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

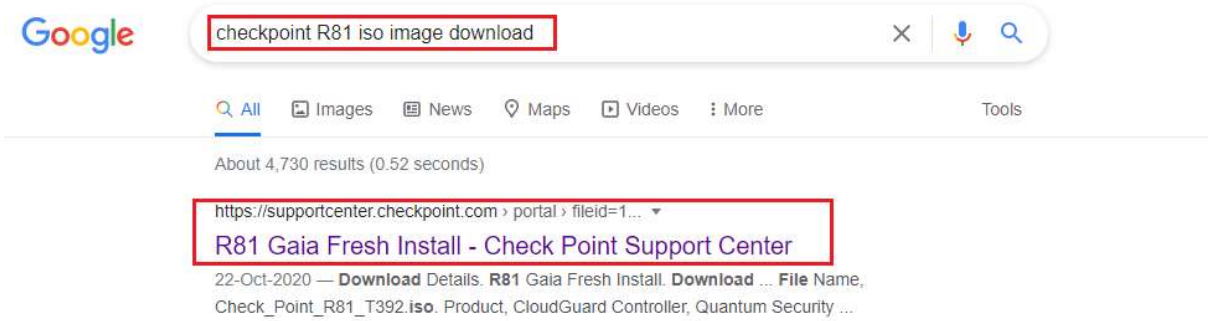
Este libro (más de 600 páginas) consta de 25 escenarios de laboratorio (paso a paso) para diferentes escenarios de configuración para CheckPoint Firewall versión R81. La plataforma utilizada para la distribución del laboratorio es un entorno PNET similar a la plataforma EVENG. Se supone que también puede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

Contents

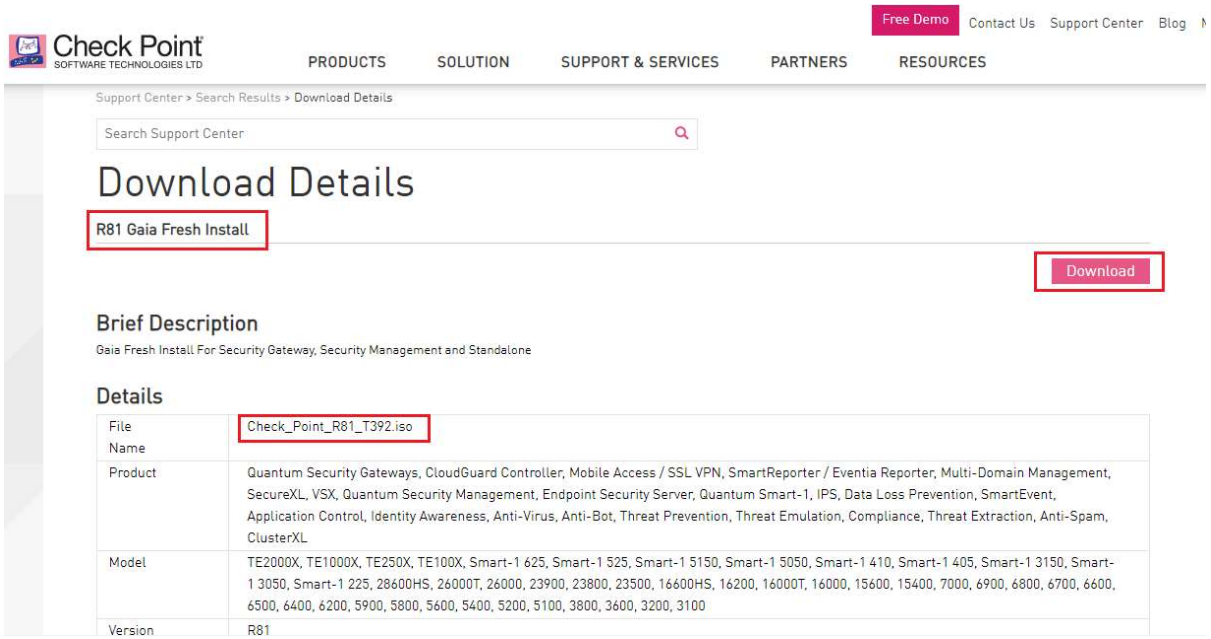
Tarea de laboratorio 1 ~ Implementación de CheckPoint ISO en un PNET LAB

Descargar imagen ISO de CheckPoint R81

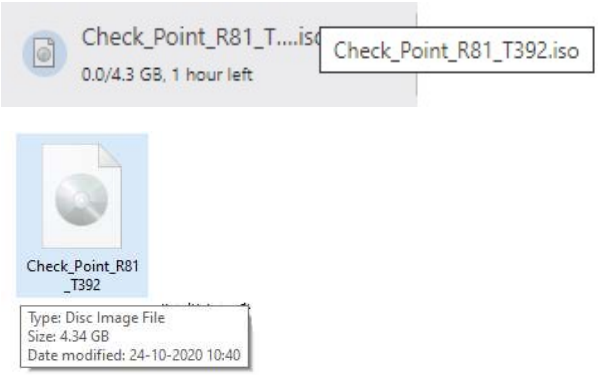
Busque la descarga de la imagen iso del punto de control R81 en Google como se muestra y haga clic en el enlace del centro de soporte.



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



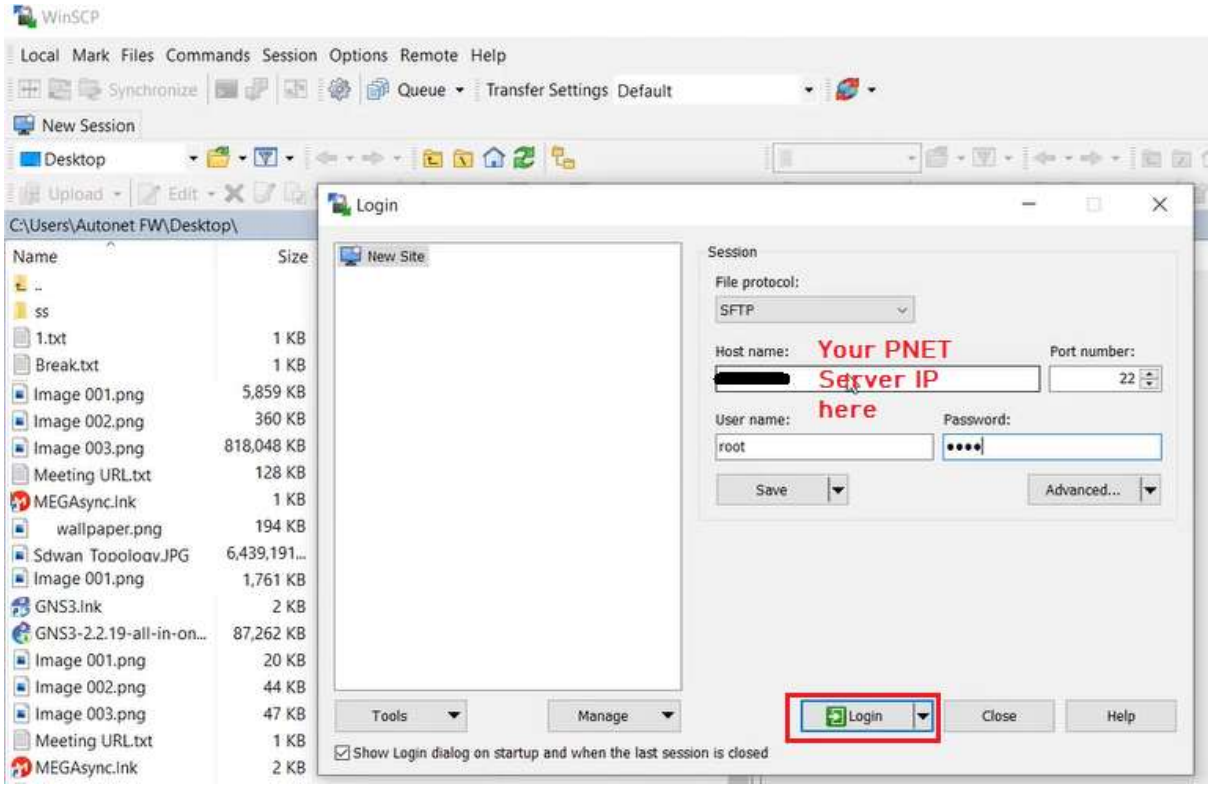
La descarga comienza como se muestra: archivo de aproximadamente 4 GB. Deje que la descarga se complete.



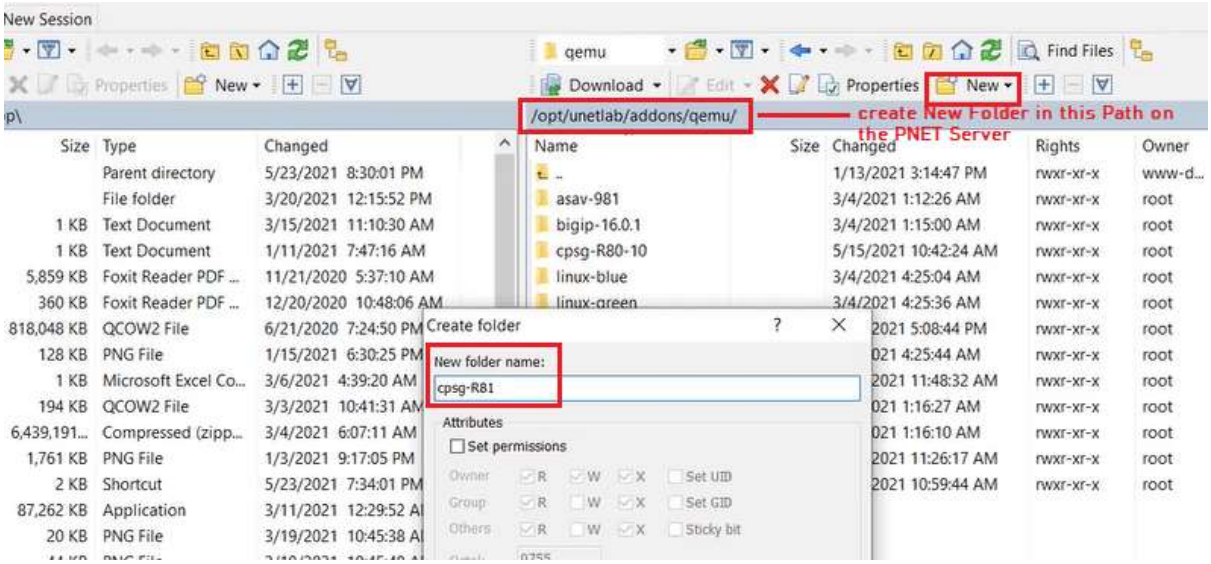
Instalar CheckPoint R81 en PNET

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

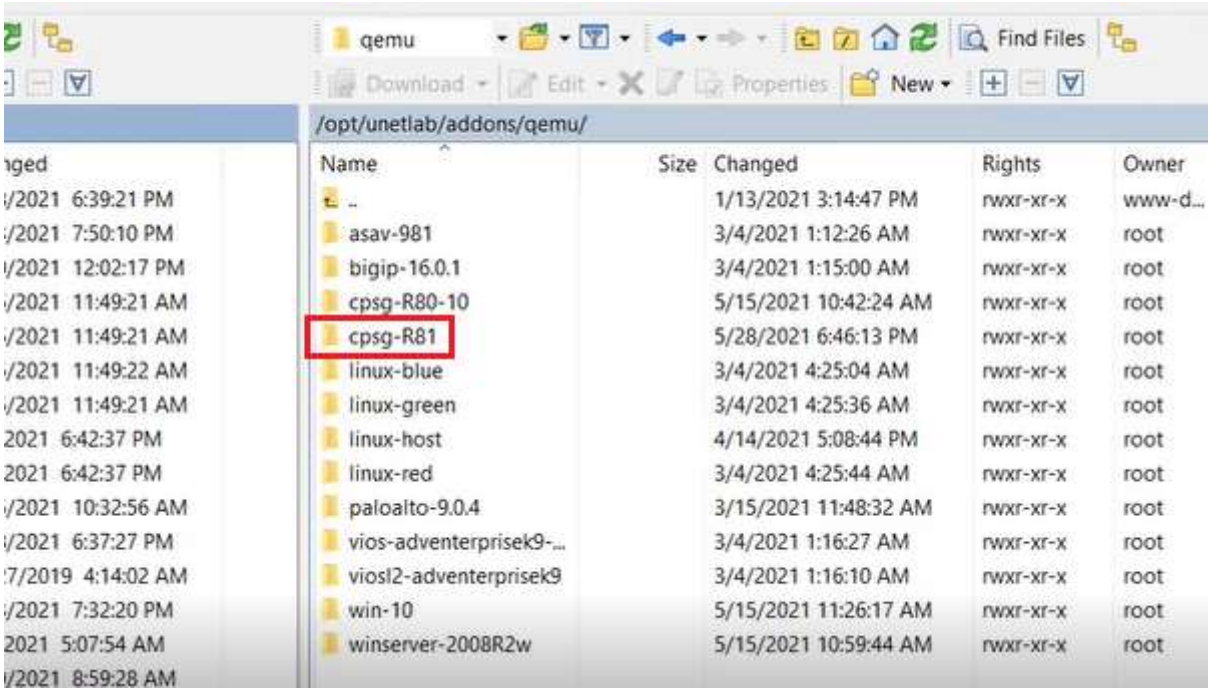
Proporcione los detalles de IP/Puerto y las credenciales de su servidor PNET LAB y haga clic en Iniciar sesión.



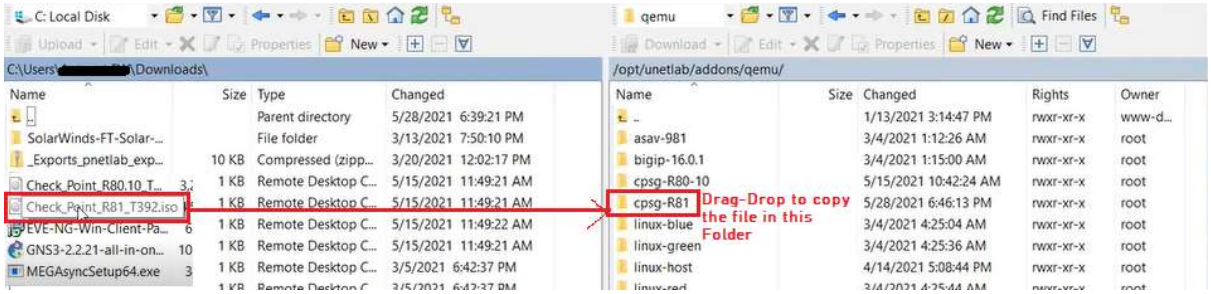
Una vez conectado al servidor PNET, Cree una Nueva Carpeta llamada “cpsg-R81” en la ruta /opt/ unetlab / addons / qemu /. Puede usar la opción Nuevo > Carpeta como se muestra.



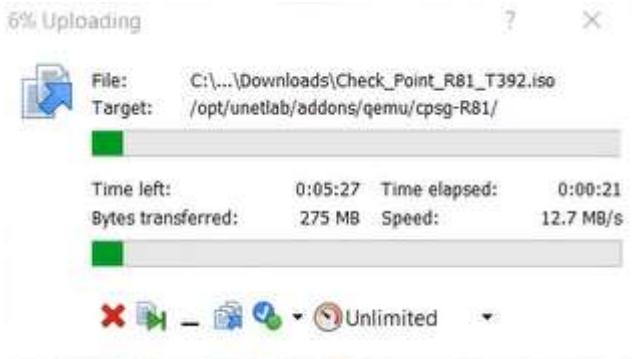
La carpeta se crea como se muestra



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

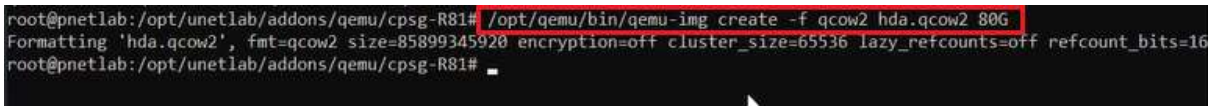


Una vez que se cargue el archivo, inicie sesión en el servidor PNET a través de Putty y busque la ruta

/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.

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

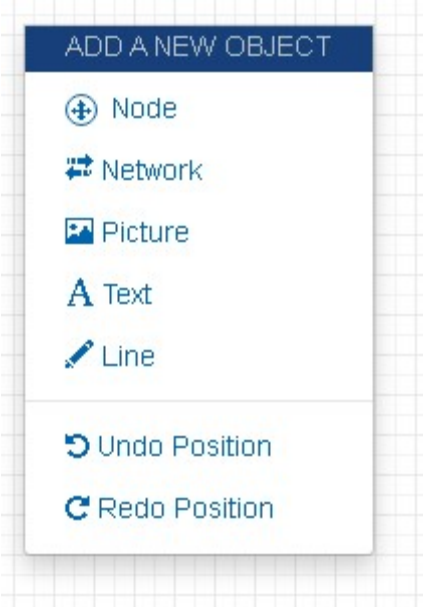
mv Check_Point_R81_T392.iso cdrom.iso
/opt/ qemu /bin/ qemu-img crear -f qcow2 hda.qcow 2 80G



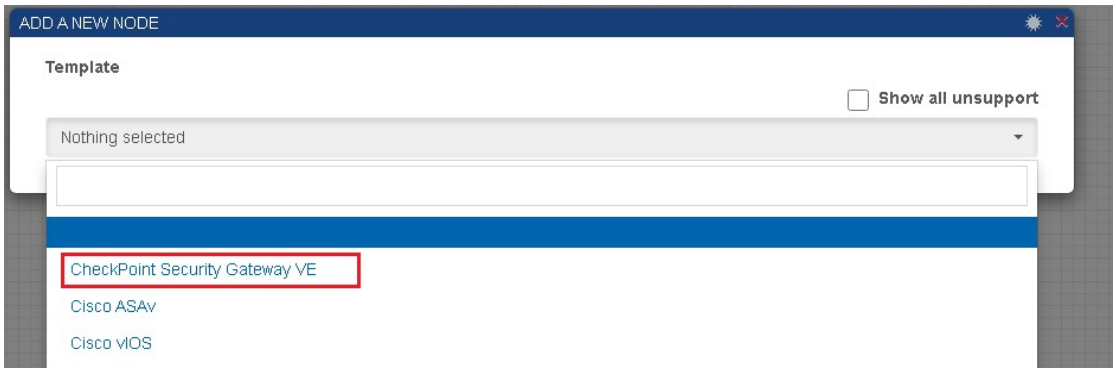
Ahora el nodo CheckPoint R81 está listo para agregarse al PNET Lab como se muestra a continuación. Puede crear un nuevo laboratorio en la consola PNET y agregar el nodo CheckPoint R81 como se muestra a continuación

Agregue el nodo CheckPoint a PNET LAB

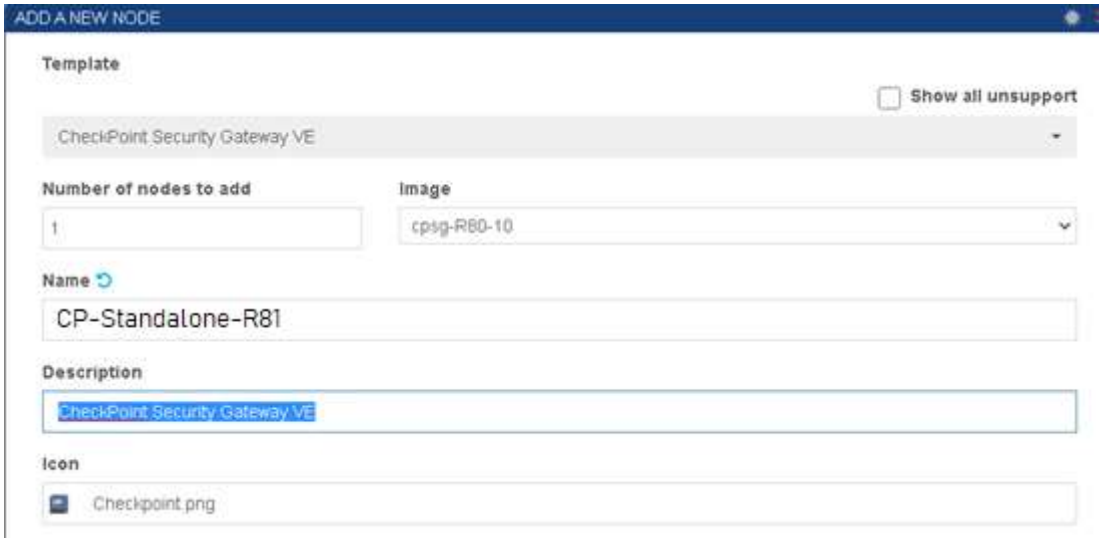
Una vez que obtenga acceso a PNET Lab, haga clic con el botón derecho en Área de laboratorio y seleccione "Nodo"



