DefensePro
Version 8.x

Training Lab Manual
Configure Signature Protection

Table of Contents

Overview

Radware DefensePro 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.

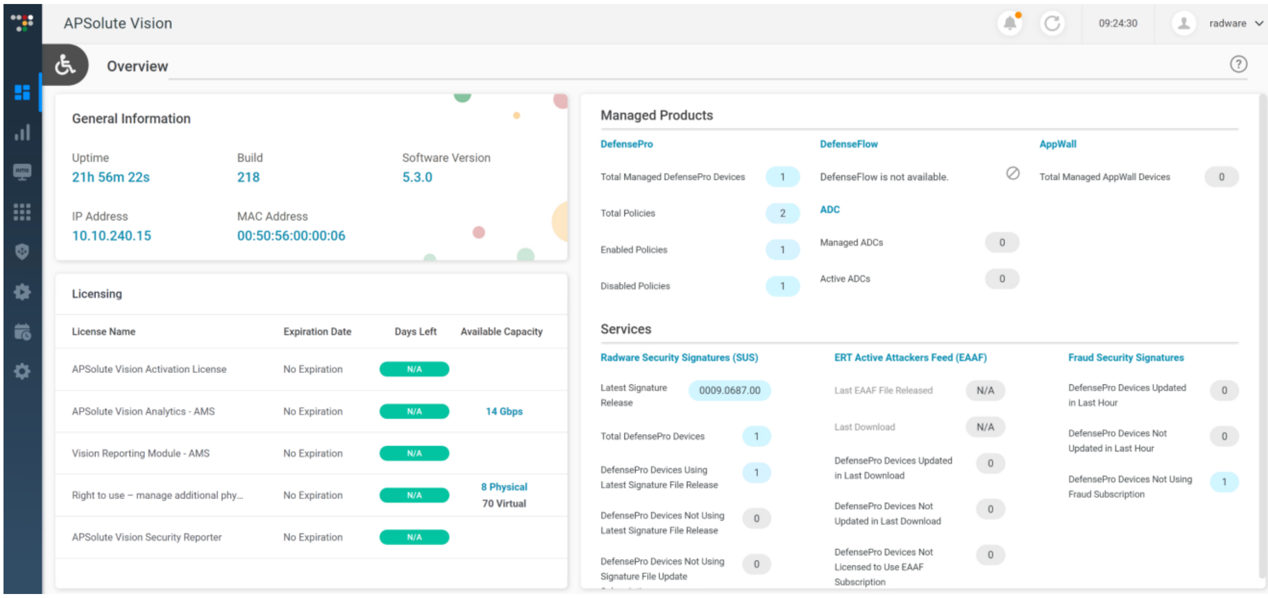
Remove The Traffic Filter Profile From Your Protection Policy

1. **Configuration → Protections → Protection Policies** select and edit your policy.
2. **Profiles → Traffic Filters Profile** remove the current filter.
3. Press **Submit** and **Update Policies Required** buttons.

Update the Signature Database

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

1. Select the **Vision Overview** perspective.
2. In the **Services** section, see **Radware Security Signature (SUS), Latest Signature Release**
3. You should see the current version like 0009.0687.00



General Information

Uptime 21h 56m 22s

Build 218

Software Version 5.3.0

IP Address 10.10.240.15

MAC Address 00:50:56:00:00:06

Licensing

License Name	Expiration Date	Days Left	Available Capacity
APSolute Vision Activation License	No Expiration	N/A	
APSolute Vision Analytics - AMS	No Expiration	N/A	14 Gbps
Vision Reporting Module - AMS	No Expiration	N/A	
Right to use – manage additional phy...	No Expiration	N/A	8 Physical 70 Virtual
APSolute Vision Security Reporter	No Expiration	N/A	

Managed Products

DefensePro

Total Managed DefensePro Devices 1

Total Policies 2

Enabled Policies 1

Disabled Policies 1

DefenseFlow

DefenseFlow is not available.

