Capítulo 13

ENCAPSULADO GENÉRICO DE ENCAMINAMIENTO Y SEGURIDAD IP (GRE/IPSEC)

GRE (Generic Routing Encapsulation) es un protocolo estándar abierto, documentado en los RFC 1701 y 1702, y actualizado en el RFC 2784. GRE es encapsulado directamente en la capa IP, la cual usa el valor 47 en el campo "número de protocolo" para identificarlo y transportarlo. GRE incluye sus propios campos en el encabezado y un campo de datos; en este último transporta diferentes protocolos de capa 3, incluyendo a IP. IPsec (IP security) es un conjunto de protocolos y algoritmos relacionados con la seguridad de los datagramas IP, documentado en los RFC 2401 a 2412, y en el RFC 2451. El marco de referencia IPsec proporciona las funciones de autenticación y cifrado del tráfico IP, y el intercambio seguro de las claves de autenticación y cifrado; siendo compatible con IPv4 e IPv6. En el presente capítulo se explora la interconexión de tres redes IP privadas de un suscriptor por medio de la Internet pública: se usa el protocolo GRE para transportar los datagramas IP de las redes privadas y al protocolo IPsec en modo transporte para proporcionar la protección y seguridad por ellos requeridas.

Objetivo

Al finalizar esta unidad, el estudiante estará en capacidad de:

- Configurar los protocolos GRE e IPsec en los encaminadores de borde de tres redes de área local, con el propósito de interconectar dichas redes mediante el uso seguro de la infraestructura pública de Internet.
- Monitorizar las redes que usan los protocolos GRE e IPsec.

Procedimiento

Red que permite emular una Internet pública básica

Montaje de emulación de la Internet pública básica

Llevar a cabo el montaje y la conexión de los encaminadores R1, R2, R3 e ISP de acuerdo con la Figura 13.1 (puede usar GNS3); los encaminadores R1, R2 y R3 representan a un suscriptor conectado a uno o varios ISP de la Internet pública, mientras que el encaminador ISP es una representación simplificada de la Internet pública (conformada por diferentes ISP).

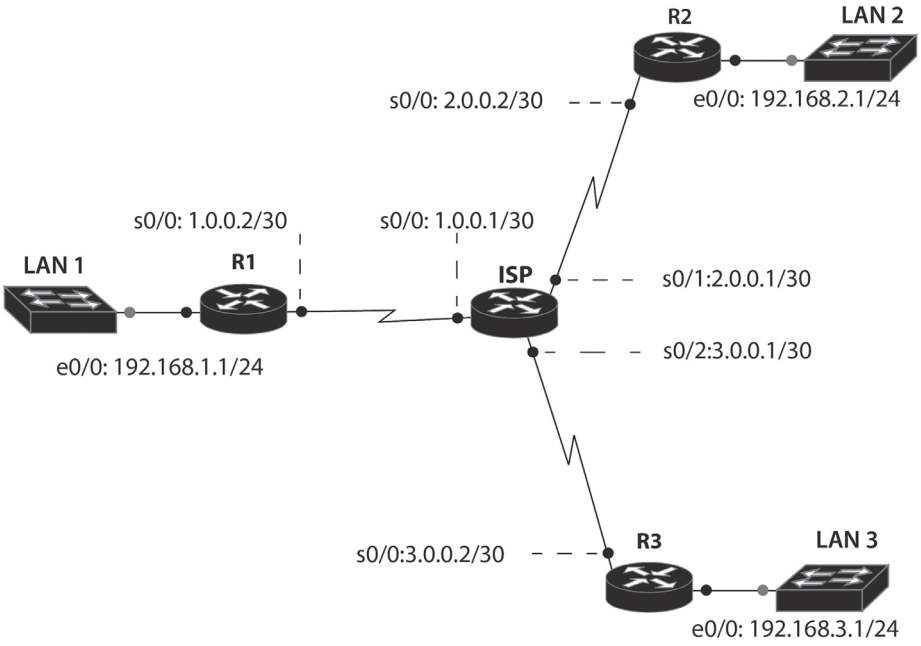

Figura 13.1. Representación básica de la conexión de tres redes privadas de un suscriptor a la Internet pública (ISP)

Configuración y prueba de la Internet pública

Configurar los encaminadores ISP, R1, R2 y R3 de acuerdo a las líneas de código de los archivos ISP-internet-cfg, R1-internet-cfg, R2-internet-cfg y R3-internet-cfg, relacionados a continuación. Estos archivos permiten establecer la funcionalidad de conexión de tres redes de área local con una Internet pública básica. Probar el funcionamiento de dicha red.

