DefensePro
Version 8.x

Training Lab Manual
Initial Setup

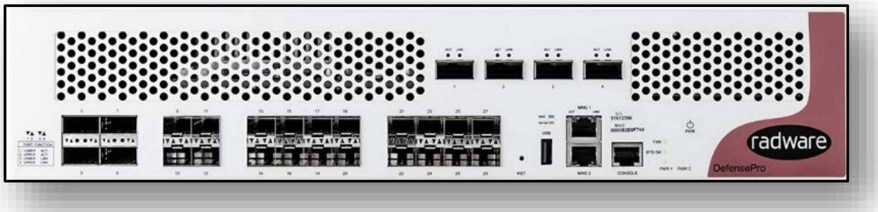


Table of Contents

Contents

Introduction

The **DefensePro** training lab comprises of several activity flows that you will need perform while reviewing the online course. It covers basic configurations and troubleshooting in DefensePro and virtual DefensePro installations.

The features and functions of Radware’s DefensePro devices in this document are based on DefensePro version 8.30 and Vision version 5.3.0.

Use the online lab together with this manual to perform lab activities.

For technical assistance, please contact Radware Virtual Lab support at radwarevirtuallab@radware.com.

Icons in this document:

C:\ How to perform an activity using CLI

🌐 How to perform an activity using APSolute Vision interface (Vision)

Lab Environment

This lab kit consists of:

- A DefensePro VA instance
- An attacker based on Kali Linux
- A legitimate client
- A vulnerable web application

Required Tools & Equipment

Local Workstation (Desktop or Laptop)	Capable of a Web-Browser to access remote lab OS MS-Windows, MAC-OS or Linux
Tablet (IOS or Android)	(Optional) For accessing documents on PDF files instead of using the ones on your local workstation

All Team-PCs and web servers are preconfigured. Your will get assign access parameters for you to use.

Access this lab by browsing to one of our remote lab locations.
Connect and use assigned user / password only.
Your trainer or lab administrator will provide this info before you start.

All devices are ready for you to perform the hands-on.

Lab Layout

DefensePro Lab

SSL-VPN Connection Information

USA	**https://njvpn.radware.net**
Germany	**https://devpn.radware.net**

Remote Client Login
Username: provided by trainer/virtual lab
Password: provided by trainer/virtual lab

Lab Access from the Remote Client:

Remote Client
NTP Server
IP address: 10.10.240.1

APSolute Vision
https://10.10.240.15
Username: radware
Password: radware

Attacker
Icon at desktop or VNC: 192.167.1.20:8931

Legitimate Client
Icon at desktop or VNC: 192.167.1.20:8231

Target Server
Icon at desktop or VNC: 192.167.1.20:8631

vDP Serial
Icon at desktop or Telnet: 192.167.1.20:6431

vDP-SSH
Icon at desktop or SSH: 10.10.244.31

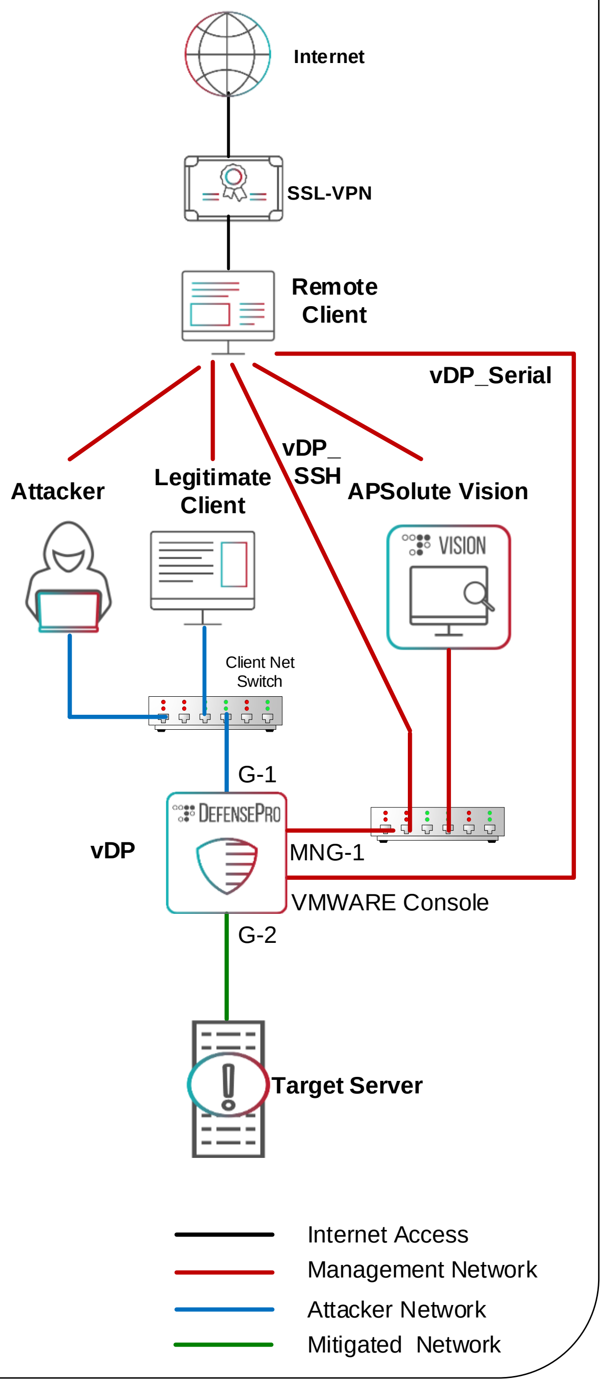
DefensePro Lab Information

vDP (VA)
login (console / serial / ssh)
Username: radware
Password: radware1
MNG 10.10.244.31/21
MNG-GW 10.10.240.1
External Network port G1
Server Network port G2

Attacker IP Address
27.1.31.10 / 24

Legitimate Client IP Address
27.1.31.20 / 24

Target Server IP Address
27.1.31.100 / 24



Connect to the Device via Your Local Workstation

Establish an SSL-VPN connection from your local workstation (desktop or laptop, MS-Windows, macOS or Linux).
This VPN gateway enables to establish an RDP connection to our remote client working with MS-Windows OS.
You establish all connections to vDP, Attacker, Legitimate Client and APSolute Vision devices from this computer.

