

Ultimate (paso a paso) Tareas de laboratorio de CheckPoint R81



R81



About Author



He estado en la industria de TI y seguridad durante casi 19 años. En Checkpoint Firewall, he logrado CCSA, CCSE y CCSE+ - Además de obtener experiencia certificada en McAfee SIEM, IBM -QRadar SIEM & BlueCoat Security Analytics (Solera).

El conocimiento del producto incluye firewall de oems múltiples, IPS, visibilidad SSL, SIEM, operaciones SOC, EDR, análisis e investigaciones de seguridad.

Entrega de múltiples implementaciones de seguridad en clientes distribuidos a verticales BFSI, Gobierno, IT-ITES.

Actualmente, estoy tratando de compartir parte de mis conocimientos a través de la enseñanza en línea a través de plataformas en línea y la creación de contenido nuevo, único, simple y de bajo costo para nuevos aspirantes a TI.

Actualmente tengo algunos cursos en línea publicados y también he comenzado mi canal de YouTube. Puedes ver todo el contenido aquí

- <https://www.udemy.com/course/checkpoint-firewall-administration-r80/?referralCode=12398B1EEF83C8D00ECD>
- <https://www.udemy.com/course/isoiec-27001-security-guidelines-for-organizational-users/?referralCode=5E63E591F2B9A9EE8C22>
- <https://www.youtube.com/c/YourITBasicsOnline> (Suscríbete y comparte)
- Enviar por correo a – amit@youritbasics.online

About The Book

Este libro (más de 600 páginas) consta de 25 escenarios de laboratorio (paso a paso) para diferentes escenarios de configuración para CheckPoint Firewall versión R81. La plataforma utilizada para la distribución del laboratorio es un entorno PNET similar a la plataforma EVENG. Se supone que también puede tener un nivel inicial de conocimiento de PNET Labs.

Contents

Tarea de laboratorio 1 ~ Implementación de CheckPoint ISO en un PNET LAB	8
Descargar imagen ISO de CheckPoint R81.....	8
Instalar CheckPoint R81 en PNET.....	8
Agregue el nodo CheckPoint a PNET LAB	12
Tarea de laboratorio 2 ~ Implementación de un firewall de CheckPoint independiente (2 niveles)	14
Configuración del enrutador de Internet	22
Instalación del sistema operativo Gaia	24
Implementación independiente de CheckPoint (2 niveles).....	30
Instalación de la consola inteligente	44
Iniciar sesión en SmartConsole.....	52
Tarea de laboratorio 3 ~ Implementar una política básica de firewall de acceso a Internet	54
Laboratorio de acceso a Internet (breve).....	54
Implementar regla de acceso a Internet	55
Implementar regla de acceso de firewall	63
Instale la política en un firewall independiente	69
Verificar el acceso a Internet desde el cliente GUI	73
Observar registros en Logs & Monitor	73
Tarea de laboratorio 4 ~ Implementación de Distributed CheckPoint Firewall (3 niveles)	76
Configuración del laboratorio de implementación distribuida de CheckPoint en PNET LAB.....	76
Instalación de CP-R81-SmartCenter/servidor de gestión	86
Instalación del módulo de cortafuegos CP-R81	96
Comunicación Interna Segura (SIC) – Integración para Firewall y Management Server	105
Tarea de laboratorio 5 ~ Resolución de problemas con SIC	122
Restablecimiento de SIC en el objeto Firewall en Smart Center Server	122
Restablecimiento de SIC en el módulo de firewall	125
Reconfigurar SIC	127
Tarea de laboratorio 6 ~ Configuración de topología de firewall de CheckPoint	129
Agregue un firewall WAN y un segmento DMZ	129
Instalación de WAN-Firewall y configuración de enrutamiento	136
Direccionamiento IP y enrutamiento en CP-Office-FW	136
Configuración de Topología (Manual) en CP-FW-R81.....	137
Configuración de Topología (Automática) en CP-FW-R81	149
Instalación del módulo de firewall distribuido CP-Office-FW	153
Comunicación interna segura (SIC): integración para firewall WAN y servidor de administración....	160
Agregar una nueva política para CP-Office-FW	165
Tarea de laboratorio 7 ~ Configurar modo experto y habilitar CheckPoint Blades	171
Habilitar el modo experto en el módulo Gaia	171
Habilitación de Blades en el objeto de firewall.....	174

Tarea de laboratorio 8 ~ Reglas implícitas y propiedades globales de CheckPoint	182
Reglas explícitas	182
Reglas implícitas y propiedades globales	182
Primero, último y antes del último Reglas implícitas	188
Tarea de laboratorio: 9 ~ Administrar administradores de seguridad y clientes de GUI de SmartConsole	197
Adición de administradores de seguridad desde Smart Console	197
Adición de administradores de seguridad desde CLISH	202
Administrar clientes GUI a través de CLISH	205
Administre clientes GUI a través de Gaia Web UI	208
Tarea de laboratorio 10 ~ Objetos de política de firewall de CheckPoint	209
Objetos de política de cortafuegos	209
Anfitrión de punto de control	209
Objeto anfitrión	210
Objeto de red	212
Objeto de grupo de red	214
Objeto de rango de direcciones	215
Objetos de servicio (Puertos)	217
Objetos de servicio (rango de puertos)	222
Objetos de tiempo	223
Tarea de laboratorio 11 ~ Capas de políticas de CheckPoint	225
Capas de políticas de cortafuegos	225
Capas ordenadas	225
Capas en línea	225
Agregar capa ordenada	227
Capas compartidas	233
Adición de capas en línea	238
Tarea de laboratorio 12 ~ Implementar una política de firewall optimizada	241
Política de diseño optimizado	241
Uso de Hit Count para optimizar la política	243
Tarea de laboratorio 13 ~ Control de revisión de la base de datos	244
Control de revisión de base de datos	244
Laboratorio de Control de Revisión de Bases de Datos	244
Informe de cambios	251
Informe de laboratorio para el cambio	253
Tarea de laboratorio 14 ~ Operaciones de registro de CheckPoint y administración de archivos de registro	255
Funcionalidad de registro en CheckPoint R81	255
Gestión de archivos de registro	260
Laboratorio de brujas Log S	264
Tarea de laboratorio 15 ~ Traducción de direcciones de red en CheckPoint Firewall	268

Conceptos de traducción de direcciones de red (NAT).....	268
OCULTAR NAT.....	268
NAT ESTÁTICO.....	269
Laboratorio NAT de CheckPoint.....	271
OCULTAR NAT (Configuración automática).....	271
OCULTAR NAT (Configuración manual).....	280
NAT ESTÁTICA (Configuración automática).....	286
NAT ESTÁTICA (Configuración Manual).....	290
Tarea de laboratorio 16 ~ Agrupación de firewall de CheckPoint.....	302
Laboratorio de agrupación en clústeres de CheckPoint.....	302
Instalación del cortafuegos de los miembros del clúster.....	304
Adición de objetos de clúster y miembros de clúster.....	306
Configuración de topología de clúster.....	311
Configuración de clúster de alta disponibilidad.....	316
Pruebas de clúster de alta disponibilidad.....	319
Observar registros de clúster de alta disponibilidad.....	324
Configuración de clústeres activo-activo.....	328
Observar registros de clúster activo-activo.....	330
Tarea de laboratorio 17 ~ Operación SSL, inspección HTTPS de CheckPoint y cuchillas UTM.....	331
Operación SSL (HTTPS) e Inspección SSL (HTTPS).....	331
Inspección HTTPS en CheckPoint (LAB).....	333
Crear certificado de CA saliente en el cortafuegos.....	333
Exportación del certificado.....	333
Habilite la inspección de HTTPS en el firewall.....	334
Configuración y prueba de la política de inspección de HTTPS.....	335
Hoja de control de aplicaciones y filtrado de URL.....	348
Hoja de conocimiento del contenido.....	355
Hoja de prevención de pérdida de datos.....	362
Tarea de laboratorio 18 ~ CheckPoint IPS (notas).....	383
Sistema de prevención de intrusiones (IPS).....	383
Hoja IPS de CheckPoint.....	386
Prevención de amenazas infinitas.....	393
Tarea de laboratorio 19 ~ Prevención de amenazas de CheckPoint (notas).....	395
Amenazas de día cero.....	395
Prevención de amenazas de día cero.....	396
Emulación de amenazas de CheckPoint.....	397
Extracción de amenazas de CheckPoint.....	399
CheckPoint Anti- Bot.....	401
Antivirus Check Point.....	402
CheckPoint Anti-Spam y seguridad del correo electrónico.....	404

Tarea de laboratorio 20 ~ Autenticación de clientes y usuarios de CheckPoint: autenticación heredada

.....	406
Autenticación de usuario	406
Configuración de autenticación de usuario.....	406
Creación de grupos de usuarios.....	408
Crear plantilla de usuario.....	409
Crear usuarios.....	413
Política de autenticación de usuarios.....	416
Autenticación del cliente	421
Configuración de la política de autenticación del cliente.....	421
Propiedades de autenticación de cliente	426
Autenticación del servidor TACACS externo	428
Autenticación del servidor RADIUS externo	431

Tarea de laboratorio 21 ~ Configuración de Blade de reconocimiento de identidad de CheckPoint

.....	434
Reconocimiento de identidad de CheckPoint	434
Instalación del servidor AD	435
Creación de usuarios y grupos en Active Directory Server.....	455
Migración de Nodo LAN a Dominio	468
Configuración de reconocimiento de identidad de CheckPoint.....	472
Configuración de acceso de usuario de Active Directory.....	477
Configuración de acceso de usuario invitado.....	484

Tarea de laboratorio 22 ~ Copia de seguridad de CheckPoint - Restaurar - Instantánea.....

.....	491
Copia de seguridad de punto de control	491
Copia de seguridad mediante la interfaz de usuario web	493
Restaurar mediante la interfaz de usuario web.....	496
Copia de seguridad usando CLISH.....	500
Restaurar usando CLISH	500
Gestión de instantáneas	501
Instantánea usando la interfaz de usuario web.....	501
Reversión de instantáneas mediante la interfaz de usuario web	502
Instantánea usando CLISH	503
Revertir instantánea usando CLISH	504

Tarea de laboratorio 23 ~ Configuración de VPN de sitio a sitio de CheckPoint Firewall

.....	505
Fundamentos de VPN.....	505
Configuración del laboratorio de VPN de CheckPoint	506
Pasos de configuración de Site-to-Site VPN	507
Configuración de VPN en el sitio A	508
Configuración de VPN en el sitio B	525
Pruebas y solución de problemas de VPN.....	542

Tarea de laboratorio 24 ~ Configuración de VPN de acceso remoto de CheckPoint.....

.....	548
Configuración VPN de acceso remoto	548

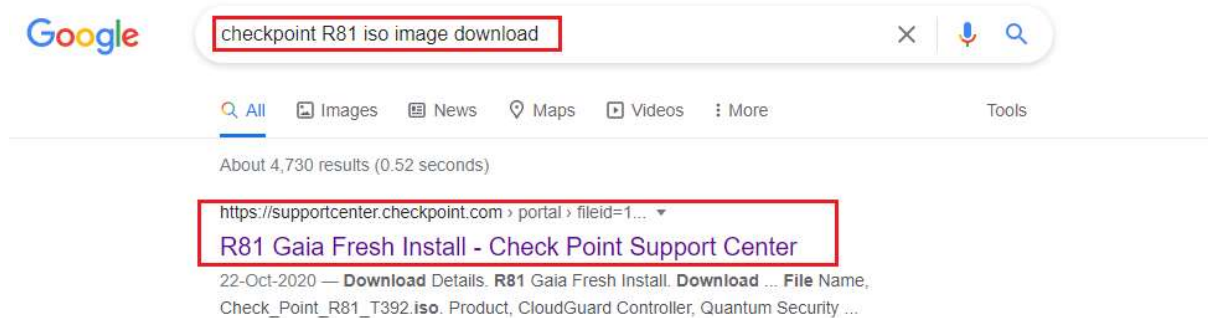
Dominio VPN de acceso remoto	550
Crear grupo de usuarios de VPN y usuario	555
Regla VPN de acceso remoto	560
Descarga e instalación del cliente VPN.....	563
Conexión al sitio VPN	568
Tarea de laboratorio 25 ~ Configuración de VPN SSL de CheckPoint	579
Configuración VPN SSL.....	579

Tarea de laboratorio 1 ~ Implementación de CheckPoint ISO en un PNET

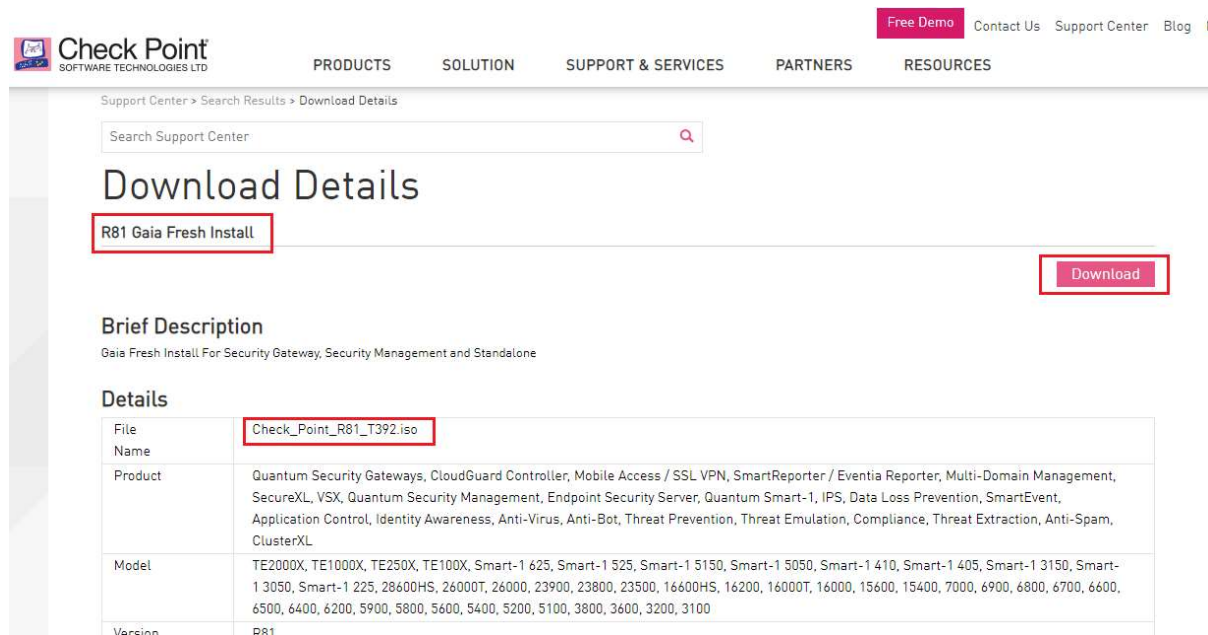
LAB

Descargar imagen ISO de CheckPoint R81

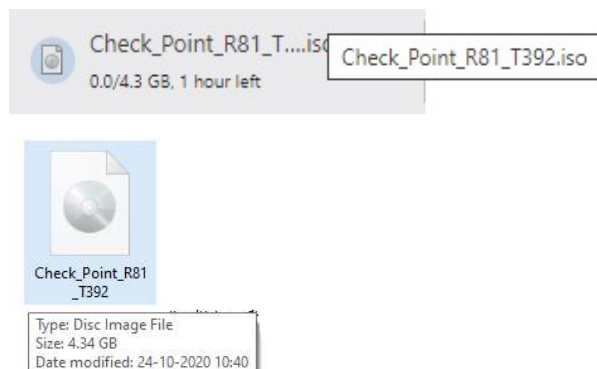
Busque la descarga de la imagen iso del punto de control R81 en Google como se muestra y haga clic en el enlace del centro de soporte.



Será redirigido a la página de descarga. El nombre del archivo es Check_Point_R81_T392.iso. Haga clic en el botón Descargar.



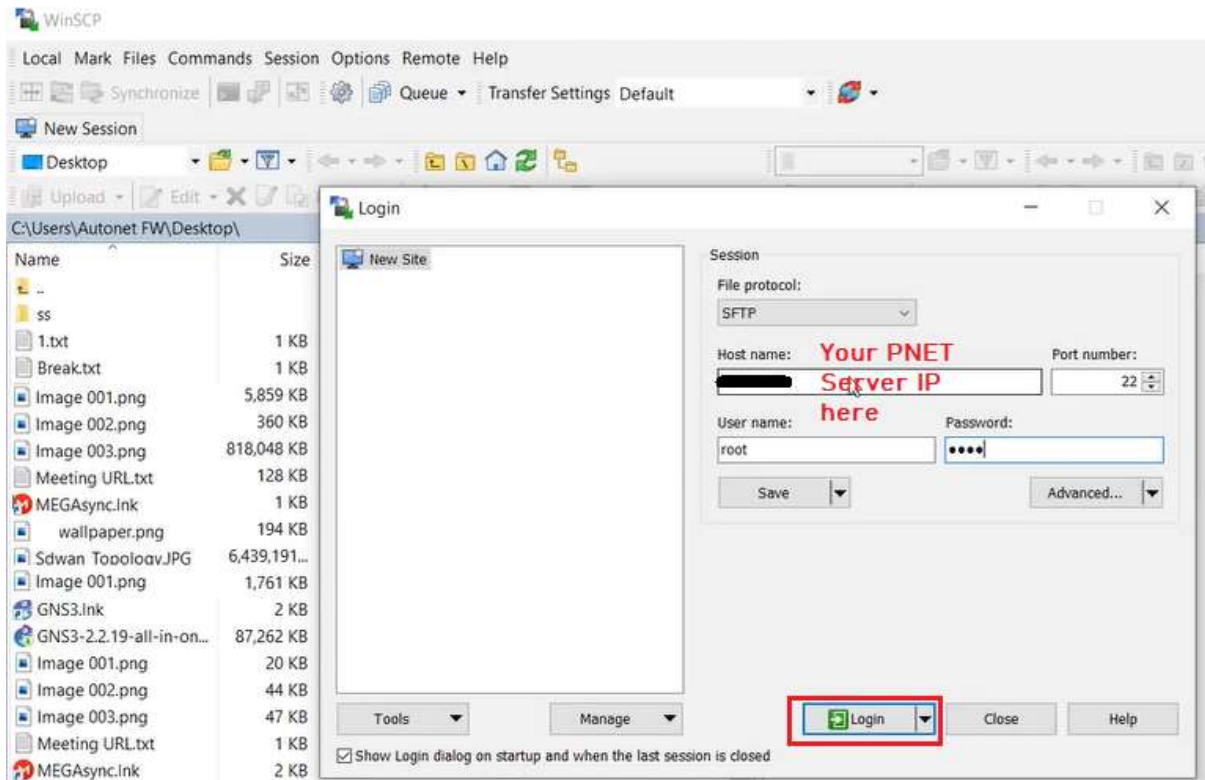
La descarga comienza como se muestra: archivo de aproximadamente 4 GB. Deje que la descarga se complete.



