radware

DefensePro X
Version 10.x

Training Lab Manual
Configure Signature Protection

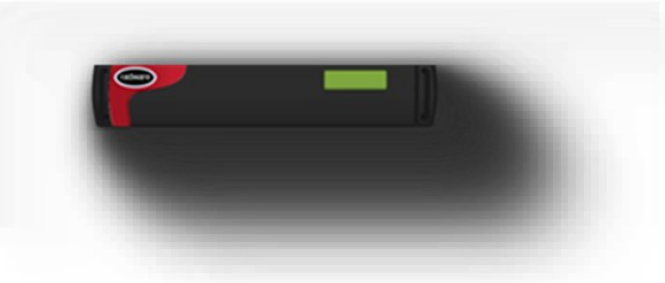


Table of Contents

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

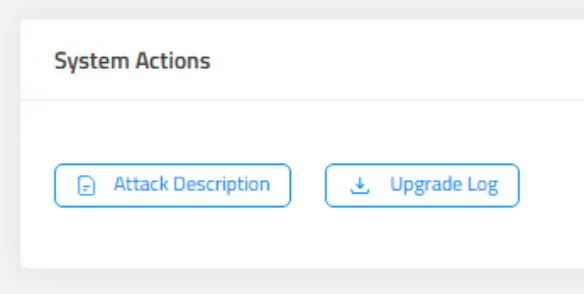
1. **Security Operations → Security Settings** select and edit your policy.
2. **Disable** the **Traffic Filters** protection.
3. Press **Submit** to update the policy.

Update the Signature Database and Attack Description

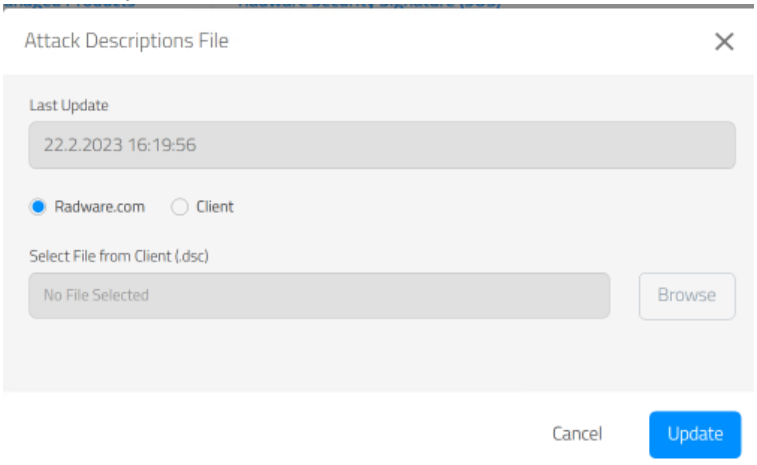
Before we start with the signature protection configuration, we want to make sure to use the lastest signatures. For this feature the device has to have the SUS service subscription.

1. Go to Cyber Controller **System Dashboard**.

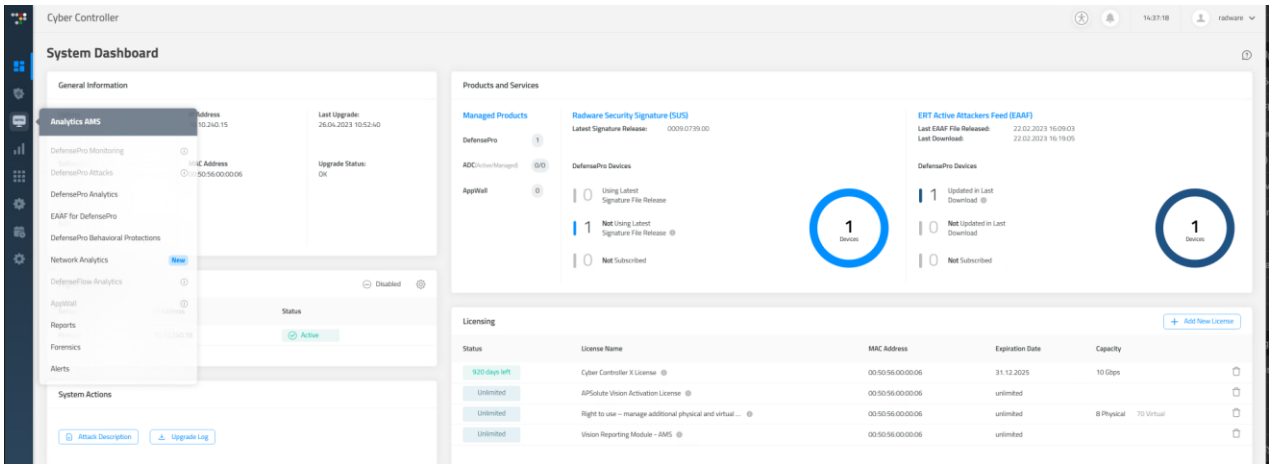
2. Under System Actions click on **Attack Description**



