



***CONSULTORES EN SEGURIDAD
TECNOLOGICA E INFORMATICA ARC. SRL***

Documento de creación de VPN Mobile en WatchGuard.
Rev. 1.0



***CONSULTORES EN SEGURIDAD
TECNOLOGICA E INFORMATICA ARC. SRL***

Contenido

VPN IPsec	3
VPN SSL	8
VPN IKEv2	15



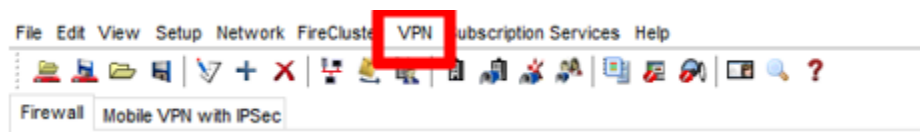
**CONSULTORES EN SEGURIDAD
TECNOLOGICA E INFORMATICA ARC. SRL**

VPN IPsec

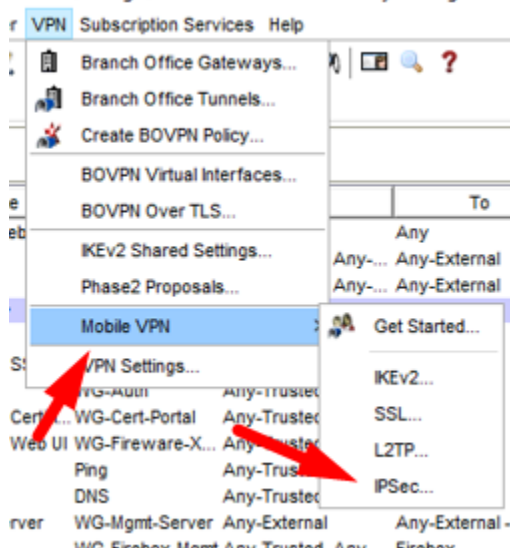
La VPN móvil con IPSec acepta conexiones del software de cliente VPN IPSec instalado en una computadora o dispositivo remoto. El cliente VPN realiza una conexión segura desde la computadora remota a su red protegida a través de una red no segura, como Internet. El cliente VPN móvil utiliza la seguridad del protocolo de Internet (IPSec) para asegurar la conexión.

Pasos para creación de la VPN IPsec:

1- Vamos a la sección de VPN del Policy manager.



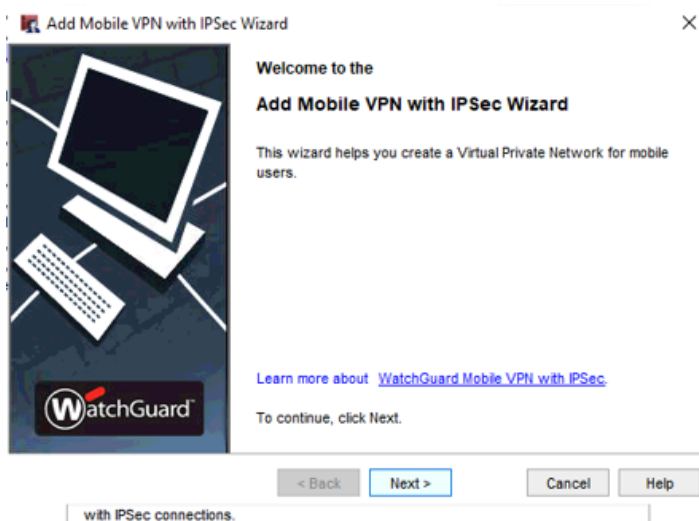
2-Seleccionamos la opción e mobile vpn, luego click a la VPN que estamos creando.