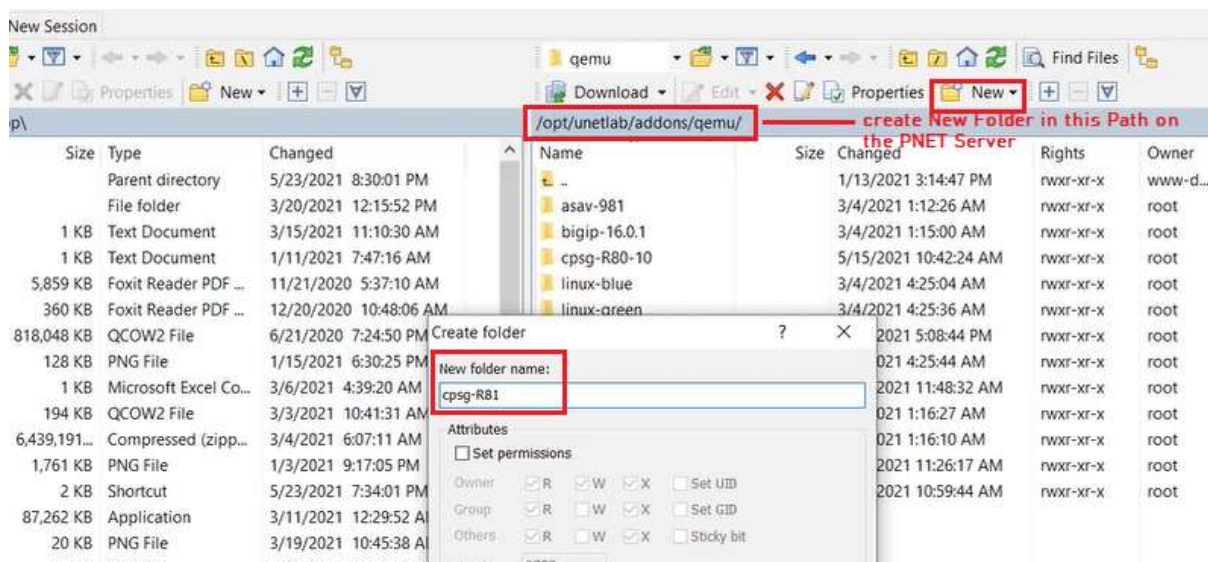
Instalar CheckPoint R81 en PNET

A través de un cliente WinSCP o cualquier otro cliente de transferencia de archivos, conéctese a su servidor PNET LAB. Ahora cargaremos el archivo ISO de CheckPoint en el servidor PNET

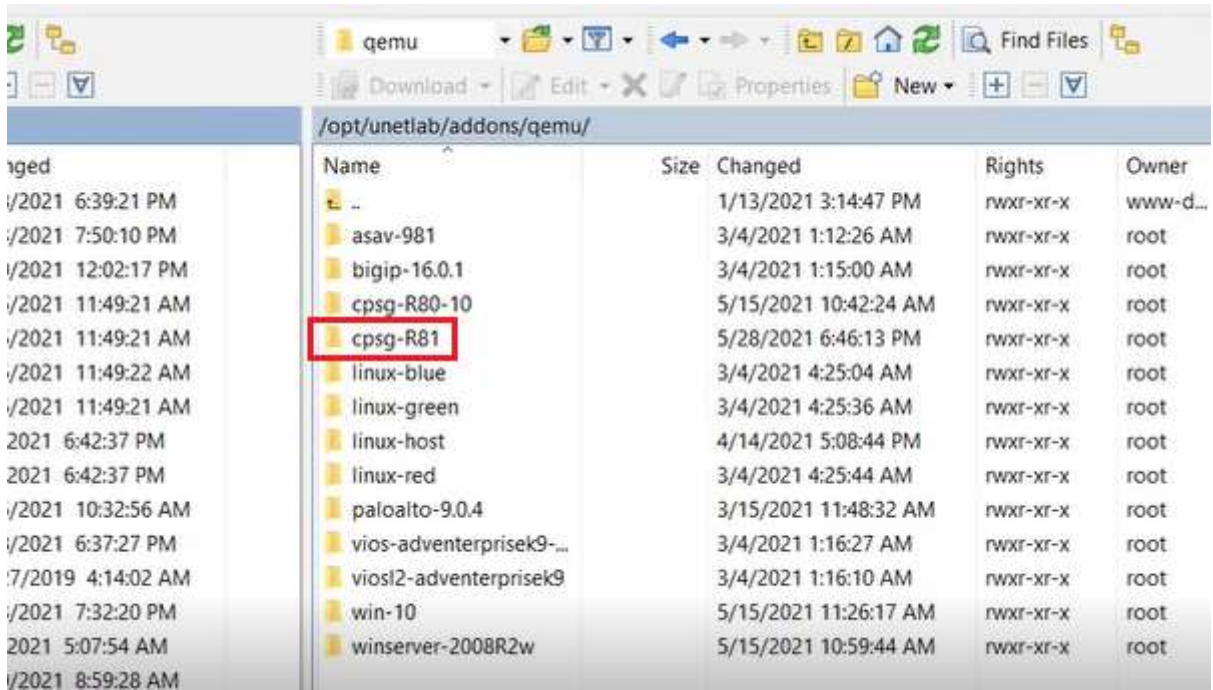
Proporcione los detalles de IP/Puerto y las credenciales de su servidor PNET LAB y haga clic en Iniciar sesión.



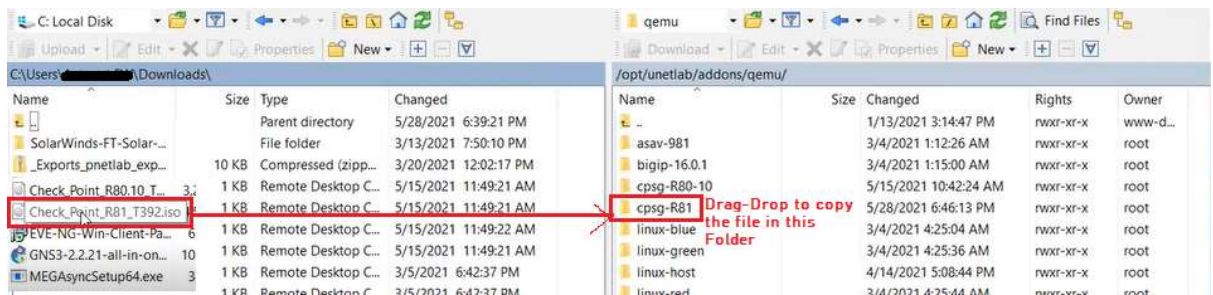
Una vez conectado al servidor PNET, Cree una Nueva Carpeta llamada "cpsg-R81" en la ruta /opt/ unetlab / addons / qemu /. Puede usar la opción Nuevo > Carpeta como se muestra.



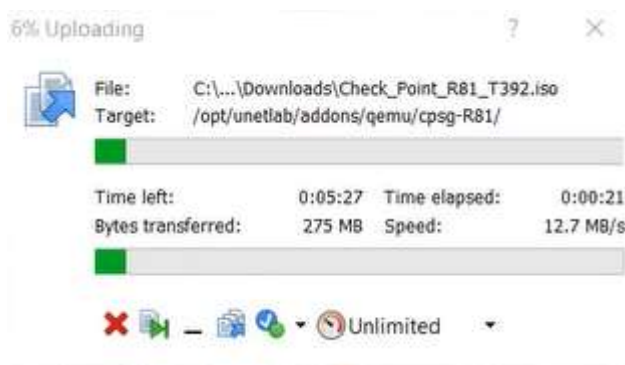
La carpeta se crea como se muestra



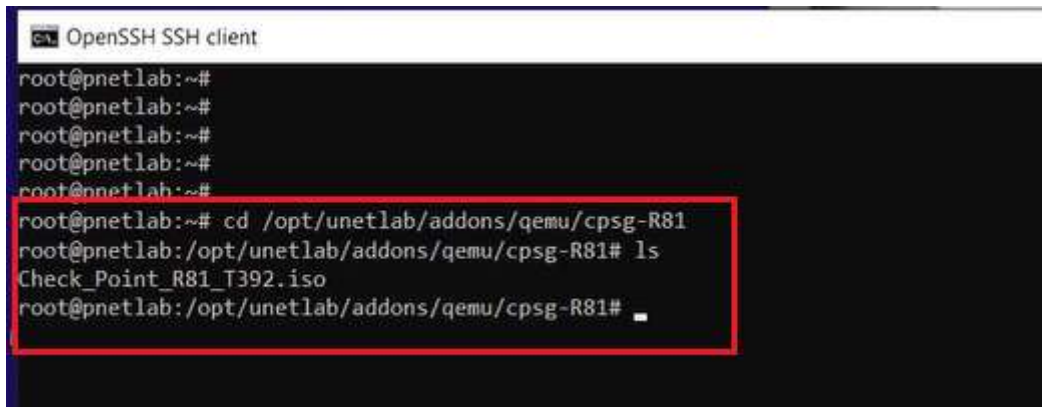
En el lado izquierdo de la ventana, busque la ruta del archivo ISO de CheckPoint y arrastre Suelte el archivo Check_Point_R81_T392.iso a la carpeta cpsg-R81 como se muestra.



La transferencia de archivos comenzará como se muestra



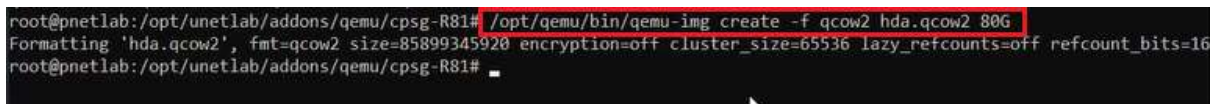
Una vez que se cargue el archivo, inicie sesión en el servidor PNET a través de Putty y busque la ruta /opt/ unetlab / addons / qemu / cpsg-R81 y escriba el comando ls para ver los archivos y verificar que la carga del archivo se haya realizado correctamente.



```
OpenSSH SSH client
root@pnetlab:~#
root@pnetlab:~#
root@pnetlab:~#
root@pnetlab:~#
root@pnetlab:~#
root@pnetlab:~# cd /opt/unetlab/addons/qemu/cpsg-R81
root@pnetlab:/opt/unetlab/addons/qemu/cpsg-R81# ls
Check_Point_R81_T392.iso
root@pnetlab:/opt/unetlab/addons/qemu/cpsg-R81#
```

Ahora crearemos una imagen QCOW2 a partir de la imagen iso con el siguiente comando 2

```
mv Check_Point_R81_T392.iso cdrom.iso
/opt/ qemu /bin/ qemu-img crear -f qcow2 hda.qcow 2 80G
```

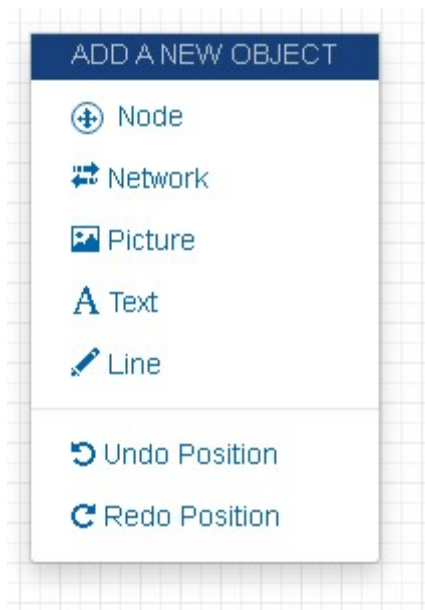


```
root@pnetlab:/opt/unetlab/addons/qemu/cpsg-R81# /opt/qemu/bin/qemu-img create -f qcow2 hda.qcow2 80G
Formatting 'hda.qcow2', fmt=qcow2 size=85899345920 encryption=off cluster_size=65536 lazy_refcounts=off refcount_bits=16
root@pnetlab:/opt/unetlab/addons/qemu/cpsg-R81#
```

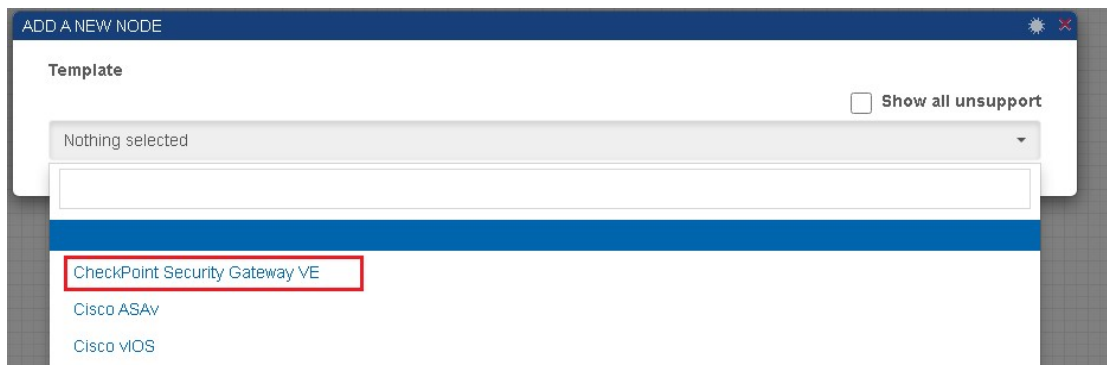
Ahora el nodo CheckPoint R81 está listo para agregarse al PNET Lab como se muestra a continuación. Puede crear un nuevo laboratorio en la consola PNET y agregar el nodo CheckPoint R81 como se muestra a continuación

Agregue el nodo CheckPoint a PNET LAB

Una vez que obtenga acceso a PNET Lab, haga clic con el botón derecho en Área de laboratorio y seleccione "Nodo"



Seleccione la opción "CheckPoint Security Gateway VE"



Cambie el nombre a "CP-independiente-R81"

ADD A NEW NODE

Template Show all unsupported

CheckPoint Security Gateway VE

Number of nodes to add: 1 Image: cpsg-R80-10

Name: CP-Standalone-R81

Description: CheckPoint Security Gateway VE

Icon: Checkpoint.png

Verifique las siguientes configuraciones en el nodo CheckPoint

CPU Limit

CPU: 4 RAM (MB): 6144

Primary Console: Telnet Primary Map Port:

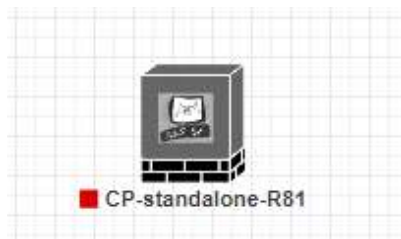
Secondary Console: Empty Secondary Map Port:

User Name: Password:

Ethernet: 4

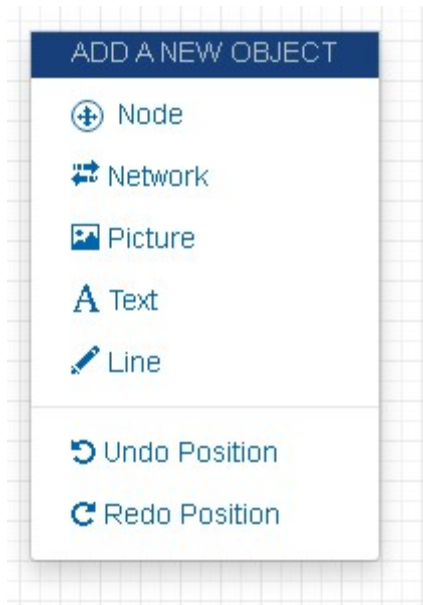
Qemu Arch: x86_64 Qemu NIC: e1000 Qemu Version: 2.4.0(Default)

Los nodos de CheckPoint se agregan al área de laboratorio.

