



DefensePro X
Version 10.x

Training Lab Manual Initial Setup

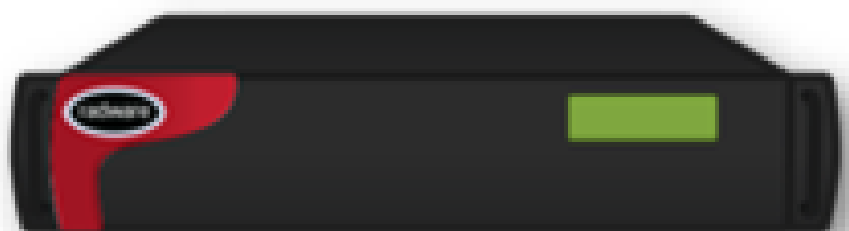


Table of Contents

Contents

INTRODUCTION.....	4
ICONS IN THIS DOCUMENT:	4
LAB ENVIRONMENT	4
REQUIRED TOOLS & EQUIPMENT	4
LAB LAYOUT	5
CONNECT TO THE DEVICE VIA YOUR LOCAL WORKSTATION.....	6
CONNECT TO SSL-VPN	6
LOGIN AT SSL- VPN	7
USE DESKTOP ICONS.....	8
END SESSION.....	9
CONNECT TO THE DEVICE VIA CONSOLE CONNECTION.....	10
LOGIN To DEFENSEPRO (DP).....	10
RESET DEFENSEPRO TO FACTORY DEFAULT	11
STARTUP CONFIGURATION MENU	12
BASIC DEFENSEPRO MANAGEMENT	13
CONNECT TO OTHER LAB DEVICES.....	15
CONNECT TO ATTACKER PC	15
CONNECT TO LEGITIMATE CLIENT PC.....	15
CONNECT TO TARGET SERVER	15
USING CYBER CONTROLLER TO MANAGE DEFENSEPRO X	16
OVERVIEW	16
SET CYBER CONTROLLER NTP PARAMETERS (OPTIONAL).....	16
CONNECT TO CYBER CONTROLLER	16
ADD DEFENSE PRO X DEVICE TO THE CYBER CONTROLLER	17
USE CYBER CONTROLLER TO CONFIGURE DEFENSEPRO X.....	18
SET DEFENSEPRO X DATE AND NTP PARAMETERS	18
ENABLE CYBER CONTROLLER SECURITY REPORTING	19
ADDITIONAL REPORTING OPTIONS.....	19
Packet Reporting	19
Enable Syslog Reporting	19

Change SNMP Reporting	19
SETUP ATTACK PROTECTION	20
CONFIGURE SECURITY POLICY VIA POLICY EDITOR	20
REVIEW SECURITY POLICY VIA DEVICE SETTINGS	22
SAVE THIS BASIC CONFIGURATION.	23

Introduction

The **DefensePro X** 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 X and virtual DefensePro installations.

The features and functions of Radware's DefensePro devices in this document are based on:

- DefensePro 10.7.0
- Cyber Controller 10.7.0.

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:



How to perform an activity using CLI



How to perform an activity using Cyber Controller interface

Lab Environment

This lab kit consists of:

- A DefensePro X VA instance
- An attacker based on Kali Linux
- A legitimate client based on Kali Linux
- A target server based on Kali Linux

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 using SSL VPN to one of our training 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.

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 X, Attacker, Legitimate Client and Cyber Controller 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.

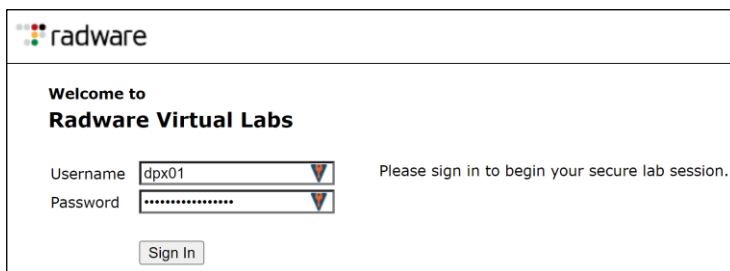
Remember: All sessions we need for the lab (browser, VNC, SSH) are started within the browser you open for this SSL VPN session. For example, don't get confused having a Firefox session within your Firefox browser . Always select the application within your local browser. The advantage is, we use only 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 Radware (example: dpx12)
Password	Provided by Radware (example: Radware59)