ADC

Managed ADCs 0

Active ADCs 0

AppWall

Total Managed AppWall Devices 0

Services

Radware Security Signatures (SUS)

Latest Signature Release 0009.0687.00

Total DefensePro Devices 1

DefensePro Devices Using Latest Signature File Release 1

DefensePro Devices Not Using Latest Signature File Release 0

DefensePro Devices Not Using Signature File Update 0

ERT Active Attackers Feed (EAAF)

Last EAAF File Released N/A

Last Download N/A

DefensePro Devices Updated in Last Download 0

DefensePro Devices Not Updated in Last Download 0

DefensePro Devices Not Licensed to Use EAAF Subscription 0

Fraud Security Signatures

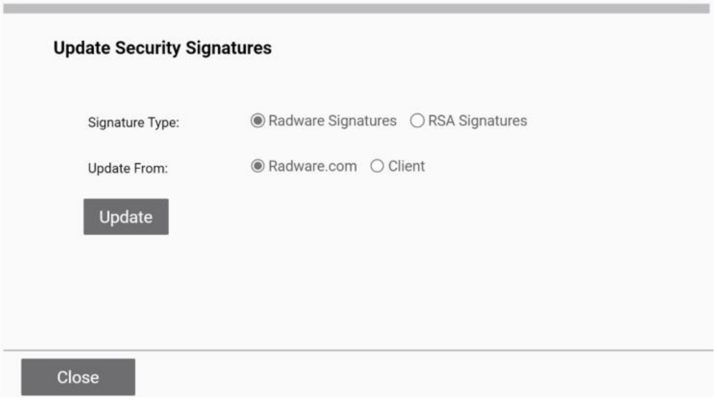
DefensePro Devices Updated in Last Hour 0

DefensePro Devices Not Updated in Last Hour 0

DefensePro Devices Not Using Fraud Subscription 1

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

5. In the **Update Security Signatures** dialog keep the defaults and click on **Update**.



Update Security Signatures

Signature Type: ● Radware Signatures ○ RSA Signatures

Update From: ● Radware.com ○ Client

6. You should see a task starting to download the latest version from the Radware website and a success message after it's finished

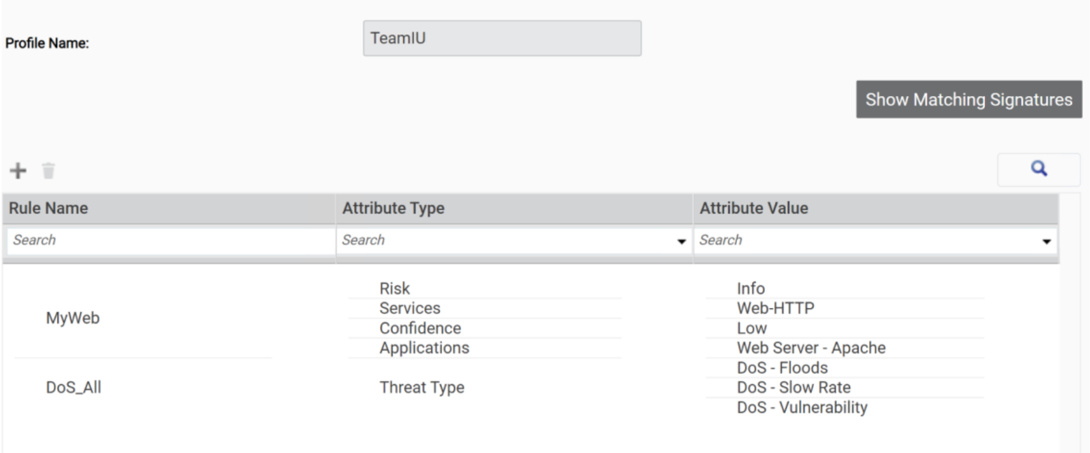
7. Click **Close** to close the dialog
8. You can check in the the **Vision Overview** perspective. In the **Services** section, see **Radware Security Signature (SUS), Latest Signature Release**
9. If a newer version is available, you should see the new file version now.

Configure Signature Protection

In this lab we configure a signature profile

1. Select the DefensePro **Configuration → Protections → Signature Protection → Profiles**.
2. Click + to **add** Signature Protection Profile.
3. In **Add New Signature Protection Profile** tab type the **Profile Name**: ***TeamXX*** (where XX are your initials)
4. Click **+** to add new rule
5. Rule Name: **MyWeb**, Attribute Type: **Services**, Attribute Value: **Web-HTTP** c**lick Submit** to accept changes
6. Select the rule and click + sign next to the **MyWeb** rule name, Attribute Type: **Applications**, Attribute Value: **Web Server – Apache** click **Submit**
7. Add to the Rule Name: **MyWeb**, Attribute Type: **Confidence**, Attribute Value: **Low** (in production this would normally be set to high) click **Submit**
8. Add to the Rule Name: **MyWeb**, Attribute Type: **Risk**, Attribute Value: **Info** (in production this would normally be set to High) click **Submit**
9. 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**

