

Training Lab Manual Administration



Table of Contents

Contents

ADMINISTRATION	3
OVERVIEW	3
UPDATING DEFENSEPRO SOFTWARE VERSION	3
VIEW LICENSE INFORMATON	3
EXPORT CONFIGURATION FILES	3
IMPORT CONFIGURATION FILES	4
UPDATING THE SIGNATURE DATABASE	4
USING THE SCHEDULER	4
EXPORTING A TECHSUPPORT FILE.....	5
INTERFACE WALKTHROUGH.....	6
IMPORT A BASE POLICY	6
RUN THE BASELINE TRAFFIC	7
RUN AN ATTACK.....	7

Administration

Overview

Radware DefensePro labs are maintained and kept up to date by Radware lab managers. This lab introduces DefensePro device administration for information only.

Exercises in this lab are viewed from the MONITORING and CONFIGURATION perspectives.

After reviewing these lab exercises, retain the information for future use.

Updating DefensePro Software Version

Since the device is already upgraded to the version of the lab manual, you should not upgrade it and just review the options. If you update the device, the screens can be different than in the lab manual.

1. In **APSolute Vision**, select DefensePro **Configuration** perspective. Select **Setup → Software Version Management** on the navigation tree. Here you can see the software versions which are on the device. Only one version can be active (see status column). In this table you can also select a different version to be active, if you do so the DefensePro will reboot using the selected version with the configuration file, which was active at this version. There will be a popup window to validate that you want to select this version and reboot.
2. To update the software select **Upload Software Version** below the **Software Version Management**
3. In the dialog you have the option to upload the software version and activate it immediately or just upload without activation.
4. Each software version needs a password, which can be generated automatically, if Vision has access to the internet to validate the support contract of the device, or can be generated on the Radware portal.

View License Information

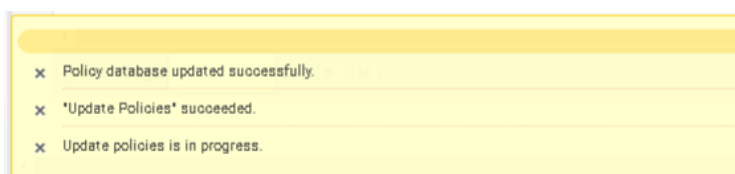
1. In **APSolute Vision**, select DefensePro **Configuration** perspective and select **Setup → Global Parameters → License Upgrade**
2. In the License Upgrade window, you can review the current licenses and update them in case it's needed.
3. NOTE: In our lab we use a virtual DefensePro, this platform has an additional license called **vCPU license**. In regular hardware platforms you will only have the **Throughput License**.

Export Configuration Files

1. In **APSolute Vision**, select DefensePro **Operations → Export Configuration File** to export a configuration file saved on the local client or on the Vision server.
2. Select Client and check Include Private Keys to make sure all keys and certificates (WebUI, SSL inspection) will be saved as well. Type **radware** as passphrase and click OK
3. Save the file at a location you remember.

Import Configuration Files

1. NOTE: If you import a configuration file, the DefensePro will reboot
2. To be able to monitor the reboot process, open the DP-Console in MobaXterm
3. In **APSolute Vision**, select DefensePro **Operations** → **Import Configuration File** to import a configuration file saved on the local client or on the Vision server.
4. Select the configuration you saved and don't forget to add the passphrase (**radware**) and click on **Import**
5. On the DP-Console you can now review the boot process. After the process is finished the device will be available again in APSolute Vision
6. You should see a "**Upload File succeed**" yellow message.




7. Click **Close** to close the Import Configuration File window.

Updating The Signature Database

1. Before we do the update, check first which version is currently on the device
2. In APSolute Vision select DefensePro **Monitoring** perspective. Select **Operational Status** → **Overview** in the navigation tree and in the Overview window see the **Signature File Update** → **Radware Signature File Version**
3. In APSolute Vision select DefensePro **Operations** → **Update Security Signatures**
4. Signatures can be updated directly from Radware.com web site, or from a local client. In case Vision has no access to the internet, the update file can be downloaded from Radware Portal.
5. Keep the defaults and click on **Update** to start the proccess from Radware.com
6. You should get a succeed message after the update is finished.
7. Click on **Close** to close the Update Security Signatures window.
8. Repeat step 2 to see the current version.