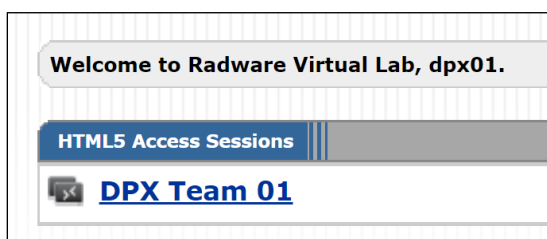
Login at SSL- VPN

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

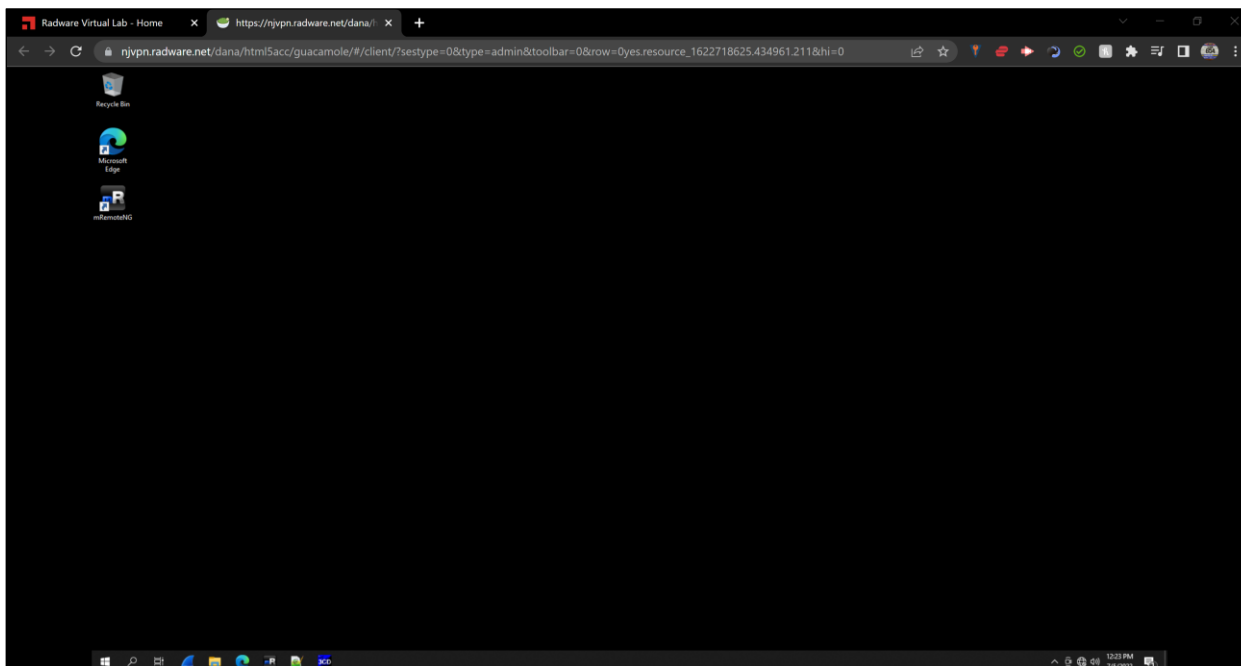


The login form for Radware Virtual Labs. It features the Radware logo at the top left. Below it, the text "Welcome to Radware Virtual Labs" is displayed. There are two input fields: "Username" with the value "dpx01" and "Password" with masked characters. To the right of the password field, the text "Please sign in to begin your secure lab session." is shown. A "Sign In" button is located at the bottom center of the form.

2. Press  or press the **Sign In** button.
3. Press the **vDP Team XX** hyperlink to connect RDP client (example: DPX Team 01)



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.

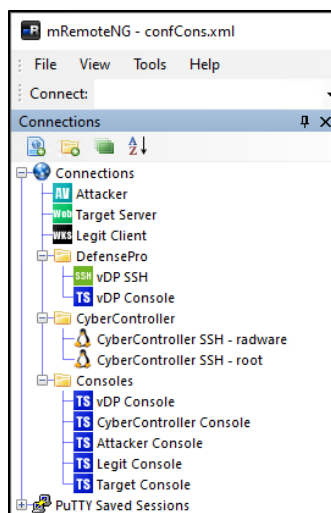


Use Desktop Icons

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.

