# *Project: Firewall Configuration Lab*

Clay Jones

Objective:

Use cisco packet tracer to create a network topology and then proceed in configuring an ASA firewall to monitor and control network traffic. Afterward, use DHCP to automatically assign IP addresses to the endpoint devices. The firewall should not allow untrusted packets to travel to the trusted network.

Network Topology:
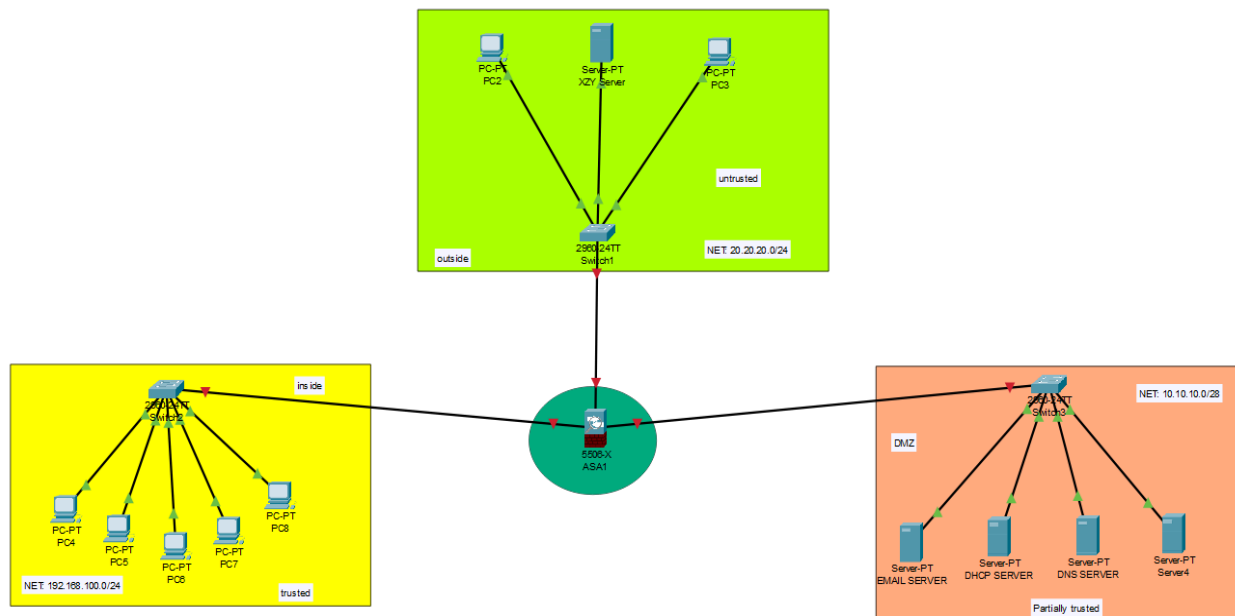
Trusted INSIDE NET: 192.168.100.0/24
Untrusted OUTSIDE NET: 20.20.20.0/24
Partially Trusted DMZ: 10.10.10.0/28

Firewall Setup:

```
ciscoasa>en
Password:
ciscoasa#conf t
ciscoasa(config)#host
% Incomplete command.
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#hostname PERIMETER-FW
PERIMETER-FW(config)#en
% Ambiguous command: "en"
PERIMETER-FW(config)#enable-password
                         ^
% Invalid input detected at '^' marker.

PERIMETER-FW(config)#enable password Gtech123
PERIMETER-FW(config)#username Gtech password Gtech
PERIMETER-FW(config)#username Gtech password Gtech123
PERIMETER-FW(config)#clock set 17:51:30 21 December 2023
PERIMETER-FW(config)#
```