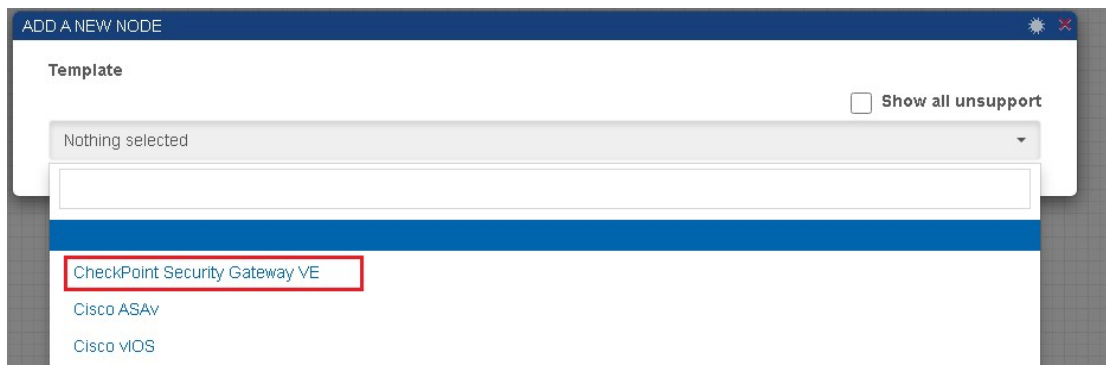


Tarea de laboratorio 2 ~ Implementación de un firewall de CheckPoint independiente (2 niveles)

Una vez que obtenga acceso a PNET Lab, haga clic con el botón derecho en Área de laboratorio y seleccione "Nodo"



Seleccione la opción "CheckPoint Security Gateway VE"



Cambie el nombre a "CP-independiente-R81"

ADD A NEW NODE

Template Show all unsupported

CheckPoint Security Gateway VE

Number of nodes to add: 1 Image: cpsg-R80-10

Name: CP-Standalone-R81

Description: CheckPoint Security Gateway VE

Icon: Checkpoint.png

Verifique las siguientes configuraciones en el nodo CheckPoint

CPU Limit

CPU: 4 RAM (MB): 6144

Primary Console: Telnet Primary Map Port:

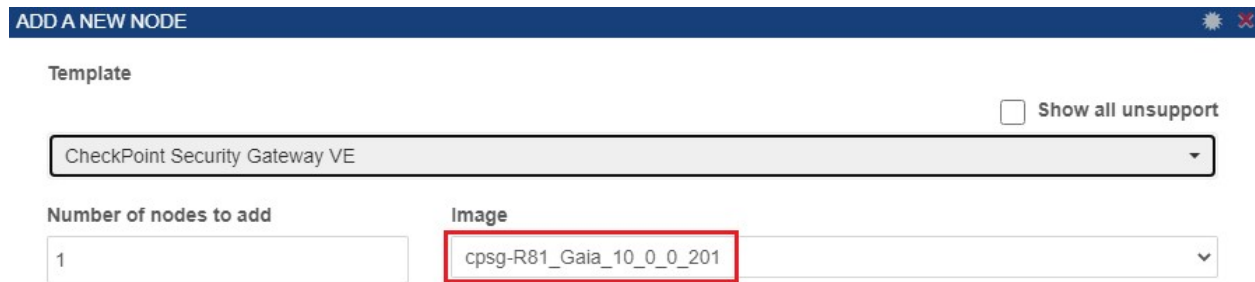
Secondary Console: Empty Secondary Map Port:

User Name: Password:

Ethernet: 4

Qemu Arch: x86_64 Qemu NIC: e1000 Qemu Version: 2.4.0(Default)

Nota : para los laboratorios usaremos la imagen de nodo comprometido de Checkpoint donde Gaia OS ya está instalado con una IP estática -10.0.0.201 configurada en la interfaz eth1 de CheckPoint como se muestra a continuación



ADD A NEW NODE

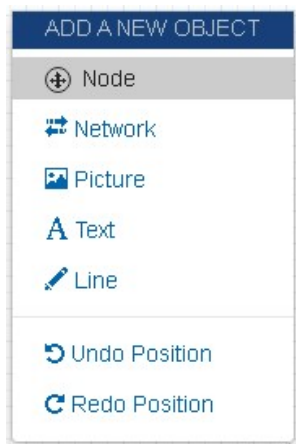
Template Show all unsupported

CheckPoint Security Gateway VE

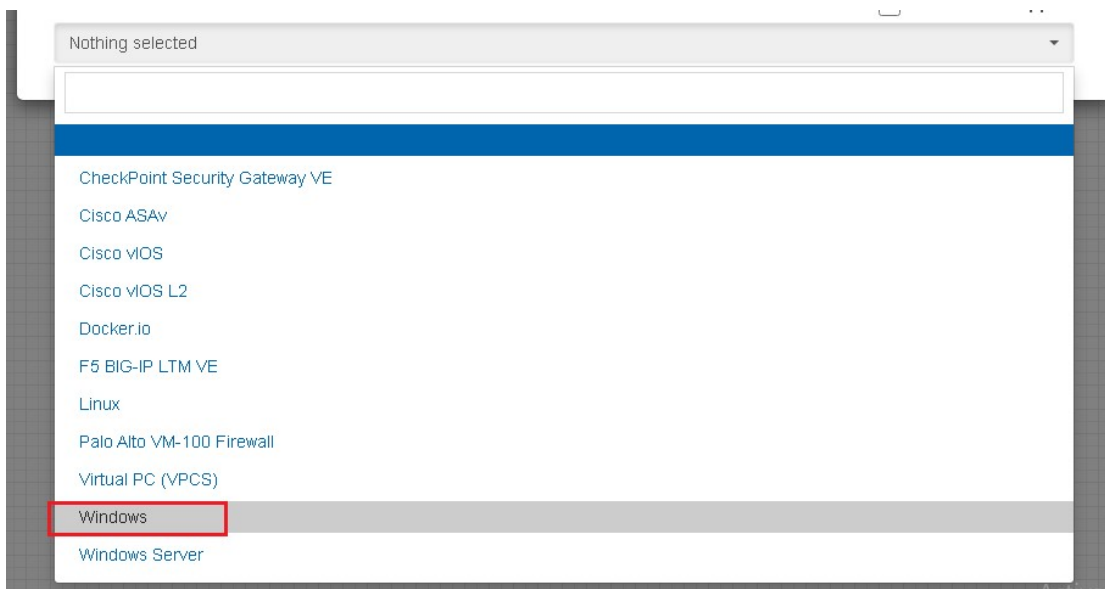
Number of nodes to add: 1

Image: cpsg-R81_Gaia_10_0_0_201

Haga clic con el botón derecho en Área de laboratorio y seleccione "Nodo"



Seleccione la opción de Windows de la lista desplegable. Este nodo de Windows-10 se usará como nuestra consola inteligente o máquina cliente GUI



Cambie el nombre del Nodo a "GUI-Client"

Show all unsupported

Windows

Number of nodes to add: 1

Image: win-10

Name: GUI-Client

Description: Windows

Icon: Desktop.png

Verifique las siguientes configuraciones en el nodo del cliente GUI

CPU Limit

CPU: 4

RAM (MB): 4096

Primary Console: VNC

Primary Map Port: |

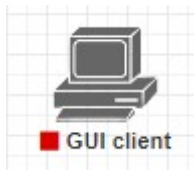
Secondary Console: Empty

Secondary Map Port:

User Name:

Password:

Ethernet: 1



Haga clic en Agregar nodo



Seleccione Cisco VIOS como se muestra a continuación para agregar un enrutador de Internet para conectividad a Internet



Haga clic en Agregar red como se muestra a continuación y agregue " Cloud_nat ". Esto es para la conectividad de nuestro segmento de Internet.

ADD A NEW OBJECT

⊕ Node

🌐 Network

🖼️ Picture

A Text

✍️ Line

↶ Undo Position

↷ Redo Position

ADD A NEW NETWORK

Number of networks to add

1

Name/Prefix

Net

Type

bridge

Left

Top

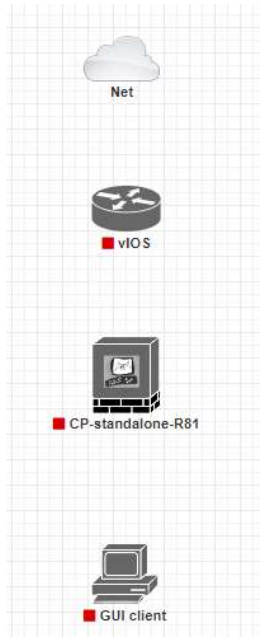
Size (px)

Icon

- bridge ✓
- Management(Cloud0)
- Cloud1
- Cloud2
- Cloud3
- Cloud4
- Cloud5
- Cloud6
- Cloud7
- Cloud8
- Cloud9
- Cloud_nat



Una vez que todos los elementos (nodos y red) se agreguen al laboratorio, la configuración del laboratorio se verá similar a la que se muestra a continuación.



Ahora procederemos con la parte de conectividad de la siguiente manera

Conecte la interfaz Gi0/0 de vIOS a Cloud_nat como se muestra



Add connection between vIOS and Net

Source ID: 3
Source Name: vIOS
type - Node

Choose Interface for vIOS

Gi0/0

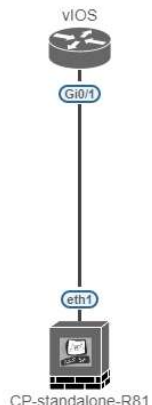
Destination ID: 1
Destination Name: Net
type - Network

Save **Cancel**

Conecte el Gi0/1 de vIOS a Checkpoint eth1 como se muestra



Add connection between vIOS and CP-standalone-R81



Source ID: 3
Source Name: vIOS
type - Node

Choose Interface for vIOS
Gi0/1

Choose Interface for CP-standalone-R81
eth1


Destination ID: 2
Destination Name: CP-standalone-R81
type - Node

Save Cancel

Conecte el CheckPoint eth-0 al nodo de Windows (cliente GUI) e0 como se muestra



Add connection between CP-standalone-R81 and GUI client



Source ID: 2
Source Name: CP-standalone-R81
type - Node

Choose Interface for CP-standalone-R81
eth0

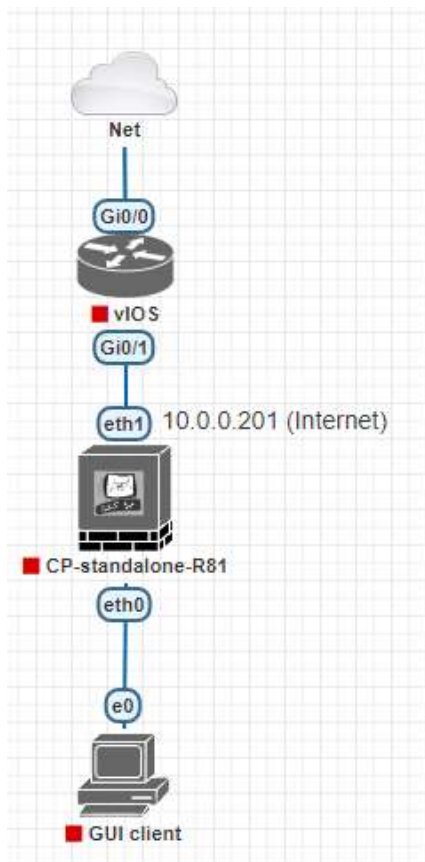
Choose Interface for GUI client
e0

Destination ID: 1
Destination Name: GUI client
type - Node

Save Cancel

Configuración del enrutador de Internet

Una vez que se agreguen todos los nodos y las redes, lo siguiente será la configuración del laboratorio con 10.0.0.201 configurado en eth1 de la interfaz de CheckPoint de forma predeterminada según la imagen confirmada.



Ahora procederemos con la configuración del enrutador de Internet para la conectividad a Internet. Configuraremos la dirección IP de 10.0.0.1 en la interfaz Gi0/1 del enrutador y en Gi0/0 configuraremos DHCP para que reciba la IP del ISP de Internet.

También configuraremos Ocultar NAT (sobrecarga) y configuraremos todas las direcciones IP internas de 10.0.0.0/24 para que estén habilitadas para Ocultar NAT y puedan acceder a Internet a través del enrutador.

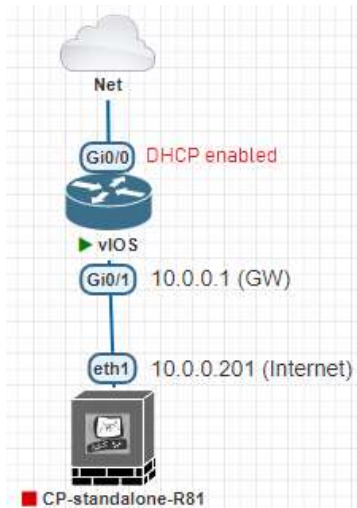
A continuación se muestra la configuración a realizar en el Router

```
( configuración )#interfaz GigabitEthernet0/0 >>>> interface GigabitEthernet0/0
( config - if ) # dirección IP dhcp >>>> ip address dhcp
( config -if)# no shut
( configuración - si) # ip natural afuera >>>> ip nat outside
```

```
( configuración )#interfaz GigabitEthernet0/1 >>>>> interface GigabitEthernet0/1
( configuración - si) # dirección IP 10.0.0.1 255.255.255.0 >>>>>> ip address 10.0.0.1 255.255.255.0
( configuración - si) # no shut
( configuración - si) # ip natural dentro >>>>> ip nat inside
```

```
( config )#access-list 1 permiso 10.0.0.0 0.0.0.255 >>>> access-list 1 permit 10.0.0.0 0.0.0.255
( configuración ) # ip nat dentro de la lista de fuentes 1 interfaz GigabitEthernet0/0 sobrecarga
>>>> ip nat inside source list 1 interface GigabitEthernet0/0 overload
```

El segmento de Internet del LAB se verá algo similar a esto



Esto completa la configuración de vIOS del enrutador para el direccionamiento IP y NAT.

Instalación del sistema operativo Gaia

A continuación veremos la instalación de Gaia.

Nota: - Esta etapa no es válida para el nodo comprometido. Esto es válido solo para la imagen qcow2 recién agregada de CheckPoint.

Inicie el nodo "CP-standalone-R81" y conéctese a la consola para comenzar la instalación del sistema operativo Gaia.



Haga clic en "Abrir" para iniciar la Consola

This site is trying to open SSH, Telnet and Rlogin client.

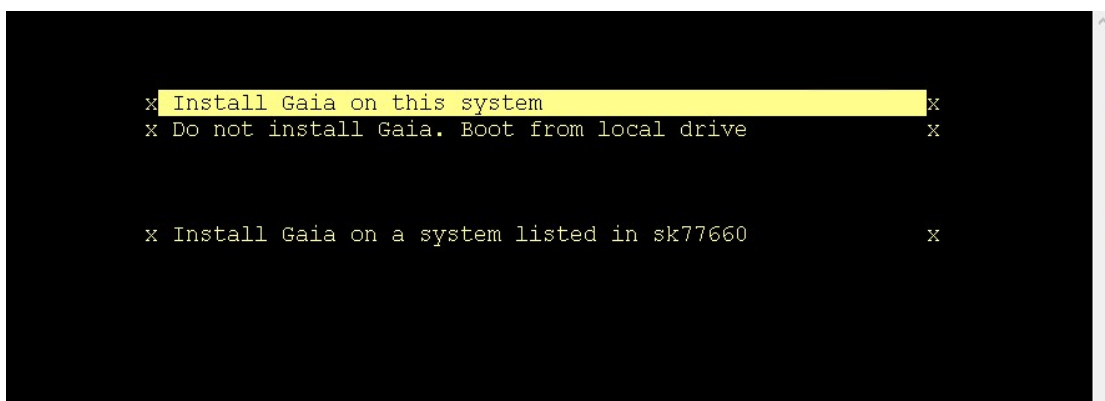
https://10.0.0.201 wants to open this application.

