TABLA DE CONTENIDO

1. Introducción

El presente documento tiene como propósito orientar a la entidad en el proceso de instalación y funcionamiento de la conexión segura VPN con los servicios de Interoperabilidad.

2. Objetivo

Detalla los lineamientos y recomendaciones para establecer la VPN desde un sistema externo para transferir archivos.

3. Definiciones

VPN SSL: Red privada virtual protocolo transmisión seguro SSL (Secure Socket Layer)

Protocolo SMB: (Server Message Block) es un protocolo cliente / servidor que gobierna el acceso a archivos y directorios completos, así como a otros recursos de red.

4. Generalidades VPN

Los modelos existentes para una conexión privada

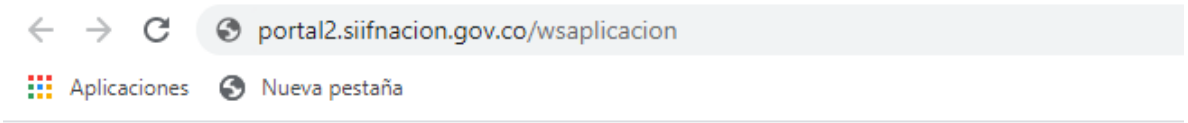
VPN IPsec: Conexión privada que realiza ciframiento desde la capa 3, utilizado para conexiones site to site, o de tipo cliente servidor.

VPN SSL: Conexión privada que realiza ciframiento desde la capa 5, utilizado para conexiones orientadas a aplicaciones web.

5. Configuración inicial Portal Seguro

Una vez prestablecidos los componentes, se recomienda a la entidad usuaria realizar la configuración inicial de manera manual, emulando los pasos de autenticación y activación de la vpn. A continuación, se presenta la configuración del portal seguro:

Llamado a portal seguro: http://portal2.siifnacion.gov.co/wsaplicacion

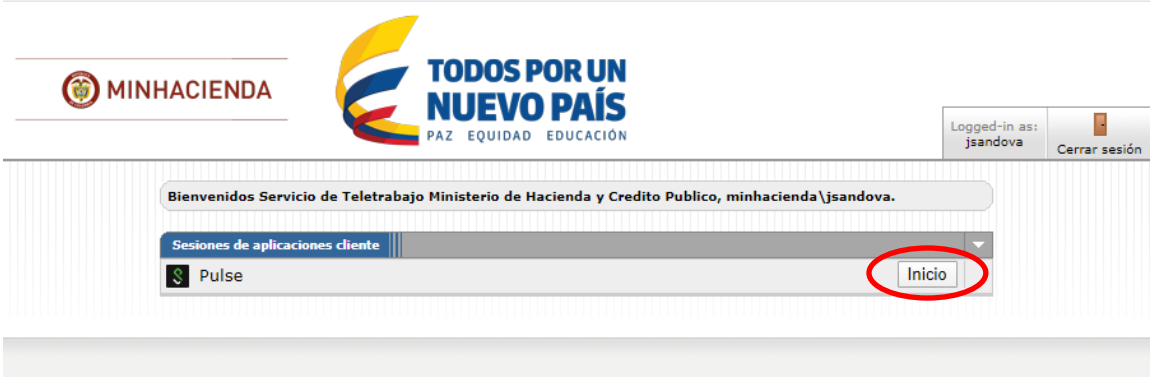


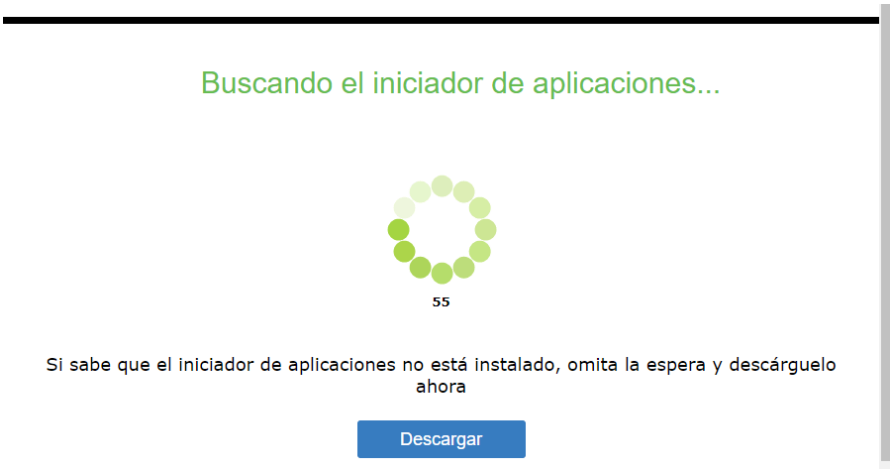
Autenticación: los modelos de autenticación para los portales pueden variar de acuerdo al requerimiento ya sea el usando el modelo de usuario/contraseña, o certificado digital o ambos.

