

Anexo I - Instalación de servicios VPN

Introducción

Este documento recopila configuraciones de ejemplo de las principales soluciones de acceso remoto VPN disponibles para utilizar en la organización y un ejemplo de configuración de cliente estándar.

Lo aquí descrito no intenta ser una guía exhaustiva de instalación, ni un manual de administración, por lo cual hay aspectos que se abordan sin el debido detalle.

La principal ventaja de contar con acceso remoto a través de una VPN es proporcionarles a los usuarios un mecanismo seguro para acceder a los recursos internos de la organización cuando se encuentran fuera de ella. Para considerarse una VPN segura, el tráfico deberá ser encriptado de extremo a extremo.

A continuación, se describe la configuración básica de distintas soluciones de acceso remoto por VPN.

Cabe aclarar que las configuraciones detalladas pueden variar de acuerdo a las diferentes versiones o al licenciamiento de cada una de las soluciones.

Contenido

Instalación Servidor PFSense	3
Asistente de Configuración de Servidor VPN.....	4
Instalación de Cliente OpenVPN	12
OpenVPN 2.4.....	18
Configuración del servidor Linux (CentOS 7).....	18
Configuración del usuario en el servidor.	21
Configuración del servidor	21
Configuración del dispositivo del cliente final.....	22
Juniper SRX.....	23
Configuración del servidor (resumen de alto nivel).	23
Configuración de los datos del cliente en el servidor.	23
Configuración del túnel en el servidor.	24
Configuración de políticas de acceso en el firewall.....	24
Configuración del lado del dispositivo del cliente.....	25
Cisco.....	26
Configuración del servidor (resumen)	26
Configuración del servidor.	26
Configuración del cliente en el servidor.....	29
Configuración del túnel en el servidor.	30

Instalación Servidor PFSense

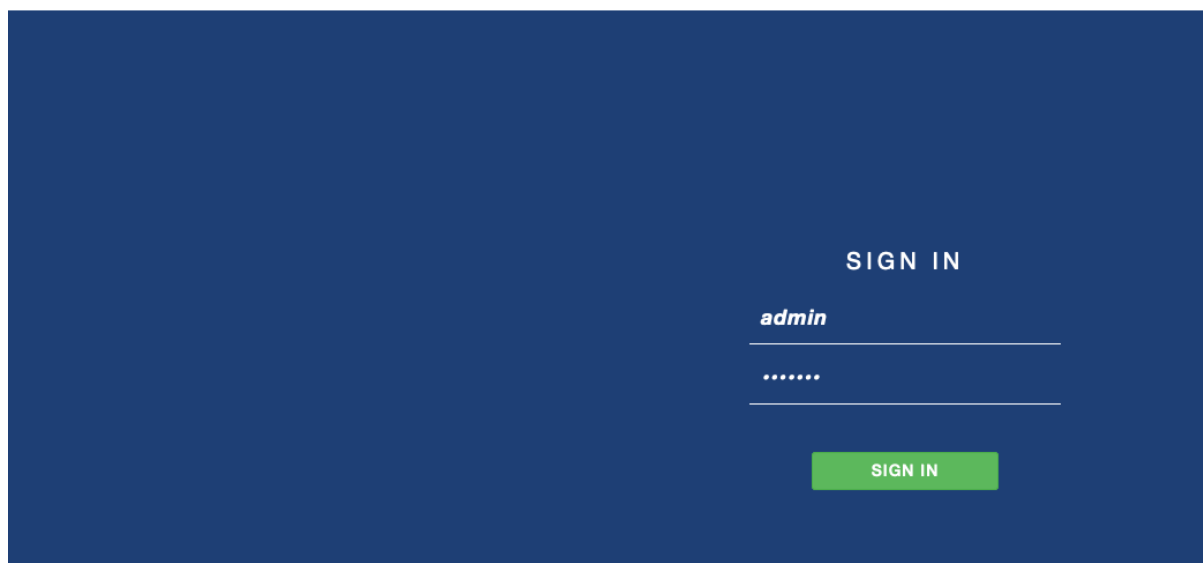
Se enumeran a continuación los pasos para la instalación de un servidor concentrador de túneles VPN utilizando PFSense en su versión 2.X.

Quedan fuera de esta guía (si bien está altamente recomendado) las configuraciones adicionales post-instalación de securización del servidor, actualización de los componentes y otras tareas básicas de seguridad como cambiar la contraseña, reforzar las reglas de firewall, etc.

- Descargar ISO de PFSense desde <https://www.pfsense.org/download/>
- Peso ~700 MB (Descargar desde USA Mirror #1 Texas o #2 NewYork).
- Elegir Arquitectura AMD64 (Procesadores Intel/AMD de 64 bits).
- Conectar ISO y bootear desde medio optico virtual o crear un USB booteable (<https://docs.netgate.com/reference/create-flash-media.html>).

- Video Tutorial de Instalación:
<https://archivos.agesic.gub.uy/nextcloud/index.php/s/ZPLkfnkq4rP42WB>

- Una vez instalado, ingresar vía Navegador Web (Ej: Firefox, aceptar certificado sin verificar) y colocar credenciales de acceso administrador.
- Usuario: [admin](#) / Contraseña: [pfsense](#)



Asistente de Configuración de Servidor VPN

Se accede mediante el Menú principal **VPN > OpenVPN** una vez dentro dirigirse al link **Wizards** y completar los campos como indica a continuación y se aprecia en las imágenes:

→ Tipo de Backend de Autenticación define de que forma autenticamos los usuarios.

Wizard / OpenVPN Remote Access Server Setup / ?

OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Select an Authentication Backend Type

Type of Server

- ✓ Local User Access
- LDAP
- RADIUS

[» Next](#)

→ Crear Autoridad Certificadora para emitir los Certificados necesarios, completar los campos con los datos acorde a su organización.

Wizard / OpenVPN Remote Access Server Setup / Add Certificate Authority ?

Step 6 of 11

Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Create a New Certificate Authority (CA) Certificate

Descriptive name
A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.

Key length
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Country Code
Two-letter ISO country code (e.g. US, AU, CA)

State or Province
Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City
City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organization
Organization name, often the Company or Group name.

[» Add new CA](#)

- Crear nuevo certificado del servidor que será el encargado del cifrado de los datos de cada conexión, completar los campos correspondientes con los datos de su organización.

Wizard / OpenVPN Remote Access Server Setup / Add a Server Certificate
?

Step 8 of 11

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Create a New Server Certificate

Descriptive name	<input style="width: 90%;" type="text" value="Certificado del Servidor"/> <p style="font-size: small; margin-top: 5px;">A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."</p>
Key length	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">2048 bit</div> <p style="font-size: small; margin-top: 5px;">Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com</p>
Lifetime	<input style="width: 90%;" type="text" value="3650"/> <p style="font-size: small; margin-top: 5px;">Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)</p>
Country Code	<input style="width: 90%;" type="text" value="UY"/> <p style="font-size: small; margin-top: 5px;">Two-letter ISO country code (e.g. US, AU, CA)</p>
State or Province	<input style="width: 90%;" type="text" value="Montevideo"/> <p style="font-size: small; margin-top: 5px;">Full State of Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).</p>
City	<input style="width: 90%;" type="text" value="Montevideo"/> <p style="font-size: small; margin-top: 5px;">City or other Locality name (e.g. Louisville, Indianapolis, Toronto).</p>
Organization	<input style="width: 90%;" type="text" value="AGESIC"/> <p style="font-size: small; margin-top: 5px;">Organization name, often the Company or Group name.</p>

» Create new Certificate

- Generar configuración de conexión para el servidor OpenVPN, puerto de escucha del servicio (1194 por omisión), protocolos de transmisión de datos (recomendado UDP solamente) en IPv4).

Wizard / OpenVPN Remote Access Server Setup / Server Setup
?