Connect to SSL-VPN

Open a browser session (Chrome, FireFox, Edge, Safari etc.) from your local computer.
Select the lab site assigned by your instructor or remote lab admin.

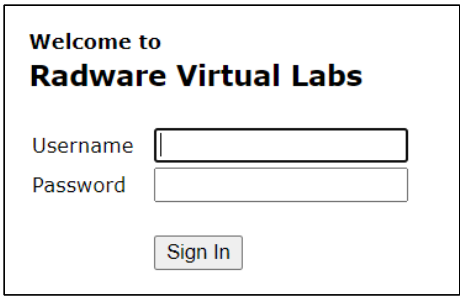
Remember: All sessions we need for the lab (browser, VNC, SSH) are started within the browser you open for this SSL VPN session. For example, don't get confused having a Firefox session within your Firefox browser . Always select the application within your local browser. The advantage is, we use only a single HTTPS session for the whole lab access!

Remote Lab Access

Parameters	
URL	USA lab: https://njvpn.radware.net German lab: https://devpn.radware.net
Username	Provided by your trainer (example: portaldp12)
Password	Provided by your trainer (example: Radware59)

Login at SSL- VPN

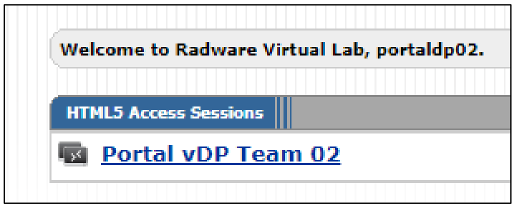
1. Insert ***Username*** and ***Password***



Welcome to
Radware Virtual Labs

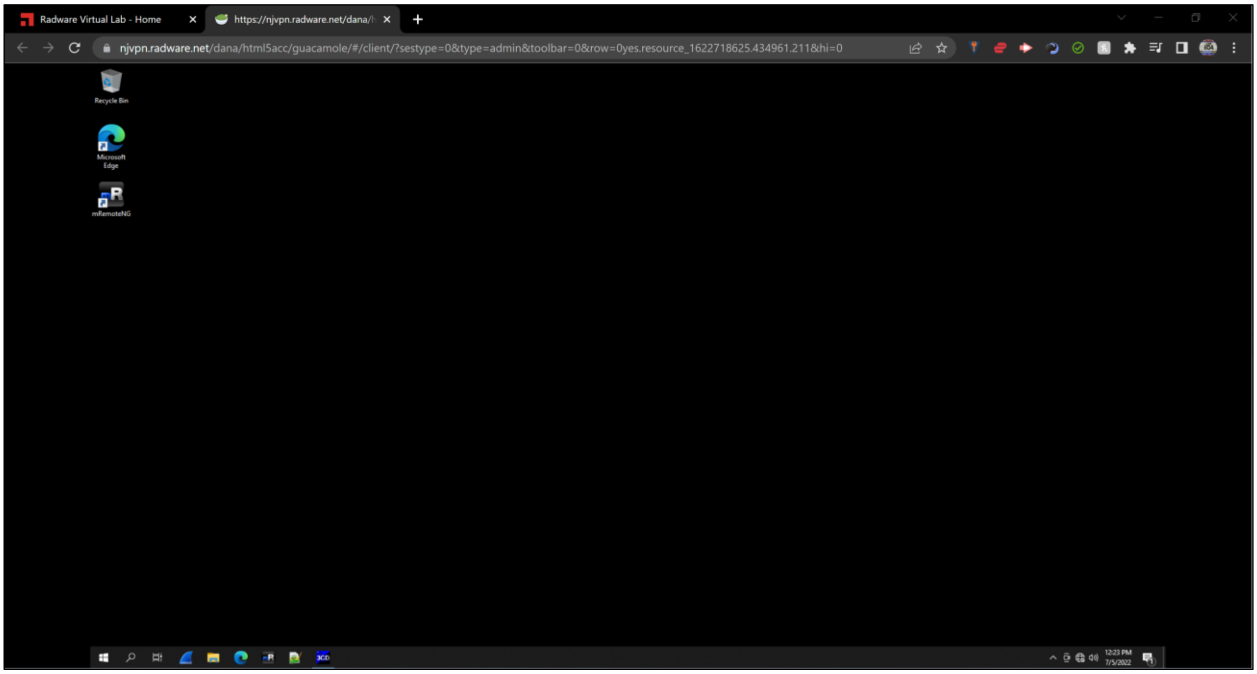
Username
Password

2. Press ↵ or press the ***Sign In*** button.
3. Press the ***vDP Team XX*** hyperlink to connect RDP client (example: Portal vDP Team 02)



Welcome to Radware Virtual Lab, portaldp02.

4. Windows virtual desktop screen appear in a new browser tab. **NOTE**: The size of your remote desktop is defined by the size of the browser window you start it from. **HINT**: If you want to have full screen, use the F11 key on the browser before you click on the link.

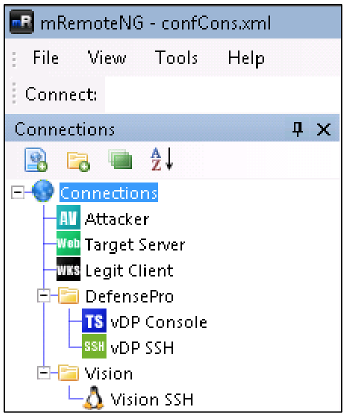


Radware Virtual Lab - Home
https://njvpn.radware.net/dana/
njvpn.radware.net/dana/html5acc/guacamole/#/client/?sestype=0&type=admin&toolbar=0&row=0yes.resource_1622718625.434961.211&hi=0
Recycle Bin
Microsoft Edge
mRemoteNG
12:23 PM
7/5/2022

Use Desktop Icons

Under Windows’ button, you will find the standard Windows File-Explorer, and other applications.

