

Installing Security Gateway

In this section, we will cover deployment and initial configuration of a Security Gateway.

Note: Kindly make sure the IP address are different here as compared to the videos so make sure to have the IP address same as in the lecture to follow us side by side.

Deployment

As mentioned in our lecture, Security Gateway can be deployed in three different options:

1. Check Point Security Appliance;
2. Open Server;
3. A Virtual Machine.

Note: in the practical part of this lecture, we will be installing our lab Security Gateway as a virtual machine.

Check Point Security Appliance

With Check Point, there are four categories of Security Gateway Appliances:

- Small and Medium Business,
- Enterprise,
- High End Enterprise and Data Center,
- Large Data Centers and Telcos, also known as Scalable Platforms (SP).

Note: SMB and SP appliances use different OS and software and are not part of our discussion.

Appliance	Model	SecurityPower™ Units (SPU)	Software			Hardware			
			Threat Prevention	SendBlast	Virtual System	Remote Mgmt (LOM)	10GbE Conn	Redundant Power Supplies	40GbE Conn
Large Data Centers and Telcos	66000	66000	●	●	●	●	●	●	●
	66000	33000	●	●	●	●	●	●	●
High End Enterprise and Data Center	22800	22800	●	●	●	●	●	●	●
	22800	6300	●	●	●	●	●	●	●
	22800	5500	●	●	●	●	●	●	●
	15600	3850	●	●	●	●	●	●	●
	15600	2400	●	●	●	●	●	●	●
Enterprise	5900	2400	●	●	●	●	●	●	●
	5800	1750	●	●	●	●	●	●	●
	5600	950	●	●	●	●	●	●	●
	5600	600	●	●	●	●	●	●	●
	5200	425	●	●	●	●	●	●	●
	5100	340	●	●	●	●	●	●	●
Small Business and Branch Offices	2200	250	●	●	●	●	●	●	●
	2100	160	●	●	●	●	●	●	●
	1690	233	●	●	●	●	●	●	●
	1670	194	●	●	●	●	●	●	●
	1650	141	●	●	●	●	●	●	●
	1620	75	●	●	●	●	●	●	●
	1200B	49	●	●	●	●	●	●	●

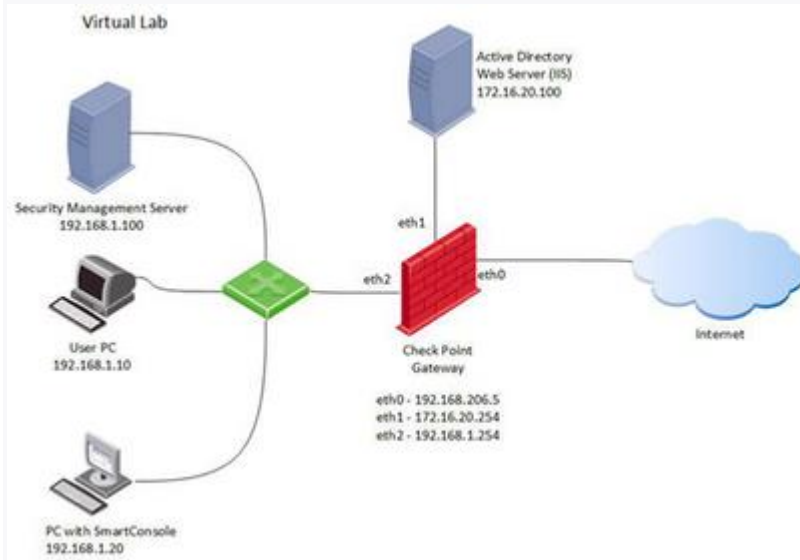
Similar to what we have [noted previously](#) for the [case of Smart-1 deployment](#), Check Point Security Gateway comes preinstalled with at least one version of Check Point Gaia software. If you want to re-image the appliance or install a software version different from the available factory defaults, look into [sk65205](#).

Open Server / virtual machine

If you are deploying your Security Gateway on an Open Server or as a virtual machine, consult with the [Hardware Compatibility List](#) to make sure your deployment option is supported by Check Point. Installation flow for open server and a virtual machine is practically identical.

