INS-1 Project

Checkpoint Firewall Key Concepts Covered by this presentation. Made by Mihir Shukla.

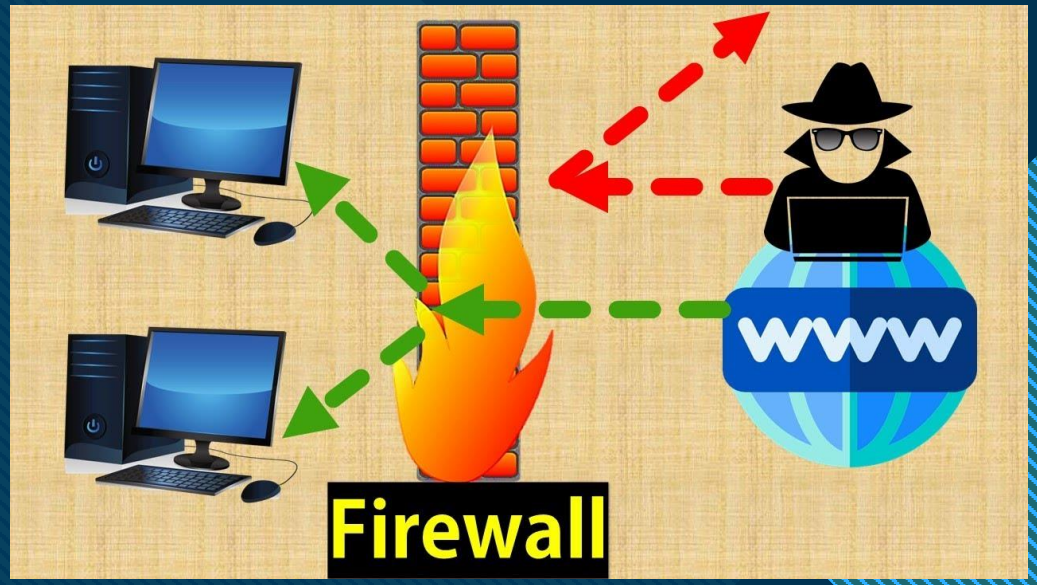
Name: Mihir Shukla

Batch: 1

Enrollment Number:202118100172

Firewall ? What is it ?

A firewall is a network security device or software that monitors, filters, and controls incoming and outgoing network traffic based on predetermined security rules. Its primary purpose is to establish a barrier between a secure internal network and untrusted external networks, such as the internet. Firewalls are a fundamental component of network security and play a crucial role in protecting systems and data from unauthorized access, cyber threats, and malicious activities.



