|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DATOS DE LA ACTIVIDAD | | | | | | | |
| No. de Actividad: | **3.6** | **Práctica 6** | Configurar y verificar VPN con IPsec sitio a sitio utilizando CLI. | | | | |
| Unidad: | 3: Configuración de SSH y VPN | | | | | | |
| Carrera: | Tgo. en Desarrollo de Software | | | | | | |
| Materia | **SEGURIDAD EN ITI** | | | | | Clave | MPF3608DSO |
| Profesor: | Andrés Figueroa Flores | | | | | | |
| Alumno: | David Alejandro López Torres | | | | | Registro: | 17300155 |
| Institución: | **Centro de Enseñanza Técnica Industrial plantel Colomos** | | | | | | |
| Semestre: | 8 | Grupo: | D1 | Período: | Feb-Jun 2021 | Fecha: | 03/06/2021 |
| Compet. Genéricas | | 4.1, 4.5, 5.2, 5.5 | | Compet. Profesional | | CP1-1 | |

**1. Objetivo(s) de la actividad**

* Verificar la conectividad en toda la red.
* Configurar el router R1 para apoyar un VPN con IPsec sitio a sitio con R3.

**2. Introducción**

Una VPN es una red privada que utiliza una red pública, generalmente Internet, para crear un canal de comunicación seguro.

**3. Instrucciones de la actividad**

1. Usar el archivo de ejemplo de prácticas para realizar el reporte esta actividad.

2. Tomar impresiones de pantalla completa de la actividad, (recuerda ir haciendo las impresiones conforme vas realizando la práctica en el simulador) , con tu nombre en la impresión.

3. Subir el reporte terminado de WORD y el archivo de PACKET TRACERT, dar clic para marcar como entregada la actividad.

**4. Resumen**

IPSec (Internet Protocol Security) es un conjunto de protocolos de seguridad en internet diseñado para proteger los paquetes de datos enviados a través de una red IP. IPSec emplea la encriptación para garantizar la privacidad de los datos enviados y para verificar que solo son leídos por sus legítimos destinatarios, impidiendo su acceso a terceros.

**Ventajas:**

 IPSec opera a nivel de red, en lugar de hacerlo en la capa de aplicación como hacen muchos otros protocolos –por ejemplo, el SSL.

 Sus dos modos diferentes hacen que sea una de las formas más seguras de encriptar datos, de ahí que IPSec sea uno de los protocolos más utilizados por las VPN.

 IPSec es prácticamente indetectable, de ahí que tantas VPN lo elijan su protocolo principal.

 IPSec opera en la capa de red en lugar de hacerlo en la capa de aplicación, lo que significa que puede gestionarse en su totalidad desde el sistema operativo, sin necesidad de hacerlo de forma individual desde cada programa.

Desventajas:

 IPSec envuelve cada paquete con una gran cantidad de información, por lo que puede ralentizar la transmisión de paquetes de datos pequeños.

 IPSec es un protocolo bastante más complicado que otros protocolos similares, lo que dificulta su mantenimiento.

**Funcionamiento:**

El protocolo VPN IPSec funciona combinando dos mecanismos fundamentales, AH y ESP, y dos modos de transmisión: el modo túnel y el modo transporte.

IPSec combina dos mecanismos fundamentales que se articulan para garantizar la completa privacidad de la información enviada. Estos mecanismos son la cabecera de autentificación (AH) y la capa de seguridad encapsulada (ESP). Veamos en qué consisten.

**Cabecera de autenticación AH:**

La función de la cabecera de autentificación de IPSec, más conocida simplemente como AH, consiste en la incorporación de una firma digital en cada paquete de datos enviado. La AH permite verificar que solo el destinatario de los datos pueda recibirlos, y a su vez impide que los datos sean modificados antes de llegar a su destino, evitando, por ejemplo, los ataques de intermediario.

**Capa de seguridad encapsulada (ESP):**

Complementaria a la AH, la capa de seguridad encapsulada –ESP– tiene la función de asegurar la encriptación de la información que se encuentra dentro del paquete, de forma que impide que los datos enviados sean accesibles por parte de terceros que puedan interceptar una transmisión. Utiliza tres partes fundamentales para operar: un encabezado ESP, un tráiler y un bloque de verificación.

**Modos de IPSec: Tunel y transporte**

La combinación de los mecanismos de la AH y la ESP permite a IPSec contar con dos modos principales de uso: el modo túnel y el modo transporte. Vamos a ver en qué consiste cada uno.

 Tunel: El modo túnel de IPSec es su modo por defecto. Cuando este modo está activado, IPSec crea un túnel VPN para intercambiar información de forma segura con el servidor. Este túnel queda encriptado por IPSec, y la dirección IP queda enmascarada para terminar de proteger los datos enviados y recibidos.En el modo túnel se introduce un encabezado IPSec (AH o ESP) entre el encabezado IP y la capa superior del protocolo.