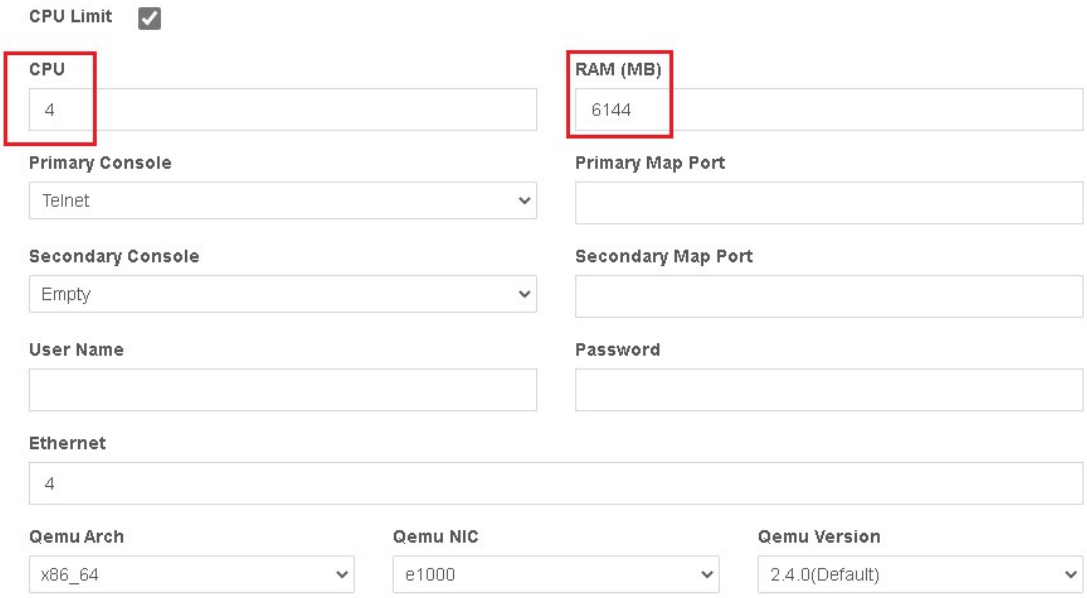
Seleccione la opción "CheckPoint Security Gateway VE"



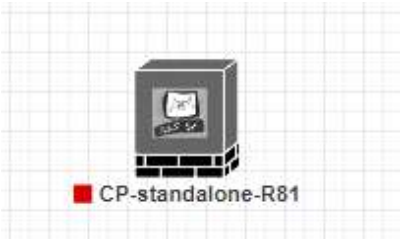
Cambie el nombre a "CP-independiente-R81"



Verifique las siguientes configuraciones en el nodo CheckPoint

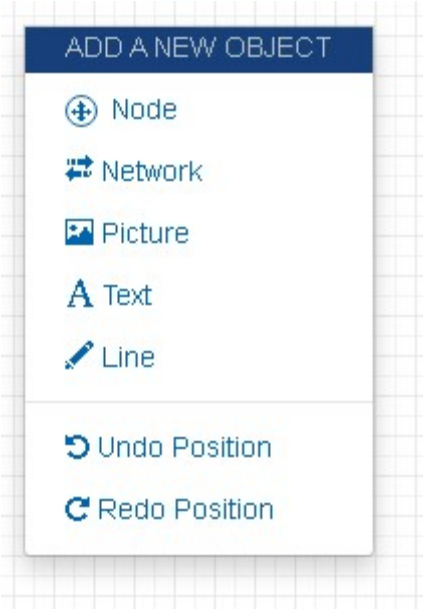


Los nodos de CheckPoint se agregan al área de laboratorio.

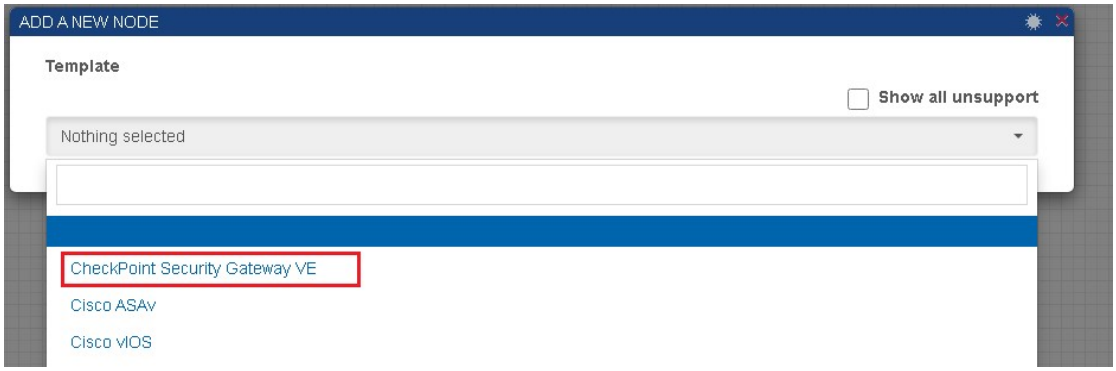


Tarea de laboratorio 2 ~ Implementación de un firewall de CheckPoint independiente (2 niveles)

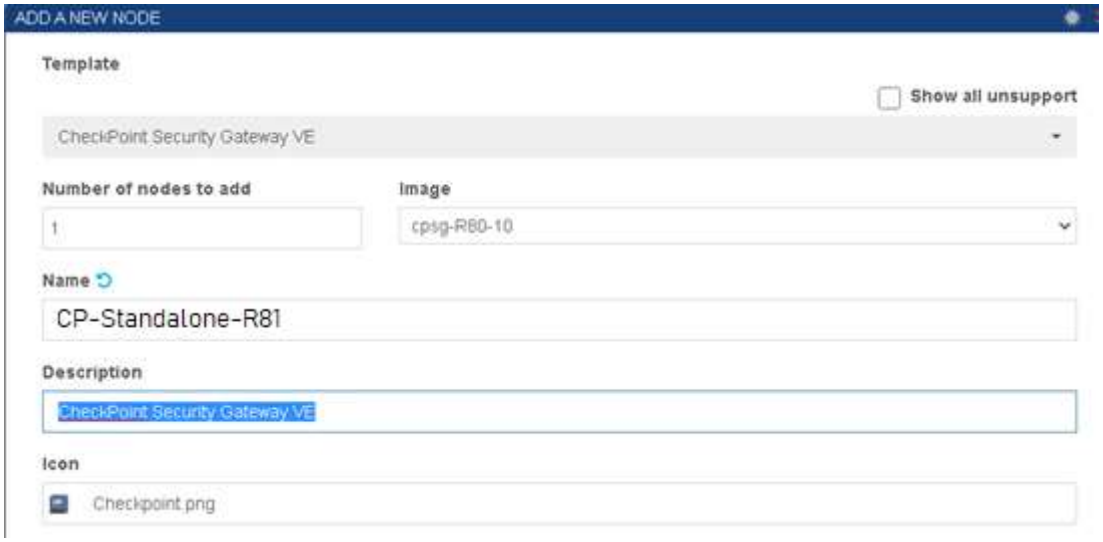
Una vez que obtenga acceso a PNET Lab, haga clic con el botón derecho en Área de laboratorio y seleccione "Nodo"



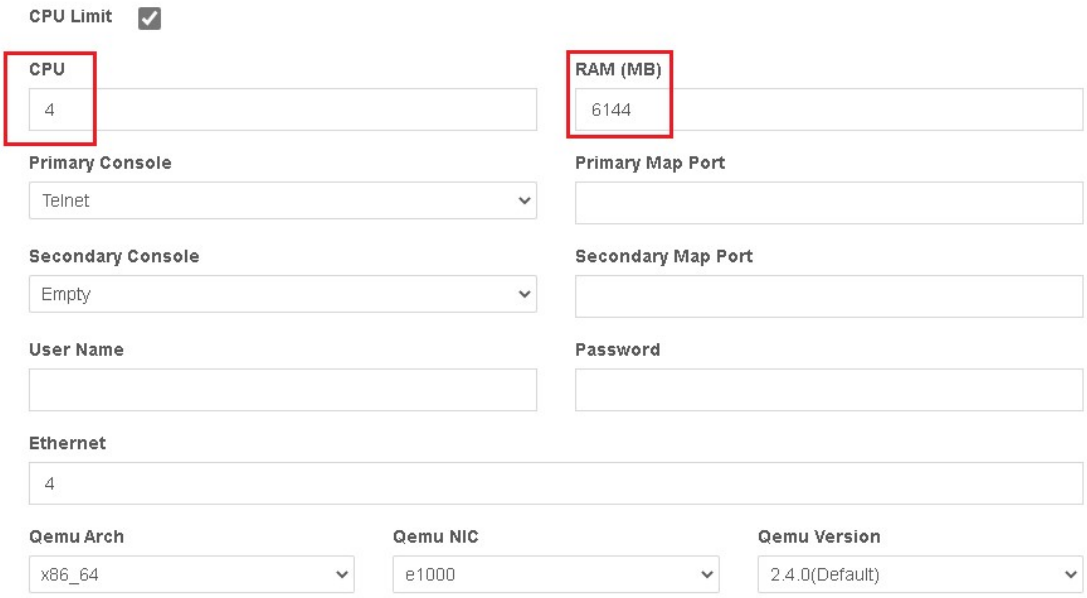
Seleccione la opción "CheckPoint Security Gateway VE"



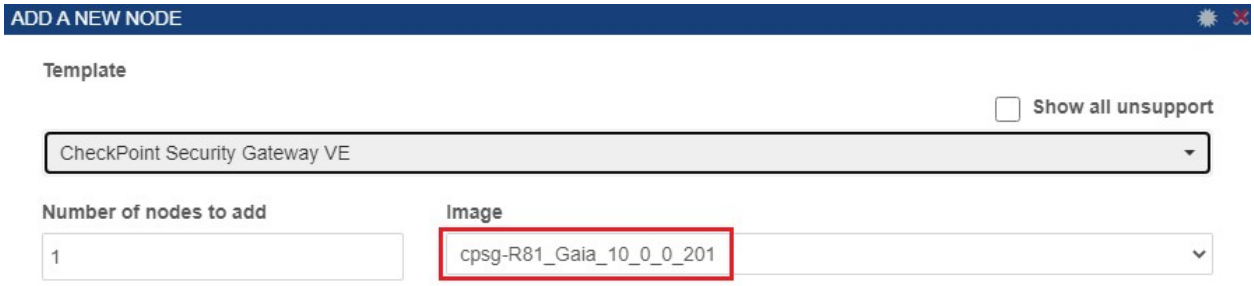
Cambie el nombre a "CP-independiente-R81"



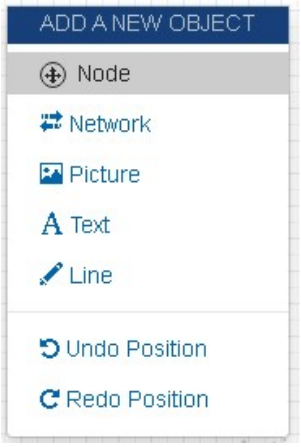
Verifique las siguientes configuraciones en el nodo CheckPoint



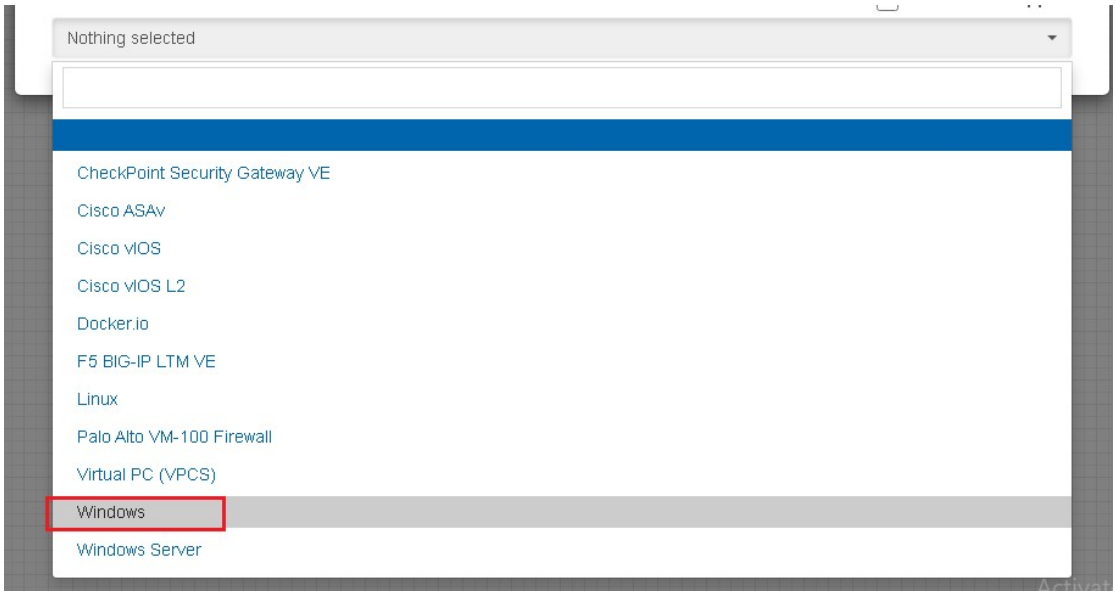
Nota : para los laboratorios usaremos la imagen de nodo comprometido de Checkpoint donde Gaia OS ya está instalado con una IP estática -10.0.0.201 configurada en la interfaz eth1 de CheckPoint como se muestra a continuación



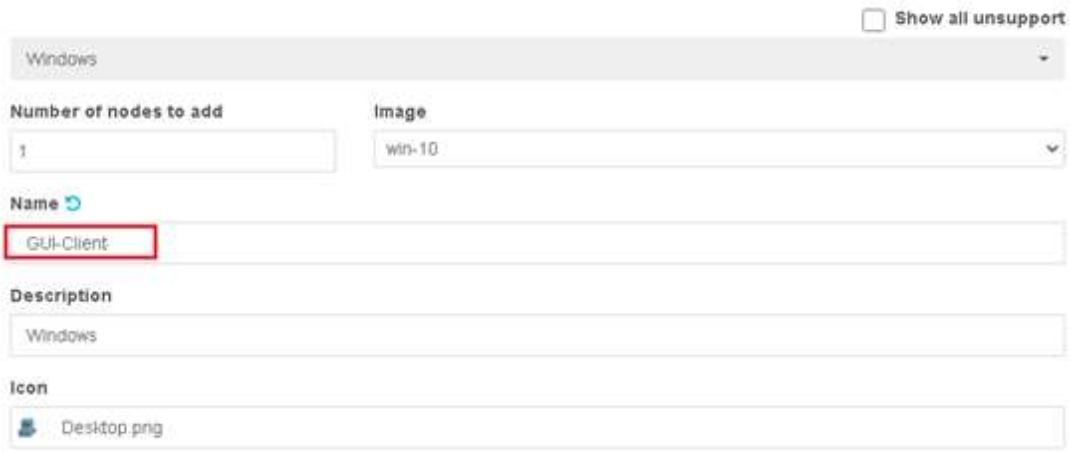
Haga clic con el botón derecho en Área de laboratorio y seleccione "Nodo"



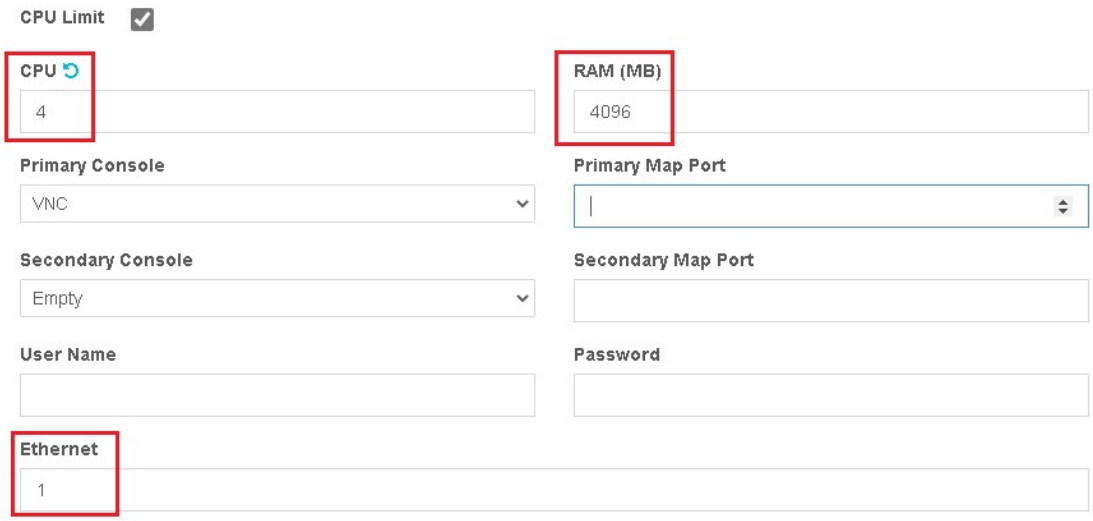
Seleccione la opción de Windows de la lista desplegable. Este nodo de Windows-10 se usará como nuestra consola inteligente o máquina cliente GUI

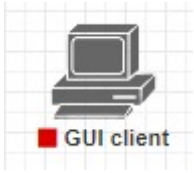


Cambie el nombre del Nodo a "GUI-Client"