Checkpoint Firewall

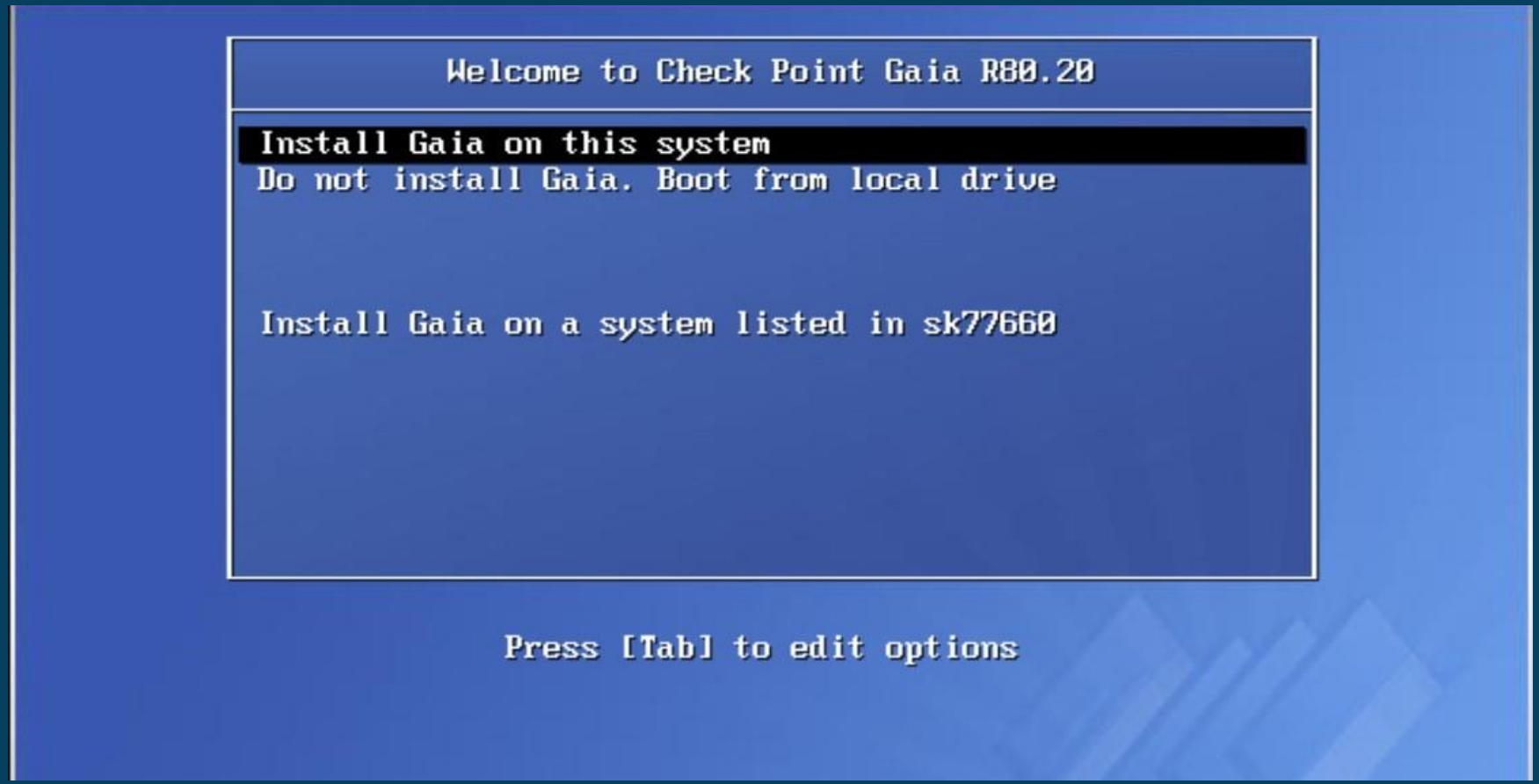
Check Point gateways provide superior security beyond any Next Generation Firewall (NGFW). Best designed for SandBlast's Zero Day protection, these gateways are the best at preventing the fifth generation of cyber attacks with more than 60 innovative security services. Based on the Infinity Architecture, the new Quantum Security Gateway™ line up of 15 models can deliver up to 1.5 Tbps of threat prevention performance and can scale on demand.