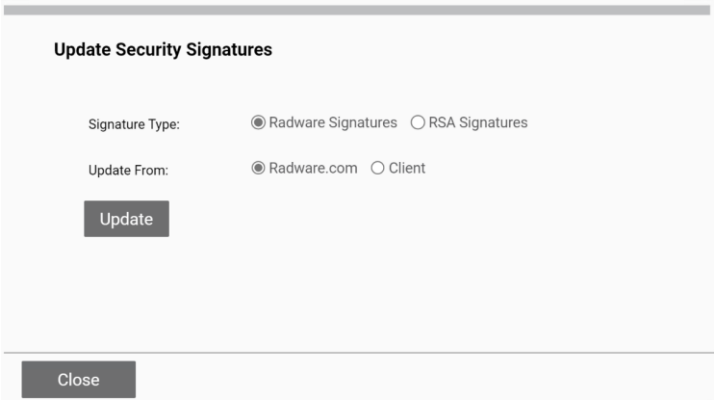
3. Click on Update.



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**

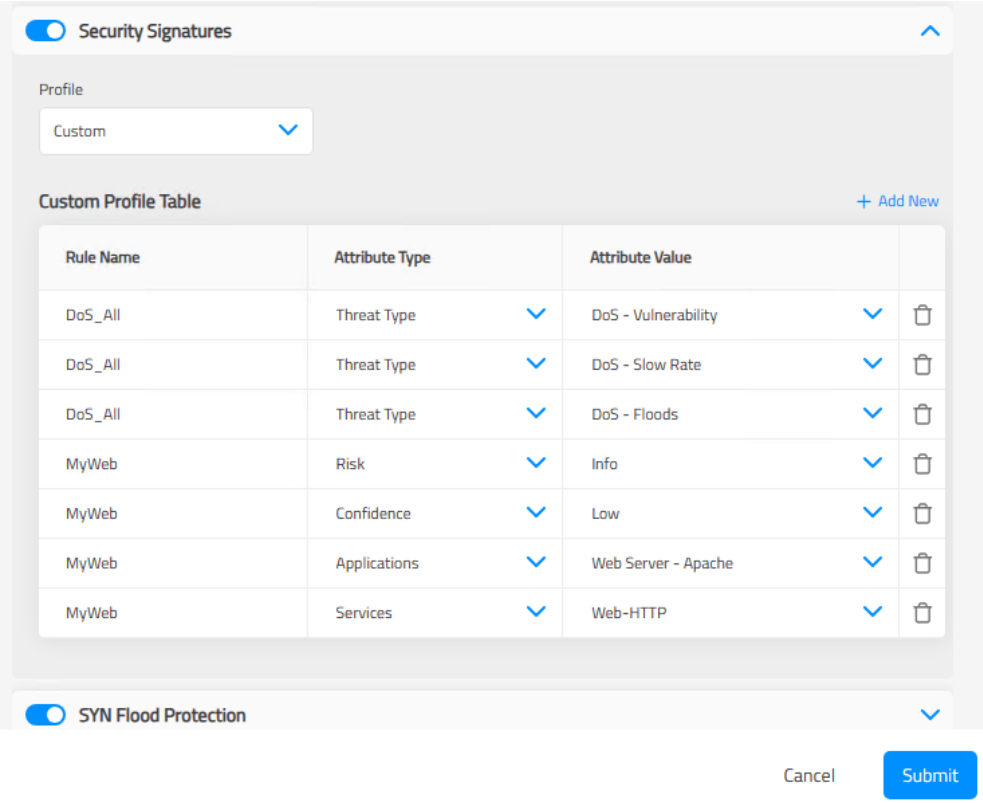


8. In the **Update Security Signatures** dialog keep the defaults and click on **Update**.
9. You should see a task starting to download the latest version from the Radware website and a success message after it's finished
10. Click **Close** to close the dialog
