Configuración básica de VPN LAN-2-LAN con routers.

Routers: Cisco ISR-2811
IOS Image: c2800nm-advipservicesk9-mz.124-22.T5.bin
Nota: Estas pruebas fueron realizadas en un entorno de Laboratorio.

Topología:

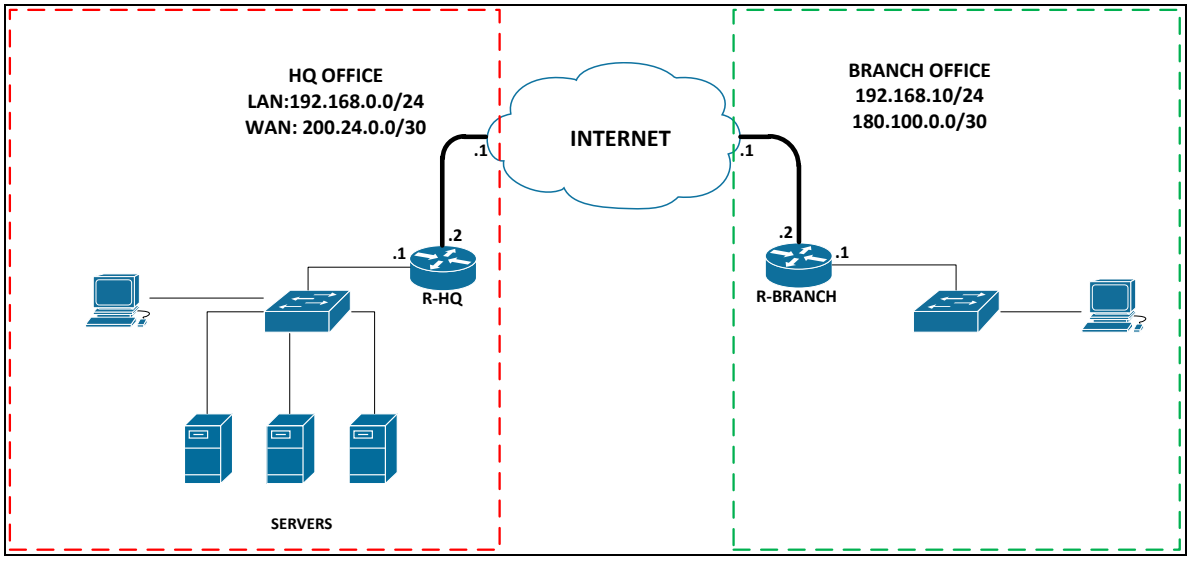

Figura 1. Topología

Antecedente y Requerimientos:

- Los Routers *R-HQ* y *R-BRANCH* debe ser configurado con NAT de manera que las redes LAN tengan conexión hacia internet.

- Los routers en cada una de las sedes no cuentan con ningún protocolo de enrutamiento definido. De manera que el tráfico se envía hacia internet mediante rutas de último recurso definidas así:

  R-HQ(config)#ip route 0.0.0.0 0.0.0.0 200.24.0.1

  R-BRANCH(config)#ip route 0.0.0.0 0.0.0.0 180.100.0.1

- Se debe crear un Túnel VPN entre las dos sedes de manera que la *BRANCH OFFICE* tenga acceso a los servidores ubicados en los *HQ*.

Definiciones:

Inicialmente se deben definir los parámetros que se usarán para establecer el túnel VPN. Para establecer un túnel VPN es necesario que se lleven a cabo dos fases de negociación IKE (Internet Key Exchange) Fase 1 y 2.

1. ***IKE fase 1:*** Esta fase es la encargada de establecer un canal autenticado de comunicación. Para esto utiliza el Algoritmo de Diffie-Hellman el cual es asimétrico y permite el intercambio seguro de llaves simétricas como DES, 3DES, AES o SEAL las cuales son utilizada para encriptar el tráfico entre los pares en la fase 2.

   La autenticación para este protocolo se puede realizar por medio de claves Pre-Compartidas (Pre-Shared Key) o de Certificados.

   Puede operar en *Main Mode* o en *Aggresive Mode*, donde la primera protege la identidad de los pares, la segunda no.

