CHECK POINT SOFTWARE TECHNOLOGIES

Education Services

Introduction to SandBlast Agent Lab Setup Guide

EDUCATION SERVICES

Introduction to SandBlast - Workshop

Check Point®
SOFTWARE TECHNOLOGIES LTD.

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

March 2017

Configuring the Lab Environment

The Check Point Introduction to SandBlast Agent 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 SandBlast 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. 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:

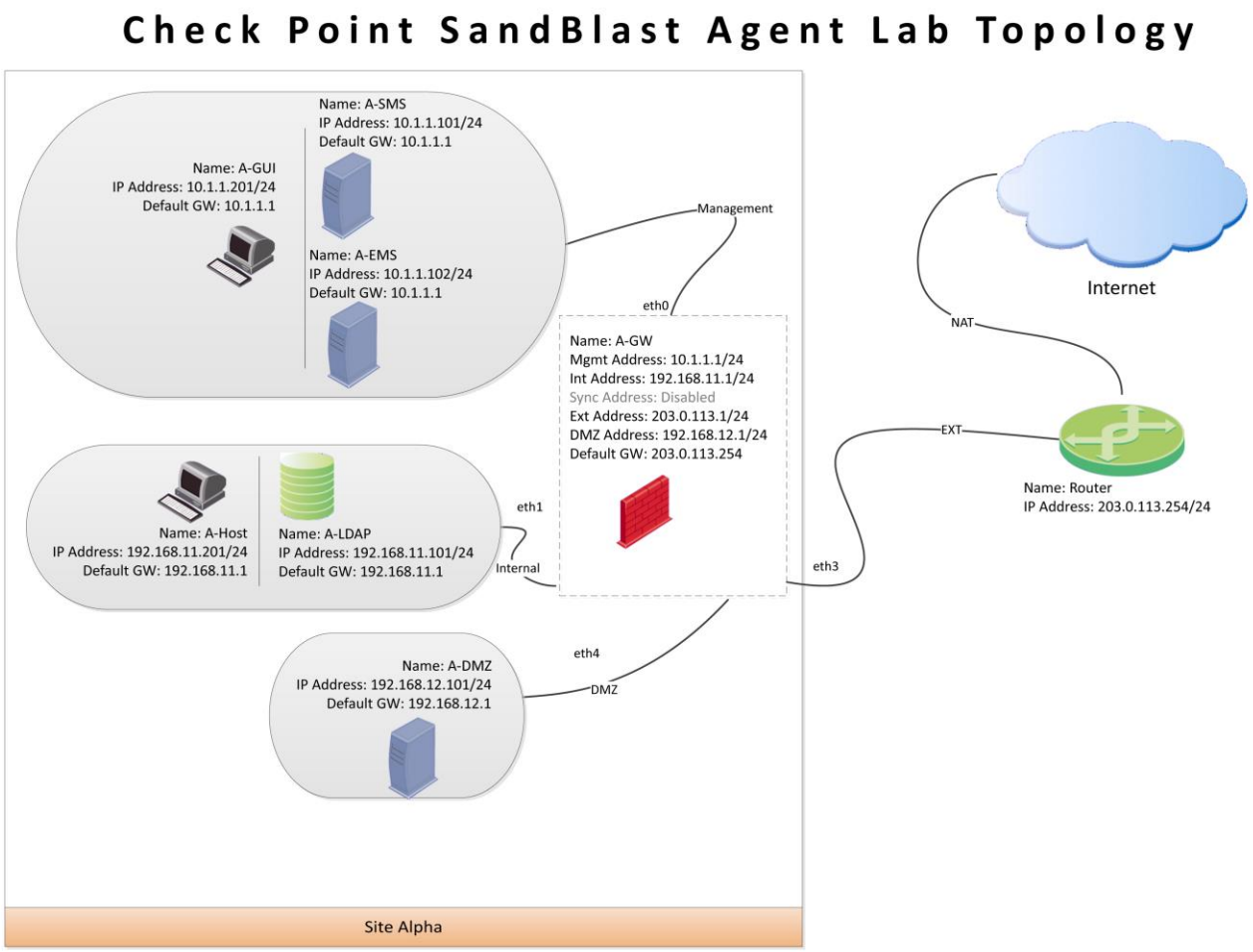
- Snapshots –Power off
- VMware Tools – Installed
- Floppy – Remove from the Hardware Settings
- Time Synchronization – Synchronization between Guest and Host should be active.

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 username should be: **admin**

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: 100GB
RAM: 2GB

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

- SmartDashboard R77.30.02
- SmartEndpoint R77.30.02

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. Install and configure an updated web browser.
2. Install and configure FTP web server.
3. A-GUI must be part of the alpha.cp domain.
4. Download the latest version of the Endpoint Security Client from sk112793. For this lab, we will only need to use the Master SBA client for 64-bit windows. Copy the client folder on the desktop.
5. Update the Management Console to R77.30.02. Refer to sk112793 for the installer and procedure.

6. For 10.1.1.101, configure the Network Policy in SmartDashboard. Refer to Configuring the Alpha Security Policy section for details.

7. For 10.1.1.102, activate the Endpoint Management Server Software Blade and install the database in SmartDashboard. Once done, install the required hotfixes. See A-EMS section for details on the hotfixes.

