



Objetivo:

A través de este manual conocerás los pasos a seguir para configurar tu servicio de VPN SSL en la Nube Pública Empresarial Telmex.

Introducción:

El servicio de VPN SSL permite a usuarios remotos instalar y configurar la aplicación un cliente de VPN en su dispositivo (PC o Laptop) y a través de un túnel por el protocolo SSL o RDP conectarse de forma segura con los servidores virtuales de su Organización dentro de la Nube Publica Empresarial

PREREQUISITOS:

Para configurar tu VPN SSL es necesario contar con alguno de los siguientes navegadores web.

- Mozilla Firefox 78.0.1 (64-bit)
- Chrome (83.0.4103.116)

CONFIGURA TU SERVICIO DE VPN SSL



- Microsoft Edge Windows 10.
- Para instalar tu cliente ligero de VPN dentro de tu equipo PC o Lap top, es necesario que cuentes con alguno de los siguientes sistemas operativos:
 - Windows 8, 10 (incluida la opción Arranque seguro de Windows 10 activada)
 - Mac OS Sierra 10.12.6
 - Mac OS High Sierra 10.13.4
 - Mac OS Mojave De 10.14.2 a 10.14.6
 - Linux Fedora 26, 28
 - Linux CentOS 6.0, 7.5
 - Linux Ubuntu 18.04

Nota: Para Linux, es necesario tener instalados los servicios de seguridad de redes (NSS), TK y TCL

A) CONFIGURA TU CONEXIÓN DE VPN SSL

1. Ingresar al portal de VCloud Director y selecciona el VDC de tu organización.

UDN-VDC

Aplicaciones	CPU	Memoria	Almacenamiento
4 vApps	20 GHz	18 GB	614 GB
5 de 6 Máquinas virtuales en ejecución	pago por uso asignación ilimitada	pago por uso asignación ilimitada	pago por uso asignación ilimitada

UDN-Analytics

Aplicaciones	CPU	Memoria	Almacenamiento
1 de 1 vApps	4 GHz	2 GB	52 GB
1 de 1 Máquinas virtuales en ejecución	pago por uso asignación ilimitada	pago por uso asignación ilimitada	pago por uso asignación ilimitada

CONFIGURA TU SERVICIO DE VPN SSL



2. Accede a tu servicio de red Edge

Selecciona en el Panel lateral Izquierdo la Opción de Redes y da clic en Instancias Edge, esto te dará acceso a la opción de **Configurar Servicios**, da clic en la Organización sobre la que deseas configurar tu VPN.

Estado	Nombre	NIC utilizadas
✓	SATI-Edge	3
✓	UDN-VDC-ESG01	5

Configuración de puerta de enlace Edge

General

Nombre UDN-VDC-ESG01

Descripción

CONFIGURA TU SERVICIO DE VPN SSL



Al dar clic en Configurar Servicios, obtendrás acceso a las funcionalidades avanzadas del panel de configuración de tu servicio EDGE.

3. Configura tu Cliente SSL

Dentro del panel de configuración de tu servicio EDGE, selecciona las Opciones de VPN-Plus SSL y Configuración del cliente. Posteriormente asegúrate de que la opción de Modo de túnel se encuentre en la opción “Dividir” (Split)

Puerta de enlace Edge: UDN-VDC-ESG01

Firewall DHCP NAT Enrutamiento Equilibrador de carga VPN **VPN-Plus de SSL** Certificados Objetos de agrupamiento Estadísticas Configuración de Edge

Configuración general **Configuración del cliente** Usuarios Grupos de direcciones IP Paquetes de instalación Redes privadas Configuración del servidor Autenticación

Configuración del cliente VPN-Plus de SSL

Modo de túnel: Completo Dividir

Excluir subredes locales

Puerta de enlace predeterminada: _____

Habilitar reconexión automática

Notificación de actualización del cliente

Selecciona

CONFIGURA TU SERVICIO DE VPN SSL



B) GENERA TUS USUARIOS Y ASIGNA DIRECCIONAMIENTO IP A TU VPN

1. Crea tus Usuarios de VPN.

Dentro del panel de configuración de tu servicio EDGE, en la opción de VPN-Plus SSL, selecciona el submenú “Usuarios” y da clic en el símbolo de “+” para crear un nuevo permiso de Usuario.