Permitir al portal la instalación de los componentes de vpn.

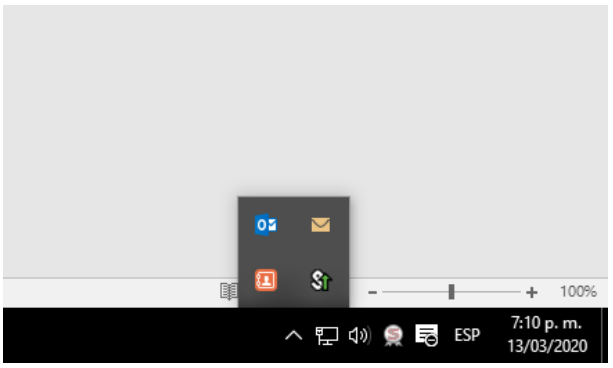
NOTA: es importante para la instalación en el servidor o equipo de usuario contar con los privilegios de instalación de aplicaciones en el sistema operativo.

Después selecciona el botón de inicio y permita instalar la aplicación

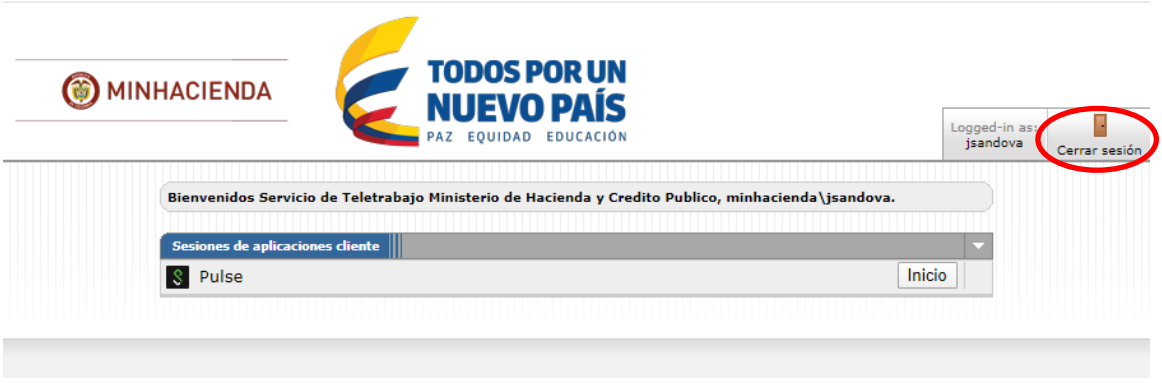


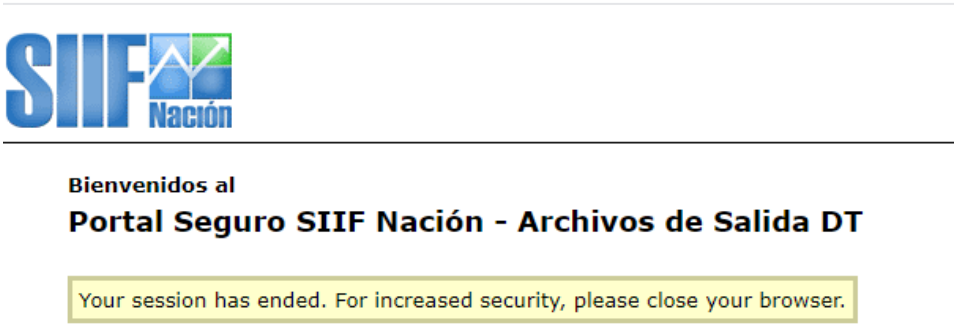


Observara el icono con la flecha apuntando hacia arriba, indicando que la VPN está conectada:



Cerramos sesión





6. Comandos establecer y cerrar VPN

Las líneas de comando permiten realizar de manera automática la activación de la vpn, especialmente para aplicaciones autónomas.