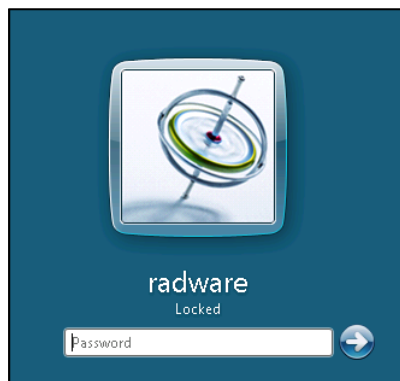


- **Attacker** generates attack traffic to be detected by a DefensePro X policy
- **Legitimate Client** generates legitimate traffic allowed by a DefensePro X policy
- **Target Server** enables monitoring traffic on in and out of a web server
- **vDP Console** is a Console (VMware Remote Console) Direct connection, IP address independent, to virtual DefensePro X (VA) Lab Device
- **vDP SSH** is a connection to a virtual DefensePro X (VA) Lab Device via MNG-1 port using SSH protocol
- **Cyber Controller SSH**, is a connection to the central management station. There are two connections, one for username **radware**, and one for username **root**.
- **Consoles** is a collection of links to VMware Remote Consoles of all virtual appliances in case you need to reboot, or power on/off devices. *Since we use VNC to connect to the Attacker, Legit Client and Target Server, these remote consoles are only useable to power-off/on or reboot.*

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

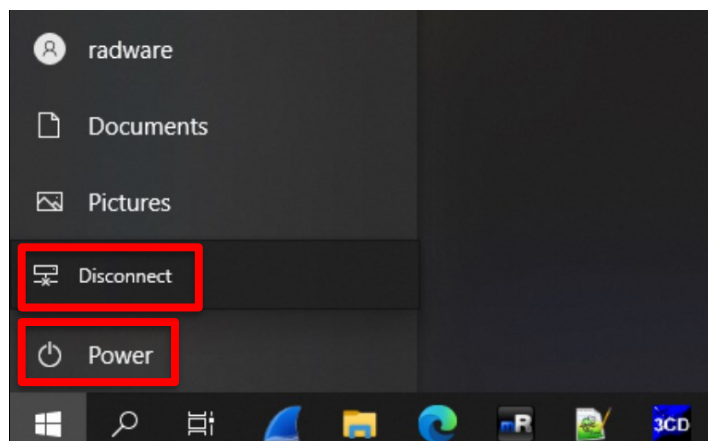


If you get locked out from your remote desktop windows session, after a break etc, the login password is **radware**.



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.

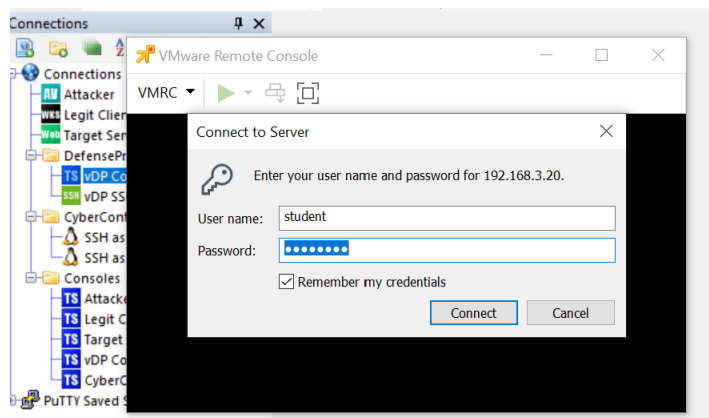
If you need help consult your trainer or send an email to RadwareVirtualLAB@Radware.com.

Connect to the Device via Console 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 window will open. This is your vDP X console window.
2. Click Connect to confirm credentials to open VMRC. (student / radware1!)



3. Move your cursor in this window and click left mouse key to select. If there is no prompt visible, press **↵** several times until you see the **vDP-X** prompt.
4. To return from the console press **Ctrl-Alt** to release VMRC cursor lock.

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 console connection with DefensePro X,

In the vDP-X prompt type **login**

User: **radware** (DefensePro's default username)

Password: **radware1** (our default password)

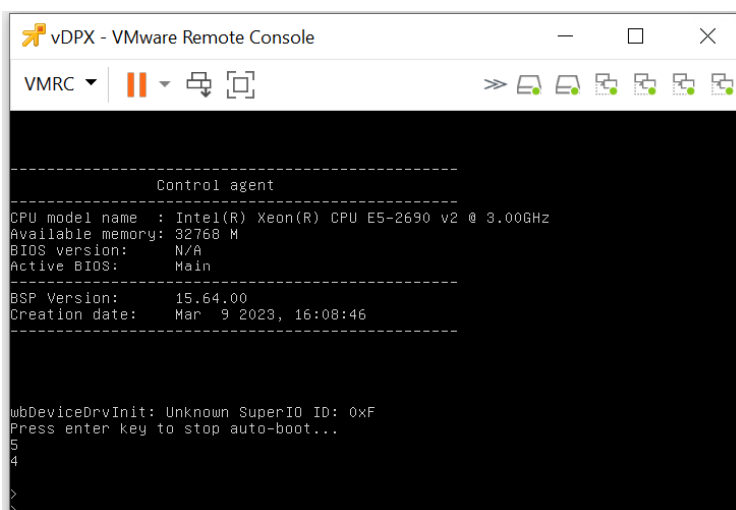


When the > symbol changes to # symbol, it indicates that you are logged in.