Puerta de enlace Edge: UDN-VDC-ESG01

Firewall DHCP NAT Enrutamiento Equilibrador de carga VPN **VPN-Plus de SSL** Certificados Objetos de agrupamiento Estadísticas Configuración de Edge

Configuración general Configuración del cliente **Usuarios** Grupos de direcciones IP Paquetes de instalación Redes privadas Configuración del servidor Autenticación

Usuarios de VPN-Plus de SSL

+

ID de usuario	Nombre
udntest	
udnuser	Usuario

Detalles de usuario de udntest

ID de usuario	udntest	La contraseña
Descripción		Permitir el
Estado	Habilitado	Cambiar el

Al dar clic en el símbolo de “+”, te aparecerá un formulario que deberás llenar con los datos del usuario, contraseña, y opcionalmente Nombre, Apellido y Descripción, y cuatro opciones más que puedes habilitar o deshabilitar para adecuar el manejo de contraseñas con tus preferencias, posteriormente da clic en el botón conservar

CONFIGURA TU SERVICIO DE VPN SSL



Crear nuevo usuario

ID de usuario *

Contraseña *

Vuelva a escribir la contraseña *

Nombre

Apellido

Descripción

Habilitado

Detalles de la contraseña

La contraseña nunca caduca

Permitir cambio de contraseña

Cambiar contraseña la próxima vez que se inicie sesión



2. Asigna un grupo de direcciones IPs para tu VPN.

Dentro del panel de configuración de tu servicio EDGE, en la opción de VPN-Plus SSL, selecciona el submenú “Grupo de direcciones IP” y da clic en el símbolo de “+” para dar de alta el pool de direcciones IP privadas que serán asignadas a cada cliente de VPN.


Puerta de enlace Edge: UDN-VDC-ESG01

Firewall DHCP NAT Enrutamiento Equilibra dor de carga VPN VPN-Plus de SSL Certificados Objetos de agrupamiento

Configuración general Configuración del cliente Usuarios **Grupos de direcciones IP** Paquetes de instalación Redes privadas Con

Grupos de direcciones IP de VPN-Plus de SSL

Rango de IP Puerta de er



Nota; Este pool deberá ser distinto y no deberá traslaparse con las direcciones IP asignadas a los servidores virtuales dentro de su DCV, el siguiente ejemplo permite asignar el rango de IPs

CONFIGURA TU SERVICIO DE VPN SSL



de 10.10.10.1 al 10.10.10.10, asegúrate de introducir la máscara de red y la puerta de enlace de tu servicio y da clic en conservar.

Editar grupo de direcciones IP ×

Rango de IP *	<input type="text" value="10.10.10.1-10.10.10.10"/>
Máscara de red *	<input type="text" value="255.255.255.0"/>
Puerta de enlace *	<input type="text" value="10.10.10.1"/>

Esto agregará una dirección IP a la interfaz de na0

Descripción

Estado

Avanzado


DNS primario

DNS secundario

Sufijo DNS

Ejemplo: engvmware.com

Servidor WINS



C) PREPARA EL PAQUETE DE INSTALACIÓN DE TU VPN

En este paso debes configurar los parámetros que el cliente VPN utilizará para establecer conexión con tus servicios, como son: dirección IP, el puerto al que se conectarán los clientes y el tipo de sistema operativo donde se instalará el cliente VPN.

Antes de iniciar con la configuración de tu paquete de instalación, asegúrate de identificar la dirección IP pública asignada al VDC de tu servicio, esta dirección la puedes encontrar en la opción de Redes-> Instancias Edge en el apartado de Direcciones IP.

CONFIGURA TU SERVICIO DE VPN SSL



The screenshot shows the 'Instancias de Edge' page in the Nube Telmex interface. The left sidebar has 'Instancias de Edge' highlighted. The main content area shows a table of edge instances:

Estado	Nombre	NIC utilizadas
✓	SATI-Edge	3
✓	UDN-VDC-ESG01	5

An orange arrow points to the 'UDN-VDC-ESG01' instance. Below the table, the 'Configuración de puerta de enlace Edge' section is visible, showing the 'Nombre' as 'UDN-VDC-ESG01'. At the bottom, a table shows network configurations:

Redes externas	Sub redes	Direcciones IP
INTERNET	201.161.100/24	201.161.100.100

An orange arrow points to the IP address '201.161.100.100' in the 'Direcciones IP' column.