Para establecer la VPN por línea de comandos la sentencia es:

C:\ruta del PulseLauncher.exe

-start *URL de la VPN*

-u <usuario> entre comillas se coloca el nombre del certificado que se va a usar, en el certificado buscar el atributo 'enviado a'

-r *Nombre dominio VPN*

C:\>PulseLauncher.exe -url portal2.siifnacion.gov.co/wsaplicacion -u <usuario> -p <contraseña> -r dominiotranferencia

Se detiene la VPN con el comando

*C:\ >PulseLauncher.exe –**stop***

7. Parámetros adicionales de conexión y códigos de retorno

Como se mencionó en el numeral anterior, PulseLauncher es una herramienta suministrada por PulseSecure que habilita el acceso al portal seguro para descargar el agente PulseSecure.

Los comandos permiten realizar la conexión y controlar el canal desde la línea del sistema, incluyendo las órdenes en un proceso batch-shell/script o desde una aplicación cliente compilada.

Estructura de línea de comando:

pulselauncher.exe [-version|-help|-stop] [-url <url> -u <user> -p <password> -r <realm>] [-d <DSID> -url <url>] [-cert <client certificate> -url <url> -r <realm>] [-signout|-suspend|-resume -url <url>] [-t timeout)]]

Utilice los siguientes argumentos para invocar y controlar PulseLauncher:

Argumento	Acción
-version	Muestra la versión
-help	Muestra los argumentos disponibles
-stop	Termina la conexión

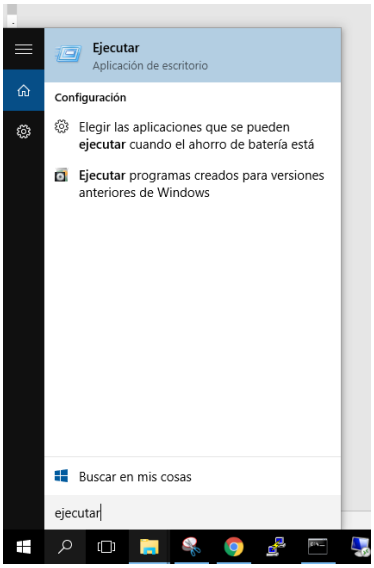
Argumento	Acción
-url <url>	Especifica la URL de la VPN asignada
-u <user>	Especificar el usuario.
-p <password>	Especificar la contraseña.
-r <realm>	Especificar el dominio (realm).
-cert <client certificate>	Especifica el certificado enviado por el usuario para autenticación. Observe que el usuario utiliza esta opción solo si es un certificado válido instalado en IVE. Si el IVE utiliza un certificado auto-firmado el usuario debe importar el certificado dentro del browser.
-signout <url>	Signout, desconecta completamente la VPN. Suspend, termina la conexión con el servidor, pero mantiene la sesión VPN. Resume, restaura la conexión con el servidor.
-suspend <url>	
-resume <url>	

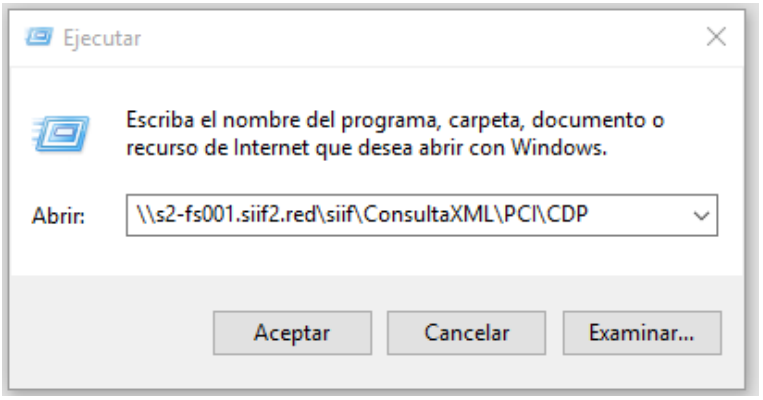
8. Acceso al Servidor de Archivos

Ruta de la carpeta asignada a la entidad:

