

Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

CCSA

**FireWall Gateway
Installation**

Step by Step Configuration Guide

Intellectual Property

*The Copyright in this work is vested in **Fortray Networks Limited** and the document is issued in confidence for the express purpose for which it is supplied. It must not be reproduced, in whole or in part, or be used for any other purpose without prior written consent being obtained from **Fortray Networks Limited**, and then only on the condition that this notice be included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party without the prior written consent of **Fortray Networks Limited**.*

© Copyright Fortray Networks Limited 2011-2020

Table of Contents

1.	Version Control	4
2.	Reference Document	4
3.	Assumption	4
4.	Network Topology	5
5.	Check Point - Security Gateway Configuration Task	6
6.	Check Point First Time Configuration	7
6.1	STEP 1: CLICK “NEXT”	7
6.2	Step 2: Choose “Setup”	8
6.3	Step 3: Assign an IP	9
6.4	Step 4: FW/SMS Name, Domain, DNS, Proxy.....	10
6.5	Step 5: Select Time and Time ZONE.....	11
6.6	Step 6: Select Gateway / Multi-Domain Server	12
6.7	Step 7: Select Security Gateway	13
6.8	Step 8: Define a SIC	14
6.9	Step 9: Summary & Finish	15
6.10	Step 10: Summary	16
6.11	Step 11: Finish & Reboot.....	17
7.	Verification	18



1. Version Control

Version	Date	Notes	Created By	Release
1.0	18/12/2018	Student Workbook for LAB	Mazhar Minhas	Initial Release
1.1	07/04/2020	Formatting	Farooq Zafar	Final Release

2. Reference Document

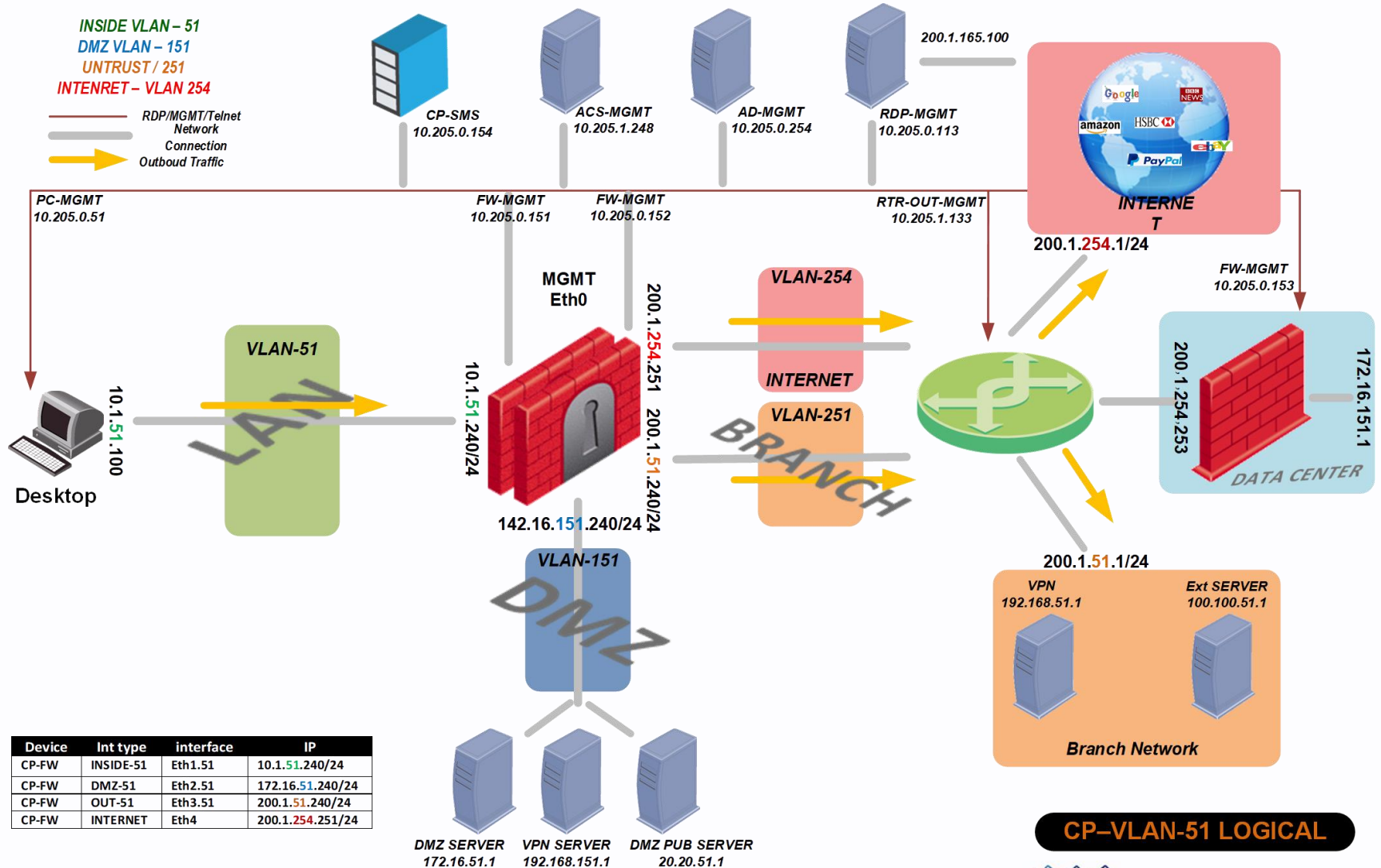
[Click for the Reference document](#)