Installing a Software Gateway

In our lab, we will be installing a Security Gateway as a virtual machine. Let us review the lab configuration:



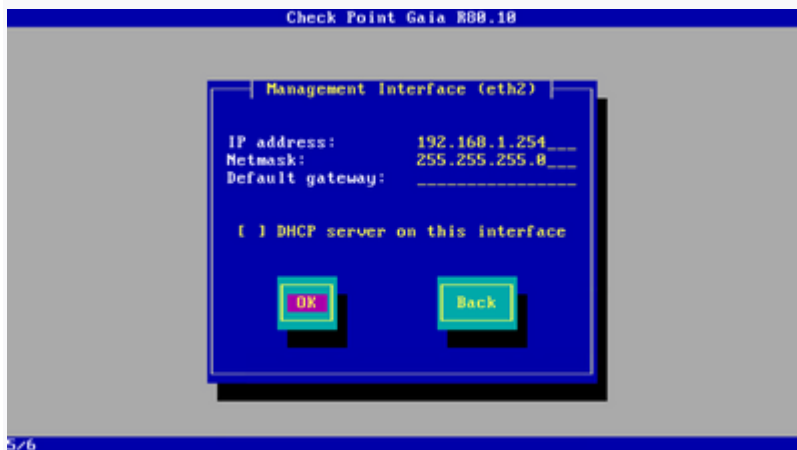
Create a new virtual machine with the following parameters:

▼ Devices	
Memory	4 GB
Processors	2
Hard Disk (SCSI)	50 GB
CD/DVD (IDE)	Using file C:\Use...
Network Adapter	NAT
Network Adapter 2	Custom (VMnet1)
Network Adapter 3	Custom (VMnet2)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Note there are three different NICs defined. The initial installation flow is very similar to the Management Server installation covered in the [previous lecture](#). The only difference is about configuring interfaces.



At this step, choose NIC that shares a network with Lab User PC (VMnet2). In our case, it is eth2. Set up IP as 192.168.1.254/24 and leave **Default gateway** settings empty.




Continue the installation and reboot.

Initializing Security Gateway

Initialization process is very similar for any Gaia based deployment: an appliance or open server, management or gateway. You are already familiar with the process [from the last lecture](#).

In your browser, connect to <https://192.168.1.254> and login with admin user and the password you have defined during installation process (vpn123 in our case). Start the First Time Configuration Wizard and choose "Continue with R80.10 configuration".

Leave interface eth2 settings as is.

Management Connection 

Interface: eth2

Configure IPv4:

IPv4 address:

Subnet mask:

Default Gateway:


Configure IPv6:


IPv6 Address:

Mask Length:

Default Gateway:

Wizard will advise you to set up other interfaces. Skip them at this point by pressing Next. We will set up other networks later on.

Internet Connection 

Configure the interface to connect to the internet (optional) 

Interface:

Configure IPv4:

IPv4 address:

Subnet mask:

Configure IPv6:

IPv6 Address:

Subnet:

In Device Information menu, set up the machine hostname (SG), domain name (testlab.local) and the Primary DNS Server (8.8.8.8):

Device Information

Check Point
SOFTWARE TECHNOLOGIES LTD.

Host Name: SG

Domain Name: testlab.local

Primary DNS Server: 8.8.8.8

Secondary DNS Server:

Tertiary DNS Server:

Proxy Settings

Use a Proxy server

Address:

Port: 8080

< Back Next > Cancel

Leave Date and Time as default and press Next.

Choose “Security Gateways and/or Security Management” for Installation Type and press Next:

Installation Type

Check Point
SOFTWARE TECHNOLOGIES LTD.

Security Gateway and/or Security Management

Multi-Domain Server

< Back Next > Cancel

For Products, chose **only** Security Gateway. Press Next to continue.

Products

Check Point
SOFTWARE TECHNOLOGIES LTD.

Products

Security Gateway
 Security Management

Clustering

Unit is a part of a cluster, type: ClusterXL

Define Security Management as: Primary

Automatically download Blade Contracts and other important data (highly recommended)
For more information click [here](#)

< Back Next > Cancel

Choose No for Dynamically Assigned IP (DAIP) and press Next:

Dynamically Assigned IP

Check Point
SOFTWARE TECHNOLOGIES LTD.


Does this gateway have a dynamically assigned IP address (DAIP gateway)?