The host was named, the username and password was created, and the clock was set.
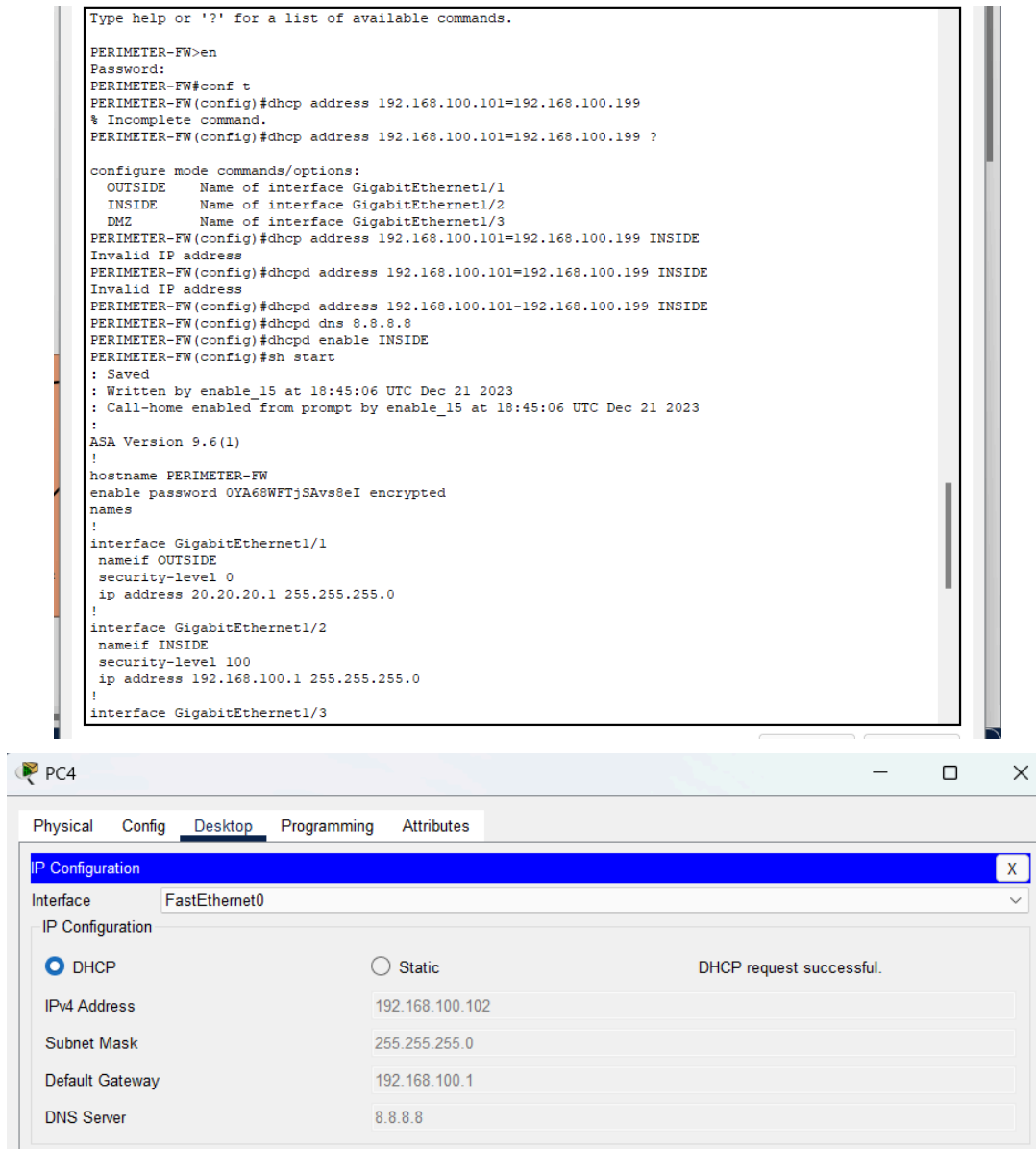
IP configuration, Naming, Adding Security level

```
PERIMETER-FW(config-if)#exit
PERIMETER-FW(config)#int gig1/2
PERIMETER-FW(config-if)#no shut
PERIMETER-FW(config-if)#ip add 192.168.100.1 255.255.255.0
PERIMETER-FW(config-if)#nameif INSIDE
ERROR: Name "INSIDE" has been assigned to interface GigabitEthernet1/3
PERIMETER-FW(config-if)#nameif INSIDEE
INFO: Security level for "INSIDEE" set to 0 by default.
PERIMETER-FW(config-if)#Security-level 100
PERIMETER-FW(config-if)#int gig1/3
PERIMETER-FW(config-if)#no shut
% 192.168.100.0 overlaps with GigabitEthernet1/2
GigabitEthernet1/3: incorrect IP address assignment
PERIMETER-FW(config-if)#ip add 10.10.10.1 255.255.255.240
PERIMETER-FW(config-if)#nameif DMZ
PERIMETER-FW(config-if)#Security-level 70
PERIMETER-FW(config-if)#exit
PERIMETER-FW(config)#int gig1/2
PERIMETER-FW(config-if)#no shut
PERIMETER-FW(config-if)#ip add 192.168.100.1 255.255.255.0
PERIMETER-FW(config-if)#nameif INSIDE
PERIMETER-FW(config-if)#Security-level 100
PERIMETER-FW(config-if)#exit
PERIMETER-FW(config)#int gig1/3
PERIMETER-FW(config-if)#no shut
PERIMETER-FW(config-if)#ip add 10.10.10.1 255.255.255.240
PERIMETER-FW(config-if)#nameif DMZ
PERIMETER-FW(config-if)#exit
PERIMETER-FW(config)#int gig1/3
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1, changed statexit^Z
PERIMETER-FW#
%SYS-5-CONFIG_I: Configured from console by console
ex^Z
PERIMETER-FW#conf t
PERIMETER-FW(config)#int gig1/1
PERIMETER-FW(config-if)#no shut
PERIMETER-FW(config-if)#ip add 20.20.20.1 255.255.255.0
PERIMETER-FW(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
PERIMETER-FW(config-if)#security-level 0
PERIMETER-FW(config-if)#exit
PERIMETER-FW(config)#
```

```
PERIMETER-FW(config)#sh start
: Saved
: Written by enable_15 at 18:45:06 UTC Dec 21 2023
: Call-home enabled from prompt by enable_15 at 18:45:06 UTC Dec 21 2023
:
ASA Version 9.6(1)
!
hostname PERIMETER-FW
enable password 0YA68WFTjSAvs8eI encrypted
names
!
interface GigabitEthernet1/1
 nameif OUTSIDE
 security-level 0
 ip address 20.20.20.1 255.255.255.0
!
interface GigabitEthernet1/2
 nameif INSIDE
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet1/3
 nameif DMZ
 security-level 70
 ip address 10.10.10.1 255.255.255.240
!
```

