



DefensePro X
Version 10.x

Training Lab Manual Configure Signature Protection



Table of Contents

OVERVIEW.....	3
REMOVE THE TRAFFIC FILTER PROFILE FROM YOUR PROTECTION POLICY.....	3
UPDATE THE SIGNATURE DATABASE AMND ATTACH DESCRIPTION	3
CONFIGURE SIGNATURE PROTECTION.....	5
TEST THE CONFIGURATION	7

Overview

Radware DefensePro X can be configured to protect against known attacks using the most accurate and effective mitigation method in the industry using Signature Protection.

Signature Protection is designed to mitigate known application-level and operating system attacks; it secures networked applications, users, and server resources.

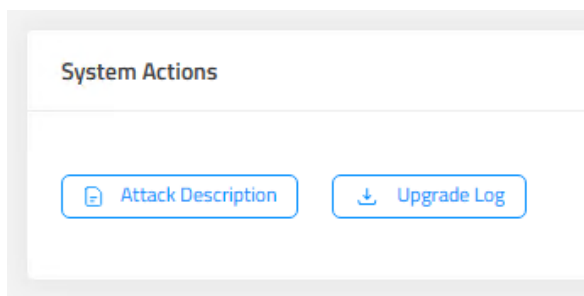
Remove The Traffic Filter Profile From Your Protection Policy

1. **Security Operations** → **Security Settings** select and edit your policy.
2. **Disable** the **Traffic Filters** protection.
3. Press **Submit** to update the policy.

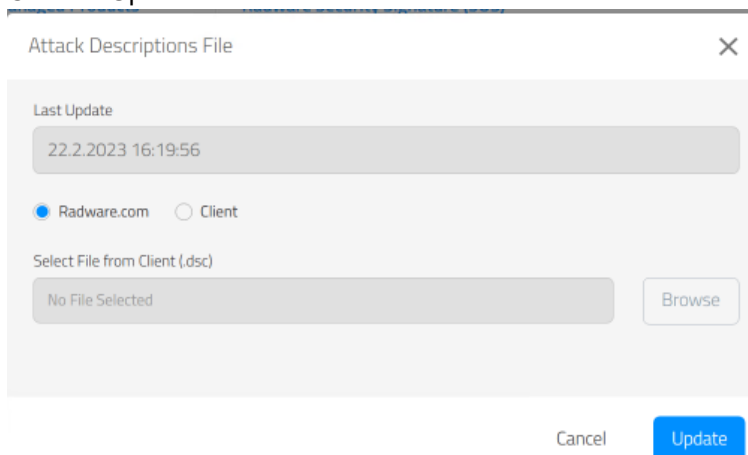
Update the Signature Database and Attack Description

Before we start with the signature protection configuration, we want to make sure to use the latest signatures. For this feature the device has to have the SUS service subscription.

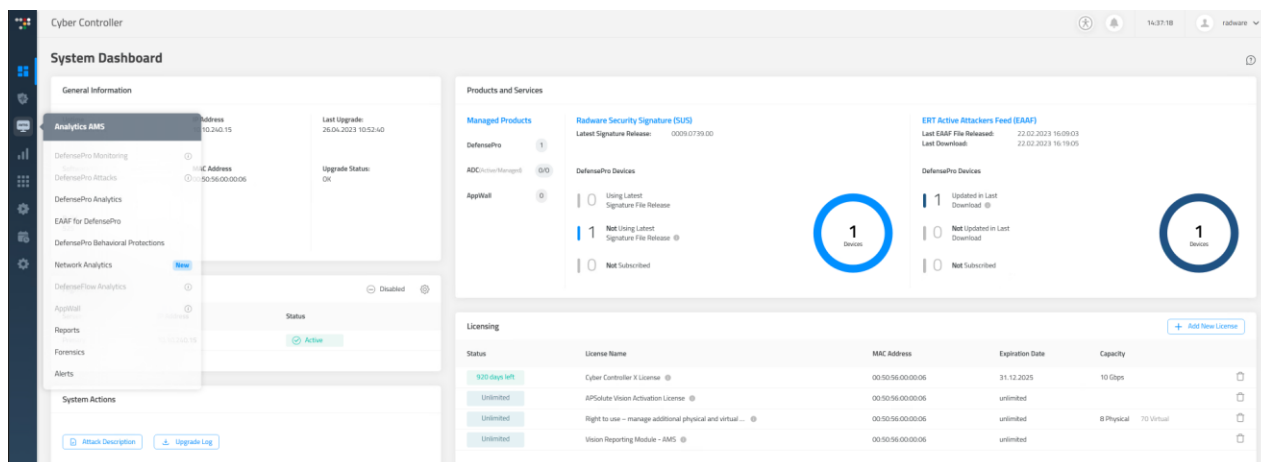
1. Go to Cyber Controller **System Dashboard**.
2. Under System Actions click on **Attack Description**



