Lab Report

Your Performance

Your Score: 6 of 6 (100%)
Elapsed Time: 7 minutes 33 seconds

Pass Status: Pass
Required Score: 100%

Task Summary

✓ Add an HTTP firewall rule that allows traffic from the WAN to the web server in the DMZ Hide Details

- ✚ From Zone: UNSECURE (WAN)
- ✚ To Zone: DMZ
- ✚ Service: HTTP
- ✚ Action: Allow Always
- ✚ Source Hosts: Any
- ✚ Internal IP Address: 172.16.2.100
- ✚ External IP Address: Dedicated WAN

✓ Add an HTTPS firewall rule that allows traffic from the WAN to the web server in the DMZ Hide Details

- ✚ From Zone: UNSECURE (WAN)
- ✚ To Zone: DMZ
- ✚ Service: HTTPS
- ✚ Action: Allow Always
- ✚ Source Hosts: Any
- ✚ Internal IP Address: 172.16.2.100
- ✚ External IP Address: Dedicated WAN

✓ Add a firewall rule to allow traffic from the LAN to the DMZ Hide Details

- ✚ From Zone: SECURE (LAN)
- ✚ To Zone: DMZ
- ✚ Service: Any
- ✚ Action: Allow Always

✓ Enable WAN security checks Hide Details

- ✚ Block Ping to WAN interface
- ✚ Enable Stealth Mode
- ✚ Block TCP Flood

✓ Enable LAN security checks Hide Details

- ✚ Block UDP Flood

✓ Enable ICSA settings Hide Details

- ✚ Block ICMP Notification
- ✚ Block Fragmented Packets
- ✚ Block Multicast Packets

Explanation

In this lab, you complete the following:

- Add an HTTP firewall rule that allows traffic from the WAN to the web server in the DMZ.
- Add an HTTPS firewall rule that allows traffic from the WAN to the web server in the DMZ. Use the following table for the HTTP and HTTPS rules:

Parameter	Setting
From Zone	UNSECURE (WAN)
To Zone	DMZ
Service	HTTP, HTTPS
Action	Allow Always
Source Hosts	Any
Internal IP Address	172.16.2.100
External IP Address	Dedicated WAN

- Add a firewall rule to allow traffic from the LAN to the DMZ.

Parameter	Setting
From Zone	SECURE (LAN)
To Zone	DMZ
Service	Any
Action	Allow Always
Source Hosts	Any
Destination Hosts	Any

- Enable all the firewall attack checks.

Complete this lab as follows:

1. Configure the firewall as follows:
    a. In the Security Appliance Configuration Utility, select **Firewall**.
    b. From the left pane, select **IPv4 Rules**.
    c. In the right pane, select **Add**.
    d. Modify the ***firewall rule parameters***; then click **Apply**.
    e. Repeat steps 1c–1d for each firewall rule.
2. Enable firewall attack checks as follows:
    a. From the left pane, select **Attacks**.
    b. Select all the ***WAN security checks***.
    c. Select all the ***LAN security checks***.
    d. Select all the ***ICSA settings***; then click **Apply**.