Step 9 of 11

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Interface	<input type="text" value="WAN"/>	The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol	<input type="text" value="UDP on IPv4 only"/>	Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Local Port	<input type="text" value="1194"/>	Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.
Description	<input type="text" value="Acceso a la LAN"/>	A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

- Red del Túnel indica la numeración IP a ser configurada para los dispositivos dentro del túnel que sean remotos, tener reparo en colocar una numeración que no se solape con otras redes, ya sean locales o de interconexión con otros organismos (Ej: evitar REDuy 10.255.0.0/16, REDSalud 10.253.0.0/16, etc).

→ Red Local indica la numeración de la red local (Ej: LAN o DMZ) hacia donde el servidor VPN generará el acceso.

Tunnel Settings	
Tunnel Network	<input type="text" value="192.168.0.0/24"/> This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect Gateway	<input type="checkbox"/> Force all client generated traffic through the tunnel.
Local Network	<input type="text" value="172.16.0.0/20"/> This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent Connections	<input type="text"/> Specify the maximum number of clients allowed to concurrently connect to this server.
Compression	<input type="text" value="Omit Preference (Use OpenVPN Default)"/> Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	<input type="checkbox"/> Allow communication between clients connected to this server.
Duplicate Connections	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

→ Topología indica el modo de asignar las direcciones IP asignadas a la red de túnel en el paso anterior, para aislar los usuarios dentro del túnel, recomendamos utilizar redes /30 por cada conexión como se aprecia debajo.

Client Settings	
Dynamic IP	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
Topology	<input type="text" value="Subnet -- One IP address per client in a common subnet"/> <input checked="" type="text" value="net30 -- Isolated /30 network per client"/> Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".
DNS Default Domain	<input type="text"/> Provide a default domain name to clients.
DNS Server 1	<input type="text" value="Ejemplo: Servidor DNS en Red Local LAN -> 172.16.0.1"/> DNS server IP to provide to connecting clients.

→ Configuración de Firewall deberá dejar pasar el tráfico desde el mundo hacia la interfaz exterior del PFSense así como el tráfico dentro del túnel OpenVPN, el asistente permite hacerlo en la etapa visible debajo, configurar acorde al ejemplo.

Wizard / [OpenVPN Remote Access Server Setup](#) / Firewall Rule Configuration ?

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule

Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule

Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

[» Next](#)

→ Configuración Finalizada permite hacer click en el botón para finalizar la configuración y ver la misma en la grilla debajo.

Wizard / [OpenVPN Remote Access Server Setup](#) / Finished! ?

Step 11 of 11

Finished!

OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

The configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

[» Finish](#)

→ En [VPN > OpenVPN > Servers](#) deberá aparecer la configuración recientemente realizada.

VPN / [OpenVPN](#) / Servers 📊 📄 ?

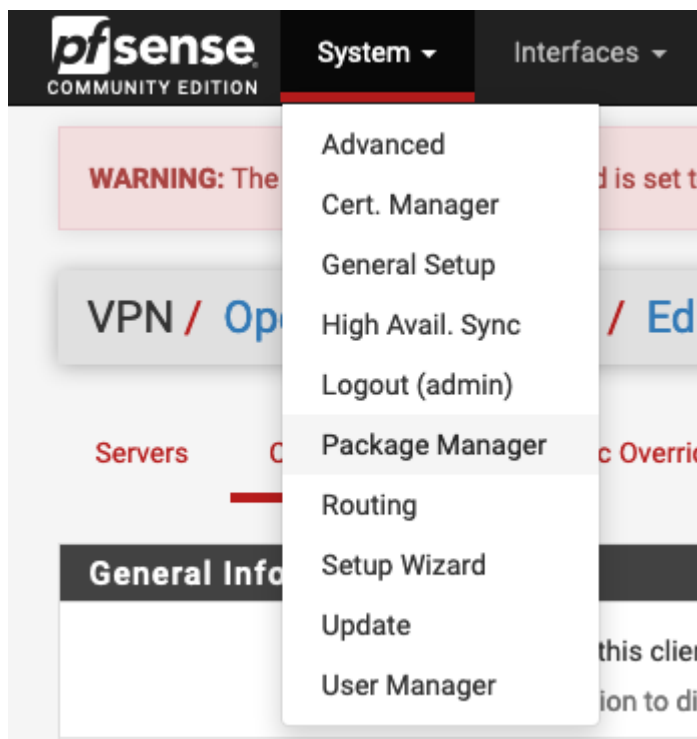
[Servers](#) [Clients](#) [Client Specific Overrides](#) [Wizards](#)

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	192.168.0.0/24	Crypto: AES-128-CBC/SHA256 D-H Params: 2048 bits	Acceso a la LAN (tun)	✎ 🗑

[+ Add](#)

→ Una vez generados los certificados y la configuración, es necesario crear los usuarios a conectarse a la VPN, esto se genera ingresando a [System > User Manager](#)



→ Es importante seleccionar la opción Certificate debajo, esta será la que permite crear un certificado asociado al usuario, para luego conectar el cliente VPN en el dispositivo elegido.

Users Groups Settings Authentication Servers

User Properties

Defined by USER

Disabled This user cannot login

Username

Password

Full name
User's full name, for administrative information only

Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings Use individual customized GUI options and dashboard layout for this user.

Group membership

Not member of: Member of:

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate Click to create a user certificate

→ Para distribuir los certificados, debemos instalar el paquete [openvpn-client-export](#) en [System](#) > [Package Manager](#) > [Available Packages](#)

System / Package Manager / Available Packages ?

Installed Packages Available Packages

Search

Search term: Both

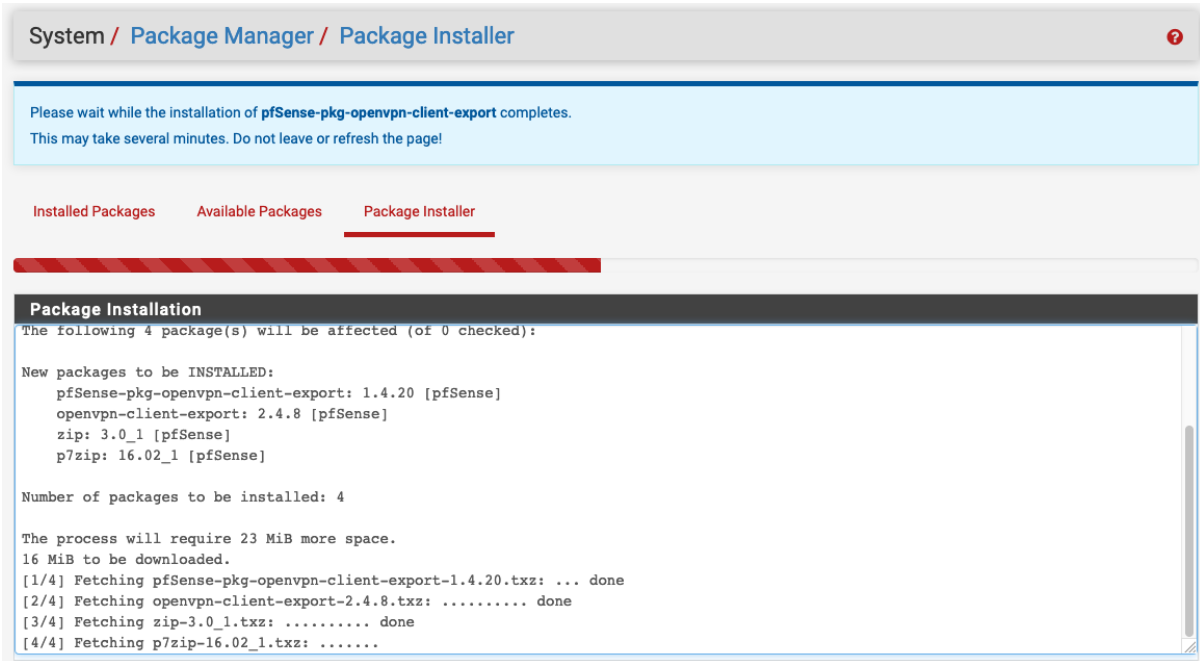
Enter a search string or *nix regular expression to search package names and descriptions.

