

CCSA

CHECK POINT SOFTWARE TECHNOLOGIES

Education Services

Security Administrator

Lab Setup Guide



Security Administrator - Lab Setup Guide

© Check Point Software Technologies

www.CheckPoint.com

courseware@checkpoint.com

6330 Commerce Dr., Suite 100, Irving, TX 75063



DOC-Lab Setup-CCSA-R81.20-v1.0

Configuring the Lab Environment

The Check Point Security Administrator course topology is a “sandbox” environment. All student machines have the same set of IP addresses. The virtual machines do connect to the Internet, with Network Address Translation through the host machine. Internet connectivity is required for each host machine used by students attending the course.

Follow the steps below to configure the virtual machines needed for the students to perform all Security Administrator labs. ATCs may use whatever virtualization software they choose, but Check Point assumes the trainer will create the Virtual Machines in either a Microsoft Hyper-V, VMware Workstation, or VMware ESXi environment. Check Point tested this environment in Microsoft Hyper-V.

A Special Note about Licensing

Check Point discourages using the built-in 15-day evaluation licenses in this classroom configuration. The student will be provided with license and contract files during the labs to install on each of the Check Point devices.

VMware Settings

Configure all virtual machines with the following options:

- Snapshots – Just Power off
- VMware Tools – Installed
- Remove the Floppy from the Hardware Settings
- Time Synchronization – Synchronization between Guest and Host should be active.

Lab Topology

Configure each student machine with the following virtual environment:

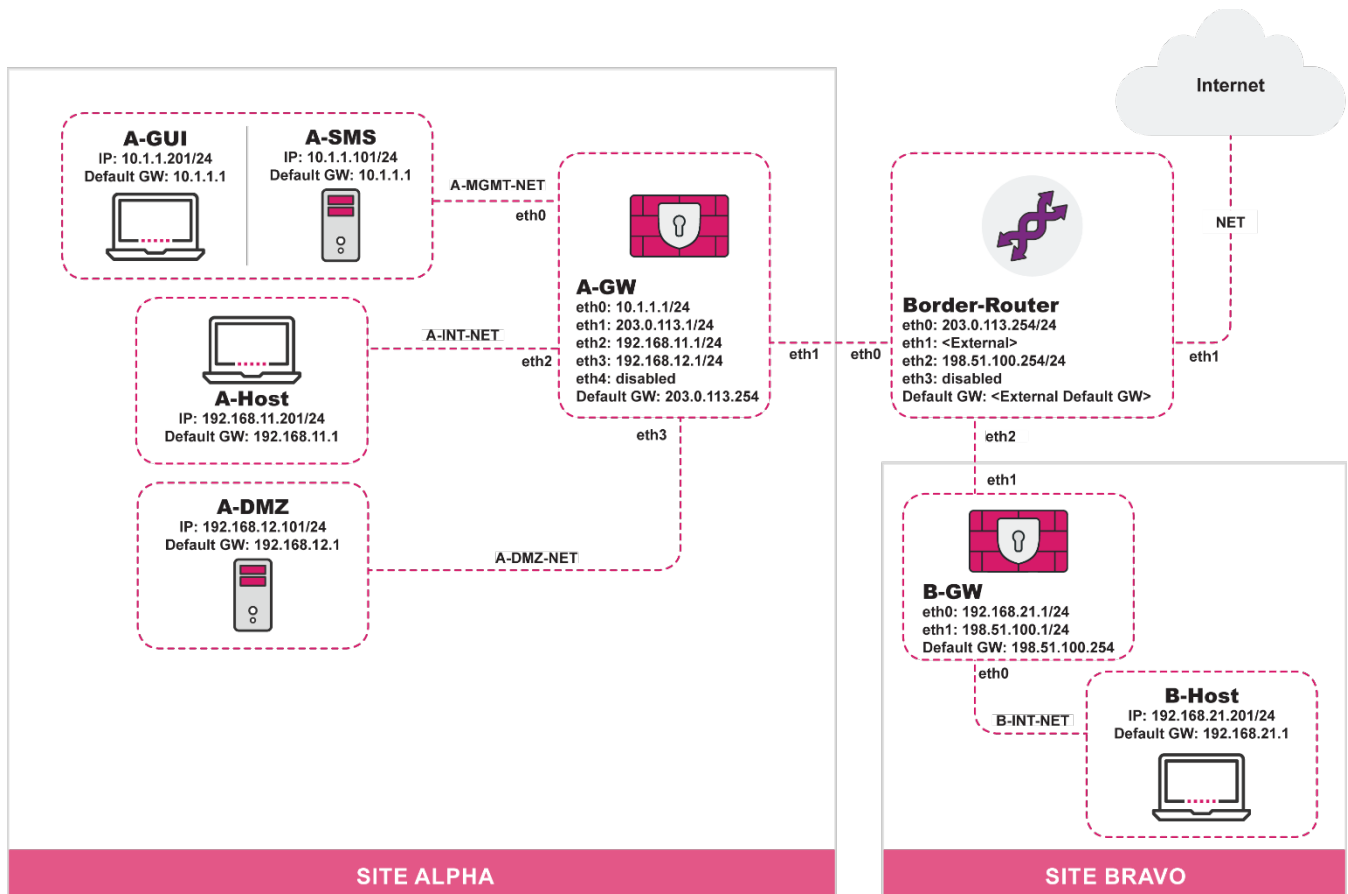


Table of Contents

1. [Border Router](#)
2. [A-GUI](#)
3. [A-SMS](#)
4. [A-GW](#)
5. [A-Host](#)
6. [A-DMZ](#)
7. [B-GW](#)
8. [B-Host](#)
9. [Policy](#)
10. [Machine Usage per Lab](#)

Border Router

Use the information below to configure the Border-Router virtual machine:

Virtual Machine Configuration	
Memory	8GB
Processors	4
Hard Disk	100 GB – Thin Provisioned
Network Adapter 1	NAT Segment (Eth0)
Network Adapter 2	External Segment (Eth1)
Check Point Configuration	
Hostname	Border-Router
Software Version	R81.20 with GA Jumbo
User – admin	Password – Chkp!234
GUI Client Admin – cadmin	Password – Chkp!234
Domain	alpha.cp
eth0	203.0.113.254/24
eth1	<External IP> (For Spektra, this is 192.168.100.2/24)
eth2	198.51.100.254/24
eth3	192.0.2.254 (disabled)
Default Gateway	<Default Route> (For Spektra, this is 192.168.100.1)
DNS (Primary)	8.8.8.8 ¹
DNS (Secondary)	4.2.2.2 ¹
NTP	time1.google.com ² , version 3 time2.google.com ² , version 3
Static Routes	<Default Route>(For Spektra, this is 192.168.100.1) 10.1.1.0/24 via 203.0.113.1 192.168.11.0/24 via 203.0.113.1 192.168.12.0/24 via 203.0.113.1 192.168.21.0/24 via 198.51.100.1

Special Configuration Notes

1. Set DNS servers to the listed IP addresses unless the lab environment requires the use of other addresses.
2. Set NTP server to google time service or other local public/internal NTP service.

A-GUI

Virtual Machine Configuration	
Memory	4GB
Processor Cores	4
Hard Disk	60 GB – Thin Provisioned
Network Adapter 0	A-MGMT-NET
Windows Configuration	
Hostname	A-GUI
Software Version	Windows 10 or later
User – admin	Password – Chkp!234
Domain Login	Enabled for alpha.cp
Network Card	10.1.1.201/24
Default Gateway	10.1.1.1
DNS	8.8.8.8 ¹ 4.2.2.2 ¹
NTP	time.google.com ²
Installed Tools	Google Chrome, Mozilla Firefox, or another Check Point Supported Web Browser WinSCP or other SFTP tool Putty or other SSH tool Wireshark Notepad++
Enabled Services	FTP, Web, Telnet, and Remote Desktop

Special Configuration Notes

1. Set DNS to the listed IP addresses unless the lab environment requires the use of other addresses.
2. Set NTP server to google time service or other local public/internal NTP service.
3. Add a Folder on the desktop named Check Point Tools. Place Latest SmartConsole build for R81.20 in folder. Place R81.10 JHFA Take 87 in folder.
4. Add a subfolder to Check Point Tools named Licenses with all of the license files for the lab in this folder.
5. Update all browsers to the latest version of the browser at the time of lab creation.

