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 con el Sistema SIIF Nación.

2. Objetivo

Detallas los lineamientos y recomendaciones para establecer la VPN desde un sistema externo que interoperar con SIIF Nación

3. Definiciones

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

WSAM: Windows Secure Application Manager.

4. Generalidades VPN

Los modelos existentes para una conexión privada son:

- 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.
- VPN SSL – WSAM: Solución propietaria de un fabricante que realiza una conexión privada que realiza ciframiento desde la capa 7, utilizado para conexiones orientadas a aplicaciones, la cual permite el control de ciframiento desde la aplicación autoejecutable del sistema operativo.

La configuración que soporta SIIF Extendido es VPN SSL - WSAM

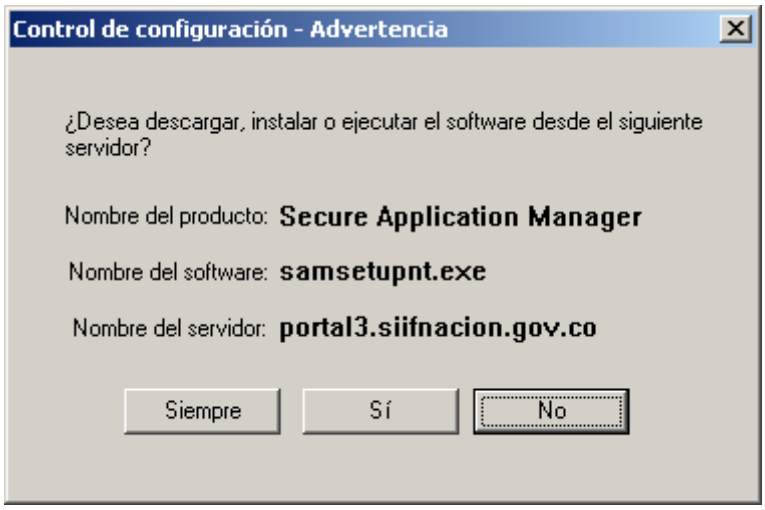
5. Configuración inicial Portal Seguro

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://portal3.siifnacion.gov.co/wsaplicacion

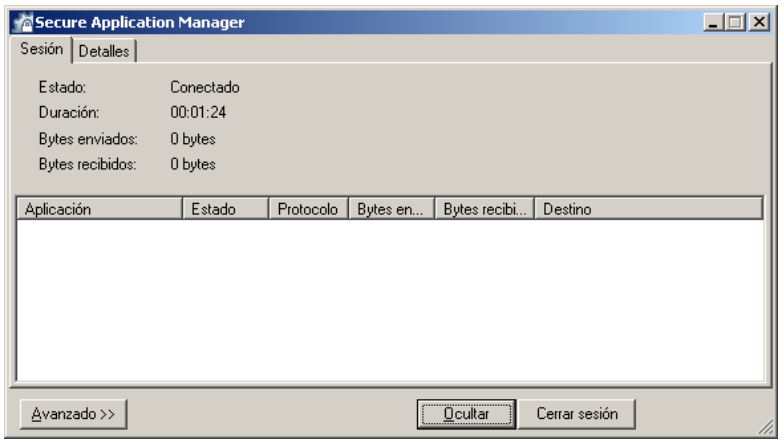
Autenticacion: Los modelos de autenticacion de VPN para web services requieren de la instacion del certificado previo.