ISP-internet-cfg

```
hostname ISP
!
interface Serial0/0
 description *Recibe a R1*
 ip address 1.0.0.1 255.255.255.252
 no shutdown
!
interface Serial0/1
 description *Recibe a R2*
 ip address 2.0.0.1 255.255.255.252
 no shutdown
!
interface Serial0/2
 description *Recibe a R3*
 ip address 3.0.0.1 255.255.255.252
 no shutdown
!
```

R1-internet-cfg

```
!
hostname R1
!
interface Serial0/0
 description *Conexión a Internet*
 ip address 1.0.0.2 255.255.255.252
 no shutdown
!
interface Fastethernet0/0
 description * Conexión de R1 a Lan1*
 ip address 192.168.1.1 255.255.255.0
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 1.0.0.1
!
```

R2-internet-cfg

```
hostname R2
!
interface Serial0/0
 description *Conexión a Internet*
 ip address 2.0.0.2 255.255.255.252
 no shutdown
!
interface Fastethernet0/0
 description * Conexión de R2 a Lan2*
 ip address 192.168.2.1 255.255.255.0
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 2.0.0.1
!
```

R3-internet-cfg

```
hostname R3
!
interface Serial0/0
 description *Conexión a Internet*
 ip address 3.0.0.2 255.255.255.252
 no shutdown
!
interface Fastethernet0/0
 description * Conexión de R3 a Lan3*
 ip address 192.168.3.1 255.255.255.0
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 3.0.0.1
!
```

Para probar el funcionamiento de la red anterior, se ejecutan los siguientes comandos desde el encaminador R1.

R1> *ping ip* 2.0.0.2 source 1.0.0.2
R1> *ping ip* 3.0.0.2 source 1.0.0.2
R1> *ping ip* 2.0.0.2 source 192.168.1.1
R1> *ping ip* 3.0.0.2 source 192.168.1.1

Los primeros dos comandos deben funcionar, mientras que los dos últimos no, puesto que el encaminador ISP no conoce la red del origen del mensaje ICMP (192.168.1.0/24). Note que el encaminador ISP solamente conoce las tres redes directamente conectadas a él: 1.0.0.0/30; 2.0.0.0/30; y 3.0.0.0/30.

Túneles GRE funcionando sobre la Internet pública

Túneles GRE

Observar y tener en cuenta las direcciones IP (lógicas) de los túneles que se van a crear entre los encaminadores R1-R2 y R1-R3, representados en la Figura 13.2, dichos túneles permiten interconectar las tres redes de área local a través de Internet.

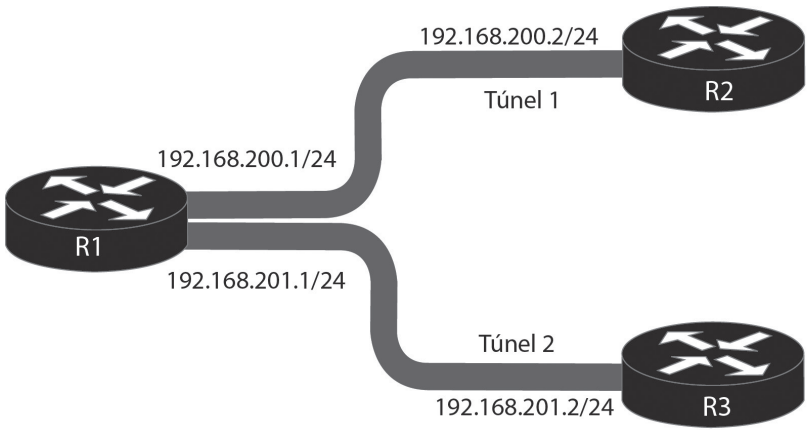

Figura 13.2. Representación de los dos túneles GRE en la Internet pública

Configuración y prueba de los túneles GRE

A la configuración de los encaminadores R1, R2 y R3 realizada anteriormente, adicionar la configuración que permite crear dos túneles mediante el protocolo GRE; los comandos correspondientes se encuentran en las líneas de código de los archivos R1-gre-conf, R2-gre-conf y R3-gre-conf. Probar el funcionamiento de la red configurada con GRE.