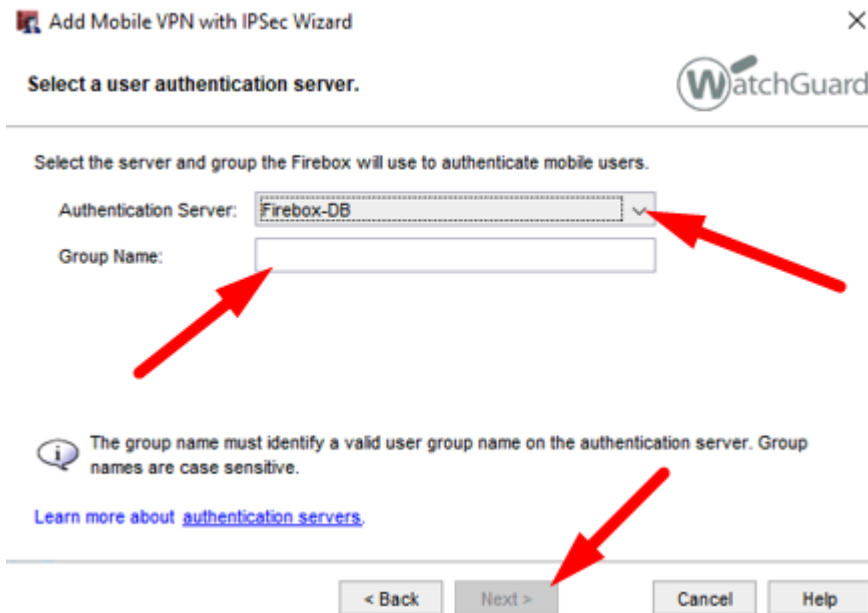


CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

3-Luego procedemos a la creación de un grupo de VPN Ipsec.



4- Luego seleccionamos el método por el cual se autenticarán los usuarios del grupo a crear y le asignamos nombre al grupo que utilizarán esos usuarios y click a siguiente.



Nota: En caso que deseemos utilizar Active Directory, el grupo especificado en el campo GROUP NAME debe de existir en el AD de lo contrario la autenticación no funcionara.



CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

5-Se procede a colocar una contraseña para encriptar el túnel de la VPN, y luego click en siguiente.

Add Mobile VPN with IPsec Wizard

Select a tunnel authentication method.

Select the authentication method the Firebox will use to establish a secure VPN tunnel.

☒ Use this passphrase:

Tunnel Passphrase:

Retype Passphrase:

☐ Use an RSA certificate issued by your WatchGuard Management Server.

Provide the administration passphrase for your server.

IP Address:

Administration Passphrase:

[Learn more about authentication methods.](#)

< Back Next > Cancel Help

with IPsec connections.

6- Luego denegamos la opción de que los usuarios naveguen con la configuración del túnel, colocamos que navegue por la configuración de los usuarios.

Add Mobile VPN with IPsec Wizard

Direct the flow of Internet traffic.

Do you want all traffic between the mobile computer and the Internet to flow through the tunnel?

☒ No, allow Internet traffic to go directly to the mobile user's ISP. (more flexible, less secure)

☐ Yes, force all Internet traffic to flow through the tunnel. (less flexible, more secure)

[Learn more about directing Internet traffic through a tunnel.](#)

< Back Next > Cancel Help

Nota: Por mejores prácticas es recomendable no forzar todo el tráfico de internet por la VPN, ya que puede saturarla.



CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

7-Procedemos a dar click en agregar la dirección de los recursos que deseamos acceder, luego click a siguiente.

Add Mobile VPN with IPsec Wizard

Identify the resources accessible through the tunnel.

Add the computers and networks which will be accessible to mobile users through the VPN tunnel.

Type	IP Address
------	------------

Add... Remove

< Back Next > Cancel Help

8-En el siguiente paso visualizamos el rango de direccionamiento de RED que se le asignara al grupo el cual podemos modificar o agregar otra, luego damos click a continuar y finalizamos la creación.

Add Mobile VPN with IPsec Wizard

Create the virtual IP address pool.

Add the IP addresses the Firebox will assign to mobile computers.

192.168.117.1-192.168.117.100

Add... Remove

Your Firebox is licensed for a maximum of 100 Mobile VPN with IPsec users.

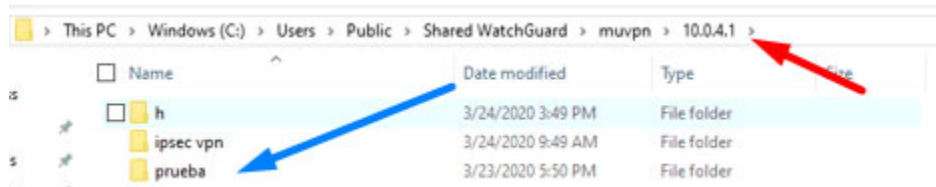
Learn more about [virtual IP addresses](#).

