



DefensePro X
Version 10.x

Training Lab Manual

Configure Connection Limit Protection



Table of Contents

| | |
|--|---|
| OVERVIEW | 3 |
| CONFIGURE CONNECTION LIMIT | 3 |
| TEST THE CONFIGURATION | 3 |
| CONFIGURE CONNECTION LIMIT WITH SUSPEND ACTION | 5 |
| TEST THE CONFIGURATION | 5 |
| CONFIGURE CONCURRENT CONNECTION LIMIT | 6 |
| TEST THE CONFIGURATION | 6 |
| CONFIGURE PACKETS PER SECOND LIMIT | 7 |
| TEST THE CONFIGURATION | 7 |

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. Before starting this lab, be sure to stop JMeter app on legit client.

1. Select the Cyber Controller **Security Operations** → **Security Settings** perspective.
2. Edit the **TeamXX** policy.
3. Enable **Connection Limit**.
4. Click on “+ Add New”
 - a. Protection Name: **http_limit**
 - b. Protection Type: **Connections Per Second**
 - c. Application Port Group: **http**
 - d. Protocol: **TCP**
 - e. Threshold: **2 CPS**
 - f. Tracking Type: **Source Count**
 - g. Action: **Drop**
 - h. Packet Reporting: **Check**
 - i. **Submit**
5. Click **Submit** to apply the policy.

Test the Configuration

Make sure you stop legitimate client jMeter before you start.

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 Cyber Controller to View the Attack. Select the **Realtime-Monitoring** dashboard and check the **Detection Events**.

- The detection events show up as category DOS with the event name starting with “CPS – http_limit”

Detection Events 18

| Action | Policy Name | Status | Category | Event Name | Event Destination | Updated Time | Duration | Detector Name (Type) | Info |
|--------|-------------|------------|----------|------------------------|-------------------|---------------------|----------|--------------------------|------|
| Drop | TeamXX | Started | DoS | CPS - http_limit_Te... | 27.1.31.100 | 14.10.2024 08:20:14 | 00:00:06 | VDefenseProX Defense Pro | |
| Drop | TeamXX | Terminated | DoS | CPS - http_limit_Te... | 27.1.31.100 | 14.10.2024 08:20:08 | 00:00:00 | VDefenseProX Defense Pro | |
| Drop | TeamXX | Terminated | DoS | CPS - http_limit_Te... | 27.1.31.100 | 14.10.2024 08:20:08 | 00:00:00 | VDefenseProX Defense Pro | |

- Click on an attack to open Attack Details.

DoS, CPS - http_limit_TeamXX

Protected Object/Policy
TeamXX

Destination Address
27.1.31.100

Start Time
14.10.2024 08:20:23

Duration
00:00:00

Attack Name
CPS - http_limit_TeamXX

Attack Details

Attack Analytics

PCAP

Sampled Data

Additional Attack Attributes

| | | | | | | |
|----------------|----------------------|--------------------------|------------------------|-----------------------------|--------------------|-------------------------|
| Risk Medium | Radware ID 450000 | Direction (In/Out) In | Action Type Drop | Attack ID 303-1728480628 | Physical Port 1 | Total Packet Count 4 |
| VLAN N/A | MPLS RD N/A | Source Port Multiple | Packet Type Regular | | | |

Characteristics

| | | | |
|--|--|----------------------------|-------------------------------|
| Current Packet Rate [Packets/Sec] 0 | Average Packet Rate [Packets/Sec] 4 | Attack Duration 0.0 Sec | Protected Host 27.1.31.100 |
|--|--|----------------------------|-------------------------------|

- You can also review the Attack Analytics, which is available after 2 minutes.

Configure Connection Limit With Suspend Action

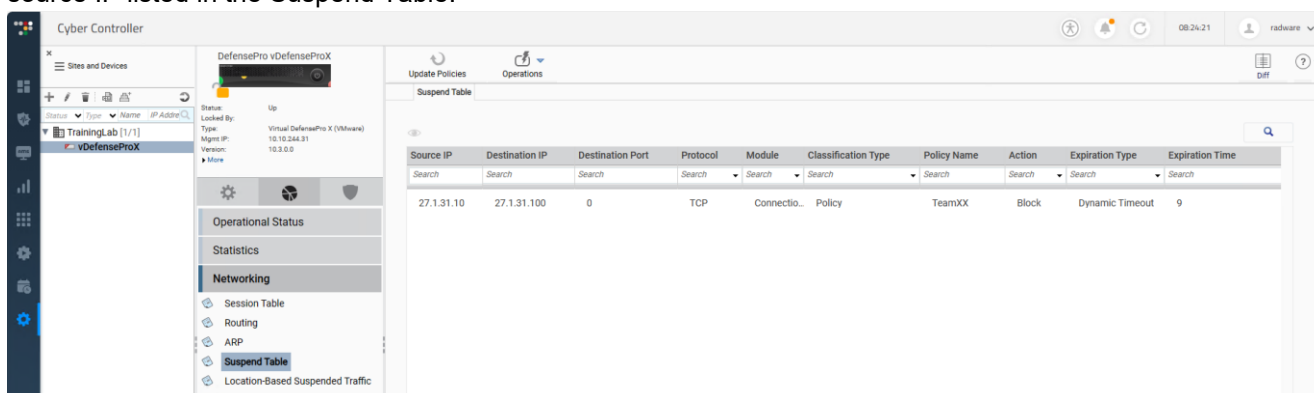
In this lab we configure a HTTP connection limit to allow only ten http connections per source per second to the same server and suspend the source in case of too many connections.