Always allow 10.0.0.201 to open links of this type in the associated app

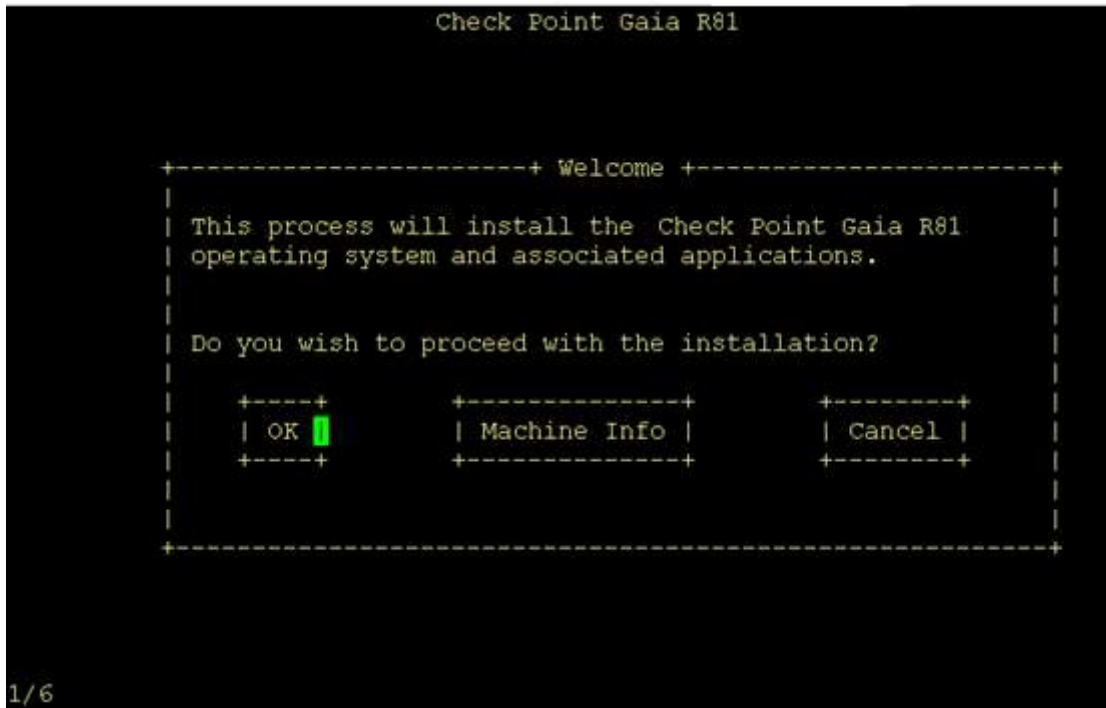


Selecciona la opción "Instalar Gaia en este sistema" y presiona "Enter"

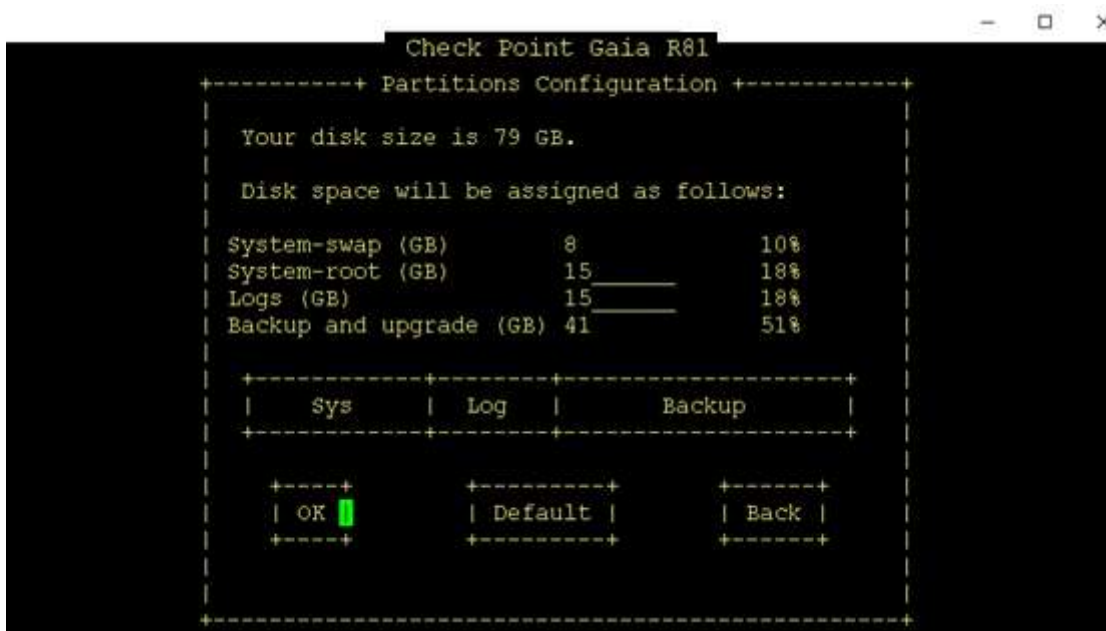
Nota: - En caso de que obtenga una pantalla en blanco, intente hacer clic en las teclas de flecha arriba / abajo para que las opciones sean visibles.



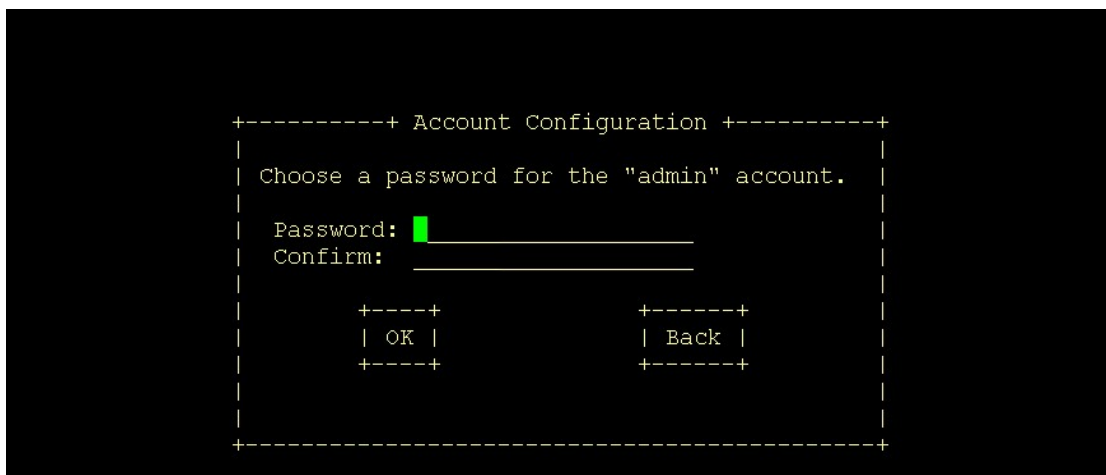
Haga clic en "Aceptar" para continuar con la instalación



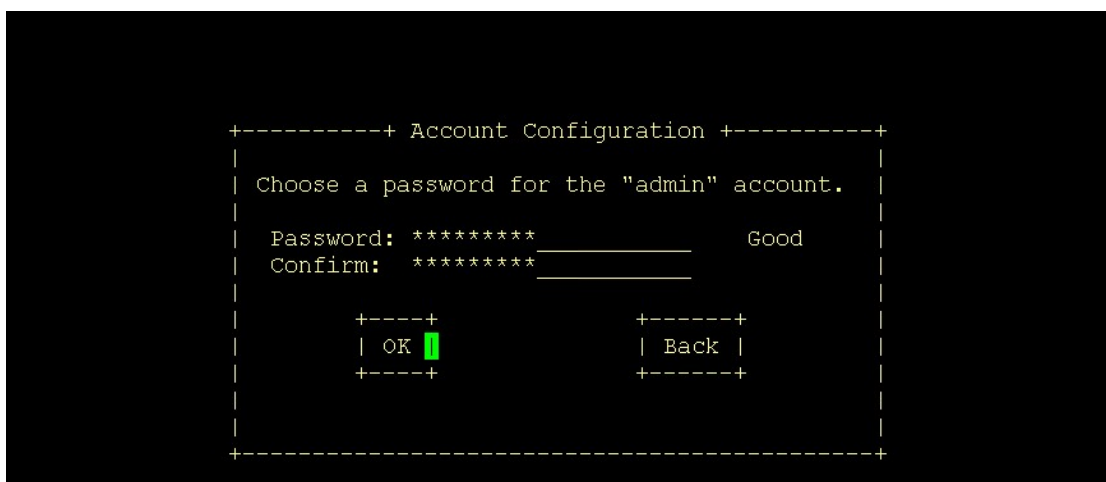
Deje los valores sin cambios y haga clic en "Aceptar" para continuar. Use TAB para navegar a la opción "OK" si es necesario y presione "Enter"



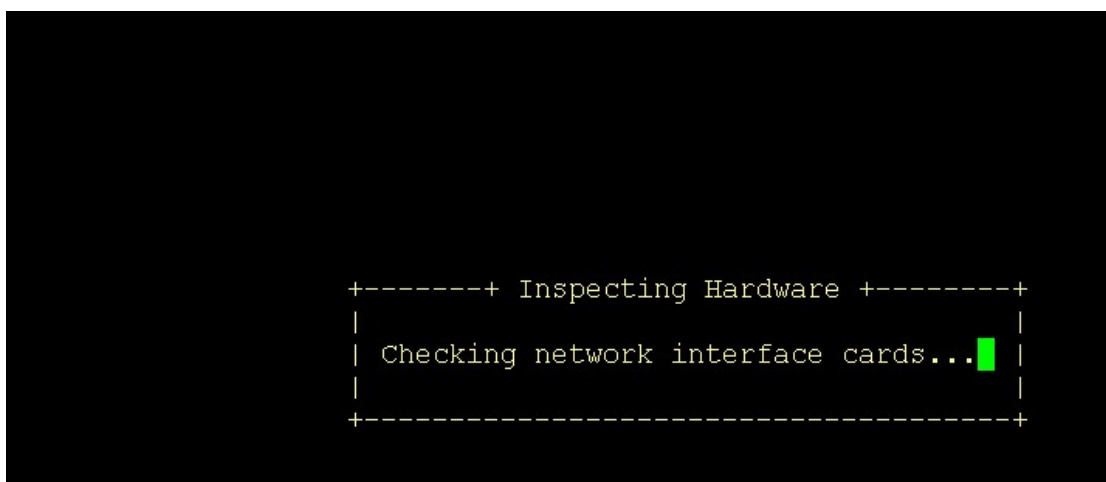
Establezca la contraseña como "admin@123" y confirme la misma.



Seleccione "OK" y luego presione "Enter"



El proceso de instalación verificará las interfaces de red instaladas en el nodo CheckPoint



Tenga en cuenta que tenemos que crear una interfaz y preparar TCP/IP antes de la instalación de Gaia. La siguiente sección puede variar según la cantidad de interfaces que haya conectado. Solo queremos que la dirección IP esté configurada en 1 de las interfaces Ethernet y debe estar conectada en estado como (UP). En nuestro caso de imagen confirmada, la dirección IP es 10.0.0.201

Puede mostrarle que eth-0 y eth-1 están activos (o tantas interfaces que pueden estar activas)

```
Check Point Gaia R81

+-----+ Management Port +-----+
| You have multiple network ports on this
| system. Choose the port you would like
| to use for managing the system.
|
| eth0 [link up]
| eth1 [link up]
| eth2 [no link]
| eth3 [no link]
|
| [ ] Blink selected port
|
| +-----+ | +-----+ | +-----+
| | OK | | | Recheck Link | | | Back |
| +-----+ | +-----+ | +-----+
+-----+


```

Seleccione eth1 y presione Entrar

```
Check Point Gaia R81

+-----+ Management Port +-----+
| You have multiple network ports on this
| system. Choose the port you would like
| to use for managing the system.
|
| eth0 [link up]
| eth1 [link up]
| eth2 [no link]
| eth3 [no link]
|
| [ ] Blink selected port
|
| +-----+ | +-----+ | +-----+
| | OK | | | Recheck Link | | | Back |
| +-----+ | +-----+ | +-----+
+-----+


```

Configure la dirección IP de 10.0.0.201 en eth1 con Netmask de 255.255.255.0 y Default Gateway de 10.0.0.1 y navegue hasta Aceptar y presione "Enter".

Esto es necesario porque la instalación de CheckPoint -Gaia requiere un mínimo de 1 interfaz preparada para TCP/IP (configurada con IP y el enlace debe estar conectado y activo)

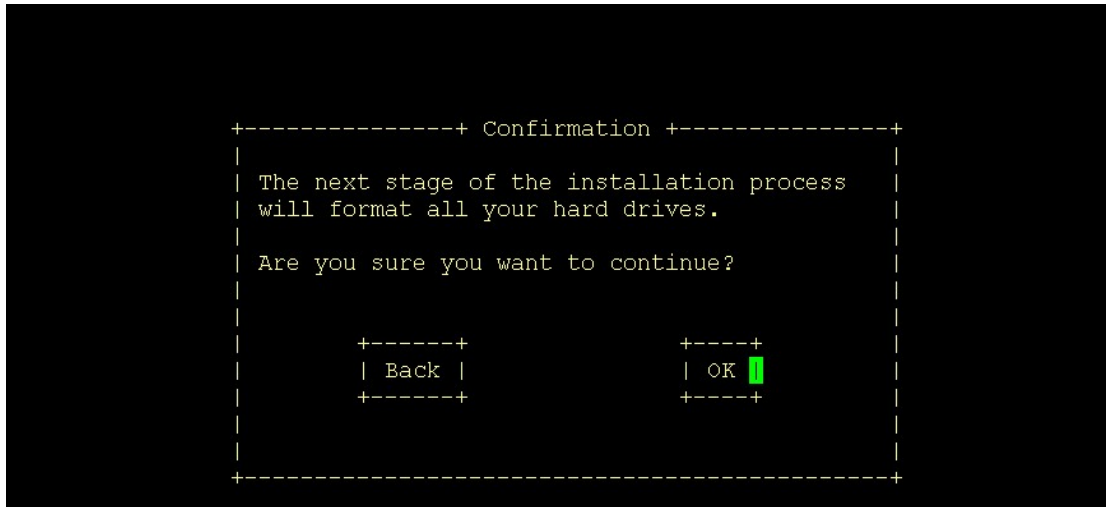
```
Check Point Gaia R81

+----+ Management Interface (eth1) +----+
| IP address: 10.0.0.201
| Netmask: 255.255.255.0
| Default gateway: 10.0.0.1
|
| [ ] DHCP server on this interface
|
| +----+ | +----+
| | OK | | | Back |
| +----+ | +----+
+----+


```

La siguiente pantalla le pedirá su confirmación para la instalación.

Seleccione "OK" y presione enter y deje que la instalación continúe



Implementación independiente de CheckPoint (2 niveles)

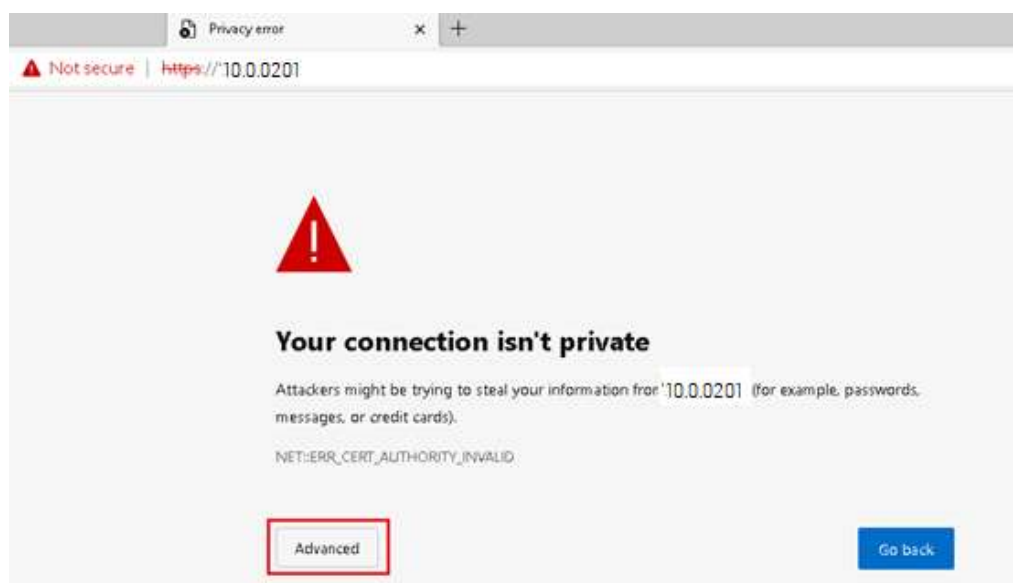
Nota: En caso de que no pueda comunicarse con la Máquina Gaia, es posible que deba configurar otra interfaz o activar la interfaz configurada.

Los comandos para el mismo son los que se mencionan a continuación.