< Back Next > Cancel Help



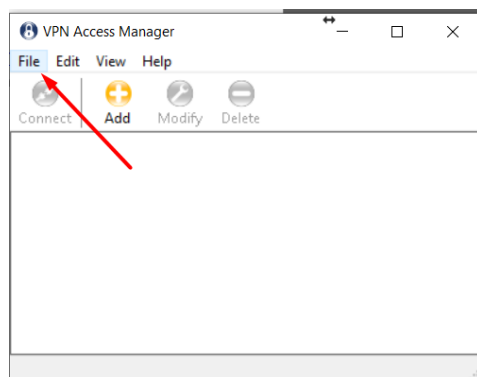
CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

9-Para el siguiente paso debemos descargar un manejador de VPN como [ShrewSoft](#) u otro parecido, procederíamos a cargar el siguiente archivo, e ingresar las credenciales del usuario. Ruta de destino del grupo creado

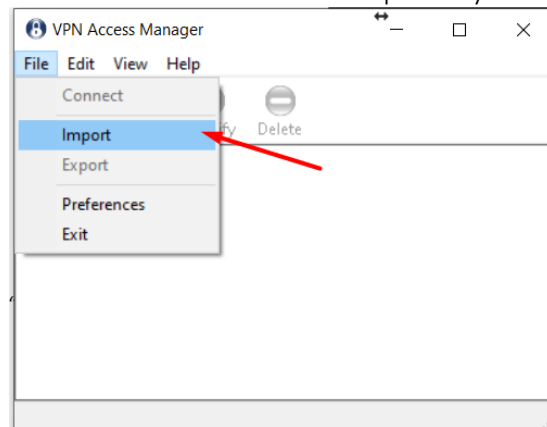


- ▣ Ruta de acceso a la VPN
- ▣ Carpeta con archivos de grupo de VPN creado.

Importar archivo a la plataforma de ShrewSoft, procedemos a dar click en “FILE”.



Procedemos a dar click en importar y seleccionamos el archivo de la VPN IPsec.



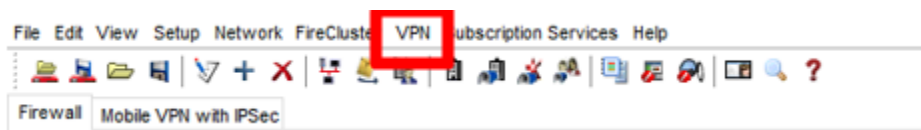


VPN SSL

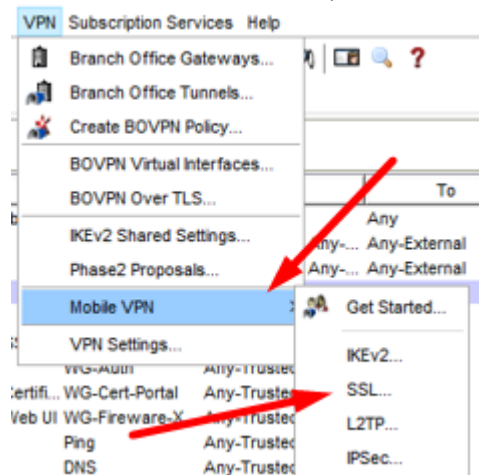
WatchGuard Mobile VPN con cliente SSL es una aplicación de software que se instala en una computadora remota. El cliente realiza una conexión segura desde la computadora remota a su red protegida a través de una red no segura, como Internet. El cliente de Mobile VPN usa Transport Layer Security (TLS) para asegurar la conexión. TLS es el sucesor de Secure Sockets Layer (SSL).

Pasos para creación de la VPN SSL:

- 1- Vamos a la sección de VPN del Policy manager.



- 2- Seleccionamos la opción de mobile vpn luego click a la VPN que estamos creando.





CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

3-Procedemos a dar click en la activación de la VPN SSL, luego colocamos la IP publica por la cual estaríamos accediendo a la vpn y un respaldo de dirección por si ocurre un error con la primera.

Mobile VPN with SSL Configuration

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

☒ **Activate Mobile VPN with SSL**

General Authentication Advanced

Firebox IP Addresses
Type or select a Firebox IP address or domain name for SSL VPN users to connect to.

Primary: 192.168.0.15 Backup:

Networking and IP Address Pool
Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge VPN traffic** if you want to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Firebox to route VPN traffic to specified networks and resources.