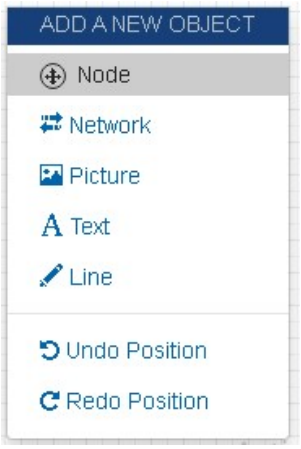


Verifique las siguientes configuraciones en el nodo del cliente GUI

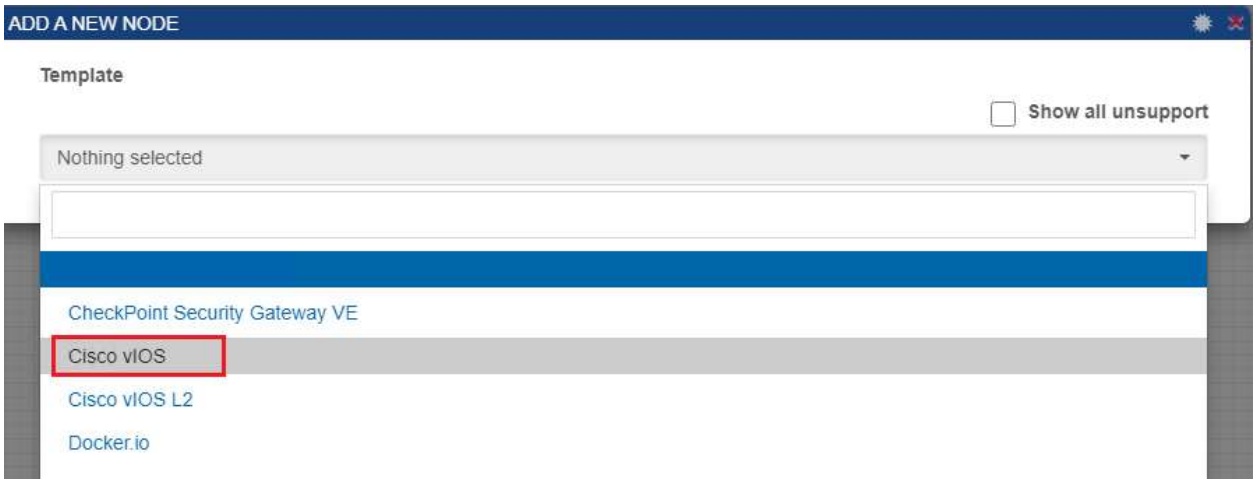




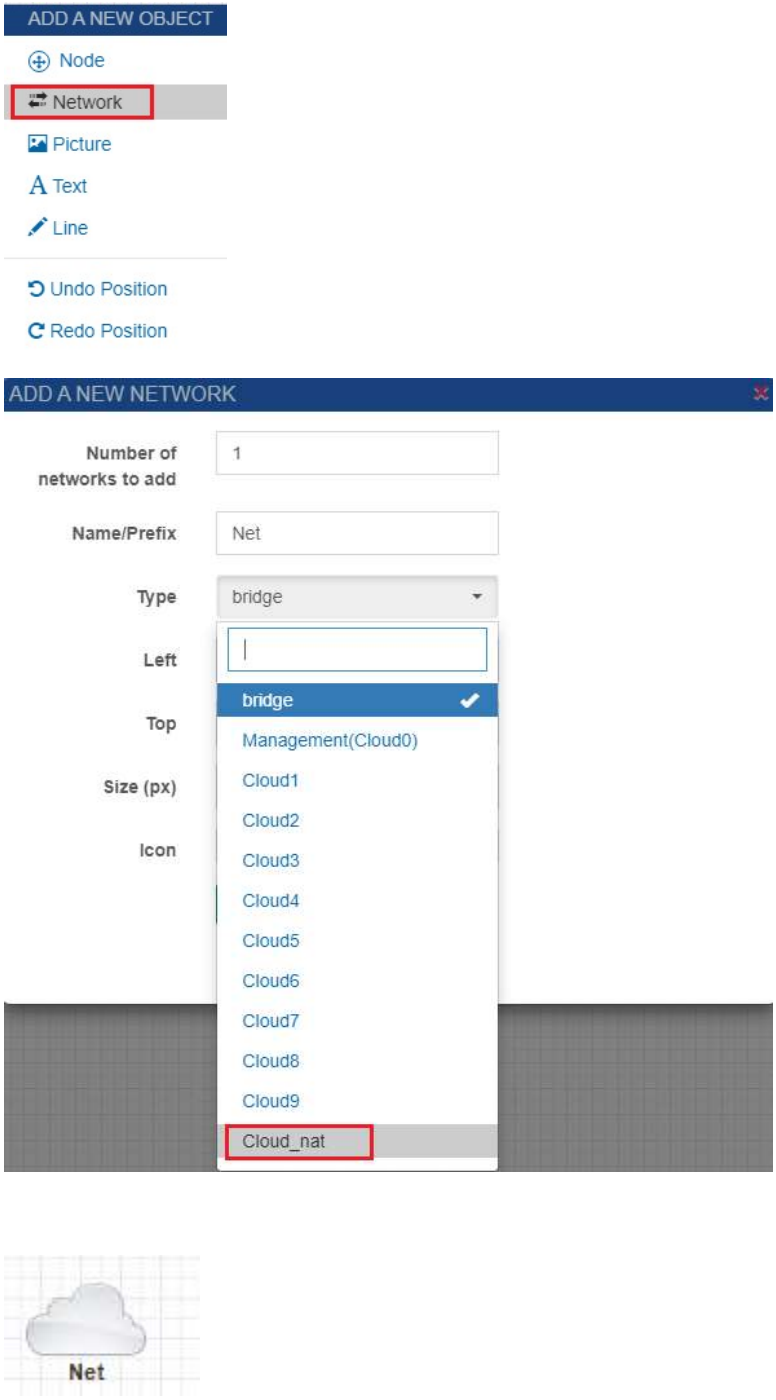
Haga clic en Agregar nodo



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

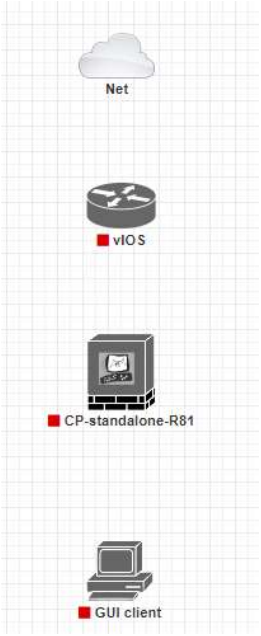


Haga clic en Agregar red como se muestra a continuación y agregue " Cloud_nat ". Esto es para la conectividad de nuestro segmento de Internet.


ADD A NEW OBJECT
Node
Network
Picture
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

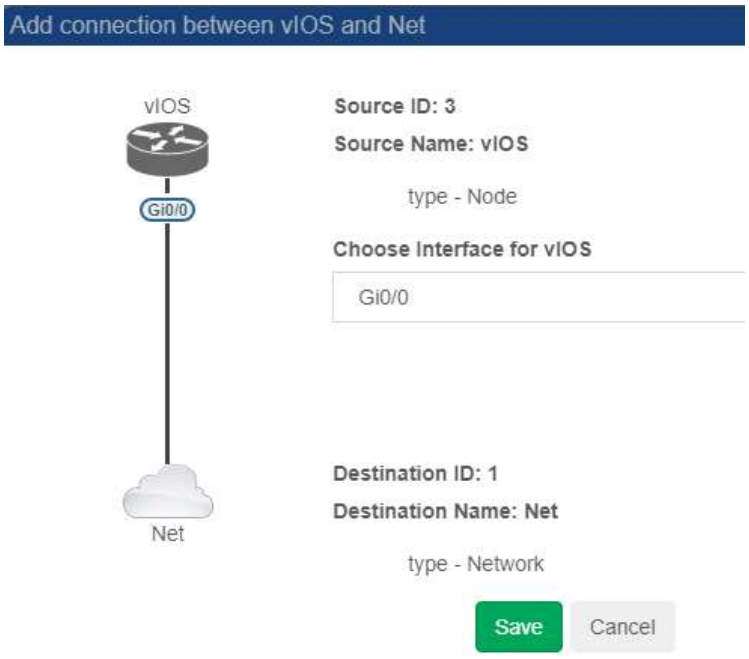
Net

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.

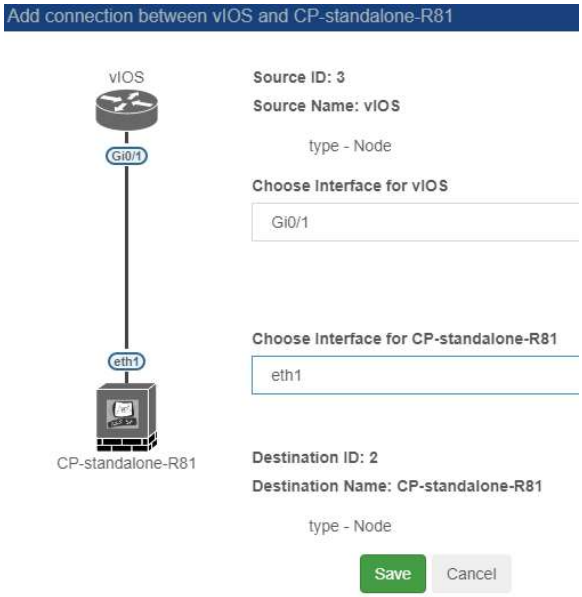


Ahora procederemos con la parte de conectividad de la siguiente manera

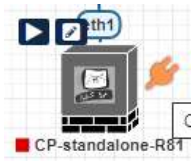
Conecte la interfaz Gi0/0 de vIOS a Cloud_nat como se muestra

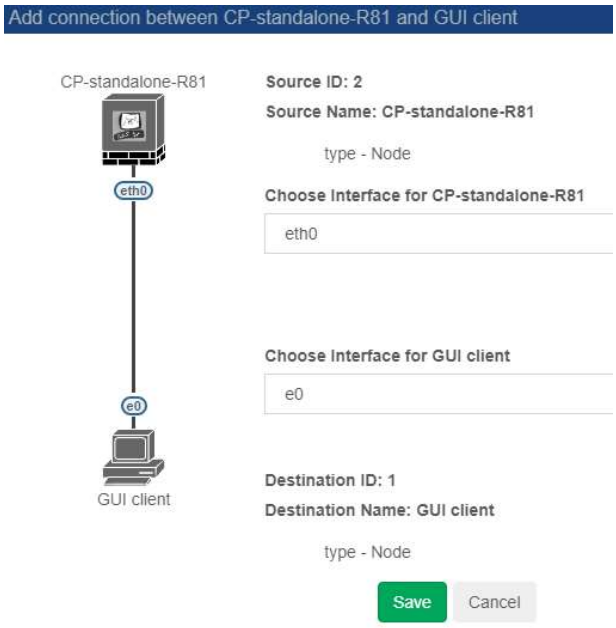


Conecte el Gi0/1 de vIOS a Checkpoint eth1 como se muestra



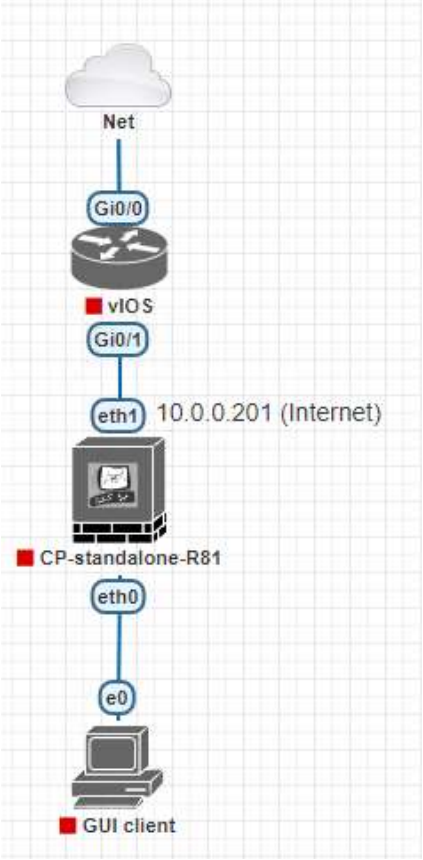
Conecte el CheckPoint eth-0 al nodo de Windows (cliente GUI) e0 como se muestra





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.

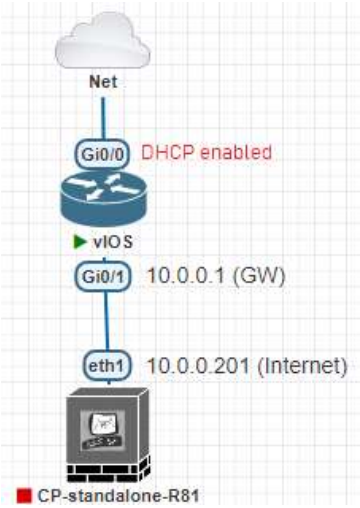
A continuación se muestra la configuración a realizar en el Router

(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.

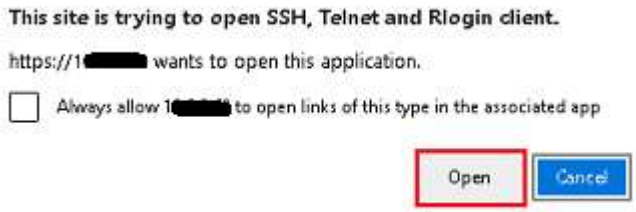
Instalación del sistema operativo Gaia

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.

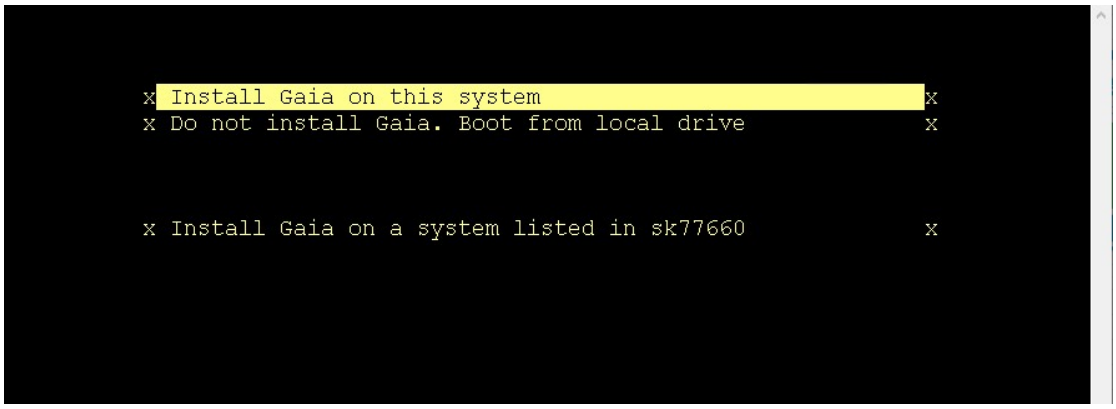
Inicie el nodo "CP-standalone-R81" y conéctese a la consola para comenzar la instalación del sistema operativo Gaia.

Haga clic en "Abrir" para iniciar la Consola

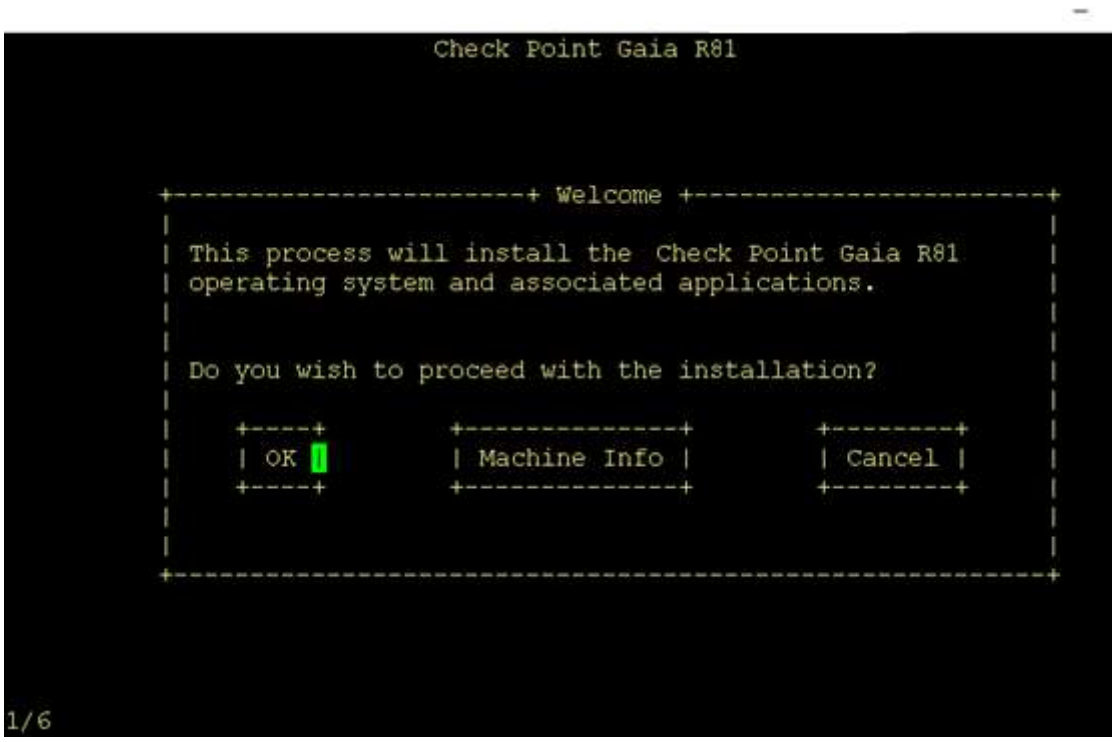


Selecciona la opción “Instalar Gaia en este sistema” y presiona “Enter”

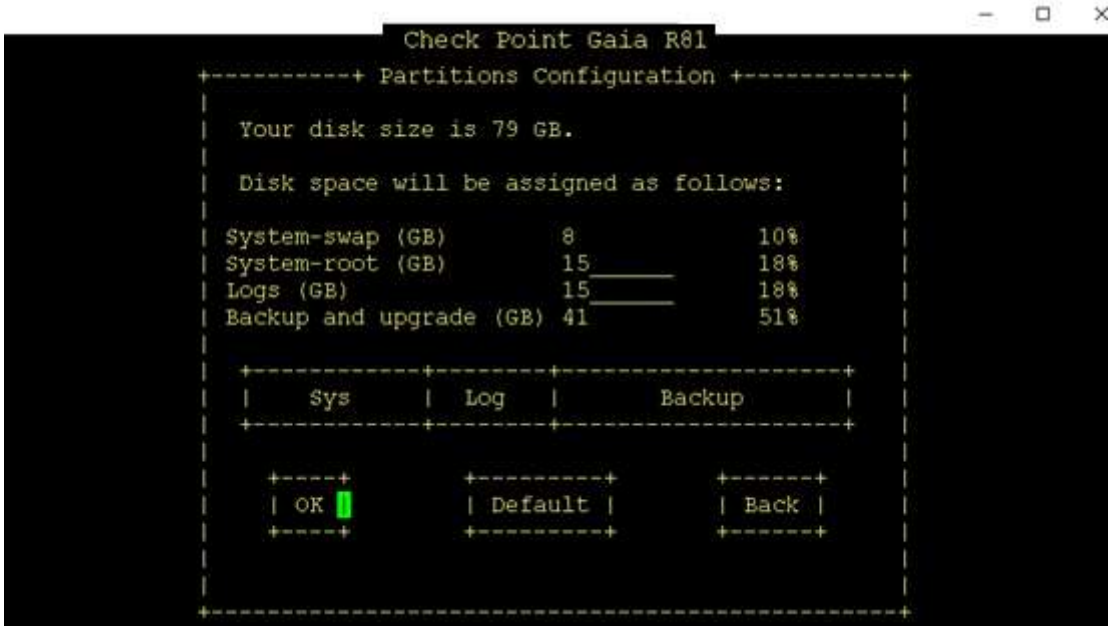
Nota: - En caso de que obtenga una pantalla en blanco, intente hacer clic en las teclas de flecha arriba / abajo para que las opciones sean visibles.