Using the Scheduler

1. APSolute Vision has the Scheduler to automate some recuring tasks.
2. The first task we add, is to daily update the attack description file for the Signature protection to make sure each time a new attack is added in the attack details window we can see the details.
3. In the left menu select the **Scheduler** icon 
4. Click **+** to add a new Task and use the information as follows:

Parameters	
Task Type	Update Attack Description File
Name	SUS Description File Update
Schedule	Daily
Time	08:00:00

5. Click **Submit** to add the new task

6. The second task we add is to daily update the security signature file
7. Click **+** to add a new Task and use the information as follows:

Parameters	
Task Type	Update Security Signatures Files
Name	SUS File Update
Schedule	Daily
Time	08:01:00
Target Device List	Highlight your device name and use the > button to add it to the Selected Device list

8. Click **Submit** to add the new task
9. The third task we add is a weekly backup of the configuration file
10. Click **+** to add a new Task and use the information as follows:

Parameters	
Task Type	Device Configuration Backup
Name	Configuration Backup
Schedule	Weekly
Time	09:00:00
Day	Select Sunday
Parameters	Select Include Private Keys Pasphrase: radware
Destination	APSolute Vision Server
Target Device List	Highlight your device name and use the > button to add it to the Selected Device list

11. Click **Submit** to add the new task
12. You can start an task at every time by highlighting the Task and use the **Run Now** ► button
13. For each task you can see the last execution date and status

Exporting A TechSupport File

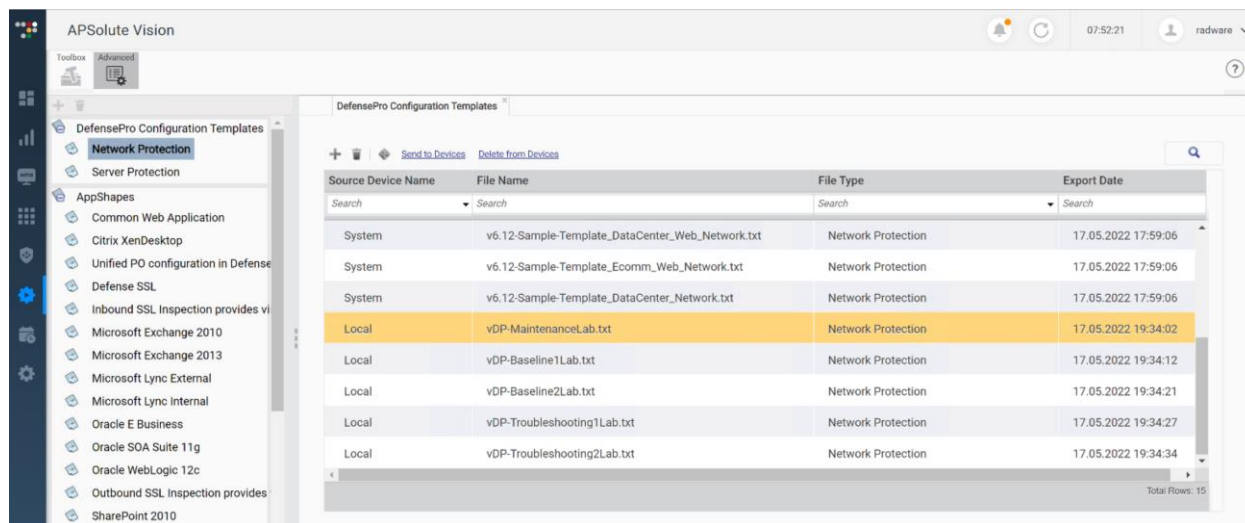
1. In **APSolute Vision**, select DefensePro **Configurartion** perspective and select **Operations → Export Technical Support File** to create and export a technical support file, which is often need to open a support case.
2. Save the file at a location you remember or open it directly to review it's content.