   Parámetros disponibles para IKE ph1:
   - Authentication: Pre-Shared Keys, RSA-Encryption, RSA-Signature
   - Encryption Algorithm: DES, 3DES, AES [128, 192, 256]
   - Key Exchange: DH-Group1 [768-bit], DH-Group 2 [1024-bit], DH-Group 5 [1536-bit]
   - Hashing: MD5, SHA-1.

2. ***IKE fase 2:*** En esta fase los pares hacen uso del canal seguro establecido en la fase 1 para compartir las claves simétricas con las cuales se encriptará el trafico.

   Parámetros disponibles para IKE ph2:

   - Encryption Algorithm: esp-des, esp-3des, esp-aes [128, 192, 256], esp-seal, esp-null.
   - Authentication: ah-md5-hmac, ah-sha-hmac, esp-md5-hmac, esp-sha-hmac.

Definicion de Parametros:

- ***IKE ph1:***
  Authentication: Pre-shared key.
  Encryption Algorithm: AES-128
  Key Exchange: DH-Group2 [1024-bit]
  Hashing: SHA-1

- ***IKE ph2:***
  Encryption Algorithm: esp-aes-128
  Authentication: esp-sha-hmac

Configuraciones:

- ***Configuración de NAT:***

1. Asumiendo que las direcciones IP estan configuradas, se debe crear una lista de acceso para definir a que IPs se le aplicara el NAT.

R-HQ(config)#ip access-list standard NAT-LIST
R-HQ(config-std-nacl)#permit 192.168.0.0 0.0.0.255
R-HQ(config-std-nacl)#deny any

R-BRANCH(config)#ip access-list standard NAT-LIST
R-BRANCH(config-std-nacl)#permit 192.168.1.0 0.0.0.255
R-BRANCH(config-std-nacl)#deny any

2. Se define en cual sentido se llevará a cabo el proceso de traducción. Para este caso solo se cuenta con una IP pública.

R-HQ(config)#ip nat inside source list NAT-LIST interface gigabitEthernet 0/1

R-BRANCH(config)#ip nat inside source list NAT-LIST interface gigabitEthernet 0/1

3. Se define que interfáz será la interior y cual la exterior.

R-HQ(config)#interface gigabitEthernet 0/0
R-HQ(config-if)#ip nat inside

R-HQ(config)#interface gigabitEthernet 0/1
R-HQ(config-if)#ip nat outside

R-BRANCH(config)#interface gigabitEthernet 0/0
R-BRANCH(config-if)#ip nat inside

R-BRANCH(config)#interface gigabitEthernet 0/1
R-BRANCH(config-if)#ip nat outside

Hasta este punto cualquier tipo de tráfico hacia internet será envía por las interfaces Outside y además se identificará mediante la IP publica del Router gracias al NAT configurado.

Si se intenta enviar tráfico hacia entre las redes LAN de las sedes, no habrá respuesta debido a que esta redes son privadas y se encuentran detrás de un NAT. Aquí es donde entra la necesidad de una conexión VPN entre las dos redes LAN.

- ***Configuración de ISAKMP (IKE ph1)***

1. Se activa el protocolo ISAKMP en cada Router

R-HQ(config)#crypto isakmp enable

R-BRANCH(config)#crypto isakmp enable

2. según los parámetros definidos se crean las políticas. Se pueden crear múltiples políticas en cada uno de los routers.

Para poder que se lleve a cabo el inicio del túnel es necesario que al menos una política de uno de los routers coincida en todos sus parámetros con alguna política del otro Router.

La política con menor numeración tiene mayor prioridad.

La numeración en las políticas es solo de carácter local, de manera que cada Router puede contar con numeraciones y prioridades diferentes para las políticas.

Las políticas de un router se comparan con las del otro una a una según su prioridad hasta que se llegue a una coincidencia total de los parámetros.

R-HQ(config)#crypto isakmp policy 10
R-HQ(config-isakmp)#authentication pre-share
R-HQ(config-isakmp)#encryption aes 128
R-HQ(config-isakmp)#hash sha
R-HQ(config-isakmp)#group 2
R-HQ(config-isakmp)#lifetime 86400

R-BRANCH(config)#crypto isakmp policy 60
R-BRANCH(config-isakmp)#authentication pre-share
R-BRANCH(config-isakmp)#encryption aes 128
R-BRANCH(config-isakmp)#hash sha
R-BRANCH(config-isakmp)#group 2
R-BRANCH(config-isakmp)#lifetime 86400

3. Se configura la identidad para este par, existen dos opciones para este comando las cuales son:

- *Address:* Si el Router remoto solo utiliza una interfaz (por lo tanto una sola dirección IP) y además se conoce la IP que utilizará (no es asignada por DHCP).
- *Hostname:* Si el par utiliza más de una interfaz para ISAKMP o si obtiene la dirección IP por medio de DHCP.

