



DefensePro X
Version 10.x

Training Lab Manual Configure Traffic Filters



Table of Contents

OVERVIEW	3
CONFIGURE LIMIT TRAFFIC PER SECOND	3
TEST THE CONFIGURATION	4
CONFIGURE LIMIT SYN PACKETS PER SECOND	6
TEST THE CONFIGURATION	7

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 values -- or traffic not matching specified values. Additionally, Traffic Filters allow you to define specific network addresses or port values within the 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 as 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

```

vDPx - VMware Remote Console
VMRC | [Icons] [Buttons]
DP-Team18#15-01-2024 02:56:08 WARNING 700000 Traffic-Filters "HTTP_Traffic" TCP
27.1.31.10 0 27.1.31.100 80 1 Regular "TeamLC" start 41 47 N/A 0 N/A high drop F
FFFFFFFF-0000-0000-0074-001705071321
DP-Team18#15-01-2024 02:56:08 WARNING 700000 Traffic-Filters "HTTP_Traffic" TCP
27.1.31.10 0 27.1.31.100 80 1 Regular "TeamLC" ongoing 64 67 N/A 0 N/A high drop
FFFFFFFF-0000-0000-0074-001705071321
DP-Team18#15-01-2024 02:56:08 WARNING 700000 Traffic-Filters "HTTP_Traffic" TCP
27.1.31.10 50090 27.1.31.100 80 1 Regular "TeamLC" sampled 1 151 N/A 0 N/A high
drop FFFFFFFFF-0000-0000-0074-001705071321
DP-Team18#15-01-2024 02:56:08 WARNING 700000 Traffic-Filters "HTTP_Traffic" TCP
27.1.31.10 50056 27.1.31.100 80 1 Regular "TeamLC" sampled 1 66 N/A 0 N/A high d
rop FFFFFFFFF-0000-0000-0074-001705071321
DP-Team18#15-01-2024 02:56:08 WARNING 700000 Traffic-Filters "HTTP_Traffic" TCP
27.1.31.10 50056 27.1.31.100 80 1 Regular "TeamLC" sampled 1 151 N/A 0 N/A high
drop FFFFFFFFF-0000-0000-0074-001705071321
DP-Team18#15-01-2024 02:56:08 WARNING 700000 Traffic-Filters "HTTP_Traffic" TCP
27.1.31.10 50106 27.1.31.100 80 1 Regular "TeamLC" sampled 1 66 N/A 0 N/A high d
rop FFFFFFFFF-0000-0000-0074-001705071321
DP-Team18#15-01-2024 02:56:08 WARNING 700000 Traffic-Filters "HTTP_Traffic" TCP
27.1.31.10 50106 27.1.31.100 80 1 Regular "TeamLC" sampled 1 151 N/A 0 N/A high
drop FFFFFFFFF-0000-0000-0074-001705071321
DP-Team18#15-01-2024 02:56:08 WARNING 700000 Traffic-Filters "HTTP_Traffic" TCP
27.1.31.10 50118 27.1.31.100 80 1 Regular "TeamLC" sampled 1 66 N/A 0 N/A high d
rop FFFFFFFFF-0000-0000-0074-001705071321
DP-Team18#_
  
```

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** icon and observe.

Cyber Controller

Under Attack

Current Traffic: 4.2 Mbps Received, 83 kbps Dropped, 000.0 kbps Excluded, 000.0 kbps Challenged

Security Operations

Traffic Bandwidth: Received, Dropped, Excluded, Challenged

Traffic-Filters, HTTP_Traffic

Protected Object/Policy: TeamXX, Destination Address: 27.1.31.100, Start Time: 20/10/23 11:11, Duration: 00:00:32, Attack Name: HTTP_Traffic

