

Ultimate (Step-by-Step) Checkpoint Firewall R81 Lab Tasks



R81



About Author



*I have been in the IT & Security Industry for close to 19 years now. On Checkpoint Firewall, I have achieved **CCSA, CCSE & CCSE+** - Alongside got certified expertise on **McAfee SIEM, IBM -QRadar SIEM & BlueCoat Security Analytics (Solera)**.*

Product knowledge include multi OEMs Firewall, IPS, SSL Visibility, SIEM, SOC Operations, EDR, Security Analytics & Investigations.

Delivered multiple Security Deployments across clients spread to BFSI, Government, IT-ITES verticals.

Currently, I am trying to share some of my knowledge by means of Online Teaching via Online Platforms and creating new, unique, simple & low-cost Content for New IT aspirants.

Currently I have a few online courses Published and have also started my YouTube Channel. You can check out all content here

- <https://www.udemy.com/course/checkpoint-firewall-administration-r80/?referralCode=12398B1EEF83C8D00ECD>
- <https://www.udemy.com/course/isoiec-27001-security-guidelines-for-organizational-users/?referralCode=5E63E591F2B9A9EE8C22>
- <https://www.youtube.com/c/YourITBasicsOnline> (Subscribe & Share)
- Mail to – amit@youritbasics.online

About The Book

This book (600+ pages) is comprised of 25 Lab Scenarios (Step-by-Step) for various configuration scenarios for the CheckPoint Firewall version R81. The Platform used for the Lab deployment is PNET environment which is similar to EVENG platform. It is presumed that you may have a starter level knowledge about PNET Labs as well.

Contents

Lab Task-1 ~ Deployment of CheckPoint ISO in a PNET LAB	6
Download CheckPoint R81 ISO image	6
Install CheckPoint R81 on PNET	7
Add CheckPoint Node to PNET LAB	11
Lab Task-2 ~ Deployment of Standalone CheckPoint Firewall (2-Tier)	13
Internet Router Configuration	21
Gaia OS Installation	23
Standalone CheckPoint Deployment (2 Tier)	29
Smart Console Installation	43
SmartConsole Login	52
Lab Task-3 ~ Deploy Basic Internet Access Firewall Policy	54
Internet Access Lab (Brief)	54
Deploy Internet Access Rule	55
Deploy Firewall Access Rule	63
Install the Policy on Standalone Firewall	69
Verify Internet Access from GUI Client	73
Observe Logs in the Logs & Monitor	74
Lab Task-4 ~ Deployment of Distributed CheckPoint Firewall (3-Tier)	76
CheckPoint Distributed Deployment Lab Setup in PNET LAB	76
CP-R81-SmartCenter / Management Server Installation	87
CP-R81-Firewall Module Installation	97
Secure Internal Communication(SIC) – Integration for Firewall and Management Server	106
Lab Task-5 ~ Troubleshooting Issues with SIC	123
SIC Reset on Firewall object in Smart Center Server	123
SIC Reset on Firewall Module	126
SIC Reconfigure	128
Lab Task-6 ~ CheckPoint Firewall Topology Configuration	131
Add a WAN Firewall and DMZ Segment	131
WAN-Firewall Installation & Routing Configuration	138
IP Addressing & Routing in CP-Office-FW	138
Topology Configuration (Manual) in CP-FW-R81	139
Topology Configuration (Automatic) in CP-FW-R81	151
CP-Office-FW Distributed Firewall Module Installation	155
Secure Internal Communication(SIC) – Integration for WAN Firewall and Management Server	163