Routed VPN traffic

☐ Force all client traffic through tunnel

☒ Allow access to all Trusted, Optional, and Custom networks

☐ Specify allowed resources

Virtual IP Address Pool
Specify the private IP addresses to assign to Mobile VPN with SSL users. Your Firebox allows 100 Mobile VPN with SSL users.

192.168.113. 0 /24



CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

4-En este paso podemos seleccionar, si queremos que la VPN sea **Bridge VPN traffic** o **Route VPN traffic**.

Bridge VPN traffic: coloca una de las direcciones disponibles de la red interna que se encuentran en el firebox, y permite el flujo de todo el tráfico local.

Route VPN traffic: Crea una red virtual la cual realizar un nat con la red interna. Es recomendable usar esta opción porque ofrece mayor seguridad.

Mobile VPN with SSL Configuration

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

☒ Activate Mobile VPN with SSL

General Authentication Advanced

Firebox IP Addresses
Type or select a Firebox IP address or domain name for SSL VPN users to connect to.
Primary: 192.168.0.15 Backup:

Networking and IP Address Pool
Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge VPN traffic** if you want to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Firebox to route VPN traffic to specified networks and resources.

Routed VPN traffic

☐ Force all client traffic through tunnel

☒ Allow access to all Trusted, Optional, and Custom networks

☐ Specify allowed resources

Virtual IP Address Pool
Specify the private IP addresses to assign to Mobile VPN with SSL users. Your Firebox allows 100 Mobile VPN with SSL users.
192.168.113. 0 /24



CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

Hay 3 maneras de especificar el tráfico en la Route VPN traffic

- Forzando a que accedan a todos los recursos de la red.
- Permitiendo que accedan a las interfaces en específico: trusted, optional y custom.
- Especificando el tráfico directamente con la dirección IP.

Networking and IP Address Pool

Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge VPN traffic** if you want to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Firebox to route VPN traffic to specified networks and resources.

Routed VPN traffic

☒ Force all client traffic through tunnel

☐ Allow access to all Trusted, Optional, and Custom networks

☐ Specify allowed resources

. . . /

Add... Remove

5-En este paso podemos seleccionar la manera de autenticar los usuarios de la VPN y especificar directamente por usuarios o grupos.

En este cuadro se puede visualizar los tipos de servidores que se pueden utilizar para la autenticación.

Y las maneras de reconexión, de recordar contraseña y autenticar luego de conectarse la primera vez.

General Authentication Advanced

Authentication Server Settings

Select one or more authentication servers. The first server in the list is the default authentication server. To configure additional authentication servers, click **Configure**.

Select	Authentication Server
☒	RADIUS (Default)
☐	Firebox-DB
☐	LDAP

Configure...
Make Default

☒ Auto reconnect after a connection is lost

☐ Force users to authenticate after a connection is lost

☐ Allow the Mobile VPN with SSL client to remember password
(Fireware OS v11.8 and higher)



CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

En el siguiente pueden visualizar y seleccionar los usuarios y grupos disponibles y con en acceso a la VPN.

☐	Name	Type	Authentication Server
☒	SSLVPN-Users	Group	Any
☐	ipsec vpn	Group	RADIUS

6-Aquí podemos visualizar y configurar los métodos de seguridad de la VPN SSL, el cambio que realizaríamos, por mejores prácticas es cambiar el puerto (443), debido a que es un puerto de uso común.

Authentication: SHA-256
Encryption: AES (256-bit)
Data channel: TCP : 443
Configuration channel: TCP : 443
Keep-alive: Interval: 10 seconds
Timeout: 60 seconds
Renegotiate data channel: Interval: 480 minutes

También podemos configurar el uso de DNS por los clientes que utilizan la VPN.

DNS Settings
Specify the DNS and WINS settings that the Firebox will assign to mobile clients.
☒ Assign the Network DNS/WINS settings to mobile clients (Fireware OS v12.2.1 and higher)
☐ Do not assign any settings to mobile clients
☐ Assign the following settings to mobile clients
Domain name:
DNS servers:
WINS servers:

7-procedemos a salvar los cambios realizados, en el botón ok.