https://www.checkpoint.com/quantum/next-generation-firewall/

CHECK POINT™

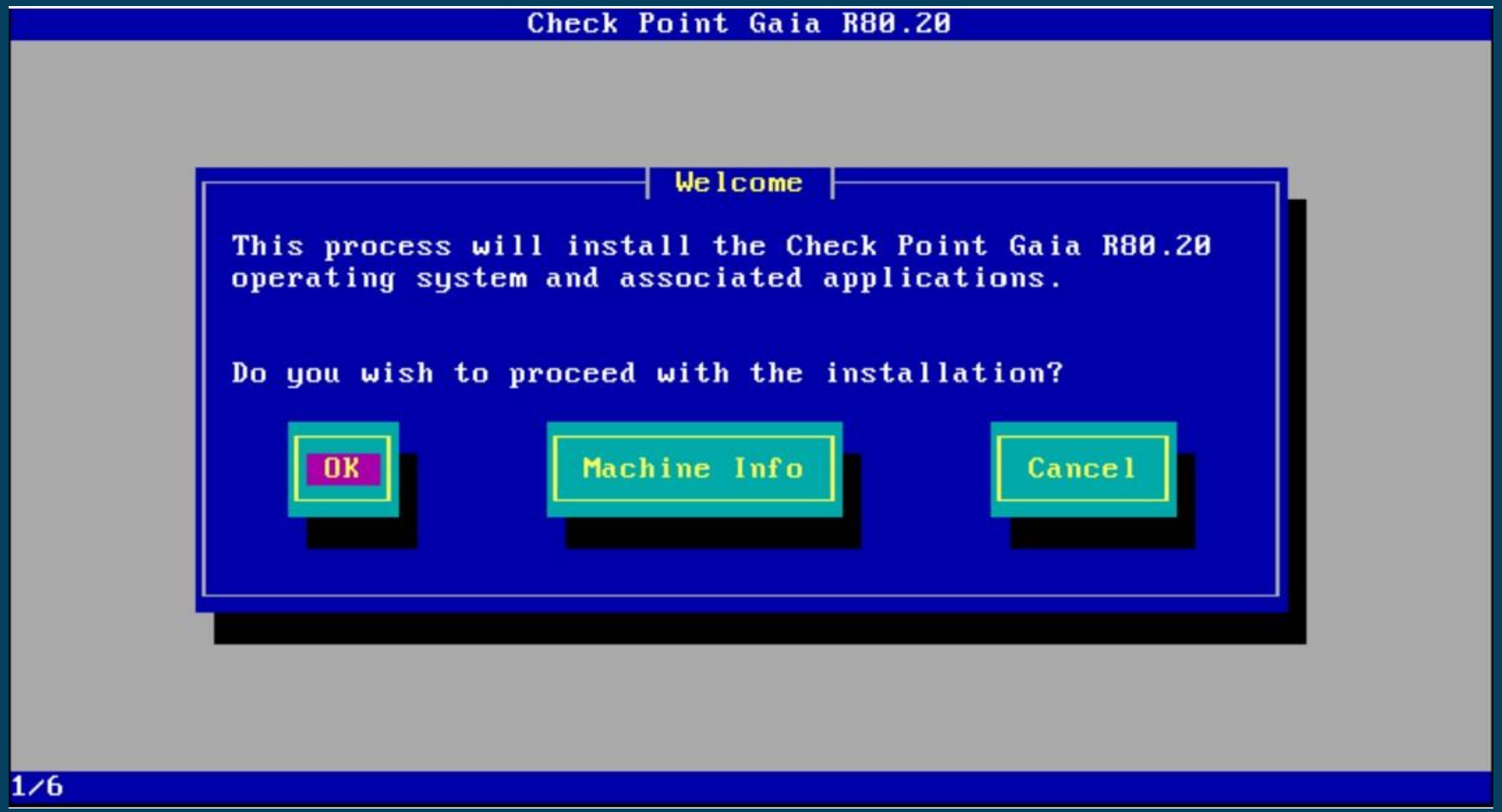
Checkpoint Installation steps:

- Now, create a VM using the downloaded image. Before going forward, you are advised to check release note to get an idea about minimum requirements.
- To install the Check Point Gaia, select "**Install Gaia on this system**" and press ENTER.



Checkpoint Installation steps:

- **Steps in CLI (Wizard):**
- **STEP #1:** A “**Welcome**” window will open and you have to confirm the installation.



Checkpoint Installation steps:

- **STEP #2:** Choose your keyboard type. I am choosing **US** as my keyboard type.

Checkpoint Installation steps:

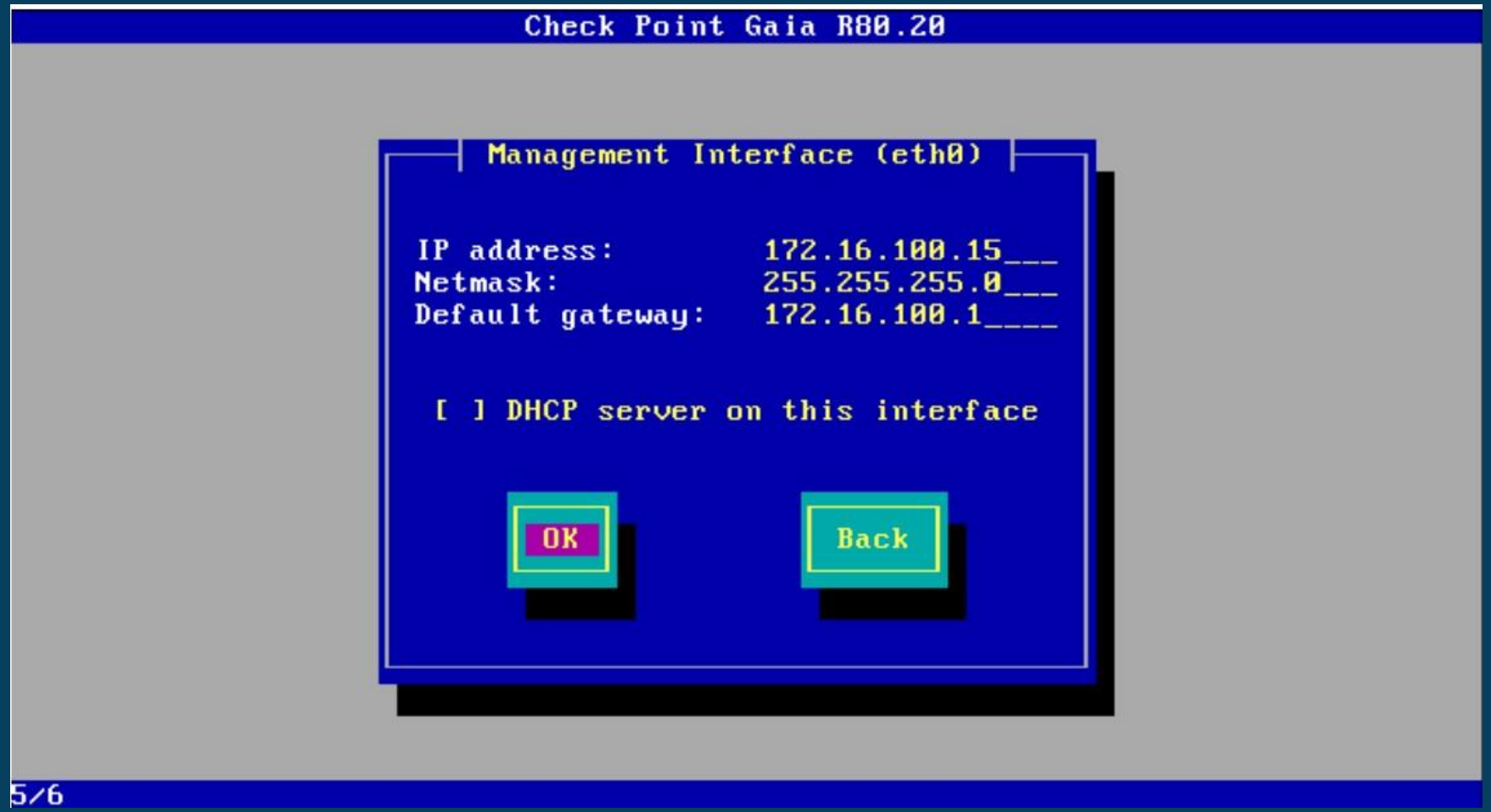
- **STEP #3:** This section is for disk partition ratio. I am OK with default segmentation ratio. However, you can change it according your own requirement. Before changing it, you are advised to check the release note for minimum requirement for each section.

Checkpoint Installation steps:

- **STEP #4:** Put the admin password.

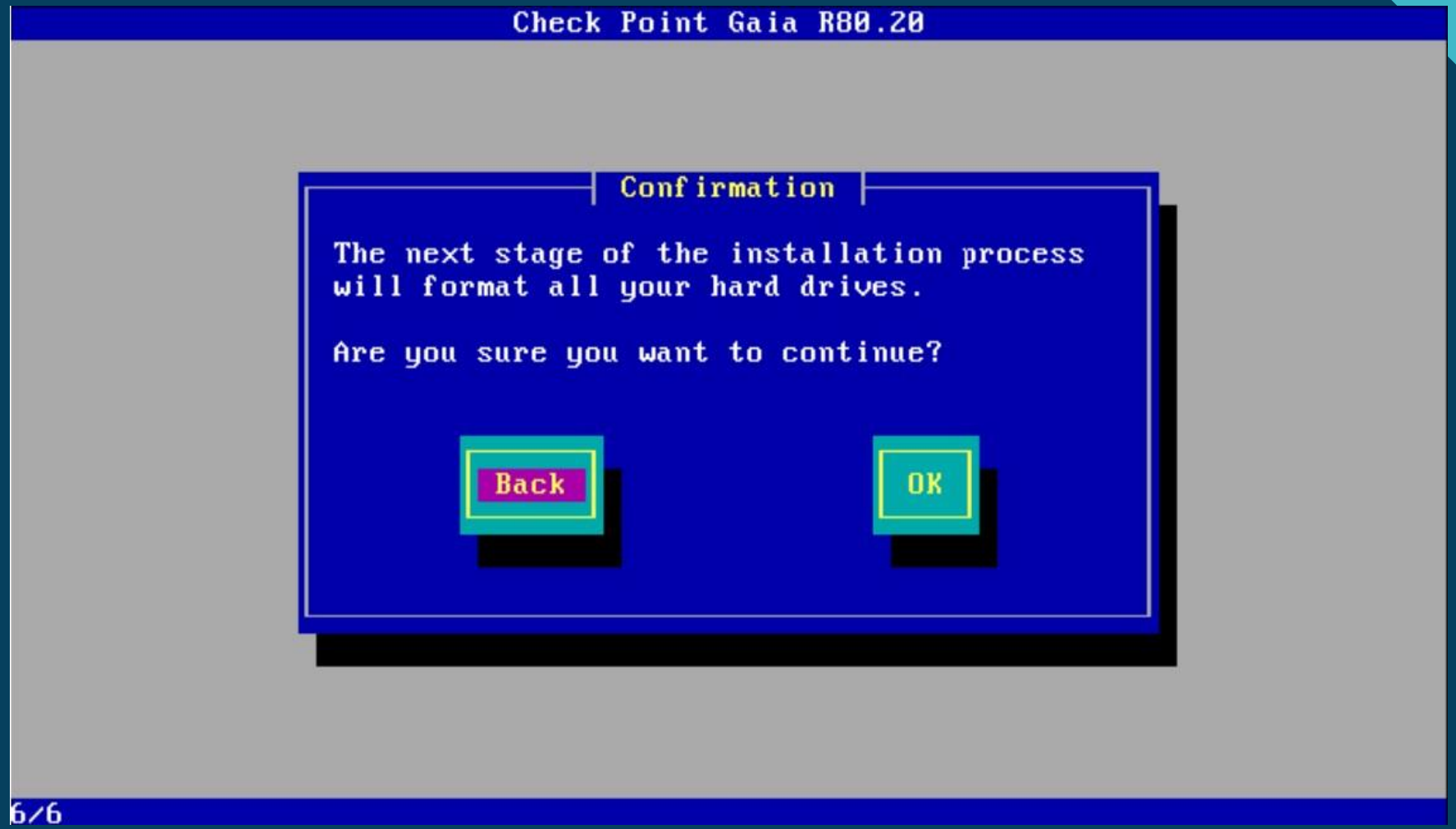
Checkpoint Installation steps:

- **STEP #5:** In this section you have to select management interface. My laptop is logically connected with “**eth0**“, so eth0 is our management interface and we are putting IP address for it.



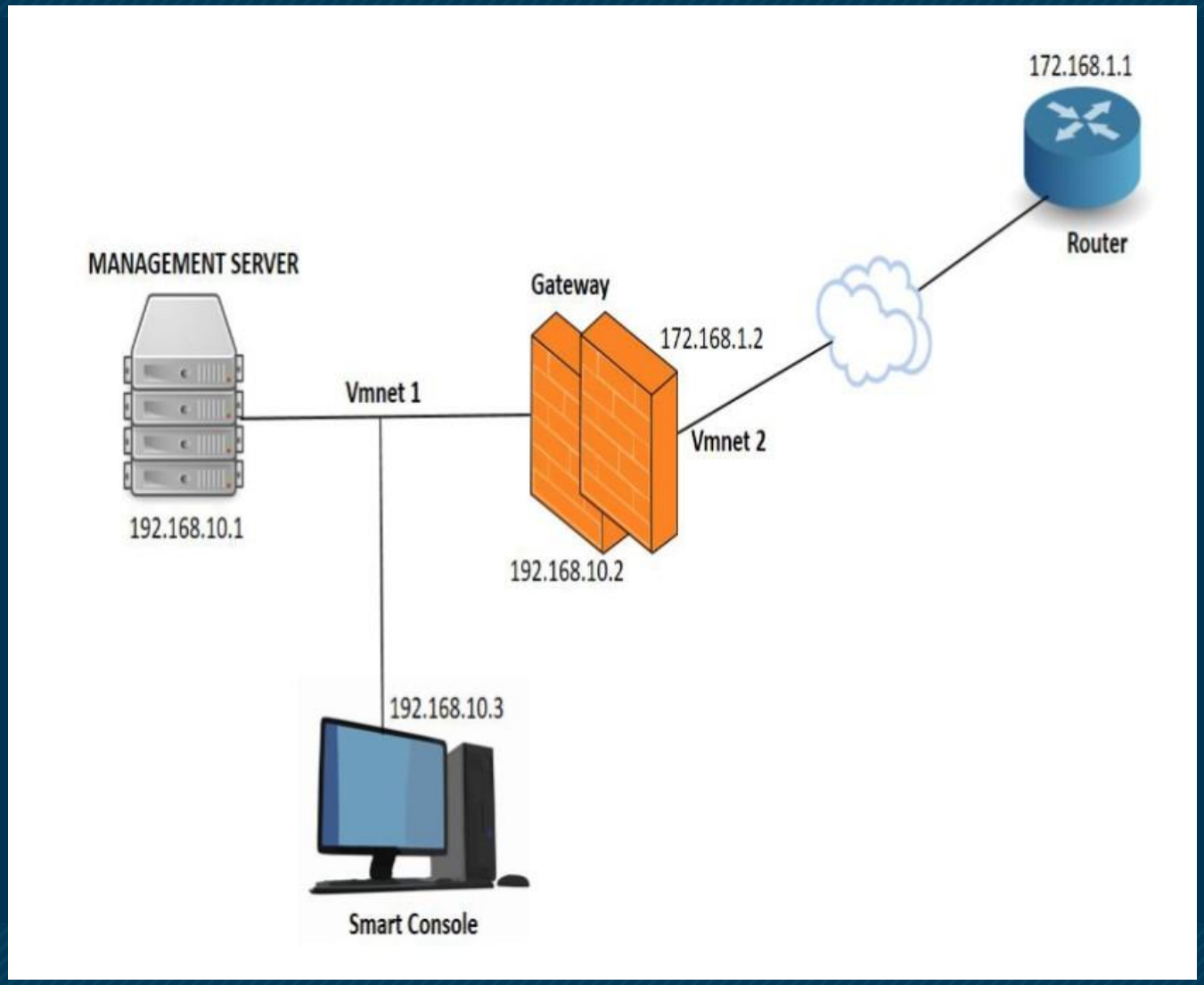
Checkpoint Installation steps:

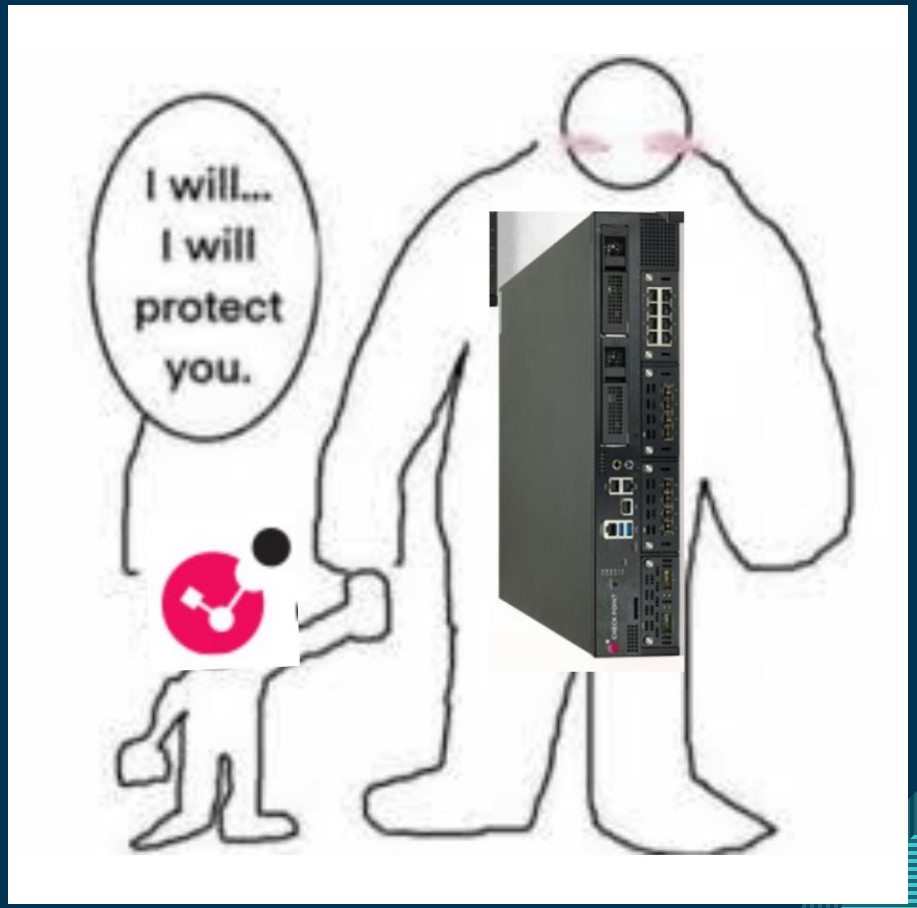
- **STEP #6:** Now confirm to complete all the section and move forward.