Add a New Policy for CP-Office-FW.....	168
Lab Task-7 ~ Configure Expert Mode & Enable CheckPoint Blades.....	174
Enable Expert Mode on Gaia Module	174
Enabling Blades on the Firewall Object.....	178
Lab Task-8 ~ CheckPoint Implied Rules & Global Properties.....	186
Explicit Rules	186
Implied Rules & Global Properties	186
First, Last & Before Last Implied Rules.....	192
Lab Task-9 ~ Manage Security Administrators & SmartConsole GUI Clients.....	201
Adding Security Administrators from Smart Console.....	201
Adding Security Administrators from CLISH	208
Manage GUI clients via CLISH	210
Manage GUI clients via Gaia Web UI.....	213
Lab Task-10 ~ CheckPoint Firewall Policy Objects.....	214
Firewall Policy Objects.....	214
CheckPoint Host.....	214
Host Object.....	215
Network Object.....	217
Network Group Object	219
Address Range Object.....	220
Service Objects(Ports).....	222
Service Objects (Range of Ports)	227
Time Objects	228
Lab Task-11 ~ CheckPoint Policy Layers.....	230
Firewall Policy Layers.....	230
Ordered Layers.....	230
Inline Layers	230
Adding Ordered Layer.....	232
Shared Layers	239
Adding Inline Layers.....	244
Lab Task-12 ~ Deploy an Optimized Firewall Policy.....	246
Design Optimized Policy	246
Using Hit Count to Optimize Policy	248
Lab Task-13 ~ Database Revision Control.....	249
Database Revision Control	249

Lab for Database Revision Control	250
Change Report.....	258
Lab for Change Report	260
Lab Task-14 ~ CheckPoint Logging Operations & Log Files Management.....	262
Logging Functionality in CheckPoint R81	262
Log File Management	268
Log Switch Lab.....	271
Lab Task-15 ~ Network Address Translation in CheckPoint Firewall	275
Network Address Translation (NAT) Concepts	275
HIDE NAT	275
STATIC NAT.....	276
CheckPoint NAT LAB	278
HIDE NAT (Auto Configuration)	278
HIDE NAT (Manual Configuration)	288
STATIC NAT (Auto Configuration).....	294
STATIC NAT (Manual Configuration).....	297
Lab Task-16 ~ CheckPoint Firewall Clustering.....	309
CheckPoint Clustering Lab	309
Cluster Members Firewall Installation	312
Adding Cluster Object & Cluster Members	314
Cluster Topology Configuration.....	320
High-Availability Cluster Configuration.....	325
High-Availability Cluster Testing	328
Observe High-Availability Cluster Logs	333
Active-Active Clustering Configuration	337
Observe Active-Active Cluster Logs.....	339
Lab Task-17 ~ SSL Operation, CheckPoint HTTPS Inspection & UTM Blades	340
SSL (HTTPS) Operation & SSL (HTTPS) Inspection.....	340
HTTPS Inspection on CheckPoint (LAB)	343
Create Outbound CA Certificate on Firewall.....	343
Exporting the Certificate.....	344
Enable HTTPS Inspection on the Firewall.....	345
HTTPS Inspection Policy Configuration & Testing.....	345
Application Control & URL Filtering Blade	358
Content Awareness Blade	366

