

Panasonic Electric Works España, S.A.

San Severo, 20, Barajas Park, 28042 Madrid, España Tel.:+34 902 414 140 • Fax: +34 913 292 976

Número	ITE0120092
Título	FPWEB. OpenVPN. Configurar PC como Servidor
Versión	1.0

0. Sobre Este Documento

Este documento tiene como único objetivo el facilitar la ejecución de las funciones más comunes. En ningún caso, este documento tiene carácter oficial ni se podrá responsabilizar a Panasonic por las erratas o información errónea contenida en el mismo. Panasonic declina toda responsabilidad por el uso de este documento

1. Descripción

Red propuesta y estación a configurar en este documento



La selección de un PC como servidor permite: Gestionar el acceso de los diferentes clientes (claves de acceso, asignación de IPs, seguridades,...)

Re direccionar la información entre los clientes entre sí

Antes de comenzar con la configuración del servidor es necesario instalar el software OpenVPN en el PC que hará de servidor y que tenga generados los certificados necesarios tanto para el servidor como para los diferentes cliente. Ver informe técnico

ITE0120091 FPWEB. OpenVPN. Creación de Certificados

Se requiere de un router con IP al que esté conectado el PC que se utilizará como servidor OpenVPN. Así mismo hay que enrutar el puerto 1194 a la IP de la LAN del servidor.

2.- Crear OpenVPN como Excepción de Firewall en Windows 7.

Compruebe que el software OpenVPN es una excepción del firewall.

Nota: Consulte a su asesor informático sobre la seguridad de su sistema y los posibles problemas que puede acarrear generar excepciones en el Firewall de Windows

1.- Seleccione Firewall de Windows del panel de control

Inicio \rightarrow Panel de control \rightarrow Firewall de Windows



2.- En el panel izquierdo, haga clic en Configuración avanzada. Si se le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación.

3.- En el cuadro de diálogo Firewall de Windows con seguridad avanzada, en el panel de la izquierda, haga clic en Reglas de entrada y, en el panel de la derecha, haga clic en Nueva regla.

4.- Siga los pasos del panel de la izquierda hasta finalizar la configuración.

4.1.- Tipo de regla → Programa



4.2.- Programa → Esta ruta de acceso del programa

Tras pulsar en siguiente, localice Openvpn.exe mediante el botón Examinar. Por defecto la ruta de acceso está localizada en

C:\ProgramFiles (x86)\OpenVPN\bin\openvpn.exe

P Asistente para nueva	regla de entrada
Programa	
Especifique la ruta completa	a y el nombre del archivo ejecutable del programa con el que coincide esta regla.
Pasos:	
Tipo de regla	¿Se aplica esta regla a todos los programas o a uno específico?
Programa	
Acción	Todos los programas
Perfil	La regla se aplica a todas las conexiones en el equipo que coinciden con otras propiedades de reglas.
Nombre	Esta ruta de acceso del programa:
,	%ProgramFiles% (x86)\OpenVPN\bin\openvpn.exe Examinar
	Ejemplo: c:\path\program.exe %Program.Files%\browser\browser.exe

4.3.- Acción → Permitir la conexión



4.4.- Perfil→ Según necesidades. En este ejemplo se aplica la excepción siempre

🔗 Asistente para nueva regla	a de entrada
Perfil Especifique los perfiles en los qu	e se va a aplicar esta regla.
Pasos: Tipo de regla Protocolo y puertos	¿Cuándo se aplica esta regla?
Acción Perfil	Dominio Se aplica cuando un equipo está conectado a su dominio corporativo.
 Nombre 	 Privado Se aplica cuando un equipo está conectado a una ubicación de redes privadas. Público Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

4.5.- Nombre → Asigne un nombre y unos comentarios que le permitan identificar la excepción

Nombre	
Especifique el nombre y la dese	ripción de esta regla.
Pasos:	
Tipo de regla	
Programa	
Acción	
Perfil	Nombre:
Nombre	OpenVPN
	Descripción (opcional):
	Excepción realizada para poder utilizar este PC como CLIENTE o SERVIDOR OpenVPN

3.- Crear Puerto 1194 como Excepción de Firewall en Windows 7.

