DefensePro X
Version 10.x

Training Lab Manual
Configure Traffic Filters

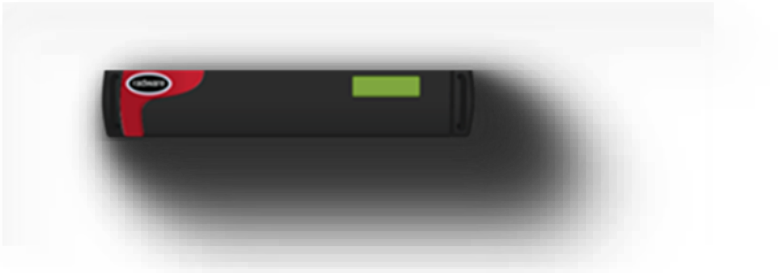


Table of Contents

Overview

Traffic Filters enable control over processing traffic through DefensePro X at the policy level.

Traffic Filters complement the DefensePro X protections with additional manual control. With Traffic Filters, you can block or rate-limit traffic that matches specified valued -- or traffic not matching specified values. Additionally, Traffic Filters allow you to define specific network addresses or port values withinthe policy as the Filter Criteria.

Configure Limit Traffic per Second

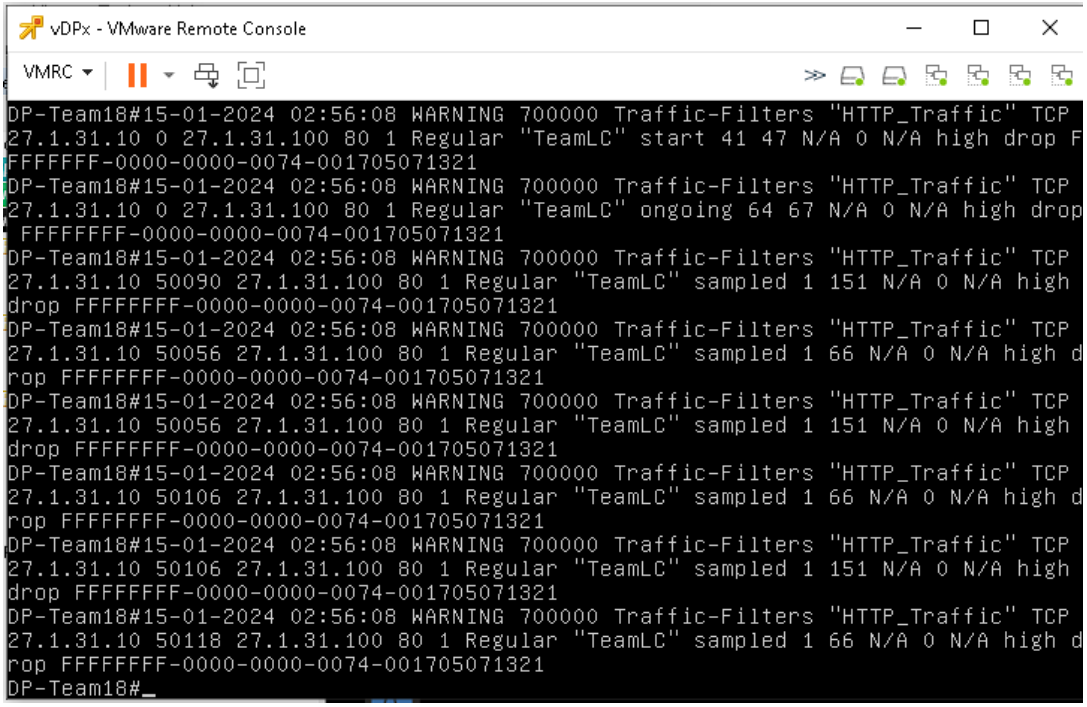
1. In **Cyber Controller**, select **Security Operations → Security Settings**. Select and edit the TeamXX policy.
2. Enable **Traffic Filters**:
3. Click **+ Add New** to add a new filter s follows:
    - Filter Name: **HTTP_Traffic**
    - Apply Traffic Filter To: **Matching Traffic**
    - Source Network: **As in Policy**
    - Destination Network: **As in Policy**
    - Protocol: **TCP**
    - Source port: **any**
    - Destination port: **http**
    - Threshold Units: **Kbits Per Second**
    - Threshold: **300**
    - Tracking Mode: **Per Source and Destination**
    - Packet Reporting: **Check**