11. You can check in the the **Cyber Controller 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

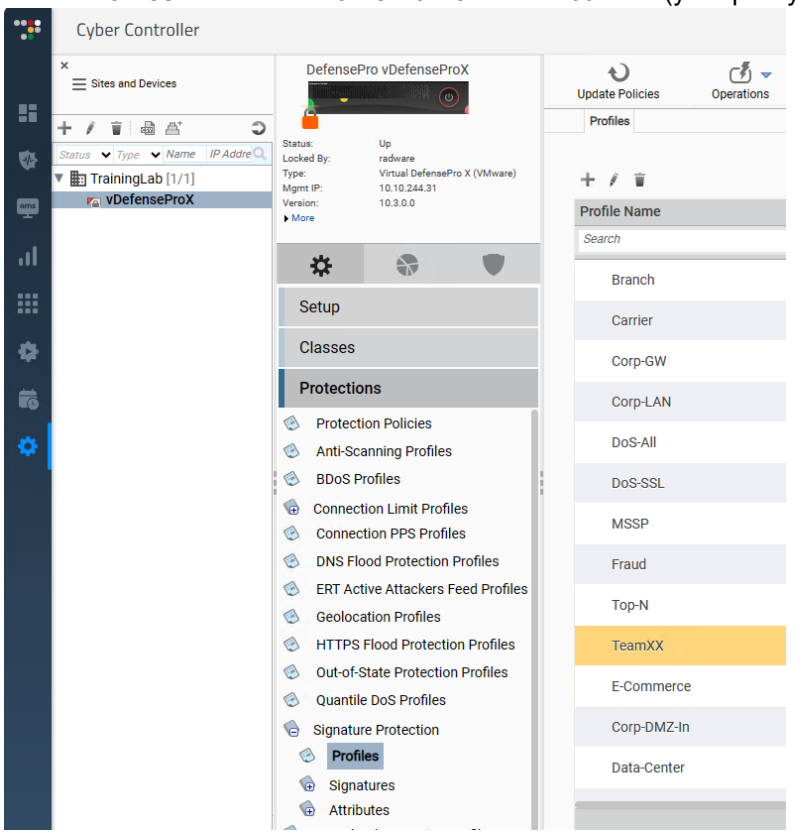
In this lab we configure a signature profile

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**

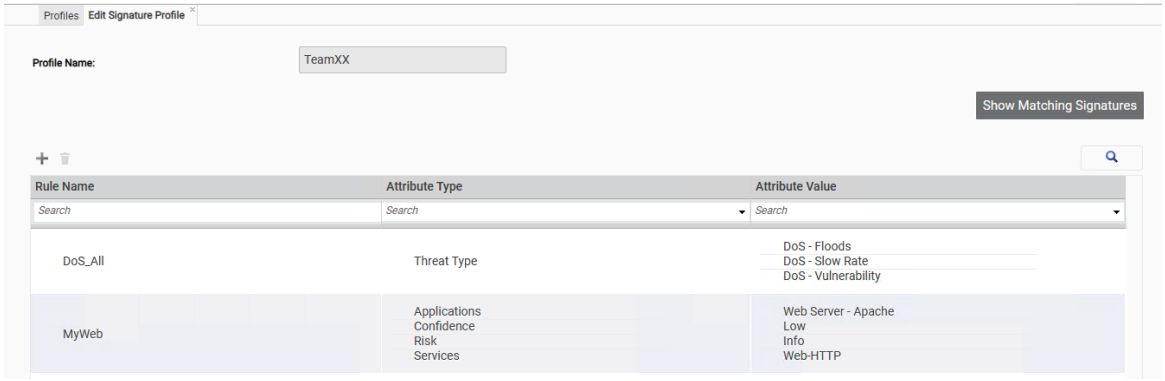


Let's see how this is translated into a signature protection profile on the DefenseProX configuration.

