CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Luis Eduar Cuesta Tautiva Cargo: Coordinador Servicios Tecnológicos	Nombre: Jaroslav Marlen Lopez Cargo: Jefe Oficina de Tecnología e Informática	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2023-10-31

1 OBJETIVO

Brindar los lineamientos necesarios para la instalación y configuración del cliente de VPN a los servidores públicos o contratistas autorizados a través de las actividades descritas en este documento, las cuales serán gestionadas la Mesa de Servicios.

2 DESTINATARIOS

Servidores públicos y contratistas de la Superintendencia de Industria y Comercio SIC.

3 GLOSARIO

CONTRASEÑA: Forma de autenticación que utiliza información secreta para controlar el acceso a algún recurso informático.

VPN: Red Privada Virtual, en inglés: Virtual Private Network (VPN), es una tecnología de red de computadoras que permite crear una extensión segura de la red de área local (LAN) sobre una red pública o no controlada.

4 GENERALIDADES

Para garantizar la disponibilidad de la información, la SIC provee a los servidores públicos y contratistas que realizan sus funciones o cumplen sus obligaciones contractuales, desde fuera de la sede principal de la entidad, de un sistema que permite conectarse a la red principal de la SIC y a los diferentes aplicativos internos de la entidad. Este sistema llamado VPN (Virtual Private Network), protege el acceso a la información que se transfiere entre en equipo externo y la entidad.

5 DESCRIPCION DE ACTIVIDADES

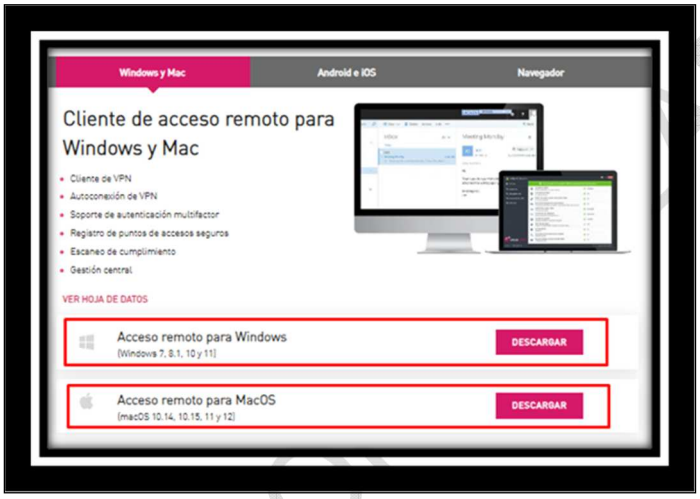
Para realizar la configuración e instalación del cliente de VPN, se debe contar con la debida autorización del jefe directo y entregar el formato de VPN diligenciado y firmado a la Mesa de Servicios de la Oficina de Tecnología e Informática OTI. Para servidores públicos: GS01-F21- Formato de solicitud usuario para VPN - funcionario.

Para contratistas: GS01-F20 Formato usuario para VPN Contratistas SIC. Posterior a esto y una vez confirmarse la autorización de acceso, por parte del Coordinador del grupo de Infraestructura Tecnológica y Seguridad Informática o quien él delegue, la Mesa de Servicios debe realizar las actividades que se presentan a continuación.