4. Click **Submit** button to add the filter
5. Click **Submit** to apply the policy.

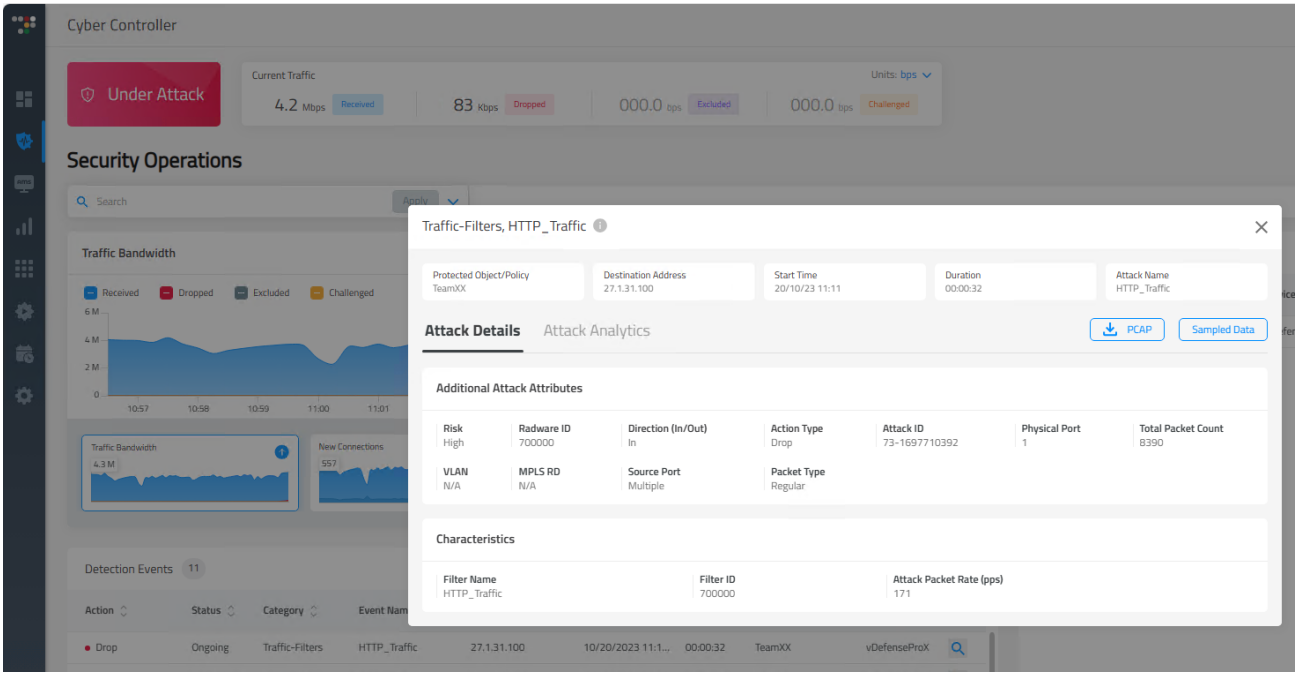
Test the Configuration

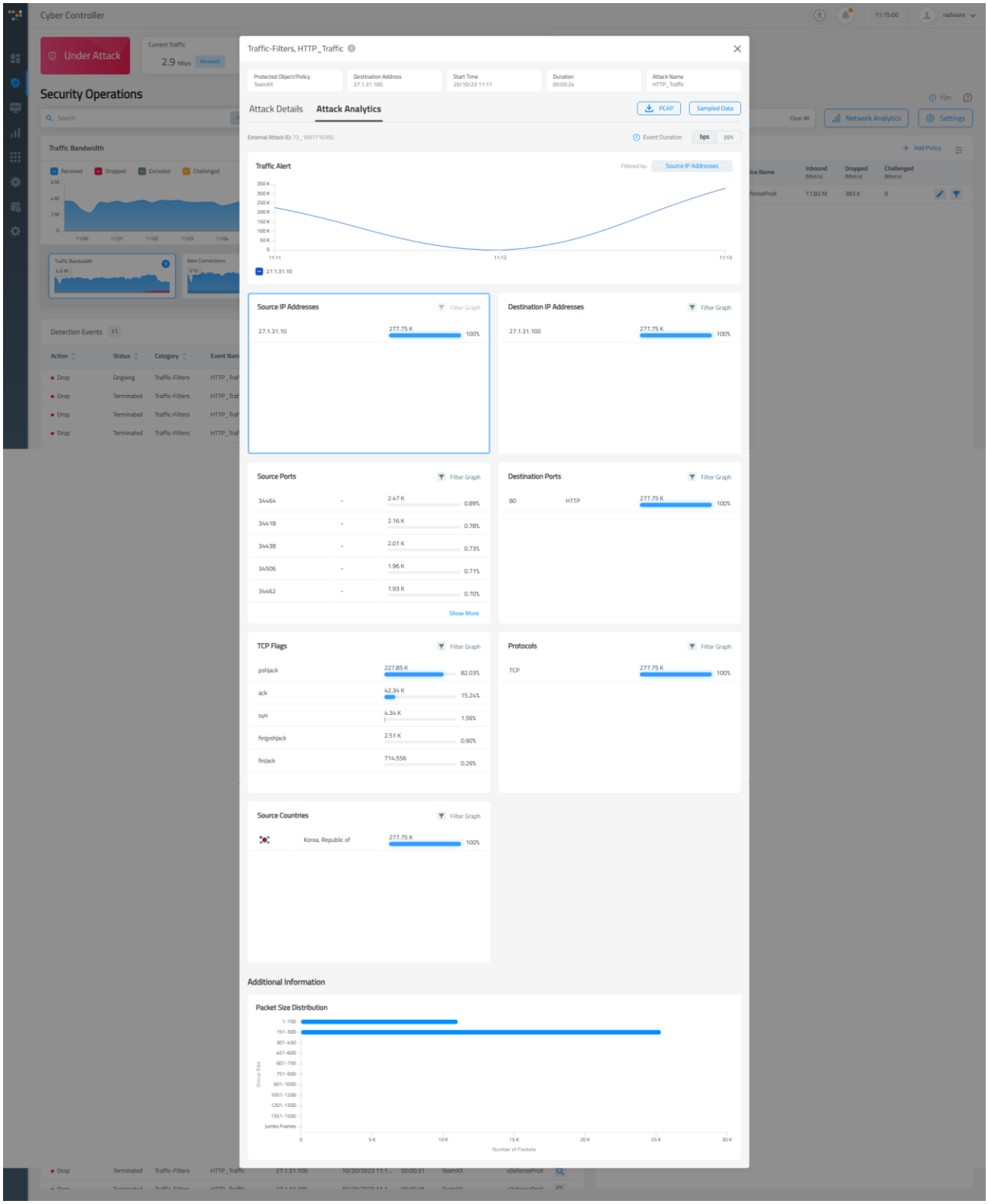
Use Raptor to send **Services Attacks → HTTP → Flooding**

1. Verify **Destination IP** address: ***27.1.31.100*** Page to flood: **/index.html**
2. After the attack begins, you should receive a CLI message that traffic filter was matching



3. Check syslog server (3CD) to see traps being sent by the DefensePro X.
4. Use Cyber Controller to View Traffic Filter Attack. Select the **Security Operations → Real-Time Monitoring**.
5. Select the Traffic Filter event in **Detection Events** section. Click on the **Info** incon and observe.