Interface Walkthrough

We will import a basic policy to demonstrate the APSolute Vision Interface.

Import a base policy

To import a base template policy, go to **Automation → Advanced → DefensePro Configuration Templates → Network Protection** and select **vDP-MaintenanceLab** template.

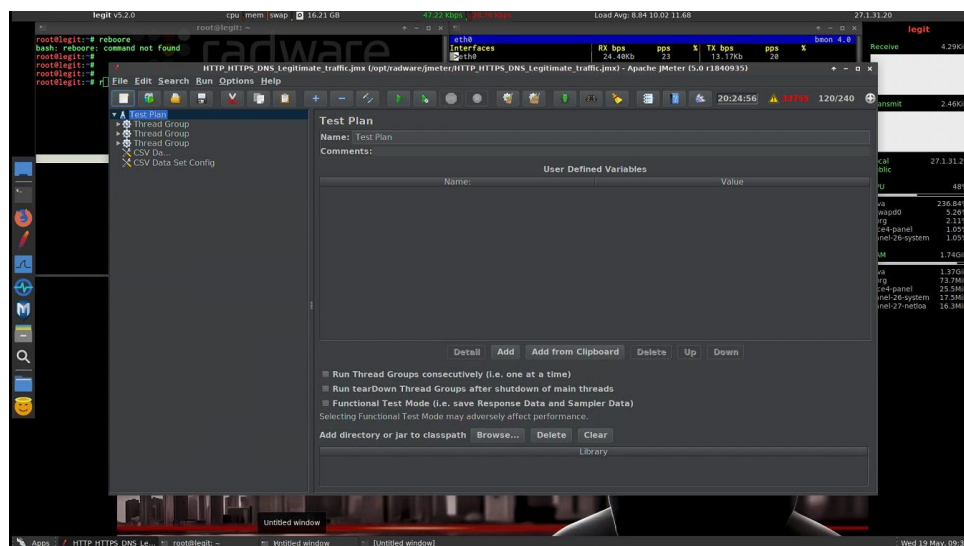


Click on **Send to Devices** and select **vDefensePro** from the list of **Available** devices and press the **>** button to move it to **Selected** section. Click **Submit**.

Go to **Configuration**, select **vDefensePro**, go to **Configuration → Protections → Protection Policies** and confirm that Policy **TeamLab** is configured. Click on the **Update Policies Required** icon.

Run the baseline traffic

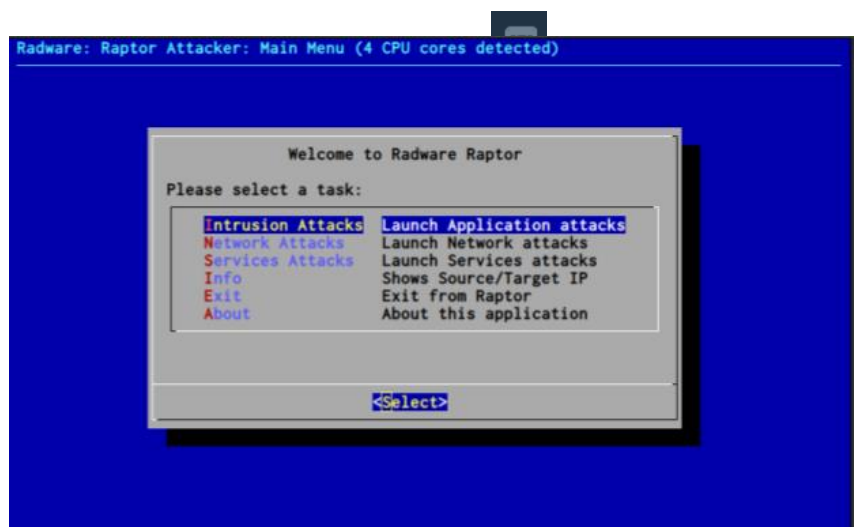
If you haven't done it already, open the MobaXterm **Legitimate Client** by clicking on the shortcut on the desktop or run it from the Sessions part of already running MobaXterm. In the JMeter window click on the green play button to start running a legitimate traffic load.