1. Preparar paquete de instalación de VPN SSL.

Una vez que lograste identificar tu IP pública dirígete al panel de configuración de tu servicio EDGE, en la opción de VPN-Plus SSL y selecciona el submenú "Paquetes de instalación".

Puerta de enlace Edge: UDN-VDC-ESG01

The screenshot shows the 'VPN-Plus de SSL' configuration page. The 'Paquetes de instalación' sub-menu is highlighted. Below the sub-menu, there are three buttons: '+', '🔗', and '✕'. The '+' button is highlighted with a red box and an orange arrow. Below the buttons, a table shows the configuration for the 'VPN UDN' profile:

Nombre del perfil	Estado
VPN UDN	Habilitado

CONFIGURA TU SERVICIO DE VPN SSL



2. Introduce los parámetros de configuración de tu cliente VPN

Para iniciar con la configuración de tu paquete de instalación da clic en el símbolo de “+” y proporcionar un nombre al perfil, La dirección IP Publica Identificada en el paso anterior y el puerto de escucha y da clic en conservar.

Adicionalmente puedes seleccionar el tipo de sistema operativo y algunos parámetros de configuración en caso de que el paquete de instalación sea preparado para sistemas operativos Windows.

Agregar paquete de instalación

Nombre de perfil ⁺ VPN UDN

Puerta de enlace	Puerto
Re llenar nombre de host	8443

Crear paquetes de instalación para

Windows

Linux

Misc

Descripción

Habilitado

Parámetros de instalación de Windows

Iniciar cliente al iniciar sesión Ocultar icono de la bandeja del sistema del cliente

Permitir recordar la contraseña **Crear icono en el escritorio**

Habilitar instalación en modo silencioso Habilitar funcionamiento en modo silencioso

Ocultar adaptador de red del cliente SSL **Validación del certificado de seguridad del servidor**

Nota: Si el usuario pretende publicar servicios Web vía https, se recomienda utilizar un puerto distinto al TCP 443 en este ejemplo emplearemos el puerto **8443** el cual ya cuenta con los permisos abiertos.

CONFIGURA TU SERVICIO DE VPN SSL



3. Prepara tu red privada para acceso VPN.

Para lograr el cifrar de tu información a través del túnel de VPN, debes asegurarte de asociar la red privada donde viven tus Máquinas Virtuales con tu VPN.

Dentro del panel de configuración de tu servicio EDGE, en la opción de VPN-Plus SSL, selecciona el submenú “Redes Privadas” y da clic en el símbolo de “+”.

Puerta de enlace Edge: UDN-VDC-ESG01

Firewall DHCP NAT Enrutamiento Equilibrador de carga VPN **VPN-Plus de SSL** Certificados Objetos de agrupamiento

Configuración general Configuración del cliente Usuarios Grupos de direcciones IP Paquetes de instalación **Redes privadas** Con

Redes privadas de VPN-Plus de SSL

+

Red Puertos Enviar a través del túnel

Para dar de alta el segmento de red con el que se establecerá comunicación debes proporcionar la Red donde viven tus Máquinas Virtuales en formato CIDR, (en este caso se consideró 10.10.20.0/24) y asegúrate de activar la casilla de Envío de tráfico a través de túnel y de mantener el estado del servicio activo y da clic en conservar.

Agregar red privada

Red * 10.10.20.0/24

La red se debe escribir con el formato CIDR, por ejemplo, 192.169.1.0/24

Descripción

Enviar tráfico

A través del túnel

Habilitar optimización de TCP

Puertos

Estado

DESCARTAR CONSERVAR

CONFIGURA TU SERVICIO DE VPN SSL



4. Iniciar servicio de VPN.

Dentro del panel de configuración de tu servicio EDGE, en la opción de VPN-Plus SSL, selecciona el submenú “Configuración del servidor”.