Solicita ejecutar el Secure Application Manager

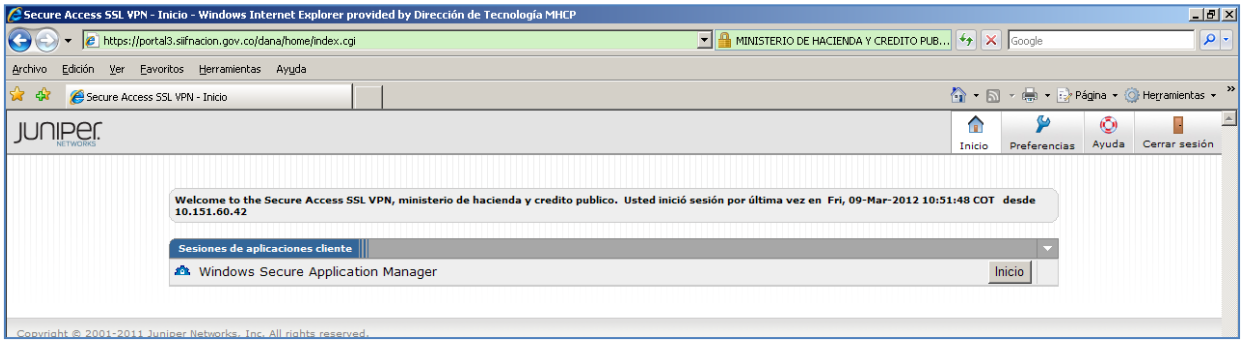


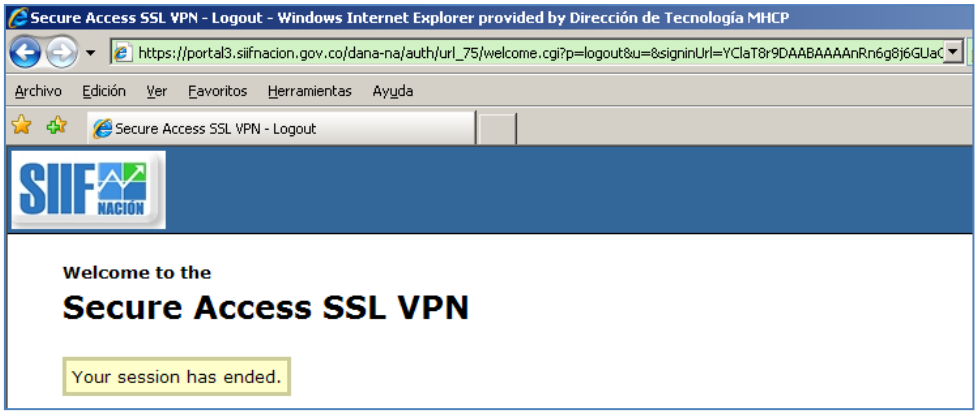
Luego de instalarse aparece el ícono 

en la barra de tareas, informando a cerca de la ejecución de WSAM



Cerramos sesión





6. Comandos establecer y cerrar VPN con Certificado Digital para Web Services

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 SamLauncher.exe

-start *URL de la VPN*

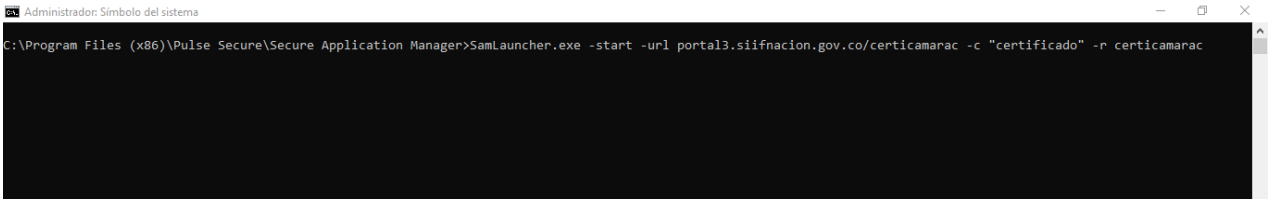
-c "certificado" entre comillas se coloca el nombre del certificado que se va a usar, en el certificado buscar el atributo 'enviado a'

-r *Nombre dominio VPN*

Ejemplo:

C:\Program Files (x86)\Pulse Secure\Secure Application Manager>SamLauncher.exe **-start** -url portal3.siifnacion.gov.co/certicamarac -c "certificado" -r certicamarac

Vista desde la línea de comandos (cmd):



Ejemplo de conexión de activación vpn:

C:\Program Files (x86)\Pulse Secure\Secure Application Manager> SamLauncher.exe -start -url portal3.siifnacion.gov.co/certicamarac –c "NOMBRE CERTIFICADO" -r certicamarac

