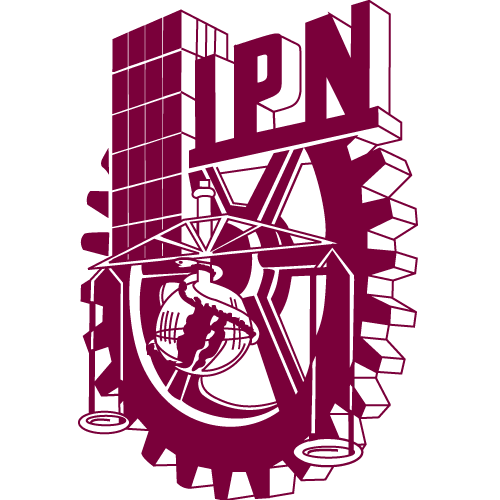
Una red virtual privada, Virtual Private Network (VPN), permite una extensión segura de una red de área local (LAN) sobre una red pública o no controlada como es Internet, ofreciendo las funcionalidades de gestión y seguridad de una red privada; para ello es necesario establecer una conexión que ofrezca mecanismos de seguridad.

 INSTITUTO POLITECNICO NACIONAL 

ESCUELA SUPERIOR DE CÓMPUTO

Materia: **Administración de Servicios en Red** Grupo:\_\_\_\_\_\_\_\_\_\_\_\_ Profesora: Leticia Henestrosa Carrasco

**Nombre alumno: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Configuración de VPN**

Un ejemplo habitual es conectar dos o más sucursales de una empresa utilizando Internet, o que un empleado acceda desde su casa a la red de datos de su empresa.

Las redes privadas virtuales se pueden configurar en la mayoría de los routers Cisco (800 a 7500). VPN puede ser implementado de múltiples formas y con diferentes niveles de seguridad.

Para entender mejor las redes VPN y comprender plenamente su potencial es necesario tener conocimientos de sistemas criptográficos y de algoritmos de cifrado.

**Métodos de implementación de VPN**

Hay dos formas principales para implementar una VPN:

* VPN basada en IPsec
* VPN basada en SSL

Ambos métodos ofrecen ventajas y desventajas.

Para implementar una VPN basada en IPsec hay que instalar el software de cliente en cada host o dispositivos que necesitan acceder a la VPN remota.

Por otro lado, las VPN SSL pueden establecer directamente la conexión entre dos máquinas sin necesidad de instalar ningún software cliente porque usa TLS, protocolo estándar de comunicación segura a nivel de transporte.

**Proceso de diseño de una VPN**

Para utilizar una VPN, por ejemplo, para una comunicación empresarial segura, es necesario diseñar un plan de implementación de VPN que debe tener en cuenta los siguientes aspectos:

1. Identificar el tipo de VPN ( SSL o IPsec ) que necesita y cuáles son los sistemas informáticos o equipos de red que necesitan ser protegidos por una conexión VPN.
2. Diseño de VPN: elegir el tipo de métodos de autenticación, filtrado y la política criptográfica.
3. Prueba: es mejor tratar de probar el diseño en un entorno de prueba antes de implementar la VPN de la organización.
4. Despliegue: una vez que se está satisfecho con el resultado de la prueba, se puede empezar a implementar la VPN según su diseño.
5. Monitorización: seguimiento de la actividad de tráfico en los puntos finales de VPN y siempre teniendo en cuenta las advertencias de seguridad o actualizaciones.

**IPsec**

IPsec es un protocolo que está sobre la capa del protocolo de Internet (IP). El objetivo principal de IPsec es proporcionar seguridad en la comunicación, mientras que los datos pasan a través de la red pública Internet. Para establecer IPsec se necesita tener dispositivos compatibles IPsec.

IPsec utiliza la siguiente tecnología de seguridad.

• Criptografía de clave pública

• Intercambio de claves mediante Diffie-Hellman • Cifrado de datos.

• Algoritmos resumen (hashing) que verifican la autenticidad e integridad de datos. Algunos algoritmos resumen utilizados son, por ejemplo, MD5 y SHA-1.

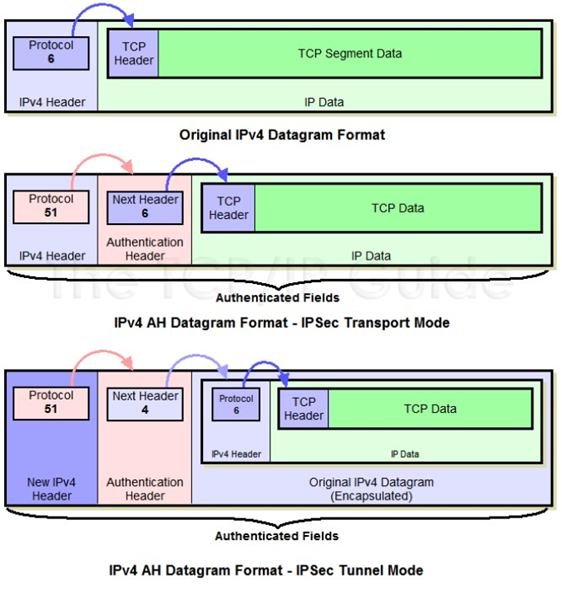
IPsec proporciona principalmente dos tipos de servicio: la autenticación y el cifrado de paquetes mediante el uso de AH y ESP.