6. At Raptor **Stop** the attack.

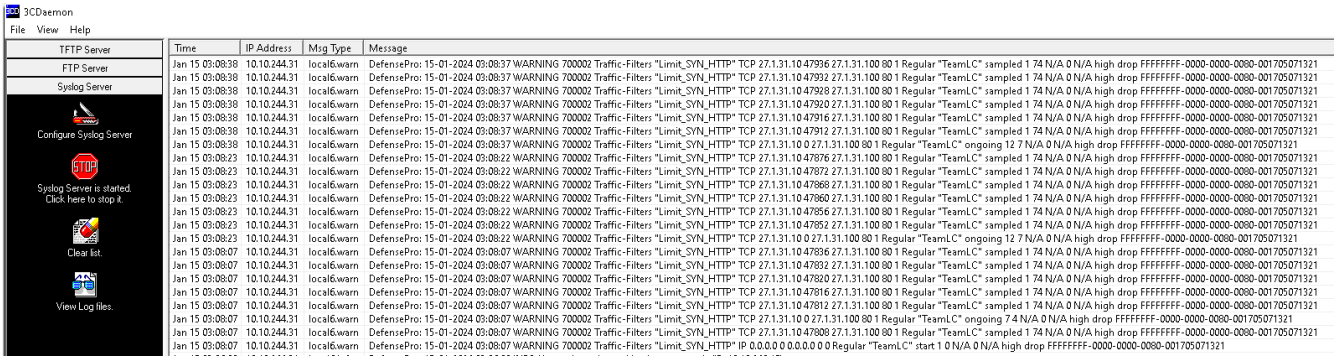
Configure Limit SYN Packets per Second

1. In **Cyber Controller**, select **Security Operations → Security Settings**. Select and edit the TeamXX policy.
2. At **Traffic Filters**:
3. Click **+ Add New** to add a new filter s follows:
    a. **Filter** Name: **Limit_SYN_HTTP**
    b. Apply Traffic Filter To: **Matching Traffic**
    c. Source Network: **As in Policy**
    d. Destination Network: **As in Policy**
    e. Protocol: **TCP**
    f. Source port: **any**
    g. Destination port: **http**
    h. TCP Flags - SYN: **Checked**
    i. Threshold Units: **Packets Per Second**
    j. Threshold: **2**
    k. Tracking Mode: **Per Source and Destination**
    l. Packet Reporting: **Check**

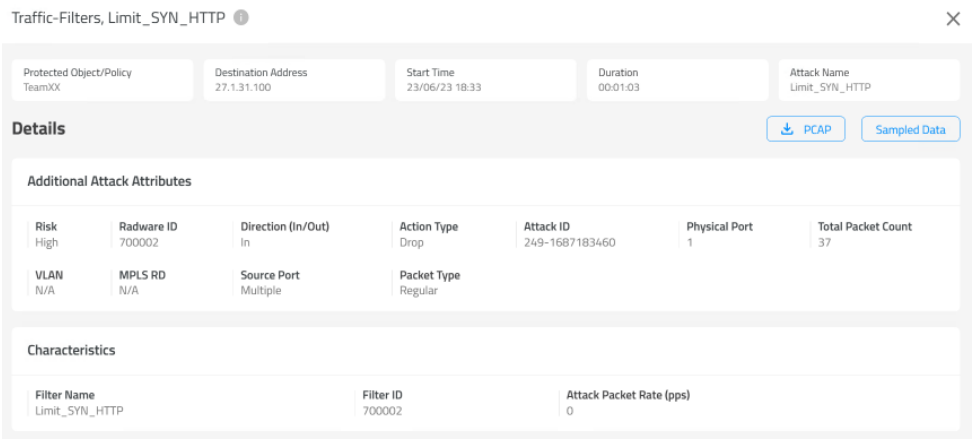
4. Click **Submit** button to add the filter
5. Click **Submit** to apply the policy.

Test the Configuration

1. Go to **Legitimate Client** and stop the **jMeter** by pressing the STOP icon. Filter limits all traffic, not only attack traffic.
2. Use Raptor to send **Service Attacks → HTTP → Cracking**
3. Verify **Destination IP** address: ***27.1.31.100.*** Use URL **/protected/** for the destination.
4. After the attack begins, you should receive a CLI message that traffic filter was matching
5. Check syslog server (3CD) to see traps being sent by the DefensePro X.



6. Use Cyber Controller to View Traffic Filter Attack. Select the **Security Operations → Real-Time Monitoring**.
7. Observe **Current Status** shows **Under Attack**. Observe **Traffic Bandwidth**, **Connection Rate**, and **Concurrent Connections**. NOTE: This is a low intensity and short period attack. You might need to repeat it a few times. It might not show being Under Attack but drill down to the policy and protection.
8. Select your event in the **Detection Events** section and see information on it.



9. At Raptor **stop** the attack.
10. **Export** and save configuration file as **dpx-TFLab_config.txt**.
11. Disable the Traffic filter protection from your policy.
12. At **Legitimate Client** start the **jMeter**

For questions, contact training@Radware.com