Packages

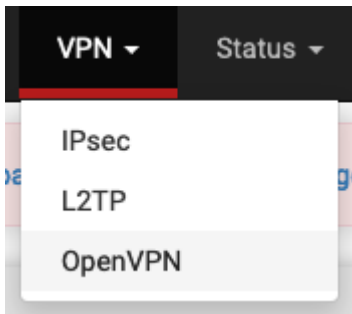
Name	Version	Description
openvpn-client-export	1.4.20	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense. + Install

Package Dependencies:
[openvpn-client-export-2.4.8](#) [openvpn-2.4.6_1](#) [zip-3.0_1](#) [p7zip-16.02_1](#)

→ Luego de buscar el paquete, dar click en [Install](#) y aguardar a la instalación.



→ Una vez instalado volvemos a VPN > OpenVPN



→ Descargamos la configuración y los certificados del cliente deseado en [OpenVPN > Client Export > Archive](#)

OpenVPN Clients		
User	Certificate Name	Export
usuario_vpn1	Usuario VPN 1	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installer (2.4.8-lx02): 7/8/8.1/2012r2 10/2016/2019 - Old Windows Installers (2.3.18-lx02): x86-xp x64-xp x86-win6 x64-win6 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

Only OpenVPN-compatible certificates are shown

Instalación de Cliente OpenVPN

Se instala y configura el cliente VPN (en este ejemplo se muestra un Windows 10) la configuración de los parámetros de conexión serán heredados del perfil creado en los pasos anteriores.

→ Descargar cliente OpenVPN de <https://openvpn.net/community-downloads/>.

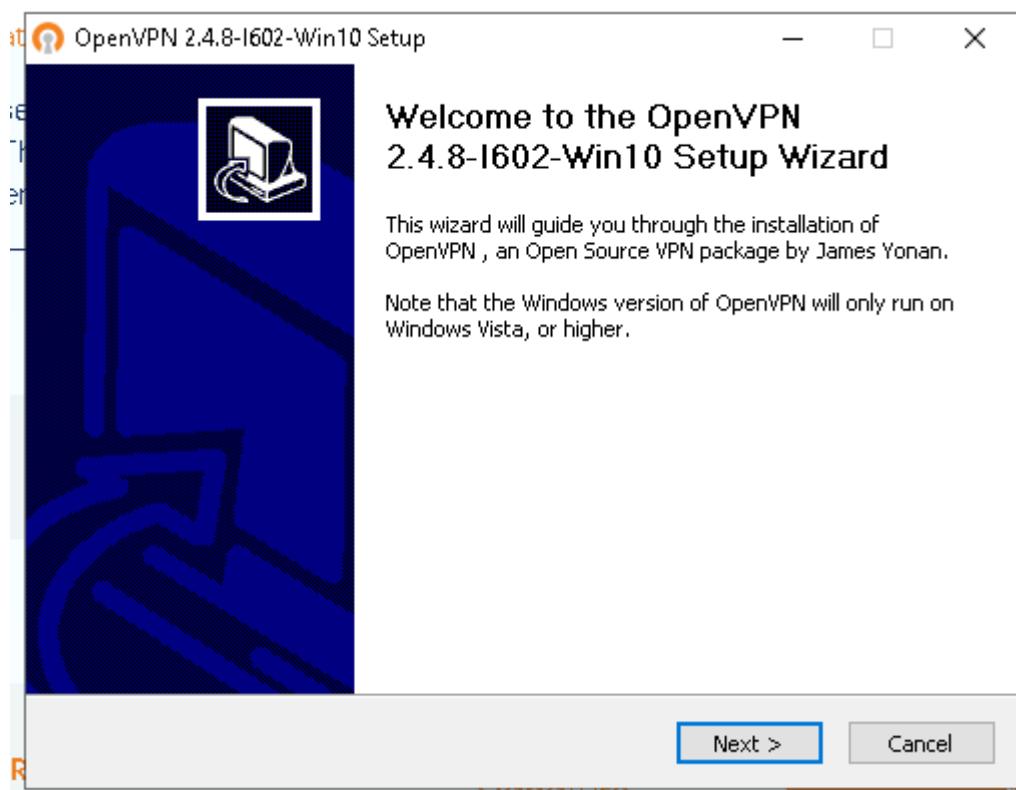

[BUSINESS VPN](#)
[PERSONAL VPN](#)
[SUPPORT](#)
[COMMUNITY](#)
[GET OPENVPN](#)

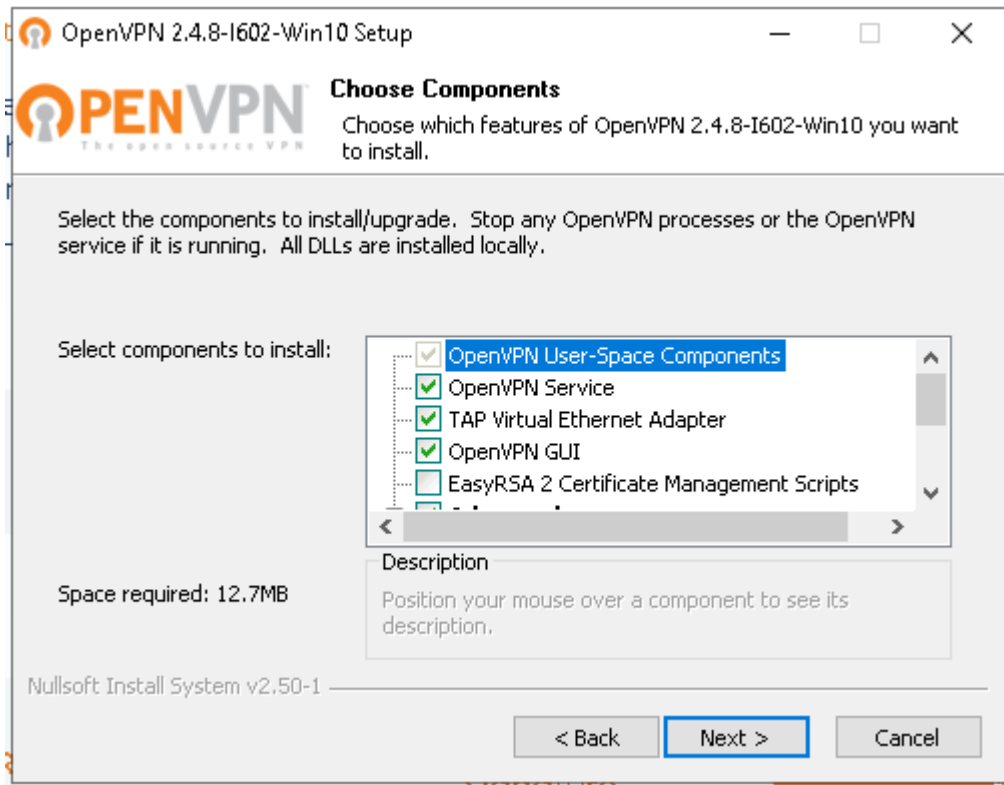
look at our official [documentation](#), [wiki](#), [forums](#), [openvpn-users mailing list](#) and user IRC channel (#openvpn at irc.freenode.net).

Important: you will need to use the correct installer for your operating system. The Windows 10 installer works on Windows 10 and Windows Server 2016/2019. The Windows 7 installer will work on Windows 7/8/8.1/Server 2012r2. This is because of Microsoft's driver signing requirements are different for kernel-mode devices drivers, which in our case affects OpenVPN's tap driver (tap-windows6).