3. Assumption

- ✓ We understand that delegate already understand L2/L3, Routing.
- ✓ The delegate already knows the “**Fortray Networks – Checkpoint Firewall**” physical and logical connection.
- ✓ The delegate already has basis Troubleshooting skill, such as ping and trace.
- ✓ The delegate already has access to the “**Fortray Networks – Checkpoint Firewall**” Spreadsheet encompassing the Basic Layer, 2, 3 and allocated subnet information. For more details refer to the “**Student Folder**”.
- ✓ This document is created to show an example for one topology only. The candidate needs to refer to his own topology and follow this step by step guide.
- ✓ We assume that delegate already have installed the VPN software and him/she have VPN user / Password. If any issue, contact our Technical team.
- ✓ Our VPN software is supported by PC, MAC, Android, and IOS devices.
- ✓ It’s also assumed that delegate has access to PC/Laptop i5 with 4GB RAM.
- ✓ For optimal connectivity, we recommend at least 10MB Internet connection.
- ✓ We assume that we already have INTERNAL, DMZ, OUTSIDE interfaces are already configured.

4. Network Topology

The below network topology is just for information purpose only. Please refer to your student folder and your designated topology. If any doubt, please ask your instructor.



CP-VLAN-51 LOGICAL

5. Check Point - Security Gateway Configuration Task



Whether this is a new device from the box or you reset to factory default, we need to assign the role to the box. Is it SMS or Gateway?