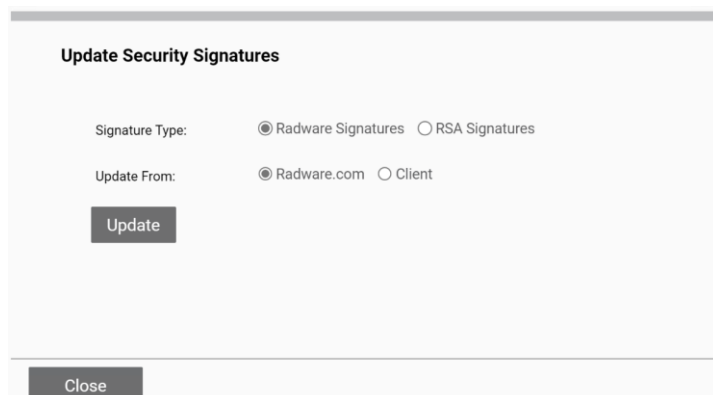
3. Click on Update.



4. Select the **Cyber Controller System Dashboard** perspective.
5. In the **Products and Services** section, see **Radware Security Signature (SUS), Latest Signature Release**
6. You should see the current version like 0009.0739.00



7. In the **DefensePro X Configuration** select **Operations → Update Security Signatures**



8. In the **Update Security Signatures** dialog keep the defaults and click on **Update**.
9. You should see a task starting to download the latest version from the Radware website and a success message after it's finished
10. Click **Close** to close the dialog
11. You can check in the the **Cyber Controller System Dashboard** perspective. In the **Products and Services** section, see **Radware Security Signature (SUS), Latest Signature Release**
12. If a newer version is available, you should see the new file version now.

Configure Signature Protection

In this lab we configure a signature profile

1. Select the Cyber Controller **Security Operations** → **Security Settings**.
2. Edit TeamXX security policy.
3. **Enable** the **Security Signatures** and expand it.
4. **Select** the **Custom** profile.
5. **Click + Add New** to add a new rule
6. Rule Name: **MyWeb**, Attribute Type: **Services**, Attribute Value: **Web-HTTP**
7. **Click + Add New** to add a new rule
8. Add Rule name: **MyWeb** rule name, Attribute Type: **Applications**, Attribute Value: **Web Server – Apache**
9. Add Rule Name: **MyWeb**, Attribute Type: **Confidence**, Attribute Value: **Low** (in production this would normally be set to high)
10. Add Rule Name: **MyWeb**, Attribute Type: **Risk**, Attribute Value: **Info** (in production this would normally be set to High)
11. Create a second rule to include all the signatures in the recommended DoS_All profile named **DoS_All** with the following attributes
 - a. **Threat Type = DoS – Floods**
 - b. **Threat Type = DoS – Slow Rate**
 - c. **Threat Type = DoS - Vulnerability**
12. Click **Submit**

☒ Security Signatures

Profile
 Custom

Custom Profile Table
 [+ Add New](#)