A-SMS

Virtual Machine Configuration	
Memory	16GB
Processor Cores	8
Hard Disk	200GB* – Thin Provisioned
eth0	A-MGMT-NET
IP Address:	10.1.1.101/24
Default Gateway	10.1.1.1
Gaia Configuration	
Hostname	A-SMS
Domain name	alpha.cp
Software Version	R81.20 – Current GA JHFA
Deployment State	Bare Metal
Check Point Configuration	
Modules	Nothing is Installed

Special Configuration Notes

1. Mount R81.20 ISO to DVD drive. Configure to connect at power on.

A-GW

Virtual Machine Configuration	
Memory	8GB
Processor Cores	4
Hard Disk	100GB – Thin Provisioned
eth0	A-MGMT-NET
eth1	External
eth2	A-INT-NET
eth3	A-DMZ-NET
eth4	A-SYNC-NET (Disabled)
Gaia Configuration	
Hostname	A-GW
Domain name	alpha.cp
Software Version	R81.20 Gaia
Deployment State	Gaia Installed and Waiting on First Time Wizard
Partition Sizes	System Root – at least 20% Log – at least 20%
User 1 – admin	Password – Chkp!234
Expert authentication method	user-password
Inactivity / Web Session Timeouts	720
Management Interface	eth0-10.1.1.1
Default Gateway	Empty
Check Point Configuration	
Modules	Waiting on First Time Wizard

Special Configuration Notes

1. Set DNS to the listed IP addresses unless the lab environment requires the use of other addresses.
2. Set NTP server to google time service or other local public/internal NTP service.
3. Disconnect Media after installing image.

A-Host

Virtual Machine Configuration	
Memory	4GB
Processor Cores	4
Hard Disk	60 GB - Thin Provisioned
Network Adapter 1	A-INT-NET
Windows Configuration	
Hostname	A-Host
Software Version	Windows 10+ Or Linux Client with GUI Support
User – admin	Password – Chkp!234
Network Card	192.168.11.201/24
Default Gateway	192.168.11.1
DNS (Primary/Secondary)	8.8.8.8 ¹
NTP	time.google.com ²
Suggested Tools	Google Chrome, Mozilla Firefox, Notepad++
Services	FTP, Web, and Java Runtime Environment

Special Configuration Notes

1. Set DNS to the listed IP addresses unless the lab environment requires the use of other addresses.
2. Set NTP server to google time service or other local public/internal NTP service
3. Update all browsers to the current version at the time of lab build.

A-DMZ

Virtual Machine Configuration	
Memory	8GB
Processors	4
Hard Disk	120 GB* – Thin Provisioned
Network Adapter 1	A-DMZ-NET
Windows Configuration	
Hostname	A-DMZ
Software Version	Windows Server 2016+ Or Linux Web Server with GUI Support
Users – administrator	Password – Chkp!234
Network Card	192.168.12.101/24
Default Gateway	192.168.12.1
DNS (Primary/Secondary)	8.8.8.8/4.2.2.2 ¹
NTP	time.google.com ²
Suggested Tools	Google Chrome, Mozilla Firefox, Notepad++
Services	Web Server
Domain	alpha.cp
All users' password	Chkp!234
User Groups	Domain Administrators - administrator

Special Configuration Notes

1. Set DNS to the listed IP addresses unless the lab environment requires the use of other addresses.
2. Set NTP server to google time services or other local public/internal NTP service
3. Install updated A-DMZWebServer.zip files in the web server folder.

B-GW

Virtual Machine Configuration	
Memory	4GB
Processors	4
Hard Disk	100 GB* - Thin Provisioned
eth 0	B-INT-NET
eth 1	External2
Gaia Configuration	
Host name	B-GW
Domain name	<Blank>
Software Version	R81.10 with JumboHFA take 45 ³
Partitions	System Root – At least 20% Log – At least 20%
User 1 – admin	Password – Chkp!234
Expert authentication method	User Password
Inactivity / Web Session Timeouts	720
eth0	192.168.21.1/24
eth1	198.51.100.1/24
Default Gateway	198.51.100.254
DNS (Primary/Secondary)	8.8.8.8 ¹ /4.2.2.2
NTP	time1.google.com ² , version 3 time2.google.com ² , version 3
Check Point Configuration	
Modules	Security Gateway Only
Auto download blade contracts	Enabled
Send data to Check Point	Disabled
Cluster	Disabled
DAIP	No

Special Configuration Notes

1. Set DNS to the listed IP addresses unless the lab environment requires the use of other addresses.
2. Set NTP server to google time services or other local public/internal NTP service
3. B-GW is intentionally left in R81.10 with an old JumboHFA take for Lab Purposes.