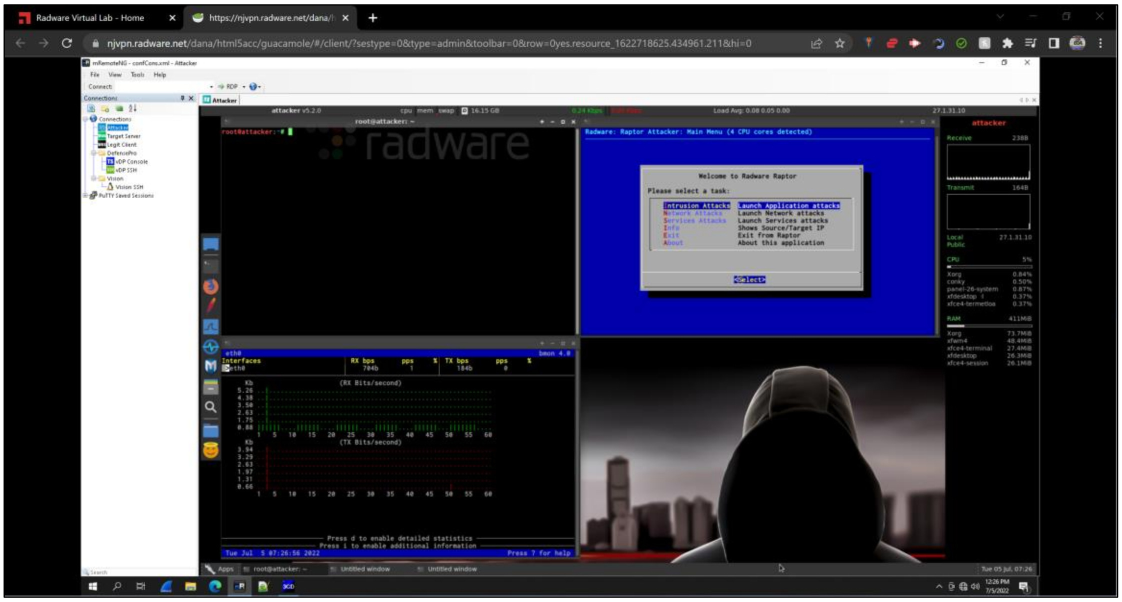
3CD is a Syslog, FTP and TFTP server, Wireshark for debugging, mRemoteNG acts as a VNC/Telnet/SSH client and Microsoft Edge browser.



Inside the mRemoteNG application, there are useful shortcuts for accessing different machines during performing hands-on lab activities.

- **Attacker** generates attack traffic to be detected by a DefensePro policy
- **Target Server** enables monitoring traffic on in and out of a web server
- **Legitimate Client** generates legitimate traffic allowed by a DefensePro policy
- **vDP_Console** is a Console (Serial) Direct connection, IP address independent, to virtual DefensePro (VA) Lab Device
- **vDP-SSH** is a connection to a virtual DefensePro (VA) Lab Device via MNG-1 port using SSH protocol
- **Vision** SSH, is a connection to the central management station

This is an example how it looks like, if you connect to the Attacker machine using mRemoteNG

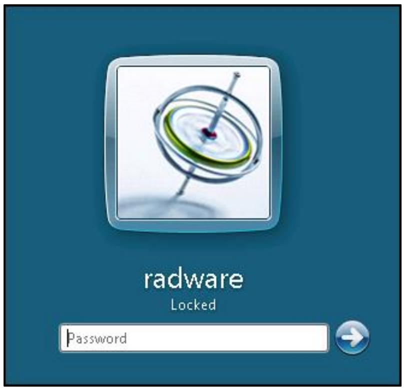


```
root@attacker:~#
```

```
Radware: Raptor Attacker: Main Menu (4 CPU cores detected)

                 Welcome to Radware Raptor
  Please select a task:

       Intrusion Attacks    Launch Application attacks
       Network Attacks      Launch Network attacks
       Services Attacks     Launch Services attacks
       Info                 Shows Source/Target IP
       Exit                 Exit from Raptor
       About                About this application

                          <Select>
```

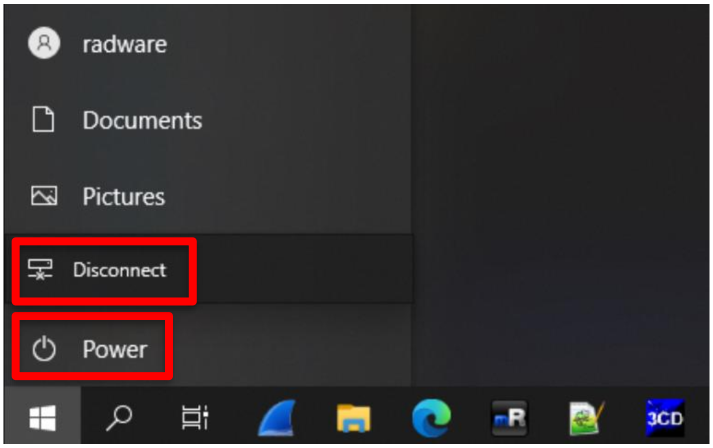
```
Press d to enable detailed statistics
Press i to enable additional information
Tue Jul  5 07:26:56 2022                    Press ? for help
```

If you get locked out from your remote desktop windows session, after a break etc, the login password is **radware.**



End Session

1. **Windows**: Press the ***Start*** icon
   ➔ Press ***Power*** button, if you finished with the lab, all applications will be closed
   ➔ Press ***Disconnect*** button, if you want to continue with the lab and keep the applications open/running.



2. Press ***Close Window*** button to exit the RDP session.

3. Logout from VPN Session: Press ***Logout*** button on right top corner.

Following this procedure enables you to logon again without any issues.
If you need help consult your trainer or send an email to RadwareVirtualLAB@Radware.com.

Connect to the Device via Console (Serial) Connection

You can connect to your DefensePro lab device directly via a console connection.
This is the equivalent to a serial connection at any virtual appliance device.

1. Click **vDP Console** at MRemoteNG application.
   At MRemoteNG a new tab open. This is your vDP console window.
2. Move your curser in this window and click left mouse key to select.
   If there is no prompt visible, press ↵ several times until you see the DefensePro prompt.

TIP: The (>) symbol denotes you are NOT LOGGED IN.
After you are logged in, the prompt will change to (#) symbol.