Reset DefensePro to Factory Default

Initiate the reboot process to reset device to factory default.

1. In the vDP-X prompt, type: **reboot**
vDP-X# reboot
2. When asked **Are you sure you want to reboot? (y/n) [n]** type **y**
The boot process will start running.
3. 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.**



```

vDPX - VMware Remote Console
VMRC
-----
Control agent
CPU model name : Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz
Available memory: 32768 M
BIOS version: N/A
Active BIOS: Main
-----
BSP Version: 15.64.00
Creation date: Mar 9 2023, 16:08:46
-----
usbDeviceDrvInit: Unknown SuperIO ID: 0xF
Press enter key to stop auto-boot...
5
4
>
>
  
```

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

4. Type in **ONLY q1 ↵**
5. When prompted with **"This action removes configuration file. Do you want to continue (y/n)?**, type **y ↵**
6. Type **@↵** to Continue the boot process

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

Startup Configuration Menu

The below settings are the one to be configured, all other settings keep the defaults.

Parameters	
IP	10.10.244.31
Mask (IP prefix)	255.255.248.0
Gateway	10.10.240.1
Physical port (Management)	MNG-1 (or just press ↵)
User Name	radware
User Password	radware1
Enable Web Access	y
Enable SSH Access	y

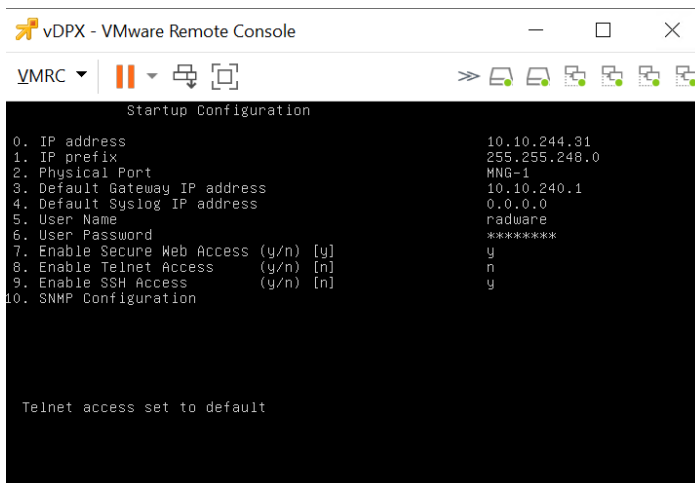
This menu appears when a configuration file is deleted.

It remains on the screen for 60 seconds if you do not type any parameters.

Please don't use numerical keypad.

1. Configure: **IP address, IP subnet mask, Physical Port, Default Gateway IP address, and Enable SSH Access.** 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.



```

vDPX - VMware Remote Console
VMRC
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             radware1
7. Enable Secure Web Access (y/n) [y] y
8. Enable Telnet Access (y/n) [n] n
9. Enable SSH Access (y/n) [n] y
10. SNMP Configuration

Telnet access set to default
  
```

After line 10, the SNMP menu is displayed. For this lab exercise, **keep all default values at the SNMP settings**, which match the configuration settings of the Cyber Controller 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 with **yes**.
3. If you detect the wrong input in previous **Startup Configuration**, type **n ↵**
4. You get at input of line 0. Press **↵** until you are 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.
8. If you are not satisfied, type **n ↵** to start **Startup** menu again.

Basic DefensePro Management



After reboot is complete and ports are loaded.

1. You are prompted to change your password. Reset password to **radware1** since the default password (radware) is not allowed anymore. The only option to reset the forgotten password is by setting the configuration back to factory defaults
2. Press **↵** to get DefensePro prompt
3. At the **DefensePro>** prompt, type **login**

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

4. Type user name **radware**
5. Type password **radware1**
6. To display all DefensePro's available commands, type **?**.
7. To display information on a specific command (ie. ping), type **ping help** (DefensePro# ping help)
8. You can browse through DefensePro CLI commands. (optional)
9. To verify management IP address, type: DefensePro# **net ip-interface**
All configured IP addresses for the management network will be displayed.
10. If you do not like the frame displayed around output parameters, turn it off by typing:
DefensePro# **manage terminal grid-mode set disable**

11. To verify basic connectivity to Cyber Controller, 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 teamXX -pw radware11** where XX are your initials)
13. (Optional) Try changing password to your teamXX
DefensePro# **manage user table set teamXX -pw radware22**
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. If you didn't enable SSH in initial configuration menu, please enable SSH connect, type :
DP-TeamXX# **manage ssh status set enable**



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

16. To open an SSH session to your DP:
In mRemtoeNG Double click the **vDP SSH** icon to open a SSH connection to the device:
Be aware timeout is 10 sec. Therefore type quickly the username and password. For your convenience the mRemoteNG already has credentials preconfigured to **radware/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.