Yes
 No

< Back Next > Cancel

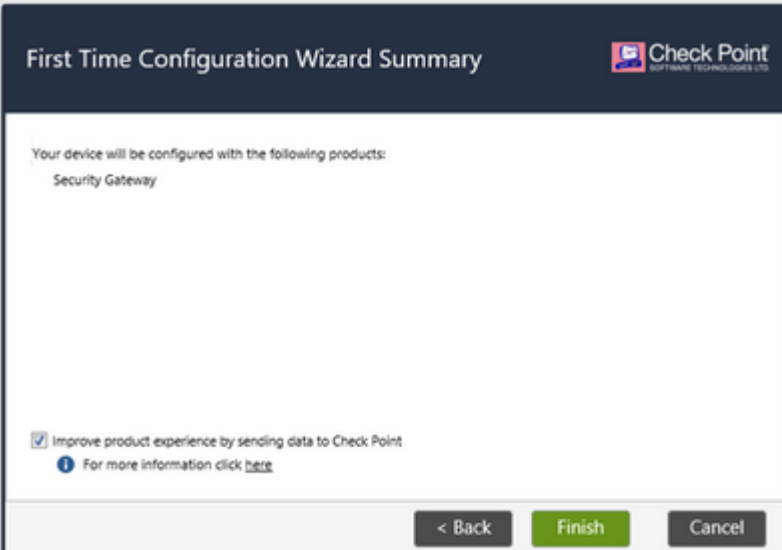
The last part of the Wizard is about SIC – Secure Internal Communication. In a few words, all parts of Check Point based Security System are using TLS encrypted channel to interconnect. This tunnel is known as SIC. It uses certificate based encryption. Certificates are issued by the Management Server and are initialized with an activation key we are defining at this step.

For further information about SIC, feel free to click on “learn more about SIC” link in the menu.



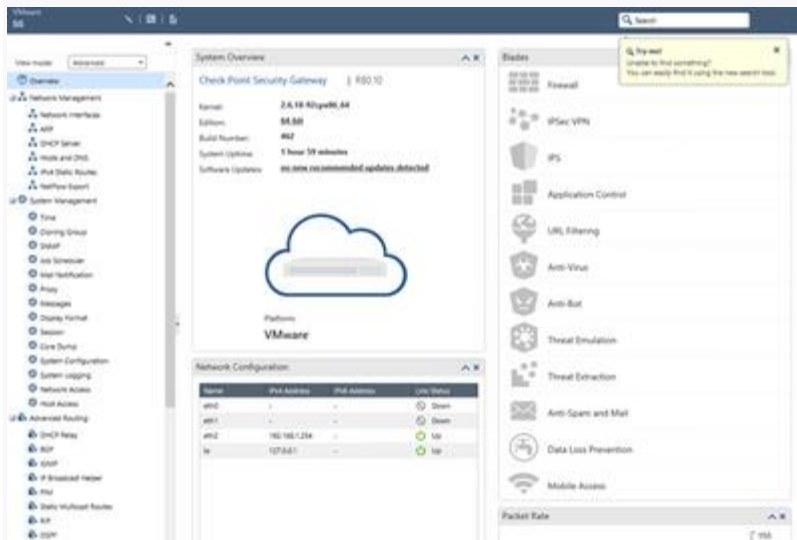
The screenshot shows the 'Secure Internal Communication (SIC)' configuration screen. At the top left, the title 'Secure Internal Communication (SIC)' is displayed. At the top right, the Check Point logo and 'SOFTWARE TECHNOLOGIES LTD.' are visible. The main content area contains two input fields: 'Activation Key:' and 'Confirm Activation Key:'. Both fields contain a series of dots representing masked characters. To the right of these fields is a progress indicator consisting of a horizontal bar with an orange segment on the left and a white segment on the right, followed by the word 'Medium'. Below the input fields is a link that says 'Learn more about SIC'. At the bottom of the screen, there are three buttons: '< Back', 'Next >' (highlighted in green), and 'Cancel'.

Press Finish to conclude the initialization process. The machine will reboot.



The screenshot shows the 'First Time Configuration Wizard Summary' screen. At the top left, the title 'First Time Configuration Wizard Summary' is displayed. At the top right, the Check Point logo and 'SOFTWARE TECHNOLOGIES LTD.' are visible. The main content area contains the text 'Your device will be configured with the following products:' followed by 'Security Gateway'. Below this, there is a checkbox that is checked, with the text 'Improve product experience by sending data to Check Point'. Underneath the checkbox is a small information icon and the text 'For more information click [here](#)'. At the bottom of the screen, there are three buttons: '< Back', 'Finish' (highlighted in green), and 'Cancel'.

After reboot, you will be able to login into Gaia WebUI, same as in the case of SMS in the [previous lecture](#).



Congratulations, you have successfully finished installation and initial configuration of two major elements of Check Point security system: Security Management and Security Gateway.