1. Select the Cyber Controller **Security Operations** → **Security Settings** perspective.
2. Edit the **TeamXX** policy **Connection Limit Protection**.
 - a. Double-Click on the existing Limit
 - b. In **Edit Connection Limit Protection** tab change the following information:
 - Threshold **5**
 - Tracking Type **Source and Destination Count**
 - Suspend Action **Source IP + Destination Port**
 - e. Click **Submit** to save the changes
3. Click on **Submit** to push the policy changes

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 Cyber Controller to View the Attack. Select the **Realtime-Monitoring** dashboard and check the **Detection Events**.
5. Since we use now the suspend action, we can verify if the source IP was suspended
6. Select the DefenseProX **Monitoring** → **Networking** → **Suspend Table** perspective and you should see the source IP listed in the Suspend Table.



| Source IP | Destination IP | Destination Port | Protocol | Module | Classification Type | Policy Name | Action | Expiration Type | Expiration Time |
|------------|----------------|------------------|----------|------------|---------------------|-------------|--------|-----------------|-----------------|
| 27.1.31.10 | 27.1.31.100 | 0 | TCP | Connection | Policy | TeamXX | Block | Dynamic Timeout | 9 |

7. If you run the attack more often, you will see the time the entry is suspended will be increased.
8. After the attack is 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. Make sure the suspend table is empty before you continue.

Configure Concurrent Connection Limit

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

1. Select the Cyber Controller **Security Operations** → **Security Settings** perspective.
2. Edit the **TeamXX** policy **Connection Limit Protection**.
 - a. Double-Click on the existing Limit
 - b. In **Edit Connection Limit Protection** tab use the following information:
 - c. Protection Type: **Concurrent Connections**
 - d. Threshold: **2**
 - e. Tracking Type **Source Count**
 - f. Click **Submit**
3. Click on **Submit** to push the policy changes

Test the Configuration

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

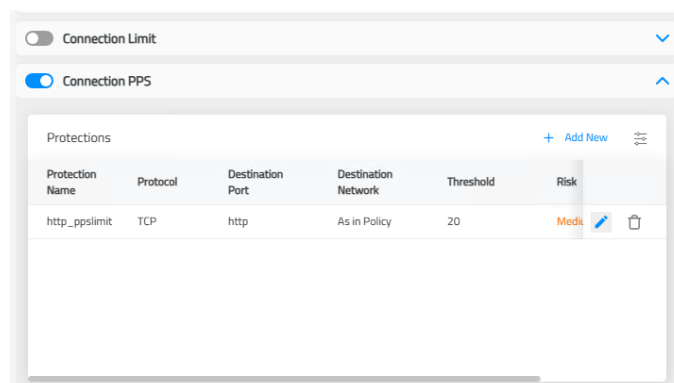
1. Access **Attacker-PC Raptor** main menu → select **Services Attacks** → **HTTP** → **Cracking**.
2. Add as **HTTP Server Address: 27.1.31.100**
3. Use **/protected/** as destination URL
4. Use Cyber Controller to View the Attack. Select the **Realtime-Monitoring** dashboard and check the **Detection Events**.
5. Click on an attack to open Attack Details.

Configure Packets Per Second Limit

In this lab we configure a HTTP packets per second limit to allow only 20 http packets per second per source.

1. Select the Cyber Controller **Security Operations** → **Security Settings** perspective.
2. Edit the **TeamXX** policy.
3. Disable **Connection Limit** protection
4. Enable **Connection PPS** protection
5. Click on **+ Add New**

- a. Protection Name: **http_ppslimit**
- b. Protocol: **TCP**
- c. Destination Port: **http**
- d. Destination Network: **As in Policy**
- e. Threshold (pps): **20**
- f. Risk: **Medium**
- g. Action: **Block and Report**
- h. Click **Submit**



6. Click on **Submit** to push the policy changes

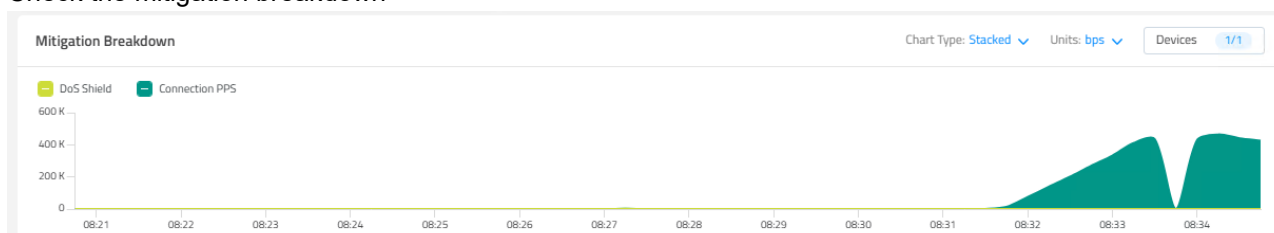
Test the Configuration

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

1. Access **Attacker-PC Raptor** main menu → select **Services Attacks** → **HTTP** → **Flooding**.
2. Add as **HTTP Server Address: 27.1.31.100**
3. Use **/index.html** as destination URL
4. Use Cyber Controller to View the Attack. Select the **Realtime-Monitoring** dashboard and check the **Detection Events**.
5. Click on an attack to open Attack Details.

| Detection Events 24 | | | | | | | | | |
|----------------------------------|-------------|---------|---------------|---------------|-------------------|---------------------|----------|--------------------------|------|
| Action | Policy Name | Status | Category | Event Name | Event Destination | Updated Time | Duration | Detector Name (Type) | Info |
| Drop | TeamXX | Ongoing | ConnectionPPS | http_ppslimit | 27.1.31.100 | 14.10.2024 08:33:44 | 00:01:50 | VDefenseProX Defense Pro | |

6. Check the mitigation breakdown



7. Make sure you stop the attack before you continue.

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



For questions, contact training@Radware.com

© 2019 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are property of their respective owners.