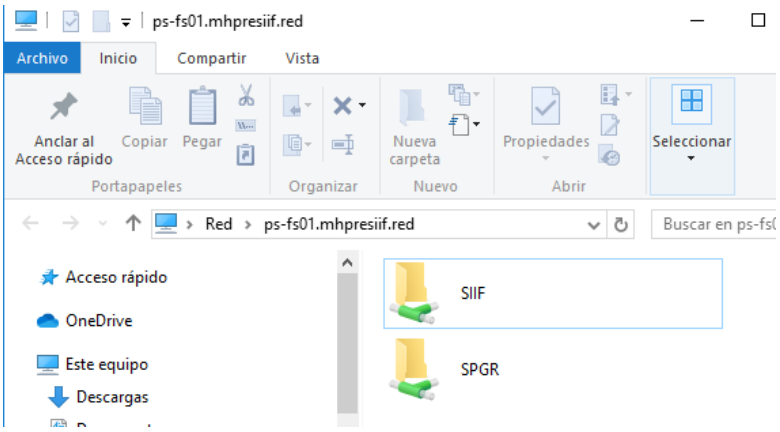
\\s2-fs001.siif2.red\siif\ConsultaXML\PCI\CDP

En búsqueda de Windows puede utilizar la función “ejecutar” ó “run” y agregar la dirección de la carpeta asignada.



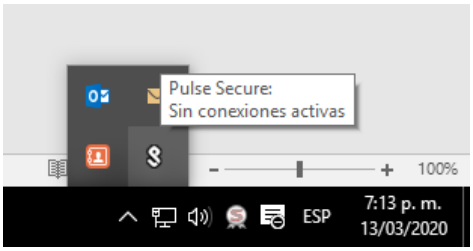


El sistema solicitara una autenticación nuevamente para acceder a la carpeta y seguido presentara el contenido.

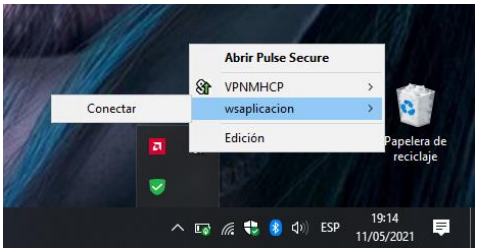


9. Ingresar por segunda vez

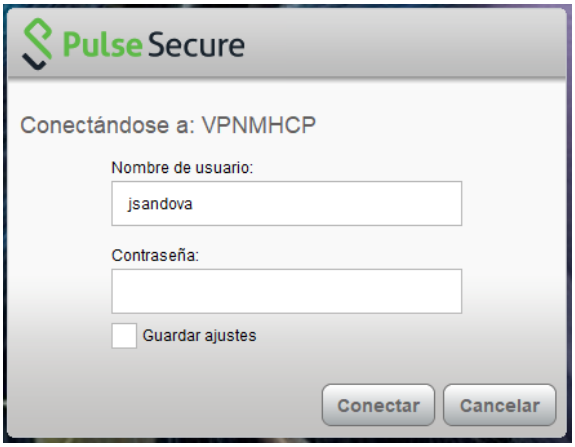
Cuando el componente está instalado, no se requiere volver a entrar al navegador, solo buscado el icono y dándole click derecho, se despliega el menú y su VPN

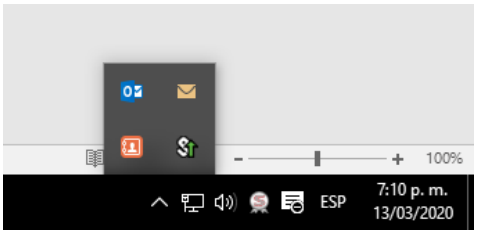


Selecciona su URL portal2.siifnacion.gov.co/wsaplicacion, luego conectar



Luego solicitará credenciales y la VPN se activará mostrando una flecha de color verde hacia arriba. una vez completada puede continuar con la conexión al servidor de archivos.


PulseSecure
Conectándose a: VPNMHCP
Nombre de usuario:
jsandova
Contraseña:
Guardar ajustes
Conectar
Cancelar


100%
ESP
7:10 p. m.
13/03/2020