

# CONFIGURA TU VPN EN ROUTER CISCO

## CISCO NETWORKING

*Muchas organizaciones necesitan proteger sus datos cuando estos se envían a la Internet*

**Cisco Networking**

---

---

# Contenido

Por que utilizar una VPN	1
Prueba tus habilidades (topologia General)	2
Configuración	3
Información de contacto	6

## Por que utilizar una VPN

---

### Las organizaciones necesitan proteger sus datos

Muchas organizaciones necesitan proteger sus datos cuando estos se envían a la Internet, se sabe que muchas organizaciones utilizan enlaces privados dedicados de alta velocidad y que estos brindan seguridad a los datos que fluyen por dichos enlaces, pero también existe conexiones que van directamente a la Internet pasando por un proveedor de servicios (ISP) para este tráfico de datos no existe protección alguna, allí es donde entra en juego la **VPN (Red Privada Virtual)** una tecnología ampliamente utilizada para dar seguridad a los datos que se envían a la Red de Redes, las VPN crean un túnel privado encriptado con tecnología como la **IPsec** para dar seguridad a las conexión o flujo de datos, este túnel o tunneling se realiza en la red pública (Internet) es decir, haces de la red pública una red privada.

Muchas personas utilizan las VPN para conectarse a una empresa u organización que solo permite conexiones establecidas en su propio lugar geográfico, aprovechando las características de funcionamiento que tienen los servicios VPN.

Por ejemplo; si se conecta a una organización que se encuentra en un **país A** desde un **país B** utilizando un servidor VPN que se encuentra ubicado en el **país A**, la empresa u organización solo ve establecida la conexión entre el servidor VPN y sus servicios locales, la conexión establecida desde el **país B** hacia el servidor VPN en el **país A** no la detecta la empresa u organización, esto hace que se permita el registro de las personas que se conectan remotamente por considerarlas provenientes del mismo país.

En mi opinión personal las VPN nunca se crearon para este fin, fueron creadas para establecer una conectividad segura a través de un túnel cifrado que permita pasar por servicios públicos (Internet) un flujo de datos sin que estos sean comprometidos.

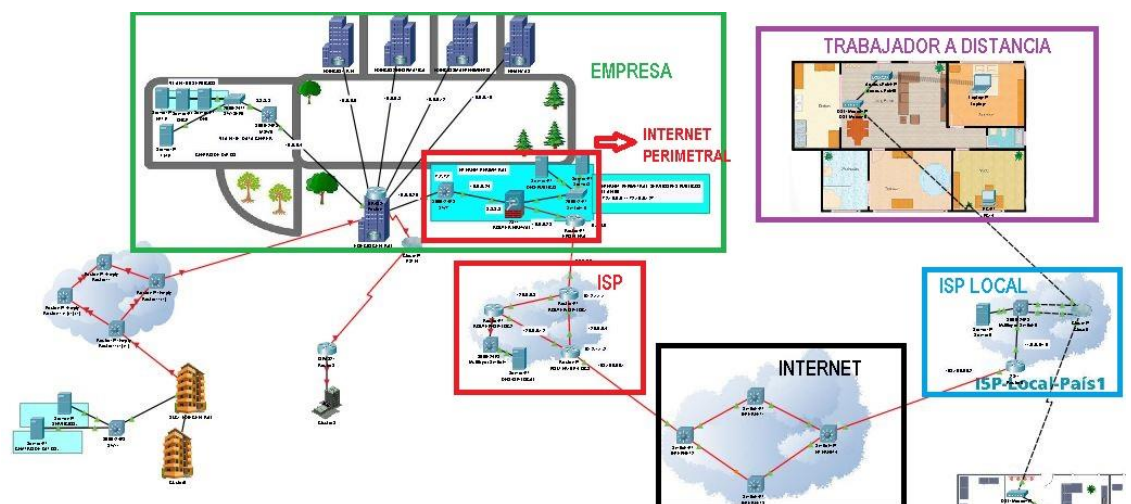
### ¿Por qué una organización utiliza la Internet?

Una organización que se extiende por el mundo puede tener una cantidad considerable de trabajadores en diferentes condiciones aquellos que son presenciales y los que son a distancia, en el caso de los trabajadores presenciales las empresas establecen un perímetro en la red que se encarga de vigilar constantemente el tráfico que estos generan, la ventaja para la empresa u organización es que el trabajador presencial está dentro de la Intranet y es muy fácil proteger