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

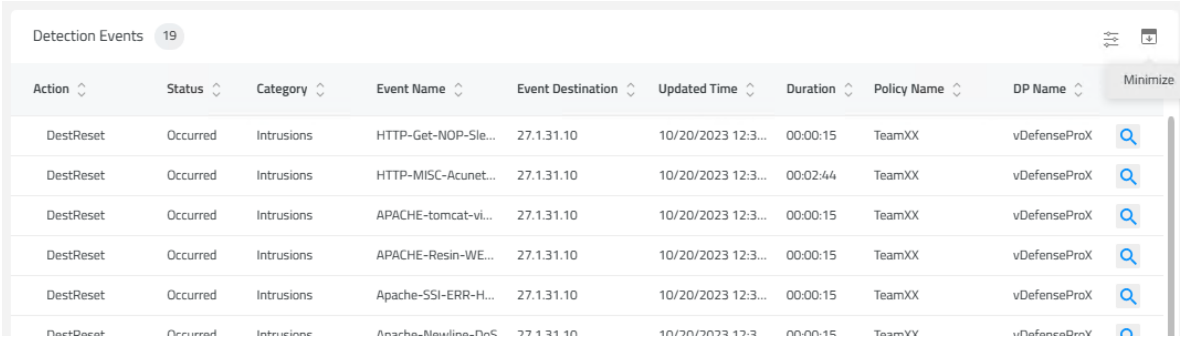


4. We see how it was translated into a profile with the two rules DoS_All and MyWeb.

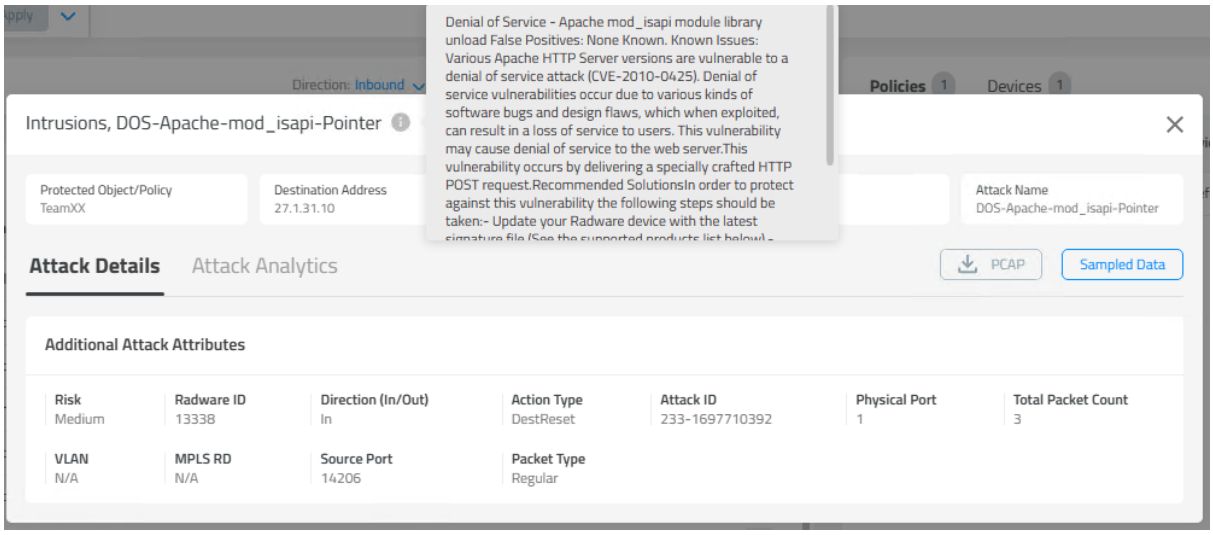


Test the Configuration

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**.



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



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