Login To DefensePro (DP)

After establishing a serial connection with DefensePro, in the DefensePro prompt type:

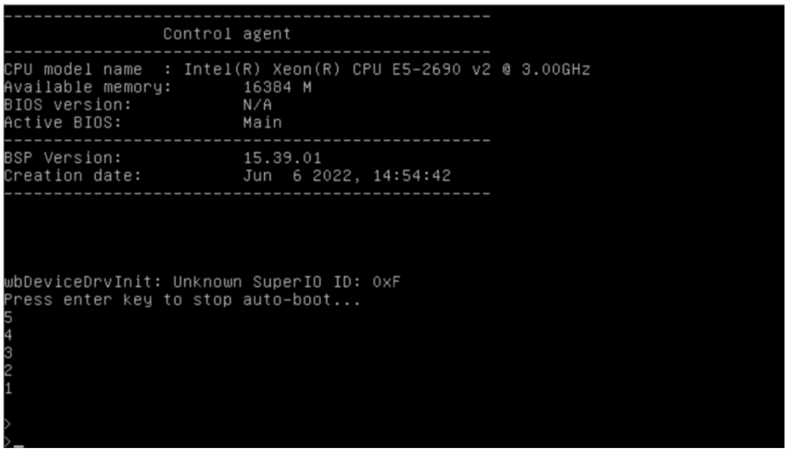
DefensePro> **login**
User: **radware** (*DefensePro's default username*)
Password: **radware1** (*our default password*)

When the **>** symbol changes to **#** symbol, it indicates that you are logged in.

Reset DefensePro to Factory Default

Initiate the reboot process to reset device to factory default.

1. In the DefensePro prompt, type:
   Type: **DefensePro# reboot**
2. When asked ***Are you sure you want to reboot***? type **y**
   The boot process will start running.
3. mRemoteNG will disconnect from the console. Please click **vDP Console** again to reconnect as soon as possible not to miss the next step.



```
-------------------------------------------------
                Control agent
-------------------------------------------------
CPU model name  : Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz
Available memory:       16384 M
BIOS version:           N/A
Active BIOS:            Main
-------------------------------------------------
BSP Version:            15.39.01
Creation date:          Jun  6 2022, 14:54:42
-------------------------------------------------



wbDeviceDrvInit: Unknown SuperIO ID: 0xF
Press enter key to stop auto-boot...
5
4
3
2
1

>
>_
```

4. When prompted with ***Press enter key to stop auto-boot …*** which appears shortly after ***Control agent*** lines, press↵ several times; note that have only 5 sec time to press the enter key.

Press **?** ↵ to display your options.

5. Type in ONLY **q1**
   Other input can destroy your vDP device!
6. When prompted with “***This action removes configuration f***ile***. Do you want to continue (y/n)***, type **y** ↵
7. Type @↵ to Continue the boot proccess

vDP will reboot and will display the ***Startup Configuration*** menu.

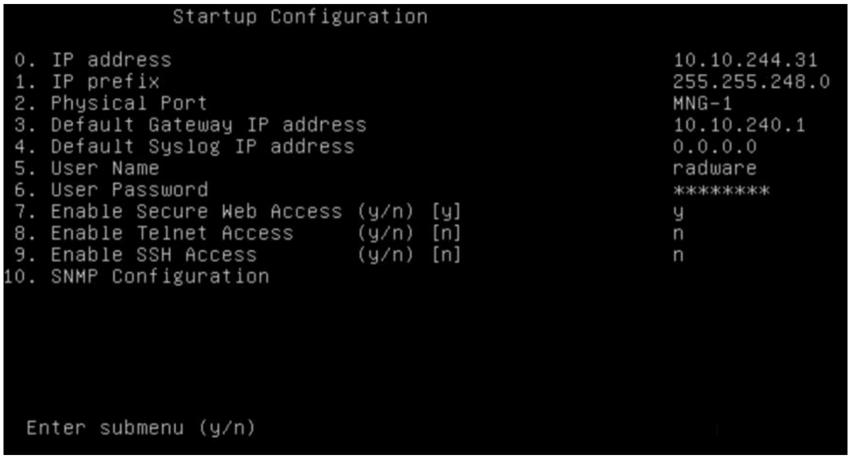
Startup Configuration Menu

This menu appears when a configuration file is deleted.
It remains on the screen for 60 seconds if you do not type any parameters.

1. Configure: **IP address, IP subnet mask, Physical Port, Default Gateway IP address**

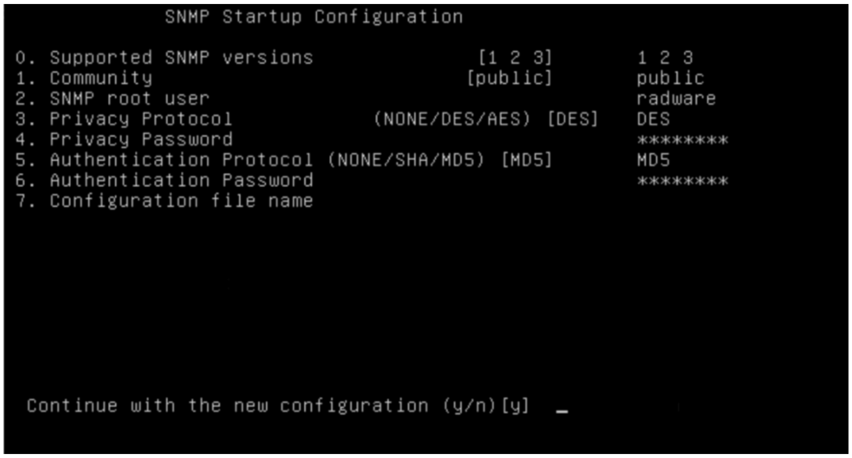
Parameters	
IP address	10.10.244.31
IP subnet mask	255.255.248.0
Physical Port	MNG-1
DefGateway IP addr	10.10.240.1