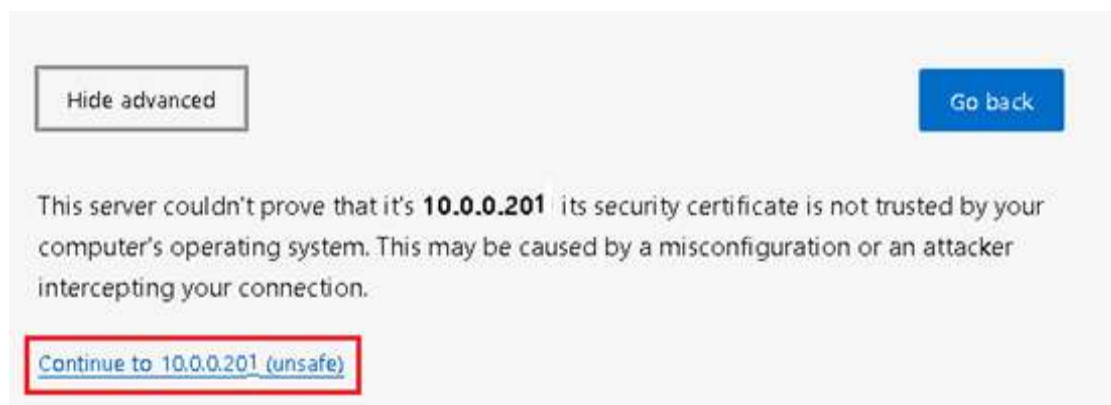
*configure la interfaz eth0 ipv4-address 172.16.30.1 mask-length 24 < esta es la IP eth0 según nuestro LAB)
establecer interfaz eth0 estado en
guardar configuración*

Tenga en cuenta que la siguiente instalación se realiza desde una máquina conectada al segmento 10.0.0.X. Puede iniciar la configuración por primera vez desde eth0 también después de configurar los comandos como se muestra arriba y conectar los nodos correctamente desde la máquina GUI-Client

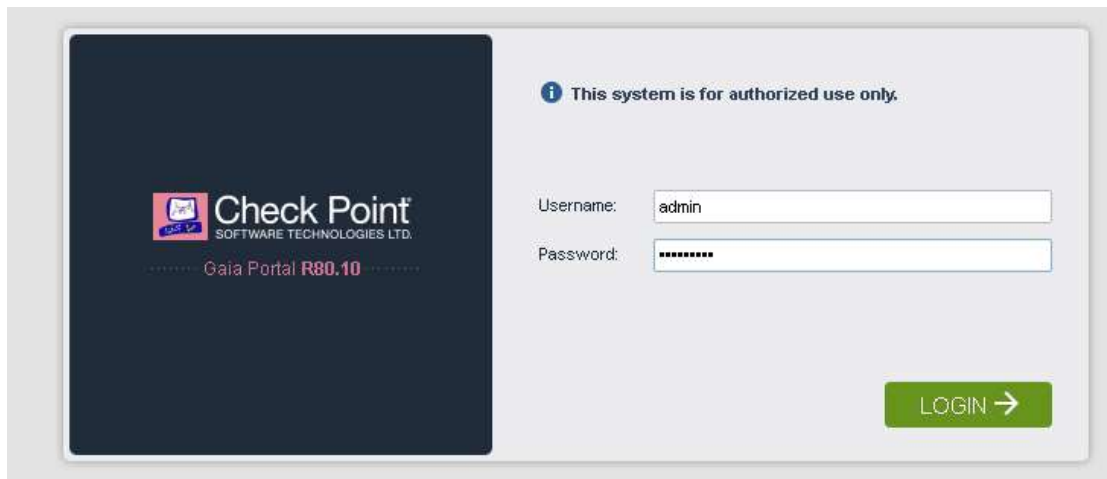
Abra un navegador web (Internet Edge" y navegue hasta la URL " <https://10.0.0.201> ")



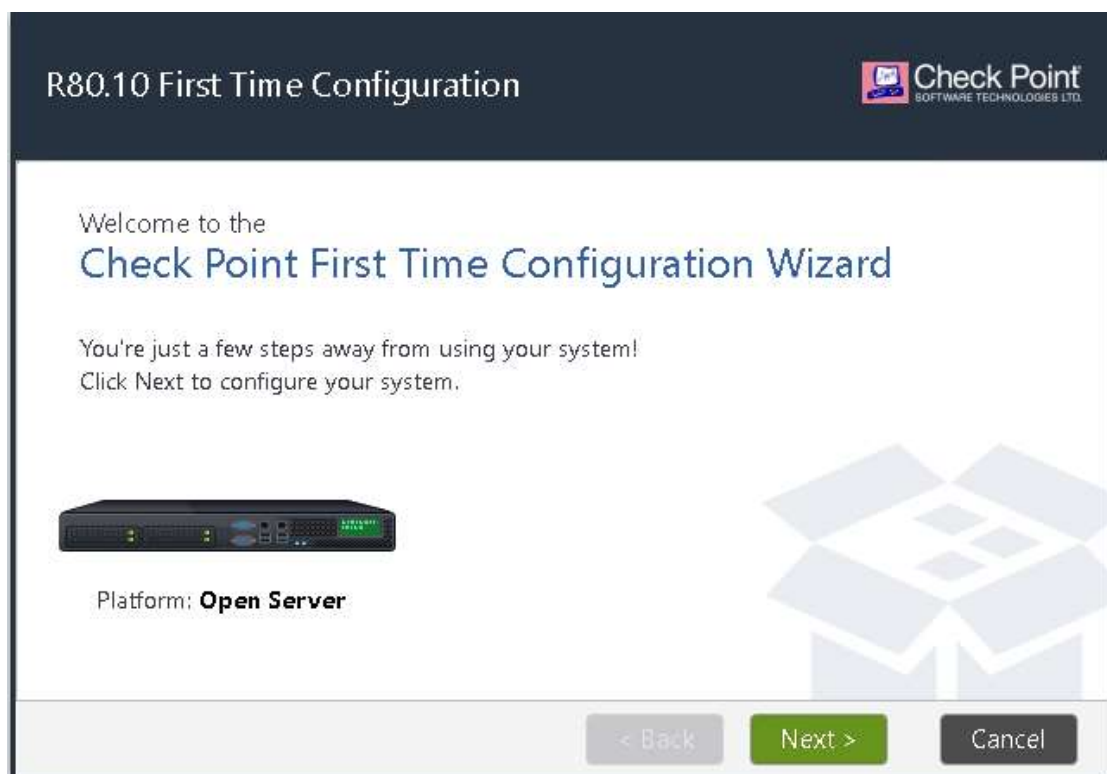
Haga clic en la opción "Avanzado" y haga clic en "continuar a 10.0.0.201"



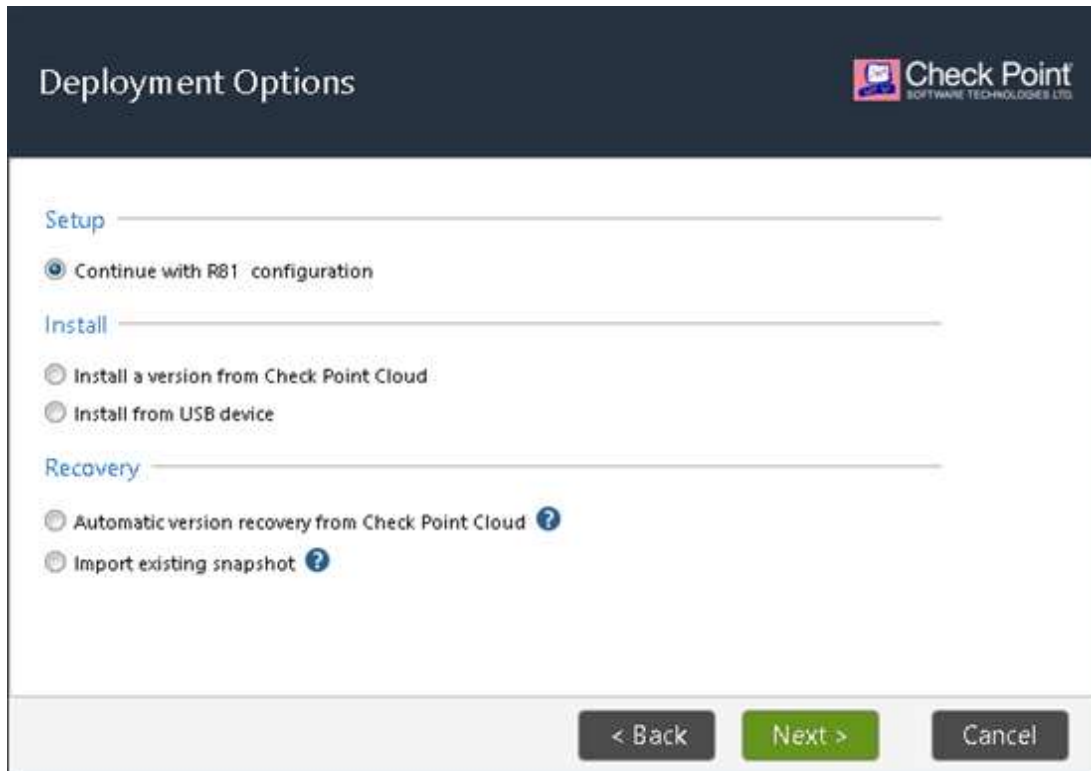
En la página siguiente, inicie sesión con las credenciales de admin / admin@123 que usamos durante la instalación y presione Iniciar sesión




El asistente de configuración por primera vez se inicia como se muestra: haga clic en Siguiente



Deje seleccionada la Opción "Continuar con la configuración de R81" y haga clic en Siguiente



The image shows a 'Deployment Options' dialog box from Check Point Software Technologies Ltd. The dialog is divided into three sections: 'Setup', 'Install', and 'Recovery'. In the 'Setup' section, the option 'Continue with R81 configuration' is selected with a radio button. The 'Install' section has two options: 'Install a version from Check Point Cloud' and 'Install from USB device', both unselected. The 'Recovery' section has two options: 'Automatic version recovery from Check Point Cloud' and 'Import existing snapshot', both unselected. At the bottom right, there are three buttons: '< Back' (disabled), 'Next >' (highlighted in green), and 'Cancel' (disabled).

Deployment Options 



Setup

- Continue with R81 configuration

Install

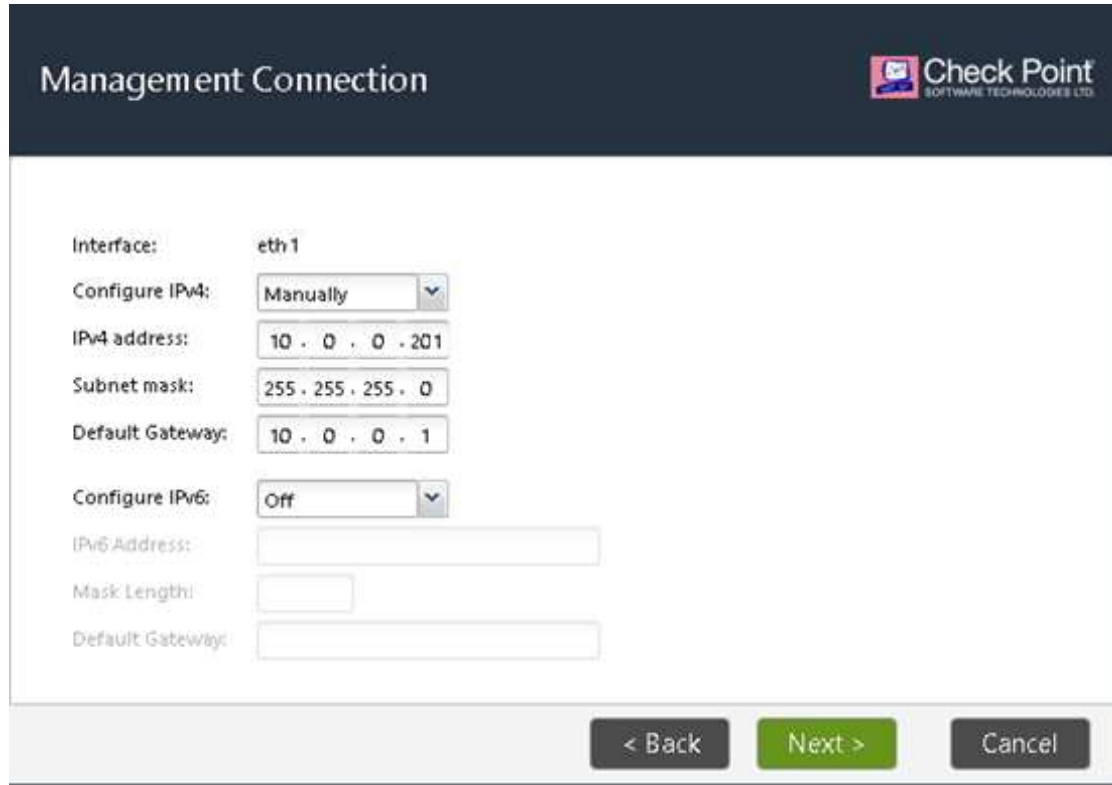
- Install a version from Check Point Cloud
- Install from USB device

Recovery

- Automatic version recovery from Check Point Cloud 
- Import existing snapshot 

< Back Next > Cancel

La siguiente pantalla muestra la dirección IP en eth1, la misma que configuramos durante la instalación del sistema operativo Gaia. Haga clic en Siguiente



The image shows a configuration window titled "Management Connection" with the Check Point logo in the top right corner. The interface is for configuring the "eth1" interface. It includes several input fields and dropdown menus for IPv4 and IPv6 settings. At the bottom, there are three buttons: "< Back", "Next >" (highlighted in green), and "Cancel".

Interface:	eth1
Configure IPv4:	Manually
IPv4 address:	10 . 0 . 0 . 201
Subnet mask:	255 . 255 . 255 . 0
Default Gateway:	10 . 0 . 0 . 1
Configure IPv6:	Off
IPv6 Address:	
Mask Length:	
Default Gateway:	

< Back Next > Cancel

En la siguiente pantalla, configuraremos la dirección IP en la interfaz eth0 del CheckPoint FW -CP-standalone-R81

Nota: Omita este paso si configuró IP a través de CLI a eth0

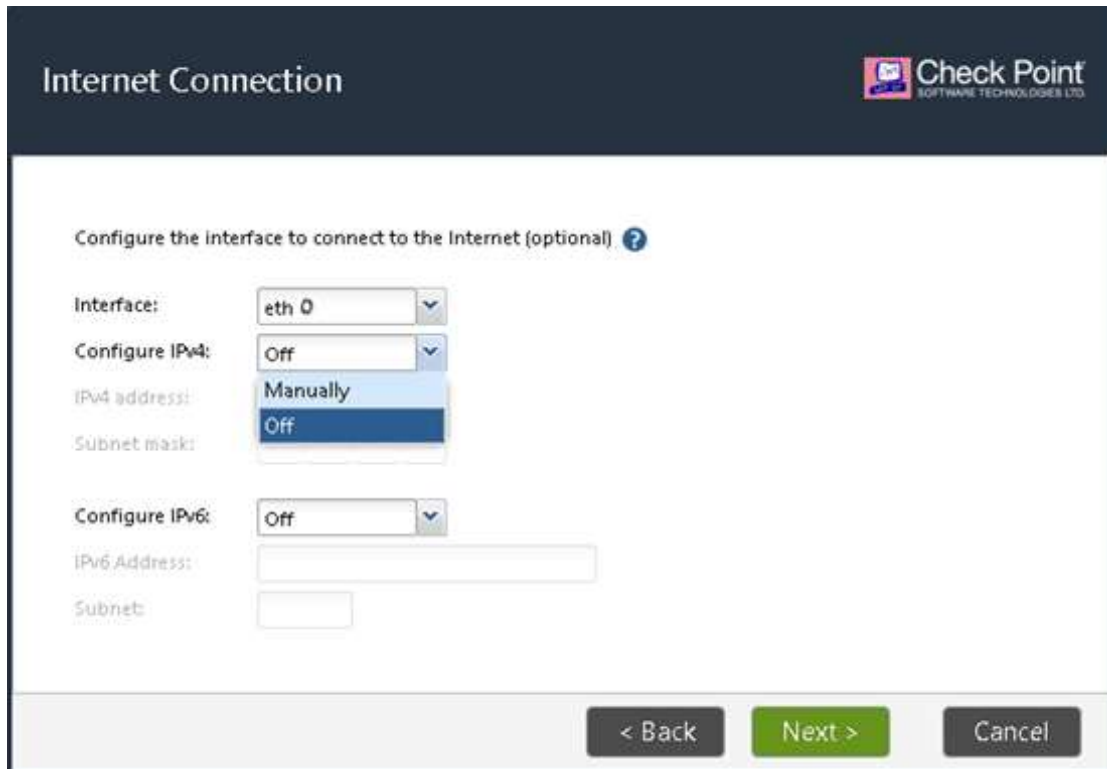
Seleccione la opción Manual como se muestra


The screenshot displays the 'Internet Connection' configuration window. At the top left, the title 'Internet Connection' is visible. At the top right, the Check Point logo and 'SOFTWARE TECHNOLOGIES LTD.' are present. The main content area contains the following configuration options:

- Interface: eth1 (dropdown menu)
- Configure IPv4: Off (dropdown menu)
- IPv4 address: Manually (dropdown menu, currently selected)
- Subnet mask: Off (dropdown menu)
- Configure IPv6: Off (dropdown menu)
- IPv6 Address: (empty text input field)
- Subnet: (empty text input field)

At the bottom of the window, there are three buttons: '< Back' (grey), 'Next >' (green), and 'Cancel' (grey).

Configure la dirección IP de 172.16.30.1 y la máscara de subred de 255.255.255.0 y haga clic en Siguiente



Internet Connection 

Configure the interface to connect to the Internet (optional) ?

Interface: eth 0

Configure IPv4: Off

IPv4 address: Manually

Subnet mask: Off

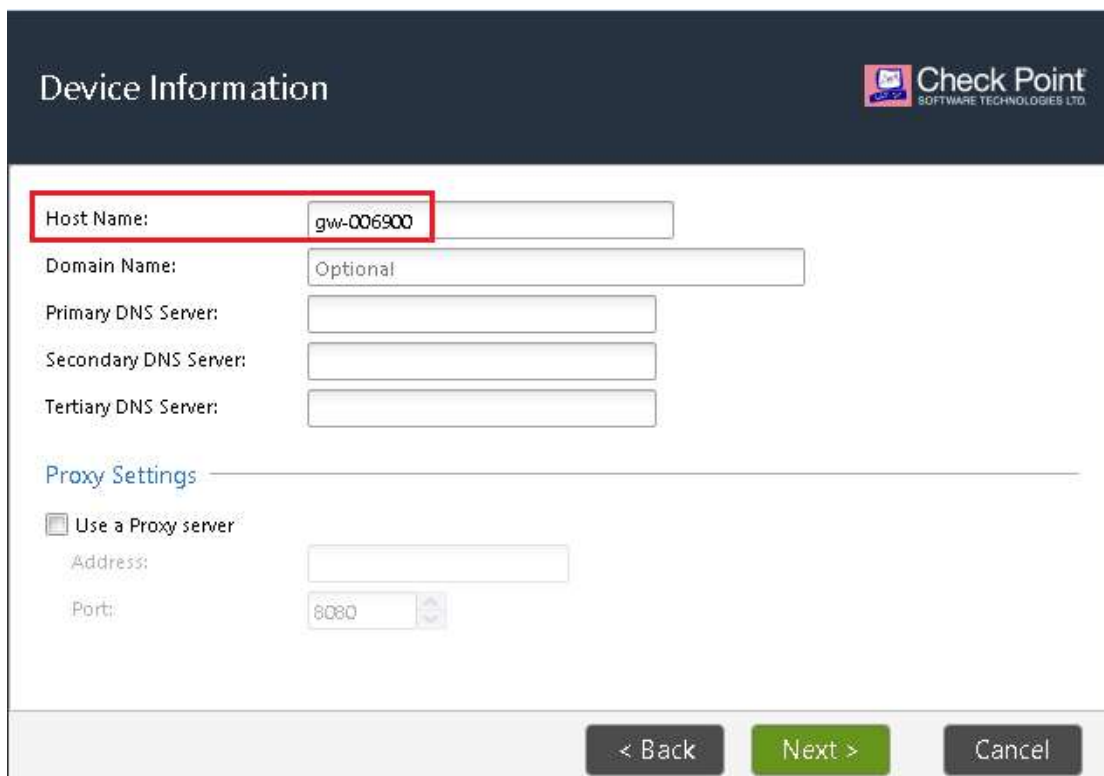
Configure IPv6: Off


IPv6 Address:

Subnet:

< Back Next > Cancel

Cambie el nombre de host a "CP-standalone-R81" en la siguiente pantalla



Device Information 

Host Name: gw-006900

Domain Name: Optional

Primary DNS Server:

Secondary DNS Server:

Tertiary DNS Server:

Proxy Settings


Use a Proxy server

Address:

Port: 8080

< Back Next > Cancel

Device Information



Host Name:

Domain Name:

Primary DNS Server:

Secondary DNS Server:

Tertiary DNS Server:

Proxy Settings

Use a Proxy server

Address:


Port:

< Back Next > Cancel

Haga clic en Siguiente

Establezca la fecha/hora y la zona horaria según sea necesario y haga clic en Siguiente

Date and Time Settings



Set time manually:

Date:

Time: :

Time Zone:

Use Network Time Protocol (NTP):

Primary NTP server: Version:

Secondary NTP server: Version:

Time Zone:

< Back Next > Cancel

Seleccione la Opción de "Puerta de enlace de seguridad y/o Gestión de seguridad y haga clic en Siguiente

Installation Type



- Security Gateway and/or Security Management
- Multi-Domain Server

< Back

Next >

Cancel

En la pantalla Siguiete, seleccione los productos "Security Gateway" y "Security Management" que desea instalar. Verifique otras configuraciones y haga clic en Siguiete para continuar con la instalación.

