Universidad Nacional Autónoma de México
Facultad de Ciencias

Asignatura: Redes de computadoras
Semestre: 2024-1

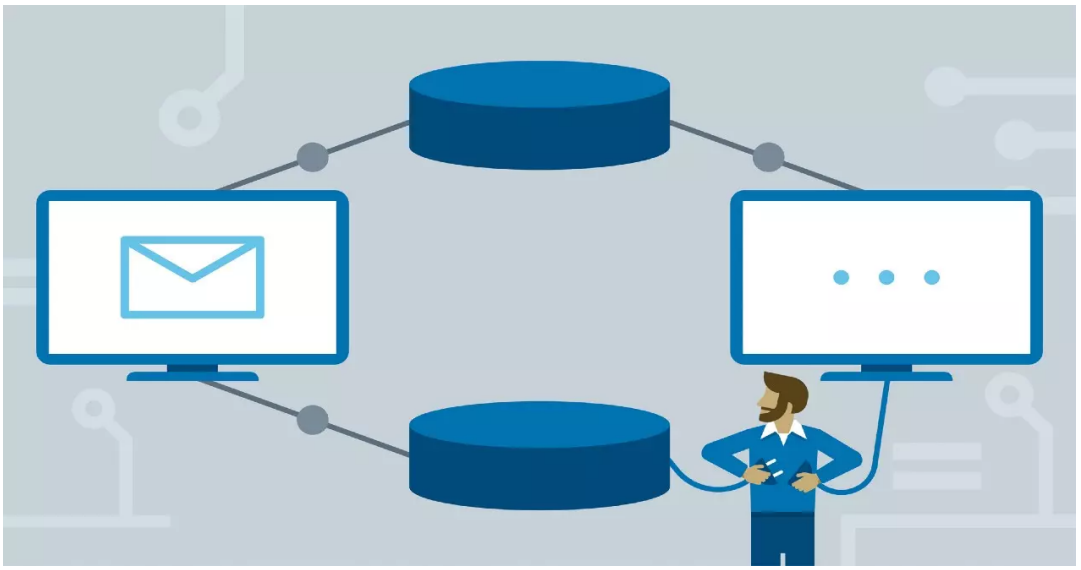
Profesor: Javier León Cotonieto

Ayudantes: Magdalena Reyes Granados
Itzel Gómez Muñoz
Sandra Plata Velázquez

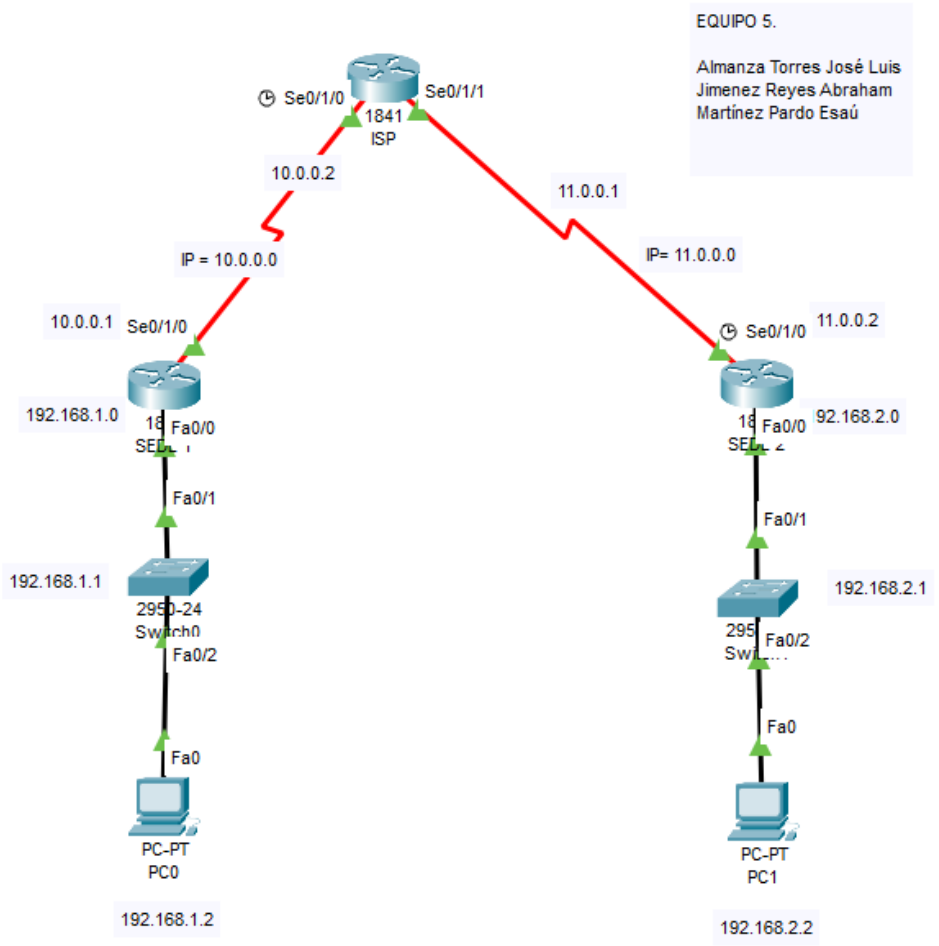
Ejercicio VPN

Equipo 5
Integrantes:

- **Almanza Torres José Luis**
- **Jimenez Reyes Abraham**
- **Martínez Pardo Esaú**



Configuración del ejercicio.



Cuestionario

Ejecute y analice cada uno de los siguientes comandos en el router Sede1 y Sede2:

show crypto isakmp sa

Sede1

```
Router>enable
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

Sede2

```
Router>enable
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

Este comando se utiliza para para ver y listar las asociaciones de Seguridad de Internet Key Exchange (ISAKMP) que están establecidas en el dispositivo. Veamos que ISAKMP es un protocolo de seguridad utilizado en redes VPN (Redes Privadas Virtuales) para establecer las primeras fases de la comunicación segura entre dos dispositivos, por lo que cuando se ejecuta el comando el dispositivo mostrará una lista de las conexiones ISAKMP activas.

show crypto isakmp policy

Sede1

```
Router#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #2 (1024 bit)
        lifetime:                86400 seconds, no volume limit
Default protection suite
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                86400 seconds, no volume limit
Router#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #2 (1024 bit)
        lifetime:                86400 seconds, no volume limit
Default protection suite
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                86400 seconds, no volume limit
Router#
```

Sede 2

```
Router#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #2 (1024 bit)
        lifetime:                86400 seconds, no volume limit
Default protection suite
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                86400 seconds, no volume limit
Router#
```

Este comando se utiliza para mostrar las políticas de seguridad relacionadas con el protocolo ISAKMP (Internet Security Association and Key Management Protocol), por lo que al utilizar este comando se puede observar una lista de las políticas ISAKMP configuradas en el dispositivo.

show crypto ipsec sa

Sede1

```
Router#show crypto ipsec sA

interface: Serial0/1/0
    Crypto map tag: ADMIN, local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.255/0/0)