R1-gre-conf

```
!
interface Tunnel1
 description túnel GRE hacia router R2
 ip address 192.168.200.1 255.255.255.0
 tunnel source 1.0.0.2
 tunnel destination 2.0.0.2
!
interface Tunnel2
 description Túnel GRE hacia router R3
 ip address 192.168.201.1 255.255.255.0
 tunnel source 1.0.0.2
 tunnel destination 3.0.0.2
!
router rip
 network 192.168.1.0
 network 192.168.200.0
 network 192.168.201.0
!
```

R2-gre-conf

```
!
interface Tunnel1
 description Túnel GRE hacia router R1
 ip address 192.168.200.2 255.255.255.0
 tunnel source 2.0.0.2
 tunnel destination 1.0.0.2
!
router rip
 network 192.168.2.0
 network 192.168.200.0
!
```

R3-gre-conf

```
!
interface Tunnel2
 description Tunnel GRE hacia R1
 ip address 192.168.201.2 255.255.255.0
 tunnel source 3.0.0.2
 tunnel destination 1.0.0.2
!
router rip
 network 192.168.3.0
 network 192.168.201.0
```

Para probar el funcionamiento de la red anterior con el túnel GRE, desde el encaminador R1 se ejecutan los siguientes comandos:

R1# *show ip route*
R1# *ping ip* 192.168.2.1 source 192.168.1.1
R1# *ping ip* 192.168.3.1 source 192.168.1.1

El primer comando debe mostrar (en la tabla de enrutamiento) las redes aprendidas a través de los dos túneles que se han configurado. El segundo y tercer comando envían un ping extendido que prueba la conexión hacia la interfaz Ethernet de los encaminadores R2 y R3.

Cifrado de los túneles mediante IPsec

Configuración y prueba del cifrado de los túneles GRE mediante IPsec

A la configuración de los encaminadores R1, R2 y R3 realizada en el paso anterior, adicionar la configuración que permite cifrar los dos túneles mediante el protocolo IPsec, cuyos comandos se encuentran en las líneas de código de los archivos R1-ipsec-cfg, R2-ipsec-cfg y R3-ipsec-cfg. Nota: los comandos demasiado largos están precedidos por un asterisco (*) para indicar que continúan en la segunda línea.

R1-ipsec-cfg	R2-ipsec-cfg
!	!
* access-list 101 permit gre host 1.0.0.2 host 2.0.0.2	* access-list 100 permit gre host 2.0.0.2 host 1.0.0.2
* access-list 102 permit gre host 1.0.0.2 host 3.0.0.2	!
!	!
crypto isakmp policy 1	!
encryption aes	crypto isakmp policy 1
authentication pre-share	encryption aes
group 5	authentication pre-share
hash sha	group 5
!	hash sha
* crypto isakmp key 0 univalle1 address 2.0.0.2	!
* crypto isakmp key 0 univalle1 address 3.0.0.2	* crypto isakmp key 0 univalle1 address 1.0.0.2
!	!
* crypto ipsec transform-set tunel-trans esp-aes esp-sha-hmac	!
mode transport	!
!	* crypto ipsec transform-set tunel-trans esp-aes esp-sha-hmac
crypto map vpn 10 ipsec-isakmp	mode transport
description VPN from R1 to R2	!
set peer 2.0.0.2	crypto map vpn 10 ipsec-isakmp
set transform-set tunel-trans	description VPN from R2 to R1
match address 101	set peer 1.0.0.2
!	set transform-set tunel-trans
	match address 100
	!