Puerta de enlace Edge: UDN-VDC-ESG01



Dentro de la Opción configurar servidor asegúrate de activar la opción de “Habilitado”, posteriormente selecciona la dirección IP pública de tu EDGE e indica el puerto del servicio y el tipo de cifrado que utilizará el túnel de VPN.

Nótese que la dirección IP pública es la 201.161.XX.XX, que es la misma definida en tu EDGE en la opción de Redes-> Instancias Edge en el apartado de Direcciones IP.

Configuración del servidor

La configuración del servidor representa los ajustes relacionados con

Habilitado	<input checked="" type="checkbox"/>
Dirección IP	201161120.29 (principal) ▾
Puerto	8443
Lista de cifrado	
AES128-SHA	<input type="checkbox"/>
AES256-SHA	<input checked="" type="checkbox"/>
DES-CBC3-SHA	<input type="checkbox"/>

Política de registro

Habilitar registro	Habilitado <input checked="" type="checkbox"/>
Nivel de registro	Aviso ▾

CONFIGURA TU SERVICIO DE VPN SSL



D) CONFIGURA TU SERVICIO DE FIREWALL

Para configurar tus reglas de firewall debes considerar el direccionamiento IP que definiste para tu VPN, en este ejemplo se asignó el siguiente direccionamiento:

Clientes de VPN 10.10.10.1 al 10.10.10.10 /24
Servidores Virtuales 10.10.20.0 /24

Dentro de la opción de Firewall debes asegurarte de agregar una regla que permita comunicar tus clientes de VPN (origen) con la red de tus Máquinas Virtuales (destino).

Red Origen	Red Destino	Puertos y Servicios	Regla
10.10.10.0/24	10.10.20.0/24	ICMP RDP (TCP 3389) SSH (TCP 22) HTTP (80) HTTPS (8443)	Permitir

1. Configura las reglas de acceso de tu Firewall

Selecciona en el Panel lateral Izquierdo la Opción de Redes y da clic en Instancias Edge, esto te dará acceso a la opción de **Configurar Servicios**, da clic en la Organización sobre la que configuraste tu VPN.

Instancias de Edge

CONFIGURAR SERVICIOS CONVERTIR EN AVANZADA VOLVER A IMPLEMENTAR

Estado	Nombre	NIC utilizadas
✓	SATI-Edge	3
✓	UDN-VDC-ESG01	5

Selecciona

CONFIGURA TU SERVICIO DE VPN SSL

Nube Telmex Centros de datos

Todos los centros de datos

Instancias de Edge

CONFIGURAR SERVICIOS

Accede

Estado	Nombre
✓	SATI-Edge
✓	UDN-VDC-ESG01

Configuración de puerta de enlace Edge

General

Nombre UDN-VDC-ESG01

Descripción

Al dar clic en Configurar Servicios, obtendrás acceso a las funcionalidades avanzadas del panel de configuración de tu servicio EDGE. Selecciona la opción de Firewall.

Puerta de enlace Edge: UDN-VDC-ESG01

Firewall DHCP NAT Enrutamiento Equilibrador de carga VPN VPN-Plus de SSL Certificados Objetos de agrupamiento

Reglas de firewall

Habilitado

+ x ↑ ↓

Mostrar solo reglas definidas por el usuario

N.º	Nombre	Tipo	Origen	Destino
-----	--------	------	--------	---------

2. Da clic en el símbolo de “+” y agrega la nueva regla de firewall configurando de tu servicio.

CONFIGURA TU SERVICIO DE VPN SSL



Habilitado



Mostrar solo reglas definidas por el usuario

N.º	Nombre	Tipo	Origen	Destino	Servicio	Acción
1✓	dns	Alto interno	internal	10.10.20.1 192.168.10.1	udp:53:any tcp:53:any	Aceptar
2✓	vpn-cliente	Usuario	10.10.10.1-10.10.10.10	10.10.20.0/24	icmp:any:any tcp:any:3389	Aceptar

3. Introduce el nombre de tu cliente vpn

Habilitado



Mostrar solo reglas definidas por el usuario

N.º	Nombre
1✓	dns
2✓	VPN-Cliente

4. Agrega el origen, da clic "IP" para agregar el origen.

Origen

internal

Any

Dirección IP de origen

Valor:

10.10.10.1-10.10.10.10

Los valores válidos pueden ser dirección IP, CIDR o rango de IP.