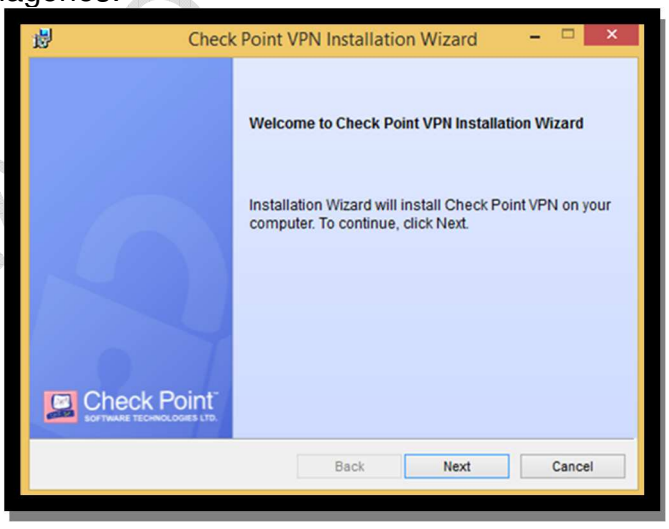
Cliente VPN para Sistemas Windows

1. Descarga el aplicativo VPN: https://support.checkpoint.com/results/download/123662

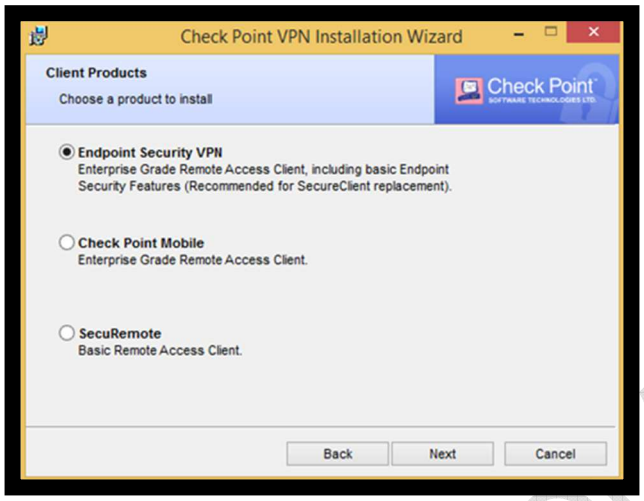
2. Dar en la opción señalada para empezar la descarga del aplicativo:



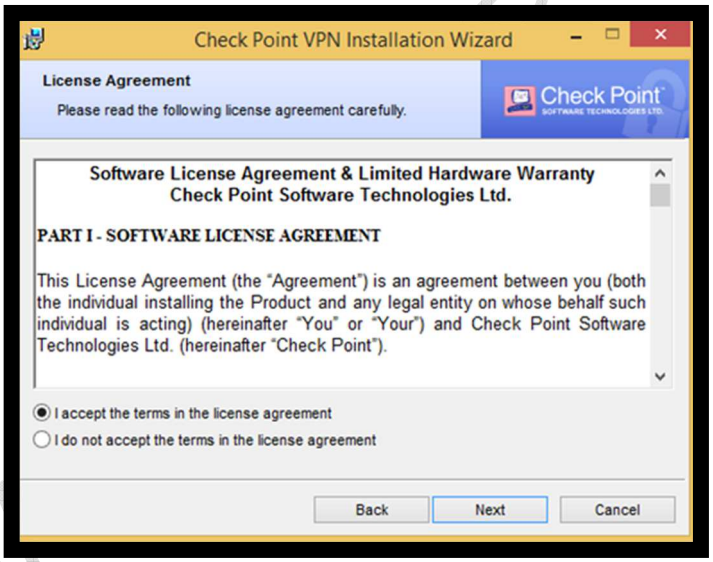
3. Ejecutamos el aplicativo descargado y seguimos los pasos explicados en las siguientes imágenes:



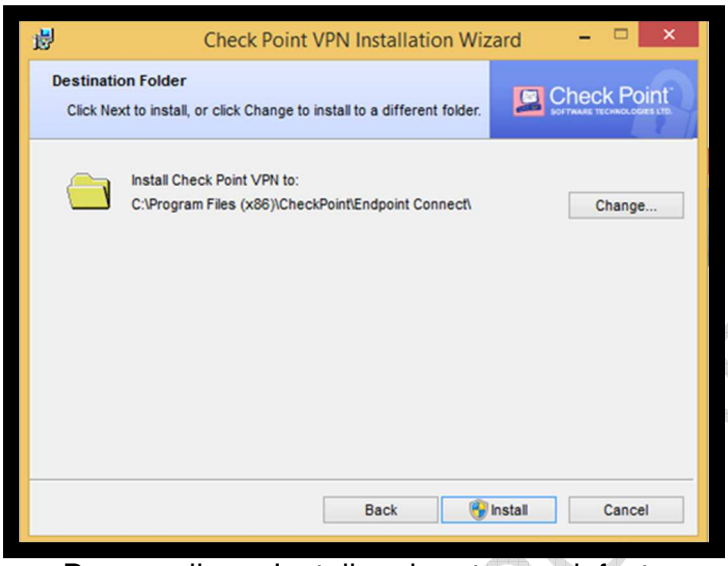
Damos clic en Next



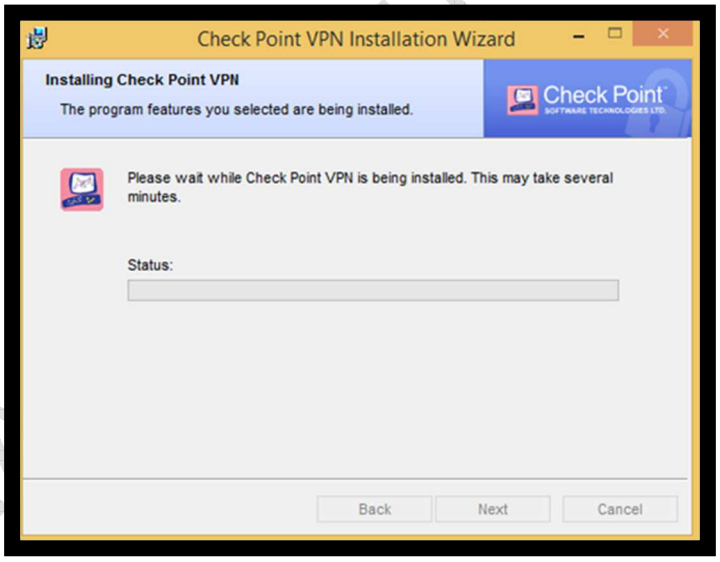
Seleccionamos la opción Endpoint Security VPN y luego en Next



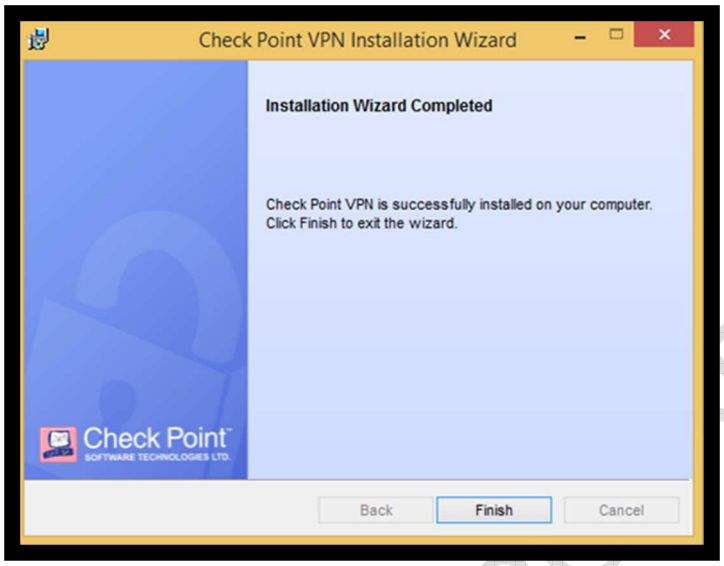
Aceptamos los términos



Damos clic en Install en la ruta por defecto



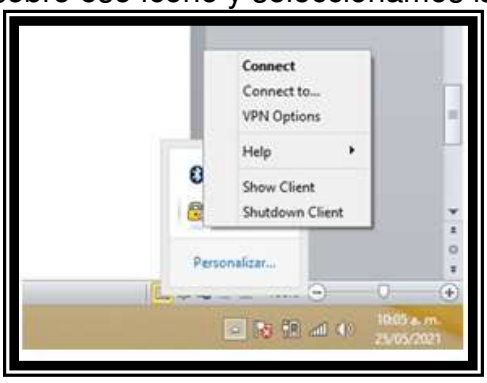
El aplicativo comenzará con la instalación



