DefensePro
Version 8.x

Training Lab Manual
Configure Connection Limit Protection

Table of Contents

Overview

Connection Limits filter out the attacks that breach the set threshold.

The DefensePro counts the number of TCP connections, or UDP sessions, opened for traffic that matches a Connection Limit policy attack definition.

Any session or connection over the threshold in the configuration of the DefensePro will be dropped, reported or suspended, depending on configuration.

Configure Connection Limit

In this lab we configure a HTTP connection limit to allow only two http connections per second per source.

1. Select the DefensePro **Configuration → Protections → Connection Limit Profiles → Connection Limit Protection** perspective.
    a. Click **+** to **add** a new Protection.
    b. In **Add Connection Limit Protection** tab use the following information:
       Protection Name: **HTTPLimit**
    c. Application Port Group **http**
    d. Protocol **TCP**
    e. Threashold: **2**
    f. Tracking Type **Source Count**
    g. Click **Submit** the to add a new protection
2. Select the **Configuration → Protections → Connection Limit Profiles**.
    a. Click **+** to **add** a new Profile
    b. Name it **TeamXX** (whereXX are your initials) and click on + to add the protection.
    c. In the **Add Connection Limit Protection** window select the Protection Name **HTTPLimit** and click **Submit**
3. Click **Close** to close the Add New Connection Limit Profile window
4. In the **Protection Policies** tab double-click your protection policy to edit.
5. In the **Profiles → Connection Limit Profile** section select the your connection limit profile
6. Click **Submit** to submit the change
7. Click on **Update Policies Required**

Test the Configuration

Use Raptor to send HTTP Flood Attack, which will trigger the connection limit

1. Access **Attacker-PC Raptor** main menu → select **Services Attacks → HTTP → Cracking**.
2. Add as **HTTP Server Address**: ***27.1.31.100***
3. Use **/protected/** as destination URL
4. Use Vision to View the Attack. Select the **Analytics AMS → DefensePro Attacks** perspective.
5. Click on an attack to open Attack Details.
6. Select **Analytics AMS → DefensePRo Monitoring** and observe the **Connection Rate**.

Configure Connection Limit With Suspend Action

In this lab we configure a HTTP connection limit to allow only ten http connections per source per second to the same server and suspend the souce in case of too many connections.

1. Select the DefensePro **Configuration → Protections → Connection Limit Profiles → Connection Limit Protection** perspective.
    a. Double-Click on the existing Limit
    b. In **Edit Connection Limit Protection** tab change the following information:

Threshold	**10**
c. Tracking Type	**Source and Destination Count**
d. Suspend Action	**Source IP + Destination Port**

    e. Click **Submit** to save the changes
2. Click on **Update Policies Required**

Test the Configuration

Use Raptor to send HTTP Flood Attack, which will trigger the connection limit

1. Access **Attacker-PC Raptor** main menu > select **Service Attacks > HTTP > Cracking**.
2. Add as **HTTP Server Address**: ***27.1.31.100***
3. Use **/protected/** as destination URL
4. Use Vision to View the Attack. Select the **Analytics AMS → DefensePro Attacks** perspective.
5. Click on an attack to open Attack Details.
6. Select **Analytics AMS → DefensePRo Monitoring** and observe the **Connection Rate**.
7. Since we use now the suspend action, we can verify if the source IP was suspended
8. Select the DefensePro **Monitoring → Networking → Suspend Table** perspective and you should see the source IP listed in the Suspend Table.
9. After the attack ist stopped, you can see in the suspend table if the source IP is still listed and after the expiration time the source IP should not reenter this list, since we stop the attack.

Configure Concurrent Connection Limit

In this lab we configure a HTTP connection limit to allow only two http connections per second per source.

8. Select the **Configuration → Protections → Connection Limit Profiles → Connection Limit Protection** perspective.
    a. Double-Click on the existing Limit
    b. In **Edit Connection Limit Protection** tab use the following information:

c. Protection Type:	**Concurrent Connections**
d. Threashold:	**2**
e. Tracking Type	**Source Count**

    f. Click **Submit**

9. Click on **Update Policies Required**

Test the Configuration

Use Raptor to send HTTP Flood Attack, which will trigger the connection limit

7. Access **Attacker-PC Raptor** main menu → select **Services Attacks → HTTP → Cracking**.
8. Add as **HTTP Server Address**: ***27.1.31.100***
9. Use **/protected/** as destination URL
10. Use Vision to View the Attack. Select the **Analytics AMS → DefensePro Attacks** perspective.
11. Click on an attack to open Attack Details.
12. Select **Analytics AMS → DefensePro Monitoring** and observe the **Concurrent Connections**.

Export and save configuration file as **dp8-ConnectionLimitLab-config.txt**.

10.

For questions, contact **training@Radware.com**