Dado que hemos seleccionado Gateway y Management para instalarlos en el mismo sistema, lo hace como una implementación independiente.

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

Seleccione Sí en la página de advertencia para continuar

Alert

It is highly recommended to keep this setting enabled to ensure smooth operation of Check Point products.
Keep this setting enabled, even if you do not currently have Internet connectivity since it determines your initial Security Management Server configuration.

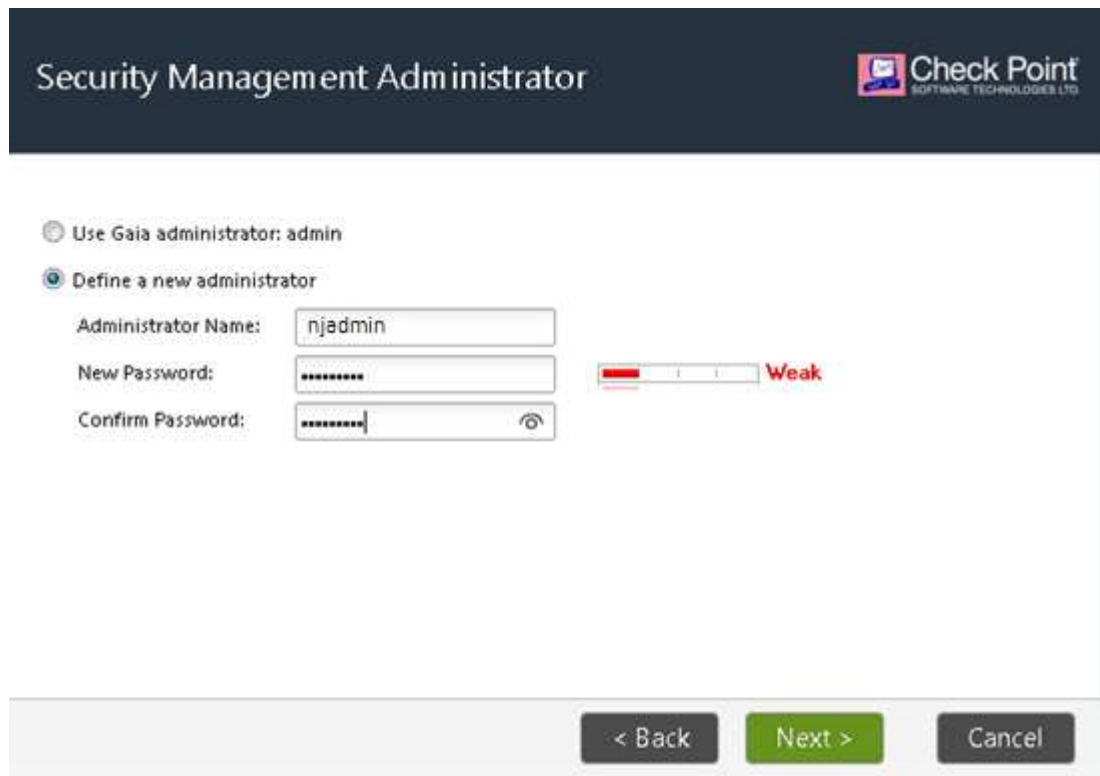
Are you sure you want to continue?

Yes No

En la siguiente pantalla configuraremos un Administrador de Gestión de Seguridad (Usuario y Contraseña) que se utilizará en la Smart Console para conectarse al "Servidor de Gestión" para la Gestión.

Configure el nombre del administrador como " nadmin " y la contraseña como " nadmin "

Haga clic en Siguiente para continuar




Security Management Administrator


Check Point
SOFTWARE TECHNOLOGIES LTD

Use Gaia administrator: admin

Define a new administrator

Administrator Name:

New Password:  Weak

Confirm Password: 

< Back Next > Cancel

En la siguiente pantalla configuraremos los clientes GUI. Los clientes GUI son direcciones IP que tienen SmartConsole instalado para la gestión de seguridad.

La dirección IP del cliente debe estar permitida en el servidor de administración para que pueda acceder y administrar la configuración.

A partir de ahora seleccionaremos la opción "Cualquier dirección IP"

Haga clic en Siguiente para continuar

Security Management GUI Clients

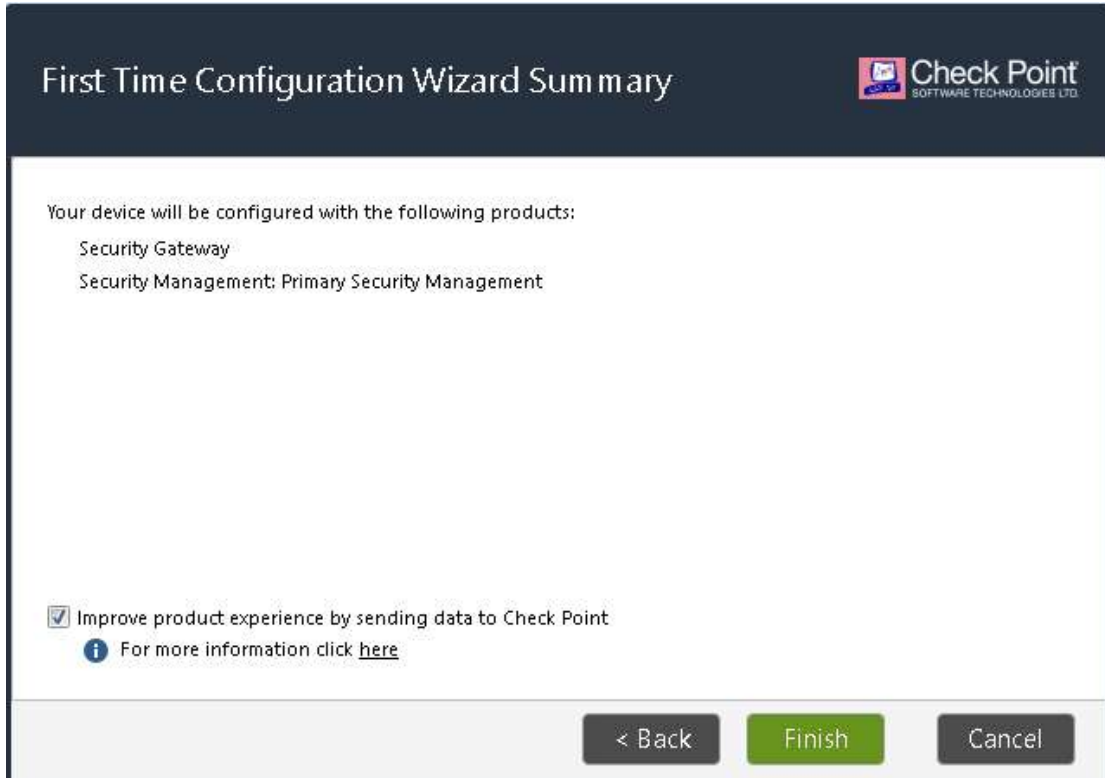
Check Point
SOFTWARE TECHNOLOGIES LTD.

GUI clients can log into the Security Management from:

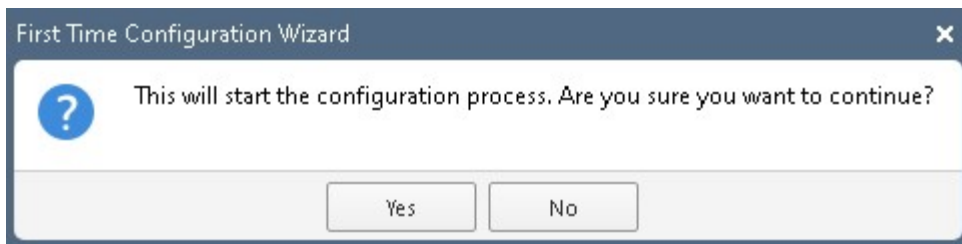
- Any IP Address
- This machine
IP address: 10.0.0.76
- Network
IP Address:
Subnet:
- Range of IPv4 addresses:
 -

< Back Next > Cancel

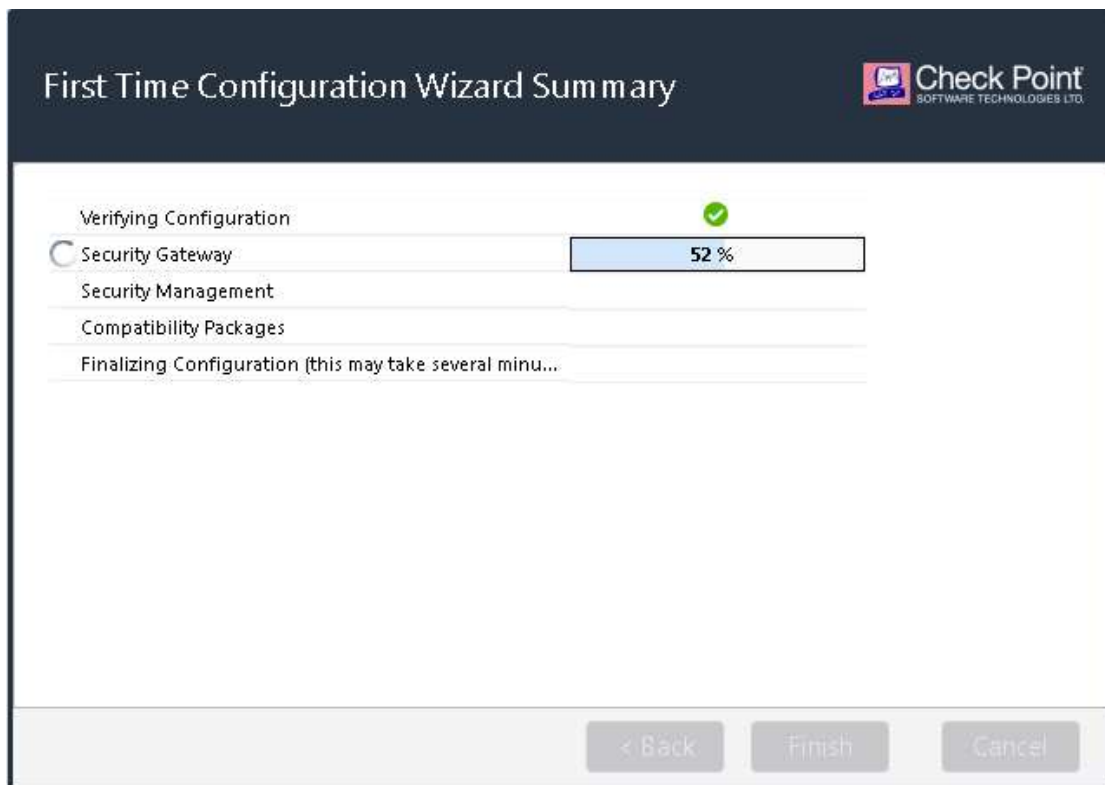
La siguiente pantalla muestra el resumen de los Productos que ha seleccionado para la instalación. Haga clic en Siguiente para continuar.



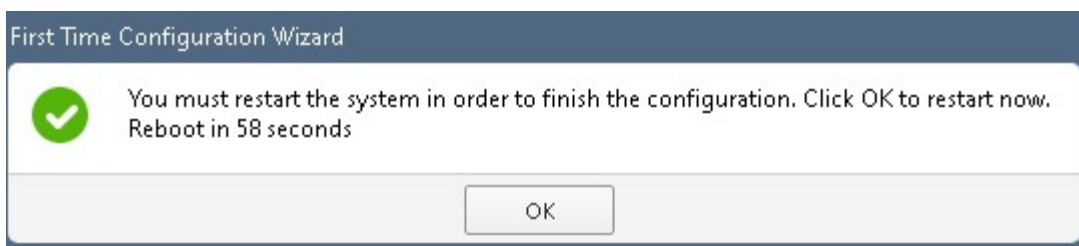
Se le pedirá confirmación como se muestra: haga clic en Sí para comenzar la instalación



El proceso de instalación se inicia y el progreso de cada componente se muestra como se muestra



Finalmente, recibe un mensaje para reiniciar el sistema como se muestra. Haga clic en "Aceptar" para reiniciar.



Una vez que se reinicie el sistema, se le dirigirá nuevamente a la página de inicio de sesión.



i This system is for authorized use only.

Username:

Password:

LOGIN →

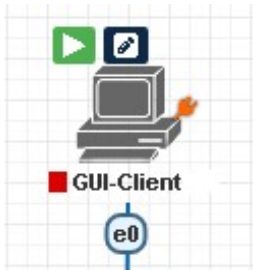
Esto completa la implementación independiente de la configuración de CheckPoint Standalone R81 con Firewall y Management Server instalados en el mismo iso .

Nota: Después de la instalación del servidor de gestión, la iso tardará de 5 a 10 minutos en inicializarse e iniciar todos los procesos. Por lo tanto, es recomendable esperar de 5 a 10 minutos y luego conectarse al servidor de administración desde SmartConsole – (máquina cliente GUI)

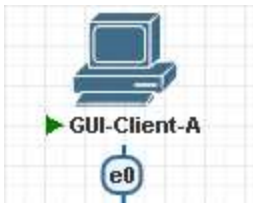
Instalación de la consola inteligente

Ahora procederemos con la instalación de SmartConsole en la máquina cliente GUI.

Haga clic en el botón Inicio para iniciar el nodo GUI-Client



Una vez que se inicia el nodo: haga doble clic para conectarse a la consola VNC



Haga clic en Abrir para conectarse a la consola VNC

This site is trying to open ultravnc_wrapper.

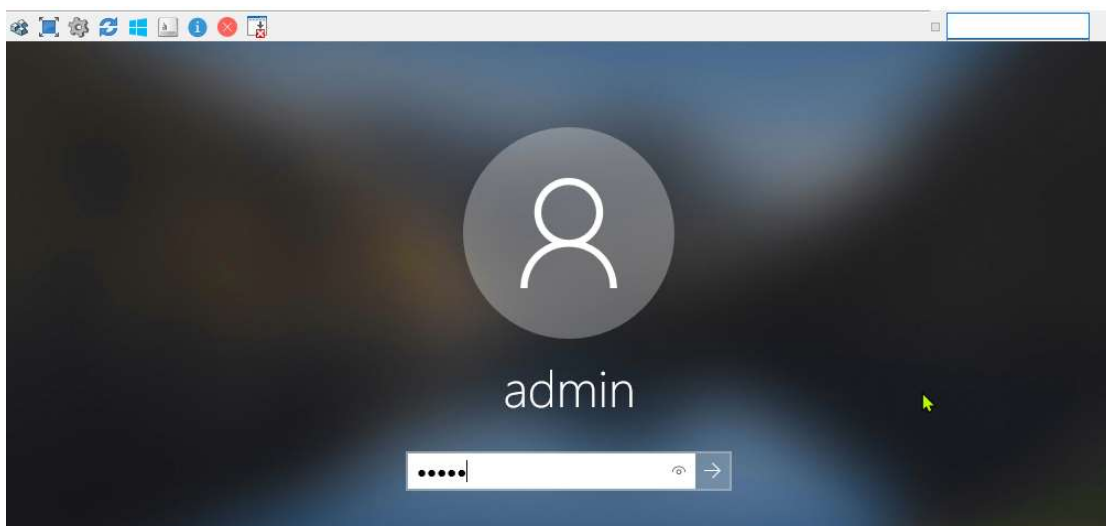
https://10.0.0.100 wants to open this application.