DP-TeamXX# **manage terminal traps-output set on** 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 target 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 running the **Raptor** attack tool (blue background)
- one displays incoming 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, or reboot the attacker.




Connect to Legitimate Client PC

Legitimate User-PC is the machine used to generate legitimate traffic through 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 incoming 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, or reboot.

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 incoming 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, or reboot.

Using Cyber Controller to Manage DefensePro X

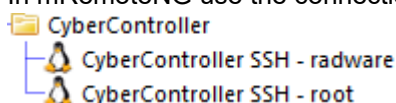
Overview

Cyber Controller offers a centralized attack management, monitoring and reporting solution across multiple DefensePro and DefenseProX devices and locations. Cyber Controller provides the user realtime identification, prioritization and response to policy breaches, cyber attacks and insider threats. In this exercise you'll manage the DefenseProX using the Cyber Controller.

Set Cyber Controller NTP Parameters (optional)


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

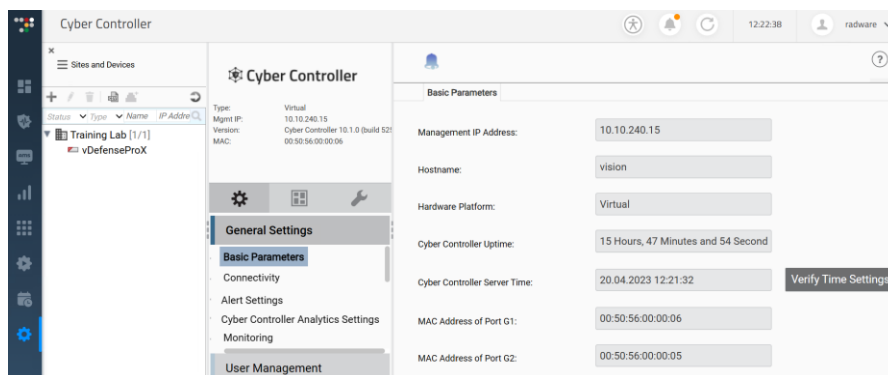
1. In mRemoteNG use the connection to Cyber Controller SSH as radware (first option)



2. Use the command: **system ntp servers get** to see if a server is defined.
3. Use **system ntp service status** to check the NTP service. It should say NTP service is running and reaches NTP server 10.10.240.1
4. If not, please look at the **Troubleshooting Aide** manual included in your lab manuals folder.

Connect to Cyber Controller

1. Open the Edge web browser and securely connect to the Cyber Controller server. Browser is already preconfigured with a shortcut to the Cyber Controller server. In case needed, type the URL **https://cybercontroller.radware.lab/**
2. If a security screen appears, click to continue to Radware server. By default a self signed certificate is used. In our lab we have lab CA signed certificate uploaded to the Cyber Controller.
3. Log in using the Cyber Controller splash-screen. UserName: **radware** Password: **radware**
If Cyber Controller asks you to change password, please use **radware1**, or see the **Troubleshooting Aide** manual how to reset the radware user password on the Cyber Controller.
4. Select Cyber Controller server, this is the gear icon  at left side labeled as **Configuration**.
5. Verify that your PC and Cyber Controller clocks are Synchronized: Select the tab **System** → **General Settings** → **Basic Parameters** → **Cyber Controller Server Time** → press **Verify Time settings**. You should get: The Cyber Controller server and the local PC date and time settings are synchronized. If not, use **Troubleshooting Aide** manual to resolve.



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

Add Defense Pro X device to the Cyber controller

In our lab DefensePro X is already added to the Cyber Controller.

However we will going to remove it and go through the steps to add it.