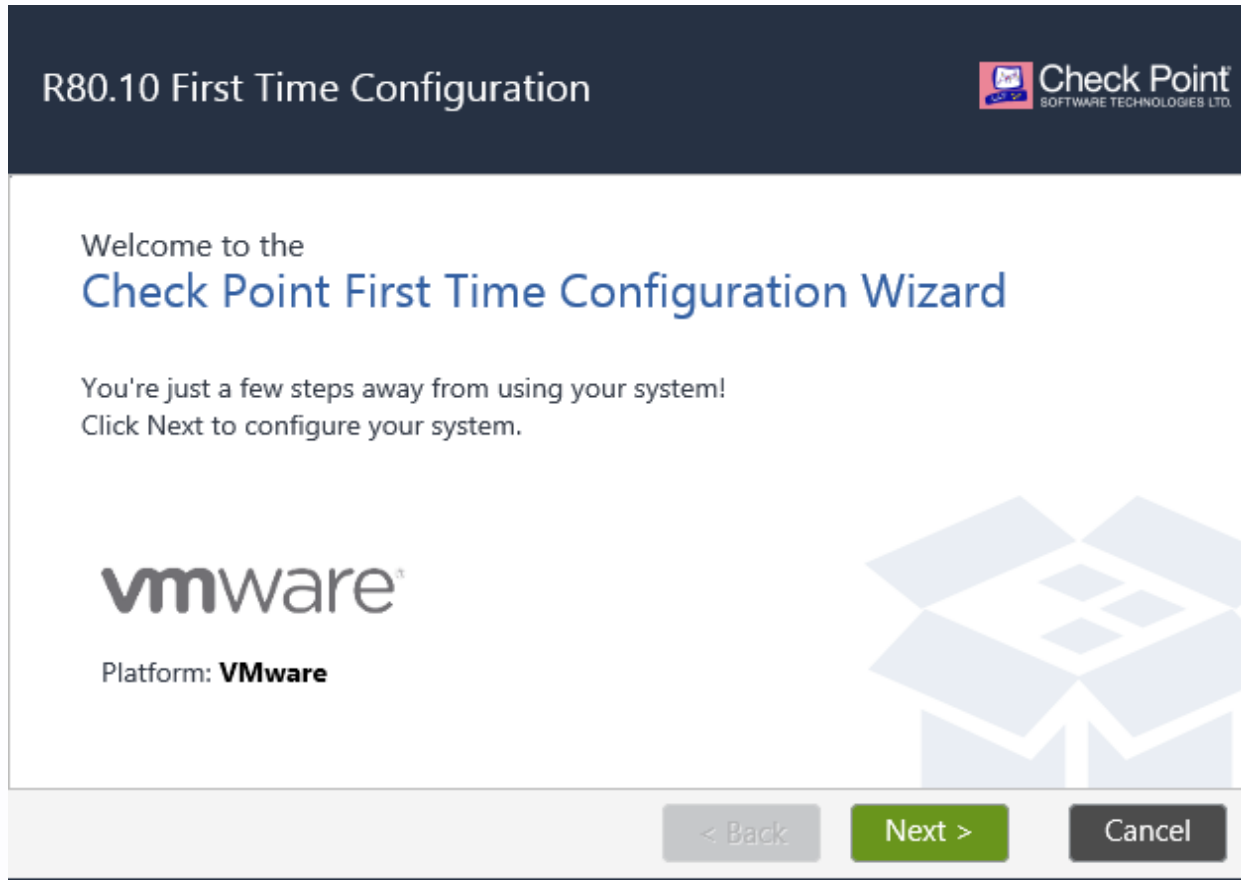
In the below guide, we show how to configure a check Point SMS (which act as a standalone box to manage others or you can configure in the HA (high availability)



When your first-time plug-in Firewall box or Start VM imagine the first time, you must set parameters.

