Práctica Extra, VPN

Objetivos

- ✓ Aprender a definir políticas de seguridad para configurar un enlace VPN.

Introducción

La VPN (*Virtual Private Network*) o Red Privada Virtual permite proveer un canal de comunicación (túnel) seguro a través de una red pública (insegura), evitando los altos costos de los enlaces dedicados equivalentes. Una VPN puede habilitarse para interconectar:

- ✓ Un usuario único a una red (*client to site connection*).
- ✓ Oficinas remotas a una oficina central (*site to site connection*).
- ✓ Dos usuarios únicos (*client to client connection*).

Una VPN puede implementarse en diferentes capas del modelo de referencia OSI. Cuando se configura una VPN en una capa determinada del modelo, sólo hay protección desde esa capa hacia los niveles superiores.

- ✓ Capa de enlace de datos. Su principal ventaja es soportar protocolos no IP. Los principales protocolos son: PPTP (*Point to Point Tunneling Protocol*), L2P (*Layer 2 Forwarding*), L2TP (*Layer 2 Tunneling Protocol*), L2SP (*Layer 2 Security Protocol*).
- ✓ Capa de Red. IPSEC (IP Security).
- ✓ Capa de Aplicación. SSH, SSL, TLS.

IP Security (IPSec)

Es una pila de protocolos y estándares que permiten proteger el tráfico que viaja sobre una red insegura (por ejemplo, Internet). Los servicios que provee IPSEC son:

- ✓ Confidencialidad al evitar el robo de las datos (algoritmos cifrado).
- ✓ Integridad asegurando que los datos no han sido manipulados o alterados (algoritmos de hashing).
- ✓ Autenticación al confirmar la identidad del host que envía los datos (usando claves precompartidas o usando una autoridad certificadora).
- ✓ Contra replicación (anti-replay) al evitar la duplicación de paquetes cifrados (asignación de identificador de secuencia único).

Los protocolos que conforman a IPSEC son:

- ✓ AH (*Authentication Header*) Su función es proveer servicios de autenticación e integridad. Utiliza algoritmos de hash para obtener valores hash del encabezado y cuerpo de paquete.
- ✓ ESP (*Encapsulation Security Payload*) provee servicios de confidencialidad, autenticación e integridad. ESP realiza cifrado y por tanto se considera más seguro que AH.

Cada uno de los protocolos de IPSEC (AH y ESP) pueden operar en 2 modos:

- ✓ Modo transporte. Los encabezados originales IP se dejan intactos. Se utiliza cuando se desea asegurar la comunicación de un dispositivo único a otro dispositivo (*client to client*).
- ✓ Modo túnel. Al paquete original se le aplican cifrado y/o hashing (encabezados y datos del paquete). Se genera un encabezado temporal para transportar el paquete a través del túnel.

IKE (*Internet Key Exchange*) para la asociación de seguridad en IPSEC

Una asociación de seguridad (SA) es el establecimiento de atributos de seguridad compartidos entre 2 entidades de red para soportar la comunicación segura. IKE es utilizado para establecer una SA. IKE debe definir un conjunto de políticas de seguridad (manejadas con ISAKMP -*Internet Security Association and Key Management Protocol*-) por cada participante. Los valores que componen una política de seguridad son:

- ✓ Algoritmo de cifrado (DES, 3DES, AES).

- ✓ Algoritmo de hashing (MD5, SHA-1).
- ✓ Método de autenticación (clave precompartida o firmas RSA).
- ✓ Grupo de Diffie-Hellman (DH) para crear y compartir llaves.
- ✓ Tiempo de vida de la asociación de seguridad (segundos o KB enviados).

IKE funciona en 2 fases de negociación:

Fase 1. Establece un túnel inicial (conocido como túnel IKE o ISAKMP-SA) para autenticación usando intercambio por Diffie-Hellman (canal bidireccional ISAKMP-SA único).

Fase 2. Con el canal seguro establecido en la fase 1, los participantes negocian la asociación de seguridad de otros servicios (IPSec SA). Al menos 2 canales (envío y recepción) unidireccionales (IPSec *Transform Set*) son establecidos.

Material

1 PC con Packet Tracer.

Desarrollo

Utiliza la topología creada y configurada en el previo para desarrollar la práctica de esta sesión.

Configuración de una VPN

Una VPN es un enlace cifrado a través de un canal inseguro. El túnel cifrado entre redes privadas se establecerá entre los *routers* Router0 y Router1, donde los segmentos LAN privada y VLAN 35 serán las redes comunicadas por la VPN.