Habilite como excepciones de Firewall el puerto 1194 en modo TCP o UDP o ambos. Para ello siga los mismos pasos que antes sólo que seleccionando:

1.- Tipo de regla → Puerto

Asistente para nueva reg Tipo de regla	jla de entrada
Seleccione el tipo de regla de f	ìrewall que desea crear.
Pasos:	(0.4 line de melo deurs envel
Tipo de regla	Carle ribo de legia desea crear :
 Protocolo y puertos Acción Perfil 	Programa Regla que controla las conexiones de un programa. Puente
Nombre	Regla que controla las conexiones de un puerto TCP o UDP.
-	Predefinida:
	Administración remota de Firewall de Windows
	Regla que controla las conexiones de una experiencia con Windows.
	Personalizada Regla personalizada.

2.- Protocolo y puertos → Seleccione modo TCP o UDP y el puerto de excepción 1194.

Protocolo y puertos Especifique los puertos y proto	colos a los que se aplica esta regla.
Pasos:	
Tipo de regla	¿Se aplica esta regla a TCP o UDP?
Protocolo y puertos	 • <u>I</u> CP
Acción	© <u>U</u> DP
Perfil	
 Nombre 	¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?
	Todos los puertos locales
	Puertos locales específicos: 1194
	E 1 00 440 5000 5010

4.- Enrutar Puerto 1194 en el Router a la IP del PC que será el Servidor

Esta acción depende de cada fabricante de Router.

Enrutar se conoce normalmente como NAT (Network Address Translation) consiste en redirigir toda la información entrante de internet que llegue por un determinado puerto (en nuestro caso el 1194) a un determinado equipo de la LAN (en nuestro caso el PC que se configurará como servidor OpenVPN)

Abra el puerto 1194 en el router y realice un NAT a la IP local del servidor 192.168.1.100

ACCESS SOLUTION	NAT	SITE M NAT - Edit SUA/NAT Server Set		SITE MAP		
inu			Start Port No.	End Port No.	IP Address	
ed Setup		1	All ports	All ports	0.0.0.0	
		2	1194	1194	192.168.1.100	
		3	0	0	0.0.0.0	
		4	0	0	0.0.0.0	

Nota: Ejemplo para router Zyxel

5.- Configuración Software OpenVPN en Modo Servidor

1.- Copiar en la carpeta *Config* donde haya instalado el OpenVPN los siguientes archivos:

C:\ProgramFiles(x86)\OpenVPN\Config

ca.crt	Certificado de autentificación raíz (CA)
server.key	Clave servidor
server.csr	Certificado servidor
dh1024.pem	Parámetros Fichero de Diffie Hellman

2.- Localice del directorio sample-config (C:\ProgramFiles(x86)\OpenVPN \ sample-config) el fichero de configuración ejemplo del servidor: server.ovpn y prepárese para editarlo y copiarlo en el directorio C:\ProgramFiles(x86)\OpenVPN\Config

Edite este documento y adáptelo a sus necesidades

Nota: No es objeto de este estudio profundizar en todas las funciones posibles del OpenVPN. Si desea más información acuda a <u>www.openvpn.net</u>

En nuestro caso hemos editado y nos hemos quedado con la siguiente configuración.

```
**********
# Ejemplo fichero de configuración servidor OpenVPN 2.0 #
# Comentarios con '#' o ';'
*****
                          # Puerto de acceso al router.
port 1194
                          # Modo de trabajo. TCP/UDP. Puerto 1194 Ha de ser
proto udp
                            excepción el firewall de Windows
dev tun
                          # Método de red OpenVPN Túnel IP
                          # Nombre del certificado CA
ca ca.crt
                          # Nombre del certificado del servidor
cert server.crt
                          # Nombre de la clave del servidor
key server.key
dh dh1024.pem
                          # Parámetros Diffie Hellman
server 10.8.0.0 255.255.255.0 # Direcciones IP a asignar dentro de la OpenVPN.
                            El Servidor es la 10.8.0.1
ifconfig-pool-persist ipp.txt # Generar fichero ipp.txt la primera vez para
                            asignar después las mimas IPs
client-to-client
                          # Permite a los clientes la comunicación entre
                            ellos
keepalive 10 120
                          # Ping cada 10 segundos y espera respuesta 120
                            segundos
cipher BF-CBC
                          # Tipo de cifrado Blowfish (es por defecto por lo
                            que no es necesario)
                          # Permitir la compresión de datos
comp-lzo
persist-kev
                          # Evitar acceso a recursos
persist-tun
                          # Evitar acceso a recursos
status openvpn-status.log
                          # Generar un fichero de estado de las conexiones
        openvpn.log
                          # Borrar el log al reiniciar la OpenVPN
loq
                          # Nivel de detalle del LOG
verb 3
mute 5
                          # Máximos mensajes secuenciales del tipo en el log
FTN
```