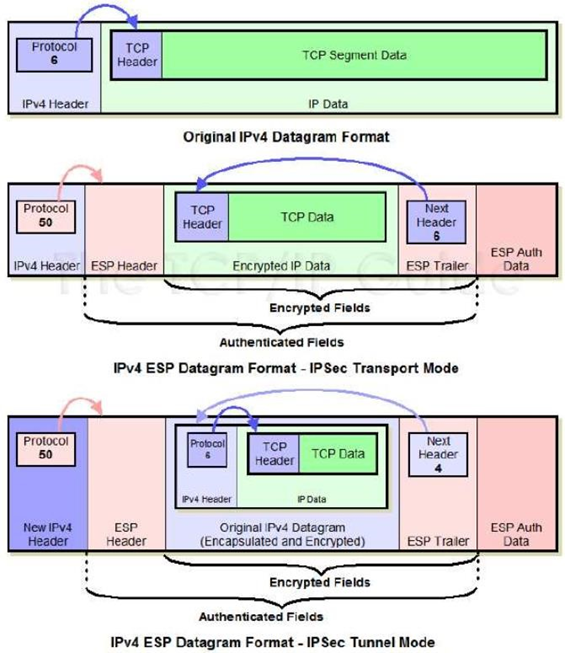
* AH (Autentication Header)- Proporciona integridad y autenticación, y evita el ataque por repetición. En cambio, AH no ofrece ningún servicio de cifrado.
* ESP (Encrypted Security Payload) – ESP proporciona los mismos servicios que AH, añadiendo además la confidencialidad.

IPsec puede proporcionar estos servicios en dos modos: modo túnel y modo transporte.

* El modo de transporte: En este modo, cada segmento TCP junto con una cabecera (AH o ESP) viaja encapsulados en un datagrama entre el router fuente y el destino.
* El modo túnel: En este modo, es el datagrama IP completo el que, junto con una cabecera (AH o ESP) viaja encapsulado en otro datagrama entre los routers fuente y destino.

En IPSec modo de transporte la fuente y el destino de la comunicación llevan a cabo los controles de seguridad, por el contrario, en IPSec modo túnel la fuente y el destino no tienen la capacidad ni los recursos para llevar a cabo estos controles de seguridad en los paquetes.

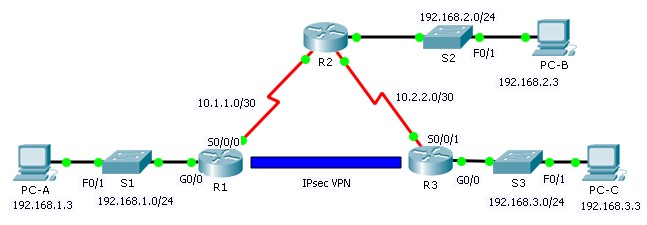




**Practica.- Configuración de VPN Site to Site**

Instrucciones.- Reproducir la siguiente topología en Packet Tracer, aplicando lo necesario para que haya conectividad entre todas las estaciones de trabajo.

**Topología**



**Tabla de direccionamiento**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dispositivo** | **Interfaz** | **Dirección IP** | **Máscara de subred** | **Gateway predeterminado** |
| R1 | G0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A |
| R2 | G0/0 | 192.168.2.1 | 255.255.255.0 | N/A |
| S0/0/0 | 10.1.1.1 | 255.255.255.252 | N/A |
| S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| R3 | G0/0 | 192.168.3.1 | 255.255.255.0 | N/A |
| S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 |

**Parámetros de política de fase 1 de ISAKMP**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parámetros** | | **R1** | **R3** |
| Método de distribución de claves | Manual o **ISAKMP** | ISAKMP | ISAKMP |
| Algoritmo de cifrado | **DES**, 3DES o AES | AES | AES |
| Algoritmo hash | MD5 o **SHA-1** | SHA-1 | SHA-1 |
| Método de autenticación | Claves previamente compartidas o **RSA** | Previamente compartidas | Previamente compartidas |
| Intercambio de claves | Grupo DH **1**, 2 o 5 | DH 2 | DH 2 |
| Vida útil de SA IKE | 86 400 segundos o menos | 86400 | 86400 |
| ISAKMP Key (Llave USB) |  | cisco | cisco |

Los parámetros **en negrita** son valores predeterminados. Los demás parámetros se deben configurar explícitamente.

**Parámetros de política de fase 2 de IPsec**

|  |  |  |
| --- | --- | --- |
| **Parámetros** | **R1** | **R3** |
| Conjunto de transformaciones | VPN-SET | VPN-SET |
| Nombre de host del peer | R3 | R1 |
| Dirección IP del peer | 10.2.2.2 | 10.1.1.2 |
| Red para cifrar | 192.168.1.0/24 | 192.168.3.0/24 |
| Nombre de la asignación criptográfica | VPN-MAP | VPN-MAP |
| Establecimiento de SA | ipsec-isakmp | ipsec-isakmp |

**Objetivos**

**Parte 1: Habilitar las características de seguridad**

**Parte 2: Configurar los parámetros de IPsec en el R1 Parte 3: Configurar los parámetros de IPsec en el R3 Parte 4: Verificar la VPN con IPsec**

**Situación**

En esta actividad, configurará dos routers para admitir una VPN con IPsec de sitio a sitio para el tráfico que fluye de sus respectivas LAN. El tráfico de la VPN con IPsec pasa a través de otro router que no tiene conocimiento de la VPN. IPsec proporciona una transmisión segura de la información confidencial a través de redes sin protección, como Internet. IPsec funciona en la capa de red, por lo que protege y autentica los paquetes IP entre los dispositivos IPsec participantes (peers), como los routers Cisco.

# Parte 1: Habilitar las características de seguridad

**Paso 1: Activar el módulo securityk9.**

Se debe activar la licencia del paquete de tecnología de seguridad para completar esta actividad.

1. Emita el comando **show version** en el modo EXEC del usuario o EXEC privilegiado para verificar si se activó la licencia del paquete de tecnología de seguridad.

----------------------------------------------------------------

Technology Technology-package Technology-package

Current Type Next reboot ----------------------------------------------------------------- ipbase ipbasek9 Permanent ipbasek9 security None None None uc None None None data None None None Configuration register is 0x2102

1. De lo contrario, active el módulo **securityk9** para el siguiente arranque del router, acepte la licencia, guarde la configuración y reinicie.

R1(config)# **license boot module c2900 technology-package securityk9**

R1(config)# **end**

R1# **copy running-config startup-config**

R1# **reload**

1. Una vez finalizada la recarga, vuelva a emitir el comando **show version** para verificar si se activó la licencia del paquete de tecnología de seguridad.

Technology Package License Information for Module:'c2900'

----------------------------------------------------------------

Technology Technology-package Technology-package

Current Type Next reboot ----------------------------------------------------------------- ipbase ipbasek9 Permanent ipbasek9 security securityk9 Evaluation securityk9 uc None None None data None None None

1. Repita los pasos 1a a 1c con el **R3**.

# Parte 2: Configurar los parámetros de IPsec en el R1

**Paso 1: Probar la conectividad.**

Haga ping de la **PC-A** a la **PC-C**.

**Paso 2: Identificar el tráfico interesante en el R1.**

Configure la ACL 110 para identificar como interesante el tráfico proveniente de la LAN en el **R1** a la LAN en el **R3**. Este tráfico interesante activa la VPN con IPsec para que se implemente cada vez que haya tráfico entre las LAN de los routers **R1** y **R3**. El resto del tráfico que se origina en las LAN no se cifra. Recuerde que debido a la instrucción implícita deny any, no hay necesidad de agregar dicha instrucción a la lista.

R1(config)# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Paso 3: Configurar las propiedades de la fase 1 de ISAKMP en el R1.**

Configure las propiedades de la política criptográfica ISAKMP **10** en el **R1** junto con la clave criptográfica compartida **escom**. Consulte la tabla de la fase 1 de ISAKMP para ver los parámetros específicos que se deben configurar. No es necesario que se configuren los valores predeterminados, por lo que solo se deben configurar el cifrado, el método de intercambio de claves y el método DH.

*Con estas líneas se establece la negociación del tunel*

R1(config)# **crypto isakmp policy 10**

R1(config-isakmp)# **encryption aes**

R1(config-isakmp)# **authentication pre-share**

R1(config-isakmp)# **group 2**

R1(config-isakmp)# **exit**

*!--- Especificar la clave compartida y la dirección remota del otro extremo del túnel.*

*!--- Se identifica la clave (****escom*** *en este caso) con la que se va a encriptar los datos*

R1(config)# **crypto isakmp key escom address 10.2.2.2**

**Paso 4: Configurar las propiedades de la fase 2 de ISAKMP en el R1.**

Cree el conjunto de transformaciones con el nombre **VPN-SET** para usar **esp-3des** y **esp-sha-hmac**. El transform set define las políticas de seguridad que se aplican al tráfico que entra o sale de la interfaz. A continuación, cree la asignación criptográfica **VPN-MAP** que vincula todos los parámetros de la fase 2. Use el número de secuencia **10** e identifíquelo como una asignación **ipsec-isakmp**.

R1(config)# **crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac**

R1(config)# **crypto map VPN-MAP 10 ipsec-isakmp**

R1(config-crypto-map)# **description VPN connection to R3**

R1(config-crypto-map)# **set peer 10.2.2.2**

R1(config-crypto-map)# **set transform-set VPN-SET**

*!--- Añadir una lista de control de acceso (ACL) para el otro extremo del tunel*

R1(config-crypto-map)# **match address 110**

R1(config-crypto-map)# **exit**

**Paso 5: Configurar la asignación criptográfica en la interfaz de salida.**

Por último, vincule la asignación criptográfica **VPN-MAP** a la interfaz de salida Serial 0/0/0.

R1(config)# **interface S0/0/0**

R1(config-if)# **crypto map VPN-MAP**

# Parte 3: Configurar los parámetros de IPsec en el R3

**Paso 1: Configurar el router R3 para admitir una VPN de sitio a sitio con el R1.**

Ahora configure los parámetros recíprocos en el **R3**. Configure la ACL **110** para identificar como interesante el tráfico proveniente de la LAN en el **R3** a la LAN en el **R1**.

R3(config)# **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Paso 2: Configurar las propiedades de la fase 1 de ISAKMP en el R3.**

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

R3(config)# **crypto isakmp policy 10**

R3(config-isakmp)# **encryption aes**

R3(config-isakmp)# **authentication pre-share**

R3(config-isakmp)# **group 2**

R3(config-isakmp)# **exit**

R3(config)# **crypto isakmp key escom address 10.1.1.2**

**Paso 3: Configurar las propiedades de la fase 2 de ISAKMP en el R1.**

Como hizo en el **R1**, cree el conjunto de transformaciones **VPN-SET** para usar **esp-3des** y **esp-sha-hmac**. A continuación, cree la asignación criptográfica **VPN-MAP** que vincula todos los parámetros de la fase 2. Use el número de secuencia **10** e identifíquelo como una asignación **ipsec-isakmp**.

R3(config)# **crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac**

R3(config)# **crypto map VPN-MAP 10 ipsec-isakmp**

R3(config-crypto-map)# **description VPN connection to R1**

R3(config-crypto-map)# **set peer 10.1.1.2**

R3(config-crypto-map)# **set transform-set VPN-SET**

R3(config-crypto-map)# **match address 110**

R3(config-crypto-map)# **exit**

**Paso 4: Configurar la asignación criptográfica en la interfaz de salida.**

Por último, vincule la asignación criptográfica **VPN-MAP** a la interfaz de salida Serial 0/0/1.

R3(config)# interface S0/0/1

R3(config-if)# crypto map VPN-MAP

# Parte 4: Verificar la VPN con IPsec

**Paso 1: Verificar el túnel antes del tráfico interesante.**

Emita el comando **show crypto ipsec sa** en el **R1**. Observe que la cantidad de paquetes encapsulados, cifrados, desencapsulados y descifrados se establece en 0.

R1# **show crypto ipsec sa**

interface: Serial0/0/0 Crypto map tag: VPN-MAP, local addr 10.1.1.2 protected vrf: (none) local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0) current\_peer 10.2.2.2 port 500 PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0 local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2 path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0 current outbound spi: 0x0(0) <resultado omitido>

**Paso 2: Crear el tráfico interesante.**

Haga ping de la **PC-A** a la **PC-C**.

**Paso 3: Verificar el túnel después del tráfico interesante.**

En el **R1**, vuelva a emitir el comando **show crypto ipsec sa**. Ahora observe que la cantidad de paquetes es superior a 0, lo que indica que el túnel VPN con IPsec funciona.

R1# **show crypto ipsec sa**

interface: Serial0/0/0 Crypto map tag: VPN-MAP, local addr 10.1.1.2 protected vrf: (none) local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0) current\_peer 10.2.2.2 port 500 PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0 local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2 path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0 current outbound spi: 0x0A496941(172583233) <resultado omitido>

**Paso 4: Crear el tráfico no interesante.**

Haga ping de la **PC-A** a la **PC-B**.

**Paso 5: Verificar el túnel.**

En el **R1**, vuelva a emitir el comando **show crypto ipsec sa**. Por último, observe que la cantidad de paquetes no cambió, lo que verifica que el tráfico no interesante no está cifrado.