B-Host

Virtual Machine Configuration	
Memory	4GB
Processors	4
Hard Disk	60 GB
Network Adapter	B-INT-NET
Windows Configuration	
Host name	B-Host
Version	Windows 10+ Or Linux Client with GUI Support
Users – administrator	Password – Chkp!234
Network Card	192.168.21.201/24
Default Gateway	192.168.21.1
DNS (Primary/Secondary)	8.8.8.8/4.2.2.2
NTP	time.google.com ²
Tools	WinSCP, Putty, Wireshark, Notepad++
Services	FTP and Web

Special Configuration Notes

1. Set DNS to the listed IP addresses unless the lab environment requires the use of other addresses.
2. Set NTP server to google time services or other local public/internal NTP service.
3. Update all browsers to current version at time of lab build.
4. Add a folder labeled Check Point Tools the contains the following files:
 - o Take 45 of the R81.10 Jumbo Hotfix
 - o Take 87 of the R81.10 Jumbo Hotfix

Policy

Border-Router

Objects

1. Gateways & Servers:
 - a. Border-Router
 - i. Name: Border-Router
 - ii. IPv4 Address: 203.0.113.254
 - iii. Comment: Sandbox Environment Border Security Gateway
 - iv. Color: Pink
 - v. Network Security Blades:
 1. Firewall
 2. Monitoring
 - vi. Threat Prevention Blades (Custom):
 1. None
 - vii. Management Blades:
 1. Network Policy Management (Greyed Out)
 2. Logging & Status
 3. Provisioning (Greyed Out)
 - viii. Network Management Settings
 1. All interfaces configured with topologies
 2. All interface anti-spoofing set to detect
 - ix. NAT Settings:
 1. Hide behind gateway IP disabled.
 - x. HTTPS Inspection: Not Configured
 - xi. HTTP/HTTPS Proxy: Not Configured
 - xii. ICAP Server: Not Configured
 - xiii. Platform Portal: Default Configuration
 - xiv. Mail Transfer Agent: : Not Configured
 - xv. Monitoring Software Blade:
 1. All counters enabled.
 - xvi. Logs
 1. Log Indexing enabled
 2. All other settings default
 - xvii. Optimizations: Default Configuration
 - xviii. Hit Count: Default Configuration
 - xix. Other Settings: Default Configuration
2. Hosts:
 - a. Jump Server (or Hyper-V Host)
 - i. Name: JumpServer
 - ii. Comment: Host for Managing Border-Router
 - iii. Color: Red
 - iv. IP address: <Address on External Network the same as Border-Router>
(For Spektra this address is 192.168.100.1)

3. Networks:

- a. A-DMZ-NET
 - i. Name: A-DMZ-NET
 - ii. Comment: Alpha Corporation DMZ Network
 - iii. Color: Crete Blue
 - iv. Network address: 192.168.12.0
 - v. Net mask: 255.255.255.0
 - vi. All other settings default
- b. A-INT-NET
 - i. Name: A-INT-NET
 - ii. Comment: Alpha Corporation Internal Network
 - iii. Color: Crete Blue
 - iv. Network address: 192.168.11.0
 - v. Net mask: 255.255.255.0
 - vi. All other settings default
- c. A-MGMT-NET
 - i. Name: A-MGMT-NET
 - ii. Comment: Alpha Corporation Management Network
 - iii. Color: Crete Blue
 - iv. Network address: 10.1.1.0
 - v. Net mask: 255.255.255.0
 - vi. All other settings default
- d. B-INT-NET
 - i. Name: B-INT-NET
 - ii. Comment: Bravo Company Internal Network
 - iii. Color: Sea Green
 - iv. Network address: 192.168.21.0
 - v. Net mask: 255.255.255.0
 - vi. All other settings default
- e. C-INT-NET
 - i. Name: C-INT-NET
 - ii. Comment: Charlie Company Internal Network
 - iii. Color: Violet Red
 - iv. Network address: 192.168.31.0
 - v. Net mask: 255.255.255.0
 - vi. All other settings default
- f. External1
 - i. Name: External1
 - ii. Comment: Sandbox Network Leading to Alpha Site
 - iii. Color: Orange
 - iv. Network Address: 203.0.113.0
 - v. Net mask: 255.255.255.0
 - vi. NAT Settings
 - 1. Translation Method: Hide
 - 2. Hide behind IP address: 192.168.100.3
 - 3. Install on gateway: Border-Router