3.- Copie el fichero Server.ovpn editado anteriormente en el directorio

C:\ProgramFiles(x86)\OpenVPN\Config

4.- Inicialice el servidor. No necesita disponer de ningún cliente para iniciar el servidor

Ejecute el fichero Open VPN GUI (Inicio→ Programas→ OpenVPN) Aparecerá un icono en la barra de herramientas inferior de Windows Con el botón derecho sobre dicho icono seleccione "conectar"



Si hemos realizado el proceso adecuadamente, el icono pasará a tener un color verde indicando que el servidor está listo para que se conecten los clientes



Nota: El color verde no implica que los clientes estén conectados al servidor, sino que el servidor dispone de una configuración para que esto suceda

9.- Compruebe el estado del servidor

Realice un Ping al servidor y al cliente (10.8.0.1)

Inicio →Ejecutar → Cmd

C:\Documents and Settings\lapique≻ping 10.8.0.1	C:\Documents and Settings\lapique>ping 10.8.0.6
Haciendo ping a 10.8.0.1 con 32 bytes de datos:	Haciendo ping a 10.8.0.6 con 32 bytes de datos:
Respuesta desde 10.8.0.1: bytes=32 tiempo<1m TTL=128 Respuesta desde 10.8.0.1: bytes=32 tiempo<1m TTL=128 Respuesta desde 10.8.0.1: bytes=32 tiempo<1m TTL=128 Respuesta desde 10.8.0.1: bytes=32 tiempo<1m TTL=128	Tiempo de espera agotado para esta solicitud. Tiempo de espera agotado para esta solicitud. Tiempo de espera agotado para esta solicitud. Tiempo de espera agotado para esta solicitud.

La unidad responde afirmativamente

No se encuentra la unidad

Otra forma de comprobar el estado del servidor es monitorizando el log de estado de la red OpenVPN

Seleccione el icono 🍱 y con el botón derecho seleccione "Mostrar estado"

🔂 Conexión OpenVPN (server)	
Estado actual: Conectado.	
Tue Jun 04 13:07:59 2013 open_tun, tt->ipv6=0 Tue Jun 04 13:07:59 2013 TAP-WIN32 device [Conexión de área local 6] opened: \\\Global\{AE37F77B Tue Jun 04 13:07:59 2013 TAP-Windows Driver Version 9.9 Tue Jun 04 13:07:59 2013 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.8.0.1/255.255.25 Tue Jun 04 13:07:59 2013 Sleeping for 10 seconds Tue Jun 04 13:08:09 2013 Successful ARP Flush on interface [4] {AE37F77B-9C6A-4DFF-ACAF-FBA536 Tue Jun 04 13:08:09 2013 C\WINDOWS\system32\route.exe ADD 10.8.0.0 MASK 255.255.255.0 10.8.0.2 Tue Jun 04 13:08:09 2013 C\WINDOWS\system32\route.exe ADD 10.8.0.0 MASK 255.255.255.0 10.8.0.2 Tue Jun 04 13:08:09 2013 DDV4 link local (bound): [undef] Tue Jun 04 13:08:09 2013 UDV4 link local (bound): [undef] Tue Jun 04 13:08:09 2013 UDV4 link remote: [undef] Tue Jun 04 13:08:09 2013 IFCONFIG POOL: base=10.8.0.4 size=62, ipv6=0 Tue Jun 04 13:08:09 2013 succeeded -> ifconfig_pool_set() Tue Jun 04 13:08:09 2013 Succeeded -> ifconfig_pool_set() Tue Jun 04 13:08:09 2013 IFCONFIG POOL LIST Tue Jun 04 13:08:09 2013 INICONFIG POOL LIST Tue Jun 04 13:08:09 2013 INICON	H9C6A-4DFF-A 5.252 on interfa EB2E06}
Desconectar Reconectar	Ocultar

<u>Ayúdenos a Mejorar</u>

Si lo desea puede ponerse en contacto con nosotros en la siguiente dirección de correo:

soporte.tecnico@eu.panasonic.com

Si desea realizar cualquier consulta sobre este informe que no le haya quedado claro, indicar una errata, corregir la información o simplemente evaluar la utilidad de este informe, le rogamos que incluya en el asunto del mail el número del mismo.

Así mismo, estaremos encantados de atender sus solicitudes sobre futuros informes o acciones que considere que Panasonic debería realizar por lo que le ruego utilice este mail como buzón de sugerencias.