6 - Blocking Packet & Protocol Based Attacks

___1. Generate SYN Flood Traffic
- You will use a script on the client host in the Users_Net zone to send numerous TCP SYN packets to a target server in the Extranet zone.

1. `File Explorer > Scripts > Clear Firewall Logs`
    1. Press `Enter` to **start** the script. **Enter** again **when done.**
2. Double-click the icon for SYN Flood.
    1. Press `Enter` to **start** the script. **Enter** again **when done

Similar nmap command

```
nping --tcp-connect -p 80 --rate 10000 -c 50 -1 192.168.50.80
```

3. Open the PA-VM Firewall
4. `Monitor > Logs > Traffic`.
5. Search `( addr.src in 192.168.1.20 ) and ( app eq incomplete )` in the filter builder.
6. Apply Filter icon, and you should see incomplete connection attempts from `192.168.1.20` to `192.168.50.80` and port 80 in the Traffic log.
7. Navigate to `Monitor > Logs > Threat`. Nothing should be logged
    - Reason: No threat protections have been configured on the firewall.

___2. Configure and Test TCP SYN Flood Zone Protection
- A Zone Protection Profile can detect and block flood attacks, including a TCP SYN flood.

1. Create a new Zone Protection Profile.

- `Network > Network Profiles > Zone Protection > Add`

2. On the Flood Protection tab, configure the following. Click OK. *(NOTE: These settings are artificially low so that the firewall will implement Zone Protection during the testing part of the lab.*)
    - Parameters
        - Name: `User_Net_Profiles`
        - SYN: Select `Check box`
        - Action: `SYN Cookies`
        - Alarm Rate: `5`
        - Activate: `10`
        - Maximum: `20`
3. `Network > Zones > Users_net`
4. Select `User_Net_Profiles` under the `Zone Protection`
    1. `Enable Packet Buffer Protection`
5. Click the Commit button at the upper-right of the web interface.
6. Commit changes.
7. `File Explorer > Scripts > SYN Flood.
8. Press Enter to start the SYN Flood script. Allow the script to complete.
9. Open the PA-VM Firewall
10. `Monitor > Logs > Threat`. Click the X icon to clear any filters. You should see entries for TCP Flood threat recorded in the log.

___3. Reconnaissance Protection

In this section, you will modify the existing Zone Protection Profile to include protection against port
scans and ping sweeps.

1. `Network > Network Profiles > Zone Protection > Select User_Net_Profiles.`
2. Select the tab for Reconnaissance Protection. Modify the TCP Port Scan with the following settings. Click OK.

- Parameter Value
  - Enable: `Check box`
  - Action: `Block-IP`
  - Track By: `select source`
  - Duration: type `2`
  - Interval (sec): `2`
  - Threshold (events): `2`

3. Commit all changes
4. `File Explorer > Scripts > TCP Scan
5. Press Enter to start the TCP Scan.

NOTE: This run an nmap command to scan for open ports

```
nmap –v1 –Pn –T4 --max-retries 1 192.168.50.80
```

10. Open the PA-VM Firewall
11. Select `Monitor > Logs > Threat.` You should see several SCAN: TCP Port Scan records populated.
12. `Network > Network Profiles > Zone Protection > User_Net Profiles`.
13. Click the `Packet Based Attack Protection > IP Drop > Record Route`
14. **Commit Changes.**
15. `File Explorer > Scripts > IP Record Ping`

__This option in the IP header records the network path from the source host to the destination host. The Record Route option is not commonly used, and an attacker could use such information for network reconnaissance.
21. In the PA-VM Firewall: `Monitor > Logs > Threat`
1. Select You should now see an informational message with a threat named *IP Option Record Route.*

__To move forward in this lab, you will need to remove your Zone Protection Profile configuration to ensure that it does not interfere while you test a DoS Protection policy and profile

23. `Select Network > Zones > Users_Net`
24. In the Zone window,
    1. Zone Protection Profile: `None`.
25. Commit changes

__4. Concurrent Sessions on a Target Host and DoS Protection
- A DoS Protection policy and profile can detect when the number of concurrent sessions to a host has exceeded a specified limit.