- After completing all the steps, open a browser to visit management IP. It will ask to acknowledge the certificate and you must agree to move forward. Login the GUI portal using the admin and the given password.
- And Continue setup in Web Ui

Sample Configuration Of Our Firewall





LAN To WAN Rule:

- Creating a LAN-to-WAN rule in a Check Point firewall involves defining a security policy that allows traffic to flow from devices within the local area network (LAN) to the wide area network (WAN) or the internet. Below are the general steps for creating a LAN-to-WAN rule using the Check Point Security Management Console:

- **Note:** The steps might vary slightly based on the specific version of Check Point software you are using. Always refer to the official documentation for your version.

LAN To WAN Rule:

- **Access Check Point Security Management Console:**
  - Open the Check Point Security Management Console on the device where the firewall is managed.
- **Login:**
  - Log in with administrative credentials.
- **Open Policy Editor:**
  - In the console, navigate to the "Policy" tab or section.
- **Add a Rule:**
  - Add a new rule to the security policy. This rule will specify the permissions for LAN-to-WAN traffic.

LAN To WAN Rule:

- **Define Source and Destination:**
  - In the rule editor, specify the source and destination of the traffic.
    - Source: Define the source as the internal network or specific LAN IP addresses.
    - Destination: Define the destination as "Any" or the specific IP ranges for the WAN/internet.
- **Specify Services:**
  - Define the services or applications that are allowed in the rule. For LAN-to-WAN traffic, you may allow common services like HTTP (port 80), HTTPS (port 443), DNS (port 53), etc.

LAN To WAN Rule:

- **Action:**
  - Specify the action to be taken for the traffic. Typically, for LAN-to-WAN traffic, the action would be "Accept" or "Allow."
- **Install Policy:**
  - After defining the rule, save the changes, and then click on "Install Policy" to apply the new security policy.
- **Verification:**
  - Test the LAN-to-WAN connectivity to ensure that the rule is working as expected. Devices in the LAN should be able to access the internet based on the defined rule.

Create Users & Groups:

1. Log in to the smart console with administrator credentials.

2. To Create Users ,

In the main menu section click on “identity awareness” or “Users” section.

Click on “New” -> User -> Fill in the user details such as username, password, and any other required information -> save the changes.

3. To Create Groups ,

In the main menu section click on identity awareness.

Click on new -> Group -> enter the group name and add members (users, machines, or network objects) to the group -> save the changes.

Multi factor Authentication:

In checkpoint firewall there are different methods for Multi factor authentication of users like :

1. Identity Awareness : This feature allows to authenticate users based on their identity rather than just their IP Address. It can integrate with external authentication servers like Active Directory or LDAP and use additional factors like certificates or tokens for authentication.

2. Two-factor Authentication (2FA) : checkpoint supports 2FA using one time password (OTP), which can be generated through SMS, email, or authenticator apps. This can be configured through the Identity Awareness setting.

Multi factor Authentication:

3. RADIUS server Integration :

checkpoint firewall can integrate with a

RADIUS server that supports multi-factor authentication. The firewall can

then use the RADIUS server for user authentication , including additional

authentication factors beyond just a username and password.

Captive Portal

A Captive Portal is a web page that intercepts and redirects network users to a login, registration, or terms of service page before granting access to the network.

To configure a captive portal :

1. Log in to Management smart console
2. In the object tab select identity awareness -> create a new captive portal object by specifying the necessary parameters such as the authentication method, portal design, and URL
3. Go to the policy tab and create a security rule to define access policies for users accessing the network. Add the captive portal object to the rule as an authentication method or a layer in the security policy.

Captive Portal

4. Ensure identity awareness is enabled in the firewall policy. Configure

identity awareness settings to integrate with the captive portal object

created earlier .

5. Apply the policy changes and test the captive portal functionality by

attempting to access the network from a client device. The portal should

intercept the connection and prompt for authentication or acceptance of

terms of service before granting access.

VPN (SSL VPN)