1. Click on the vDefensePro X device to select it.
2. Click on the **Trash Can** icon.
3. When asked for confirmation on the question "**The device will be deleted. Continue?**" Please click **Yes**.
4. Select **Training Lab** site.
5. Click on Plus sign.
6. Fill in the following information:
 - a. Type: **DefensePro**
 - b. Name: **vDefenseProX**
 - c. **SNMP** tab
 - i. Management IP: **10.10.244.31**
 - ii. SNMP Version: **SNMPv3**
 - iii. User Name: **radware**
 - iv. Select **Use Authentication**
 - v. Authentication Protocol: **MD5**
 - vi. Authentication Password: **radware**
 - vii. Select **Use Privacy**
 - viii. Privacy Protocol: **DES**
 - ix. Privacy Password: **radware**
 - x. NOTE: If you selected different SNMP settings in the initial DefensePro X configuration, use those settings.
 - d. **HTTP/S Access** tab
 - i. Uncheck **Verify HTTP Access**
 - ii. Check **Verify HTTPS Access**
 - iii. User name: **radware**
 - iv. Password: **radware1**
 - v. HTTP Port: **80**
 - vi. HTTPS port **443**
 - e. **SSH Access** tab
 - i. User Name: **radware**
 - ii. Password: **radware1**
 - iii. SSH Port: **22**
 - f. Event Notification tab
 - i. Check **Register This Cyber Controller Server for Device Events**
 - ii. Register Cyber Controller Server IP: **G1 (10.10.240.15)**
 - iii. Check **Remove All Other Targets of Device Events**
7. Click **Submit**
8. Cyber Controller should display: **M_01093: The Request has succeeded**
9. If you used different credentials during the Defense Pro X initial setup, please use those.

Use Cyber Controller to Configure DefensePro X.

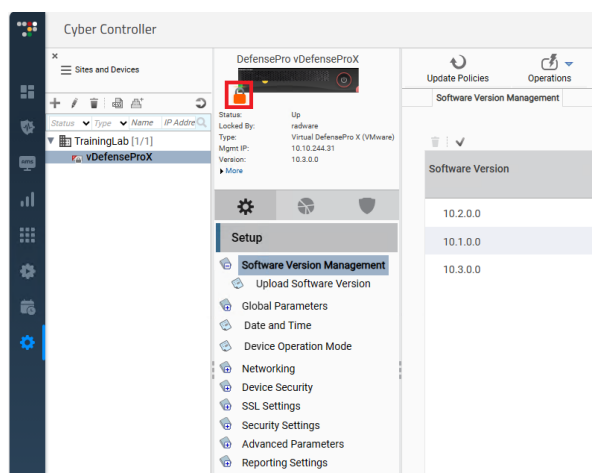


DO NOT SHUT DOWN YOUR DEVICE. You will need to use DefensePro X VMRC to power it on via mRemoteNG.

1. Lock your DefensePro X device by clicking LOCK icon.
2. Locking DefensePro X prevents other users from making configuration changes during your session.

You may lock/unlock the DP device by clicking on the lock (toggle) icon.

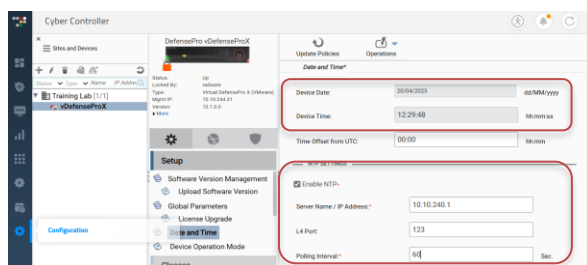
Default is unlock, this is read only for all parameters.



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

Set DefensePro X 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** button 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 properly.
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 60 seconds.
6. Click **Submit** button to save changes.



Enable Cyber Controller 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 Cyber Security Security Reporting settings. These are not covered here.

Additional Reporting Options

Packet Reporting

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

1. Select the **Configuration** perspective
2. In the **Setup** section, select **Reporting Settings** and then **Advanced Reporting**
3. Select **Packet Reporting** section
4. Check 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. In vDefenseProX, 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.

