CHECK POINT SOFTWARE TECHNOLOGIES

Education Services

Security Administration

Lab Setup Guide

EDUCATION SERVICES

Security Administration - Lab Setup Guide

Check Point®
SOFTWARE TECHNOLOGIES LTD.

www.CheckPoint.com
courseware@checkpoint.com
6330 Commerce Dr., Suite 120, Irving, TX 75063

March 3, 2017

Configuring the Lab Environment

The Check Point Security Administration class topology was designed as a "sandbox" environment. All student machines have the same set of IP addresses. The virtual machines connect to the Internet using a NAT connection 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 Administration labs. ATCs may use whatever virtualization software they choose, but Check Point assumes most Virtual Machines will be created in either a VMware Workstation or an ESX environment. Our tests were all performed on VMware Workstation 12.

A Special Note about Licensing

The built-in 15 day evaluation licenses are no longer used in this classroom configuration. All Check Point servers at the Alpha site are required to have a license before the students begin this class. The Bravo license will be added during a specific lab by the students and should not be preloaded. To get 6-month BCK licenses provided to you for use in this and other Check Point classes, contact your ATC coordinator.

Configuring Virtual Machine Settings

All virtual machines should be configured with the following options:

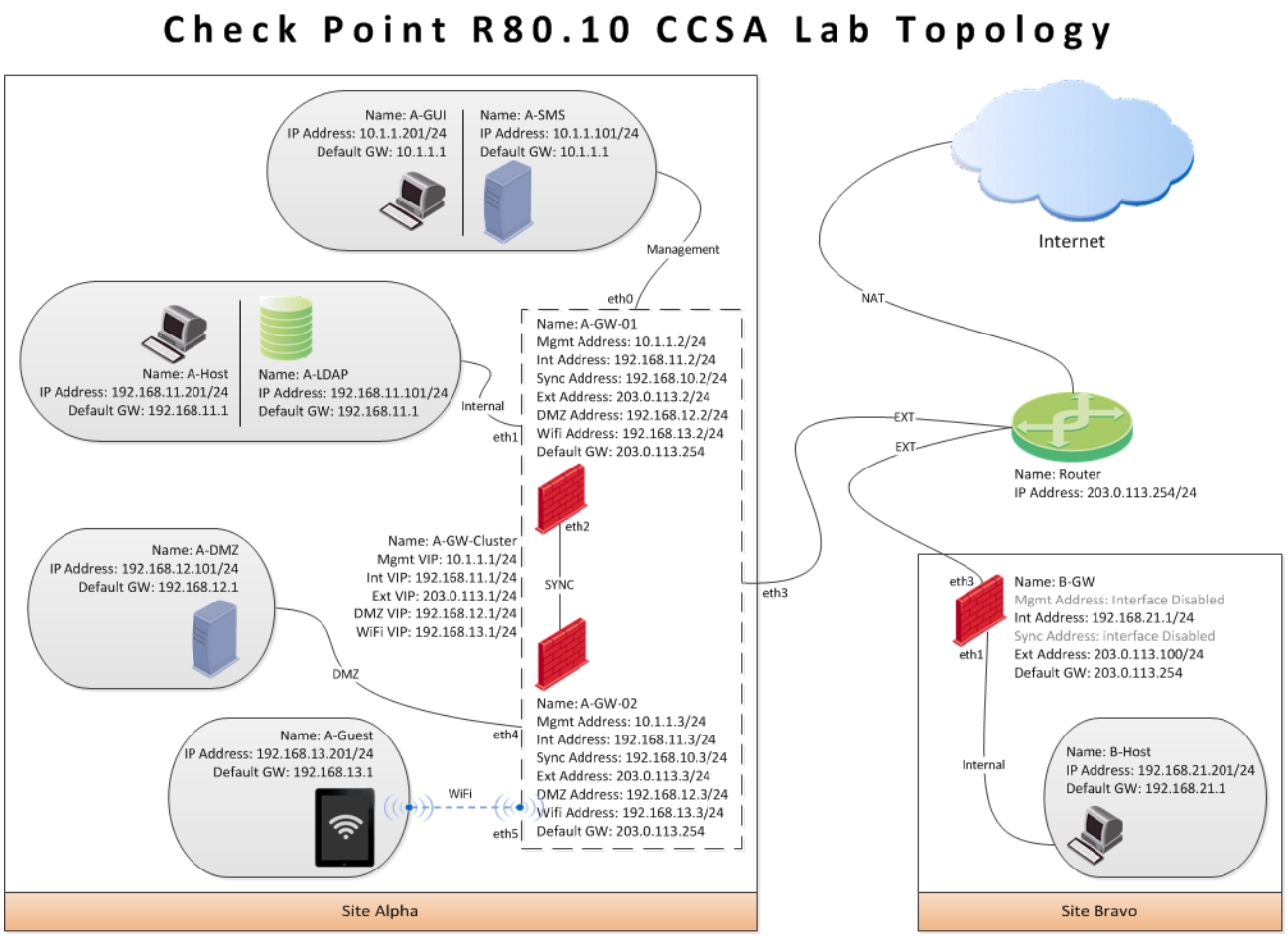
- Snapshots –Power off
- VMware Tools – Installed
- Floppy – Remove from the Hardware Settings
- Time Synchronization – Synchronization between Guest and Host should be active.