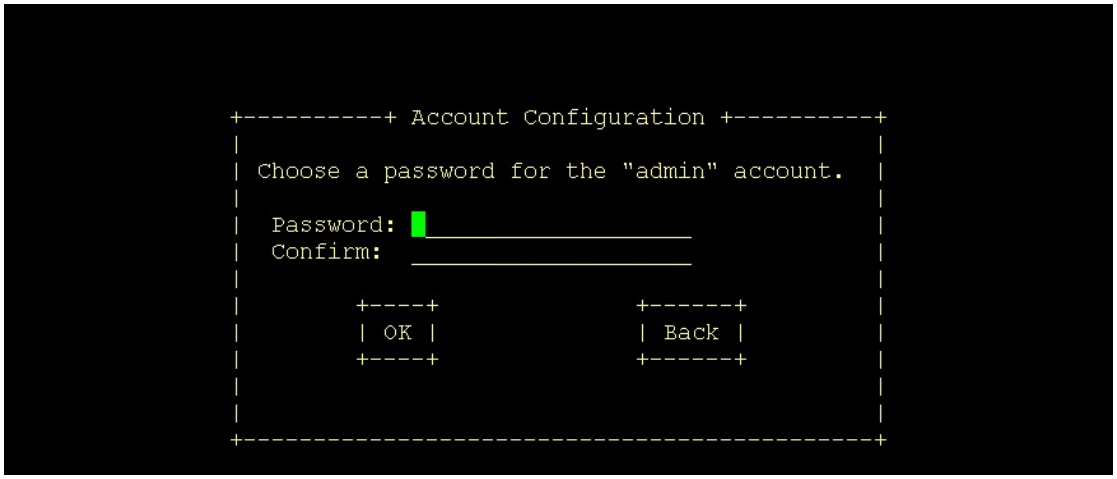
Haga clic en "Aceptar" para continuar con la instalación



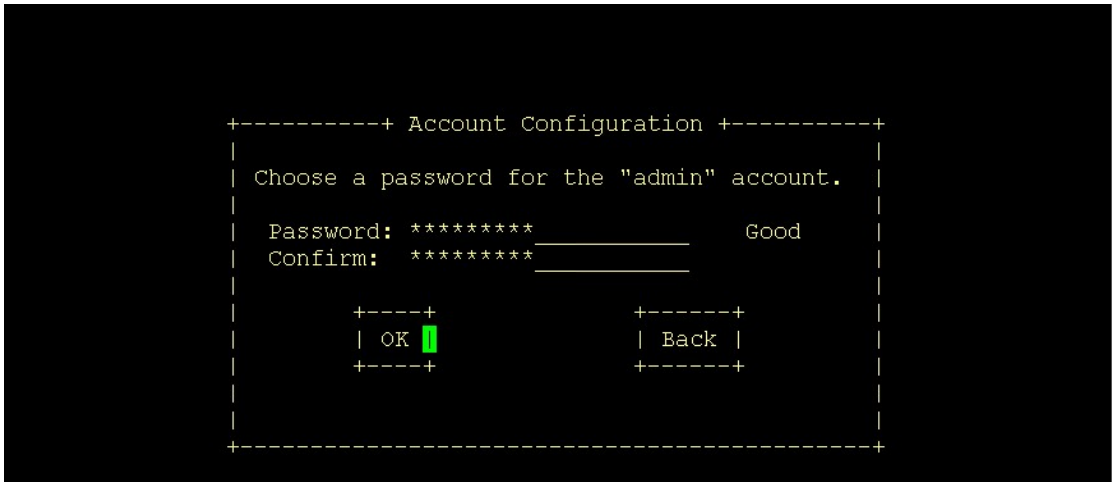
Deje los valores sin cambios y haga clic en "Aceptar" para continuar. Use TAB para navegar a la opción "OK" si es necesario y presione "Enter"



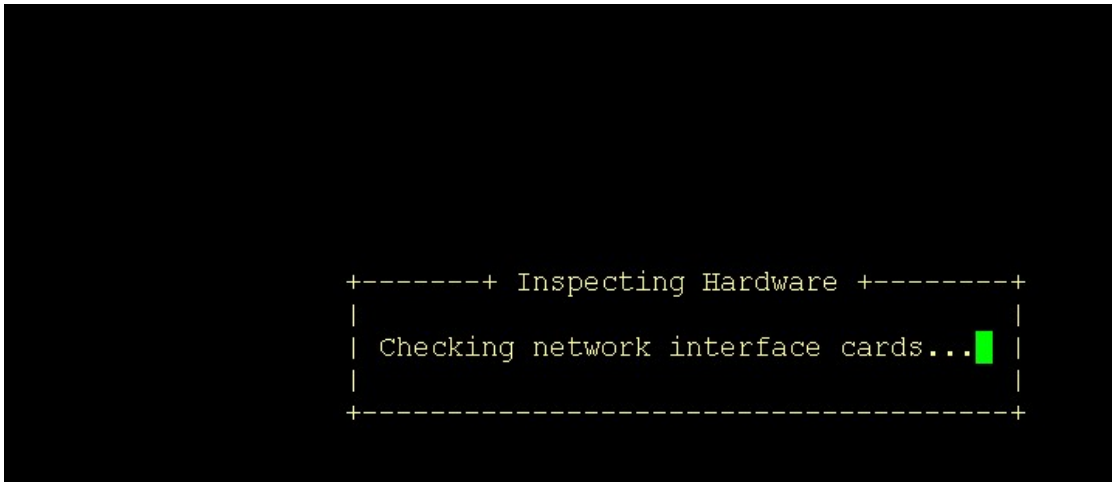
Establezca la contraseña como "admin@123" y confirme la misma.



Seleccione "OK" y luego presione "Enter"

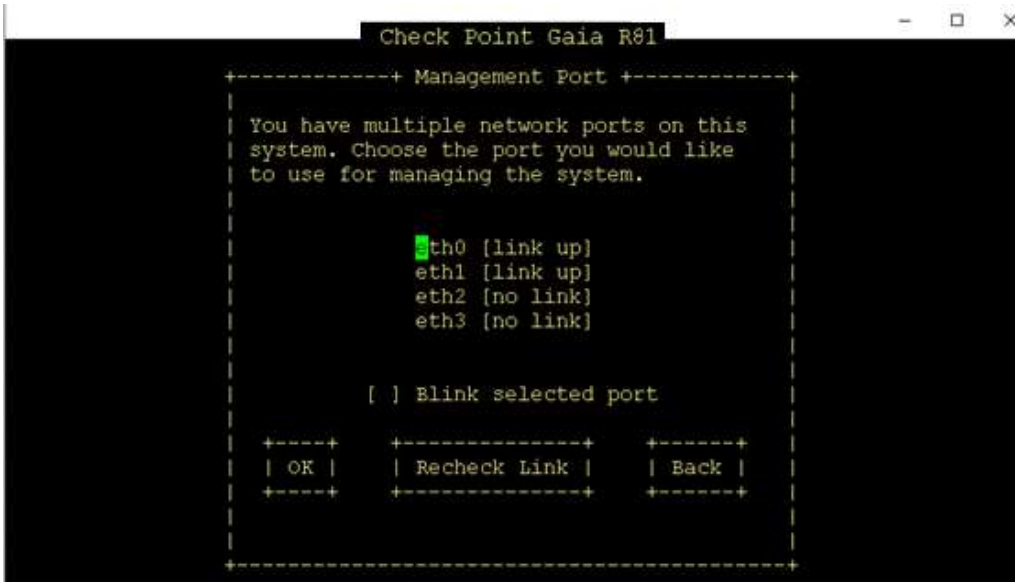


El proceso de instalación verificará las interfaces de red instaladas en el nodo CheckPoint

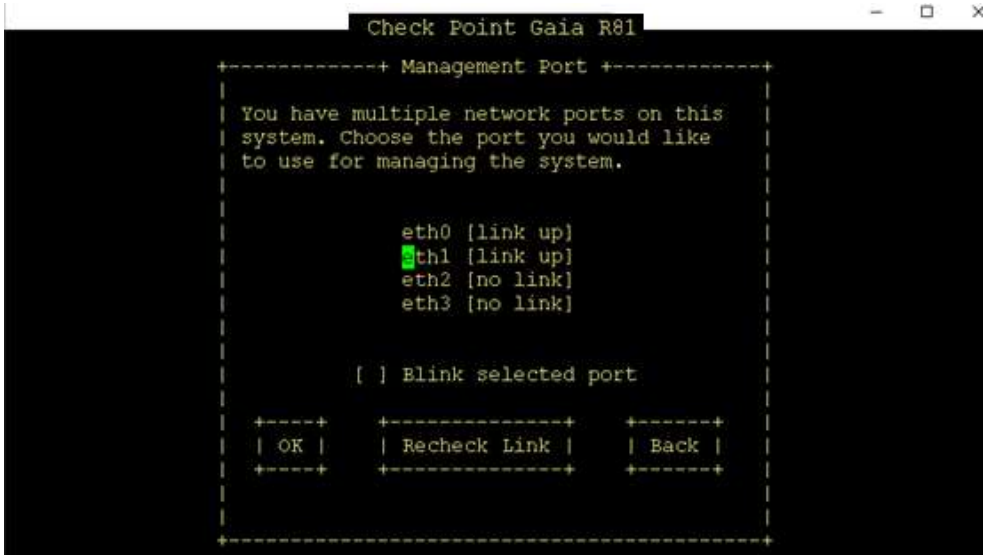


Tenga en cuenta que tenemos que crear una interfaz y preparar TCP/IP antes de la instalación de Gaia. La siguiente sección puede variar según la cantidad de interfaces que haya conectado. Solo queremos que la dirección IP esté configurada en 1 de las interfaces Ethernet y debe estar conectada en estado 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)



Seleccione eth1 y presione Entrar

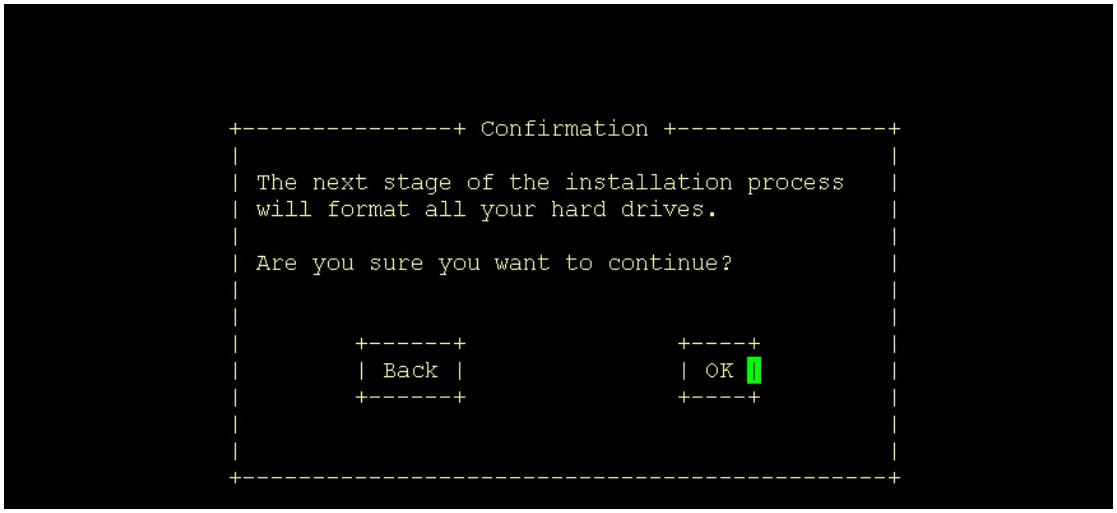


Configure la dirección IP de 10.0.0.201 en eth1 con Netmask de 255.255.255.0 y Default Gateway de 10.0.0.1 y navegue hasta Aceptar y presione "Enter".

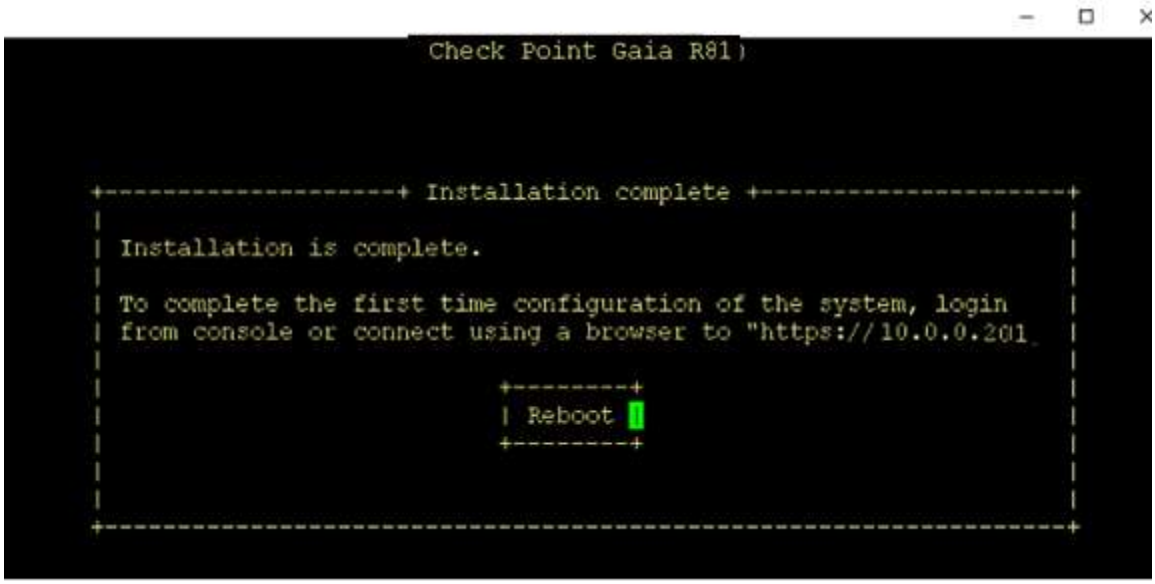
Esto es necesario porque la instalación de CheckPoint -Gaia requiere un mínimo de 1 interfaz preparada para TCP/IP (configurada con IP y el enlace debe estar conectado y activo)

La siguiente pantalla le pedirá su confirmación para la instalación.

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



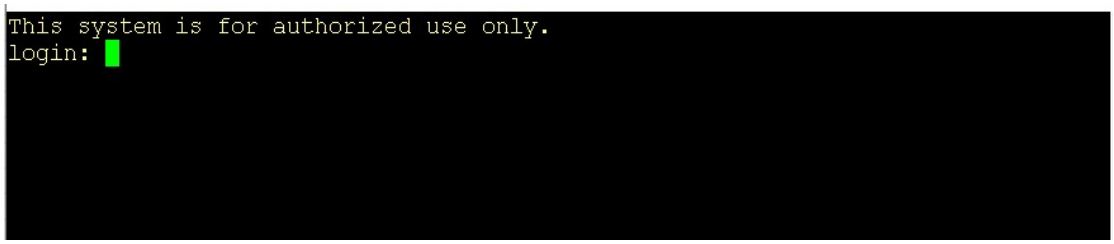
Las próximas pantallas instalarán varios módulos y finalmente recibirá un mensaje para reiniciar y volver a conectarse a " https://10.0.0.201 " para la configuración del sistema por primera vez.



Presione Enter para continuar con el proceso de reinicio.

Esto completa la instalación del sistema operativo Gaia. Ahora procederemos con la primera configuración del cortafuegos (implementación independiente)

Verifique que el sistema se reinicie y que pueda ver la pantalla de inicio de sesión como se muestra



Implementación independiente de CheckPoint (2 niveles)

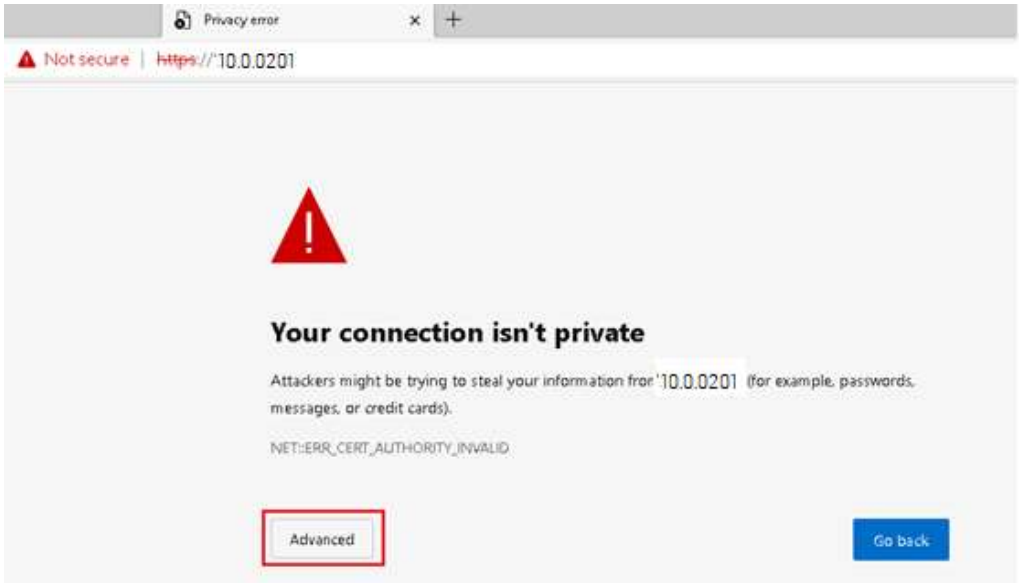
Nota: En caso de que no pueda comunicarse con la Máquina Gaia, es posible que deba configurar otra interfaz o activar la interfaz configurada.

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

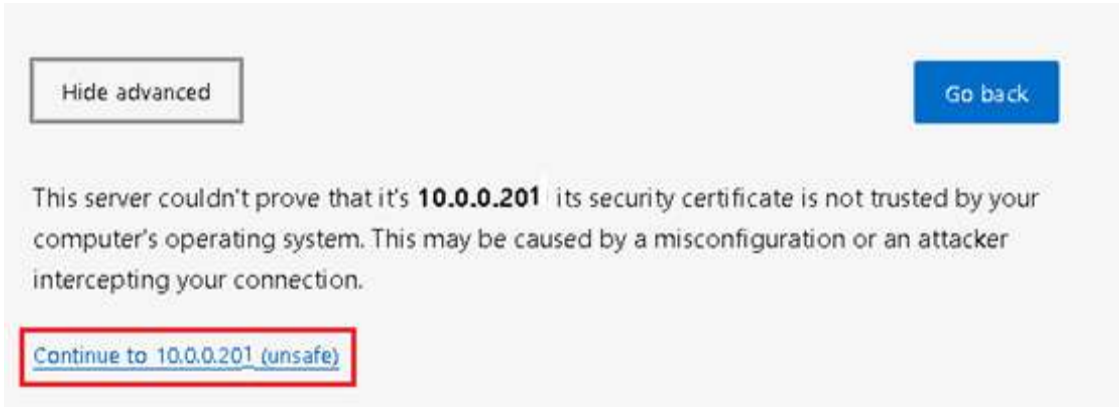
> *configure la interfaz eth0 ipv4-address 172.16.30.1 mask-length 24* ***< esta es la IP eth0 según nuestro LAB)***
> *establecer interfaz eth0 estado en*
> *guardar configuración*

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

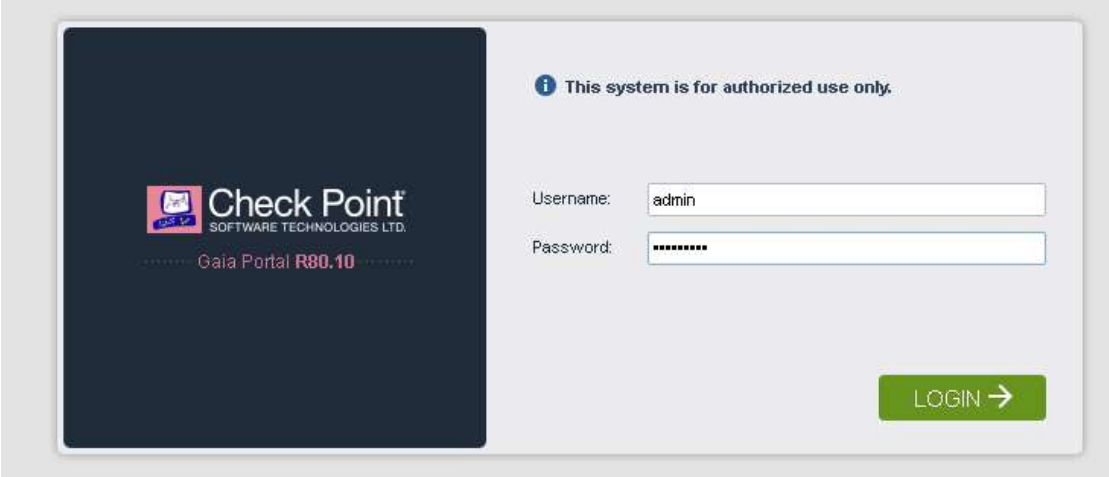
Abra un navegador web (Internet Edge" y navegue hasta la URL " https://10.0.0.201 ")