Cable Connection	IP configuration	Subnet Mask	Name	Security-level
gig1/1	20.20.20.1	255.255.255.0	OUTSIDE	0
gig1/2	192.168.100.1	255.255.255.0	INSIDE	100
gig1/3	10.10.10.1	255.255.255.240	DMZ	70

Using DHCP to automatically assign IP addresses to INSIDE network

```
Type help or '?' for a list of available commands.

PERIMETER-FW>en
Password:
PERIMETER-FW#conf t
PERIMETER-FW(config)#dhcp address 192.168.100.101=192.168.100.199
% Incomplete command.
PERIMETER-FW(config)#dhcp address 192.168.100.101=192.168.100.199 ?

configure mode commands/options:
  OUTSIDE    Name of interface GigabitEthernet1/1
  INSIDE     Name of interface GigabitEthernet1/2
  DMZ        Name of interface GigabitEthernet1/3
PERIMETER-FW(config)#dhcp address 192.168.100.101=192.168.100.199 INSIDE
Invalid IP address
PERIMETER-FW(config)#dhcpd address 192.168.100.101=192.168.100.199 INSIDE
Invalid IP address
PERIMETER-FW(config)#dhcpd address 192.168.100.101-192.168.100.199 INSIDE
PERIMETER-FW(config)#dhcpd dns 8.8.8.8
PERIMETER-FW(config)#dhcpd enable INSIDE
PERIMETER-FW(config)#sh start
: Saved
: Written by enable_15 at 18:45:06 UTC Dec 21 2023
: Call-home enabled from prompt by enable_15 at 18:45:06 UTC Dec 21 2023
:
ASA Version 9.6(1)
!
hostname PERIMETER-FW
enable password 0YA68WFTjSAvs8eI encrypted
names
!
interface GigabitEthernet1/1
 nameif OUTSIDE
 security-level 0
 ip address 20.20.20.1 255.255.255.0
!
interface GigabitEthernet1/2
 nameif INSIDE
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet1/3
```