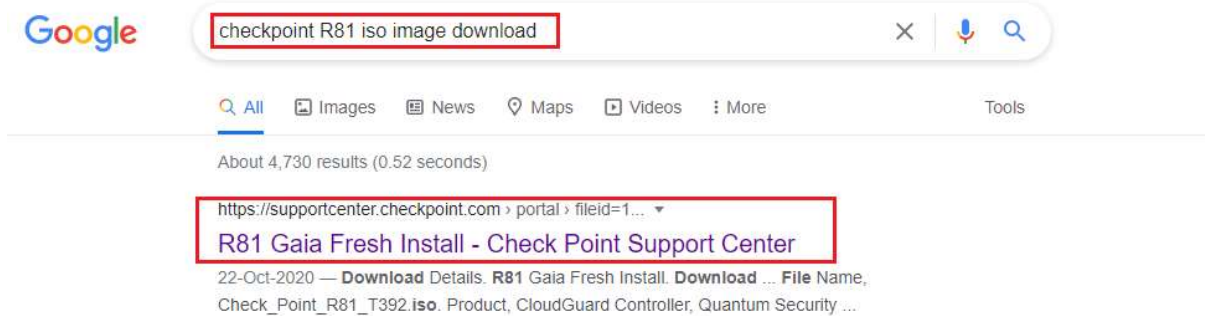
Data Loss Prevention Blade	373
Lab Task-18 ~ CheckPoint IPS (Notes).....	393
Intrusion Prevention System(IPS)	393
CheckPoint IPS Blade	397
Infinity Threat Prevention	404
Lab Task-19 ~ CheckPoint Threat Prevention (Notes).....	406
Zero Day Threats.....	406
Zero-Day Threat Prevention	407
CheckPoint Threat Emulation.....	408
CheckPoint Threat Extraction.....	411
CheckPoint Anti-BoT	413
CheckPoint Anti-Virus.....	414
CheckPoint Anti-Spam & Email Security	416
Lab Task-20 ~ CheckPoint User & Client Authentication – Legacy Authentication	418
User Authentication.....	418
User Authentication Configuration	418
Creating User Groups.....	420
Creating User Template	421
Create Users	425
User Authentication Policy	428
Client Authentication.....	433
Client Authentication Policy Configuration	433
Client Authentication Properties.....	438
External TACACS Server Authentication	440
External RADIUS Server Authentication	444
Lab Task-21 ~ CheckPoint Identity Awareness Blade Configuration.....	447
CheckPoint Identity Awareness.....	447
AD server Installation	448
Creating Users & Groups in Active Directory Server	469
Migration of LAN Node to Domain.....	483