2. `File Explorer > Scripts > Clear Firewall Logs.
3. Reopen the PA-VM and verify the logs have been cleared.
    1. `Monitor > Logs > Threat`

This script uses the XML API to clear the Threat, Traffic and URL Filtering log files. We are clearing the log files to make it easier to identify traffic and threats blocked by DoS Protection.

4. `File Explorer > Scripts > Concurrent Connections`

The exact syntax for this command is:

```
nmap --script http-slowloris --max-parallelism 10 192.168.50.80
```

11. In Palo Alto: `Monitor >Logs > Traffic`. Clear filters

__As the command execution progressed, you should see multiple web browsing log entries for traffic to multiple ports, but especially to port 80 and 443. The traffic was not blocked by any Security Profiles or Security policy rules.

12. `Monitor > Logs > Threat`.

    1. Notice there are no logs present.
13. Configure maximum concurrent sessions with DoS protection:
    1. `Objects > Security Profiles > DoS Protection > Add`
14. Configure the following. Click OK.
    - Parameter Value
        - Name: `protect-session-max`
        - Classified: Yes
            - Resources > Protections
                - Sessions: `check box`
                - Maximum: `Concurrent`
                - Sessions: `9`
15. `Polices > DoS Protection > Add`.
16. Configure the following.

- Parameter Value
    - General tab
        - Name: `internal-protection`
    - Source tab
        - Zone: `Users_Net`
    - Destination tab
        - Zone Select Extranet
    - Option/Protection tab Click it
        - Action: `Protect`
        - Classified: `Check box`
        - Profile: `protect-session-max`
        - Address: `destination-ip-only`

17. Verify the i`nternal-protection` rule is present in the DoS Protection policies.
18. Commit Changes.

19. `File Explorer > Scripts > Concurrent Connections`
20. Press Enter to start the Concurrent Connections script.
    The exact syntax for this command is:

```
nmap --script http-slowloris --max-parallelism 10 192.168.50.80
```

26. `Monitor > Logs > Threat`
    1. Notice the new Threats.
27. `Navigate to Objects > Security Profiles > DoS Protection`.
    `protect-session-max` to edit the profile.
28. Several columns have been hidden in this example.
    You should see Session Limit Event entries in the Threat log because the number of concurrent connection requests to the protected host has exceeded the configured session maximum limit.
29. DoS Protection Profile window > Resources Protection tab > Deselect Sessions
30. `Network > Network Profiles > Zone Protection.`
    1. Click `User_Net_Profile`.
31. On the Flood Protection tab, configure the following.
    - Parameter Value
      - SYN: `Check box`
      - Action SYN: `Cookies`
      - Alarm Rate: `1000`
      - Activate: `1100`
      - Maximum: `1300`

___The threshold values here are configured with high values to ensure that the lower DoS Protection Profile thresholds are reached first during testing in a later lab section.

31. Reconnaissance Protection tab.

    1. Disable `TCP Port Scan`
32. `Network > Zones > Users_Net zone`
33. Zone Protection Profile menu
34. select `User_Net_Profiles`.
35. `Objects > Security Profiles > DoS Protection`.
    1. `protect-session-max`.
36. In the DoS Protection Profile window, configure the following. Click OK.
    - Parameter Value
        - Flood Protection tab
            - SYN Flood: `Check box`
            - Action SYN: `Cookies`
            - Alarm Rate: `5`
            - Activate Rate: `10`
            - Max Rate: `20`
37. Commit All changes
38. `File Explorer > Scripts > Concurrent Connections`
    The exact syntax for this command is:

```
nmap --script http-slowloris --max-parallelism 10 192.168.50.80
```

39. Reopen the PA-VM Firewall by clicking on the Chromium tab in the taskbar on the client desktop.
40. `Monitor > Logs > Threat.` Notice the new Threats.

Several columns have been hidden in this example.
You should see TCP Flood Threat log entries because the number of connection requests to the target host has exceeded the configured flood threshold maximum in the DoS Protection Profile. The flood

threshold in the DoS Protection Profile is lower than the Zone Protection Profile, so it should have been triggered first.