PC4 — □ ✕

Physical   Config   Desktop   Programming   Attributes

IP Configuration   X

Interface   FastEthernet0   ⌄

IP Configuration

○ DHCP   ○ Static   DHCP request successful.

IPv4 Address   192.168.100.102

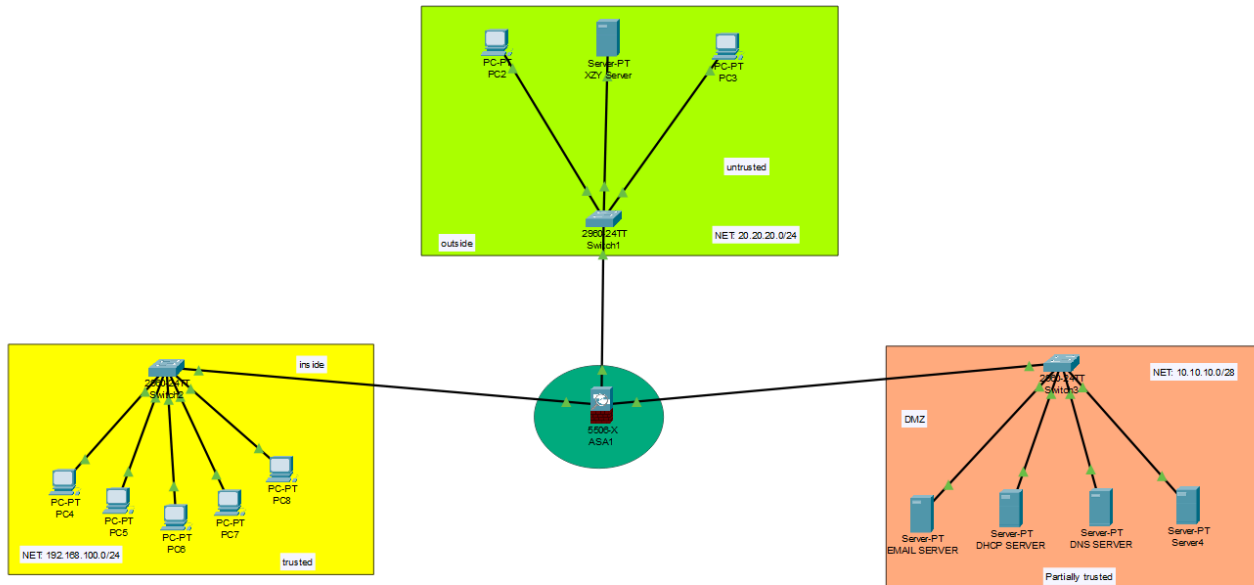Subnet Mask   255.255.255.0

Default Gateway   192.168.100.1

DNS Server   8.8.8.8

DHCP automatically assigned IP addresses to the endpoint devices on the INSIDE network.

Blocking Packets from Untrusted Zone

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC4	PC6	ICMP		0.000	N	0	(edit)	
●	Failed	PC2	PC8	ICMP		0.000	N	1	(edit)	

The packet sent within the INSIDE network was successful meanwhile the packet sent from the OUTSIDE network to the INSIDE was failed showing the firewall rules are working.