VPN :Virtual Private Network

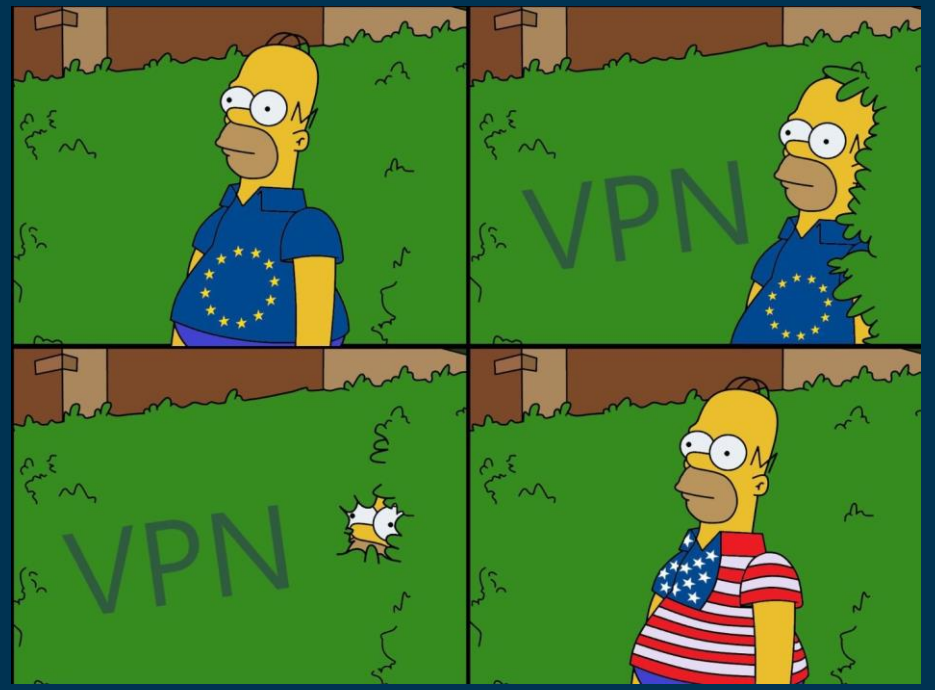
SSL VPN : Secure Sockets Layer VPN

VPN is a technology that allows to create a secure

connection over the internet, providing privacy and

anonymity by encrypting data as it travels between

device and the VPN server .



VPN (SSL VPN)

1. Access to smart console -> policy tab -> select “Global Properties” -> under “Remote access” enable “SSL

Network Extender “ and configure it’s setting.

2. Define rules, access control, and encryption settings for SSL VPN users.

3. Set up VPN profiles that include settings like encryption, authentication, and user access control.

4. Enable the Remote Access VPN blade in the Security Gateway properties.

5. Test the SSL VPN connection with a test user account to ensure proper functionality. Monitor logs and

troubleshoot any issues that may arise during the configuration process.

Sync server with checkpoint firewall

• Synchronization can be establish using various methods such as :

1. Policy Installation: Use SmartConsole to push the security policy

to synchronize rules and settings between the firewall and the

managed servers.

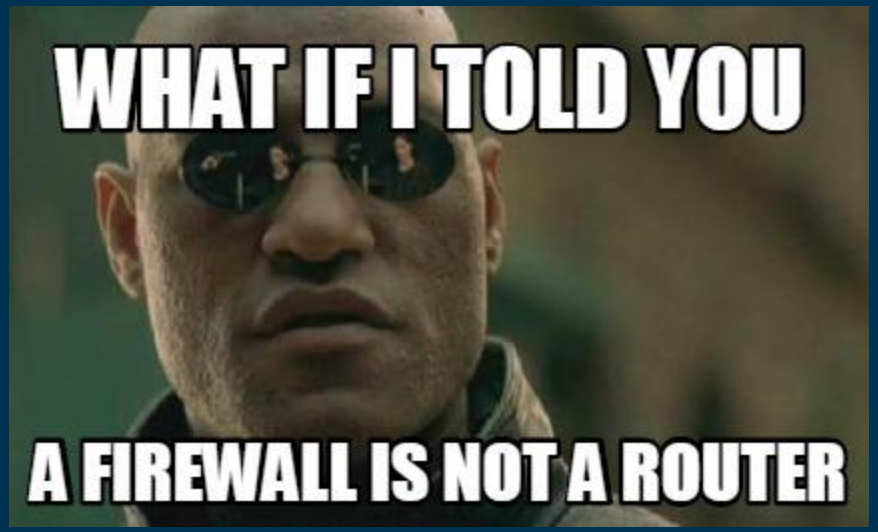
2. Check Point Management API: Leverage the Check Point

Management API to automate and manage the synchronization

process between the server and the firewall.

3. Manual Configuration: Manually configure the server settings to

match the rules and requirements set on the Check Point Firewall.



Passwords are like underwear.
Don’t let people see it, change it very often, and you shouldn’t share it with strangers.”

Thank You!

- **Name: MIHIR SHUKLA**
- **Batch: 1**
- **Enrollment Number.:202118100172**