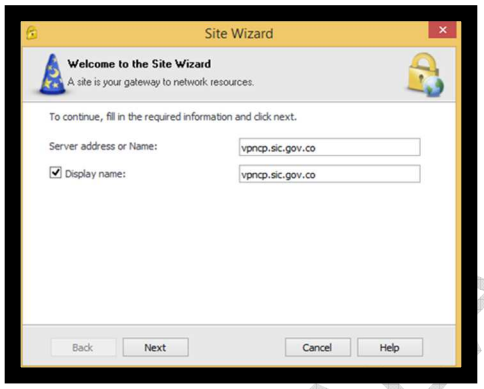
Finalizamos la instalación

4. En la parte inferior derecha de la barra de tareas de Windows aparecerá el ícono de la VPN Check Point:

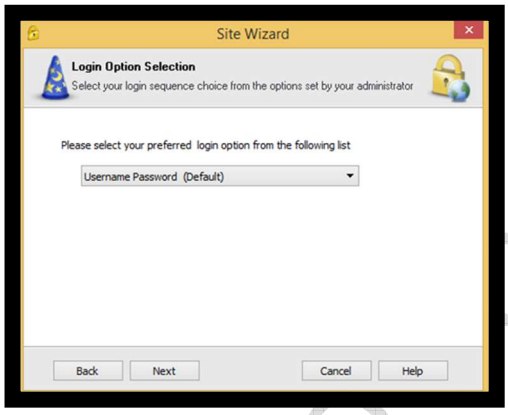
5. Damos clic derecho sobre ese ícono y seleccionamos la opción "Connect":

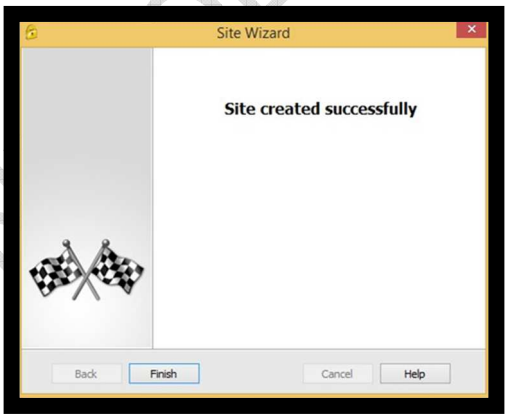


6. Configuramos el sitio o servidor al cual nos conectaremos:



El nombre del servidor VPN se llama vpncp.sic.gov.co o 45.227.5.254





Damos clic en Finish, ya el sitio está creado.

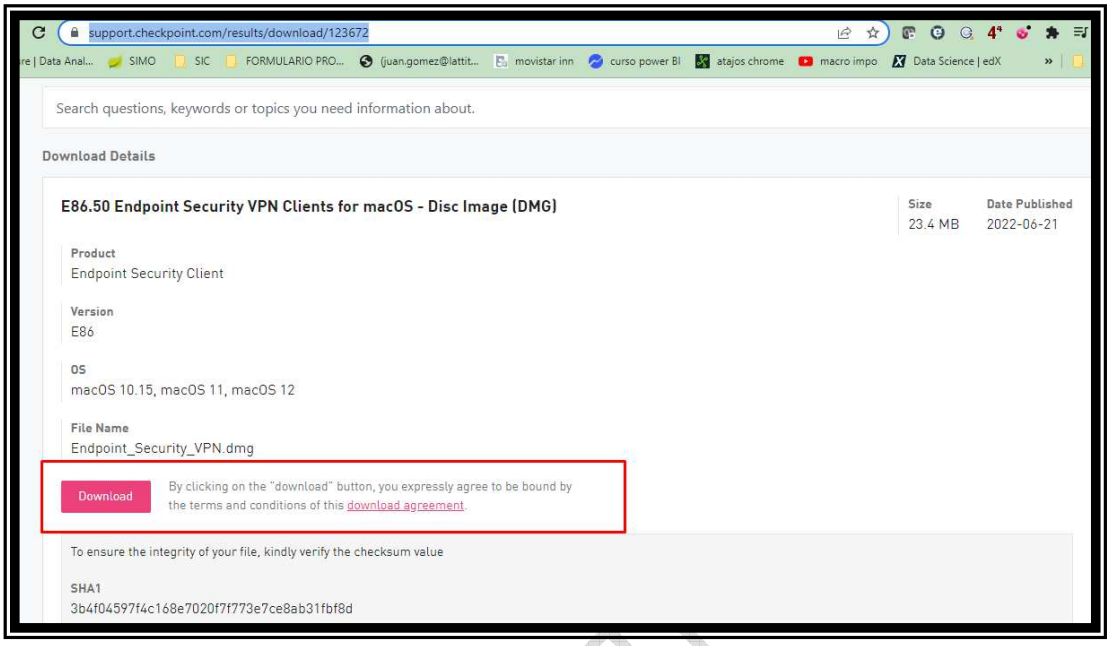
7. Nos conectamos al sitio creado con nuestras credenciales de dominio:

