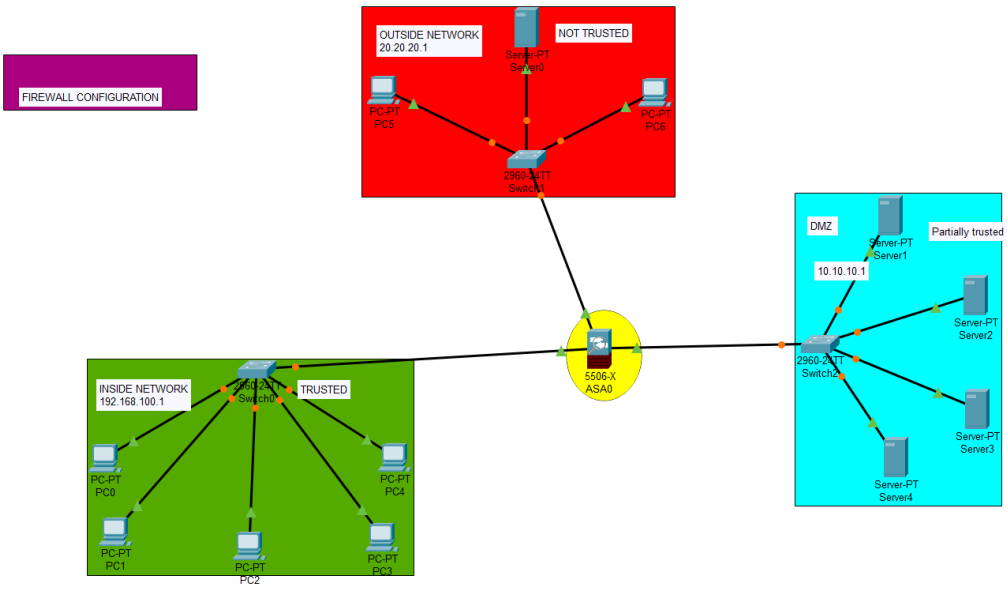
Cisco ASA Firewall Configuration Notes

1. Overview

This document provides configuration notes for the Cisco ASA 5506-X firewall setup simulated in Cisco Packet Tracer. The network consists of three main security zones — Inside (Trusted), DMZ (Partially Trusted), and Outside (Untrusted). The ASA firewall provides segmentation, access control, and basic NAT functionality to secure traffic flow between these zones.

2. Network Topology Diagram

The topology below represents the firewall configuration implemented in Cisco Packet Tracer:



3. Network Zones

The ASA is configured with three main interfaces corresponding to different security zones:

Zone	Interface / IP Address	Security Level
Inside (Trusted)	GigabitEthernet0/1 – 192.168.100.1	100
DMZ (Partially Trusted)	GigabitEthernet0/2 – 10.10.10.1	70
Outside (Untrusted)	GigabitEthernet0/0 – 20.20.20.1	0

4. Basic ASA Configuration Steps

Below are the key configuration steps used in the Cisco ASA firewall setup:

1. 1. Assign interface names and security levels.
2. 2. Configure IP addresses for each interface.
3. 3. Enable interfaces using the `no shutdown` command.
4. 4. Set up default routes and static routes as necessary.
5. 5. Implement Network Address Translation (NAT) for inside-to-outside communication.
6. 6. Create Access Control Lists (ACLs) to define allowed traffic flows.
7. 7. Apply ACLs to appropriate interfaces.
8. 8. Verify connectivity and firewall behavior using ICMP and HTTP tests.

5. Example ASA Configuration Commands

Below are example commands that can be entered in the ASA CLI to configure the firewall. Adjust IP addresses as needed.

```
Configure interface names and security levels
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 20.20.20.1 255.255.255.0
 no shutdown

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
 no shutdown

interface GigabitEthernet0/2
 nameif dmz
 security-level 70
 ip address 10.10.10.1 255.255.255.0
 no shutdown

Set default route to outside network
route outside 0.0.0.0 0.0.0.0 20.20.20.2

NAT configuration
object network INSIDE-NET
 subnet 192.168.100.0 255.255.255.0
 nat (inside,outside) dynamic interface
```

Access control - Allow Inside to access Outside
access-list OUTSIDE-IN extended permit tcp any host 192.168.100.0 eq 80
access-group OUTSIDE-IN in interface outside

Allow DMZ servers limited access
access-list DMZ-IN permit tcp any host 10.10.10.0 eq 80
access-group DMZ-IN in interface dmz

Save configuration
write memory

---

6. Verification & Testing

After configuration, the following verification steps were performed:

- Ping from Inside network (192.168.100.0/24) to Outside (20.20.20.0/24).
- Ping from Inside to DMZ servers (10.10.10.0/24).
- Verify that Outside cannot initiate connections to Inside.
- Access DMZ web server from Inside via HTTP to verify NAT and ACL behavior.

7. Observations and Recommendations

The firewall effectively segments the network into secure zones, restricting external access while allowing internal communication. It is recommended to implement logging, advanced ACL rules, and intrusion prevention for production-level environments.