CheckPoint Identity Awareness Configuration	487
Active Directory User Access Configuration	491
Guest User Access Configuration	498
Lab Task-22 ~ CheckPoint Backup -Restore -Snapshot	505
CheckPoint Backup	505

Backup using the Web UI.....	507
Restore using Web UI	510
Backup using CLISH	514
Restore using CLISH	515
Snapshot Management	515
Snapshot using Web UI.....	515
Snapshot Revert using Web UI.....	516
Snapshot using CLISH.....	517
Snapshot Revert using CLISH	518
Lab Task-23 ~ CheckPoint Firewall Site-to-Site VPN configuration.....	519
VPN Fundamentals	519
CheckPoint VPN Lab Setup	521
Site-to-Site VPN Configuration Steps	522
VPN Configuration at Site-A	522
VPN Configuration at Site-B	542
VPN Testing & Troubleshooting	560
Lab Task-24 ~ CheckPoint Remote Access VPN Configuration.....	566
Remote Access VPN Configuration.....	566
Remote Access VPN Domain	568
Create VPN User Group & User	573
Remote Access VPN Rule.....	579
VPN Client Download and Install	583
Connecting to VPN Site.....	588
Lab Task-25 ~ CheckPoint SSL VPN Configuration.....	598
SSL VPN Configuration	598

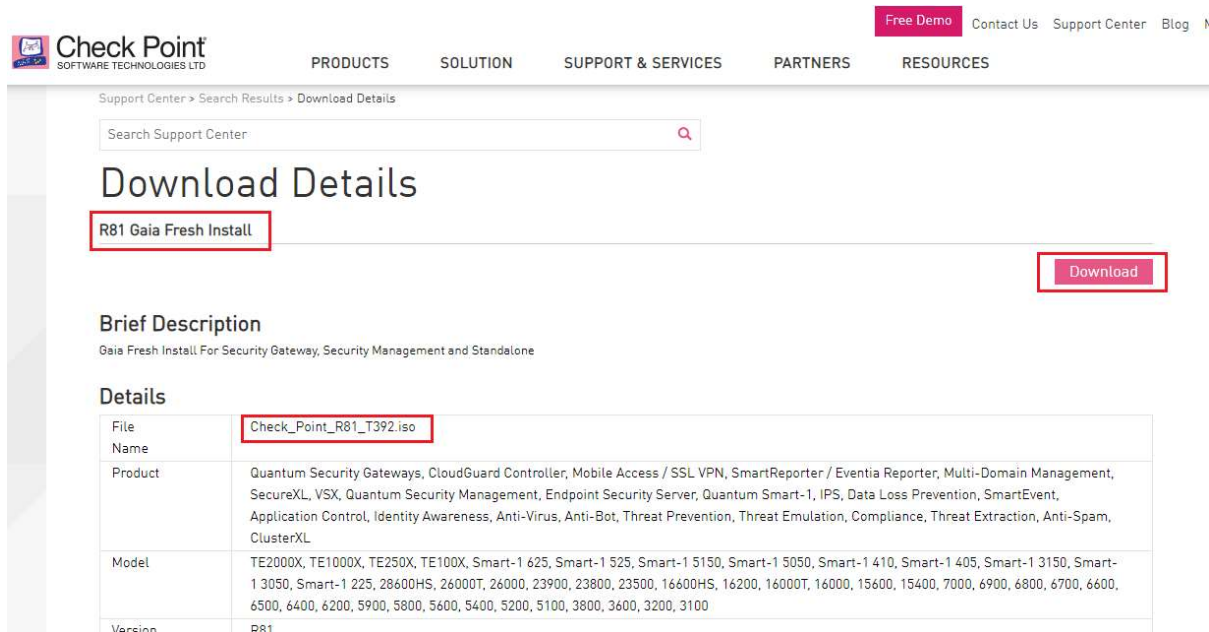
Lab Task-1 ~ Deployment of CheckPoint ISO in a PNET LAB