Damos clic en Connect.

Nos aparecerá un mensaje de que ya está conectado.

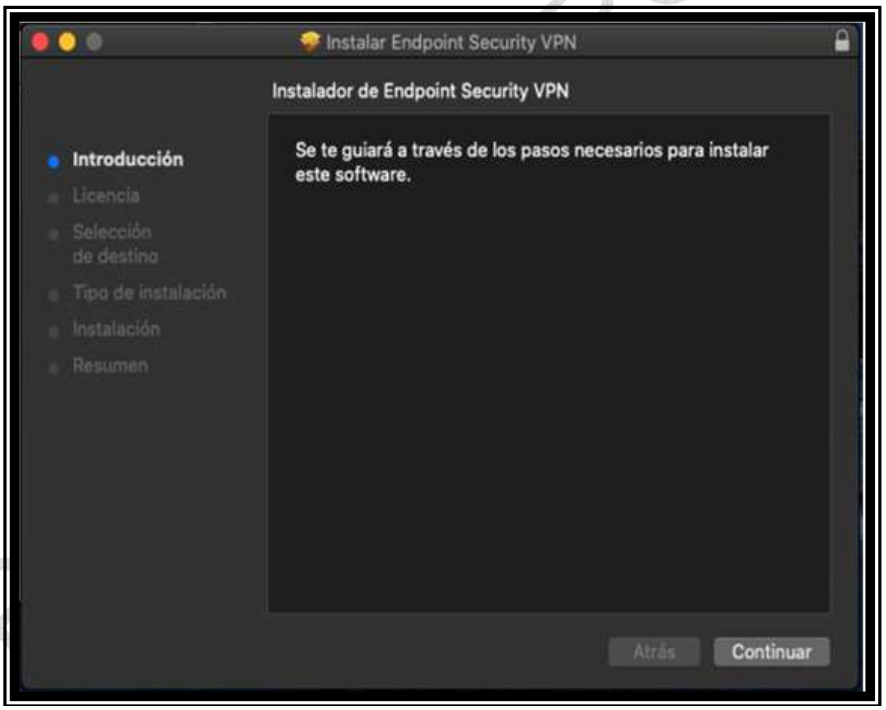
Cliente VPN para Sistemas MacOS

1. Descarga el aplicativo VPN: https://support.checkpoint.com/results/download/123672



Al ejecutarlo saldrá esta ventana. Damos clic en Endpoint_Security_VPN.pkg

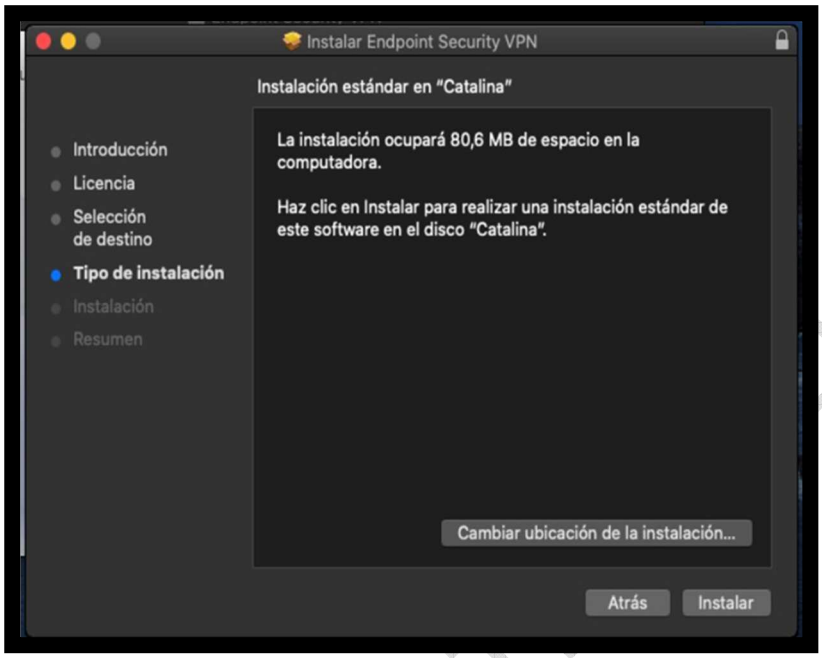
Damos clic en continuar



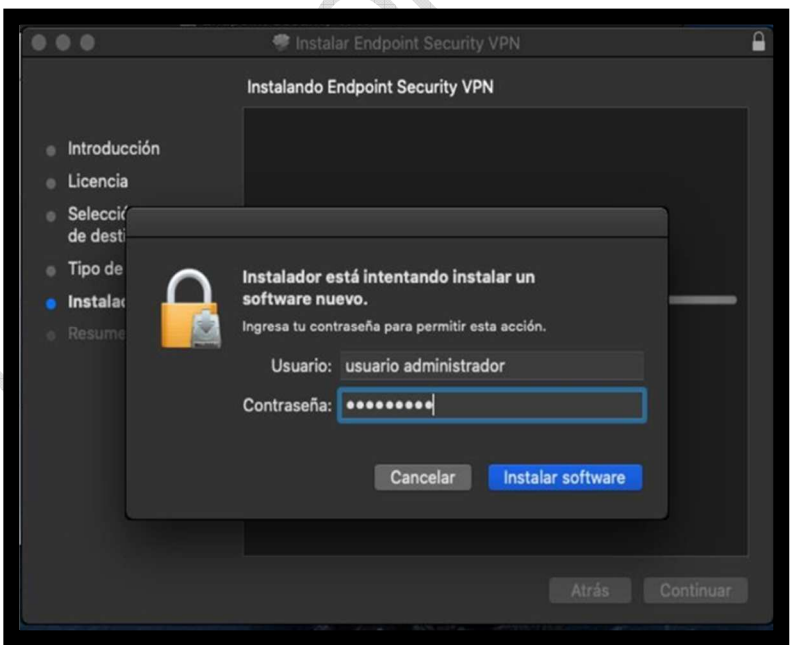
Nuevamente Damos clic en continuar.

Aceptamos el contrato de licencia dando clic en continuar.

Acepto



A continuación, damos clic en Instalar.

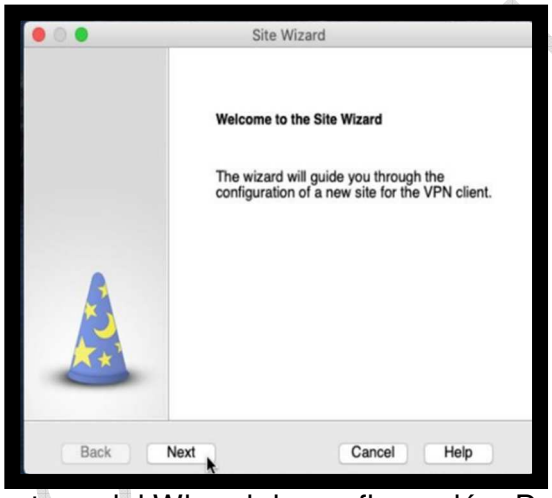


Ahora ingresamos credenciales de usuario administrador para autorizar la instalación.

Para desbloquear el funcionamiento de la aplicación damos clic en "abrir el panel de preferencias de seguridad".

