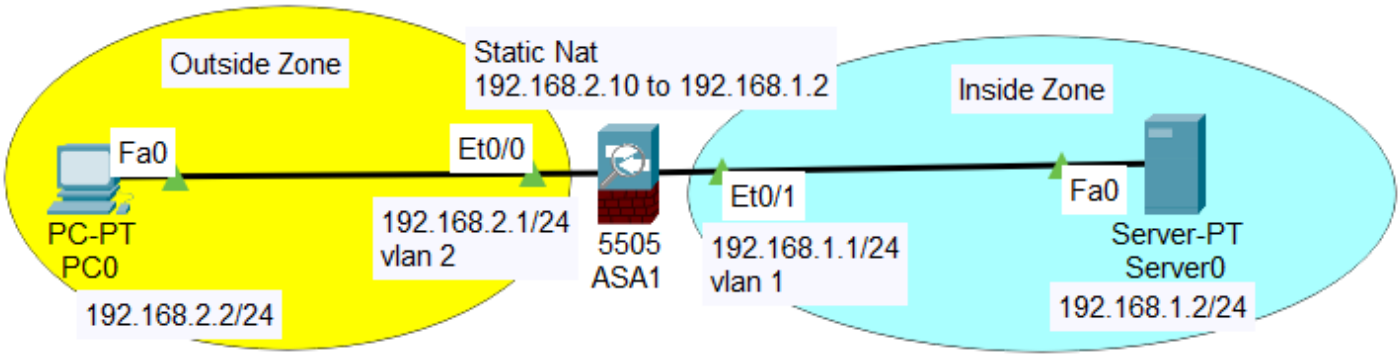
# **Cisco ASA Firewall Lab Assignment** (version 1.7)

Using Cisco Packet Tracer, create a network comprising of one Cisco ASA 5505 firewall, one computer, and one web server. Connect the computer to interface Eth0/0 of the firewall. Connect the server to the interface Eth0/1 of the Cisco ASA firewall. Make sure that port labels are shown (via Options > Preferences > Always Show Port Labels)




IP address of outside computer should be 192.168.2.2 with subnet mask 255.255.255.0

IP address of inside web server should be 192.168.1.2 with subnet mask 255.255.255.0

Eth0/0 interface of Cisco ASA 5505 firewall should be associated with a vlan that is configured with a low security level number in order that the firewall believes that this interface is connected to an untrusted outside network. (Hint: go to *enable* mode, followed by *config* mode and use cli commands *interface, switchport access, nameif, security-level*)

Eth0/1 interface of Cisco ASA 5505 firewall should be associated with another vlan that is configured with a high security level number in order that the firewall believes that this interface is connected to a trusted inside network.

Both interface vlans associated with the inside (Eth0/1) and outside (Eth0/0) interfaces of the firewall need to be assigned IP addresses and subnet mask as shown in above diagram. (Hint: use cli commands *interface, ip address)*

Outside computer and inside web server need to be configured with appropriate default gateway.

Configure static NAT on the firewall to translate server traffic from IP 192.168.1.2 to 192.168.2.10 (Hint: use cli commands *object network, host, nat)*

Configure an access list rule on the firewall to permit any computer from the outside to initiate web traffic to the web server. Also configure another rule to permit any outside computers to ping the web server (Hint: use cli commands *access-list*).

Configure a third rule for the same access list to deny all other traffic initiated from the outside network to the inside network.

Apply access list to the outside interface in the inbound direction. (Hint: use cli commands *access-group*).

Generate various traffic (such as ping, telnet, ssh, web) from the computer to the server by running ping, a telnet/ssh client and web browser on computer. Firewall should permit only icmp and web traffic from the computer to reach the web server.

**1. (2pts)** **Submit** a screenshot of the Packet Tracer network topology. Each network interface should be labelled with port number and IP address.

**2. (2pts)** **Submit** screenshots showing (i) PC0 can ping and traceroute to the web server, and (ii) PC0's web browser can successfully download a web page from web server.

**3.** (**2pts**) In Simulation mode, capture and decode web traffic (i) from PC0 to ASA5505 firewall, and (ii) from ASA5505 firewall to web server. **Submit** screenshots of the decoded IP and TCP header fields within the packets and circle the field in the two packets that shows the IP address prior to and after NAT translation.

**4. (2pts) Submit** outputs of “show switch vlan” , “show nat”, “show xlate”, “show access-list” as evidence that firewall is properly configured and is blocking all traffic initiated from outside except for icmp and http traffic.

**5. (2pts) Submit** a copy of the entire Cisco ASA 5505 firewall configuration file (copy and paste to Word document the entire output of “show running-config” from enable mode of CLI ). Also **submit** a copy of the Cisco Packet Tracer file.

Watch “Packet Tracer ASA” YouTube videos for assistance. Cisco ASA Firewall configuration guide available at http://cs3.calstatela.edu/~egean/cs5781/cisco-asa5505-firewall/