Se detiene la VPN con el comando

C:\Program Files (x86)\Pulse Secure\Secure Application Manager >SamLauncher.exe –stop

Ejemplo de conexión de cierre de VPN:

C:\Program Files (x86)\Pulse Secure\Secure Application Manager>SamLauncher.exe -stop -url portal3.siifnacion.gov.co/certicamarac –c "NOMBRE CERTIFICADO" -r certicamarac

7. Parámetros adicionales de conexión y códigos de retorno

Como se mencionó en el numeral anterior, WSAM Launcher es una herramienta suministrada por Juniper que habilita el acceso a IVE para descargar el agente WSAM.

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.

Utilice los siguientes argumentos para invocar y controlar WSAM:

Argumento	Acción
-start	Inicializa la conexión WSAM
-stop	Termina la conexión WSAM
-signout	Termina la conexión WSAM y la sesión IVE
-version	Presenta la versión de WSAM
-help	Presenta los argumentos habilitados
-u <usuario>	Especifique el nombre de usuario
-p<clave>	Especifique la clave de autenticación
-c <nombre del certificado>	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.
-u <URL>	Especifica la página URL de validación para el IVE.
-r <realm>	Especifica el dominio real al que IVE envía las credenciales del usuario para validación.

La siguiente tabla muestra los códigos de retorno de WSAM:

Código	Descripción
0	Éxito
1	Argumentos inválidos
2	No se pudo conectar
3	Credenciales inválidas
4	Role no especificado (credenciales mapeadas para múltiples roles)
5	Error de Pre-autenticación (el Host Checker ó el Cache Cleaner no cargaron).
6	La instalación falló
7	Reinicio requerido (si el argumento '-reboot' no ha sido especificado)
8	No se pudo realizar la actualización del software requerida.
10	El IVE no soporta esta característica.
12	Falló al autenticar el certificado del cliente.
100	No se pudo detener Secure Application Manager (SAM o WSAM).
101	No se pudo iniciar Secure Application Manager debido a que existe un conflicto con otro servicio.

8. Modelo para Carga y Descarga de Archivos XML

8.1 Manual

El modelo de autenticación manual exige el ingreso de un usuario válido de SIIF Nación con perfil para carga y descarga de información y una clave (password).

8.2 Automático

El modelo de autenticación automático requiere que el Cliente implemente un autoejecutable que permita hacer llamados http-post donde se envían los parámetros de autenticación, valor de carga/descarga y nombre del archivo.

9. Tiempos de conexión VPN

Para evitar que una conexión segura sea interceptada y decodificada su llave de ciframiento el sistema de conexión segura cuenta con controles de tiempo de vida de la conexión.

- **Tiempo de conexión sin tráfico (Idle Time):** si una conexión cumple 15 minutos si realizar ningún tráfico, esta sesión se finaliza automáticamente y se requiere de una nueva autenticación.
- **Tiempo máximo de Conexión:** una conexión segura cuenta con un tiempo máximo de utilización de 240 minutos (4 horas), desde de cumplir con este tiempo, el sistema termina la sesión y solicita nuevamente la autenticación.

Se recomienda activar el comando “start” previo a iniciar la trasmisión y una vez finalizada la consulta finalizar con el comando “stop”, de esta manera la aplicación no tendrá restricciones de tiempo en su sesión.

10. Recomendaciones

- El certificado de persona Jurídica que se instala en el servidor debe estar alojado en el repositorio Raíz, si se instala a nivel perfil de usuario, la solución VPN no va a tomar el certificado de manera automática.

- Se recomienda utilizar las líneas de comando “start” y “stop”, para controlar el acceso hacia el sistema SIIF Nación. Ya que no es permitido un tiempo de vida de la VPN ilimitado.

- Es importante conocer la arquitectura de la solución, debido a que la conexión inicial solo permite una sesión, si la solución cuenta con granjas de servidores, se deben crear más sesiones de conexión.

- Para el proceso automático de carga y descarga de archivos, se recomienda tener en cuenta el modelo GET/POST de HTTP.