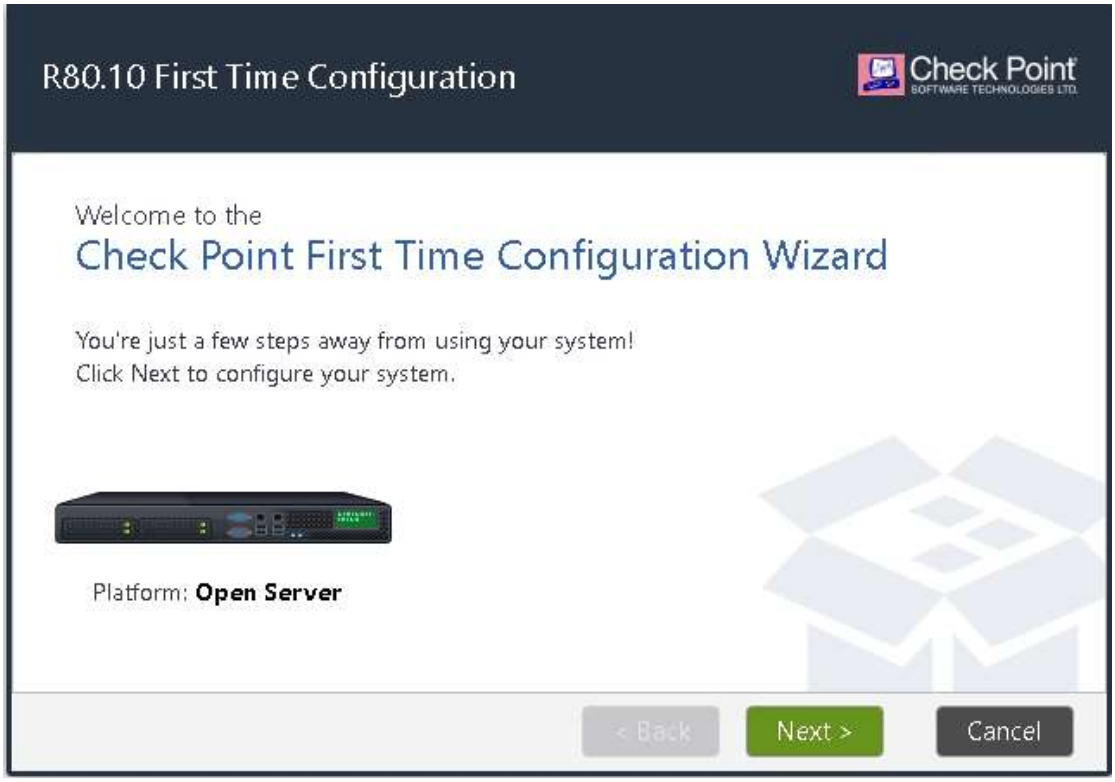
Haga clic en la opción "Avanzado" y haga clic en "continuar a 10.0.0.201"



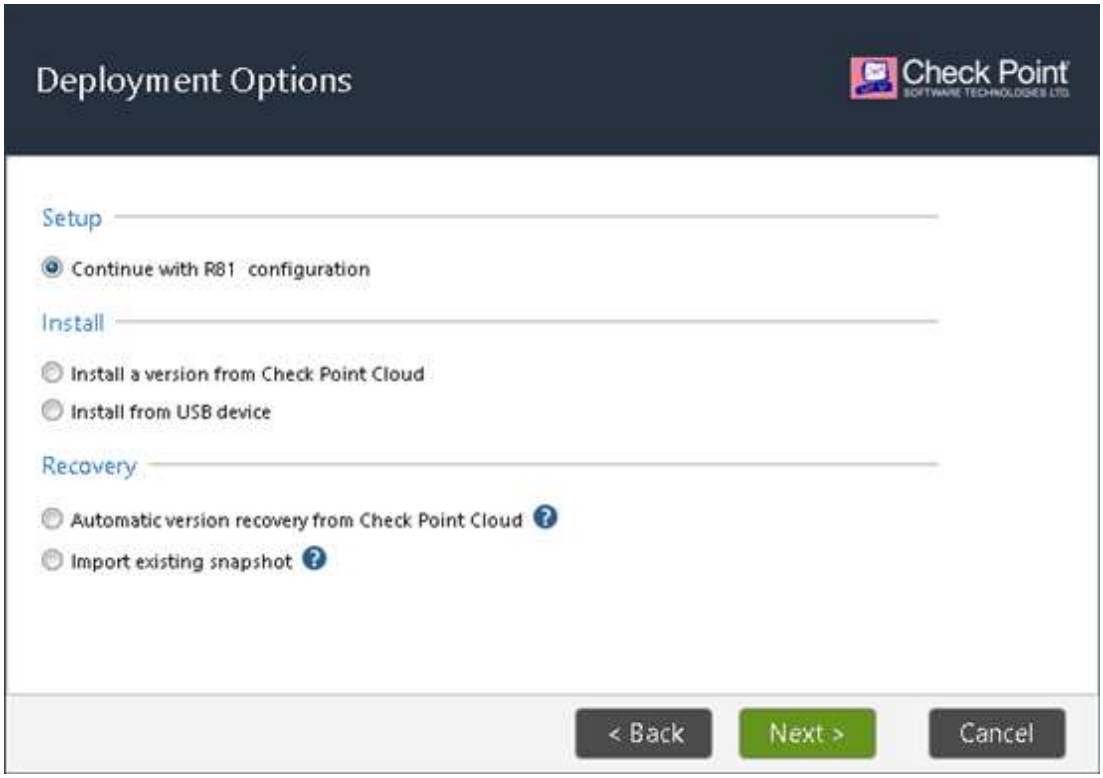
En la página siguiente, inicie sesión con las credenciales de admin / admin@123 que usamos durante la instalación y presione Iniciar sesión



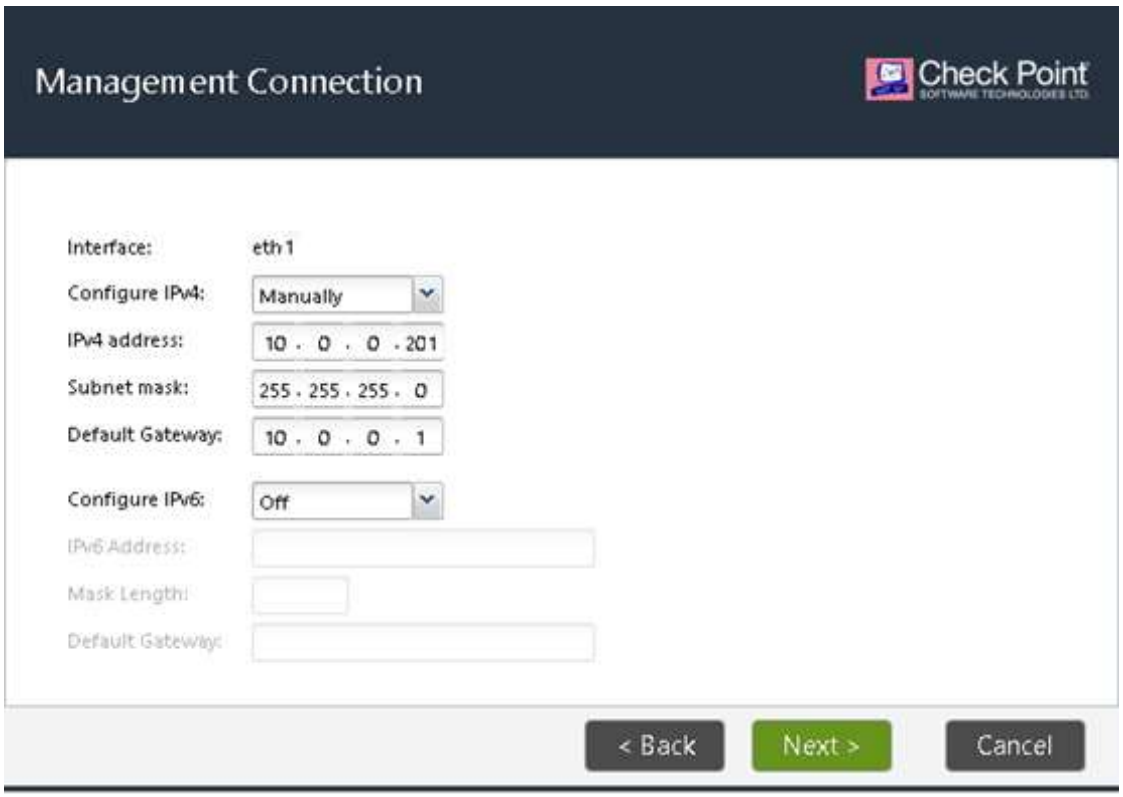
El asistente de configuración por primera vez se inicia como se muestra: haga clic en Siguiente



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



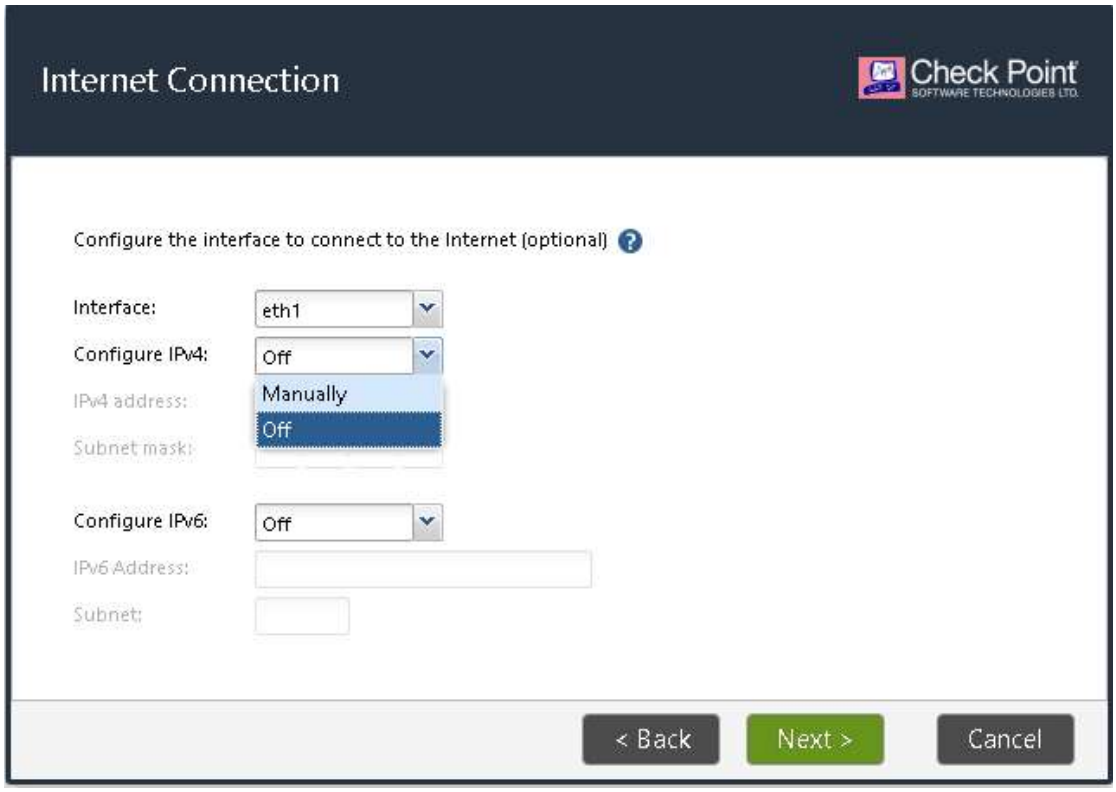
La siguiente pantalla muestra la dirección IP en eth1, la misma que configuramos durante la instalación del sistema operativo Gaia. Haga clic en Siguiente



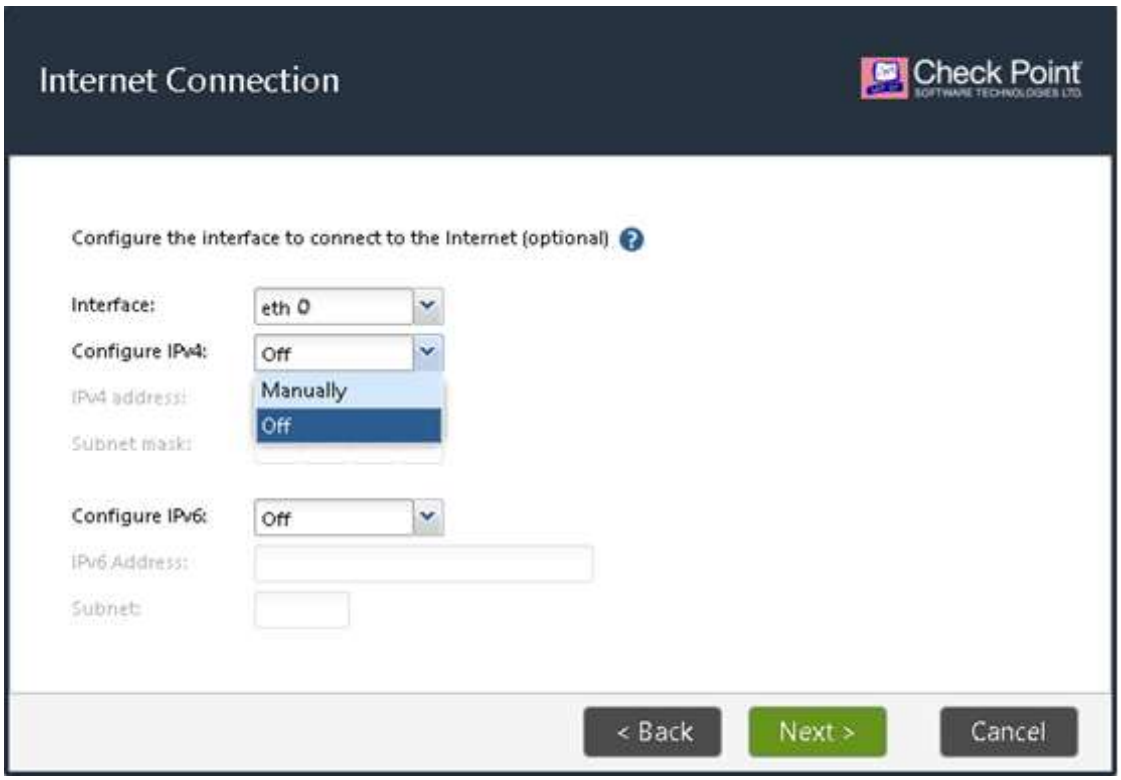
En la siguiente pantalla, configuraremos la dirección IP en la interfaz eth0 del CheckPoint FW -CP-standalone-R81

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

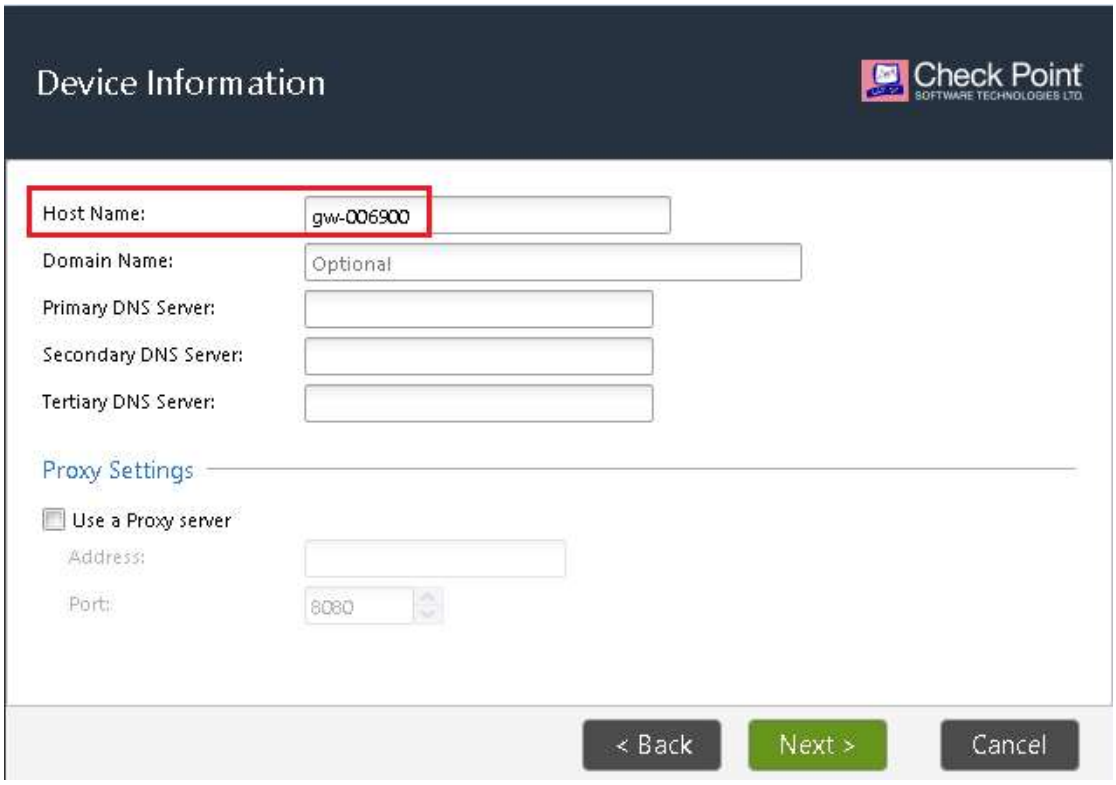
Seleccione la opción Manual como se muestra