OK Cancel Help



CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

8-Para descargar el agente buscamos la dirección IP pública y el puerto que colocamos en el navegador acompañado de HTTPS://

Luego ingresamos con las credenciales de uno de los usuarios que tiene acceso.

⚠ Not secure | 192.168.0.15:444/sslvpn_logon.shtml

WatchGuard™

Username:

Password:

Login Reset

9-Procedemos a descargar el agente de VPN para el dispositivo a utilizar.

WatchGuard™ Fireware XTM

Items available to download

 **Mobile VPN with SSL client software for Windows**
Use this client to make a secure VPN connection to the company network from a Windows computer.
[Download](#)

 **Mobile VPN with SSL client software for Mac**
Use this client to make a secure VPN connection to the company network from a Mac computer.
[Download](#)

 **Mobile VPN with SSL client profile**
Import this profile to enable a secure VPN connection from any SSL VPN client that supports .ovpn configuration files.
[Download](#)

[Logout](#)

Otra manera de realizar la descarga, puede ser accediendo al Portal de Watchguard
En la dirección: <https://watchguardsupport.secure.force.com/software>.



***CONSULTORES EN SEGURIDAD
TECNOLOGICA E INFORMATICA ARC. SRL***

10-Luego de realizar la instalación procedemos a colocar las credenciales y el puerto por el cual se comunica la VPN SSL.





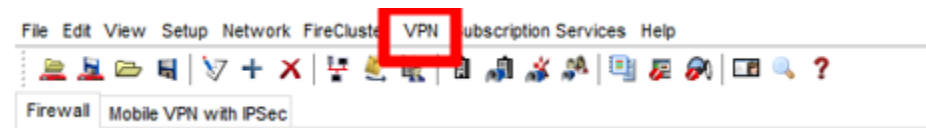
**CONSULTORES EN SEGURIDAD
TECNOLOGICA E INFORMATICA ARC. SRL**

VPN IKEv2

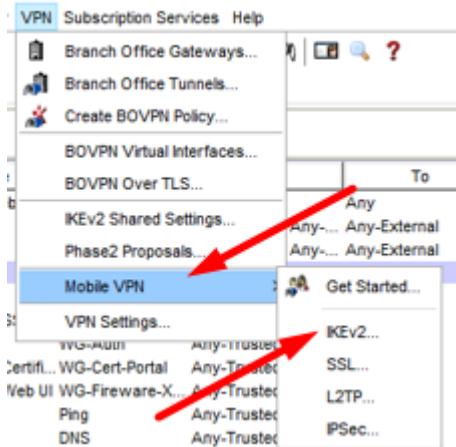
La red privada virtual móvil (VPN móvil) con IKEv2 (Internet Key Exchange v2) crea una conexión segura entre una computadora remota y los recursos de red detrás de Firebox. La VPN móvil con IKEv2 usa IPSec para proporcionar un cifrado y autenticación sólidos.

Pasos para creación de la VPN IKEv2:

1- Vamos a la sección de VPN del Policy Manager.



2- Seleccionamos la opción de Mobile vpn luego click a la VPN que estamos creando.



3- Procedemos a especificar la ruta por la cual accederemos a la VPN, la cual sería la IP pública del firebox, click a agregar dirección, luego click a continuar.





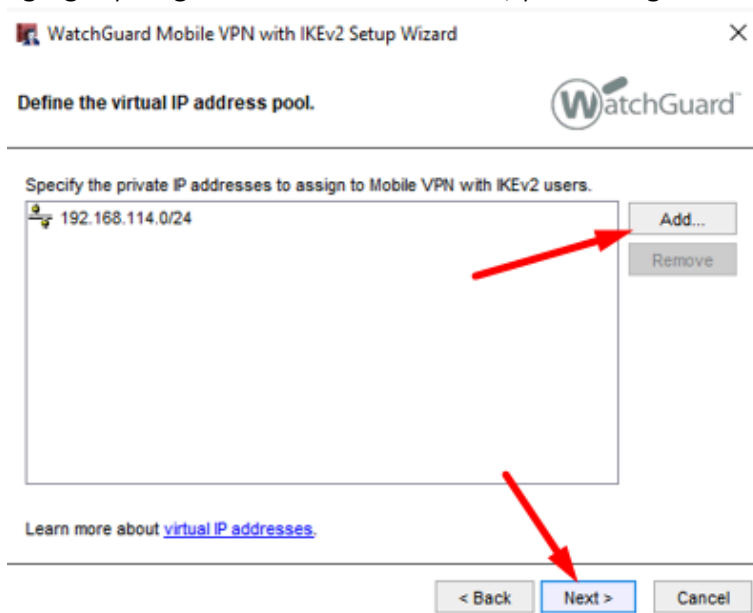
CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

4-Procedemos a colocar o configurar la manera en la cual se autenticarán los usuarios de la VPN. La cual puede ser **Firebox DB** o **Radius**.