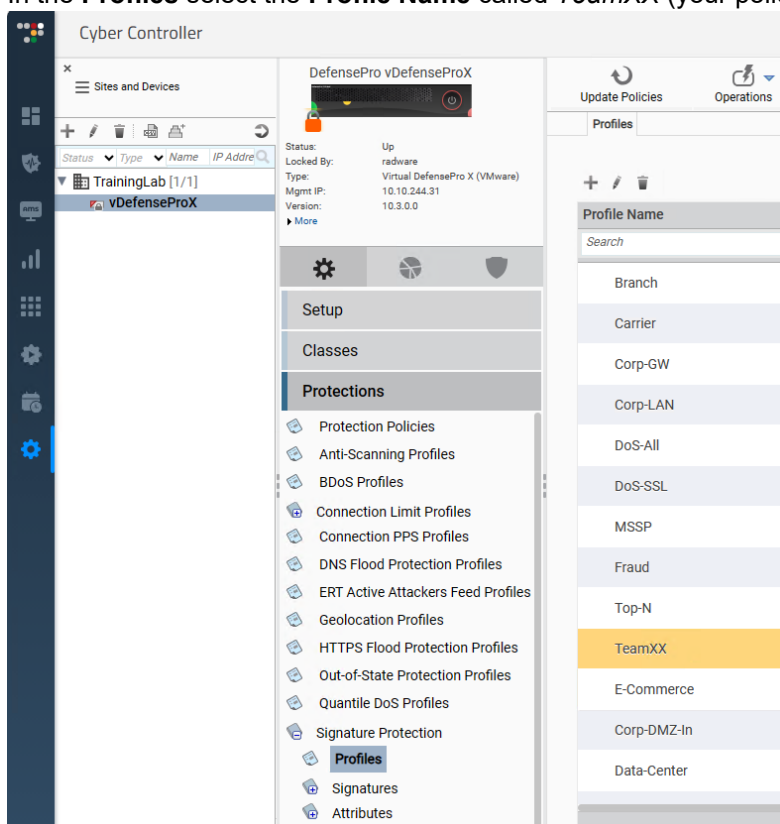
Rule Name	Attribute Type	Attribute Value	
DoS_All	Threat Type	DoS - Vulnerability	
DoS_All	Threat Type	DoS - Slow Rate	
DoS_All	Threat Type	DoS - Floods	
MyWeb	Risk	Info	
MyWeb	Confidence	Low	
MyWeb	Applications	Web Server - Apache	
MyWeb	Services	Web-HTTP	

☒ SYN Flood Protection

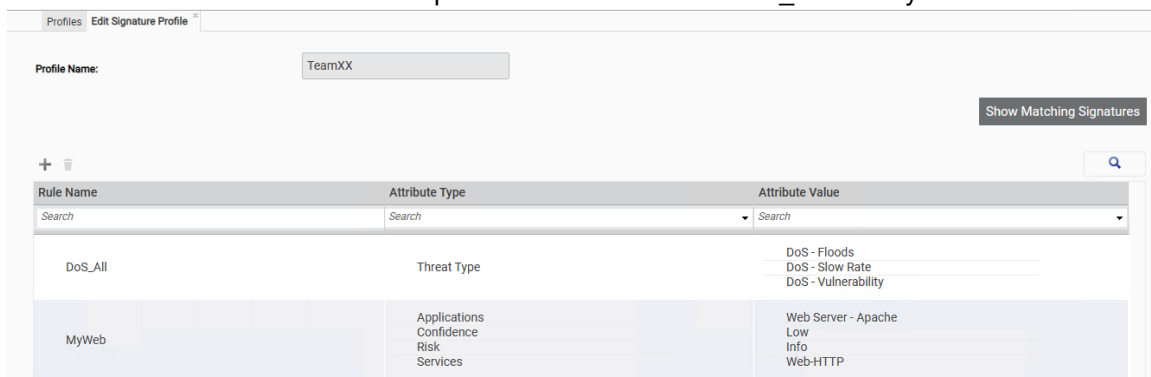
Cancel
 Submit

Let's see how this is translated into a signature protection profile on the DefenseProX configuration.