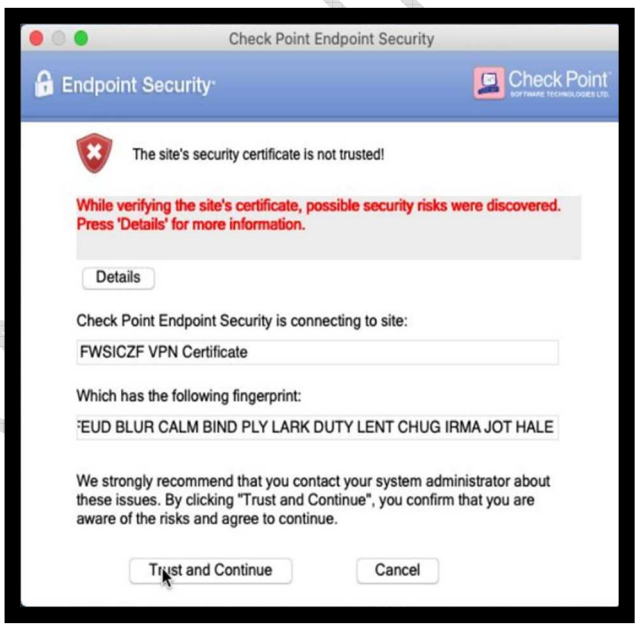
Finalizada la instalación aparecerá arriba el ícono del candado de Check Point. Al darle clic le damos en la opción "Connect to".

Nos preguntara si deseamos configurar un nuevo sitio damos clic en Yes.

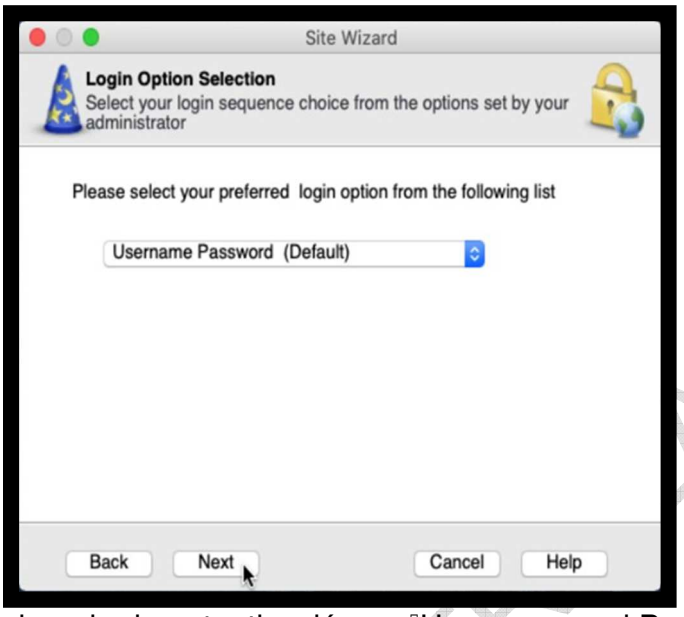


Aparecerá esta ventana del Wizard de configuración. Damos clic en Next.

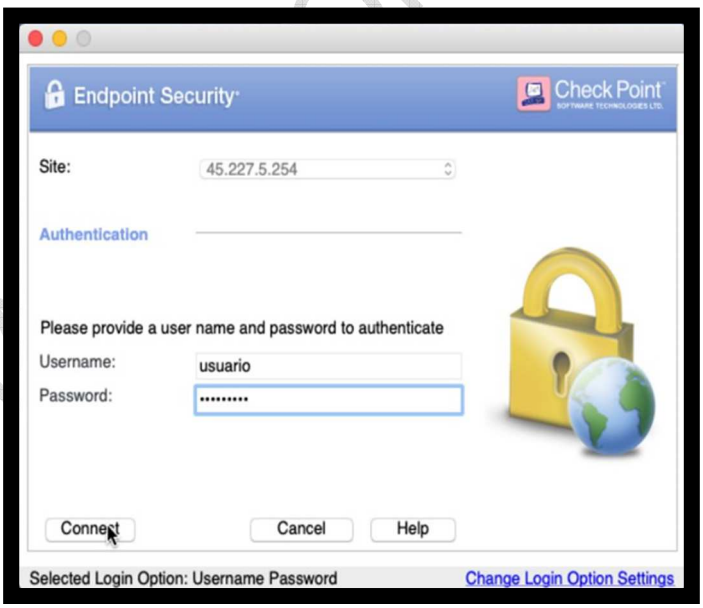
Colocamos la URL de conexión.