For all other fields keep the default values.
If you mistype a value, there is NO way to correct this value. In that case, type in an invalid value and press enter and you will return to the beginning of the line.



```
              Startup Configuration

 0. IP address                                       10.10.244.31
 1. IP prefix                                        255.255.248.0
 2. Physical Port                                    MNG-1
 3. Default Gateway IP address                       10.10.240.1
 4. Default Syslog IP address                        0.0.0.0
 5. User Name                                        radware
 6. User Password                                    ********
 7. Enable Secure Web Access (y/n) [y]               y
 8. Enable Telnet Access     (y/n) [n]               n
 9. Enable SSH Access        (y/n) [n]               n
10. SNMP Configuration




  Enter submenu (y/n)
```

After line 10, the SNMP menu is displayed. For this lab excerise, keep all default values, which match the configuration settings of other devices and of APSolute Vision at this lab.



```
              SNMP Startup Configuration

0. Supported SNMP versions              [1 2 3]       1 2 3
1. Community                           [public]       public
2. SNMP root user                                     radware
3. Privacy Protocol             (NONE/DES/AES) [DES]   DES
4. Privacy Password                                   ********
5. Authentication Protocol (NONE/SHA/MD5) [MD5]       MD5
6. Authentication Password                            ********
7. Configuration file name









 Continue with the new configuration (y/n)[y]  _
```

In a custom installation, you’ll need to adjust these values to your management device.

2. After line 7 of SNMP menu, press ↵ again to confirm all parameter by **y**es.
3. If you detect the wrong input in previous ***Startup Configuration***, type **n** ↵
4. You get at input of line 0. Press ↵ until you in wrong line.
5. Type the correct value and press ↵ until the prompt ***Enter submenu*** appears.
6. Type **n** ↵ otherwise SNMP Configuration appear again.
7. If you are satisfied, press ↵ again and vDP will reboot and load this configuration. Keep in mind mRemoteNG will disconnect, you will have to click on **vDP Console** again to connect.
   If you are not satisfied, type **n** ↵ to start ***Startup*** menu again.

Basic DefensePro Management

After reboot is complete and ports are loaded You are prompted to reset your password. Reset password to ***radware1***.
The only option to reset the password is by setting the configuration back to factory defaults.

1. Press ↵ to get DefensePro prompt.

Parameters	
User Name	radware (*DP default username*)
Password	**radware1** (*our default password*)

2. At the **DefensePro>** prompt, type login
3. Type user name
4. Type password
5. To display all DefensePro’s available commands, type **?**.
6. To display information on a specific command (ie. ping), type ***ping ?*** (DefensePro# *ping ?*)
7. You can browse through DefensePro CLI commands. (optional)
8. To verify management IP address, type: DefensePro# ***net ip-interface***
   All configured IP addresses for the management network will be displayed.
9. If you do not like the frame displayed arround output parameters, turn it off by typing:
   DefensePro# **manage terminal grid-mode set disable**
10. To verify basic connectivity for APSolute Vision server, type: DefensePro# ***ping 10.10.240.15***

Leave DefensePro connected to the CLI. Error messages and traps generated through
the CLI can be helpful to review when troubleshooting

12. Manage Other Elements Using CLI.
    To add an additional user, type:
    DefensePro# **manage user table create Team31 -pw radware1**
13. (Optional) Try changing password to your Team31
    DefensePro# **manage user table set Team31 –pw radware2**
14. To change prompt to display an individual string, type:
    DefensePro# **manage terminal prompt set DP-TeamXX** (where XX are your initials)

Keep in mind you can expand incomplete command string by pressing <TAB> key.

15. To enable SSH connect, type :
    Team31# **manage ssh status set 1**

You can type 1 or enable, or type 2 or disable.

16. To open an SSH session to your DP:
    Double click the **vDP-SSH** icon to open a SSH connection to the device:
    Be aware timeout is 10 sec. Therfore type quickly the username and password.

17. When prompted, type username and password:
    - login as: radware
    - radware@10.10.244.31’s password: radware1

You should be able to repeat the same commands as already practiced on your DefensePro device such as net ip-interface.

By default, only the serial session displays event traps.
You can enable output also on SSH sessions.
Team31# **manage terminal traps-output set 2** default 1 normal (serial only); 2 on (every CLI interface); 3 off

It’s up to you to decide which session from this point on to use (console or ssh).

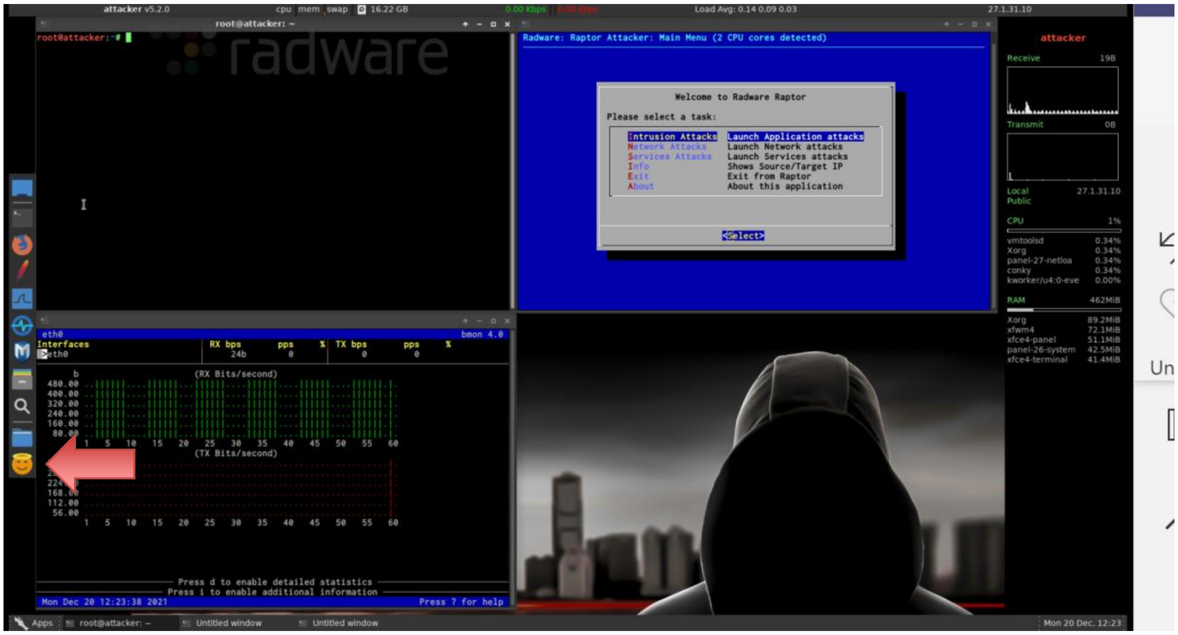
Connect To Other Lab Devices

Connect to Attacker PC

Your Attacker-Client uses Radware's Raptor Attack Bot to inflict artificial attacks on your assigned DefensePro device during these lab exercises.
Use **Attacker** icon at mRemoteNG to open a VNC viewer session to your Attacker-Client.
You will see three windows:

- one runing the Raptor attack tool
- one displays incomming and outgoing traffic at Ethernet connection
- one terminal to run your own attacks or allowing you to start the war games (only available for advanced classes)

If you mistakenly close any window, click on the “angel” icon on the bottom of left side icon tray.



```
root@attacker:~#
```

```
Radware: Raptor Attacker: Main Menu (2 CPU cores detected)

              Welcome to Radware Raptor

 Please select a task:

     Intrusion Attacks   Launch Application attacks
     Network Attacks     Launch Network attacks
     Services Attacks    Launch Services attacks
     Info                Shows Source/Target IP
     Exit                Exit from Raptor
     About               About this application

                      <Select>
```

```
 eth0                                                       bmon 4.0
Interfaces                RX bps       pps     %  TX bps       pps     %
 >eth0                       24b         0            0          0

         b                (RX Bits/second)
    480.00
    400.00
    320.00
    240.00
    160.00
     80.00
           1   5   10   15   20   25   30   35   40   45   50   55   60
                          (TX Bits/second)
    224.00
    168.00
    112.00
     56.00
           1   5   10   15   20   25   30   35   40   45   50   55   60

                Press d to enable detailed statistics
               Press i to enable additional information
 Mon Dec 20 12:23:38 2021                                Press ? for help
```

```
attacker
Receive               19B
Transmit               0B
Local          27.1.31.10
Public
CPU                    1%
vmtoolsd            0.34%
Xorg                0.34%
panel-27-netloa     0.34%
conky               0.34%
kworker/u4:0-eve    0.00%
RAM                462MiB
Xorg              89.2MiB
xfwm4             72.1MiB
xfce4-panel       51.1MiB
panel-26-system   42.5MiB
xfce4-terminal    41.4MiB
```

Connect to Legitimate Client PC

Legitimate User-PC is the machine used to generate legitimate traffic on your DefensePro device during these lab exercises. Use the **Legit Client** icon at MRemoteNG to open a VNC viewer session to your Legitimate Client.
A common task on the legit client is to start Firefox to browse to the Target Server.
You will see three windows:

- one displays incomming and outgoing traffic at Ethernet connection
- one terminal for your own commands
- jMeter with a predefined configuration to generate legitimate background traffic. To start the traffic click on the green arrow (▶)

If you mistakenly close any window, click on the “angel” icon on the bottom of left side icon tray.

Connect to Target Server

The target server is the destination of all legitimate and attack traffic. Use **Target Server** icon at MRemoteNG to open a VNC viewer session to your Target Server machine.
You will see three windows:

- one displays incomming and outgoing traffic at Ethernet connection
- one running iptraf-ng showing the packets arriving at the server
- one terminal for your own commands

If you mistakenly close any window, click on the “angel” icon on the bottom of left side icon tray.

Using APSolute Vision to Manage DefensePro

Overview

APSolute Vision™ offers a centralized attack management, monitoring and reporting solution across multiple DefensePro devices and locations. Vision provides the user realtime identification, prioritization and response to policy breaches, cyber attacks and insider threats.

In this exercise you'll manage DefensePro using APSolute Vision.

Set APSolute Vision NTP Parameters

Check that Vision is using NTP server to ensure that the PC, DefensePro and Vision are synced.

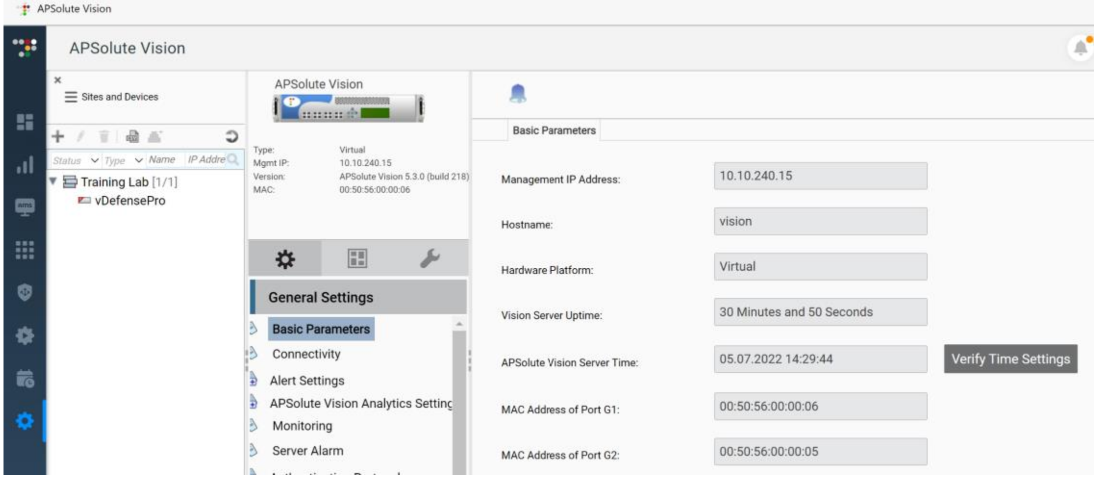
1. Login to Vision (10.10.240.15) via SSH; credentials: *radware / radware*.
2. If there is no SSH existing connection on mRemoteNG, create a new SSH connection to 10.10.240.15.
3. Use the command: ***system ntp servers get*** to see if a server is defined.
   If no server is defined, use this command: ***system ntp servers add*** **< server IP address>** to define the server, lab server IP address is 10.10.240.1. Answer yes on the restarting services if asked.
4. If you restarted the services in above step you don't need to perform this, otherwise use ***system ntp service restart*** to restart the NTP service.
   At the prompt asking if you want to restart APSolute Vision services, select **Y**.
   NOTE: In a production environment you will only need to start the service.
5. Check to make sure all services are started and healthy. Issue a command **system vision-server status**. If any service is still in **"(health: starting)"** mode, wait a few minutes and issue the command again. Services should be in **"(healthy)"** status (or not labeled).