Una vez definida la identida se configura la Pre-share key con el siguiente formato:

R(config)#crypto isakmp key *<key>* [address/hostname] *<Remote Address/Hostname>*

Utilizando "*Address*":

R-HQ(config-isakmp)#crypto isakmp identity address
R-HQ(config-isakmp)#crypto isakmp key myvpnkey 180.100.0.2 255.255.255.252

R-BRANCH(config)#crypto isakmp identity address
R-BRANCH(config)#crypto isakmp key myvpnkey address 200.24.0.2 255.255.255.252

Utilizando "*Hostname*":

R-HQ(config-isakmp)#crypto isakmp identity hostname
R-HQ(config-isakmp)#crypto isakmp key myvpnkey hostname R-BRANCH.bdomain.com
R-HQ(config)#ip host R-BRANCH.bdomain.com 180.100.0.2

(Si el Router está mapeado directamente a un DNS la última línea se puede obviar)

R-BRANCH(config)#crypto isakmp identity hostname
R-BRANCH(config)#crypto isakmp key vpnkey hostname R-HQ.hqdomain.com
R-BRANCH(config)#ip host R-HQ.hqdomain.com 200.24.0.2 255.255.255.252

(Si el Router está mapeado directamente a un DNS la última línea se puede obviar)

- ***Configuración de IPSec (IKE ph2)***

1. Crear una transformación para los datos. Al igual que las politicas, las transformaciones deben coincidir en sus parámetros en los dos Pares.

R-HQ(config)#crypto ipsec transform-set TRANSF esp-aes 128 esp-sha-hmac

R-BRANCH(config)#crypto ipsec transform-set TRANSF esp-aes 128 esp-sha-hmac

2. Se establecen parámetros para la SA (Security Association) como el tiempo de vida (lifetime) del túnel.

El tiempo de vida puede estar definido o por tiempo o por tráfico.

Una vez el tiempo de vida se haya cumplido, los routers deben renegociar los parámetros, creando así unas nuevas pre-share keys y brindándole seguridad al túnel.

Por Cantidad de Tiempo (sec):

R-HQ(config)#crypto ipsec security-association lifetime seconds 86400

R-BRANCH(config)#crypto ipsec security-association lifetime seconds 86400

Por Cantidad de Tráfico (Kbytes):

R-HQ(config)#crypto ipsec security-association lifetime kilobytes 2560

R-BRANCH(config)#crypto ipsec security-association lifetime kilobytes 2560

3. Para determinar cuál es el tráfico que debe atravesar el túnel y por ende estar encriptado, se deben crear ACLs equivalentes en cada uno de los routers, de manera que el tráfico de origen en la ACL de un Router corresponda al tráfico de destino en la ACL del otro Router.

Si estas ACLs no se definen correctamente la comunicación a través del túnel no será efectiva.

Para este caso, el tráfico que interesa es aquel que va desde la LAN de los HQ hasta la LAN remota y viceversa. Por lo tanto:

R-HQ(config)#ip access-list extended VPN-TRAFFIC
R-HQ(config-ext-nacl)#permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
R-HQ(config-ext-nacl)#deny ip any any

R-BRANCH(config)#ip access-list extended VPN-TRAFFIC
R-BRANCH(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255
R-BRANCH(config-ext-nacl)#deny ip any any

4. Se crea entonces un Mapa donde se agruparan todas las características para el Tunel IPSec.

Dado que a una interfaz solo puede asociársele un único Mapa se maneja entonces el concepto de Número de Secuencia mediante el cual se pueden crear diversas configuraciones y asociarlas a una única interfaz.