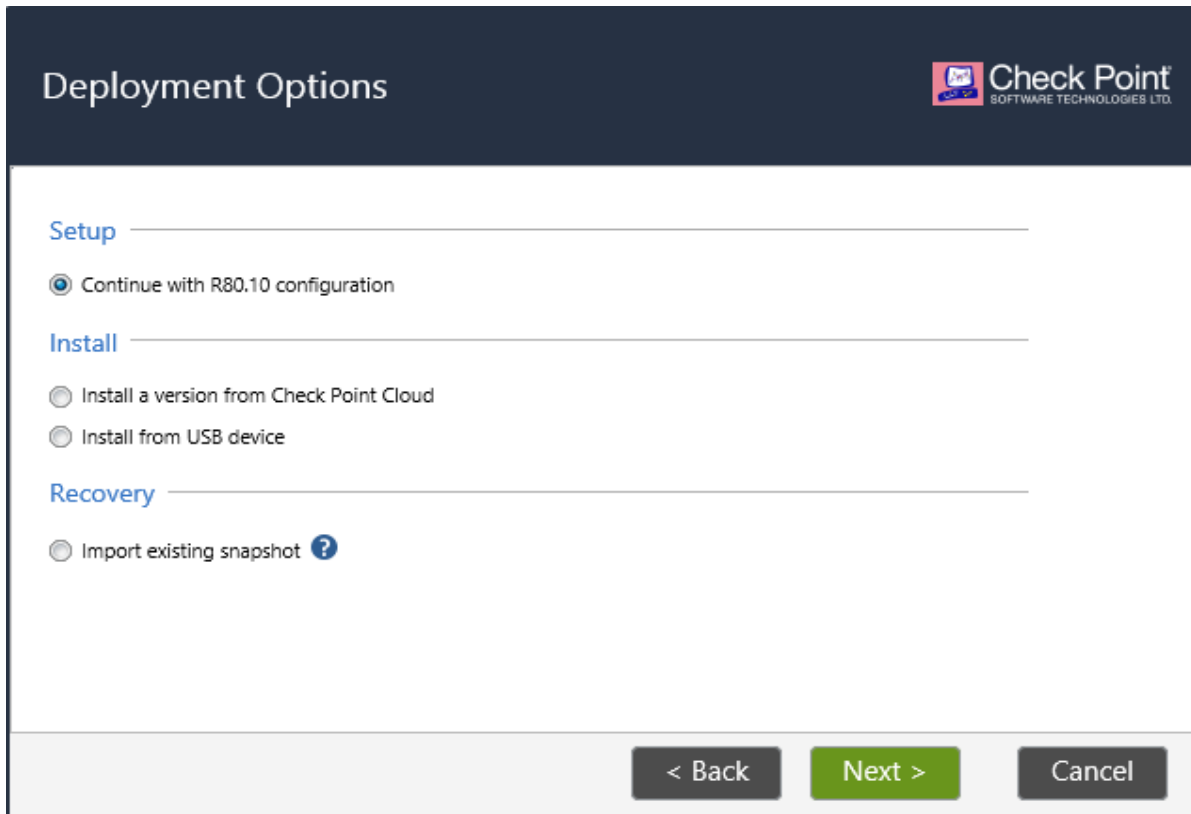
6. Check Point First Time Configuration

6.1 STEP 1: CLICK “NEXT”




6.2 Step 2: Choose “Setup”

Setup – Fresh install without backing up any configuration



6.3 Step 3: Assign an IP

Assign the IP as per your network design. This IP will be used for https/SSH later, Type IP Address 10.205.0.152 for Gateway

Management Connection 

Interface: eth0

Configure IPv4:

IPv4 address:

Subnet mask:

Default Gateway:

Configure IPv6:


IPv6 Address:

Mask Length:

Default Gateway:

6.4 Step 4: FW/SMS Name, Domain, DNS, Proxy

Assign the name, domain name, DNS and proxy if required.

Device Information 

Host Name: FN-CP-HO-152

Domain Name: FORTRAY.LOCAL

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 4.4.4.4 X

Tertiary DNS Server:

Proxy Settings

Use a Proxy server

Address:

Port: 8080

< Back Next > Cancel

6.5 Step 5: Select Time and Time ZONE

Set the time zone as per your time zone

Date and Time Settings

Set time manually:

Date: Thursday, December 27, 2018

Time: 12 : 33

Time Zone: Belfast, Europe (GMT)

Use Network Time Protocol (NTP):