10. Click **Close** to close the profile dialog
11. If you want to see how many signatures are selected by this profile, select this profile and edit it.
12. In the **Edit Signature Profile** window click on **Show Matching Signatures**



Profile Name: TeamIU

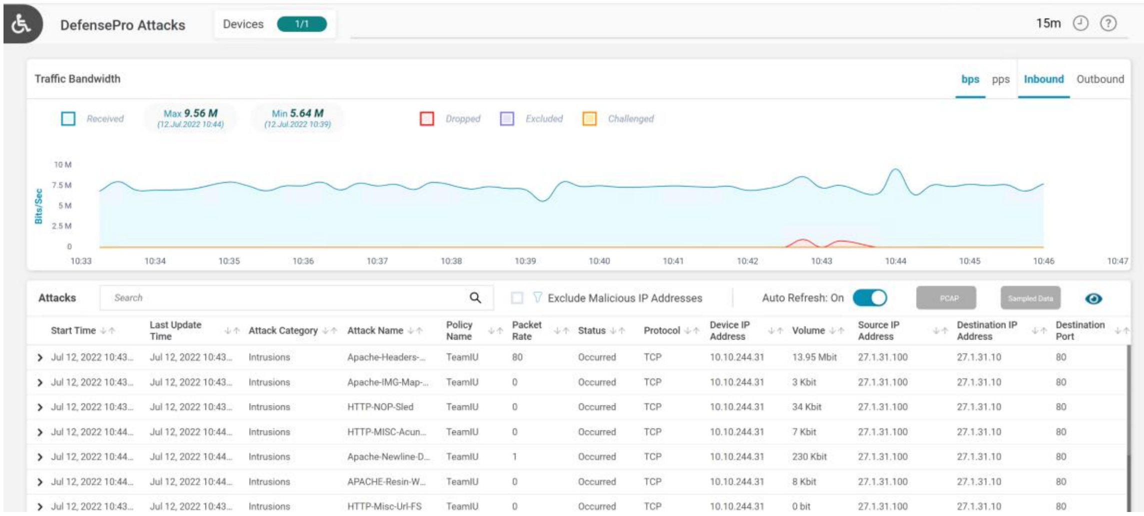
Rule Name	Attribute Type	Attribute Value
MyWeb	Risk Services Confidence Applications	Info Web-HTTP Low Web Server - Apache
DoS_All	Threat Type	DoS - Floods DoS - Slow Rate DoS - Vulnerability

13. In the **Matching Signatures** window, you can see the number in the lower right corner "Displaying Rows 1 – X of zzz", where zzz is the number of signatures. For this lab we expect ~620 signatures. The exact value depend about weekly update of signatures file. If you change confidence to medium or high.
14. We need to add the profile to the protection policy.
15. In the **Protections** section, select **Protection Policies** on navigation tree.
16. In the **Protection Policies** tab double-click your policy to edit.
17. Select the **Profiles** section → **Signature Protection Profile**
18. Select the profile you just created for the **Signature Protection Profile**.
19. Select **Packet Reporting** section and enable ***Packet Reporting***. This will generate a pcap file for each attack packet matching the signatures.
20. Click on **Submit**
21. Click **Update Policies Required** button and wait for completion.