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

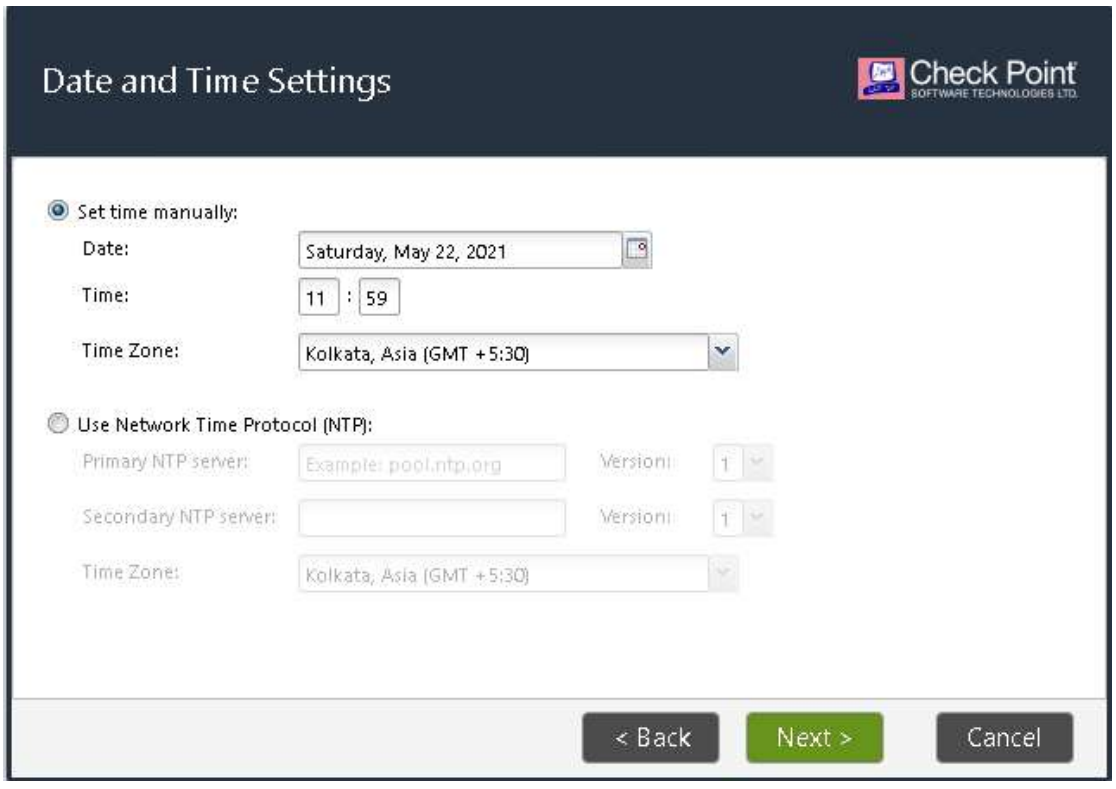


Cambie el nombre de host a "CP-standalone-R81" en la siguiente pantalla

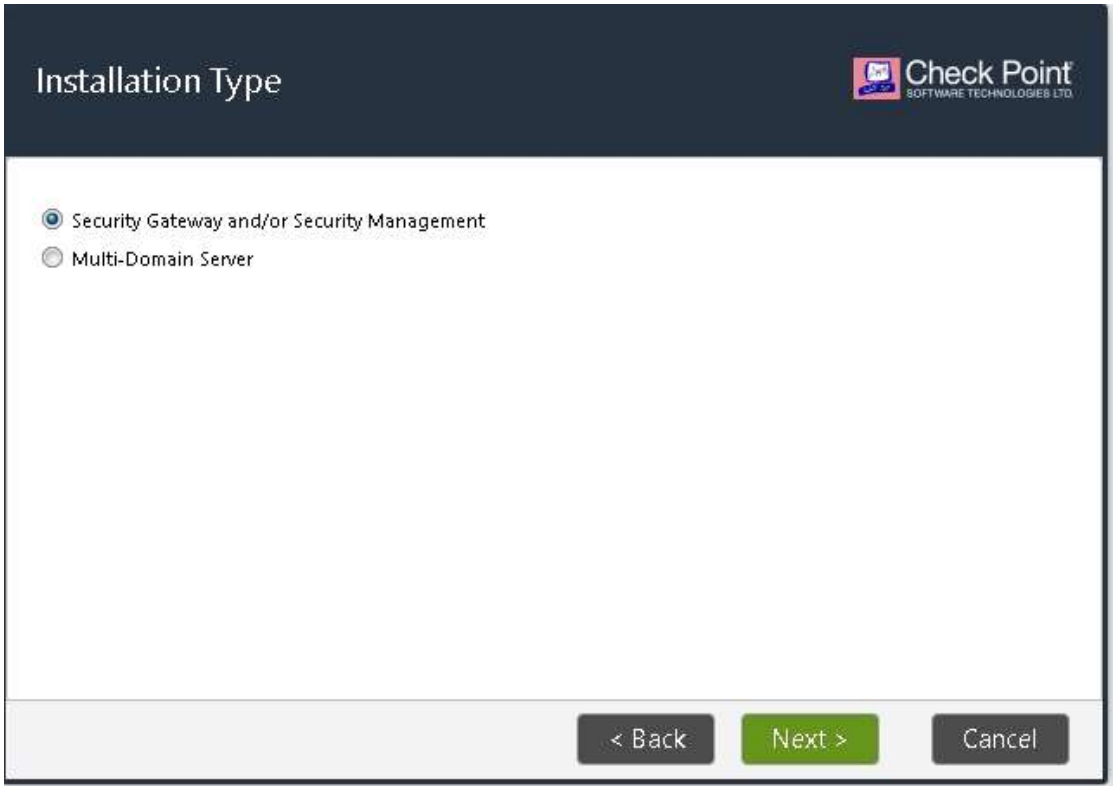


Haga clic en Siguiente

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

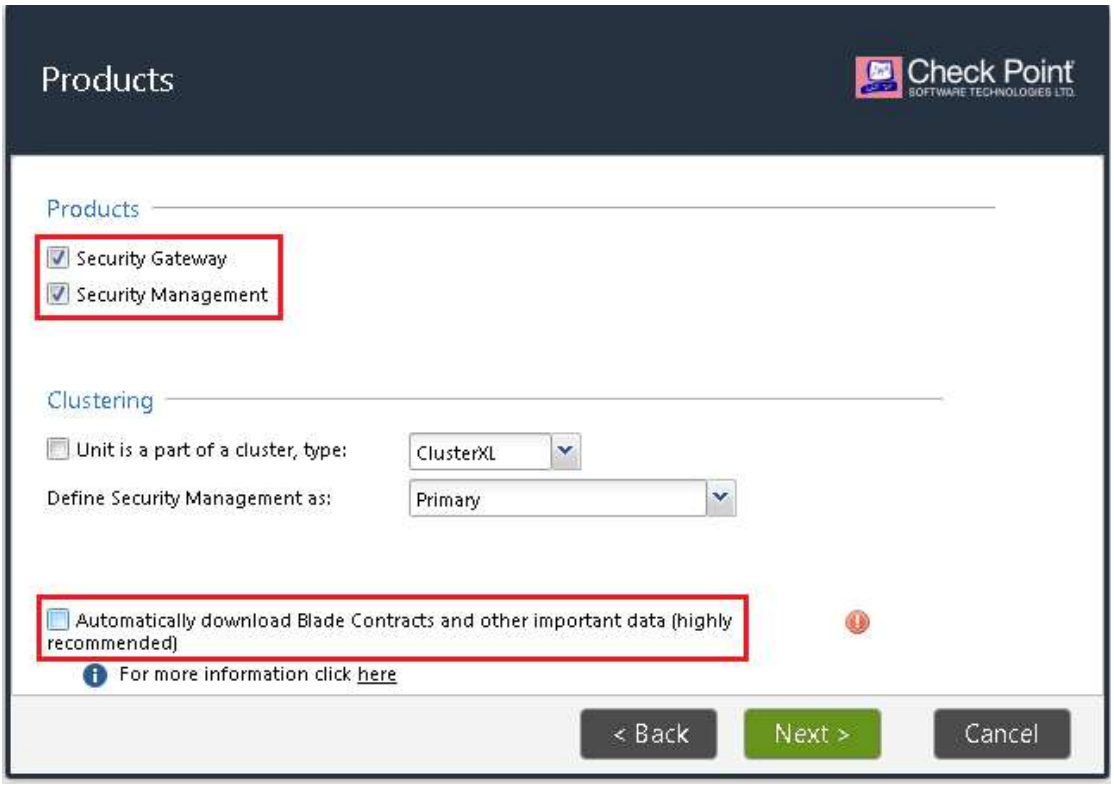


Seleccione la Opción de "Puerta de enlace de seguridad y/o Gestión de seguridad y haga clic en Siguiente

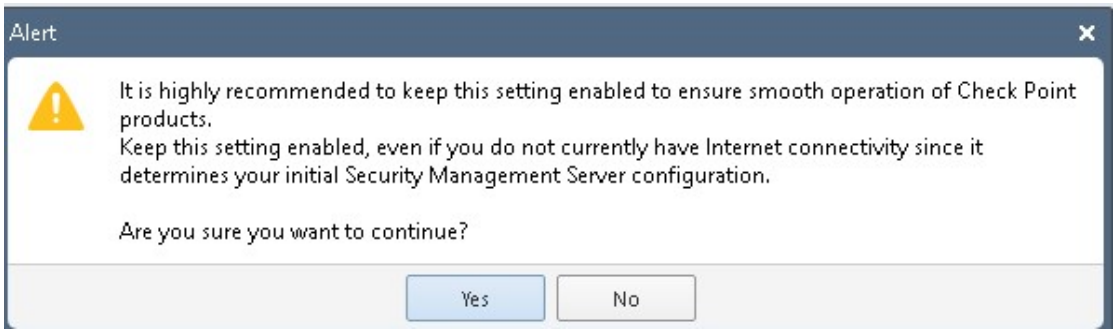

Installation Type
Check Point
SOFTWARE TECHNOLOGIES LTD.
Security Gateway and/or Security Management
Multi-Domain Server
< Back
Next >
Cancel

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

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



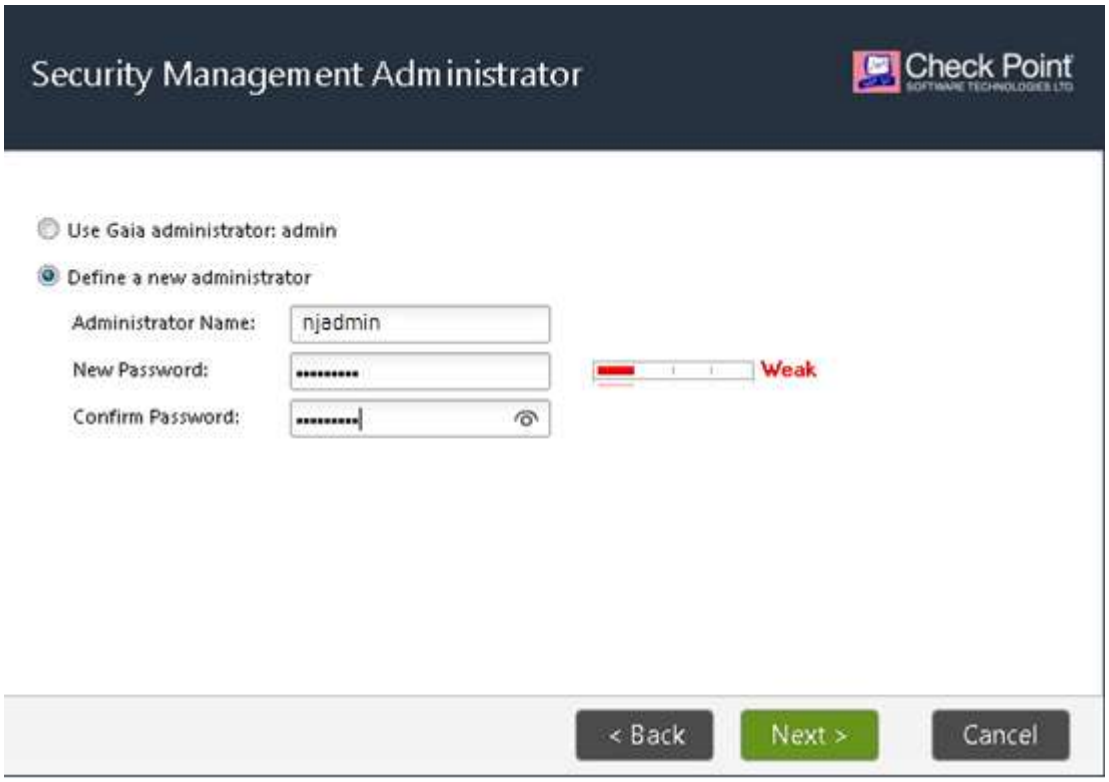
Seleccione Sí en la página de advertencia para continuar



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 " njadmin " y la contraseña como " njadmin "

Haga clic en Siguiente para continuar

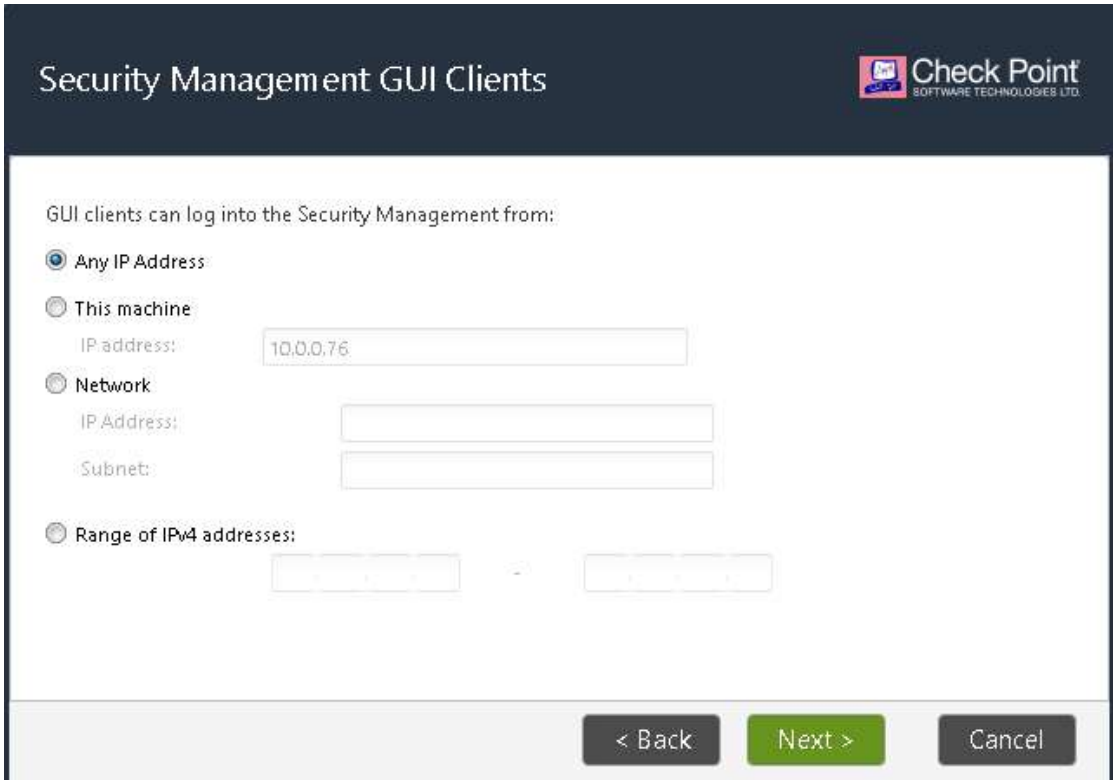


En la siguiente pantalla configuraremos los clientes GUI. Los clientes GUI son direcciones IP que tienen SmartConsole instalado para la gestión de seguridad.

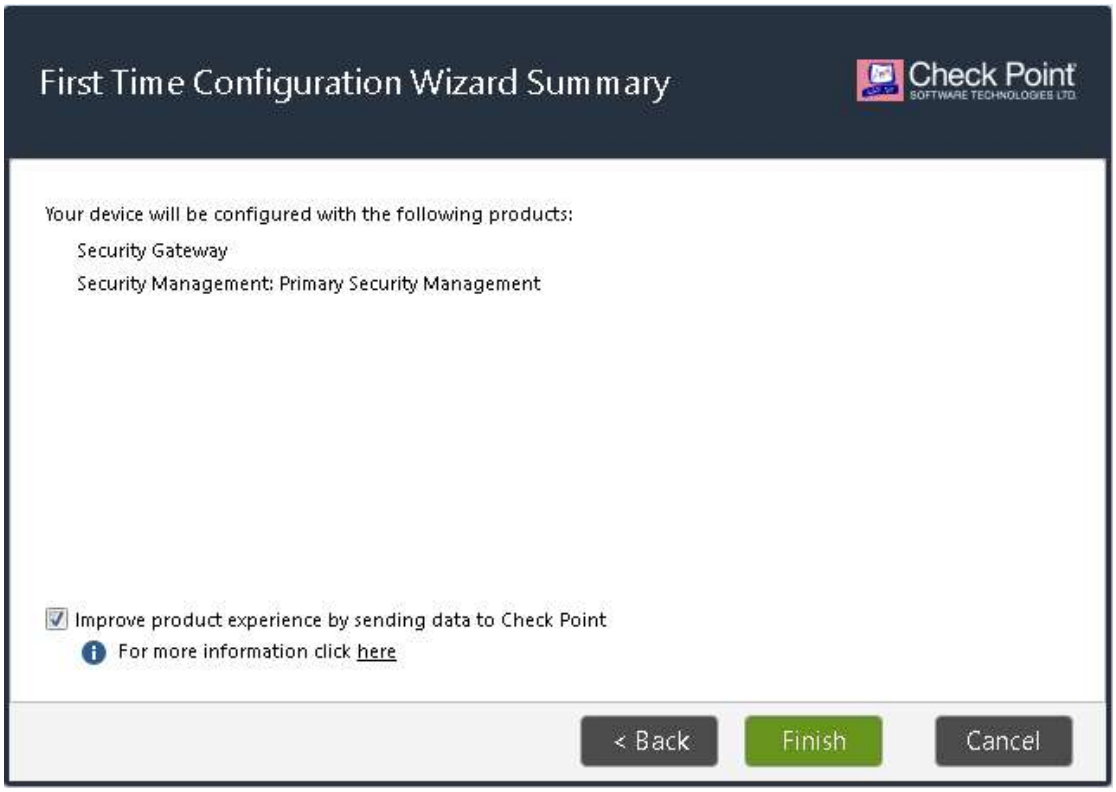
La dirección IP del cliente debe estar permitida en el servidor de administración para que pueda acceder y administrar la configuración.

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

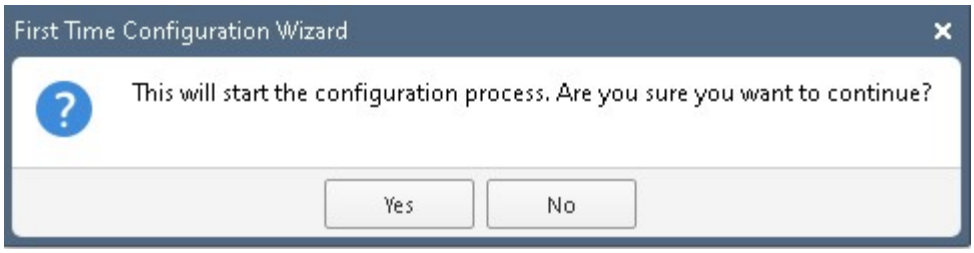
Haga clic en Siguiente para continuar



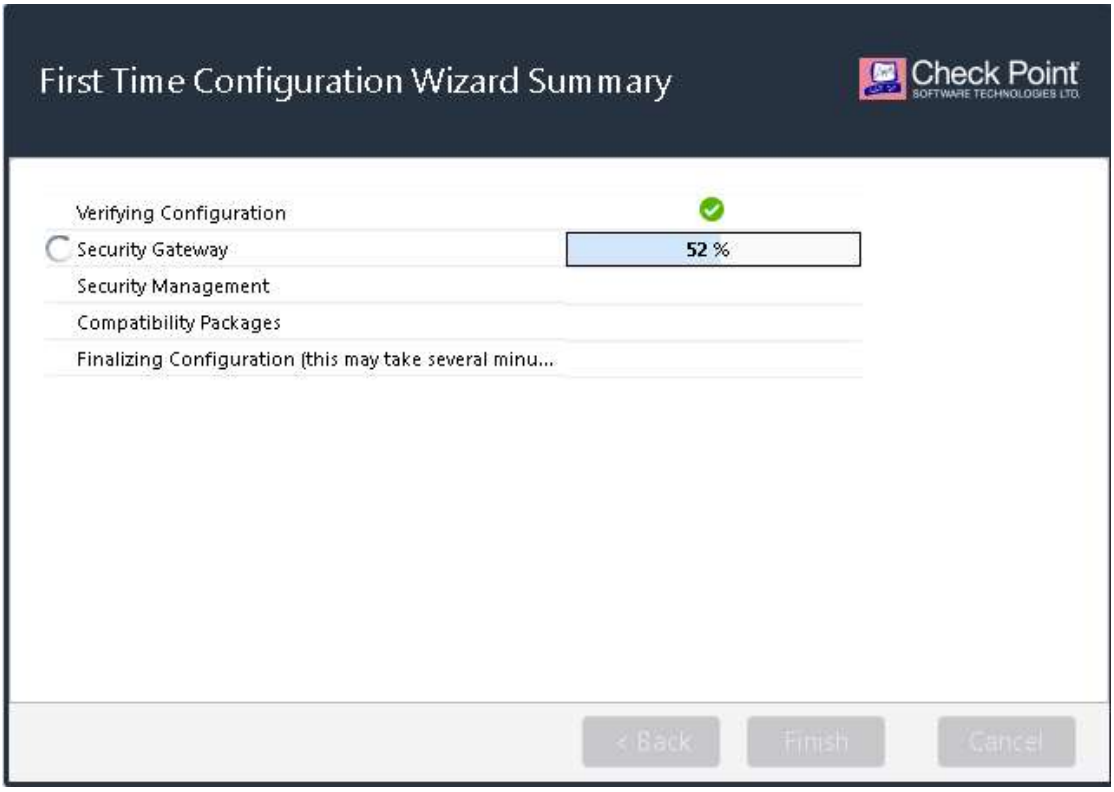
La siguiente pantalla muestra el resumen de los Productos que ha seleccionado para la instalación. Haga clic en Siguiente para continuar.