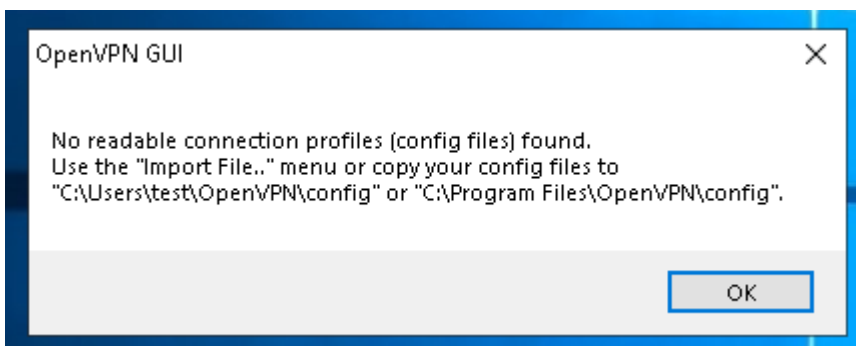
SOURCE TARBALL (GZIP)	GnuPG Signature	openvpn-2.4.8.tar.gz
SOURCE TARBALL (XZ)	GnuPG Signature	openvpn-2.4.8.tar.xz
SOURCE ZIP	GnuPG Signature	openvpn-2.4.8.zip
WINDOWS 7/8/8.1/SERVER 2012R2 INSTALLER (NSIS)	GnuPG Signature	openvpn-install-2.4.8-i602-win7.exe
WINDOWS 10/SERVER 2016/SERVER 2019 INSTALLER (NSIS)	GnuPG Signature	openvpn-install-2.4.8-i602-win10.exe

→ Iniciar la Instalación, la configuración por omisión es funcional al tutorial.

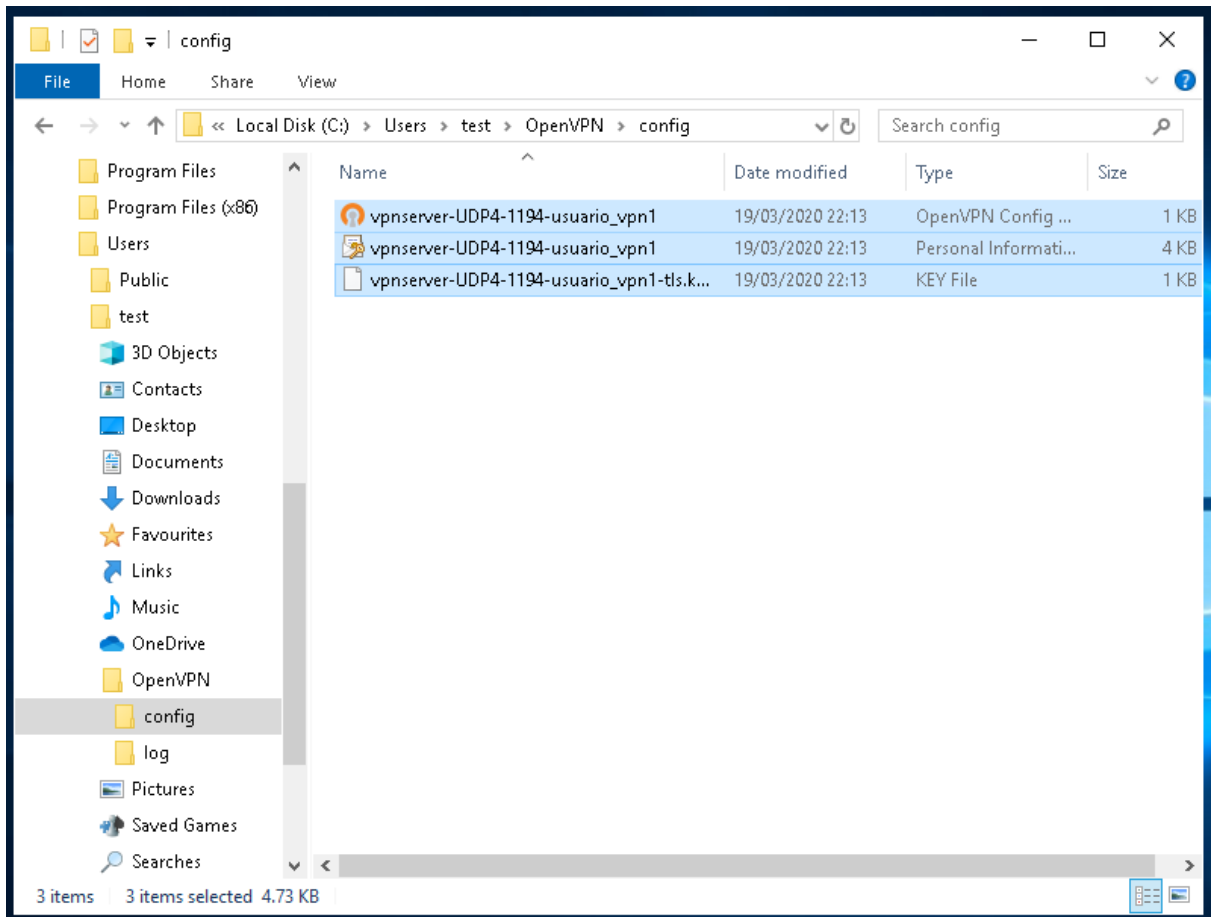




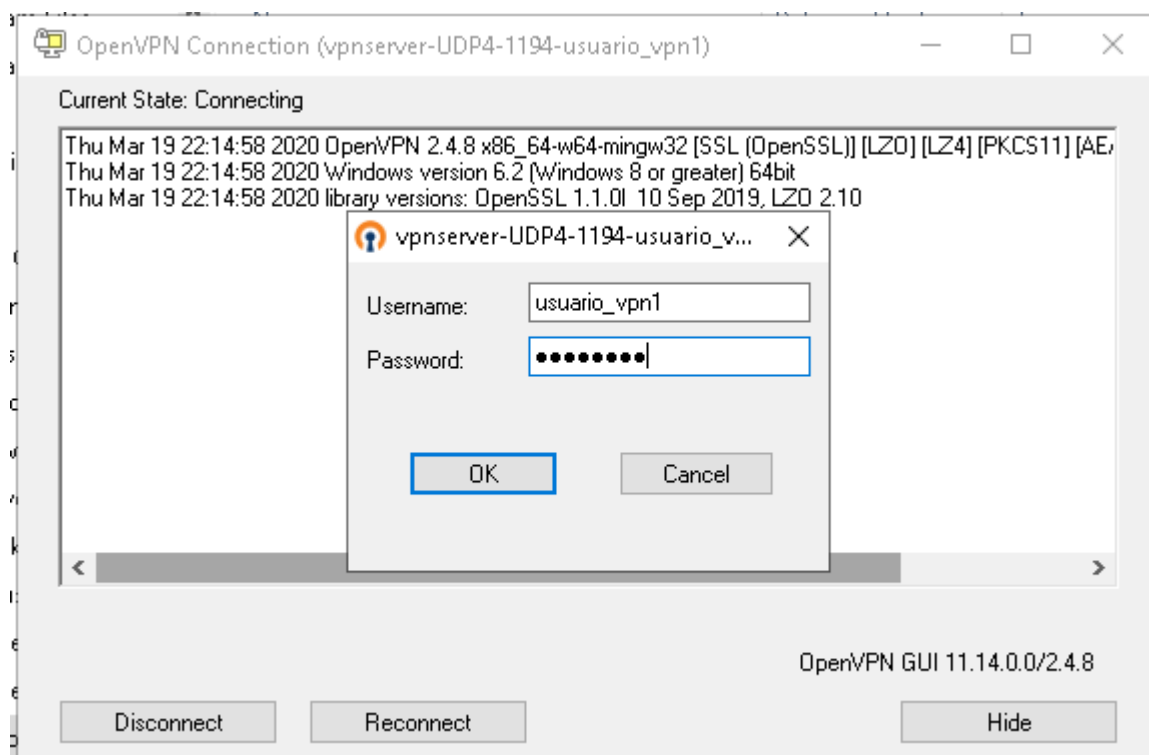
- Al finalizar la instalación intentamos iniciar el Cliente OpenVPN, nos indicará que falta el perfil de conexión, debemos copiar dichos archivos en cualquiera de los directorios sugeridos (recomendamos hacerlo dentro del perfil del usuario, en este caso el usuario de windows se llama test).