Always allow 10.0.0.100 to open links of this type in the associated app

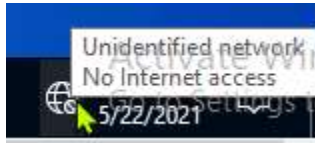
Open

Cancel

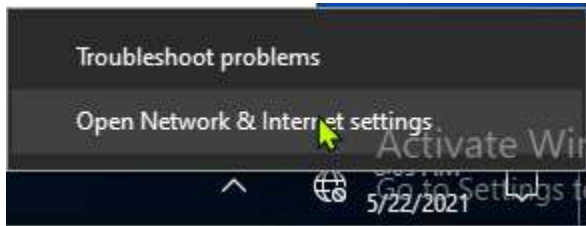
Use admin/admin para iniciar sesión en el nodo de cliente de la GUI de Windows



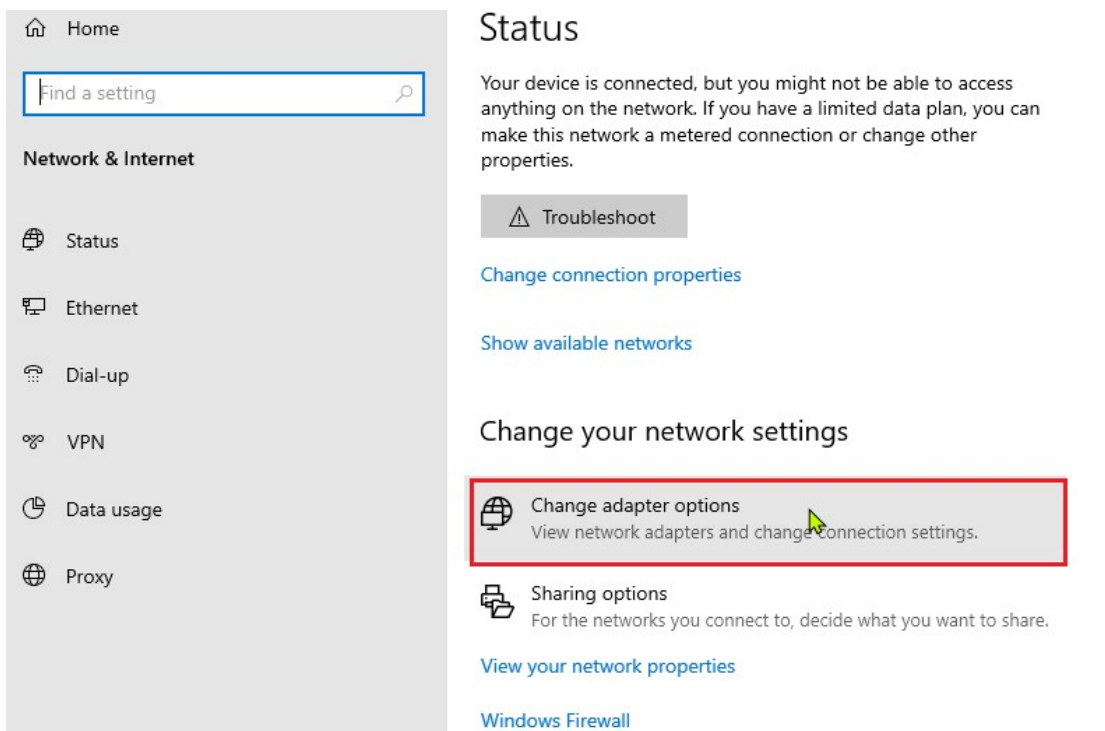
Haga clic en Configuración de red para configurar la dirección IP en el nodo GUI-Client



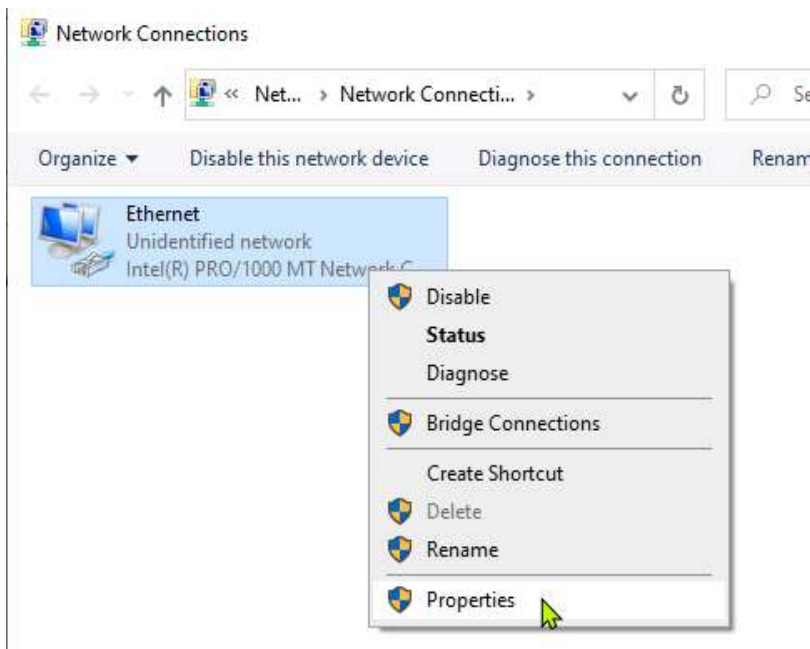
Haga clic en Abrir configuración de red e Internet



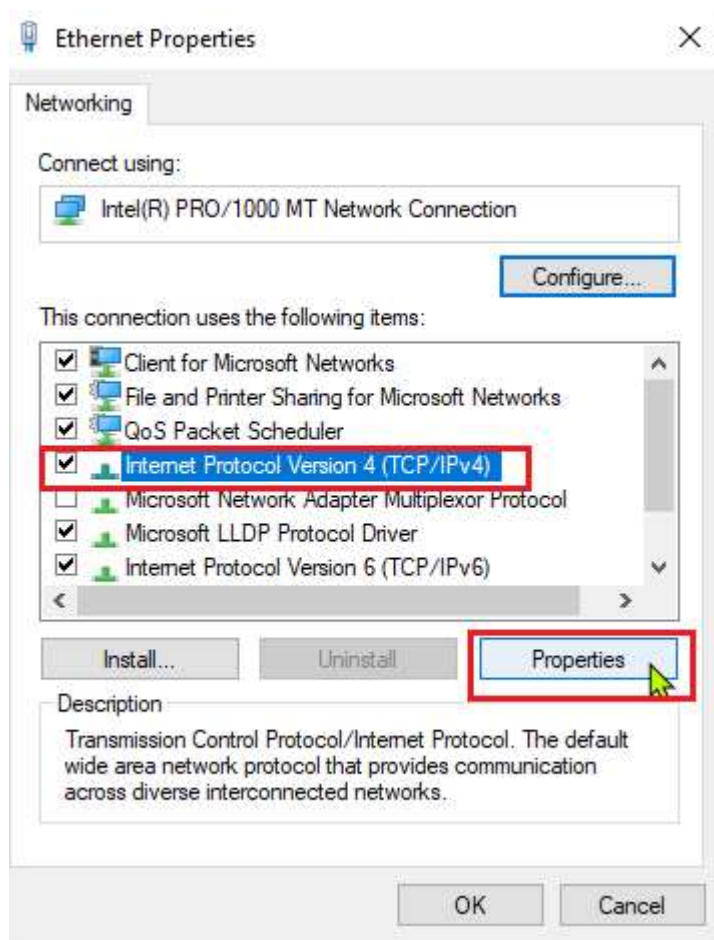
Haga clic en las opciones de Cambiar Adaptado



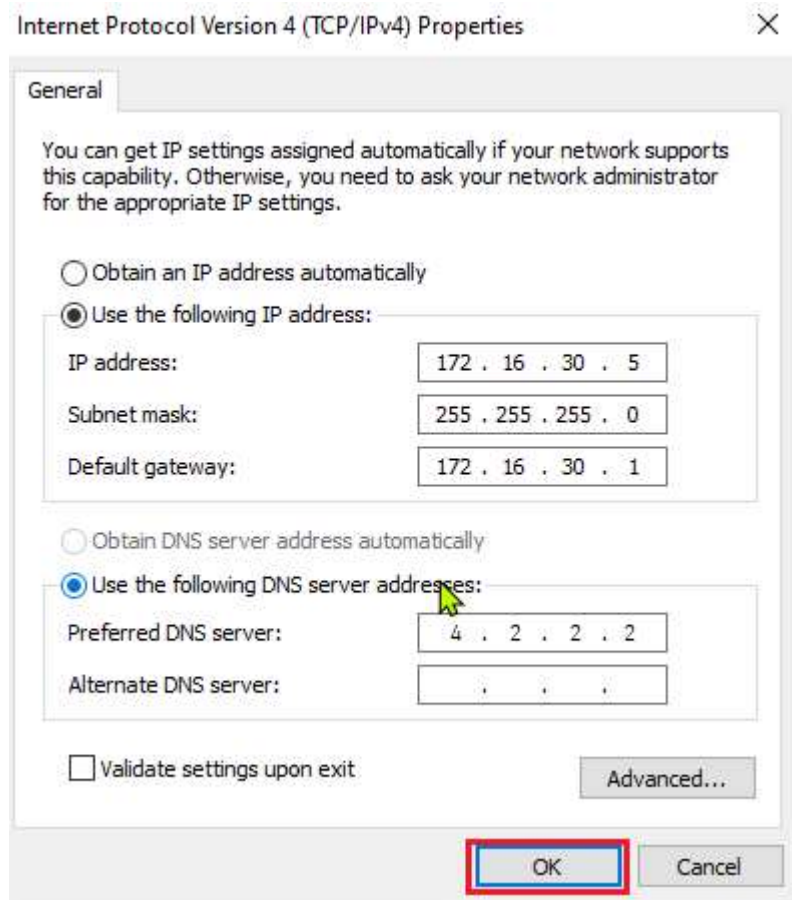
Haga clic derecho en la interfaz de red y haga clic en Propiedades



Haga clic en la opción de configuración de IPv4 y haga clic en Propiedades



Configure la dirección IP: 172.16.30.5, máscara de subred de 255.255.255.0 y puerta de enlace predeterminada de 172.16.30.1 y cierre la pestaña Redes y configure el servidor DNS de 4.2.2.2



Con el navegador Edge, conéctese a <https://172.16.30.1> para descargar la configuración de SmartConsole . Tenga en cuenta que estamos utilizando la dirección IP eth0 del nodo de firewall para conectarnos a la interfaz de usuario web desde la máquina del cliente GUI



This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

 [Go to your Start page](#)

Details

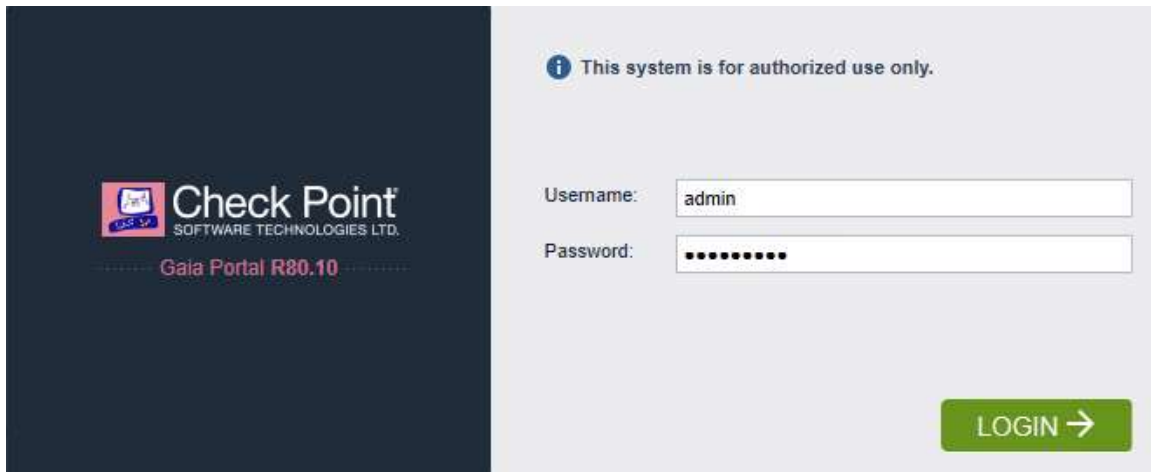
Your PC doesn't trust this website's security certificate.

The hostname in the website's security certificate differs from the website you are trying to visit.

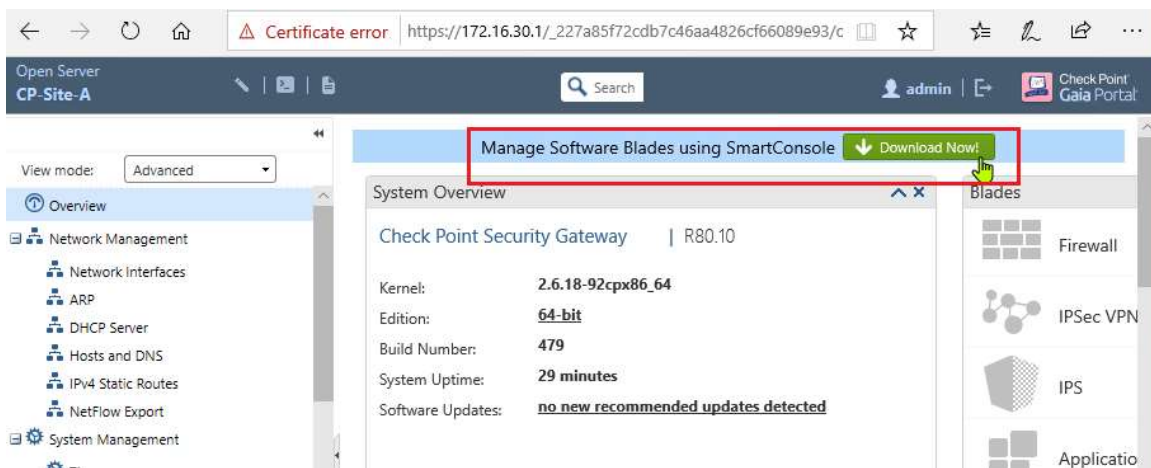
Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

[Go on to the webpage](#) (Not recommended)

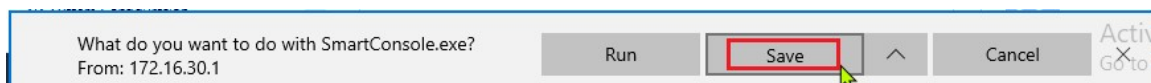
Inicie sesión con las credenciales admin/admin@123



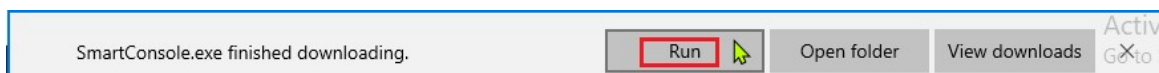
Haga clic en el botón para descargar la configuración de SmartConsole



Haga clic en la opción Guardar

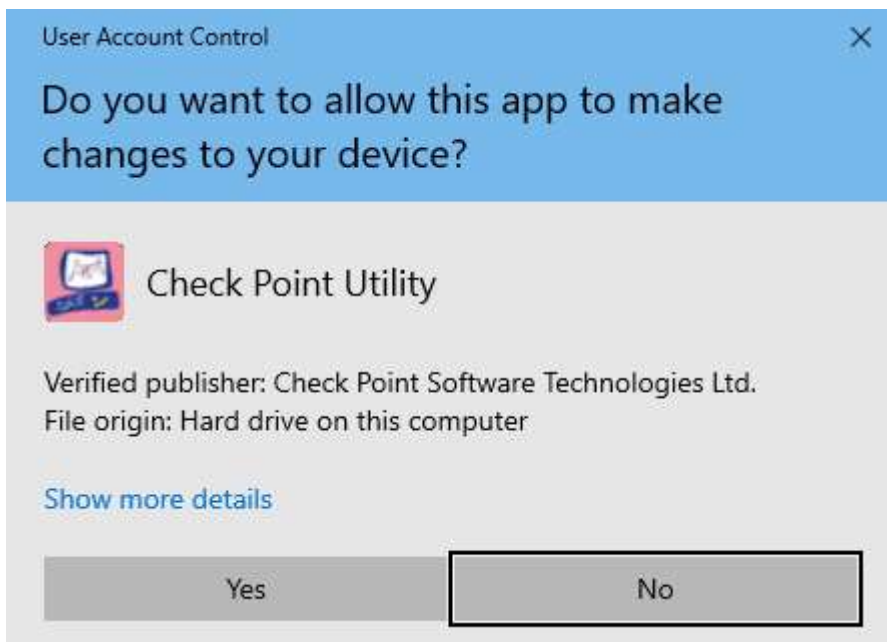


Haga clic en Ejecutar para iniciar la configuración de Smart Console

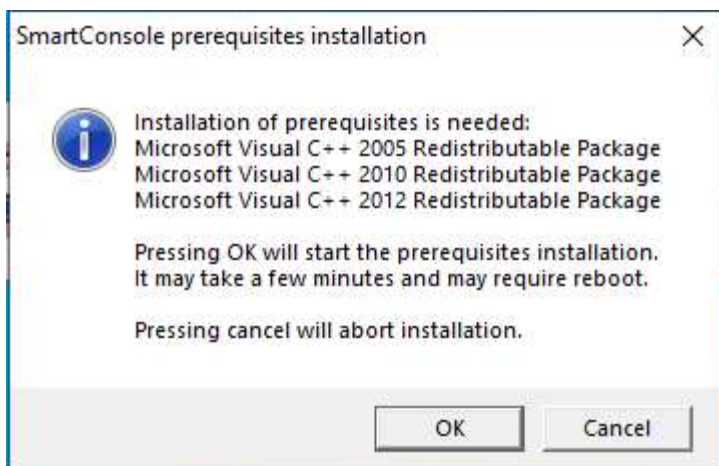


La instalación comenzará

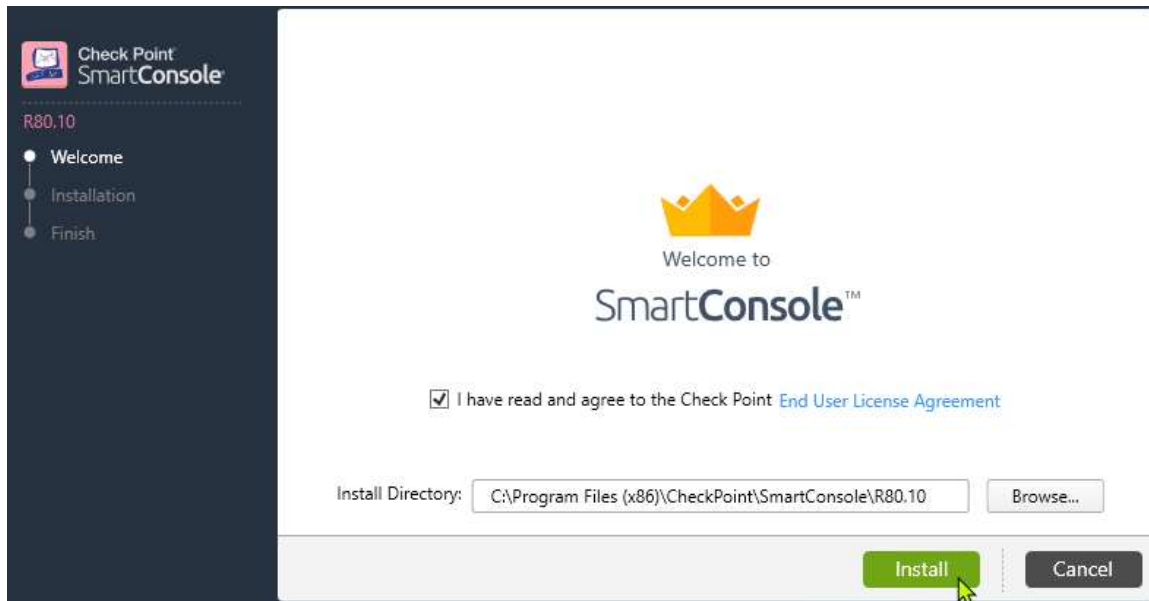
Haga clic en Sí para el cuadro de diálogo Control de cuentas de usuario si se le solicita



