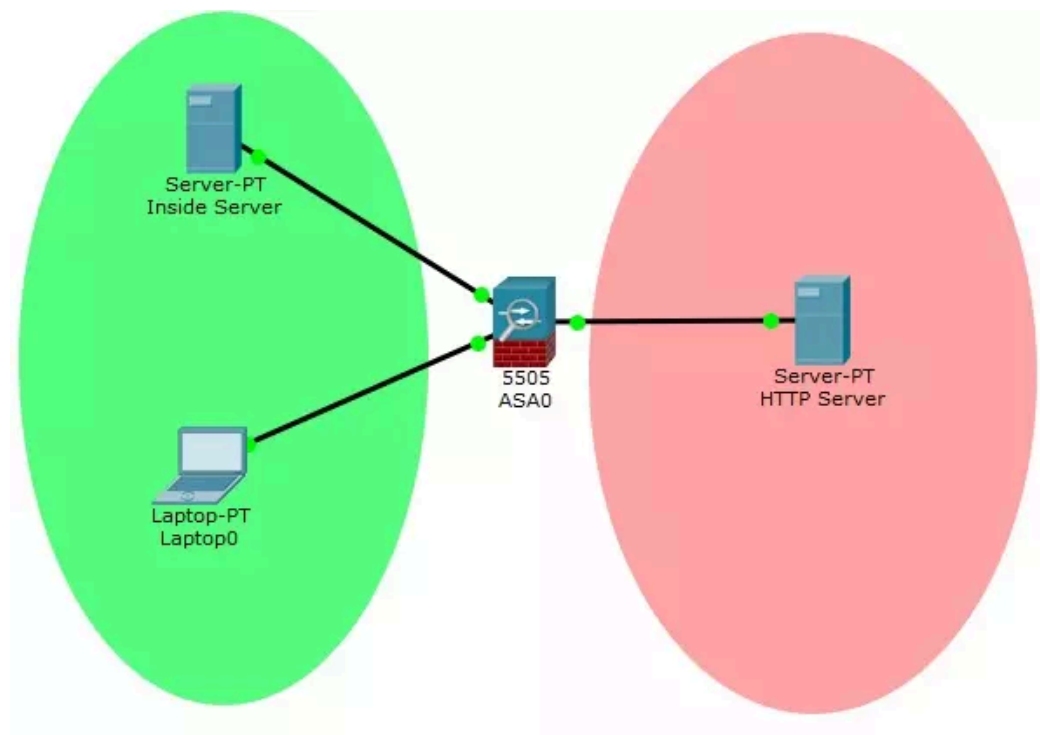


Network diagram

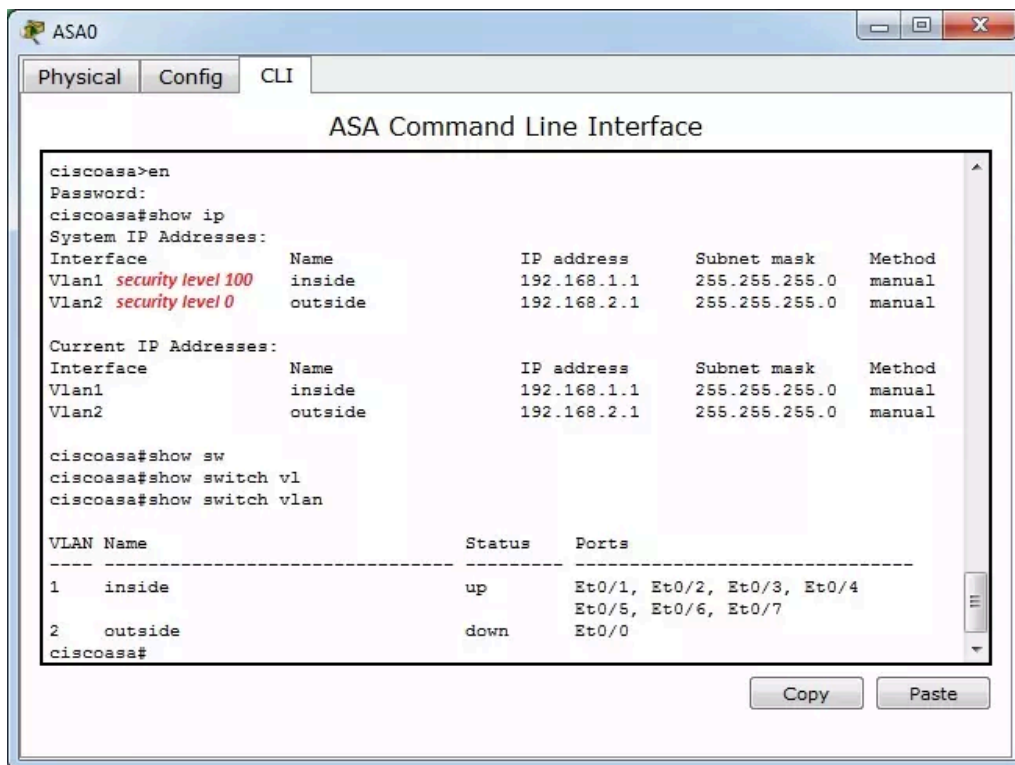


Lab instructions

Configure the ASA firewall to allow HTTP traffic from the laptop (inside network) to the HTTP server located on the other side of the firewall. The traffic will be deeply inspected by the firewall to make sure it contains real HTTP instead of rogue traffic.

All the communication from the outside to the inside network have to remain denied. Only the statefull sessions established from the inside network have to be allowed by the firewall.

Interfaces and vlans default configuration is provided below. The default vlan security levels have been manually added in the picture.



Lab Solution

The default ASA 5505 firewall behavior is to allow traffic to flow from interfaces with higher security levels ("inside" interfaces) to interfaces with lower security levels ("outside" interfaces), but to deny traffic on the other way. Access-lists must be configured to allow the traffic flow from lower security levels to higher security levels.

Default ASA 5505 security levels :

- Inside vlan : Security level 100
- Outside vlan : Security level 0

Despite this default behavior, the simulated ASA 5505 available in Packet Tracer 6.1 does not allow the laptop to establish a working TCP connection with the HTTP server located in the outside network. The TCP SYN is allowed to flow from the laptop to the server, but the TCP ACK is blocked by the firewall.

The following configuration has to be applied to the firewall to establish a working TCP session between the laptop and the HTTP server. This configuration uses the Modular Policy Framework available in Cisco PIX/ASA products :

- Configure a class-map to define the traffic flow having to be inspected
- Define a policy-map to define the particular policy having to be applied to this traffic flow
- Assign the policy to a specific interface (inside interface in the lab)

```
class-map HTTP
  match default-inspection-traffic
!
policy-map TestPolicy
  class HTTP
    inspect http
!
service-policy TestPolicy interface inside
```