Download CheckPoint R81 ISO image

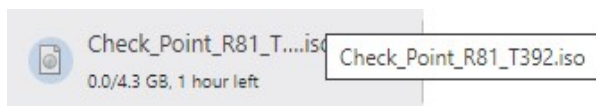
Search for checkpoint R81 iso image download on Google as shown – and Click the support center link.



You will be redirected to the Download Page. The file name is Check_Point_R81_T392.iso. Click the Download button.



The Download begins as shown – Roughly 4GB file. Let the Download complete.

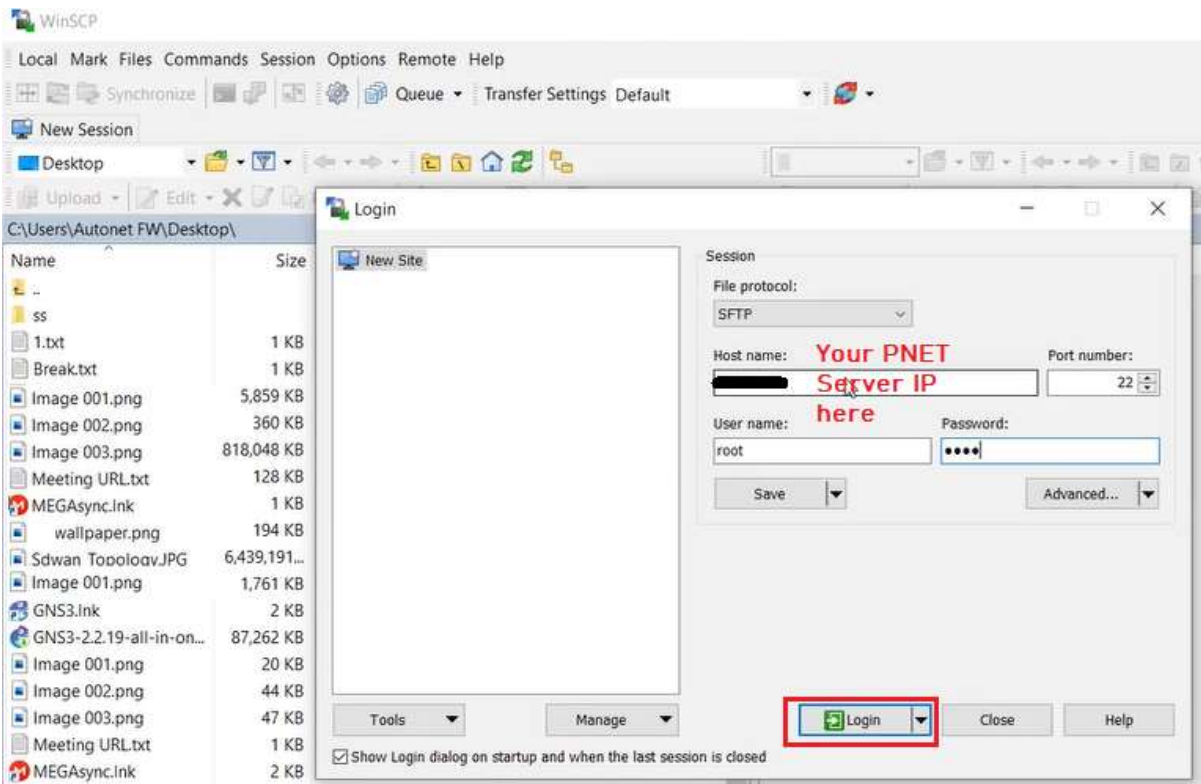




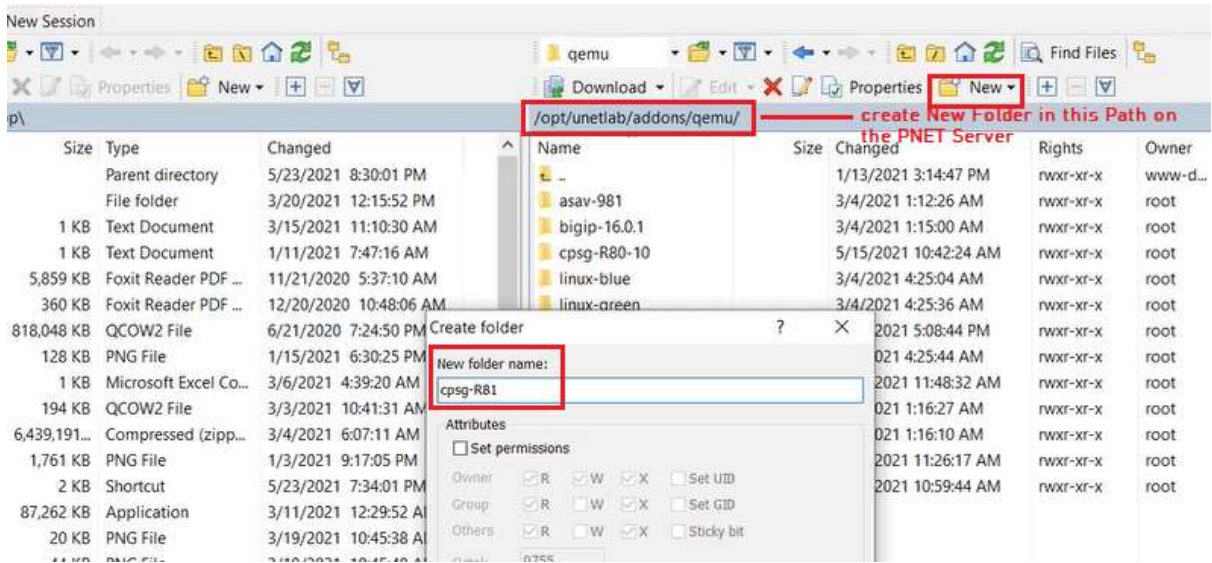
Install CheckPoint R81 on PNET

Through a WinSCP client or any other File transfer client – connect to your PNET LAB server. We will now upload the CheckPoint ISO file in the PNET server