Connect to APSolute Vision

1. Open the web browser and securely connect to the APSolute Vision server.
   Browser is already preconfigured with a shortcut to the Vision server. In case needed, type the URL **https://*vision.radware.net/***
2. If a security screen appears, click to continue to Radware server. By default a self signed certificate is used.
3. Log in using the APSolute Vision splash-screen.   UserName: **radware**   Password: **radware**
   If Vision asks you to change password, please use **radware1**.

4. Select Vision server, this is the gear icon ⚙ at left side labeled as Configuration.

5. Verify that your PC and Vision clocks are Syncronized: Select the tab **System → General Settings → Basic Parameters → APSolute Vision Server Time →** press **Verify Time settings**. You should get: The APSOlute Vision server and the local PC date and time settings are synchronized



Type: Virtual
Mgmt IP: 10.10.240.15
Version: APSolute Vision 5.3.0 (build 218)
MAC: 00:50:56:00:00:06

Management IP Address: 10.10.240.15
Hostname: vision
Hardware Platform: Virtual
Vision Server Uptime: 30 Minutes and 50 Seconds
APSolute Vision Server Time: 05.07.2022 14:29:44
MAC Address of Port G1: 00:50:56:00:00:06
MAC Address of Port G2: 00:50:56:00:00:05

6. In Sites and Devices tab (on left): click on (select/Highlight) your vDefensePro device.

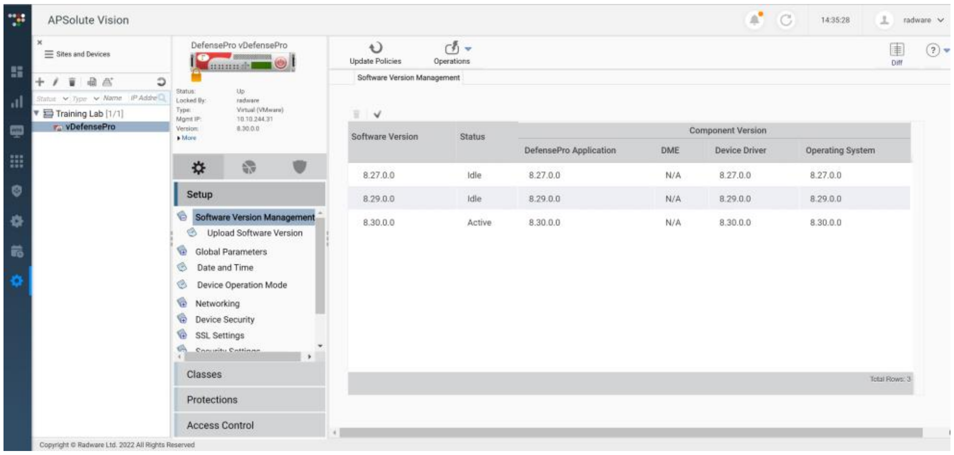
Use Vision to Configure DefensePro.

⚠ If your DefensePro Device is not visible, notify your instructor or Radware Lab Tech.
Beware -- avoid deleting your Vision device.
DO NOT DELETE YOUR DEVICE from APSolute Vision.
DO NOT SHUT DOWN YOUR DEVICE. Only a virtual lab admin can start it again.

7. Lock your DefensePro device by clicking LOCK icon.
8. Locking DefensePro prevents other users from making configuration changes during your session.

You may lock/unlock the DP device by clicking on the lock (toggle) icon. 🔓 > 🔒
Default is unlock, this is read only for all parameters.

Be sure your device is locked. The DefensePro device MUST be locked to make configuration changes.



Status: Up
Locked By: radware
Type: Virtual (VMware)
Mgmt IP: 10.10.244.31
Version: 8.30.0.0

Software Version	Status	Component Version			
		DefensePro Application	DME	Device Driver	Operating System
8.27.0.0	Idle	8.27.0.0	N/A	8.27.0.0	8.27.0.0
8.29.0.0	Idle	8.29.0.0	N/A	8.29.0.0	8.29.0.0
8.30.0.0	Active	8.30.0.0	N/A	8.30.0.0	8.30.0.0

Unlocking "radware" User

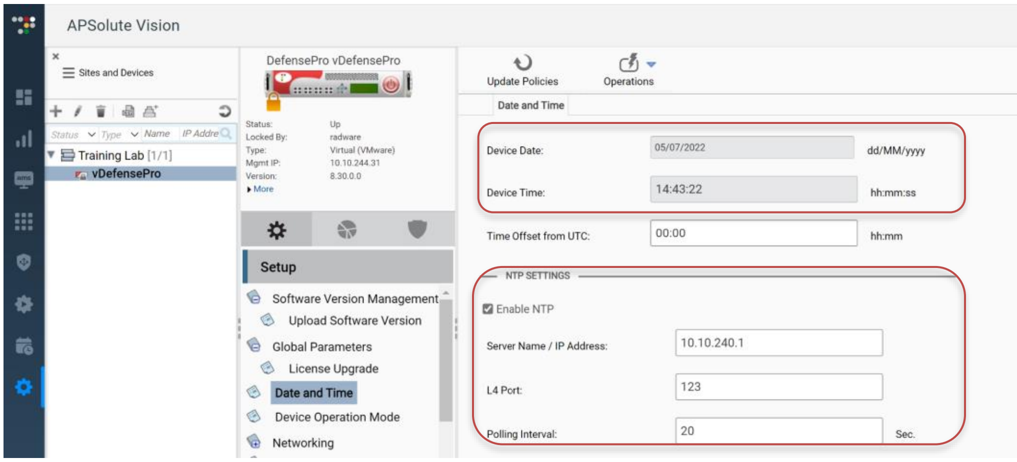
If the **radware** user becomes locked, there are several ways to unlock the user.
To unlock the radware user:

- Use another username with Administrator role to login to APSolute Vision WebUI and unlock the **radware** user.
- If it is not possible to log in to APSolute Vision WebUI, then use the root user to log in via ssh and execute the **restore_radware_user_password** command to recover the **radware** user.
- If both above suggested method are not possible, use the VM administrator to login as **root** via direct console and execute the **restore_radware_user_password** command.