LDAP Information

Configure the virtual machines on the Alpha Internal network to be in the alpha.cp domain. All users should log into the domain and not the local virtual machine.

Lab Topology

Configure each student machine with the following virtual environment:



Configuring the Virtual Machines

Configure each of the virtual machines listed below on all student machines. The specifications shown here in terms of Hard Drive and RAM are considered minimum requirements. To function optimally, each student's host machine should be allotted a minimum of 32GB of RAM. For better performance, these numbers should be increased.

All network settings described below are suggestions. You may use LAN segments or vmnets at your discretion. The only requirement is that eth3 interfaces be configured for Internet access.

All user, OS, and application passwords should be: **Chkp!234**

A-GUI

Use the information below to configure the Alpha GUI Client virtual machine:

Name: A-GUI
OS: Windows Client
Hard Drive: 40GB
RAM: 2GB

The following Check Point modules will be installed during the labs:

- SmartConsole R80.10

Use the following information to configure the interface for this virtual machine:

IP Address: 10.1.1.201
Subnet Mask: 255.255.255.0
Default Gateway: 10.1.1.1
Interface: eth0
Network: Management (LAN 1)

Special instructions for the Alpha GUI Client virtual machine:

1. Configure a folder on the desktop that can be shared with Read/Write privileges to anonymous users. This will be used to transfer files through FTP.

2. Install and configure an FTP client and server.

A-SMS

Use the information below to configure the Alpha Security Management Server virtual machine:

Name: A-SMS
OS: Gaia R80.10
Hard Drive: 80GB
RAM: 10GB

The following Check Point modules should be installed and configured:

- Security Management Server

Use the following information to configure the interface this virtual machine:

IP Address: 10.1.1.101
Subnet Mask: 255.255.255.0
Default Gateway: 10.1.1.1
Interface: eth0
Network: Management (LAN 1)

A-GW-01

Use the information below to configure the first Security Gateway virtual machine:

Name: A-GW-01
OS: Gaia R80.10
Hard Drive: 60GB
RAM: 1GB

The following Check Point modules should be installed and configured:

- Security Gateway

Use the following information to configure the interfaces for the first Security Gateway virtual machine:

IP Address: 10.1.1.2
Subnet Mask: 255.255.255.0
Interface: eth0
Network: Alpha Management (LAN 1)

IP Address: 203.0.113.2
Subnet Mask: 255.255.255.0
Default Gateway: 203.0.113.254
Interface: eth3
Network: External (vmnet8 - NAT)

IP Address: 192.168.11.2
Subnet Mask: 255.255.255.0
Interface: eth1
Network: Alpha Internal (LAN 11)

IP Address: 192.168.12.2
Subnet Mask: 255.255.255.0
Interface: eth4
Network: Alpha DMZ (LAN 12)

IP Address: 192.168.10.2
Subnet Mask: 255.255.255.0
Interface: eth2
Network: Alpha Synchronization (LAN 10)

IP Address: 192.168.13.2
Subnet Mask: 255.255.255.0
Interface: eth5
Network: Alpha WiFi (LAN 13)

A-GW-02

Use the information below to configure the second Security Gateway virtual machine:

Name: A-GW-02
OS: Gaia R80.10
Hard Drive: 60GB
RAM: 1GB

The following Check Point modules should be installed and configured:

- Security Gateway

Use the following information to configure the interfaces for the second Security Gateway virtual machine:

IP Address: 10.1.1.3
Subnet Mask: 255.255.255.0
Interface: eth0
Network: Alpha Management (LAN 1)

IP Address: 203.0.113.3
Subnet Mask: 255.255.255.0
Default Gateway: 203.0.113.254
Interface: eth3
Network: External (vmnet8 - NAT)

IP Address: 192.168.11.3
Subnet Mask: 255.255.255.0
Interface: eth1
Network: Alpha Internal (LAN 11)

IP Address: 192.168.12.3
Subnet Mask: 255.255.255.0
Interface: eth4
Network: Alpha DMZ (LAN 12)

IP Address: 192.168.10.3
Subnet Mask: 255.255.255.0
Interface: eth2
Network: Alpha Synchronization (LAN 10)

IP Address: 192.168.13.3
Subnet Mask: 255.255.255.0
Interface: eth5
Network: Alpha WiFi (LAN 13)

A-Host

Use the information below to configure a protected host virtual machine:

Name: A-Host
OS: Windows Client
Hard Drive: 40GB
RAM: 2GB

Use the following information to configure the interface for this virtual machine:

IP Address: 192.168.11.201
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.11.1
Interface: eth0
Network: Alpha Internal (LAN 11)

Special instructions for the Alpha Host virtual machine:

1. Configure a folder on the desktop that can be shared with Read/Write privileges to anonymous users. This will be used to transfer files through FTP.