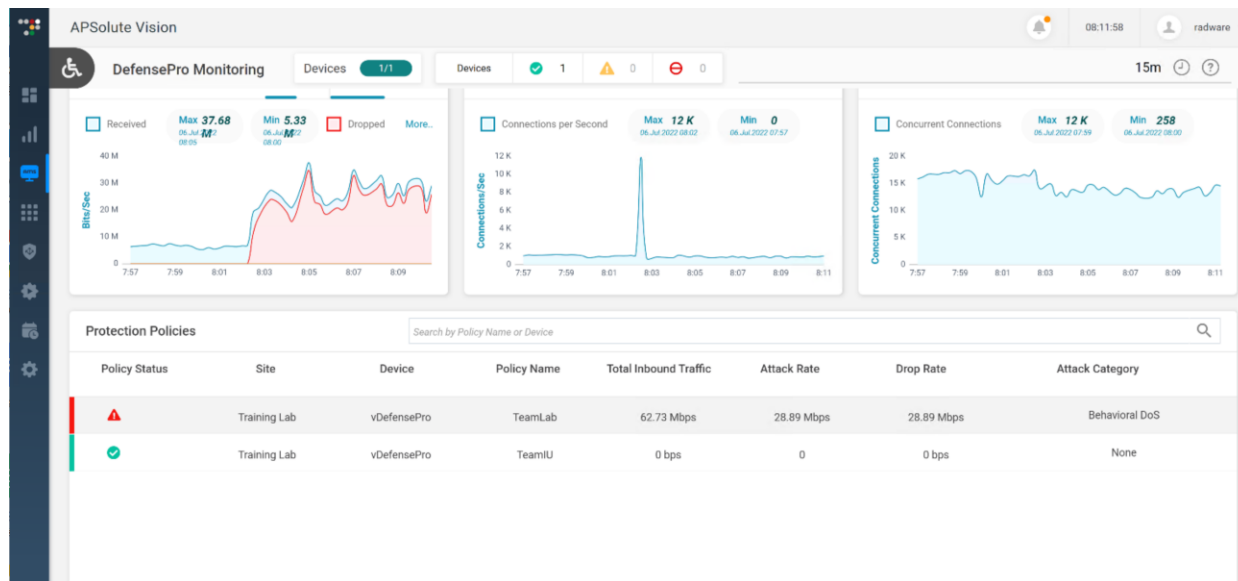
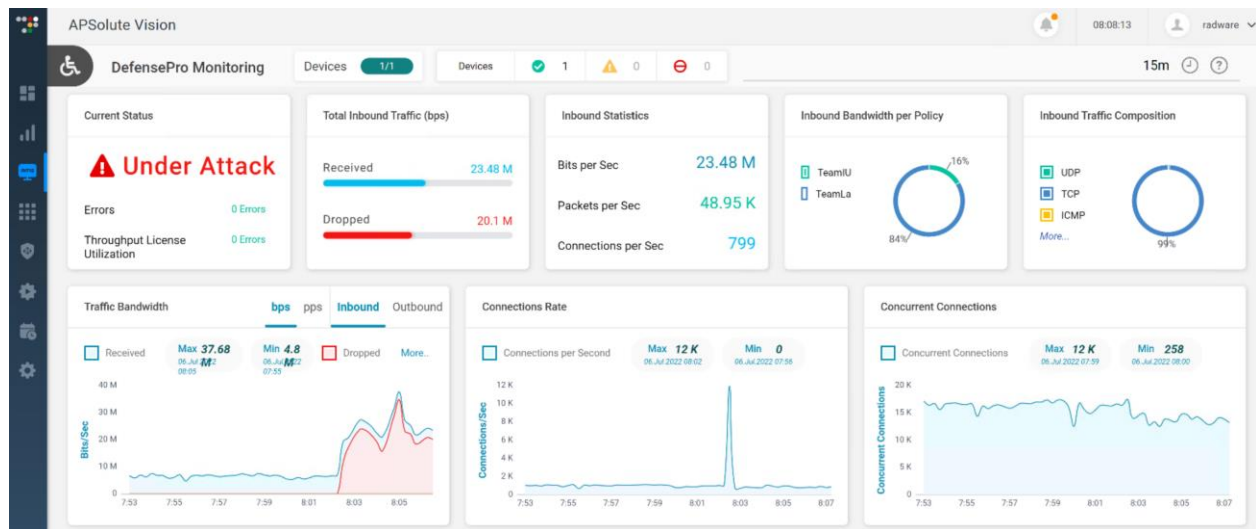
Run an attack