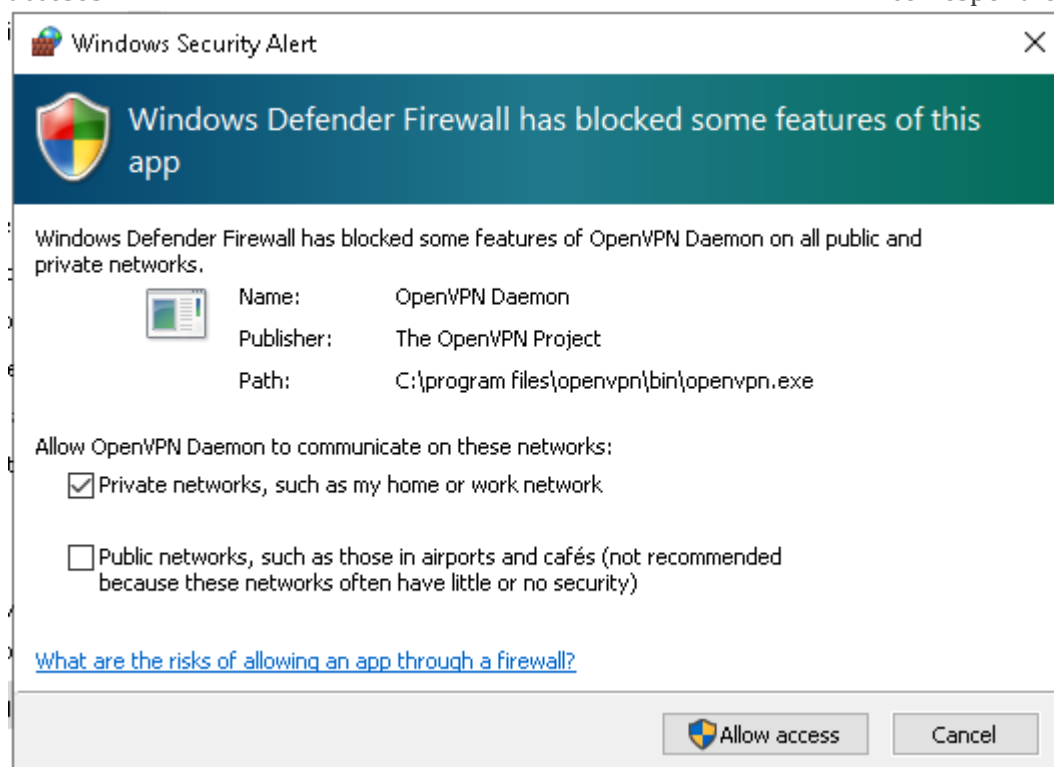
- Colocar los 3 archivos dentro del directorio config y ejecutamos nuevamente el Cliente OpenVPN.



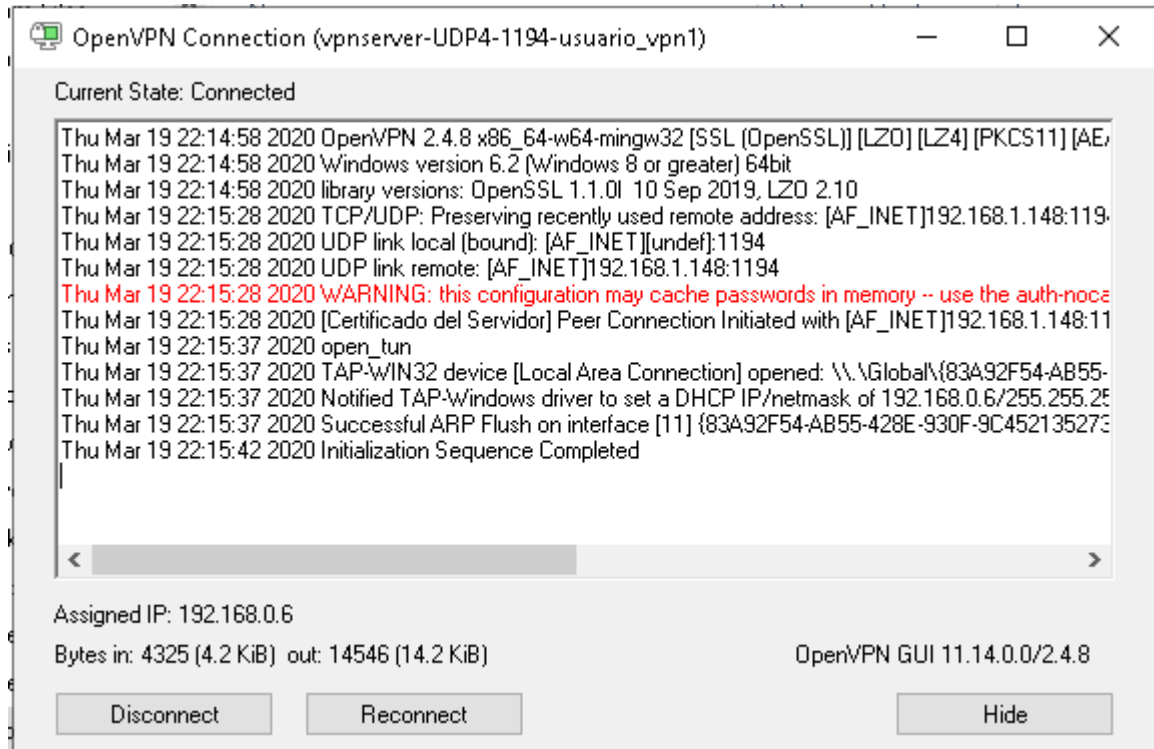
→ Al ejecutar nuevamente, colocamos el juego de credenciales Usuario y Contraseña creados anteriormente.



→ Si el Firewall de Windows solicita permiso para acceder a redes, podemos darle los accesos correspondientes.



→ Conexión realizada satisfactoriamente, debería de poder acceder sin problemas a la red de destino, configurada en el servidor.



→ Del lado del servidor, podemos ver en la consola el mensaje de conexión satisfactoria.

```

Message from syslogd@vpnserv at Mar 19 21:36:24 ...
vpnserv php-fpm[340]: /index.php: Successful login for user 'usuario_vpn1' from
m: 192.168.1.144 (Local Database)
    
```

OpenVPN 2.4

OpenVPN es una tecnología de conexiones privadas virtuales cuyo principal diferencial es la de ser un proyecto de código abierto de fácil integración y configuración. Esta solución es multiplataforma y soporta múltiples configuraciones de seguridad y compresión de tráfico.

Configuración del servidor Linux (CentOS 7)

1 - Instalar OpenVPN

```
yum -y install epel-release
yum -y install openvpn
```

2 - Instalar EasyRSA

```
yum install -y easy-rsa
export PATH=$PATH:/usr/share/easy-rsa/3.0.6/
```

3 - Configuración del servidor

Editar o crear el archivo `etc/openvpn/server.conf` con la siguiente información

```
port 1194
proto tcp
dev tun
user nobody
group nobody
ca /etc/openvpn/easy-rsa/ca.crt
cert /etc/openvpn/easy-rsa/issued/server.crt
key /etc/openvpn/easy-rsa/private/server.key
dh /etc/openvpn/easy-rsa/dh.pem
topology subnet
cipher AES-256-CBC
auth SHA512
server 192.168.2.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
persist-key
persist-tun
status /var/log/openvpn-status.log
log-append /var/log/openvpn.log
```

```
verb 3
tls-server
tls-auth /etc/openvpn/tls.key
```

4 - Generación de claves y certificados

```
mkdir /etc/openvpn/easy-rsa
semanage fcontext -a -t openvpn_etc_t /etc/openvpn/easy-rsa/
easyrsa init-pki
easyrsa build-ca
easyrsa gen-dh
easyrsa gen-req server nopass
easyrsa sign-req server server
openvpn --genkey --secret /etc/openvpn/tls.key
cp -a /root/pki/* /etc/openvpn/easy-rsa/
restorecon -R /etc/openvpn/easy-rsa/
```