2. Install and configure an FTP client and server.

3. Install and configure an updated web browser.

4. A-Host must be part of the alpha.cp domain.

5. Install and configure a mail client. (optional)

   Note: The Mail server is not currently used in the CCSA class but will be used in other courses and may be used in the CCSA at a later date.

A-LDAP

Use the information below to configure the Alpha LDAP server virtual machine:

Name: A-LDAP
OS: Windows Sever
Hard Drive: 40GB
RAM: 2GB

Use the following information to configure the interface for this virtual machine:

IP Address: 192.168.11.101
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.11.1
Interface: eth0
Network: Alpha Internal (LAN 11)

Special instructions for the Alpha Active Directory virtual machine:

1. Configure the following role in the Manage Your Server applet:
    - Active Directory Server (LDAP)

3. The domain for this site is: alpha.cp
4. The following are the required users. Each should be configured with **Chkp!234** as their password.
    - User1
    - User2
    - User3
    - User4
    - Guest
5. The following are the required groups.
    - Odd (include all odd numbered users)
    - Even (include all even numbered users)

    Note: The Guest user is not part of any user group.
6. Configure A-LDAP to be the DNS server for the Alpha site.
7. Install and configure the NTP server for the Alpha site.

A-DMZ

Use the information below to configure the FTP, SMTP, and Web Server virtual machine:

Name: A-DMZ
OS: Windows Server
Hard Drive: 40GB
RAM: 2GB

Use the following information to configure the interface for the FTP, SMTP, and Web Server virtual machine:

IP Address: 192.168.12.101
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.12.1
Interface: eth0
Network: DMZ (LAN 12)

Special instructions for the Alpha DMZ virtual machine:

1. Configure a Web Server to run at startup.
2. Install and configure an FTP server.
3. Install and configure a Web server.
4. Install and configure a Mail server. (optional)

   Note: The Mail server is not currently used in the CCSA class but will be used in other courses and may be used in the CCSA at a later date.

A-Guest

Use the information below to configure the guest tablet virtual machine:

Name: A-Guest
OS: Windows 10 in Mobile Mode/Android Tablet
Hard Drive: 20GB
RAM: 1GB

Use the following information to configure the interface for the guest tablet virtual machine:

IP Address: 192.168.13.201
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.13.1
Interface: eth0
Network: WiFi (LAN 13)

Bravo Host

Use the information below to configure the B-Host virtual machine:

Name: B-Host
OS: Windows Client
Hard Drive: 20GB
RAM: 1GB

Use the following information to configure the interface for this virtual machine:

IP Address: 192.168.21.201
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.21.1
Interface: eth0
Network: Bravo Internal (LAN 21)

Special instructions for the Bravo Host virtual machine:

1. Configure a folder on the desktop that can be shared with Read/Write privileges to anonymous users. This will be used to transfer files through FTP.

2. Install and configure an FTP client and server.

3. Install and configure an updated web browser.

Bravo Security Gateway

Use the information below to configure the Bravo Security Gateway virtual machine:

Name: B-GW
OS: Other/Other
Hard Drive: 60GB
RAM: 1GB

The following Check Point modules will be installed during the labs:

- Security Gateway

Use the following information to configure the interfaces for the Bravo Security Gateway virtual machine:

Interface: eth0 (Disabled)
Network: Bravo Management (LAN 2)

Interface: eth1
Network: Bravo Internal (LAN 21)

Interface: eth2 (Disabled)
Network: Bravo Sync (LAN 20)

Interface: eth3
Network: External (vmnet8 - NAT)

Note: The eth0 and eth2 interfaces for B-GW are not used at the beginning of this class but should be configured so that the eth1 connects to the internal network and the eth3 interfaces connects to the external network. The other two interfaces should not be connected or powered on until they are needed.