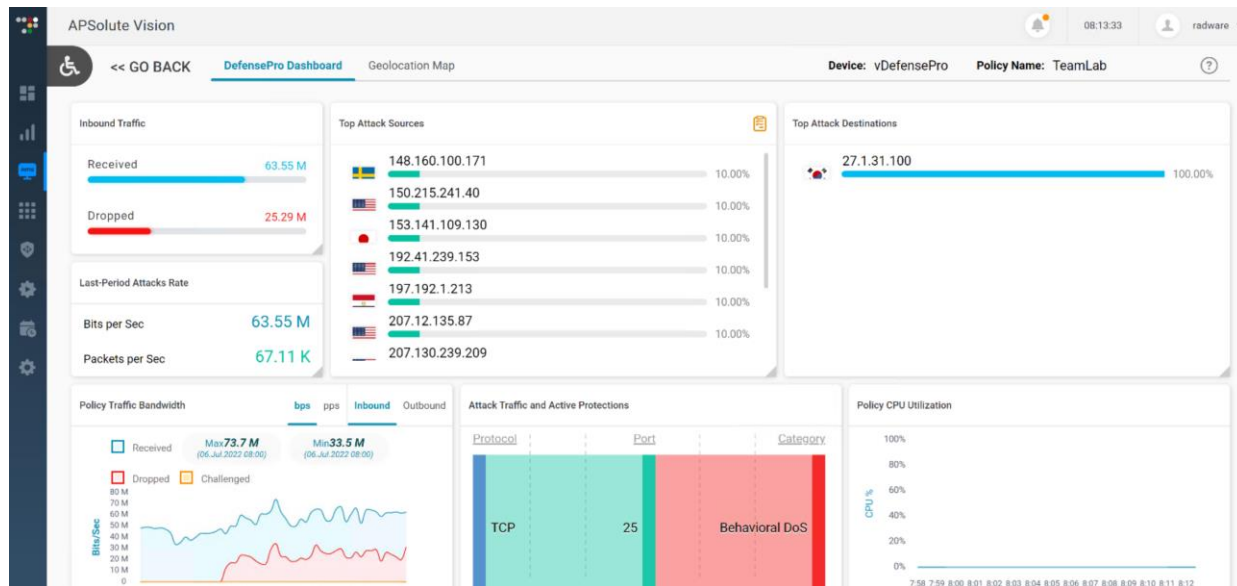
If you haven't done it already, open the MobaXterm **Attacker** by clicking on the shortcut on the desktop or run it from the Sessions part of already running MobaXterm.

In Raptor (blue window) launch an attack **Network Attacks → Floods → Multiple Sources → TCP → RST Attack**. Enter **27.1.31.100** as an attack destination.



Go to APSolute Vision **Analytics AMS** and select **DefensePro Monitoring**. Explore the GUI.





Save the configuration file as ***dp8-Maintenance-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.