Como primer paso, es necesario que los *routers* se pongan de acuerdo en la forma de autenticarse. Para ello es necesario el establecimiento de una negociación para el intercambio de autenticación; esto se logra mediante el servicio ISAKMP, que indicará la política de cifrado y autenticación de la VPN. Cada enlace VPN requiere de su propia política para el uso de algoritmos en el canal de comunicación.

```
Router(config)# crypto isakmp enable
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# encryption aes
Router(config-isakmp)# hash sha
Router(config-isakmp)# group 2
Router(config-isakmp)# exit
```

Una vez establecida la política, se requiere establecer un conjunto de transformaciones en ambos *routers* para poder comunicarse en el canal (cómo se utilizará la política dada de alta):

```
Router(config)# crypto isakmp key [VPNPASS] address [PEER] 0.0.0.0
Router(config)# crypto ipsec transform-set [VPNTS] esp-aes esp-sha-hmac
Router(config)# crypto ipsec security-association lifetime seconds 86400
```

donde **VPNPASS** es la clave sin cifrar que se intercambiará para el acceso a la VPN; **PEER** es la dirección de final del túnel VPN, por ejemplo, si se configura Router0 el final del túnel es la dirección pública de Router1; **VPNTS** es el nombre del conjunto de transformaciones. Nótese que la wildcard del **PEER** es 0.0.0.0, lo cual designa a un solo host.

Es necesario utilizar una lista de acceso extendida para ligarla a la política, al conjunto de transformaciones y al mapa criptográfico de la VPN. El objetivo de la lista es darle a conocer al *router* qué tráfico está permitido ingresar a la VPN y qué tráfico no.

```
Router(config)# access-list 102 permit ip [SRC] [WILDCARD_SRC] [DTN] [WILDCARD_DTN]
```

donde **SRC** es la dirección de red de la red privada conectada al *router* que se está configurando (origen), **WILDCARD_SRC** es la respectiva máscara *wildcard*; en tanto que **DTN** es la dirección de red de la red privada conectada al otro extremo del túnel (destino), y **WILDCARD_DTN** es la respectiva máscara *wildcard* de dicha red privada. Por ejemplo, si se está configurando Router0, la red privada será la VLAN 35 con segmento de red 192.Y.X.0, el origen (SCR); la red de destino es la red privada conectada a Router1: 192.Y.X.64, el destino (DTN).

Una vez establecidos la política y el conjunto de transformaciones, el *router* debe saber cómo y dónde aplicar dichas configuraciones; para ello se construye el mapa criptográfico que indicará cuál es el destino del túnel creado, sobre qué interface debe aplicarse, qué política de autenticación se usará y cómo se hará el cifrado de datos. El mapa criptográfico enlaza la política de cifrado, el conjunto de transformaciones y se aplica a la interface de salida del *router* que se está configurando. Se requiere un mapa por cada enlace VPN que se requiera configurar, así como la lista de control de acceso adecuada.

```
Router(config) #crypto map [VPNMAP] 100 ipsec-isakmp
Router(config-crypto-map) #match address 102
Router(config-crypto-map) #set peer [PEER]
Router(config-crypto-map) #set pfs group2
Router(config-crypto-map) #set transform-set [VPNTS]
Router(config-crypto-map) #exit
Router(config) #interface Fa0/1
Router(config-if) #crypto map [VPNMAP]
```

donde **VPNMAP** es el nombre del mapa criptográfico.

Este proceso debe realizarse en los dos *routers* que conectan las redes privadas (Router0 y Router2). Si se configura un solo *router*, se perderá la comunicación entre dichas redes, ya que el *router* perteneciente a la VPN no podrá autenticar a uno de los segmentos.

Verifica con los siguientes comandos que la VPN está configurada correctamente.

```
Router#  show crypto isakmp policy
Router#  show crypto isakmp sa
Router#  show crypto map
Router#  show crypto ipsec transform-set
```

Argumenta qué muestra la salida de cada comando. Envía un ping de una Intranet a otra y verifica la asociación de seguridad con

```
Router#  show crypto isakmp sa
```

En este caso, se debe mostrar que la VPN ya está activa. Para verificar que los paquetes están siendo cifrados a nivel de red, ejecuta el modo de simulación de Packet Tracer y analizalos en su camino de una VPN a otra.

Cuestionario

¿Qué beneficios aporta una comunicación mediante VPN?

¿Qué tipo de VPN, atendiendo al tipo de conexión, se configuró en el ejercicio?

Si se quisiera habilitar una VPN con conexión *client to site*, ¿qué configuración debe realizarse?

Mencione los elementos que le dan la confidencialidad a la VPN.

Conclusiones