

Training Lab Manual Configure Traffic Filters



Table of Contents

OVERVIEW.....	3
CONFIGURE LIMIT TRAFFIC PER SECOND	3
TEST THE CONFIGURATION	3
CONFIGURE LIMIT SYN PACKETS PER SECOND	4
TEST THE CONFIGURATION	5

Overview

Traffic Filters enable control over processing traffic through DefensePro at the policy level. Traffic Filters complement the DefensePro 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 **APSolute Vision**, select **CONFIGURATION** perspective. Select **Protection** → **Traffic Filters Profiles** on the navigation tree.
2. In the Traffic Filters Profiles:
 - a. Click **+** to add a new profile as follows:
 - b. Profile Name: **TeamXX** (where XX are your initials)
 - c. Profile Action: **Block and Report**
 - d. Click **+** to add a new filter to the new profile as follows:

Parameters	
Enabled	CHECKED
Filter Name	HTTP_Traffic
Filter Mode	Matching Traffic
Apply Traffic Filter To	
Filter Mode	As in Profile
Filter Action	
Basic Filter Criteria	
Source/Destination Network	As in Policy
Basic Filter Criteria	
Source Port	Any
Basic Filter Criteria	
Destination Port	http
Basic Filter Criteria	
Protocol	TCP
Filter Threshold	
Threshold Units	Kbits per Second
Filter Threshold	
Threshold	800
Filter Threshold	
Tracking Mode	Per Source and Destination Pair

3. Click **Submit** button to add the filter
4. Click **Close** to close the profile.
5. Add the new profile to your protection policy, **HINT: Make sure the Connection Limit Profile is not selected!**
6. Click the **Update Policies Required** button to apply the changes.

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.
4. Use Vision to View Traffic Filter Attack. Select the **Analytics AMS → DefensePro Monitoring**.
5. Observe **Current Status** shows **Under Attack**. Observe **Traffic Bandwidth**, **Connection Rate**, and **Concurrent Connections**.
6. Select your policy in the **Protection Policies** section and click on it.
7. Observe **Attack Traffic and Active Protections**
8. In **Protections** section select **Traffic Filters**
9. Select a HTTP_Traffic traffic filter and observe details.
10. At Raptor **Stop** the attack.

Configure Limit SYN Packets per Second

1. In **APSolute Vision**, select DefensePro **Configuration** perspective. Select **Protection → Traffic Filters Profiles** on the navigation tree.
2. In the Traffic Filters Profiles:
3. Edit the existing profile and Click **+** to add a new filter to the profile as follows:

Parameters	
Enabled	CHECKED
Filter Name	Limit_SYN_HTTP
Filter Mode	Matching Traffic
Apply the Traffic Filter To	
Filter Mode	As in Profile
Filter Action	
Basic Filter Criteria	
Source/Destination Network	As in Policy
Basic Filter Criteria	
Source Port	Any
Basic Filter Criteria	
Destination Port	http
Basic Filter Criteria	
Protocol	TCP
Advanced Filter Criteria	
TCP Flags	SYN checked
Filter Threshold	
Threshold Units	Packets per Second
Filter Threshold	
Threshold	2
Filter Threshold	
Tracking Mode	Per Source and Destination Pair

4. Click **Submit** button to add the filter

5. Click **Close** to close the profile.
6. Click the **Update Policies Required** button to apply the changes.

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.
6. Use Vision to View Traffic Filter Attack. Select the **ANALYTICS AMS → DefensePro 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 policy in the **Protection Policies** section and click on it.
9. Observe **Attack Traffic and Active Protections**
10. In **Protections** section select **Traffic Filters**
11. Select an ongoing traffic filter and observe details.
12. At Raptor **stop** the attack.
13. At **Legitimate Client** start the **jMeter**.
14. Remove the Traffic filter protection from your policy.
15. **Export** and save configuration file as **dp8-TFLab_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.