Luego procedemos a colocar el Checkbox del método de autenticación que se usara, y luego click a siguiente.



5-Luego procede con las direcciones IP asignadas a los usuarios de la vpn, la cual nos asigna por defecto una IP con mascara de 24, en caso de querer modificar, procedemos a dar click en agregar y luego removemos la anterior, y click a siguiente.



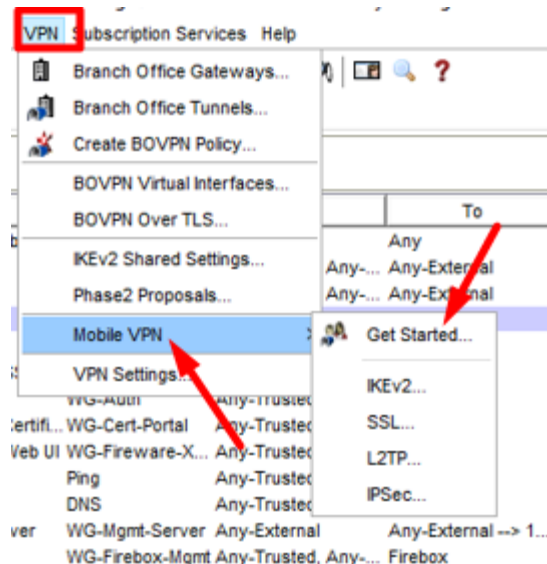


CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

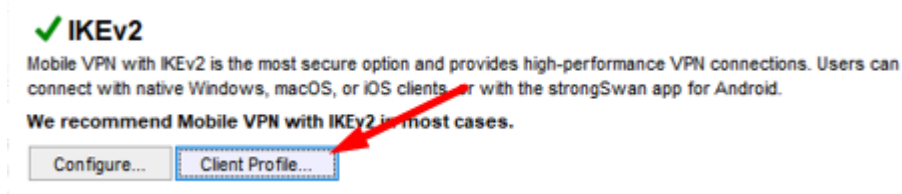
Luego de realizar estos pasos procedemos a guardar los cambios.



6-Para proceder a descargar el perfil damos click en VPN luego click en vpn Mobile y después en Get Started...



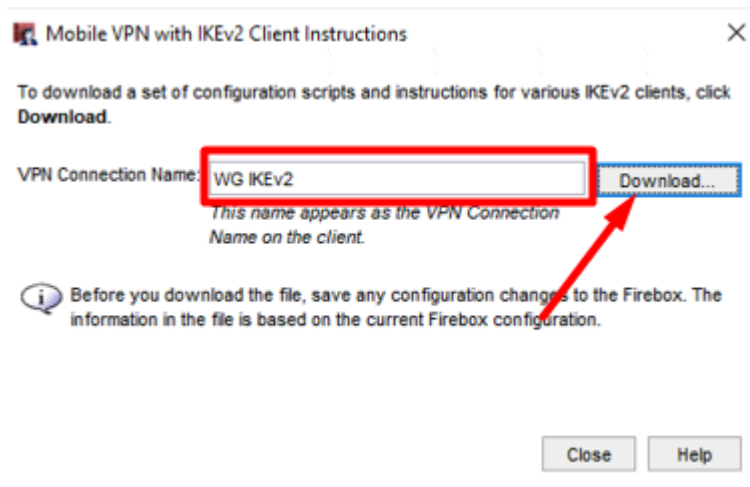
Después de estar dentro damos click en client profile.