Iniciar el servicio

```
systemctl start openvpn@server.service
```

Habilitar tráfico en el firewall del servidor

```
firewall-cmd --permanent --add-port=1194/tcp
firewall-cmd --permanent --add-masquerade
firewall-cmd --reload
```

4.5 Crear claves para los clientes (este proceso debe repetirse para cada cliente)

```
easyrsa build-serverClient-full usuario1
```

4.6 Crear archivo de configuración para los clientes (este proceso debe repetirse para cada cliente)

Crear archivo *nombreDelUsuario.ovpn* en este caso *usuario1* con el siguiente contenido

```
client
dev tun
proto tcp
remote <ip pública del servidor> 1194
tls-version-min 1.2
tls-cipher LS-ECDHE-RSA-WITH-AES-128-GCM-SHA256:TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256:TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256
cipher AES-256-CBC
auth SHA512
resolv-retry infinite
```

```
auth-retry none
nobind
route-nopull
persist-key
persist-tun
ns-cert-type server
comp-lzo
verb 3
tls-client
```

Agregar las claves para autenticar

```
echo -e "<ca>\n$(cat /root/pki/ca.crt)\n</ca>" >> usuario1.ovpn
echo -e "<cert>\n$(cat /root/pki/issued/usuario1.crt)\n</cert>" >> usuario1.ovpn
echo -e "<key>\n$(cat /root/pki/private/usuario1.key)\n</key>" >> usuario1.ovpn
echo -e "<tls-auth>\n$(cat /etc/openvpn/tls.key)\n</tls-auth>" >> usuario1.ovpn
```

5 - Configurar reglas de ruteo para la interface tun0

Configurar reglas para llegar desde la red de VPN a servidores DNS, HTTP y lo que se requiera.

6 - Configuración del cliente

Instalar cliente

En Linux:

```
yum -y install epel-release
yum -y install openvpn
```

En Windows:

Descargar el cliente (<https://openvpn.net/client-connect-vpn-for-windows/>)

Usar el archivo *nombreDelUsuario.ovpn* generado para conectarse desde un cliente con el siguiente comando:

```
openvpn nombreDelUsuario.ovpn
```

- **FortiGate 6.0**

Las soluciones de FortiGate son un empaquetado de múltiples tecnologías para controlar y mejorar la seguridad a nivel de red; estas pueden ser inspección de SSL, Proxy server, IPS y VPN, entre otros. FortiGate ofrece una administración simple basada en su WebGUI de forma intuitiva y de fácil asimilación. La VPN de FortiGate ofrece una robusta encriptación de datos, así como de identificación de los usuarios que la utilizan.

Configuración del usuario en el servidor.

1. Crear grupo de usuarios para los usuarios remotos.
 - 1.1. En FortiOS, ir a User & Device > User > User Definition.
 - 1.2. Creá tantos usuarios locales como sea necesario utilizando el asistente de creación de usuarios.
 - 1.3. Dirigite al menú Device > User > User Groups
 - 1.4. Creá un grupo de usuarios para los usuarios remotos y agregá los usuarios que acabás de crear.

Configuración del servidor

2. Agregar políticas del firewall para la red local y rutas.
 - 2.1 En FortiOS, ir a Policy & Objects > Objects > Addresses
 - 2.2 Agregá el direccionamiento para una red local LAN y la interfaz de la red LAN.
3. Configuración de la conexión IPsec VPN.
 - 3.1 En FortiOS, ir a VPN > IPsec > Wizard.
 - 3.2 Ingresá el nombre de la conexión VPN y en Template, seleccioná Dialup - FortiClient (Windows, Mac OS, Android). Hacé clic en "Siguiente".
 - 3.3 En interfaz de entrada, seleccioná de la lista la interfaz WAN. Por ejemplo: wan1.
 - 3.4 En método de autenticación, seleccioná Pre-shared Key.
 - 3.5 En el campo *Pre-shared Key*, ingresá la clave deseada.
 - 3.6 En *User Group*, seleccioná el grupo de usuarios creado en el punto 1. Hacé clic en "Siguiente".
 - 3.7 En *Local Interfaz*, seleccioná la interfaz de la LAN.
 - 3.8 En el campo *Local Address*, seleccioná la red LAN que accederá el grupo de usuarios remotos seleccionados.
 - 3.9 En el campo *Client Address Range*, seleccioná un direccionamiento IP que será usado por los clientes/equipos remotos.
 - 3.10 Asegurate de que la opción *Enable IPv4 Split Tunnel* no esté seleccionada para que el acceso a internet sea a través de Fortigate. Hacé clic en "Siguiente".

3.11 Seleccioná la opción *Save Password* en el paso Client Options

4. Crear políticas de seguridad para que los clientes remotos puedan acceder a destinos específicos dentro de la organización.
 - 4.1 En FortiOS, dirigite a *Policy & Objects > IPv4 Policies* y seleccioná *Create New*. Ingresá un nombre para poder identificar el sentido. Por ejemplo: IPsec-to-Internet
 - 4.2 En la opción *Incoming Interface*, seleccioná la interface virtual de la VPN.
 - 4.3 En la opción *Outgoing interface*, seleccioná la interface que conecta al destino.
 - 4.3 En la opción *Source*, seleccioná el direccionamiento utilizado para los clientes remotos.
 - 4.4 En la opción *Destination*, especificá los servidores destino.
 - 4.5 En la opción *Service*, especificá los puertos destino.
 - 4.6 En caso de que el destino sea externo a la organización, la opción NAT debe estar habilitada.

Configuración del dispositivo del cliente final

1. Instalación y configuración del lado del cliente de acceso remoto.
 - 5.1 Descargá e instalá el software FortiClient https://filestore.fortinet.com/forticlient/downloads/FortiClientVPNOnlineInstaller_6.2.exe
 - 5.2 Luego de instalarla, abrí la aplicación, agregá una nueva conexión VPN, accedé a *Remote Access* y agregá una nueva conexión "*Add a new connection*".
 - 5.3 Seleccioná el tipo IPsec VPN.
 - 5.4 En "*Connection Name*", ingresá un nombre.
 - 5.5 En "*Remote Gateway*", ingresá la dirección IP pública o nombre del servicio publicado. Por ejemplo: dirección asignada para la interfaz wan1, vpn.xxxxxx.gub.uy
 - 5.6 En "*Authentication Method*", seleccioná Pre-shared key.
 - 5.7 En "*Authentication (XAuth)*", seleccioná Prompt on login.

Referencia: <https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/589121/ipsec-vpn-with-forticlient>

Juniper SRX

La tecnología de Juniper ofrece seguridad, robustez y escalabilidad en distintos niveles. Acompañada del software de Pulse Secure, ofrece una VPN altamente performante, robusta y con configuraciones granulares en todos los sentidos, ya sea identificación, acceso o autenticación.

Configuración del servidor (resumen de alto nivel).

Se necesita definir y configurar el pool de las IP que debe alojar a los clientes remotos; este tiene nomenclatura CIDR (X.X.X.X/XX).

Se deben configurar los perfiles que utilizarán los clientes.

A nivel de túnel, se debe configurar las políticas de IKE. También es necesario configurar el gateway local que van a tener los clientes VPN; esta sería la interfaz por la cual saldrán estos usuarios. Este tipo de VPN utiliza el protocolo IPSEC, el cual necesita ser configurado mediante políticas y perfiles.

Configurando estos datos, ya se va a poder alojar los usuarios en nuestro pool VPN y permitir que estos se sitúen dentro de la organización. Lo que estaría restando sería permitir el tráfico de estos clientes hacia los distintos servicios internos; aquí entrarían en juegos las reglas de acceso.

Una serie de sentencias para configurar el equipo sería:

Configuración de los datos del cliente en el servidor.

1 Definir el pool de usuarios VPN

```
set pool vpn-address-pool family inet network 10.10.10.0/24
```

2. Definir el dns primario para los usuarios.

```
set pool vpn-address-pool family inet xauth-attributes primary-dns 10.10.10.100/32
```

3. Definir el usuario carlos.perez con la password "AGESIC12341234" y el perfil perfil_remote_access

```
set access profile perfil_remote_access client carlos.perez firewall-user password "AGESIC12341234"
```

4. Asignar al perfil perfil_remote_access el pool de IPS vpn-address-pool

```
set access profile perfil_remote_access address-assignment pool vpn-address-pool
```

Configuración del túnel en el servidor.