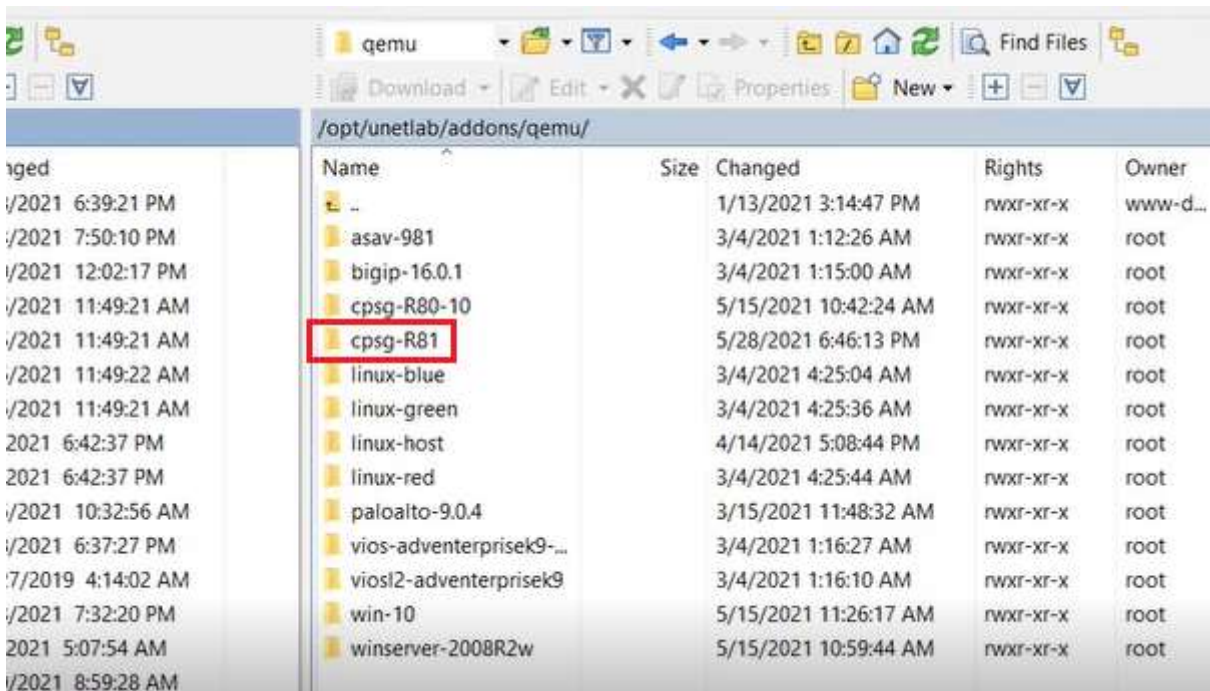
Provide the IP / Port details and credentials of your PNET LAB server and click on Login.



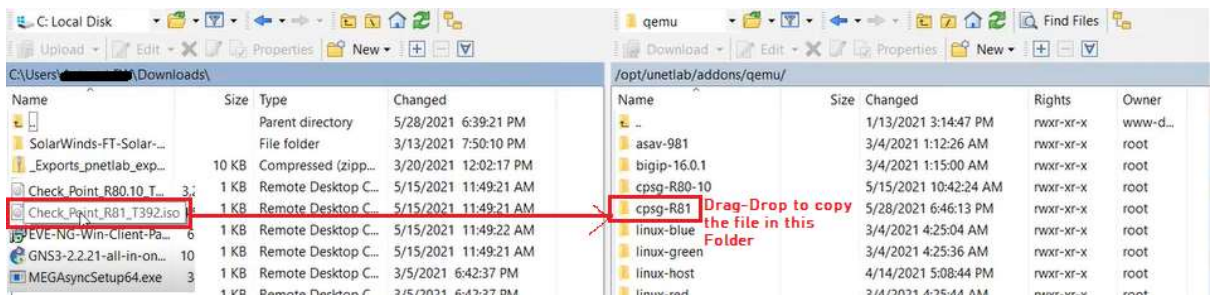
Once connected to the PNET server, Create a New Folder named “cpsg-R81” in the path /opt/unetlab/addons/qemu/. You can use the New > Folder option as shown.



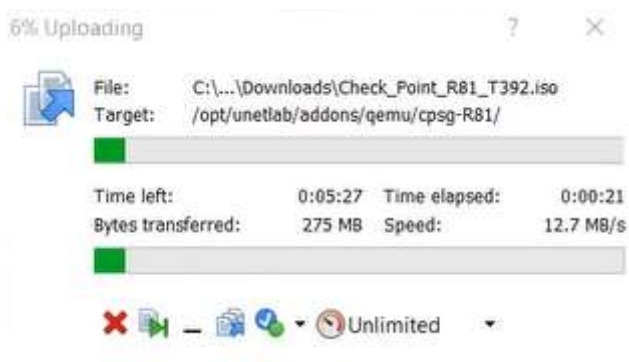
The Folder is created as shown




On the Left side of the window, browse to the CheckPoint ISO file path, and drag Drop the Check_Point_R81_T392.iso file to the folder cpsg-R81 as shown.