Si es necesario, la configuración instalará componentes de terceros: haga clic en Aceptar

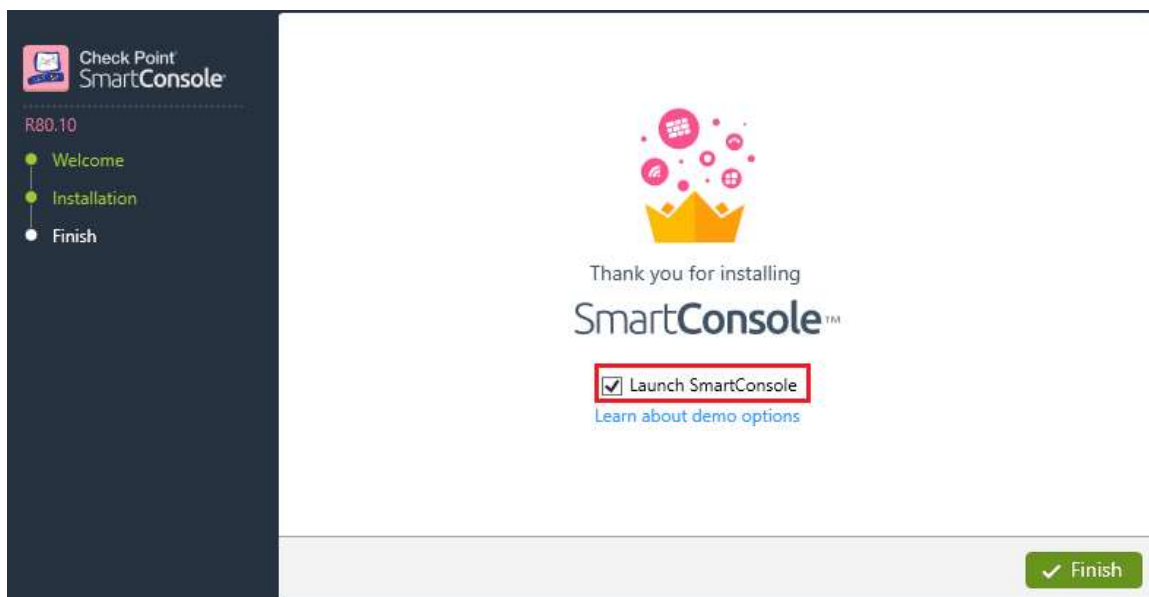


Haga clic en el Acuerdo de licencia de usuario final y haga clic en Instalar



de SmartConsole continuará.

Haga clic en Finalizar para iniciar la SmartConsole

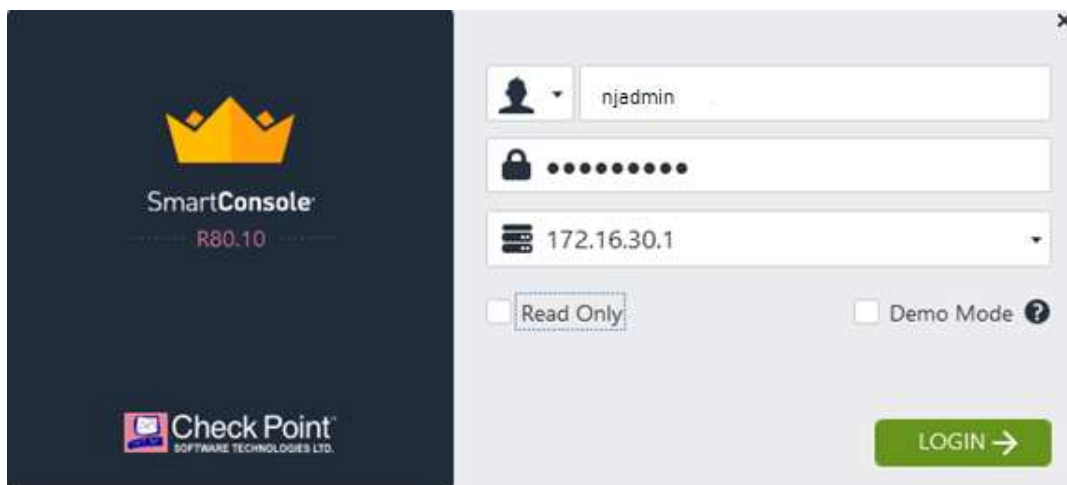


En este punto se completa la instalación de SmartConsole

Iniciar sesión en SmartConsole

Ahora iniciaremos sesión en el sistema Standalone CheckPoint usando la consola inteligente

La SmartConsole solicitará 3 cosas como se muestra: nombre de usuario, contraseña e IP del servidor

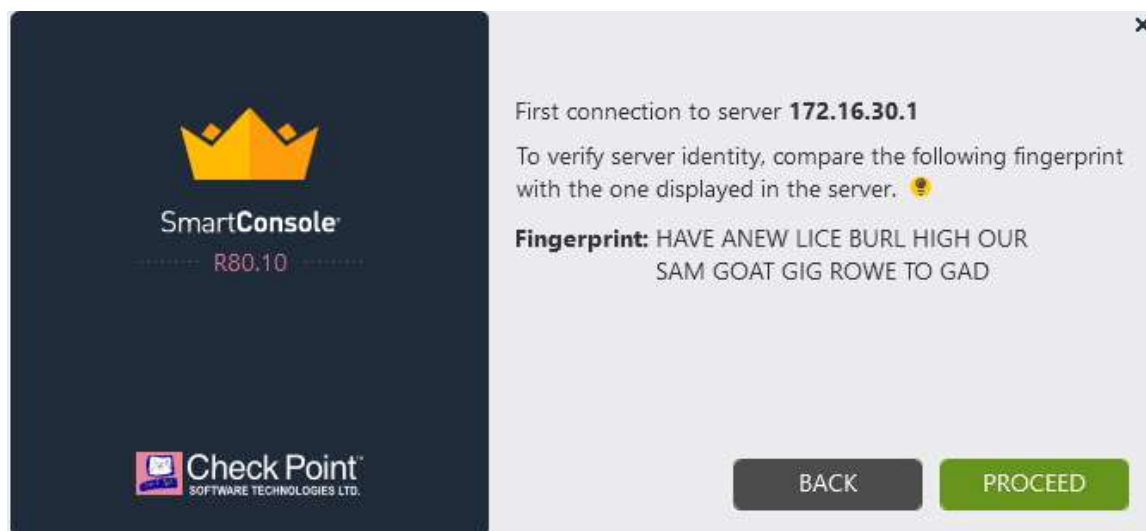


The image shows the SmartConsole login interface. On the left is a dark blue panel with the SmartConsole logo (a crown) and the version 'R80.10'. Below it is the Check Point logo. On the right is a light gray login form with a close button (X) in the top right corner. The form contains: a user selection dropdown with 'nadmin' selected; a password field with 10 dots; an IP address field with '172.16.30.1' and a dropdown arrow; a 'Read Only' checkbox; a 'Demo Mode' checkbox with a help icon; and a green 'LOGIN' button with a right-pointing arrow.

Las credenciales son nadmin / nadmin que creamos durante la etapa de administración de seguridad de la instalación. La dirección IP es la dirección IP eth0 del sistema CheckPoint

Haga clic en Iniciar sesión para continuar

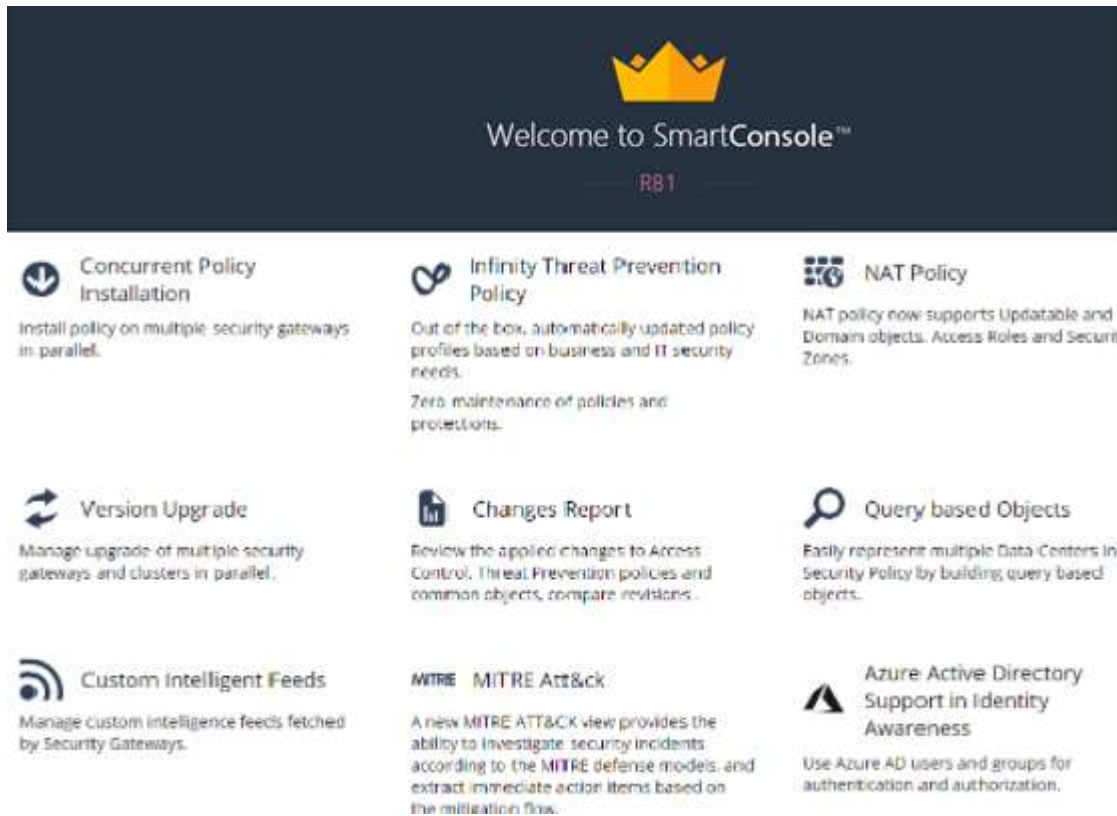
Se le presentará una huella digital durante la primera vez que inicie sesión en SmartConsole



The image shows the SmartConsole fingerprint verification screen. On the left is the same dark blue panel as in the previous image. On the right is a light gray panel with a close button (X) in the top right corner. The text reads: 'First connection to server 172.16.30.1', 'To verify server identity, compare the following fingerprint with the one displayed in the server. ⚠️', and 'Fingerprint: HAVE ANEW LICE BURL HIGH OUR SAM GOAT GIG ROWE TO GAD'. At the bottom are two buttons: a gray 'BACK' button and a green 'PROCEED' button.

Haga clic en Continuar

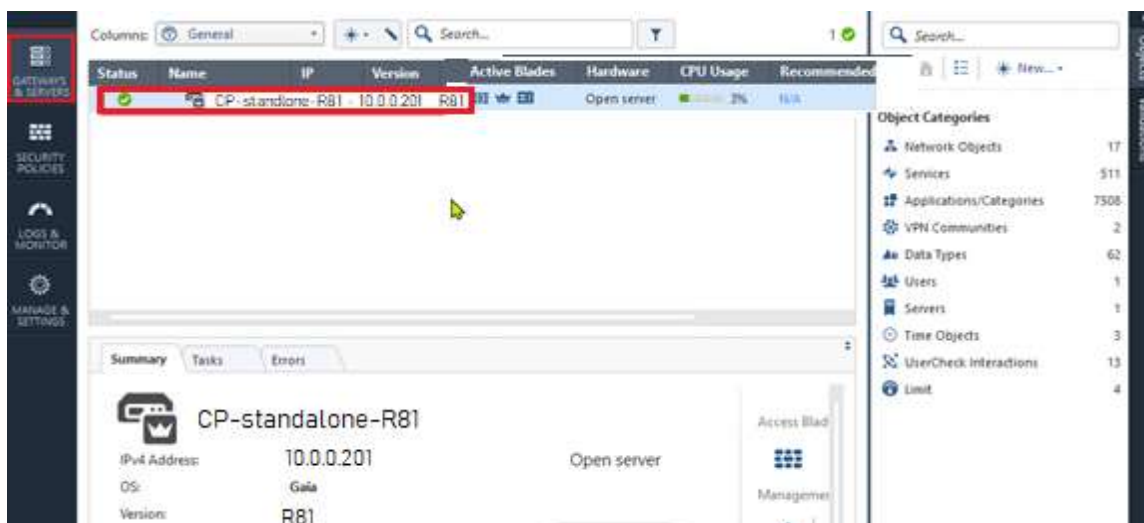
Se le presentarán las "Novedades de R81" durante el primer inicio de sesión en la consola. Puede presionar Esc para continuar



Welcome to SmartConsole™
R81

- Concurrent Policy Installation**
Install policy on multiple security gateways in parallel.
- Infinity Threat Prevention Policy**
Out of the box, automatically updated policy profiles based on business and IT security needs.
Zero maintenance of policies and protections.
- NAT Policy**
NAT policy now supports Updatable and Domain objects. Access Roles and Security Zones.
- Version Upgrade**
Manage upgrade of multiple security gateways and clusters in parallel.
- Changes Report**
Review the applied changes to Access Control, Threat Prevention policies and common objects, compare revisions.
- Query based Objects**
Easily represent multiple Data Centers in Security Policy by building query based objects.
- Custom Intelligent Feeds**
Manage custom intelligence feeds fetched by Security Gateways.
- MITRE MITRE Att&ck**
A new MITRE ATT&CK view provides the ability to investigate security incidents according to the MITRE defense models, and extract immediate action items based on the mitigation flow.
- Azure Active Directory Support in Identity Awareness**
Use Azure AD users and groups for authentication and authorization.

Finalmente, iniciamos sesión en la consola con nuestra implementación de firewall independiente.



The screenshot shows the SmartConsole interface with a table of security gateways. The table has columns for Status, Name, IP, Version, Active Blades, Hardware, CPU Usage, and Recommended. One gateway is highlighted with a red box: CP-standalone-R81, IP 10.0.0.201, Version R81. Below the table, there is a summary card for CP-standalone-R81 showing its IPv4 Address (10.0.0.201), OS (Gaia), and Version (R81). The right sidebar shows Object Categories with counts: Network Objects (17), Services (511), Applications/Categories (7308), VPN Communities (2), Data Types (62), Users (1), Servers (1), Time Objects (3), UserCheck Interactions (13), and Limit (4).

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended
✓	CP-standalone-R81	10.0.0.201	R81	1	Open server	2%	N/A

Summary CP-standalone-R81

IPv4 Address: 10.0.0.201
OS: Gaia
Version: R81

Open server

Access Blade Management

Object Categories

- Network Objects: 17
- Services: 511
- Applications/Categories: 7308
- VPN Communities: 2
- Data Types: 62
- Users: 1
- Servers: 1
- Time Objects: 3
- UserCheck Interactions: 13
- Limit: 4