DESCARTAR

CONSERVAR

Puedes dar clic en el símbolo de "+" si deseas agregar una red ya existente.

CONFIGURA TU SERVICIO DE VPN SSL



Seleccionar objetos

Examinar objetos del tipo: **Interfaces de puerta de enl** ▾
INTERFACES DE PUERTA DE ENLACE ▶

Filtrar...

- INTERNET
- RED-PRODUCCION
- RESPALDOS-BAAS2
- SERVICIOS
- LAN
- Internal
- External
- ALL

Página actual: 1

DESCARTAR CONSERVAR

5. Agrega un destino, da clic en “IP” para agregar el destino.

Destino

- 10.10.20.1
- 192.168.10.1
- Any

IP +

Dirección IP de destino

Valor: 10.10.20.0/24

Los valores válidos pueden ser dirección IP, CIDR o rango de IP.

DESCARTAR CONSERVAR

Puedes dar clic en el símbolo de “+” si deseas agregar una red ya existente.

6. Agrega los permisos (servicios) que serán permitidos por el firewall dando clic en el símbolo de “+”.

i. Agregamos permiso Any to Any en el protocolo ICMP

Servicio

- udp:53:any
- tcp:53:any
- Any

+

Agregar servicio

Protocolo: ICMP ▾

Puerto de origen: any

Puerto de destino: any

Si se deja el campo en blanco, la regla se aplicará a cualquier puerto

DESCARTAR CONSERVAR

CONFIGURA TU SERVICIO DE VPN SSL



- ii. Agregamos puerto 8443 para acceso vía ssh o 3389 para acceso vía RDP (escritorio remoto), y da clic en conservar.

Agregar servicio

Protocolo TCP

Puerto de origen any

Puerto de destino 8443

DESCARTAR CONSERVAR

Agregar servicio

Protocolo TCP

Puerto de origen any

Puerto de destino 3389

DESCARTAR CONSERVAR

7. Una vez configuradas las políticas de firewall, de clic en la opción de Guardar Cambios

Guardar cambios Descartar cambios

CONFIGURA TU SERVICIO DE VPN SSL



E) DESCARCA TU CLIENTE VPN Y ACCEDE A TU SERVICIO

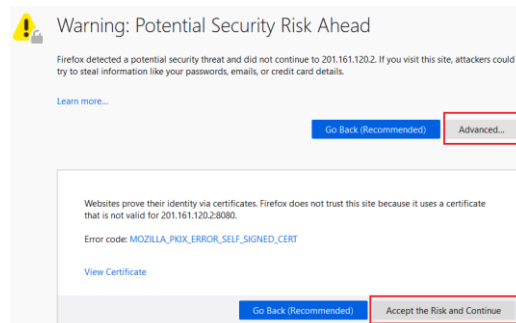
1. Descarga y Configura tu Cliente de VPN en tu equipo de cómputo

Para instalar el cliente de VPN es necesario descargar el cliente de VPN SSL accediendo desde tu navegador web a la IP pública que declaraste en tu servicio de VPN en el punto 4, apartado C) de esta guía (201.161.XX.XX), en el puerto de acceso VPN definido, (en este caso el 8443).

Ejemplo: <https://201.161.XX.XX:8443>

Debido a que el certificado generado es auto firmado (self signed) mostrará una advertencia de seguridad.

- Para Mozilla Firefox seleccione **Advanced** y posteriormente **Accept the Risk and Continue**



- Para Chrome seleccione **Advanced** y posteriormente **Proceed to 201.161.120.2 (unsafe)**



Your connection is not private

Attackers might be trying to steal your information from **201.161.120.2** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_COMMON_NAME_INVALID

Help improve Chrome security by sending [URLs of some pages you visit](#), limited system information, and some page content to Google. [Privacy policy](#)

Hide advanced

Back to safety

This server could not prove that it is **201.161.120.2**; its security certificate is from ***,triarra.com**. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 201.161.120.2 \(unsafe\)](#)

CONFIGURA TU SERVICIO DE VPN SSL



- Para Microsoft Edge Seleccione **Details** y Seleccione **Go on to the webpage (Not recommended)**
2. Introduzca el usuario y contraseña creados en el paso 4 de esta Guía.

vmware SSL VPN-Plus

Portal Login

Enter your login credentials here

User Name

Password

3. Seleccione el Perfil creado que desea descargar, (en este ejemplo se descarga el instalador de Windows vpntest)

vmware SSL VPN-Plus

Full Access Tools

Full Access

Available Network Extension clients.