Attack Details | Attack Analytics

Additional Attack Attributes

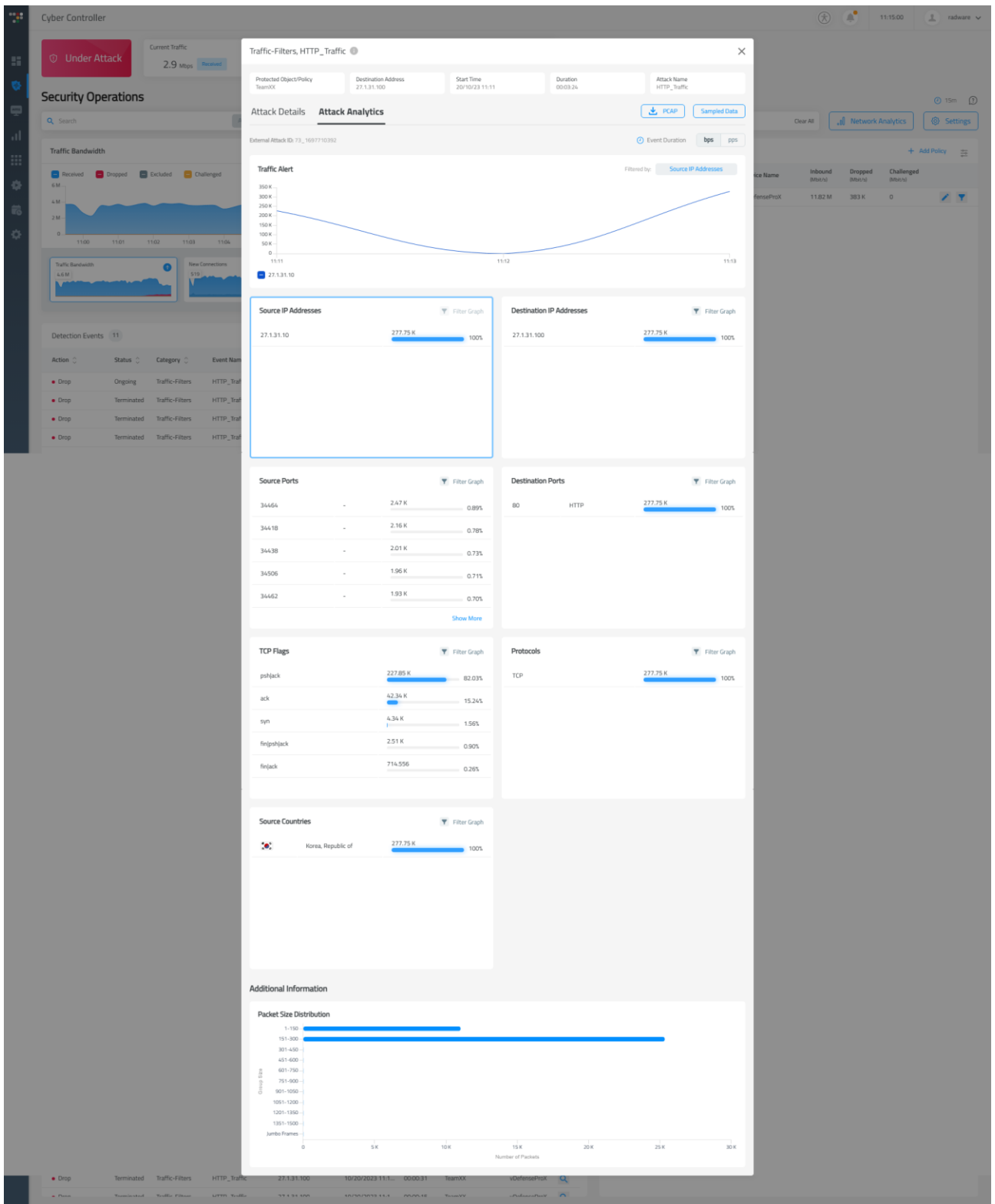
Risk: High	Radware ID: 700000	Direction (In/Out): In	Action Type: Drop	Attack ID: 73-1697710392	Physical Port: 1	Total Packet Count: 8390
VLAN: N/A	MPLS RD: N/A	Source Port: Multiple	Packet Type: Regular			

Characteristics

Filter Name: HTTP_Traffic	Filter ID: 700000	Attack Packet Rate (pps): 171
---------------------------	-------------------	-------------------------------

Detection Events: 11

Action: Drop, Status: Ongoing, Category: Traffic-Filters, Event Name: HTTP_Traffic, 27.1.31.100, 10/20/2023 11:11, 00:00:32, TeamXX, vDefenseProX



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.

[illegible]

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.

Traffic-Filters, Limit_SYN_HTTP

Protected Object/Policy
Team0X

Destination Address
27.1.31.100

Start Time
23/06/23 18:33

Duration
00:01:03

Attack Name
Limit_SYN_HTTP

Details

[PCAP](#)
[Sampled Data](#)

Additional Attack Attributes

Risk High	Raidware ID 700002	Direction (In/Out) In	Action Type Drop	Attack ID 249-1687183460	Physical Port 1	Total Packet Count 37
VLAN N/A	MPLS RD N/A	Source Port Multiple	Packet Type Regular			

Characteristics

Filter Name Limit_SYN_HTTP	Filter ID 700002	Attack Packet Rate (pps) 0
-------------------------------	---------------------	-------------------------------

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

© 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.