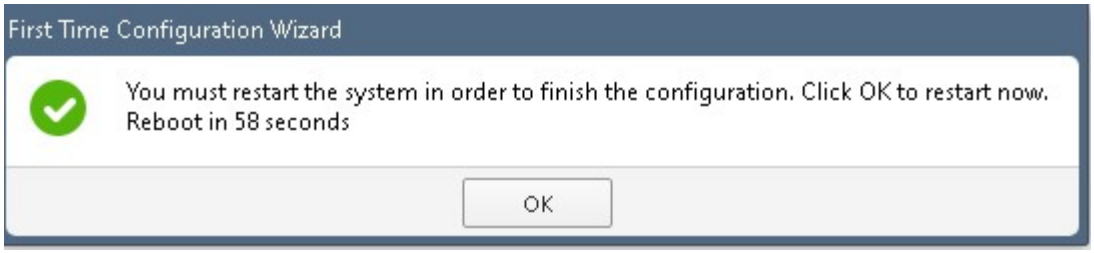
Se le pedirá confirmación como se muestra: haga clic en Sí para comenzar la instalación



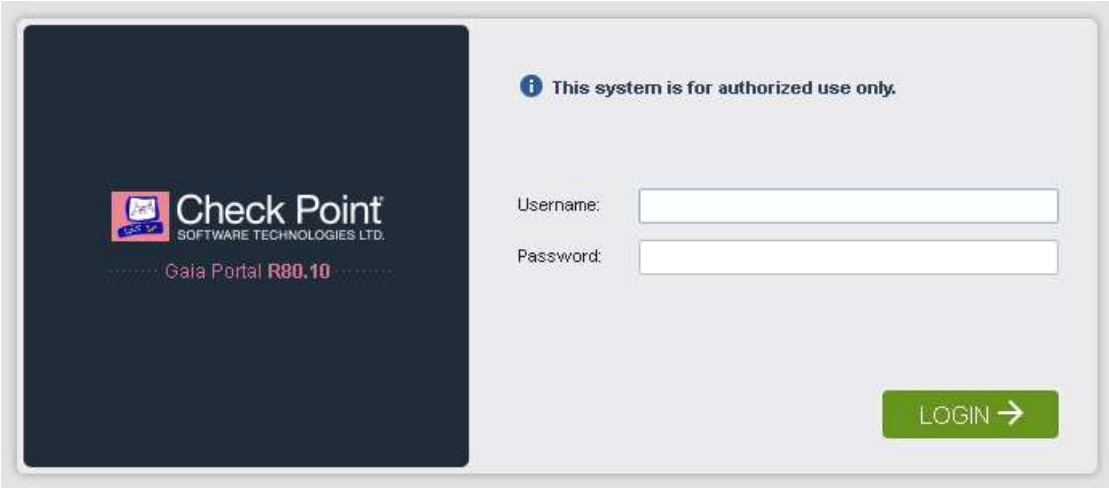
El proceso de instalación se inicia y el progreso de cada componente se muestra como se muestra



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.



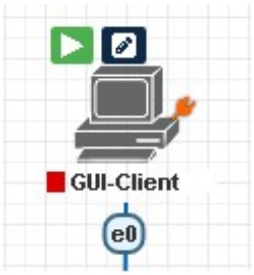
Esto completa la implementación independiente de la configuración de CheckPoint Standalone R81 con Firewall y Management Server instalados en el mismo iso .

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

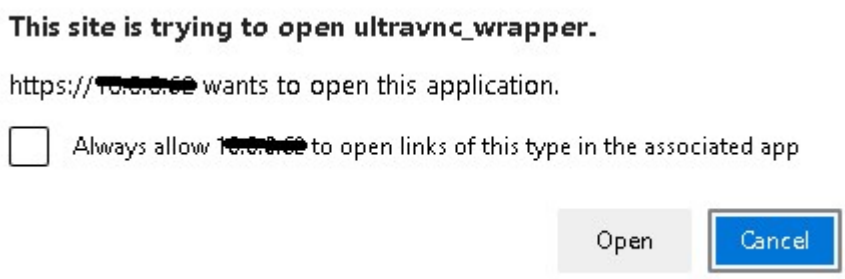
Ahora procederemos con la instalación de SmartConsole en la máquina cliente GUI.

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

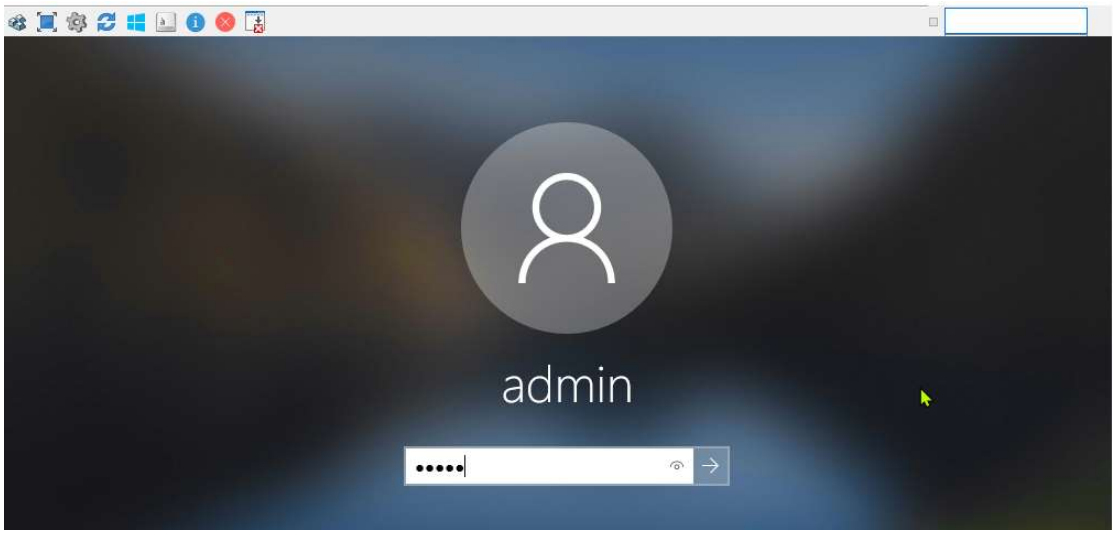


Una vez que se inicia el nodo: haga doble clic para conectarse a la consola VNC

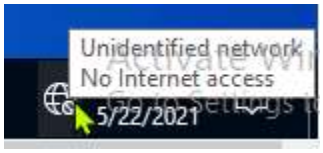
Haga clic en Abrir para conectarse a la consola VNC



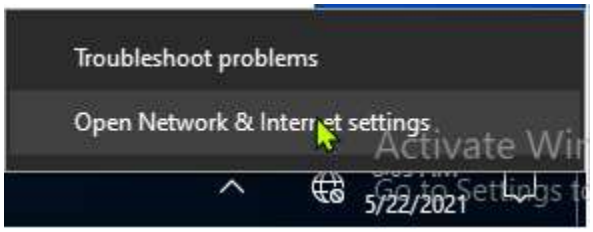
Use admin/admin para iniciar sesión en el nodo de cliente de la GUI de Windows



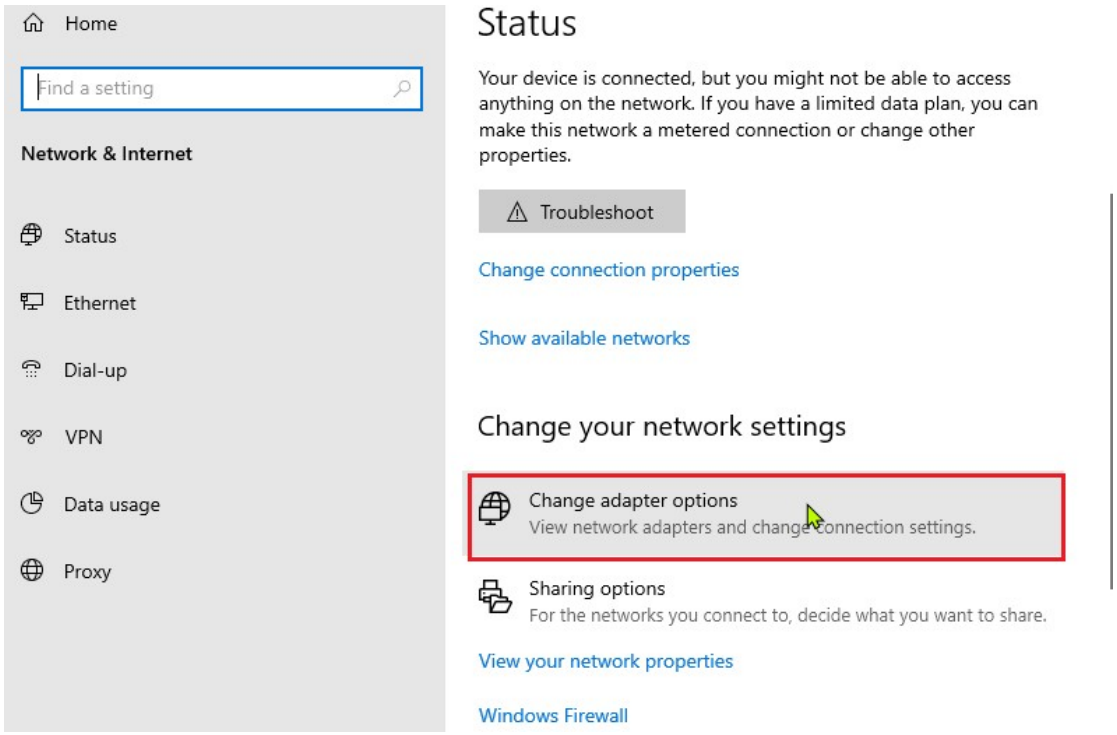
Haga clic en Configuración de red para configurar la dirección IP en el nodo GUI-Client



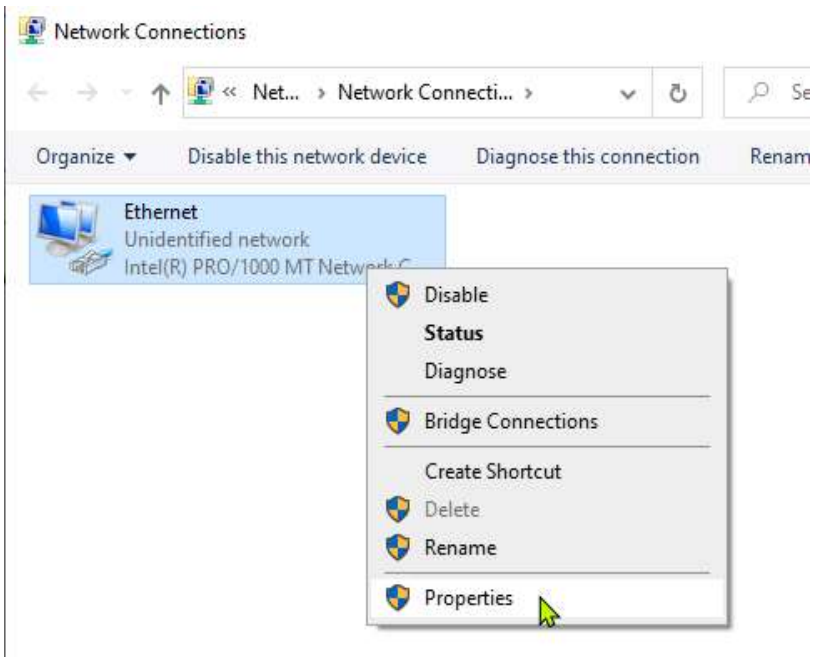
Haga clic en Abrir configuración de red e Internet



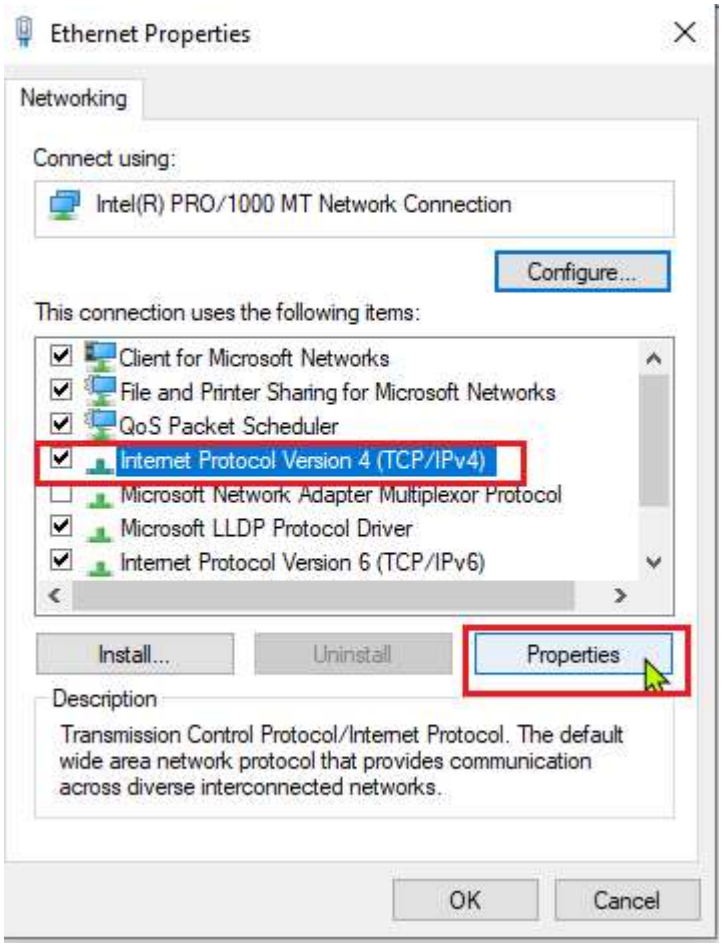
Haga clic en las opciones de Cambiar Adaptado



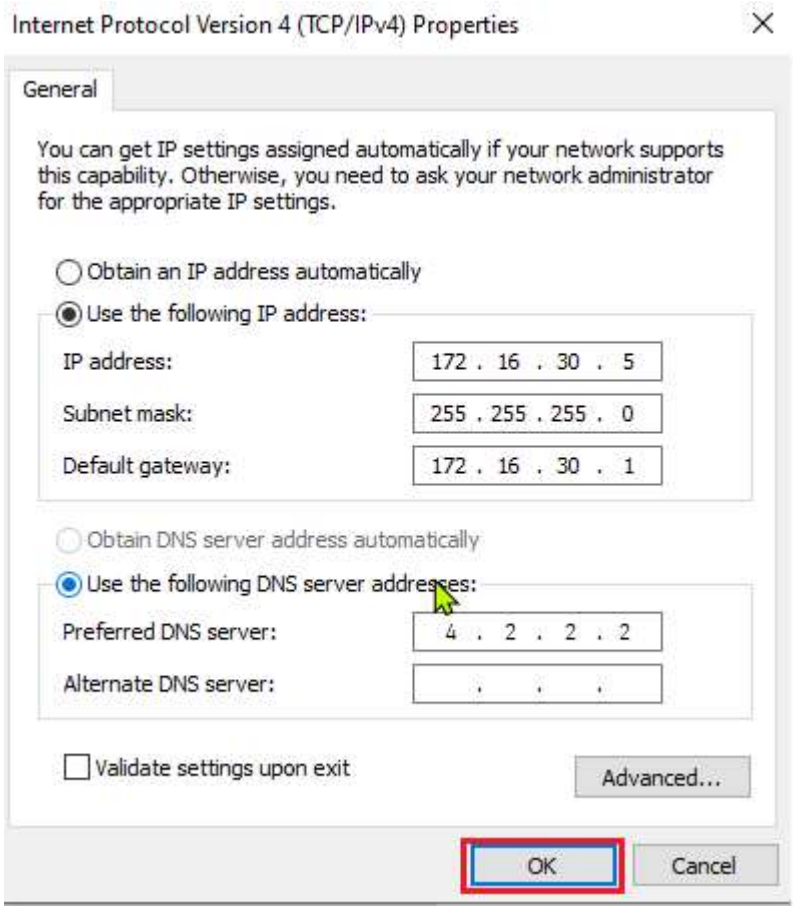
Haga clic derecho en la interfaz de red y haga clic en Propiedades



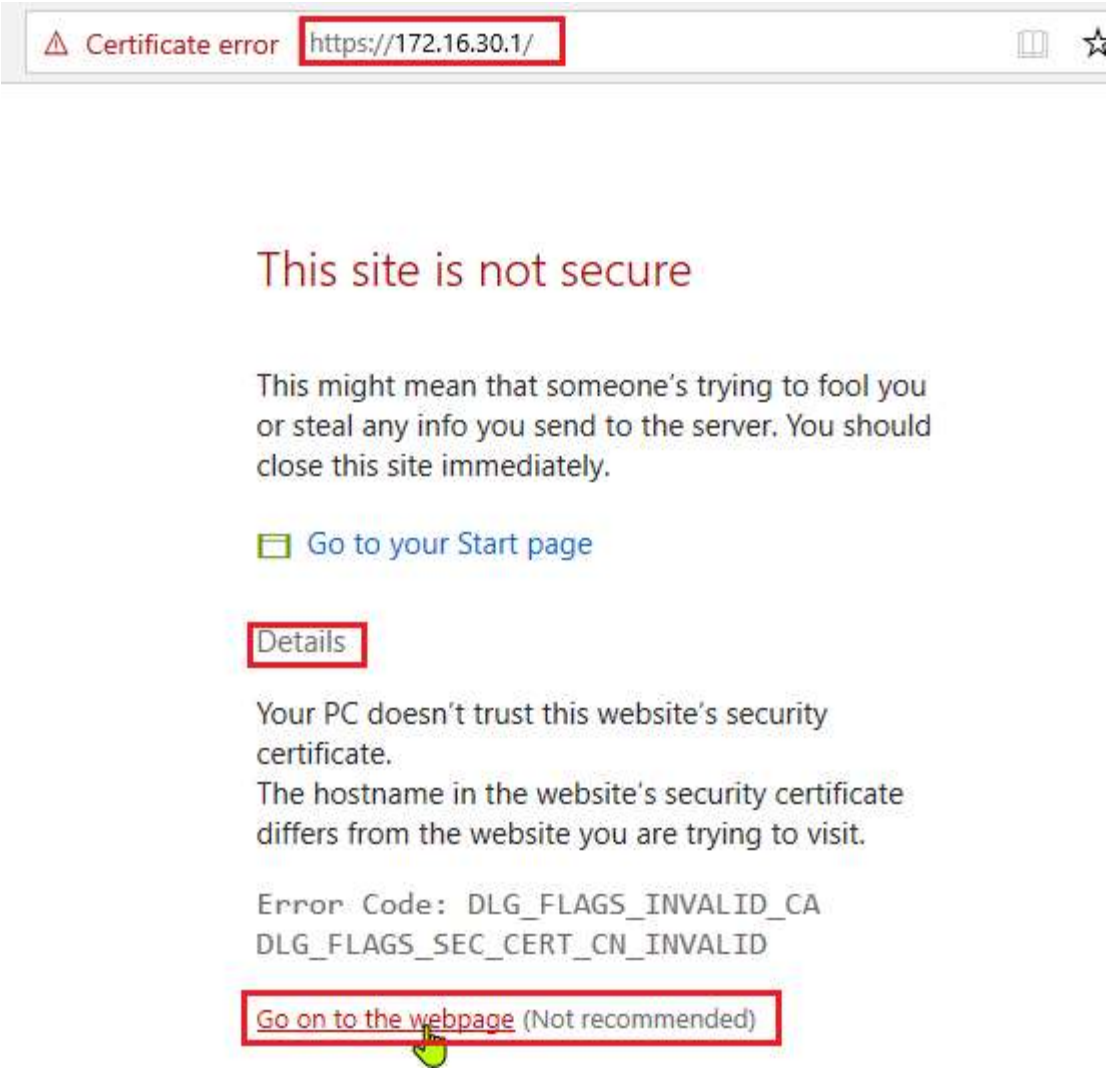
Haga clic en la opción de configuración de IPv4 y haga clic en Propiedades



