA1(config-if)#no shutdown

### R1

R1>en

R1#config t

R1(config)#do show run | incl ip address

!

ip address 172.17.0.1 255.255.255.252

ip address 200.101.0.2 255.255.255.0

no ip address

!

R1(config)#int g0/1

R1(config-if)#no ip address 200.101.0.2 255.255.255.0

R1(config-if)#ip address 172.19.0.2 255.255.255.248

### R2

R2>en

R2#config t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#do show run | incl ip address

!

ip address 172.18.0.1 255.255.255.252

ip address 200.101.0.3 255.255.255.0

no ip address

!

R2(config)#int g0/1

R2(config-if)#no ip address 200.101.0.3 255.255.255.0

R2(config-if)#ip address 172.19.0.3 255.255.255.248

## Update OSPF configuration and default route on R1 and R2

### R1

R1#show run | section ospf

!

router ospf 1

log-adjacency-changes

network 172.17.0.0 0.0.255.255 area 0

network 200.101.0.0 0.0.0.255 area 0

default-information originate

!

R1#config t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#router ospf 1

R1(config-router)#no network 172.17.0.0 0.0.255.255 area 0

R1(config-router)# no network 200.101.0.0 0.0.0.255 area 0

R1(config-router)#network 172.0.0.0 0.255.255.255 area 0

R1(config-router)#exit

R1(config)#ip route 0.0.0.0 0.0.0.0 172.19.0.1

R1(config)#router ospf 1

R1(config-router)#default-information originate

### R2

R2#show run | section ospf

!

router ospf 1

log-adjacency-changes

network 172.18.0.0 0.0.255.255 area 0

network 200.101.0.0 0.0.0.255 area 0

!

R2#config t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#router ospf 1

R2(config-router)#no network 172.18.0.0 0.0.255.255 area 0

R2(config-router)#no network 200.101.0.0 0.0.0.255 area 0

R2(config-router)#network 172.0.0.0 0.255.255.255 area 0

R2(config-router)#exit

R2(config)# ip route 0.0.0.0 0.0.0.0 172.19.0.1

## Configure OSPF and default route on ASA1

### ASA1

ASA1#config t

ASA1(config)#router ospf 1

ASA1(config-router)#network 172.19.0.0 255.255.255.248 area 0

ASA1(config)#route outside 0.0.0.0 0.0.0.0 200.101.0.1

## Create Object Network and Configure Address Translation using PAT on ASA1

### ASA1

ASA1#config t

ASA1(config)#object network INSIDE-NET

ASA1(config-network-object)#subnet 172.0.0.0 255.0.0.0

ASA1(config-network-object)#nat (inside,outside) dynamic interface

ASA1(config-network-object)#exit

## Create ACL on ASA1

### ASA1

ASA1# config t

ASA1(config)#access-list NAT-IP-ALL extended permit tcp any any

ASA1(config)#access-list NAT-IP-ALL extended permit icmp any any

ASA1(config)#access-group NAT-IP-ALL in interface outside

ASA1(config)#exit

ASA1#copy run start

Source filename [running-config]?

Cryptochecksum: 3242414f 76390dfd 4d1b3eb0 56931cb5

1397 bytes copied in 2.726 secs (512 bytes/sec)

# Verification & Discussion

Traffic from the LAN and WLAN subnets can now travel in and out the Cisco ASA 5506-X firewall that stands between the service provider router and the 3-Tier Campus LAN. With OSPF enabled on the inside interface of the ASA 5506-X appliance, routes to/from the firewall inside interface are established. A static default route on the firewall is established, directing traffic to the service provider gateway. All traffic on the network 172.0.0.0 255.0.0.0 is now being translated using PAT to the outside interface on the firewall. Figure 1 &2 show that end hosts in VLAN 30 and 31 on the LAN have two-way communication to end host on the other side of the service provider gateway. Figure 3 demonstrates that wireless end host in the WLAN configured on the Meraki Security Appliance also have two-way communication to the Meraki server. Finally, we see in figure 4 that the HTTPS connection is allowed to the Meraki server and corresponding return traffic is allowed inside the network.

Text

Description automatically generated

Figure -Eng-PC4 in VLAN 30 on the LAN is pinging the Meraki Server

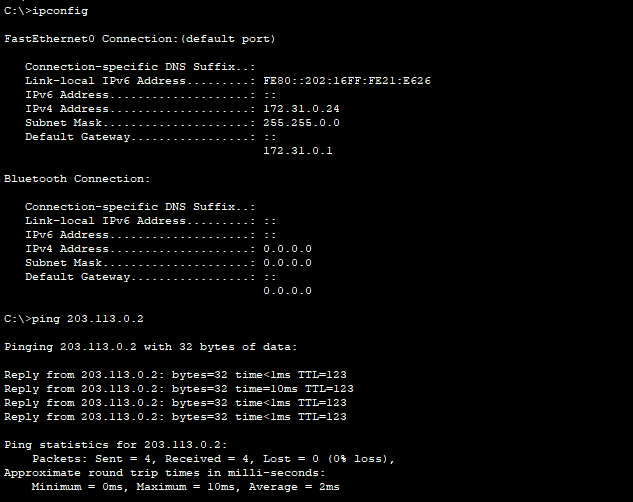


Figure -CompSci-PC1 in VLAN 31 on the LAN is pinging the Meraki Server

Text

Description automatically generated

Figure -Student-Laptop2 on the WLAN can ping the Meraki Server

Graphical user interface, application

Description automatically generated

Figure -Https traffic from the Meraki Security Appliance is allowed through the ASA 5506-X

# Reference

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/firewall/asa-96-firewall-config.html>