A-SMS

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

Name: A-SMS
OS: Gaia R77.30
Hard Drive: 60 GB
RAM: 8GB

The following Check Point modules should be installed and configured:

- Security Management Server

Use the following information to configure the interface of 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-EMS

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

Name: A-EMS
OS: Gaia R77.30
Hard Drive: 60 GB
RAM: 8GB

The following Check Point modules should be installed and configured:

- Security Management Server

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

IP Address: 10.1.1.102
Subnet Mask: 255.255.255.0
Default Gateway: 10.1.1.1
Interface: eth0
Network: Management (LAN 1)

Special instructions for the A-EMS Client virtual machine:

1. Apply the following hotfixes:

    - Dedicated Jumbo Hotfix Take_143 (see instructions below).
    - R77.30.02 Hotfix (see instructions below).

    Note: Before applying these hotfixes, make sure to do the following:

    - Upgrade CPUSE Agent to 1130.
    - Activate the Endpoint Management Server software blade in the SmartDashboard.
    - Install the database in the Policy menu.
    - In SmartUpdate, apply the following licenses:
        - SandBlast Agent - full package, Includes forensic incident analysis, Threat Emulation and anti-bot Eval
        - CPEP-EVAL-SM-CLIENT-100 (Endpoint Package and Management)

Installing Jumbo Hotfix Take 143

1. Create temporary folder /var/log/sba/jhfa and copy the Jumbo hotfix to the folder using WinSCP.
2. Connect to the Endpoint Management with SSH on Expert Mode.

3. Type the following and press Enter to unzip and execute the installer:

   /var/log/sba/jhfa

   tar -zxvf R77.30_jhf_T143_EP.tgz

   ./UnixInstallScript

   (Follow the onscreen instructions)

Installing the R77.30.02 hotfix

1. Create temporary folder /var/log/sba/hfa and copy the R77.30.02 hotfix.
2. Connect to Endpoint Management with SSH on Expert mode.
3. Type the following and press Enter to unzip and execute the installer:

   cd /var/log/sba/hfa

   tar -zxvf R77.30.02.Gaia.tgz

   ./UnixInstallScript

   (Follow the onscreen instructions)

A-GW

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

Name: A-GW
OS: Gaia R77.30
Hard Drive: 100 GB
RAM: 16GB

The following Check Point modules should be installed and configured:

- Security Gateway

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

IP Address: 10.1.1.1
Subnet Mask: 255.255.255.0
Interface: eth0
Network: Alpha Management (LAN 1)

IP Address: 203.0.113.1
Subnet Mask: 255.255.255.0
Default Gateway: 203.0.113.254
Interface: eth3
Network: External (vmnet8 - NAT)

IP Address: 192.168.11.1
Subnet Mask: 255.255.255.0
Interface: eth1
Network: Alpha Internal (LAN 11)

IP Address: 192.168.12.1
Subnet Mask: 255.255.255.0
Interface: eth4
Network: Alpha DMZ (LAN 12)

A-Host

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

Name: A-Host
OS: Windows 7, 8, or 10
Hard Drive: 100GB
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. Install and configure an updated web browser.

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

3. If using Windows 7, install and update the virtual machine with the latest Microsoft security patch. Ensure that the Microsoft security patch described in KB3033929 is applied to the machine. Skip this step if using Windows 8 or 10.

A-LDAP

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

Name: A-LDAP
OS: Windows Sever
Hard Drive: 60GB
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 A-LDAP to be the DNS server for alpha.

2. A-Host and A-GUI should be a part of the alpha.cp domain.

A-DMZ

Use the information below to configure the virtual machine:

Name: A-DMZ
OS: Windows Server
Hard Drive: 60GB
RAM: 2GB

Use the following information to configure the interface for mail 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:

1. Install and configure a web server.
2. Create a simple HTML web page with a hyperlink to the malicious sample.
3. Sample malicious files can be downloaded from Check Point Threat Wiki.

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 traffic out through the host machine's physical address.

External interfaces of the Security Gateway in the topology should point to 203.0.113.254. Network routes for the internal networks should be placed on the Security Gateway.

Configuring the Alpha Security Policy

The Alpha Gateways and Management Servers should be configured and licensed before the students arrive for class. Here is a screenshot of the required initial Security Policy for Alpha:

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	Comment
1	51K	Noise	Any	Any	Any Traffic	udp-high-ports bootp NBT	drop	None	Policy Targets	Any	
2	89K	DNS	Any	Any	Any Traffic	dns ntp	accept	None	Policy Targets	Any	
3	4K	LDAP	Any	Any	Any Traffic	ldap_udp ldap-ssl ldap	accept	None	Policy Targets	Any	
4	3K	Management	Any	A-GW	Any Traffic	https ssh_version_2	accept	Log	Policy Targets	Any	
5	116	Stealth	Any	A-GW	Any Traffic	Any	drop	Log	Policy Targets	Any	
6	795	DMZ	Any	A-DMZ	Any Traffic	smtp https http imap pop-3 ftp HTTP_and_HTTPS_proxy	accept	Log	Policy Targets	Any	
7	19K	Outgoing	ALPHA-NET-GR	Any	Any Traffic	smtp https http ftp	accept	Log	Policy Targets	Any	
8	24K	Cleanup	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any	

For the DMZ rule, it is important to to allow port 8080 traffic from the web server in A-DMZ.

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

Check Point objects (for 10.1.1.101)

- A-SMS
- A-GW

Nodes

- A-DMZ
- A-GUI
- A-LDAP

Networks

- ALPHA-DMZ-NET
- ALPHA-INT-NET

- ALPHA-MGMT-NET
- CP_default_Office_mode_address_pool

Group

- ALPHA-NET-GROUP

Address Ranges

- All_Internet
- LocalMachine_Loopback

Dynamic objects

- AuxiliaryNet
- CPDShield
- DMZNet
- InternalNet
- LocalMachine
- LocalMachine_All_Interfaces

Check Point objects (for 10.1.1.102)

- A-EMS