Test the Configuration

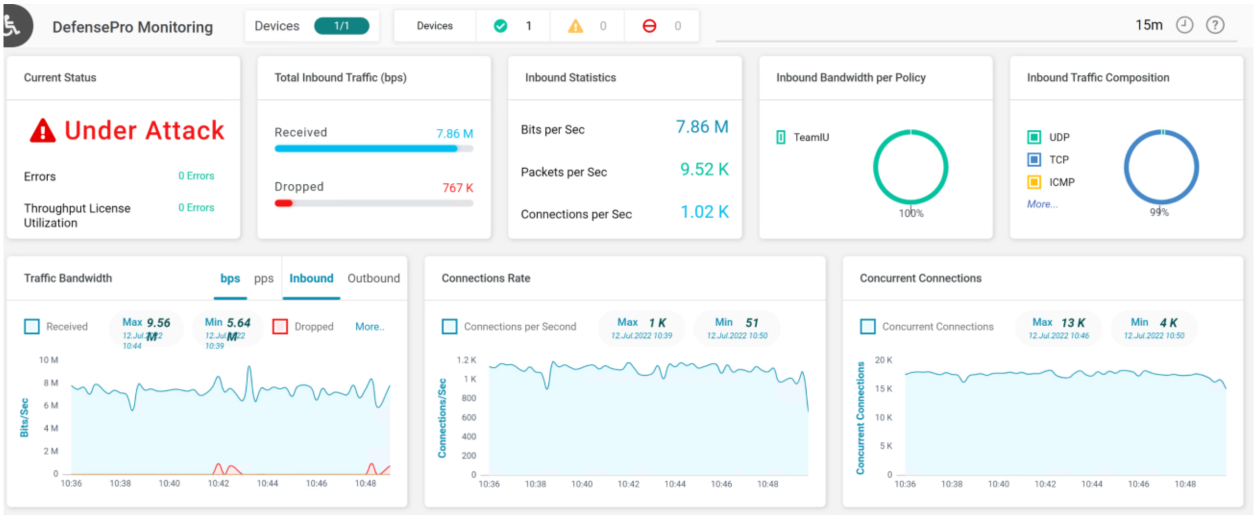
1. Use Raptor to send Signature Attacks .
2. Access **Attacker-PC Raptor** main menu → select **Intrusion Attacks → Batch → Edit**
3. Select **Apache-Advanced → OK**
4. Select attacks using SPACEBAR and DOWN-KEY. Select all attacks for this attach-batch.
5. Save selection with ENTER
6. Select **Apache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

15. In the attack details you can use the PCAP icon to export a pcap from Vision. Review it with wireshark to see the attack packet information.



Start Time	Last Update Time	Attack Category	Attack Name	Policy Name	Packet Rate	Status	Protocol	Device IP Address	Volume	Source IP Address	Destination IP Address	Destination Port
Jul 12, 2022 10:43...	Jul 12, 2022 10:43...	Intrusions	Apache-Headers-...	TeamIU	80	Occurred	TCP	10.10.244.31	13.95 Mbit	27.1.31.100	27.1.31.10	80
Jul 12, 2022 10:43...	Jul 12, 2022 10:43...	Intrusions	Apache-IMG-Map-...	TeamIU	0	Occurred	TCP	10.10.244.31	3 Kbit	27.1.31.100	27.1.31.10	80
Jul 12, 2022 10:43...	Jul 12, 2022 10:43...	Intrusions	HTTP-NOP-Sled	TeamIU	0	Occurred	TCP	10.10.244.31	34 Kbit	27.1.31.100	27.1.31.10	80
Jul 12, 2022 10:44...	Jul 12, 2022 10:44...	Intrusions	HTTP-MISC-Acun...	TeamIU	0	Occurred	TCP	10.10.244.31	7 Kbit	27.1.31.100	27.1.31.10	80
Jul 12, 2022 10:44...	Jul 12, 2022 10:44...	Intrusions	Apache-Newline-D...	TeamIU	1	Occurred	TCP	10.10.244.31	230 Kbit	27.1.31.100	27.1.31.10	80
Jul 12, 2022 10:44...	Jul 12, 2022 10:44...	Intrusions	APACHE-Resin-W...	TeamIU	0	Occurred	TCP	10.10.244.31	8 Kbit	27.1.31.100	27.1.31.10	80
Jul 12, 2022 10:43...	Jul 12, 2022 10:43...	Intrusions	HTTP-Misc-Url-FS	TeamIU	0	Occurred	TCP	10.10.244.31	0 bit	27.1.31.100	27.1.31.10	80

16. Select **Analytics AMS > DefensePro Monitoring**



Under Attack

Errors 0 Errors

Throughput License Utilization 0 Errors

Received 7.86 M

Dropped 767 K

Bits per Sec 7.86 M

Packets per Sec 9.52 K

Connections per Sec 1.02 K

17. Click on your protection policy. The policy information opens.
18. Click on Intrusions line. The intrusion attacks table opens.
19. You can toggle between Event category or event table view.
20. Select one of the attacks to see details.
21. Click on << Go Back to return to the dashboard.
22. In the AMS menu, select "DefensePro Analytics"
23. Here you can see all the attacks detected. Change the time frame to 24H or select a different time range to see all your attacks from previous labs as well.
24. **Export** and save configuration file. Save as: **dp8-SigLab-config.txt**

For questions, contact **training@Radware.com**