- g. External2
 - i. Name: External2
 - ii. Comment: Sandbox Network Leading to Bravo Site
 - iii. Color: Orange
 - iv. Network Address: 198.51.100.0
 - v. Net mask: 255.255.255.0
 - vi. NAT Settings
 - 1. Translation Method: Hide
 - 2. Hide behind IP address: 192.168.100.4
 - 3. Install on gateway: Border-Router
- h. External3
 - i. Name: External3
 - ii. Comment: Sandbox Network Leading to Charlie Site
 - iii. Color: Orange
 - iv. Network Address: 192.0.2.0
 - v. Net mask: 255.255.255.0
 - vi. NAT Settings
 - 1. Translation Method: Hide
 - 2. Hide behind IP address: 192.168.100.5
 - 3. Install on gateway: Border-Router
- 4. Network Groups
 - a. Sandbox_Networks
 - i. Name: Sandbox_Networks
 - ii. Comment: Lab Sandbox Networks
 - iii. Color: Orange
 - iv. Members:
 - 1. A-DMZ-NET
 - 2. A-INT-NET
 - 3. A-MGMT-NET
 - 4. B-INT-NET
 - 5. C-INT-NET
 - 6. External1
 - 7. External2
 - 8. External3

Access Control Rules:

1. Noise Rule
 - a. Source: Any
 - b. Destination: Any
 - c. VPN: Any
 - d. Services & Applications: NBT and bootp
 - e. Action: Drop
 - f. Track: None
2. Management Rule
 - a. Source: JumpServer
 - b. Destination: Border-Router
 - c. VPN: Any
 - d. Services & Applications: Any
 - e. Action: Accept
 - f. Track: Log
3. Stealth Rule
 - a. Source: Any
 - b. Destination: Border-Router
 - c. VPN: Any
 - d. Services & Applications: Any
 - e. Action: Drop
 - f. Track: Log
4. IntraSandbox Traffic Rule
 - a. Source: Sandbox Networks
 - b. Destination: Sandbox Networks
 - c. VPN: Any
 - d. Services & Applications: Any
 - e. Action: Accept
 - f. Track: Log
5. Sandbox Outbound Allow Rule
 - a. Source: External1, External2, External3
 - b. Destination: All_Internet
 - c. VPN: Any
 - d. Services & Applications: Any
 - e. Action: Accept
 - f. Track: Log

6. Cleanup Rule

- Source: Any
- Destination: Any
- VPN: Any
- Services & Applications: Any
- Action: Drop
- Track: Log

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
Management rules (1-3)							
1	Noise Rule	* Any	* Any	* Any	NBT UDP bootp	Drop	None
2	Management Rule	JumpServer	Border-Router	* Any	* Any	Accept	Log
3	Stealth Rule	* Any	Border-Router	* Any	* Any	Drop	Log
Traffic rules (4-5)							
4	IntraSandbox Traffic Rule	Sandbox_Networks	Sandbox_Networks	* Any	* Any	Accept	Log
5	Sandbox Outbound Allow Rule	External1 External2 External3	All_Internet	* Any	* Any	Accept	Log
Cleanup rule (6)							
6	Cleanup Rule	* Any	* Any	* Any	* Any	Drop	Log

NAT Policy

1. IntraSandbox No-NAT Rule

No.	Name	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On
1	IntraSandBox No-NAT	Sandbox_Networks	Sandbox_Networks	* Any	= Original	= Original	= Original	* Policy Targets
Automatic Generated Rules : Machine Static NAT (No Rules)								
Automatic Generated Rules : Machine Hide NAT (No Rules)								
Automatic Generated Rules : Address Range Static NAT (No Rules)								
Automatic Generated Rules : Network Static NAT (No Rules)								
Automatic Generated Rules : Address Range Hide NAT (No Rules)								
Automatic Generated Rules : Network Hide NAT (2-9)								
2	Automatic Rule: CP_default_Office_Mode_addresses_pool	CP_default_Office...	CP_default_Office_N	* Any	= Original	= Original	= Original	* All
3	Automatic Rule: CP_default_Office_Mode_addresses_pool	CP_default_Office...	* Any	* Any	CP_default_Offic	= Original	= Original	* All
4	Automatic Rule: External1	External1	External1	* Any	= Original	= Original	= Original	Border-Router
5	Automatic Rule: External1	External1	* Any	* Any	External1 (Hidin	= Original	= Original	Border-Router
6	Automatic Rule: External2	External2	External2	* Any	= Original	= Original	= Original	Border-Router
7	Automatic Rule: External2	External2	* Any	* Any	External2 (Hidin	= Original	= Original	Border-Router
8	Automatic Rule: External3	External3	External3	* Any	= Original	= Original	= Original	Border-Router
9	Automatic Rule: External3	External3	* Any	* Any	External3 (Hidin	= Original	= Original	Border-Router
Manual Lower Rules (No Rules)								

Machine Usage per Lab

S.No.	Lab No./ Name	VMs used in Lab	VM Memory	Lab Dependencies	Time Required