 Modo de transporte: El modo de transporte de IPSec se utiliza para comunicaciones de extremo a extremo (entre un cliente y un servidor). Este tipo de encriptación se puede utilizar para realizar sesiones de escritorio remoto. Emplea un encabezado TCP/UDP a través de un encabezado AH o ESP. Suele utilizarse cuando se emplea otro protocolo de tunelización para encapsular el paquete de datos IP, que a su vez queda protegido por el protocolo IPSec.

**Articulación de Ipsec con otros protocolos**

Cuando opera en el contexto de una VPN, IPSec suele utilizarse en combinación con otros protocolos para garantizar la seguridad de los datos y la velocidad de la conexión. Los más comunes son IKEv2 y L2TP.

IKEv2: IKEv2 (Internet Key Exchange version 2) es un protocolo desarrollado por Microsoft y Cisco. Se trata de un protocolo de túnel que cuenta con la principal ventaja de ser particularmente flexible a los cambios de la red, además de ser compatible con diversos sistemas operativos. Usar IPSec con IKEv2 VPN garantiza una conexión robusta con una gran velocidad y estabilidad.

L2TP: El protocolo L2TP (Layer 2 Tunnel Protocol) es un protocolo de túnel que carece de encriptación por sí mismo, de ahí que sea necesario utilizarlo en combinación con un protocolo que sí la tenga, como IPSec. La principal ventaja de L2TP es su velocidad, con lo que muchas VPNs eligen la combinación L2TP/IPSec para garantizarles a sus usuarios una conexión rápida y segura.

**Referencias**

Configuring Ipsec and ISAKMP. Recuperado el 25/05/2021 de: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/ike.pdf>

(07/05/2021) Ipsec que es y cómo funciona. Recuperado el 25/05/2021 de:

<https://nordvpn.com/es/blog/protocolo-ipsec/>

**5. Material y Equipo**

• Computadora

• Acceso a Packet Tracer

**6. Desarrollo**

• Tabla de Comandos

|  |
| --- |
| **Tabla de Comandos** |
| license boot module c1900 technology-package securityk9 |
| crypto isakmp policy 10 |
| encryption aes 256 |
| authentication pre-share |
| group 5 |
| crypto isakmp key vpnpa55 address “IP” |
| crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac |
| crypto map VPN-MAP 10 ipsec-isakmp |

* Diagrama

  Descripción generada automáticamenteTopología
* Tabla de direcciones

|  |  |  |  |
| --- | --- | --- | --- |
| **Dispositivo** | **Interface / vlan** | **IP** | **Mascara** |
| R1 | G0/0.1 | 192.168.20.100 | 255.255.255.0 |
| G0/0.2 | 192.168.20.100 | 255.255.255.0 |
| G0/0.3 | 192.168.20.100 | 255.255.255.0 |
| SW-A | vlan20 | 192.168.20.1 | 255.255.255.0 |
| SW-B | vlan20 | 192.168.20.2 | 255.255.255.0 |
| SW-1 | vlan20 | 192.168.20.3 | 255.255.255.0 |
| SW-2 | vlan20 | 192.168.20.4 | 255.255.255.0 |
| Central | Vlan20 | 192.168.20.5 | 255.255.255.0 |
| C1 | F0/1 – vlan20 | 192.168.20.50 | 255.255.255.0 |
| C2 | F0/1 – vlan10 | 192.168.10.1 | 255.255.255.0 |
| C3 | F0/1 – vlan10 | 192.168.10.2 | 255.255.255.0 |
| C4 | F0/1 – vlan5 | 192.168.5.1 | 255.255.255.0 |
| D1 | F0/1 – vlan5 | 192.168.5.2 | 255.255.255.0 |
| D2 | F0/1 – vlan5 | 192.168.5.3 | 255.255.255.0 |
| D3 | F0/1 – vlan5 | 192.168.5.4 | 255.255.255.0 |
| D4 | F0/1 – vlan10 | 192.168.10.3 | 255.255.255.0 |

* Procedimiento

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Texto

Descripción generada automáticamenteInterfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Interfaz de usuario gráfica

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**7. Observaciones**

Al implementar las VLANs con sus respectivas medidas de seguridad pudimos observar como un diseño temprano que tome en cuenta la existencia de estos recursos de red puede facilitar mucho que se desarrolle el diseño que se tenía planteado. Además, siguiendo los pasos de la actividad no hubo mayor complicación para conseguir el objetivo de la actividad.

**8. Conclusiones**

Con el desarrollo de esta práctica hemos comprendido la importancia de una correcta gestión de las VLANs en caso de ser implementadas para añadir seguridad y cumplir con los principios de integridad y confidencialidad dentro de la red de trabajo. Además, la última parte nos ayudó a reforzar nuestros conocimientos relacionados a las listas de acceso y pudimos apreciar como es posible combinar las diferentes herramientas de seguridad que hemos abordado para generar una mejor protección de la red

**9. Referencias**

(14/08/2020) Seguridad VLANs en entornos virtuales. Recuperado el 24/05/2021 de: <https://www.infosecuritymexico.com/es/blog/seguridad-vlans-virtuales.html>

Seguridad en las VLANs. Recuperado el 24/05/2021 de:

<https://techclub.tajamar.es/seguridad-vlans-tipos-ataques/>