Change SNMP Reporting

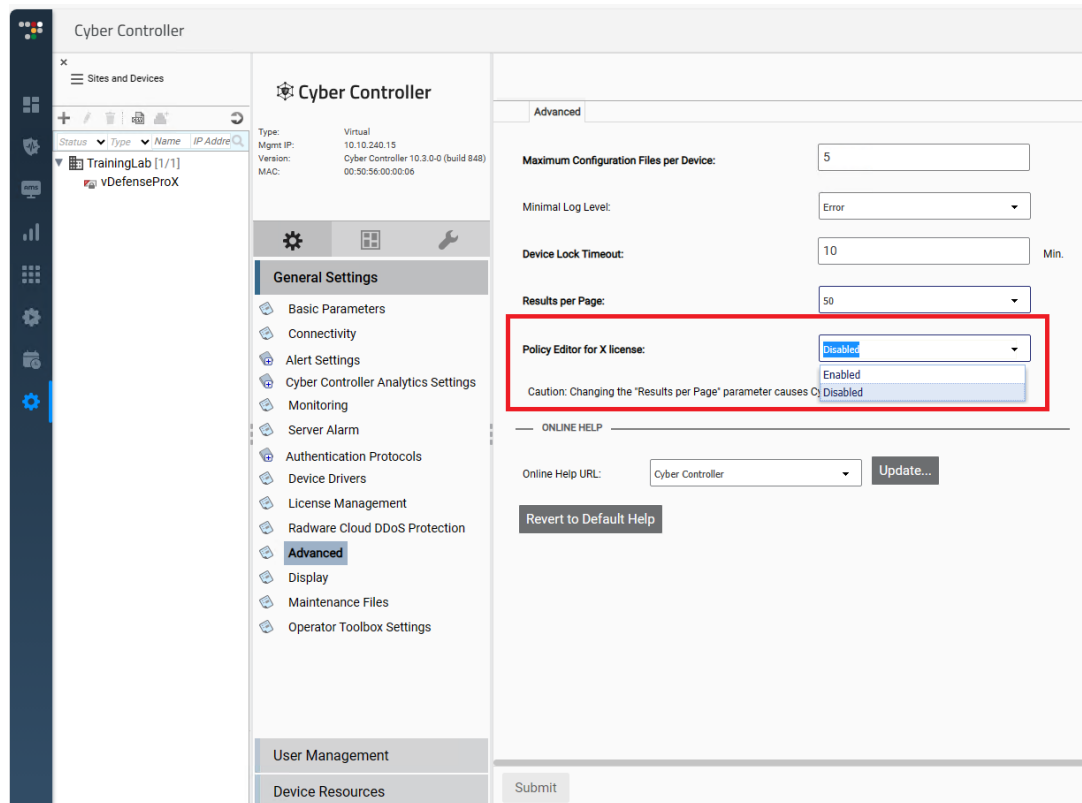
1. Go to **Configuration** → **Setup** → **Device Security** → **SNMP** → **Target Address** and double click "Vision-V3-10.10.240.15" entry (or select entry and click **Edit** (pencil) icon. Set **Minimal Risk Level for Sending Traps**: **Info**.
2. Click **Submit** and confirm **Yes** when asked to continue.

Setup Attack Protection

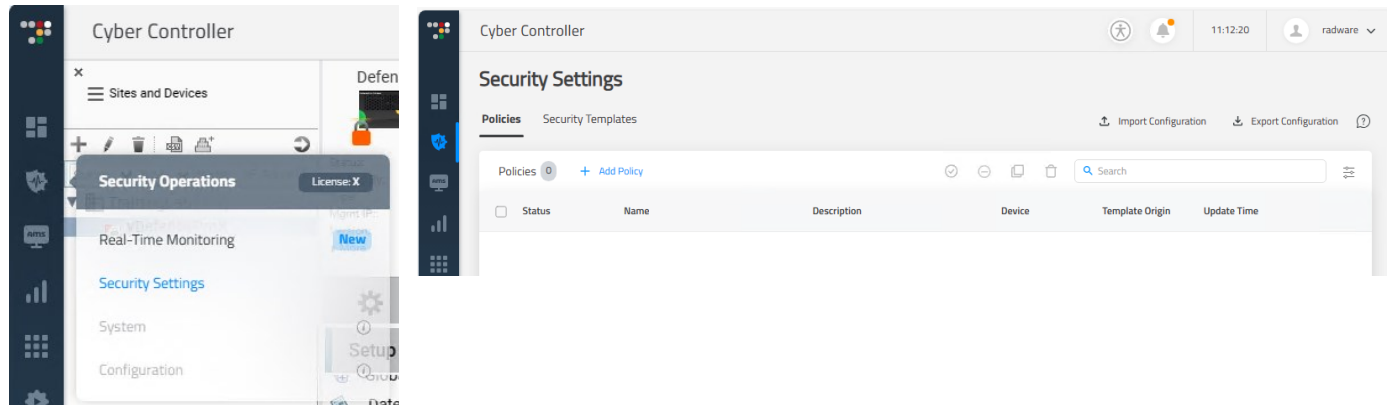
Configure Security Policy via Policy Editor

Cyber Controller for DefensePro X introduces a new way of configuring the DefenseProX using the so called policy editor.

Go to the Cyber Controller settings > General Settings > Advanced and set the Policy Editor for X license to **enabled** and click **Submit**



Uses **Security Operations** area to configure **Security Settings** like the protection policies.



Click on “+ Add Policy” and use this information:

Policy Name	TeamXX (exchange XX with your initials like JD)
Device	vDefenseProX
Description	DefenseProX Level 1 Class
Network Table → Network Address	27.1.0.0
Network Table → Prefix	16
Security Policy → Priority	10
Security Policy → Template	Basic-Global-10.6.0.0
Protection Settings	Disable all protections

Once you configured click on **Submit**.