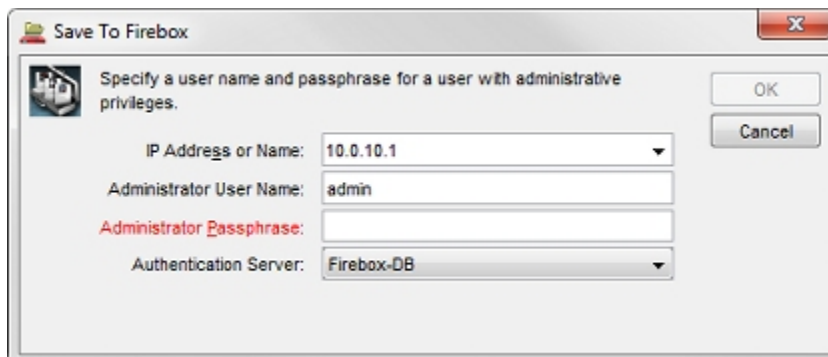


CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

Luego le colocamos el nombre deseado al perfil de IKEv2, y procedemos a descargar el archivo.



Luego de Dar click en descargar nos pide guardar los cambios realizados.





CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

Luego procedemos a descomprimir el archivo descargado.

	Name	Date modified	Type	Size
	configs	3/24/2020 7:16 PM	File folder	
	M300	3/24/2020 5:23 PM	PCAP File	557 KB
	Shared WatchGuard	3/23/2020 12:29 PM	Shortcut	1 KB
	WG IKEv2_prueba	3/24/2020 7:17 PM	WinRAR archive	7 KB

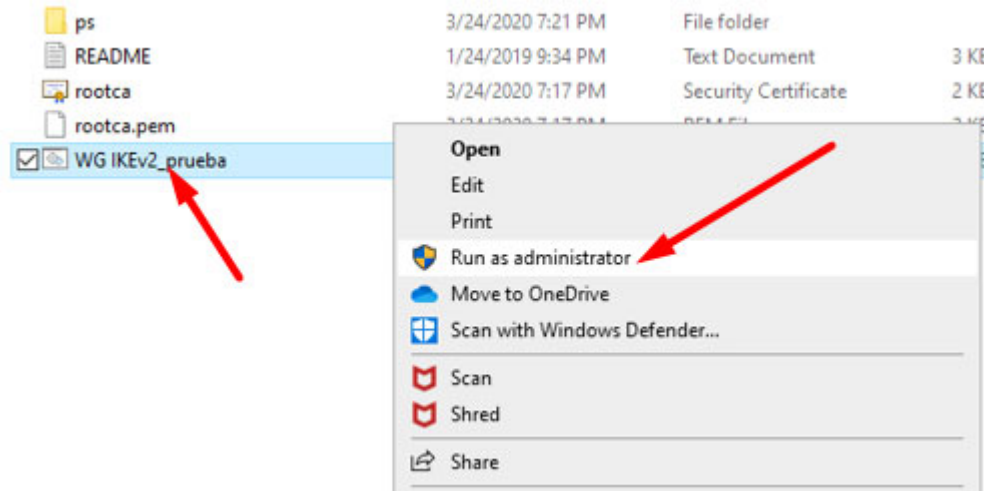
Luego abrimos la carpeta creada, y procedemos a seleccionar la carpeta con el sistema operativo que se estaría utilizando.

	Android	3/24/2020 7:21 PM	File folder	
	MacOS_iOS	3/24/2020 7:21 PM	File folder	
	Windows_8.1_10	3/24/2020 7:21 PM	File folder	
	README	1/24/2019 9:34 PM	Text Document	2 KB
	rootca	3/24/2020 7:17 PM	Security Certificate	2 KB
	rootca.pem	3/24/2020 7:17 PM	PEM File	2 KB

