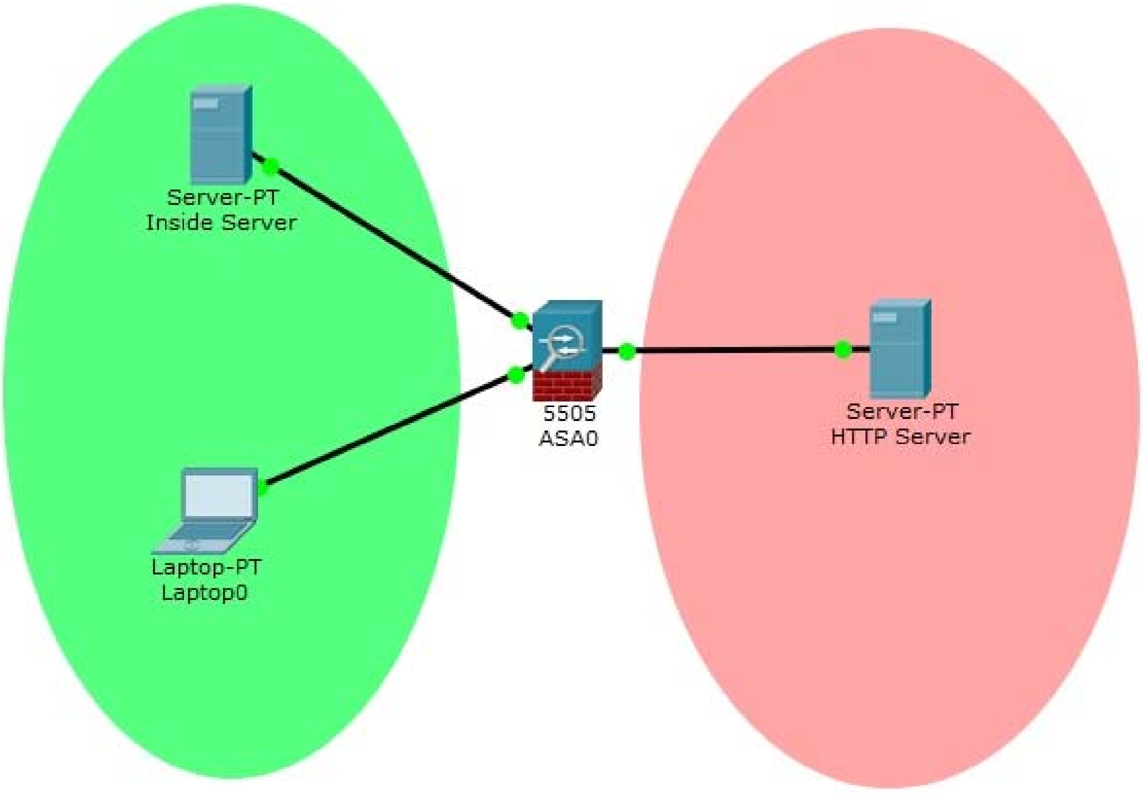
Packet Tracer lab 19 - DPI with ASA 5505

Last Updated: Tuesday, 16 July 2019 21:13
Published: Saturday, 18 October 2014 07:35
Written by PacketTracerNetwork

Network diagram

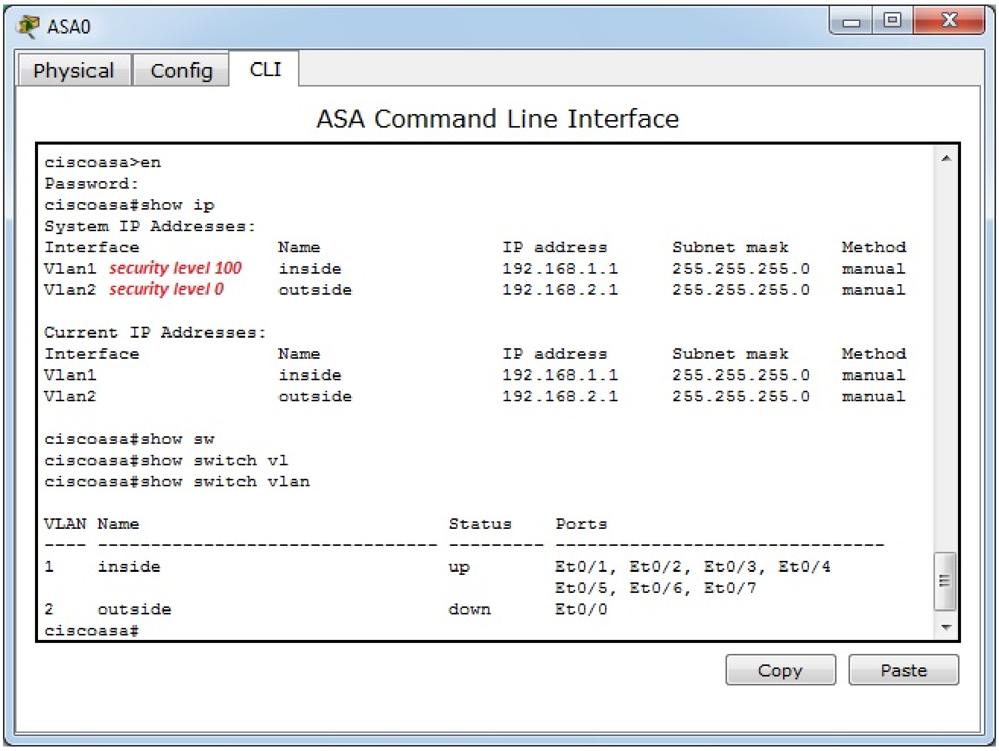


Lab instructions

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.



```
ciscoasa>en
Password:
ciscoasa#show ip
System IP Addresses:
Interface              Name                 IP address      Subnet mask     Method
Vlan1  security level 100 inside            192.168.1.1     255.255.255.0   manual
Vlan2  security level 0   outside           192.168.2.1     255.255.255.0   manual

Current IP Addresses:
Interface              Name                 IP address      Subnet mask     Method
Vlan1                  inside               192.168.1.1     255.255.255.0   manual
Vlan2                  outside              192.168.2.1     255.255.255.0   manual

ciscoasa#show sw
ciscoasa#show switch vl
ciscoasa#show switch vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    inside                           up        Et0/1, Et0/2, Et0/3, Et0/4
                                                Et0/5, Et0/6, Et0/7
2    outside                          down      Et0/0
ciscoasa#
```

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
```