Primary NTP server: Example: pool.ntp.org Version: 1

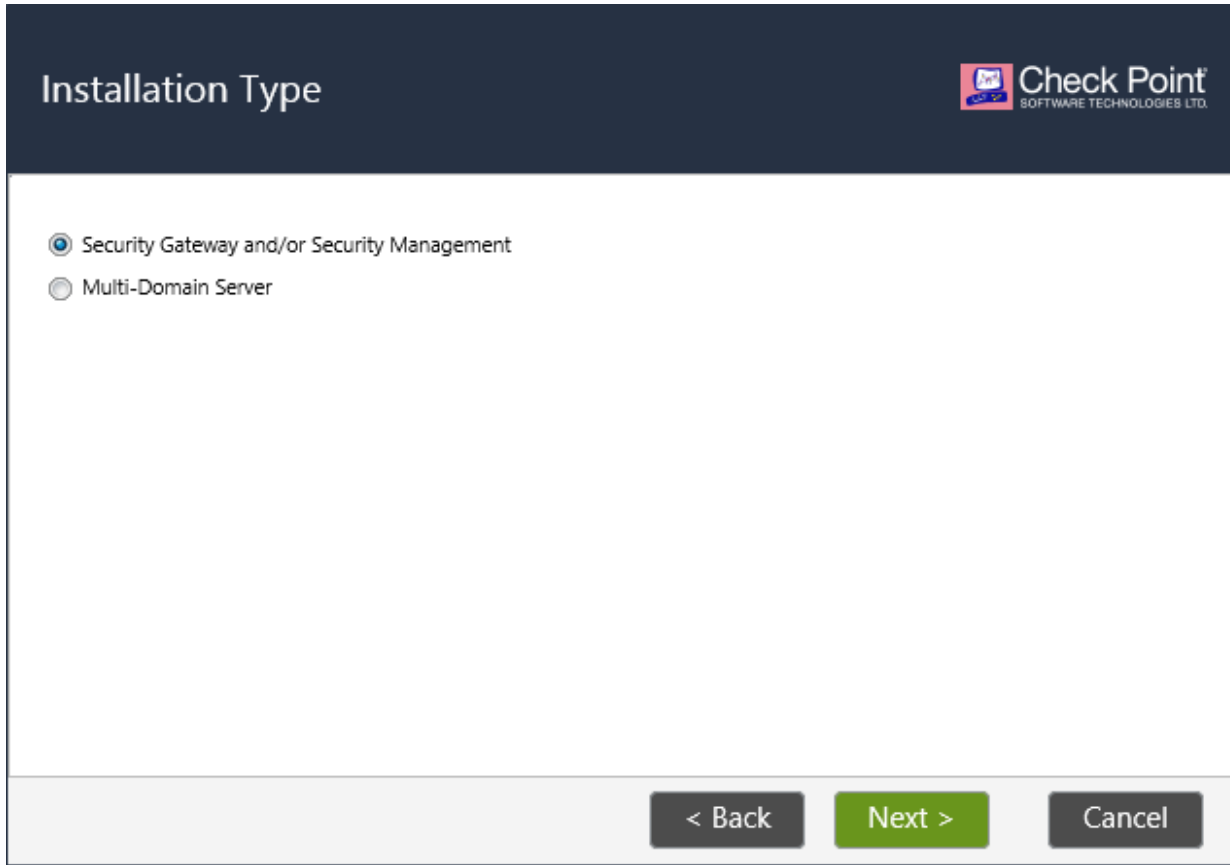
Secondary NTP server: Version: 1

Time Zone: Mawson, Antarctica (GMT +5:00)

< Back Next > Cancel

6.6 Step 6: Select Gateway / Multi-Domain Server

Here we have an option to select this will be Provider-1 which is MDS (Multi-domain Server), in our environment we are using. MDS means 1 x management server will be divided into Multi Management server to manage multiple regions



6.7 Step 7: Select Security Gateway

If we are only creating SMS then we need to select only Security Management or select Gateway if you want this to act as a Gateway.

The screenshot shows the 'Products' configuration page in the Check Point management console. The page is divided into two main sections: 'Products' and 'Clustering'. In the 'Products' section, there are two checkboxes: 'Security Gateway' (checked) and 'Security Management' (selected with a mouse cursor). In the 'Clustering' section, there is a checkbox 'Unit is a part of a cluster, type:' which is unchecked, and a dropdown menu set to 'ClusterXL'. Below this, there is a dropdown menu 'Define Security Management as:' set to 'Primary'. At the bottom of the page, there is a checkbox 'Automatically download Blade Contracts and other important data (highly recommended)' which is checked, and a link 'here' for more information. The page also features navigation buttons: '< Back', 'Next >', and 'Cancel'.

6.8 Step 8: Define a SIC

Here we are defining a one-time password (SIC), which will be used later add/manage via the SMS. For simplicity we are using 123456