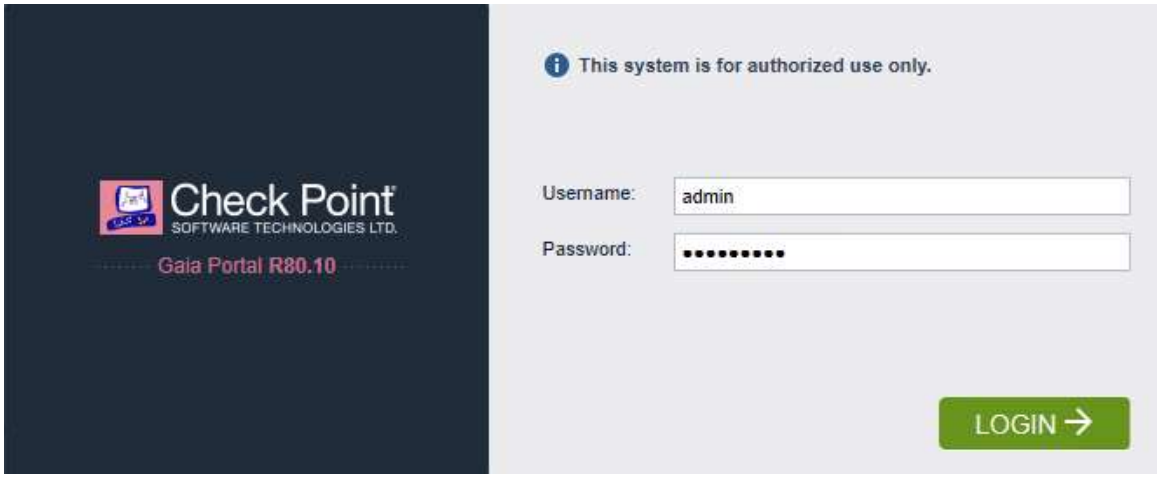
Configure la dirección IP: 172.16.30.5, máscara de subred de 255.255.255.0 y puerta de enlace predeterminada de 172.16.30.1 y cierre la pestaña Redes y configure el servidor DNS de 4.2.2.2



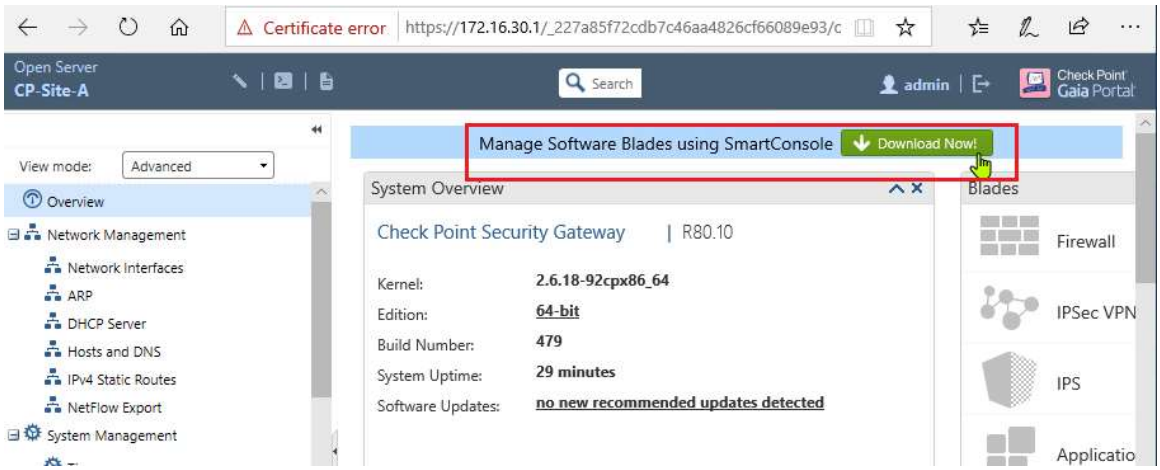
Con el navegador Edge, conéctese a https://172.16.30.1 para descargar la configuración de SmartConsole . Tenga en cuenta que estamos utilizando la dirección IP eth0 del nodo de firewall para conectarnos a la interfaz de usuario web desde la máquina del cliente GUI



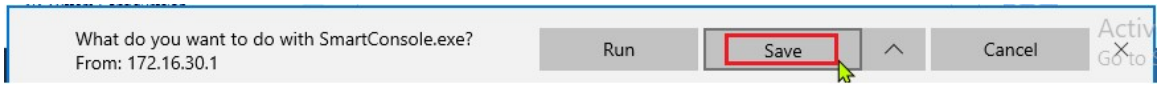
Inicie sesión con las credenciales admin/admin@123



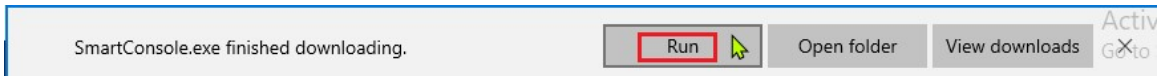
Haga clic en el botón para descargar la configuración de SmartConsole



Haga clic en la opción Guardar

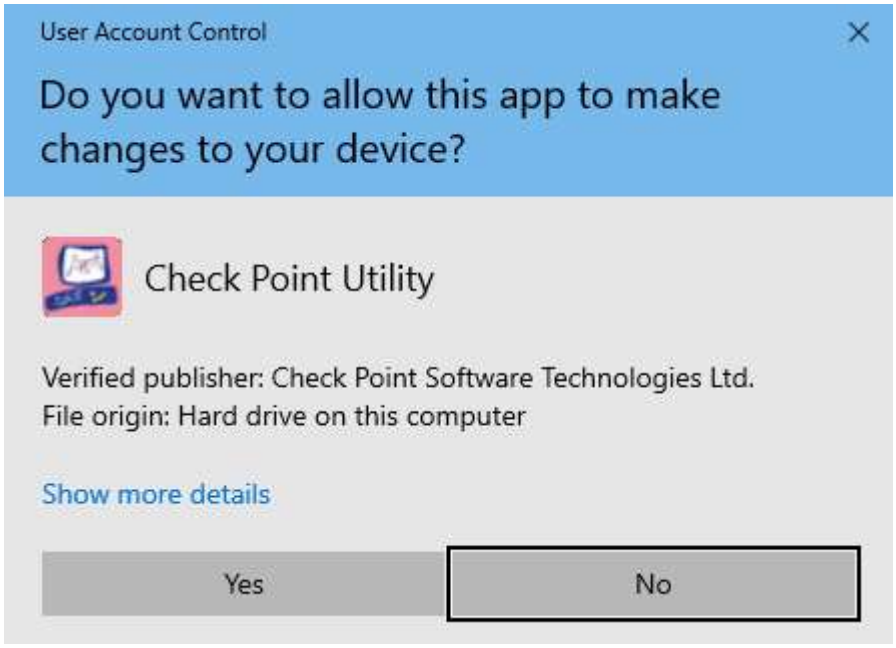


Haga clic en Ejecutar para iniciar la configuración de Smart Console

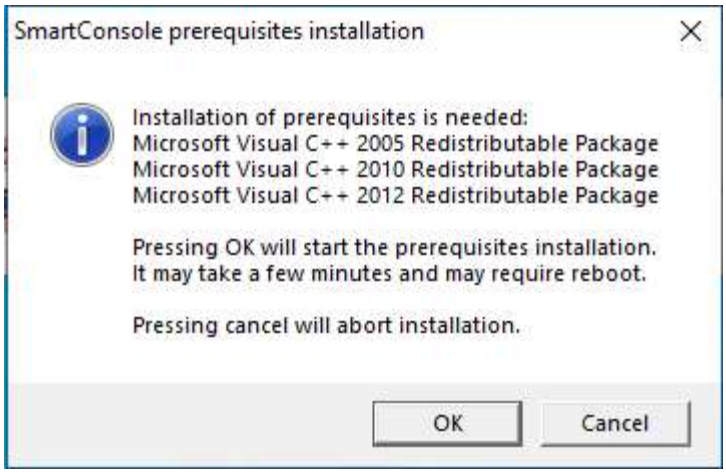


La instalación comenzará

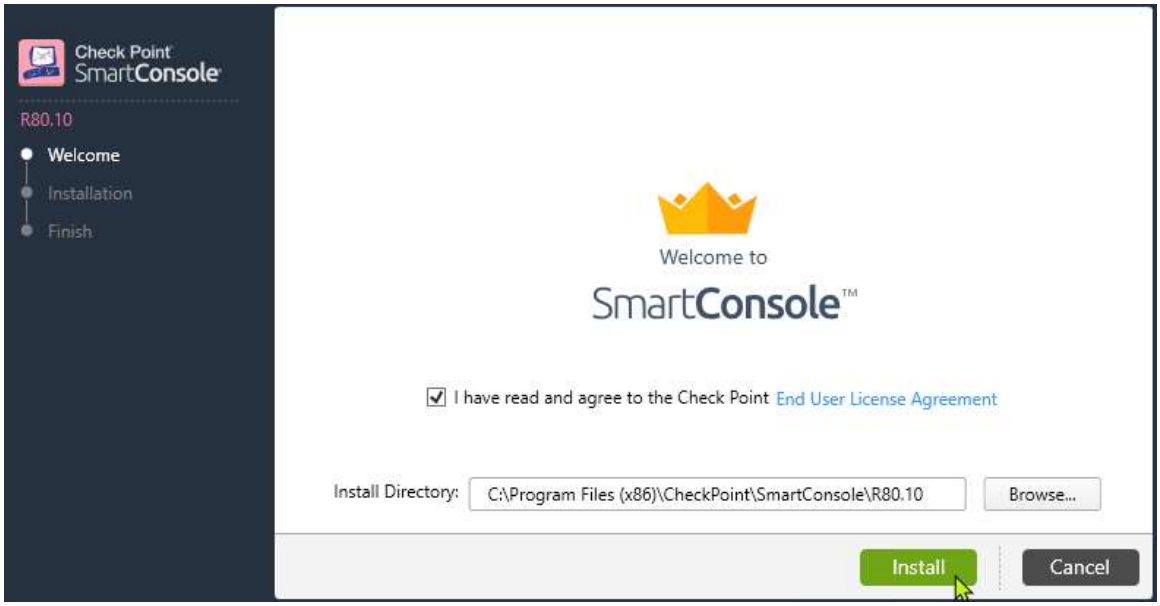
Haga clic en Sí para el cuadro de diálogo Control de cuentas de usuario si se le solicita



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

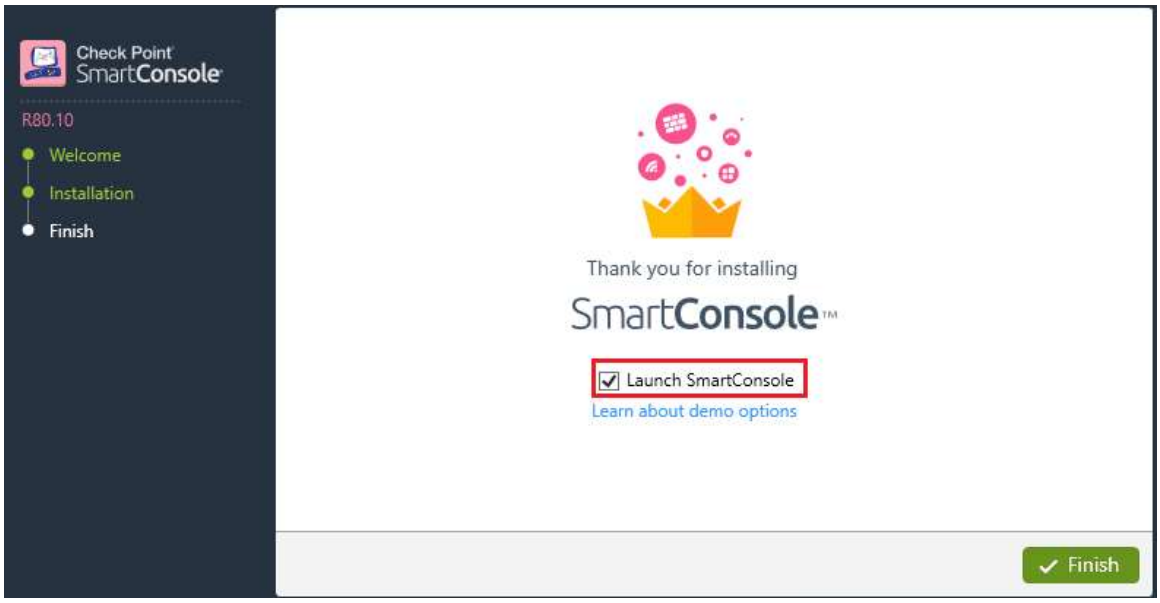


Haga clic en el Acuerdo de licencia de usuario final y haga clic en Instalar



de SmartConsole continuará.

Haga clic en Finalizar para iniciar la SmartConsole

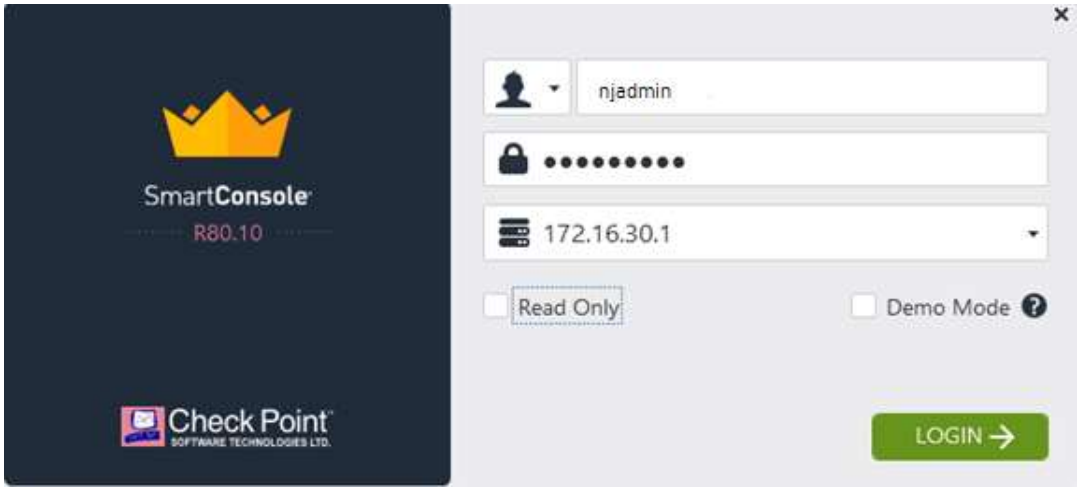


En este punto se completa la instalación de SmartConsole

Iniciar sesión en SmartConsole

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

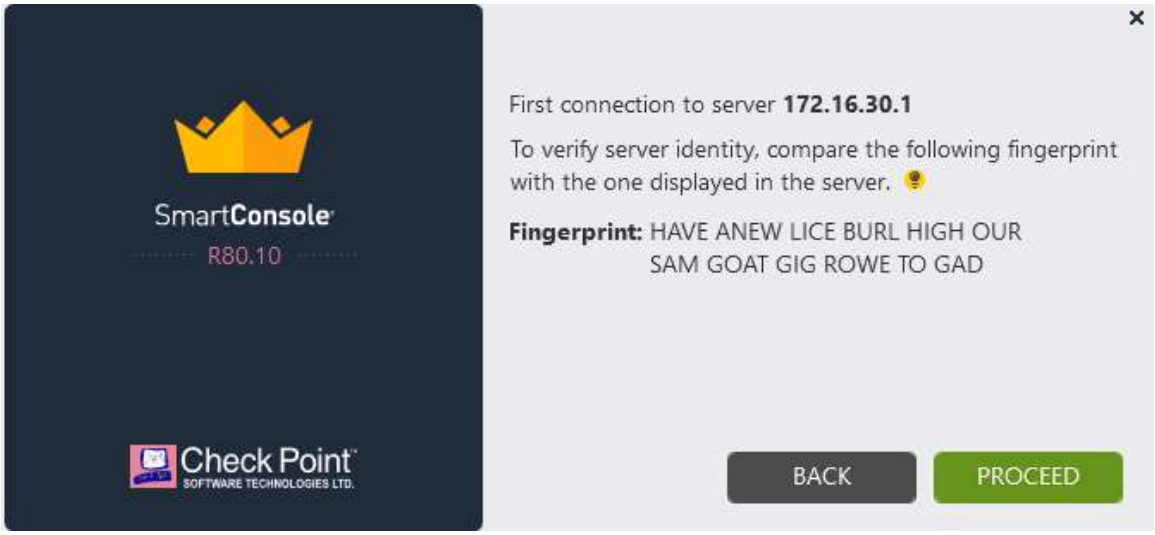
La SmartConsole solicitará 3 cosas como se muestra: nombre de usuario, contraseña e IP del servidor



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

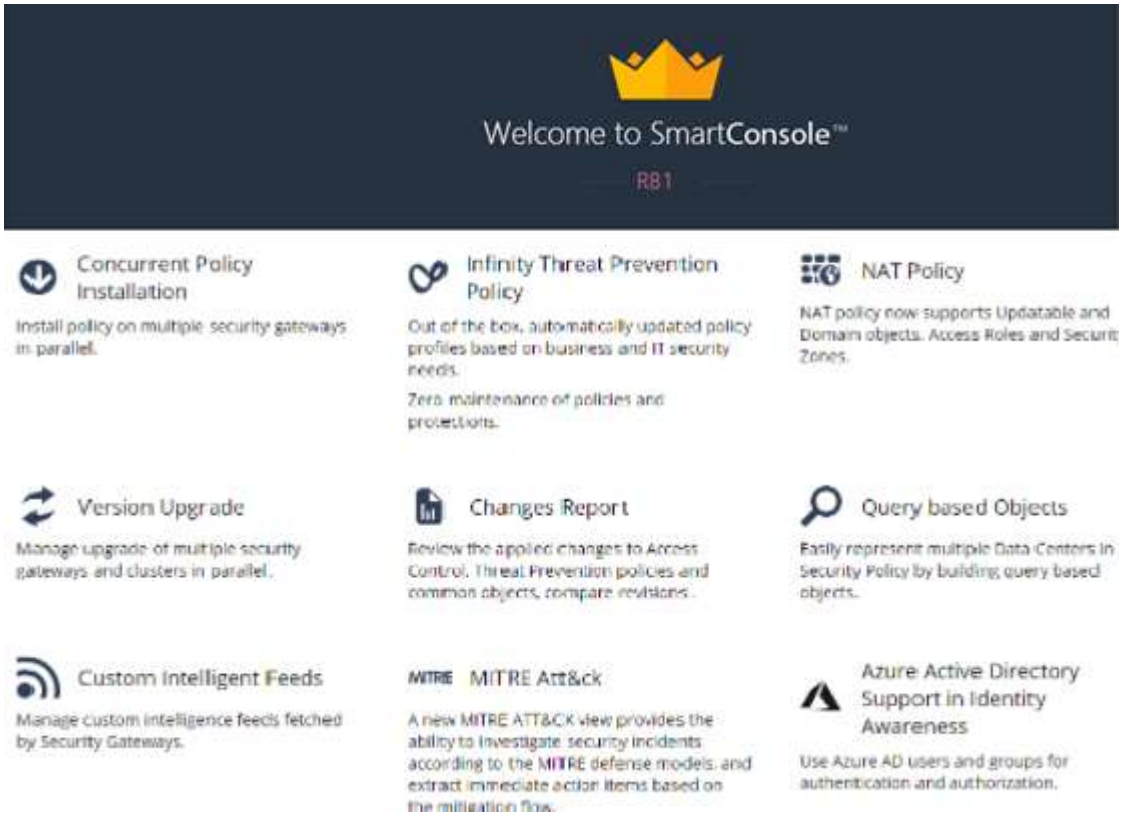
Haga clic en Iniciar sesión para continuar

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



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



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