List	Description
vpntest	Download full access client (PHAT Client)
VPNMAC	Download full access client (PHAT Client)

SSL VPN-Plus

VMware Full Access Client (PHAT) Download page

Profile Name: vpntest
Version : v6.4.0

Please [click here](#) to download the installer.

4. Descomprima el archivo instalador una vez descargado y ejecute el archivo Insstaller.exe

CONFIGURA TU SERVICIO DE VPN SSL



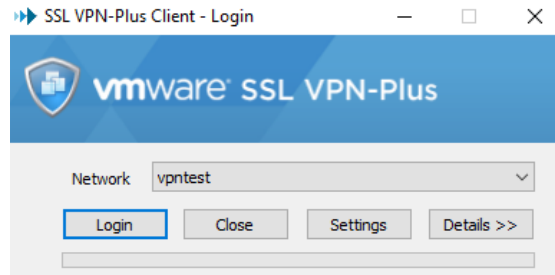
VMware_VPN_Client-Setup.zip - ZIP archive, unpacked size 2,950,066 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
connected.ico	355,574	22,276	Icon	4/11/2019 12:0...	E28F87AC
desktopconnected.ico	355,574	22,276	Icon	4/11/2019 12:0...	E28F87AC
disconnected.ico	4,286	256	Icon	4/11/2019 12:0...	CA481AF5
errorconnected.ico	1,406	496	Icon	4/11/2019 12:0...	CEE9F2D7
Installer.exe	60,032	31,835	Application	4/11/2019 12:0...	55E7DED7
InstallerRes_040c.dll	52,352	24,756	Application extens...	4/11/2019 12:0...	9DEC3B13
InstallerRes_0407.dll	52,864	24,789	Application extens...	4/11/2019 12:0...	E27B0A65
InstallerRes_0409.dll	50,304	24,418	Application extens...	4/11/2019 12:0...	4B6CB40A
InstallerRes_0411.dll	48,256	24,344	Application extens...	4/11/2019 12:0...	A38364D0
InstallerRes_0412.dll	47,744	24,329	Application extens...	4/11/2019 12:0...	359D887D
InstallerRes_0804.dll	45,696	23,972	Application extens...	4/11/2019 12:0...	4475A554
naconf.cfg	52	52	CFG File	7/2/2020 5:02 ...	E92A1830
nafiles.exe	1,611,152	1,594,245	Application	4/11/2019 12:0...	7E4A1344
nainstaller.exe	135,808	65,854	Application	4/11/2019 12:0...	8D5649E3
phat_banner.bmp	85,318	9,381	BMP File	4/11/2019 12:0...	5C439C17
upgrade.exe	43,648	23,360	Application	4/11/2019 12:0...	85210D2C

CONFIGURA TU SERVICIO DE VPN SSL



5. Una vez instalado el cliente, abrirlo y seleccionar la opción **login**



6. Introduzca las credenciales de usuario generadas en el punto 4 de esta guía y verifique que su conexión es correcta.

Para validar las direcciones IP asignadas al cliente y los pools para cifrar tráfico, puede abrir el icono de la barra de tareas, y seleccionar **Statistics, Connection Information**; al abrir la ventana emergente, seleccione **Advanced**.

Red de Servidores Virtuales dentro del Centro de Datos

IP Asignada al Cliente de VPN

General **Advanced**

Gateway Hostname

Network configuration

Gateway IP Address

Port **IP Pública 8443**

Tunnel Mode Split Tunnel

Private Subnets **10.10.20.0/255.255.255.0**

Exclude Subnets No subnets configured

Compression Disabled

Adapter Details

Virtual IP **10.10.10.1**

Network 10.10.10.0

Netmask 255.255.255.0

OK Cancel