UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

ADMINISTRACIÓN DE REDES
GRUPO: 03
M. C. JAVIER LEÓN COTONIETO

VPN CON IPSEC E ISAKMP

EQUIPO 07
GUTIERREZ SILVESTRE, GRISELDA
ROSALES ROMERO, RICARDO
SANCHEZ BAUTISTA, VELIA
SANTOS ESCOBAR, CHRISTIAN ALEXIS

FECHA DE ENTREGA:
31 DE ENERO DE 2021

CONTENIDO

INTRODUCCIÓN

Comunicar equipos remotos de modo directo es imprescindible en muchas organizaciones, independientemente de donde se encuentren físicamente, y esta necesidad crece cada día más. Las empresas ya tienen redes LAN y WLAN, pero para conseguir que sus empleados puedan entrar a la red desde cualquier lugar de Internet necesitan una red virtual.

Las redes privadas virtuales permiten, mediante el uso de Internet, establecer esta conexión realizando una inversión económica pequeña. Además, como utilizan protocolos de seguridad, el acceso a los recursos tiene carácter privado, por lo que una persona podría acceder a los datos de la empresa en la que trabaja con seguridad.

Montar una VPN (Virtual Private Network, red privada virtual) es establecer una VLAN entre el ordenador del trabajador y la LAN de la empresa, usando Internet. Una VPN o red privada virtual es, básicamente, una red virtual que se crea dentro de otra red, habitualmente Internet.

OBJETIVOS

Objetivo general. Implementar una red privada virtual (VPN) con túnel IPsec que permite la comunicación segura y estable, entre dos sucursales de una empresa.

Objetivos específicos.

- ❏ Establecer lineamientos para el control y buen uso de los sistemas de cómputo y servicios informáticos.
- ❏ Mantener la integridad de los datos.

- ❏ Implementar VPN para crear una comunicación aislada de Internet.
- ❏ Implementar IPsec para encriptación de los datos.
- ❏ Implementar ISAKMP para la asignación de claves criptográficas y la autenticación.
- ❏ Implementar un servidor Syslog para notificar errores.

¿QUÉ ES VPN?

Una red privada virtual VPN (Virtual Private Network), se le conoce al tipo de red que permite una extensión de una red local sobre una red pública o no controlada, como por ejemplo Internet.

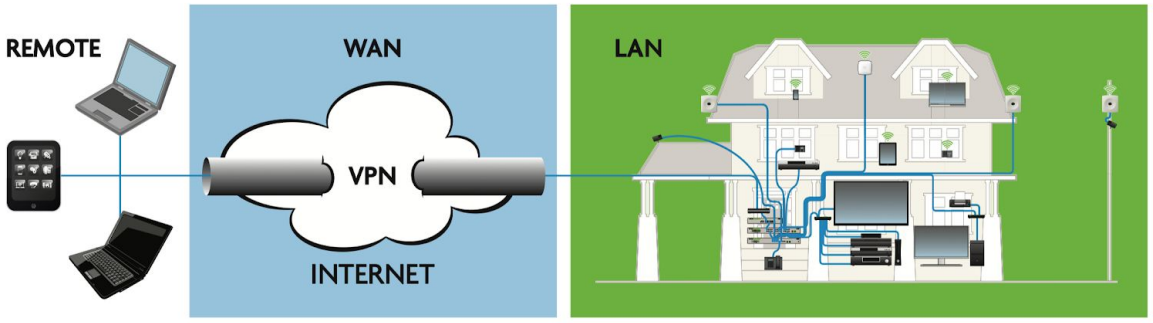


Image 4: Typical VPN Topology

Las VPN's surgen ante la necesidad de las organizaciones o corporativos de proveer a su personal con la capacidad de acceder a su infraestructura de red interna, o intranet desde cualquier lugar y en cualquier momento de forma segura. Así las VPNs aparecen como las redes privadas con la capacidad de utilización de la infraestructura de Internet para el transporte de datos, implementando técnicas de seguridad para mantener la confidencialidad de los datos que se manejan entre los usuarios.

Una VPN correctamente diseñada, debe incorporar estos elementos:

★ Seguridad
★ Confiabilidad
★ Escalabilidad
★ Administración de la red
★ Administración de políticas

PROTOCOLO IPsec

Protocolo que actúa en la capa de red que ofrece seguridad a las redes VPN's. Al actuar en la capa 3 protege protocolos de red, transporte y aplicación. Lo que lo vuelve más seguro y flexible, que por ejemplo, los https que solo funcionan en la capa de aplicación.

¿Qué ofrece IPsec?

- ➔ **Autenticación mutua.** Cada extremo de la comunicación verifica su identidad. Ya sea a través de contraseñas, smart cards, certificados, datos biométricos, etc. Además los paquetes enviados en la comunicación se verifican para confirmar que han sido enviados desde el emisor real. