Configuración de VPN

**Se debe activar el paquete de seguridad para permitir la encriptación del tunel VPN.**

license boot module c1900 technology-package securityk9

Aceptar los terminos y reiniciar

**Configure las propiedades de la política criptográfica ISAKMP 10 en el R1 Y R3 junto con la clave criptográfica compartida cisco**

CONFIGURACIÓN IPSEC:

* crypto isakmp policy 10 (se establece la prioridad en 10 de la politica de seguridad del tunel)
* encryption aes 256 (establece el cifrado aes en 256 bits)
* authentication pre-share (se establece autenticación por clave pre compartida)
* group 5 (usa el grupo 5 de DIFFIE-HELLMAN. Existen 1,2,5,14,15,19,20 grupos, entre mas alto el grupo más seguro es, entre mas seguro mas tiempo gasta en la creación de la clave)
* crypto isakmp key secretkey address **x.x.x.x** **(es la ip del router extremo por el cual se accede al router, para esta practica será la ip serial del R3 o la ip del serial de R1 según corresponda)(dirección ip del dispositivo con quien vas a compartir la clave)**

**Cree el conjunto de transformaciones VPN-SET para usar esp-3des y esp-sha-hmac. A continuación, cree la asignación criptográfica IPSEC-MAP que vincula todos los parámetros del punto anterior. Use el número de secuencia 10 e identifíquelo como una asignación ipsec-isakmp.**

* crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac (establecer el conjunto y reglas de cifrado y autenticación aes con hmac R1-R3 es el nombre de la unión de cifrado y autenticación, en este caso se nombro de manera que se entienda que dispositivos estaran creando el tunel)
* crypto map IPSEC-MAP 10 ipsec-isakmp (creación del mapa criptografico con secuencia 10)
* set peer **x.x.x.x** **(es la ip del router extremo por el cual se accede al router, para esta practica será la ip serial del R3)**
* set pfs group5
* set security-association lifetime seconds 86400 (TIEMPO DE VIDA de la asociación)
* set transform-set R1-R3 (habilitamos el conjunto de transformación creado)
* match address 100 (número de la ACL que se creará en pasos posteriores)(la vpn solo va a permitir trafico asociado con la ACL 100)

**Vincule la asignación criptográfica IPSEC-MAP a la interfaz de salida hacia el router vecino**

* interface g0/0 (ejemplo de interfaz)
* crypto map IPSEC-MAP (es el mismo nombre del punto anterior en la asignación criptográfica con el router externo)

**Configure la ACL que permita el trafico en el tunel de la red con la que se hará la VPN**

* access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 (ejemplo de ACL, cambiar los parametros correctos, se debe colocar la LAN del dispositivo que se esta configurando)

**REPITE LOS PASOS ANTERIORES EN EL ROUTER DEL OTRO EXTERMO DE LA VPN. Recuerda cambiar los parametros necesarios.**

Verifica el túnel una vez que se configuraron los dos routers implicados en la vpn con:

* show crypto isakmp sa
* show crypto ipsec sa