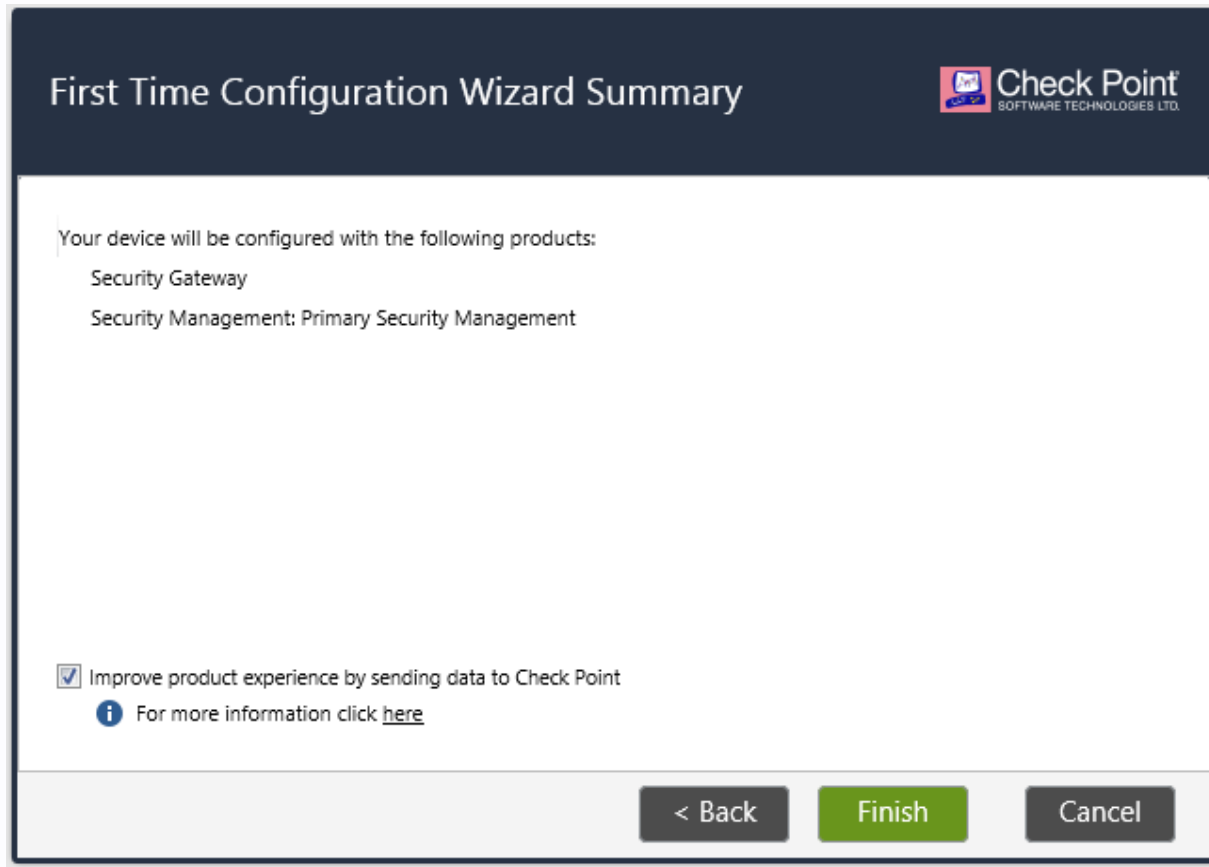
Secure Internal Communication (SIC) 

Activation Key:  Weak

Confirm Activation Key:

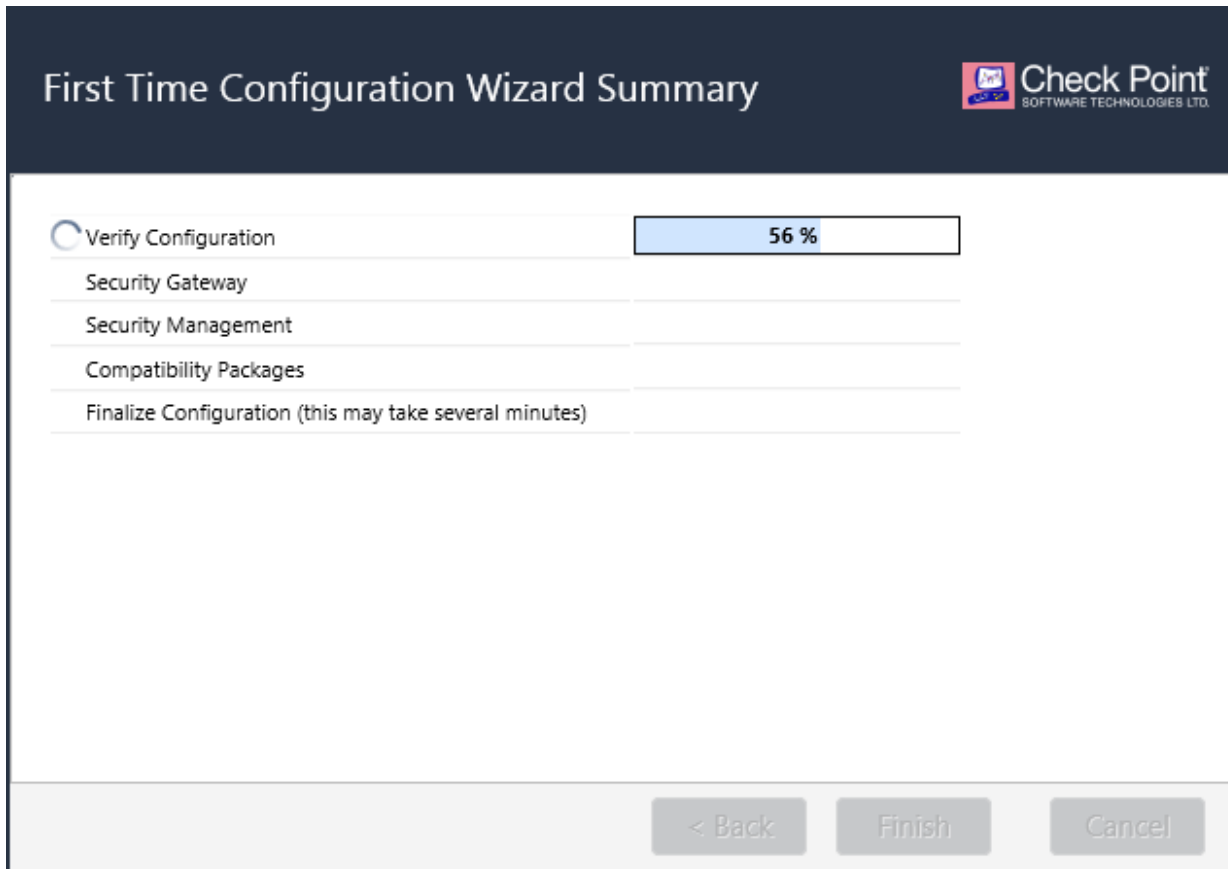
[Learn more about SIC](#)