Continua

Viene

```
crypto map vpn 11 ipsec-isakmp
 description VPN from R1 to R3
 set peer 3.0.0.2
 set transform-set tunel-trans
 match address 102
!
interface Tunnel1
 ip mtu 1500
 ip tcp adjust-mss 1400
 keepalive
!
interface Tunnel2
 ip mtu 1500
 ip tcp adjust-mss 1400
 keepalive
!
interface Serial0/0
 crypto map vpn
!
```

```
!
!
!
!
!
!
interface Tunnel1
 ip mtu 1500
 ip tcp adjust-mss 1400
 keepalive
!
!
!
!
!
!
interface Serial0/0
 crypto map vpn
!
```

R3-ipsec-cfg

```
!
* access-list 100 permit gre host 3.0.0.2 host 1.0.0.2
!
crypto isakmp policy 1
 encryption aes
 authentication pre-share
 group 5
 hash sha
!
* crypto isakmp key 0 univalle1 address 1.0.0.2
!
!
* crypto ipsec transform-set tunel-trans esp-aes esp-sha-hmac
 mode transport
!
crypto map vpn 10 ipsec-isakmp
 description VPN from R3 to R1
 set peer 1.0.0.2
 set transform-set tunel-trans
 match address 100
!
```

Continua

Viene

```
!
interface Tunnel2
 ip mtu 1500
 ip tcp adjust-mss 1400
 keepalive
!
interface Serial0/0
 crypto map vpn
!
```

Para probar el funcionamiento de la red anterior, configurada con dos túneles GRE cifrados con IPsec, se ejecutan los siguientes comandos desde el encaminador R1.

```
R1# show crypto engine connections active
R1# show crypto ipsec sa
R1# show ip route
```

Problemas

1. Por defecto, la interfaz "tunnel" opera encapsulando el protocolo GRE (*tunnel mode gre ip*). ¿Qué otros protocolos soporta dicha interfaz?, use el comando "*tunnel mode ?*". Reconocer el propósito de los comandos "*tunnel path-mtu-discovery*" y "*tunnel path-mtu-discovery min-mtu 1000*" en el siguiente trozo de código.

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode ?
R1(config-if)# tunnel path-mtu-discovery
R1(config-if)# tunnel path-mtu-discovery min-mtu 1000
```

2. Por defecto, las conexiones IPsec usan el modo túnel. ¿Qué significa poner a IPsec a operar en modo de transporte? ¿Cuándo es necesario usar el modo túnel de IPsec?

```
R1(config-if)# crypto ipsec transform-set tunel-trans esp-aes esp-sha-hmac
R1(config-if)# mode transport
```

3. ¿Qué cambios son necesarios en la configuración de las dos conexiones protegidas por IPsec de la Figura 13.2 para que el modo de autenticación use claves RSA (Rivest, Shamir, and Adelman)? Implemente los cambios y verifique los resultados.

Glosario

Cifrado: técnica que combina claves y algoritmos complejos para transformar los paquetes que transportan datos en texto claro a datos ininteligibles, con el fin de proporcionar seguridad.

Internet pública: la red de redes, está conformada por la interconexión de redes de los ISP de acuerdo a su jerarquía, caracterizada por usar direcciones IP públicas.

Mensaje ICMP: hace referencia al protocolo ICMP, el cual forma parte integral de IP. Sirve para reportar errores, realizar funciones de control y generar mensajes de prueba o depuración.

Túnel: conexión lógica superpuesta sobre otra conexión lógica. Por ejemplo, IP versión 4 encima de IP versión 4, o IP versión 6 encima de IP versión 4.

Bibliografía

BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.

COMER, D. (2005). *Internetworking with TCP/IP, Volumen 1: Principles, Protocols, and Architecture*. 5th Ed. Upper Saddle River, NJ: Pearson Prentice Hall.

DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook ™*. 2nd Ed. Sebastopol, CA: O'Reilly.

KUROSE J. F.; ROSS, K. W. (2012). *Computer Networking: A Top-down Approach*. 7th Ed. Boston: Addison-Wesley.