Saldrá el mensaje de certificado de confianza. Damos click en Trust and Continue.



Seleccionamos el modo de autenticación en Username and Password, damos clic en Next y luego en Finish.



Al abrir nuevamente la aplicación Aparecerá ya la ventana de autenticación. luego de digitar usuario y contraseña se tiene acceso a la VPN de la SIC.

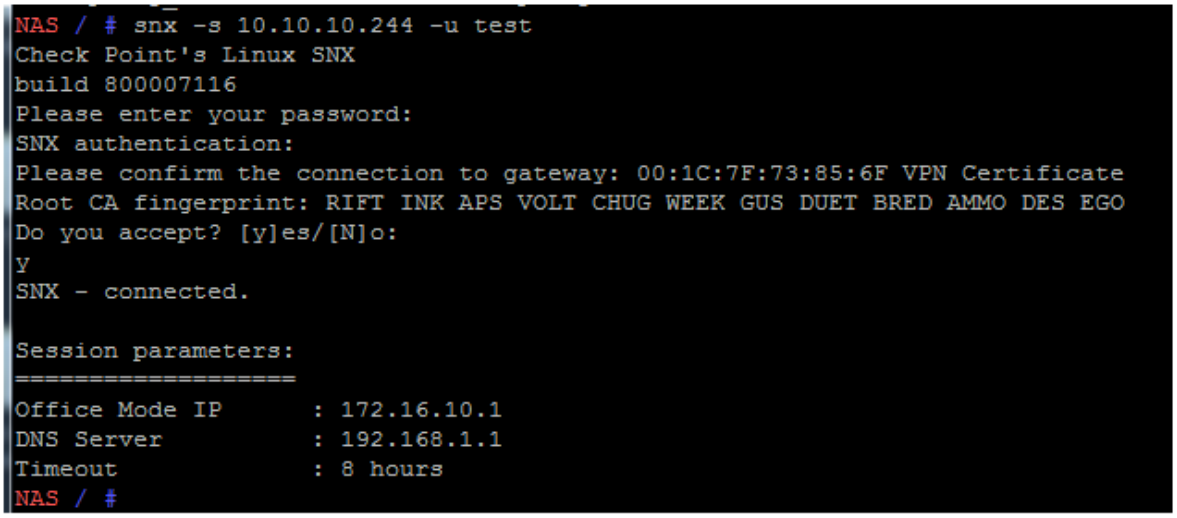
Cliente VPN para Sistemas LINUX.
Asegurarse de tener los privilegios de administrador o ejecuta los comandos con `sudo` según sea necesario.

1. Instalar el componente SNX en el computador del cliente. Para el usuario root , ejecute:
   `# sudo sh ./snx_install.sh`

Para establecer Client-to-Site VPN entre una máquina Linux y un dispositivo SMB administrado localmente, use el agente CLI SNX:

2. Instale SNX con el archivo *snx_install_linux30.sh* .

3. Establezca la VPN con el cliente SSL Network Extender (SNX):



El comano snx -d finaliza la conexión de acceso remoto.

Si cambia el puerto de acceso remoto predeterminado (443), debe especificar el puerto con la -p opción.

6 DOCUMENTOS RELACIONADOS

SC05-POL01 Políticas del sistema de Gestión de seguridad de la información- SGSI
GS01-F21 Formato de solicitud usuario para VPN funcionario.
GS01-F20 Formato usuario para VPN Contratistas SIC.

7 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

- Se actualizan los enlaces para las descargas de los agentes y se documenta de forma más detallada las instrucciones para trabajar con Linux. - Se actualizan en los documentos relacionados GS02-I05 y GS02-I06 por SC05-POL01 Políticas del sistema de Gestión de seguridad de la información- SGSI. - Se elimina el documento relacionado GS02-P01.

_____

Fin documento