6.9 Step 9: Summary & Finish

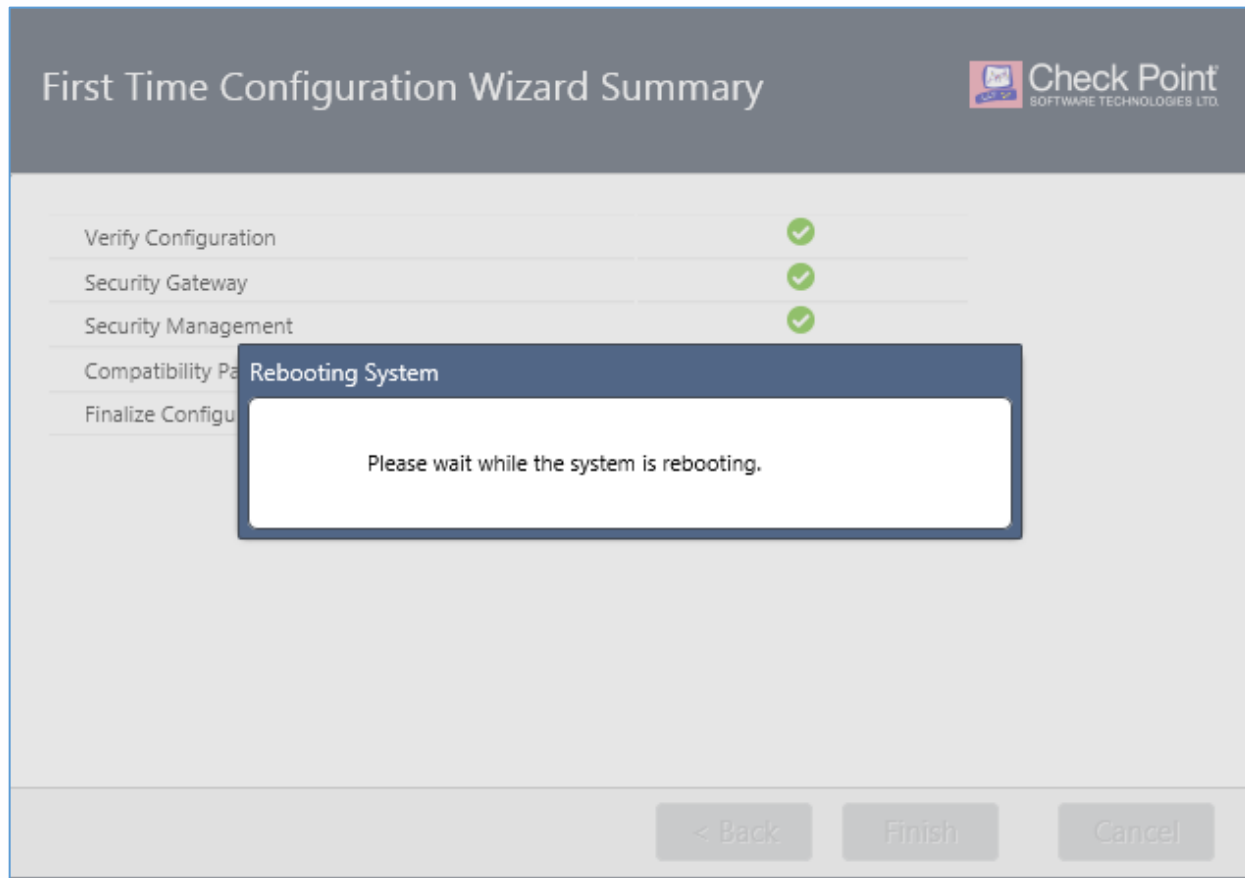


6.10 Step 10: Summary

This will take 5 to 10 min to finish the summary



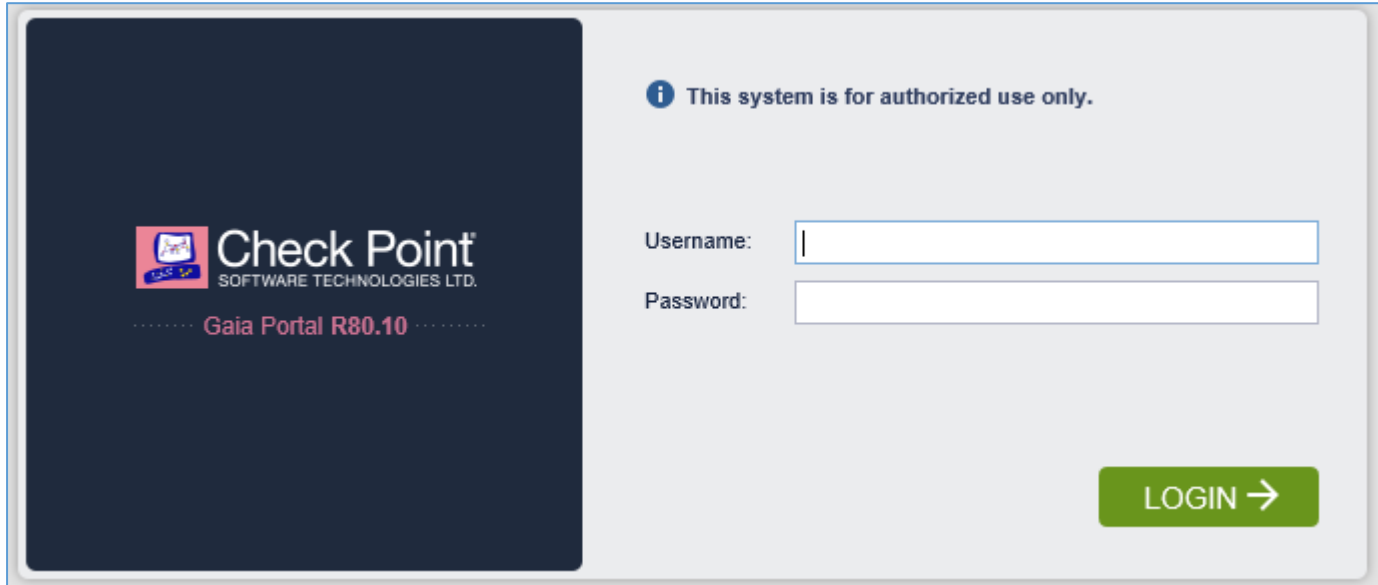
6.11 Step 11: Finish & Reboot



7. Verification

Access the IP 10.205.0.152 from Internet Explorer. And you will be prompted on

Give admin and password ... (Refer to your workbook)



i This system is for authorized use only.

Username:

Password:

LOGIN →

Thanks, and Good Luck