   remote  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.255/0/0)
   current_peer 11.0.0.2 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.: 10.0.0.1, remote crypto endpt.:11.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x0(0)

     inbound esp sas:

 --More--
```

Sede2

```
Router#show crypto ipsec sA

interface: Serial0/1/0
    Crypto map tag: ADMIN, local addr 11.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.255/0/0)
   remote  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.255/0/0)
   current_peer 10.0.0.1 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.: 11.0.0.2, remote crypto endpt.:10.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x0(0)

     inbound esp sas:

 --More--
```

Este comando se utiliza para poder ver las asociaciones de seguridad (SA) IPsec activas en el dispositivo. Estas asociaciones son muy importantes en la configuración de una VPN para garantizar la confidencialidad, la integridad y la autenticación de los datos que se envían a través de la red.

Conclusiones

Revise los objetivos de la práctica y las actividades realizadas y emita sus conclusiones.

Al realizar este ejercicio, aprendimos los conceptos esenciales de una Red Privada Virtual (VPN) y la importancia que tiene, ya que es una solución que permite a las organizaciones establecer conexiones seguras y económicas entre sus oficinas y usuarios remotos a través de la infraestructura de la red pública, como Internet. Estudiamos que las VPN utilizan tecnologías como IPsec y SSL para proporcionar un alto nivel de seguridad al cifrar y autenticar los datos que se transmiten. Esto asegura que los datos estén protegidos contra accesos no autorizados. Además, las VPN extienden la seguridad a usuarios remotos y adaptan los derechos de acceso de manera individual, lo que mejora la productividad y reduce los costos de comunicación. En el contexto del ejercicio Cisco, se implementó una conexión VPN entre SEDE 1 y SEDE 2, utilizando tecnologías como IPsec para garantizar la seguridad de la comunicación y aprendimos sobre comandos importantes para conocer la estructura y características de una VPN.

Referencias.

- Comprensión y uso de comandos de depuración para solucionar problemas de IPSEC. (2022, 10 octubre). Cisco. https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.htm
- Configuración de la detección del punto extremo del túnel IPSEC. (2022, 13 marzo). Cisco. https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14145-tedpreshare.html