los datos ya que estos deben atravesar todo el perímetro de seguridad interno, en el caso de los trabajadores a distancia es un poco difícil pero toda la tecnología de seguridad creada hasta ahora permite verlo realmente posible, la desventaja más grande que se puede ver para la empresa es que el trabajador a distancia se encuentra en cualquier parte del mundo y que dicho trabajador utiliza la Internet para conectarse, esto se debe a que por lo general en los hogares se cuenta con medios como el DSL para la conexión a Internet, cuando nos conectamos por este medio u otro siempre lo hacemos a través de un proveedor de servicios (ISP) local, este proveedor debería estar localizado en el mismo país donde se encuentra el trabajador, sin embargo dicho trabajador primero debe conectarse al proveedor y luego este lo redirige a la red de la empresa, algunos ISP protegen los datos de sus clientes por motivos de reglamento interno y a través de algún ente Internacional pero como la Internet está basada en Proveedores de servicios interconectados en todos el mundo, después que tus datos salen del ISP local dicho ISP no se hace responsable de lo que pueda pasar más allá, es decir, de lo que pueda pasar en la Internet ese mundo que es un territorio de nadie y que está lleno de lobos cibernéticos muy hambrientos algunos aprendices y otros muy expertos, es por esta razón que es necesario utilizar una **VPN de acceso remoto** para que el trabajador a distancia acceda a la red empresarial y que los datos no sean alterados en el trayecto comprometiendo la seguridad de la empresa.

## Prueba tus habilidades y configura una VPN de Acceso Remoto en Router 2811

### Topología General



La conexión presente en esta topología involucra la red empresarial conectada al ISP que le brinda el servicio de conexión a Internet, se puede decir que este es el enlace público de la empresa, la configuración de la VPN de acceso remoto se realizará en el Router 2811 ubicado en el Internet perimetral, el ISP que conecta a la empresa da salida a Internet, si vemos la topología desde el punto de vista del trabajador a distancia se puede notar que este está conectado a su proveedor de servicio local y a su vez le proporciona salida a Internet, la idea de crear una VPN de Acceso Remoto es para crear un túnel privado y proporcionar una conexión segura entre la empresa y el trabajador a distancia para así no comprometer la seguridad de la empresa.

## **Configuración**

### **Creamos un POOL de direcciones que serán asignadas a los usuarios**

```
RouterFirewall(config)#IP local pool poolvpn 172.16.1.10 172.16.1.20
```

### **Establecemos un Nuevo modelo AAA**

```
RouterFirewall(config)#aaa new-model
```

### **Definimos el método de Autenticación**

```
RouterFirewall(config)#aaa authentication login usuariosvpn local
```

### **Restringimos los parámetros que niegan el acceso de usuarios a la red**

```
RouterFirewall(config)#aaa authorization network pdvvpn local
```

### **Si la autenticación la generamos de manera local creamos los usuarios en el dispositivo**

```
RouterFirewall(config)#username michely secret cisco
```

```
RouterFirewall(config)#username jose secret cisco
```

### **Generamos una nueva política IKE**

```
RouterFirewall(config)#crypto isakmp policy 10
```

```
RouterFirewall(config-isakmp)#encryption aes 256
```

**Algoritmo de generación de hash puede ser también md5**

```
RouterFirewall(config-isakmp)#hash sha
```

**Esta es la autenticación de clave compartida**

```
RouterFirewall(config-isakmp)#authentication pre-share
```

**Identificador de grupo diffie hellman**

```
RouterFirewall(config-isakmp)#group 5
```

**Grupo IKE para los clientes vpn**

```
RouterFirewall(config-isakmp)#crypto isakmp client configuration group pdvvpn
```

**Generamos la clave**

```
RouterFirewall(config-isakmp-group)#key cisco
```

**Identificamos el pool de direcciones**

```
RouterFirewall(config-isakmp-group)#pool poolvpn
```

**Establecemos las políticas de seguridad que se van a utilizar**

```
RouterFirewall(config-isakmp-group)#crypto ipsec transform-set setvpn esp-aes esp-sha-hmac
```

**Establecemos un mapa dinámico crypto que será utilizado si se desconoce la IP del host remoto.**

```
RouterFirewall(config)#crypto dynamic-map dinamicovpn 10
```

**Asociamos el transform set al mapa dinámico**

```
RouterFirewall(config-crypto-map)#set transform-set setvpn
```

**Activamos el route inverso**

```
RouterFirewall(config-crypto-map)#reverse-route
```

**Configuramos un mapa dinámico crypto para signarlo a la interfaz**

```
RouterFirewall(config-crypto-map)#crypto map mapavpn client configuration address respond
```

```
RouterFirewall(config)#crypto map mapavpn client authentication list usuariosvpn
```

```
RouterFirewall(config)#crypto map mapavpn isakmp authorization list grupovpn
```

```
RouterFirewall(config)#crypto map mapavpn 20 ipsec-isakmp dynamic dinamicovpn
```

**Configuramos la interfaz externa que va realizar la respuesta**

```
RouterFirewall(config)#interface f0/0
```

```
RouterFirewall (config-if)#crypto map mapavpn
```

## Información de contacto

---



**Michely Lopez**

[Ingmjls.14@gmail.com](mailto:Ingmjls.14@gmail.com)

YouTube

<http://www.youtube.com/c/GuerrerosdelaRedMichelyLopez>

---

Cisco Networking