1. Definir el modo en el que trabajará el protocolo.
set policy ike-dyn-vpn-policy mode aggressive
2. Definir el proposal de fase 2 que utilizará las políticas.
set policy ike-dyn-vpn-policy proposal-set standard
3. Definir una clave compartida para permitir el acceso.
set policy ike-dyn-vpn-policy pre-shared-key ascii-text "AGESIC12341234"
4. Agregar el grupo de seguridad y las políticas IKE al gateway VPN.
set security ike gateway dyn-vpn-local-gw ike-policy ike-dyn-vpn-policy
5. Definir el nombre que será utilizado como identificador.
set security ike gateway dyn-vpn-local-gw dynamic hostname Juniper01
6. Definir el número máximo de conexiones.
set security ike gateway dyn-vpn-local-gw dynamic connections-limit 10
7. Definir un grupo de seguridad para el gateway.
set security ike gateway dyn-vpn-local-gw dynamic ike-user-type group-ike-id
8. Definir la interfaz a la cual se conectarán los usuarios.
set security ike gateway dyn-vpn-local-gw external-interface ge-0/0/15.0
9. Asignar el perfil de acceso al gateway configurado anteriormente.
set security ike gateway dyn-vpn-local-gw aaa access-profile dyn-vpn-access-profile
10. Definir el proposal de fase 2 que utilizará la política de IPSEC.
set security ipsec policy ipsec-dyn-vpn-policy proposal-set standard.
11. Asignar al gateway el perfil de seguridad para VPN.
set security ipsec vpn dyn-vpn ike gateway dyn-vpn-local-gw
12. Asignar las políticas de IPSEC para VPN.
set security IPsec vpn dyn-vpn ike ipsec-policy ipsec-dyn-vpn-policy

Configuración de políticas de acceso en el firewall.

1. Generar una política para identificar los orígenes.

```
set security policies from-zone untrust to-zone trust policy dyn-vpn-policy match source-address any
```

2. Generar una política para identificar los destinos.

```
set security policies from-zone untrust to-zone trust policy dyn-vpn-policy match destination-address any
```

3. Generar una política para identificar las aplicaciones.

```
set security policies from-zone untrust to-zone trust policy dyn-vpn-policy match application any.
```

4. Generar una política para permitir el tráfico IPSEC y permitir la conexión.

```
set security policies from-zone untrust to-zone trust policy dyn-vpn-policy then permit tunnel ipsec-vpn dyn-vpn
```

5. Generar una zona para permitir el tráfico IKE en la interfaz de VPN.

```
set security zones security-zone untrust interfaces ge-0/0/15.0 host-inbound-traffic system-services ike
```

6. Generar una zona para permitir el tráfico HTTPS en la interfaz de VPN.

```
set security zones security-zone untrust interfaces ge-0/0/15.0 host-inbound-traffic system-services https
```

7. Generar una zona para permitir el tráfico ICMP en la interfaz de VPN.

```
set security zones security-zone untrust interfaces ge-0/0/15.0 host-inbound-traffic system-services ping
```

Configuración del lado del dispositivo del cliente.

1. Descargar el cliente Pulse Secure de Juniper

2. Agregar una nueva configuración

3. Escribir IP del Juniper o hostname público.

4. Escribir usuario.

5. Generar conexión.

Cisco

La solución VPN de Cisco utiliza IPSec como protocolo de encapsulamiento. Cisco es una de las marcas con mayor trayectoria en el mercado de las redes; su VPN ofrece una conexión segura de punto a punto entre los clientes y el terminador VPN.

En este caso, se presenta un resumen de la configuración utilizando Cli y la versión 9.14 de IOS. Para los dispositivos remotos se utilizará el cliente AnyConnect, el cual se descarga del sitio de Cisco de acuerdo al dispositivo y versión de sistema operativo. <https://software.cisco.com/download/home/283000185>

Configuración del servidor (resumen)

1. Se necesita definir y configurar el pool de las IP que obtendrán los clientes remotos, este tiene nomenclatura CIDR (X.X.X.X/XX).
2. Se deben configurar los perfiles que utilizarán los clientes.
3. A nivel de túnel, se deben configurar las políticas de IKE. También es necesario configurar el gateway local que van a tener los clientes VPN; esta sería la interfaz por la cual saldrán estos usuarios. Este tipo de VPN utiliza el protocolo IPSEC, el cual necesita ser configurado mediante políticas y perfiles.
4. Configurando estos datos, ya se va a poder alojar los usuarios en nuestro pool VPN y permitir que se sitúen dentro de la organización. Lo que estaría restando sería permitir el tráfico de estos clientes hacia los distintos servicios internos; aquí entrarían en juegos las reglas de acceso.

Configuración del servidor.

1. Configuración de interfaces

- 1.1 Acceder al modo de configuración de interface desde el modo global de configuración.

```
interface {interface}
```

Ejemplo:

```
hostname(config)# interface ethernet0  
hostname(config-if)#
```

1.2 Configurar la dirección IP y máscara de subred en la interface expuesta a internet.

```
ip address ip_address [mask] [standby ip_address]
```

Ejemplo:

```
hostname(config)# interface ethernet0  
hostname(config-if)# ip address 10.10.10.200 255.255.0.0
```

1.3 Definir un nombre para la interface (hasta 48 caracteres). No se puede cambiar en el futuro.

```
nameif nombre
```

Ejemplo:

```
hostname(config-if)# nameif outside  
hostname(config-if)#
```

1.4 Habilitar la interface; por defecto, las interfaces están deshabilitadas.

Ejemplo:

```
hostname(config-if)# no shutdown  
hostname(config-if)#
```

2. Configurar la política ISAKMP

2.1 Especificá el método de autenticación y el conjunto de parámetros que se utilizarán durante la negociación de IKEv1.

La prioridad identifica de forma exclusiva la política de Intercambio de Claves de Internet (IKE) y asigna una prioridad a la política. Usá un número entero de 1 a 65.534, siendo 1 la prioridad más alta y 65.534 la más baja.

En los pasos que siguen, se establece la prioridad en 1.

2.2 Especificá el método de cifrado que se usará dentro de una política IKE.

Ejemplo:

```
crypto ikev1 policy priority encryption{aes-192 | aes-256 | | }
```

2.3 Especificá el algoritmo hash para una política IKE (también denominada variante HMAC).

hash de prioridad de política *crypto ikev1 {/ sha}*

Ejemplo:

```
hostname (config) # crypto ikev1 policy 1 hash sha
nombre de host (config) #
```

2.4 Especificá el grupo Diffie-Hellman para la política IKE: el protocolo criptográfico que permite al cliente IPsec y al ASA establecer una clave secreta compartida.

grupo de prioridad de política *crypto ikev1 {14 | El | El | 19 20 | 21}*

Ejemplo:

```
hostname (config) #crypto ikev1 policy 1 group 14
nombre de host (config) #
```

2.5 Especificá la duración de la clave de cifrado: la cantidad de segundos que debe existir cada asociación de seguridad antes de que caduque.

Cripto ikev1 prioridad de la política de por vida {segundos}

El rango para una vida útil finita es de 120 a 2147483647 segundos. Usá 0 segundos para una vida infinita.

Ejemplo:

```
nombre de host (config) # crypto ikev1 política 1 de por vida 43200
nombre de host (config) #
```

2.6 Habilitá ISAKMP en la interfaz nombrada fuera.

```
crypto ikev1 habilita nombre-interfaz
```

Ejemplo:

```
hostname (config) # crypto ikev1 enable outside  
nombre de host (config) #
```

2.7 Guardá los cambios en la configuración.

```
write memory
```

Configuración del cliente en el servidor.