The file transfer will begin as shown



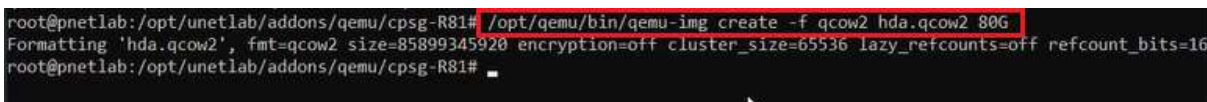
Once the File is uploaded, Login to the PNET server via Putty and browse to the Path /opt/unetlab/addons/qemu/cpsg-R81 and type ls command to view the files and verify that the file upload is successful.

A terminal window titled "OpenSSH SSH client" showing a root user at pnetlab. The user navigates to the directory /opt/unetlab/addons/qemu/cpsg-R81 and runs the ls command, which lists the file Check_Point_R81_T392.iso. The terminal output is highlighted with a red box.

```
root@pnetlab:~#  
root@pnetlab:~#  
root@pnetlab:~#  
root@pnetlab:~#  
root@pnetlab:~#  
root@pnetlab:~# cd /opt/unetlab/addons/qemu/cpsg-R81  
root@pnetlab:/opt/unetlab/addons/qemu/cpsg-R81# ls  
Check_Point_R81_T392.iso  
root@pnetlab:/opt/unetlab/addons/qemu/cpsg-R81#
```

We will now create a QCOW2 image from the iso image with the following 2 command

```
mv Check_Point_R81_T392.iso cdrom.iso  
/opt/qemu/bin/qemu-img create -f qcow2 hda.qcow2 80G
```

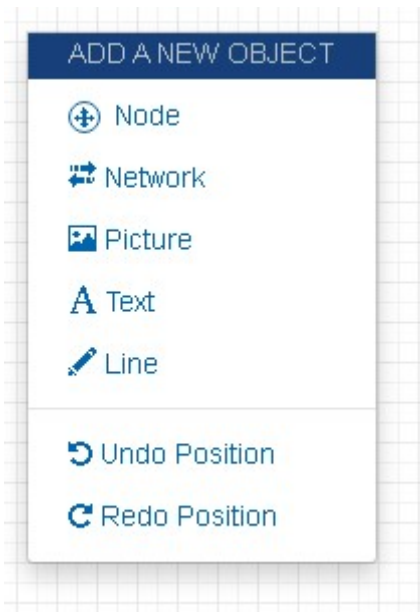
A terminal window showing the execution of the qemu-img create command. The command is highlighted with a red box. The output shows the image is being formatted as qcow2 with a size of 85899345920 bytes.

```
root@pnetlab:/opt/unetlab/addons/qemu/cpsg-R81# /opt/qemu/bin/qemu-img create -f qcow2 hda.qcow2 80G  
Formatting 'hda.qcow2', fmt=qcow2 size=85899345920 encryption=off cluster_size=65536 lazy_refcounts=off refcount_bits=16  
root@pnetlab:/opt/unetlab/addons/qemu/cpsg-R81#
```

Now the CheckPoint R81 Node is ready to be added to the PNET Lab as shown below. You can create a new Lab on the PNET Console and Add the CheckPoint R81 Node as shown below

Add CheckPoint Node to PNET LAB

Once you get access to PNET Lab Right click on Lab Area and Select "Node"



Select " CheckPoint Security Gateway VE" option



Change the Name to "CP-standalone-R81"

ADD A NEW NODE

Template Show all unsupported

CheckPoint Security Gateway VE

Number of nodes to add: 1

Image: cpsg-R80-10

Name: CP-Standalone-R81

Description: CheckPoint Security Gateway VE

Icon: Checkpoint.png

Check the following settings on the CheckPoint Node

CPU Limit

CPU: 4

RAM (MB): 6144

Primary Console: Telnet

Primary Map Port:

Secondary Console: Empty

Secondary Map Port:

User Name:

Password:

Ethernet: 4

Qemu Arch: x86_64

Qemu NIC: e1000

Qemu Version: 2.4.0(Default)

The CheckPoint Nodes gets added to the Lab area.