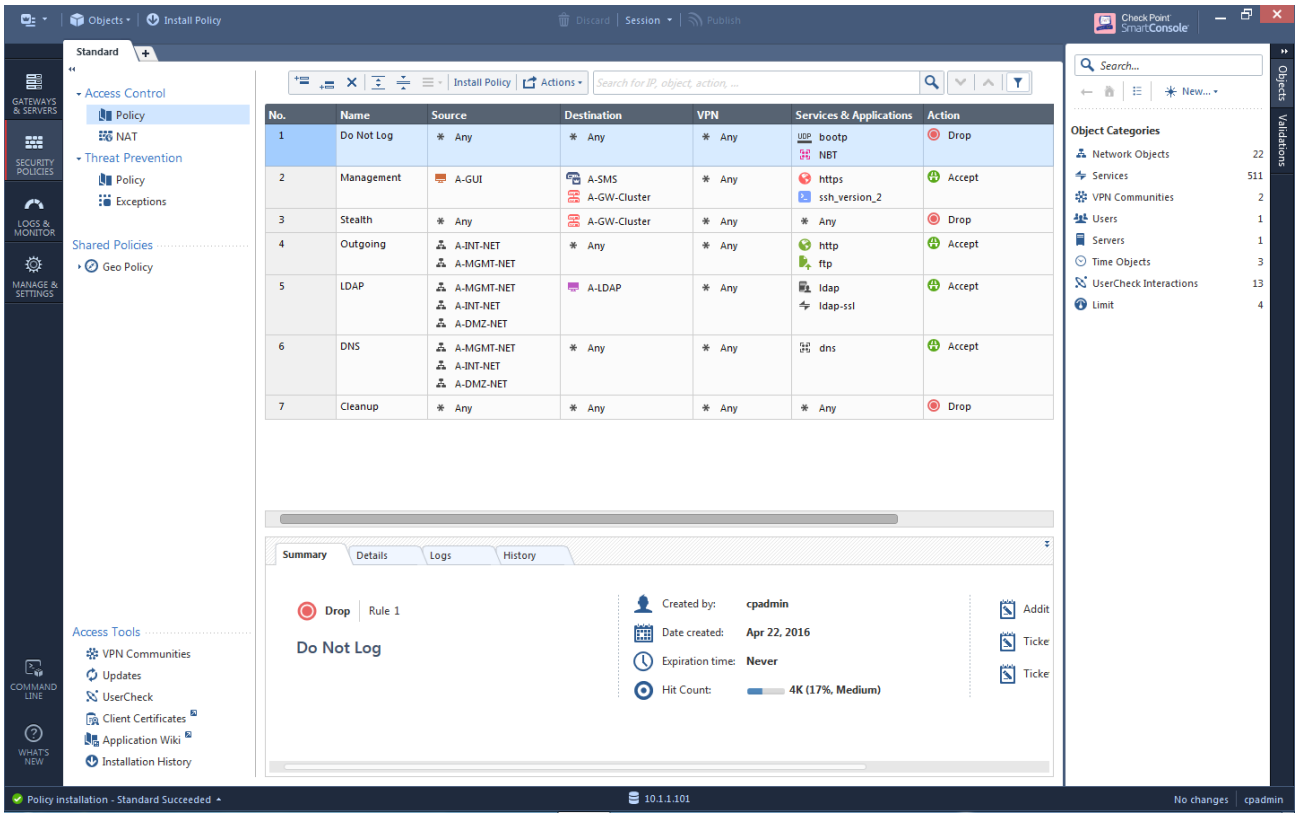
Router

The router may be either a specific virtual machine or you may use the virtualization software's router function. In our testing, we use VMware's Network Editor to configure a NAT address on the 203.0.113.0/24 network that NAT's "guest" VM traffic out through the "host" machine's physical address.

All external interfaces of gateways in the topology should all point to 203.0.113.254 as their default gateway. Network routes for all internal networks should be placed on both the Alpha and Bravo gateways. This will allow traffic between the two sites but also traffic to exit the environment and reach the Internet.

Configuring the Alpha Security Policy

The Alpha Gateways and Management Server should be configured and licensed before the students arrive for class. You must also configure a basic Security Policy that includes the cluster object. No NAT should be configured, as that is part of the labs to be performed in class. Here is a screen shot of the required initial Security Policy for Alpha:



Note: No initial Security Policy is configured for the Bravo site.

The following objects are required to be pre-configured in the Alpha Security Policy:

- A-GUI
- A-SMS
- A-GW-Cluster
- A-LDAP
- A-INT-NET
- A-MGMT-NET
- A-DMZ-NET

The cluster virtual IPs for the gateway should be the .1 addresses, whereas the individual gateway interfaces are configured as .2 or .3. For example, the management interface for Alpha should have a VIP of 10.1.1.1 and the individual member interfaces should be configured as 10.1.1.2 on A-GW-01 and 10.1.1.3 on A-GW-02.

Use the 203.0.113.1 IP address for the main IP of the Cluster Object. When defining the cluster members, they should be defined with their 10.1.1.0 addresses (the same two addresses listed in the paragraph above).

Add network routes on the gateways to all internal networks for both sites Alpha and Bravo.