R-HQ(config)#crypto map VPN-MAP 1 ipsec-isakmp
R-HQ(config-crypto-map)#set peer 200.24.0.2
R-HQ(config-crypto-map)#set pfs group2
R-HQ(config-crypto-map)#set transform-set TRANSF
R-HQ(config-crypto-map)#match address VPN-TRAFFIC

R-BRANCH(config)#crypto map VPN-MAP 1 ipsec-isakmp
R-BRANCH (config-crypto-map)#set peer 180.100.0.2
R-BRANCH (config-crypto-map)#set pfs group2
R-BRANCH (config-crypto-map)#set transform-set TRANSF
R-BRANCH (config-crypto-map)#match address VPN-TRAFFIC

En este punto se pude considerar finalizada la configuración de la VPN. Ahora bien, si se intentase establecer el túnel al generar tráfico considerado interesante según las ACLs, se

obtendría que ni siquiera se intercambian los parámetros de configuración del túnel. Esto sucede si y solo si se ha establecido el NAT en alguno de los routers.
Sucede que el proceso de traducción de redes se lleva a cabo antes de que se proceda con el establecimiento del túnel, por lo tanto, cuando el tráfico de salida es evaluado por la ACL configurada para el "Crypto Map" esta no vería como red de origen una IP de la LAN (que es trafico considerado interesante) sino que vería la dirección IP Publica del Router que sirve para el Outside del NAT. Hasta este punto la configuración permite navegar hacia internet desde cualquier IP de la LAN mediante la IP Publica, pero impide el establecimiento del Tunel y por ende, evita que se tenga conexión entre las LAN de las sedes.

Si por el contrario decidimos quitar el NAT configurado entonces se presentaran las siguientes situaciones:

- Si no publicamos las redes LAN hacia internet (Lo cual no se debe y puede hacer para este caso) entonces el trafico puede salir desde las LAN, pero no se recibirá ninguna respuesta ya que el direccionamiento es Privado y no aparecerá ninguna ruta de vuelta definida en Internet. Adicionalmente los ISP filtran o bloquean cualquier tipo de tráfico desde Segmentos de Red Privados ya que estos no deberían salir hacia internet

- Para lograr tener acceso hacia internet sin el uso de NAT todos y cada uno de los PCs que requieran navegación en al Web tendrían que utilizar una IP pública.

La solución para esto es excluir el tráfico interesante del NAT, de manera que se permita tanto el tráfico hacia internet como el tráfico a través de la VPN.

• *Configuración Route-Map*

1. Se configura una ACL para excluir el tráfico que va desde la LAN local hacia la LAN remota ya que este se considera tráfico de interés.

R-HQ(config)#ip access-list extended NAT-LIST
R-HQ(config-ext-nacl)#deny ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
R-HQ(config-ext-nacl)#permit ip 192.168.0.0 0.0.0.255 any
R-HQ(config-ext-nacl)#deny ip any any

R-BRANCH(config)#ip access-list extended NAT-LIST
R-BRANCH(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255
R-BRANCH(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 any
R-BRANCH(config-ext-nacl)#deny ip any any

Se crea un route-map que incluya la lista de acceso definida, de manera que podamos excluir del NAT el tráfico de interés. Para este caso se podría solamente utilizar la lista de acceso definida como NAT-LIST.

R-HQ(config)#route-map VPN-TRAFFIC
R-HQ(config-route-map)#match ip address NAT-LIST

R-BRANCH(config)#route-map VPN-TRAFFIC
R-BRANCH(config-route-map)#match ip address NAT-LIST

Teniendo configurados los route-maps se procede a cambiar el formato del NAT en cada uno de los routers:

R-HQ(config)#ip nat inside source route-map VPN-TRAFFIC interface gigabitEthernet 0/1

R-BRANCH(config)#ip nat inside source route-map VPN-TRAFFIC interface gigabitEthernet 0/1

Al final de todas estas configuraciones tendremos navegación hacia internet y adicionalmente un tunel VPN el cual interconecta las oficinas.

Es de tener en cuenta que se puede realizar el mismo procedimiento para cada una de las Branch Office que se tengan, bajo la consideración del ancho de banda del canal de internet con el que contemos.

Documento desarrollado por:

Ing. Jose Manuel Cortés Hurtado.
CCNA, CCDA
Email: ***jose.cortes@sona.com.co***
MSN: ***jose_hurtado@hotmail.com***
Skype: josemcortesh
Santiago de Cali - Colombia