1. Select the DefensePro X **Configuration** perspective.
2. In **Protections** section, select **Signature Protection** and then **Profiles**.
3. In the **Profiles** select the **Profile Name** called *TeamXX* (your policy name) and double click it



4. We see how it was translated into a profile with the two rules DoS_All and MyWeb.



Test the Configuration

1. Use Raptor to send Signature Attacks .
2. Access **Attacker-PC Raptor** main menu → select **Intrusion Attacks** → **Batch** → **Edit**
3. Select **Apache-Advanced** → **OK**
4. Select attacks using SPACEBAR and DOWN-KEY. Select all attacks for this attach-batch.
5. Save selection with ENTER
6. Select **Apache** → **OK** and again select all attacks for this attach-batch.
7. Repeat with **HTTP-Anomalies**, **HTTP-Misc-Advanced**, and **HTTP-MISC** groups as well.
8. Save the attack-batch.
9. Select **Back** → **Launch** to start the attacks.
10. Based on signature updates, it is possible that not all of the attack captures used by the attack tool will be detected.
11. Verify Destination IP address: **27.1.31.100**
12. Soon after the attack is initiated, you should see traps in the CLI / syslog
13. View the attack details in Cyber Controller.
14. Use Cyber Controller to view the Attacks. Select the **Security Operations** → **Real-Time Monitoring**.

Detection Events 19									
Action	Status	Category	Event Name	Event Destination	Updated Time	Duration	Policy Name	DP Name	Minimize
DestReset	Occurred	Intrusions	HTTP-Get-NOP-Sle...	27.1.31.10	10/20/2023 12:3...	00:00:15	TeamXX	vDefenseProX	
DestReset	Occurred	Intrusions	HTTP-MISC-Acunet...	27.1.31.10	10/20/2023 12:3...	00:02:44	TeamXX	vDefenseProX	
DestReset	Occurred	Intrusions	APACHE-tomcat-vi...	27.1.31.10	10/20/2023 12:3...	00:00:15	TeamXX	vDefenseProX	
DestReset	Occurred	Intrusions	APACHE-Resin-WE...	27.1.31.10	10/20/2023 12:3...	00:00:15	TeamXX	vDefenseProX	
DestReset	Occurred	Intrusions	Apache-SSI-ERR-H...	27.1.31.10	10/20/2023 12:3...	00:00:15	TeamXX	vDefenseProX	
DestReset	Occurred	Intrusions	Apache-ModSecurity...	27.1.31.10	10/20/2023 12:3...	00:00:15	TeamXX	vDefenseProX	

15. Select an attack in **Detection Events** to see details and use the (i) to see the attack description

Direction: Inbound

Intrusions, DOS-Apache-mod_isapi-Pointer

Protected Object/Policy: TeamXX

Destination Address: 27.1.31.10

Denial of Service - Apache mod_isapi module library unload False Positives: None Known. Known Issues: Various Apache HTTP Server versions are vulnerable to a denial of service attack (CVE-2010-0425). Denial of service vulnerabilities occur due to various kinds of software bugs and design flaws, which when exploited, can result in a loss of service to users. This vulnerability may cause denial of service to the web server. This vulnerability occurs by delivering a specially crafted HTTP POST request. Recommended Solutions In order to protect against this vulnerability the following steps should be taken:- Update your Radware device with the latest signature file (See the supported products list below).

Policies 1 Devices 1

Attack Name: DOS-Apache-mod_isapi-Pointer

PCAP Sampled Data

Attack Details Attack Analytics

Additional Attack Attributes

Risk: Medium	Radware ID: 13338	Direction (In/Out): In	Action Type: DestReset	Attack ID: 233-1697710392	Physical Port: 1	Total Packet Count: 3
VLAN: N/A	MPLS RD: N/A	Source Port: 14206	Packet Type: Regular			

16. **Export** and save configuration file. Save as: **dp8-SigLab-config.txt**

17. Export and save configuration file. Save as: dpx-SigLab-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.