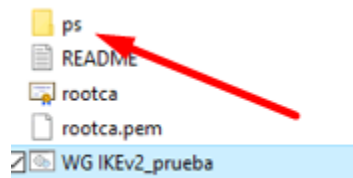


CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

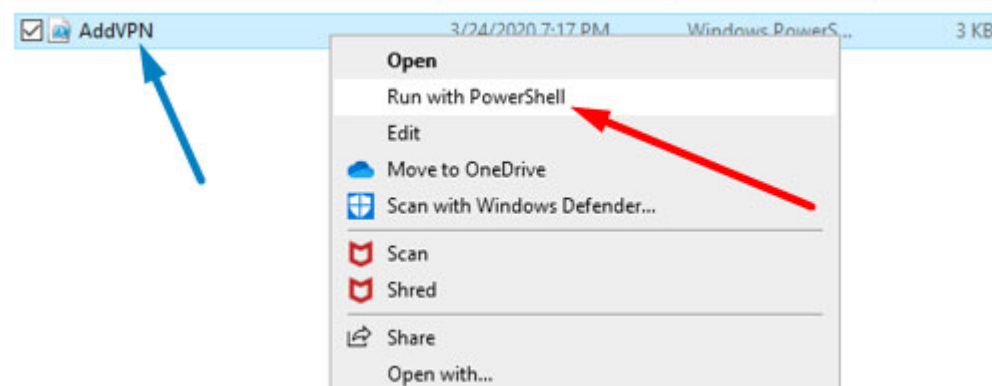
Luego de estar dentro de la carpeta procedemos a ejecutar como administrador el archivo (.bat), click derecho sobre el archivo luego click en “run as administrator”.



Luego entramos a la carpeta (PS) y ejecutamos el archivo que se encuentra con PowerShell.



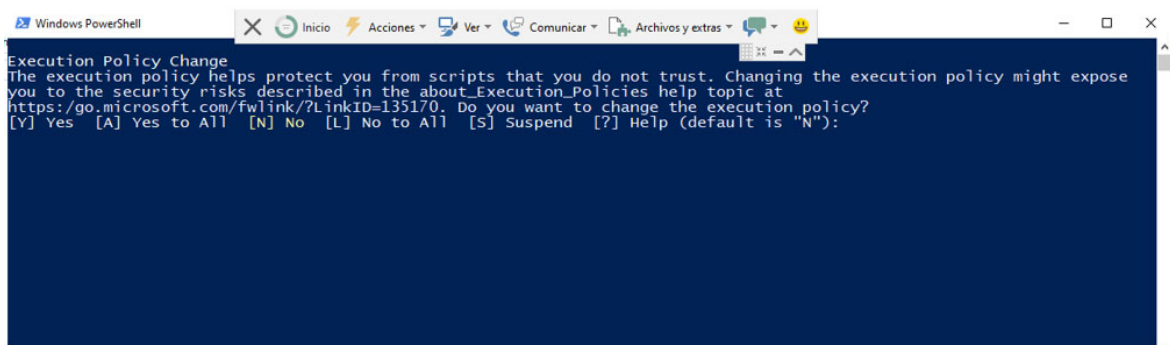
Click derecho sobre el archivo luego click en “Run with PowerShell”.



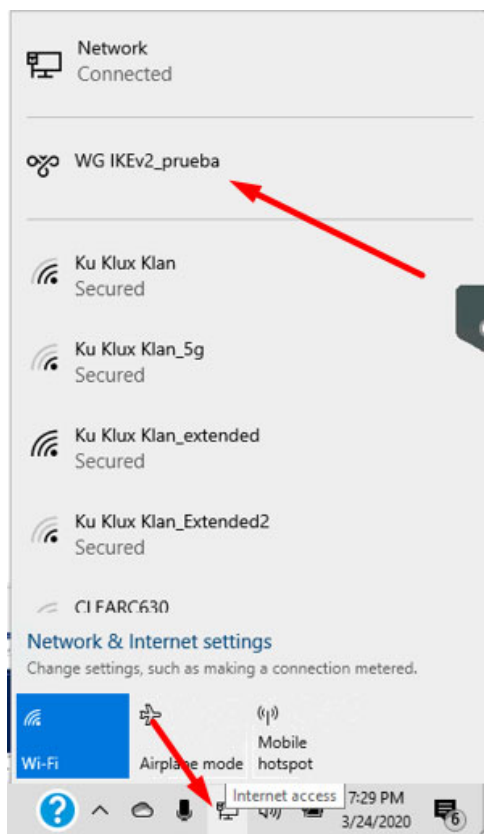


CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC. SRL

Luego de estar dentro del PowerShell procedemos a marcar la letra “Y”, para así permitir la política de cambio.



7-Y por último abrimos, la configuración de redes de Windows o el sistema que estemos utilizando, y procedemos a colocar las credenciales de uno de los usuarios autorizados. La VPN IKE v2 saldrá con el nombre que le estuvimos colocando al archivo. Luego click sobre la VPN.





***CONSULTORES EN SEGURIDAD
TECNOLOGICA E INFORMATICA ARC. SRL***

Luego proceder con las credenciales de uno de los usuarios.