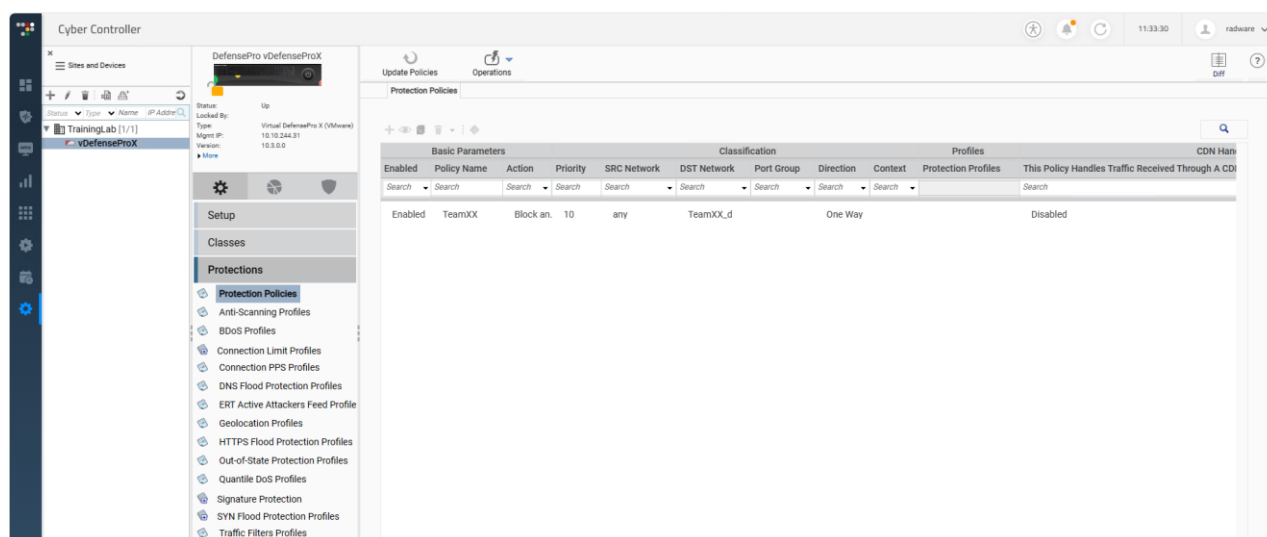
Note: At this time we are only defining the classification and no protection profiles are associated with the specific policy because we'll enable various protections step by step.

Review Security Policy via Device Settings

We are mainly using the policy editor for changing the protection policies, but we want to show you as well how it looks on the device level.

Important Note: Don't use both methods to change settings in parallel, since the Policy Editor is using only his settings to push the next protection policy changes and overwrites the local changes. Also if you configure a protection policy via the device, you can't edit or change it with the policy editor.

1. Select the **Configuration** perspective.
2. In the **Protections** section, select **Protection Policies** in navigation tree.
3. You will see the policy we created. At the moment it has no profiles / protections configured.
4. If you want you can review each time we configured a protection with the policy editor how it being translated in the policy and profiles.



The screenshot shows the Cyber Controller interface. On the left, the navigation tree is expanded to 'Protections' > 'Protection Policies'. The main panel displays a table of protection policies. The table has columns for 'Enabled', 'Policy Name', 'Action', 'Priority', 'SRC Network', 'DST Network', 'Port Group', 'Direction', 'Context', 'Protection Profiles', and 'This Policy Handles Traffic Received Through A CDI'. A single policy is listed with the name 'TeamXX', action 'Block an.', priority '10', and SRC Network 'any'.

Enabled	Policy Name	Action	Priority	SRC Network	DST Network	Port Group	Direction	Context	Protection Profiles	This Policy Handles Traffic Received Through A CDI
Enabled	TeamXX	Block an.	10	any	TeamXX,d		One Way		Disabled	

Save this basic configuration.

You might need it for restoring it later for other configuration setup. With DefenseProX and CyberController, we can save the configuraton in the policy editor format (to restore only the policies) or in the DefensePro CLI format, which allows to restore the complete device from the backup. In production the DefensePro CLI format is the recommended format.

1. At Cyber Controller, above policy setup select **Securty Operations → Security Settings**
 - Click **Export Configuration**
 - After you saved the file change the file name: ***dpX-BasicLab-config.zip***
 - This saves the policy in the policy editor format
2. DefensePro **Configuration → Operations → Export Configuration File**
 - Destination: **Client**
 - Check **Include Private Keys**
 - Passphrase: **radware**
 - Confirm Passphrase: **radware**
 - Click **OK**
 - Rename the file to **dpX-BasicLab-config.txt**
 - This saves the device configuration in the DefensePro CLI format



For questions, contact
radwarevirtuallab@Radware.com

© 2023 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.