Set DefensePro Date and NTP Parameters

1. Select the **Configuration** perspective. ⚙
2. In the **Setup** section, scroll down and select **Date and Time** in the navigation tree.
3. Verify that NTP is not enabled. If it is enabled unselect the check box and click **submit** botton to save.

4. Change the device date for today date, set current time and click **Submit**. If the time different is more than 24 hours, sync will not work propperly.
5. Configure NTP settings:
    a. Check the “Enable NTP”.
    b. Configure **Server Name / IP address** as: 10.10.240.1 L4 Port: 123 for training reduce polling interval to 20 seconds.
6. Click **Submit** button to save changes.



Status: Up
Locked By: radware
Type: Virtual (VMware)
Mgmt IP: 10.10.244.31
Version: 8.30.0.0

Device Date: 05/07/2022 dd/MM/yyyy
Device Time: 14:43:22 hh:mm:ss
Time Offset from UTC: 00:00 hh:mm

☑ Enable NTP
Server Name / IP Address: 10.10.240.1
L4 Port: 123
Polling Interval: 20 Sec.

Enable Vision Security Reporting

1. Select the **Configuration** perspective.
2. In the **Setup** section, scroll down to select **Reporting Settings → Advanced Reporting Settings** in navigation tree.
3. In **Security Reporting Parameters**, enable sending security traps to serial and SSH port

- **Enable Sending Terminal Echo**: check checkbox, Minimal Risk Level for Sending Terminal Echo: **Info**

- **Enable Security Logging**: check checkbox

4. Click **Submit** button to save changes.

CLI commands are also available to Enable all Vision Security Reporting settings. These are not covered here.

Register DefensePro for Security Reporting

1. In **Sites and Devices** (tree view - left side), select the DefensePro device to be registered. **vDefensePro** Locking is not required for device registration.
2. In **Sites and Devices** click ***Edit*** (pencil) button to edit ***Device Propeties***.
3. In **Device Properties** window click ***Event Notification***
4. Make sure select both checkboxes ***Register This*** … and ***Remove All…*** and double check APSolute Vision register on G1 (10.10.240.15)
5. Click **Submit** button to save changes.
6. Go to **Configuration → Setup → Device Security → SNMP → Target Address** and double click "Vision-V3-10.10.240.15" entry (or select entry and click **Edit** (pencil) icon. Set **Minimal Risk Level for Sending Traps: Info.**
7. Click **Submit** and confirm **Yes** when asked to continue.

Additional Reporting Options

Packet Reporting

Packet reporting specifies whether the DefensePro device sends sampled attack packets along with the attack event information to Vision.

1. Select the **Configuration** perspective
2. In the **Setup** section, select **Reporting Settings** and then **Advanced Reporting**
3. Select **Packet Reporting** section
4. Chec the **Enable Packet Reporting** checkbox
5. Destination IP Address: **10.10.240.15**
6. Click the **Submit** button to accept configuration changes in **Advanced Reporting Settings** tab.

Enable Syslog Reporting

1. Select the **Configuration** perspective
2. In **Setup** section, select **Reporting Settings** and then **Syslog** in navigation tree.
3. Use your **3CD** application at RDP Client for Syslog Server.
4. Double check **Enable Syslog** checkbox (Hint: Be sure to LOCK your device.)
5. Click to Add Syslog Server, in Add New Syslog Server tab at Syslog Server: **10.10.240.1**
6. Double check default: Source Port: 514 and Destination Port: 514 and Facility: Local Use 6.
7. Set the **Reporting Format** to either **BSD** (legacy DefensePro format) or **IETF (RFC 5424)** (new format).
8. Set **Minimal Risk Level for Sending Messages: Info**.
9. Click **Submit** button to save changes.

Setup Attack Protection

Configure Classes

Classes definition is always an association between a name and parameter for Networks or Context Groups (VLAN) or Application Ports or Physical Ports.

Setup a Protected Network

1. Select the **Configuration** perspective
2. In the **Classes** section, click ***Networks*** in navigation tree
3. In **Networks** tab click **+** to ***Add*** Network in Add Network tab.
4. Type Network Name: **TeamXX** (where XX are your initials)
5. Click to **Add** Network Group
6. Enter for Network Address: **27.1.0.0** and for Mask: **255.255.0.0** (you can also use CIDR mask notation as **16**).
7. Click **Submit** button to accept configuration for Add Network Group.
8. Click **Close** button.

Create Protection Policy

A policy is used to provide protection to the networks defined in it's classification.

1. Select the **Configuration** perspective
2. In the **Protections** section, click **Protection Policies**.
3. In **Add New Protection Policy** tab:
   - Check the **Enabled** checkbox.
   - For **Policy Name** type: **TeamXX** (where XX are your initials)
   - For **Priority** type: **10**
   - For **SRC Network** select: ***any***
   - For **DST Network** select: ***TeamXX***.
   - For **Port Group** leave: (blank)
   - For **Direction** select: ***One Way***
4. Click **Submit** button to accept configuration in Add Protection Policy.
5. Click on **Update Policies Required** in the menu above the protection policies.

Note: At this time we are only defining the classification and no protection profiles are associated with the specific policy.

Save this basic configuration.

You will need restoring it later for other configuration setup.

1. At APSolute Vision, above policy setup select **Operations**, **Export Configuration File**:
   - For **Destination** select: ***Client***
   - Check the **Include Private Keys** checkbox
   - For **Passphrase** type: ***radware***
   - For **Confirm Passphrase** type: ***radware***
   - Press **OK** button
   - A dialog box open, how to handle this file.
   - Select **Save File** and click **OK**
   - *Click **Save** button*
   - After you saved the file change the file name: ***dp8-BasicLab-config.txt***

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