3. Configurar pool de direcciones IP.

El ASA requiere un método para asignar direcciones IP a los usuarios. Esta sección utiliza grupos de direcciones como ejemplo.

3.1 Creá un grupo de direcciones con un rango de direcciones IP desde el cual el ASA asigna direcciones a los clientes.

```
ip local pool poolname first-address – last-address [máscara de máscara]
```

La máscara de dirección es opcional. Sin embargo, debe proporcionar el valor de la máscara cuando las direcciones IP asignadas a los clientes VPN pertenecen a una red no estándar y los datos podrían enrutarse incorrectamente si se utiliza la máscara predeterminada.

Un ejemplo típico es cuando el grupo local de IP contiene direcciones 10.10.10.0/255.255.255.0, ya que esta es una red de Clase A por defecto. Esto podría causar problemas de enrutamiento cuando el cliente VPN necesita acceder a diferentes subredes dentro de la red 10 a través de diferentes interfaces.

Ejemplo:

```
nombre de host (config) # grupo de pruebas de IP local 192.168.0.10-192.168.0.15  
nombre de host (config) #
```

4. Configuración de usuarios.

4.1 Cree un usuario, contraseña y nivel de privilegio.

```
username name {nopassword | password password [mschap | encrypted | nt-encrypted]}  
[SEP:][privilege priv_level]
```

Ejemplo:

```
Nombre de host (config) # username testuser password 12345678
```

Configuración del túnel en el servidor.

4.2 Generar IKEv1 o IKEv2 Poposal

Creá un conjunto de transformación IKEv1 o una propuesta IKEv2

Esta sección muestra cómo configurar un conjunto de transformación (IKEv1) o una propuesta (IKEv2), que combina un método de cifrado y un método de autenticación.

Configurá un conjunto de transformación IKEv1 que especifique el cifrado IPsec IKEv1 y los algoritmos hash que se utilizarán para garantizar la integridad de los datos.

```
crypto ipsec ikev1 transform-set transform-set-name método de cifrado [autenticación]
```

Utilizá uno de los siguientes valores para el cifrado:

- esp-aes to use AES with a 128-bit key.
- esp-aes-192 to use AES with a 192-bit key.
- esp-aes-256 to use AES with a 256-bit key.
- esp-null to not use encryption.

Utilizá uno de los siguientes valores para la autenticación:

- esp-md5-hmac to use the MD5/HMAC-128 as the hash algorithm.
- esp-sha-hmac to use the SHA/HMAC-160 as the hash algorithm.
- esp-none to not use HMAC authentication.

Ejemplo:

Para configurar un conjunto de transformación IKEv1 usando AES:

```
hostname (config) # crypto ipsec transform set FirstSet esp-aes esp-sha-hmac
```

4.3 Configurá un conjunto de propuestas IKEv2 que especifiquen el protocolo IPsec IKEv2, el cifrado y los algoritmos de integridad que se utilizarán.

esp especifica el protocolo IPsec de Encapsulating Security Payload (ESP) (actualmente el único protocolo compatible para IPsec).

```
crypto ipsec ikev2 ipsec-proposal proposal_name
```

```
protocol {esp} {encryption { | aes | aes-192 | aes-256 | } | integrity { | sha-1 }
```

Utilizá uno de los siguientes valores para el cifrado:

- aes para usar AES (predeterminado) con un cifrado de clave de 128 bits para ESP.
- aes-192 para usar AES con un cifrado de clave de 192 bits para ESP.
- aes-256 para usar AES con un cifrado de clave de 256 bits para ESP.

4.4 Usá uno de los siguientes valores para integridad:

sha-1 (predeterminado) especifica el Algoritmo de hash seguro (SHA) SHA-1, definido en el Estándar federal de procesamiento de información (FIPS) de EE. UU., para la protección de integridad ESP.

Para configurar una propuesta IKEv2:

Ejemplo:

```
nombre de host (config) # crypto ipsec ikev2 ipsec-proposal secure_proposal
nombre de host (config-ipsec-Proposition) # protocol esp encryption aes integrity sha-1
```

Definir Tunnel Group

Un grupo de túnel es una colección de políticas de conexión de túnel.

Configurá un grupo de túnel para identificar servidores AAA, especificá parámetros de conexión y definí una política de grupo predeterminada.

El ASA almacena grupos de túneles internamente.

Hay dos grupos de túneles predeterminados en el sistema ASA: DefaultRAGroup, que es el grupo de túneles de acceso remoto predeterminado; y DefaultL2Lgroup, que es el grupo de túneles de LAN a LAN predeterminado.

Podés cambiar estos grupos, pero no los elimines. El ASA usa estos grupos para configurar los parámetros de túnel predeterminados para el acceso remoto y los grupos de túnel de LAN a LAN cuando no se identifica un grupo de túnel específico durante la negociación del túnel.

4.5 Creá un grupo de túnel de acceso remoto IPsec (también denominado perfil de conexión).

Tipo de tipo de nombre de grupo de túnel

Ejemplo:

```
nombre de host (config) # túnel-grupo testgroup tipo ipsec-ra
nombre de host (config) #
```

4.6 Ingresá al modo de atributos generales del grupo de túnel donde puede ingresar un método de autenticación.

nombre-grupo-túnel atributos-generales

Ejemplo:

```
hostname (config) # tunnel-group testgroup general-atributos
nombre de host (config-tunnel-general) #
```

4.6 Especificá un grupo de direcciones para usar para el grupo de túnel.

address-pool [(interface name)] address_pool1 [...address_pool6]

Ejemplo:

```
hostname(config-general)# address-pool testpool
```

4.7 Ingresá al modo de atributos de ipsec del grupo de túnel donde pueden ingresar atributos específicos de IPsec para conexiones IKEv1.

tunnel-group name ipsec-attributes

Ejemplo:

```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-tunnel-ipsec)#
```

(Opcional) Configurá una clave previamente compartida (solo IKEv1). La clave puede ser una cadena alfanumérica de 1 a 128 caracteres.

Las claves para el dispositivo de seguridad adaptable y el cliente deben ser idénticas. Si un cliente Cisco VPN con un tamaño de clave previamente compartido diferente intenta conectarse, el cliente registra un mensaje de error que indica que no pudo autenticar al igual.

ikev1 pre-shared-key key

Ejemplo:

```
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx
```

5. Crear Crypto Map dinámico

Creá un mapa criptográfico dinámico

Los mapas criptográficos dinámicos definen plantillas de políticas en las que no se configuran todos los parámetros.

Esto permite que el ASA reciba conexiones de pares que tienen direcciones IP desconocidas, como clientes de acceso remoto.

Las entradas del mapa criptográfico dinámico identifican el conjunto de transformación para la conexión.

También se puede habilitar el enrutamiento inverso, que permite al ASA conocer la información de enrutamiento para los clientes conectados y anunciarla a través de RIP u OSPF.

5.1 Creá un mapa criptográfico dinámico y especificá un conjunto de transformación IKEv1 o una propuesta IKEv2 para el mapa.

Para IKEv1, usá este comando:

```
crypto dynamic-map dynamic-map-name seq-num set ikev1 transform-set transform-set-name
```

Para IKEv2, usá este comando:

```
crypto dynamic-map dynamic-map-name seq-num set ikev2 ipsec-proposal proposal-name
```

Ejemplo:

```
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet
hostname(config)#
```

```
hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal secure_proposal
hostname(config)#
```

5.2 (Opcional) Habilitá la inyección de ruta inversa para cualquier conexión basada en esta entrada de mapa criptográfico.

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set reverse-route
```

Ejemplo:

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse route
hostname(config)#
```

5.3 Creá una entrada de mapa criptográfico que use un mapa criptográfico dinámico.

```
crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name
```

Ejemplo:

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
```

5.4 Aplica el mapa criptográfico a la interfaz externa.

```
crypto map map-name interface interface-name
```

Ejemplo:

```
hostname(config)# crypto map mymap interface outside
```

5.5 Guarda los cambios en la configuración.

```
write memory
```

Fuente: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/vpn/asa-913-vpn-config/vpn-remote-access.html>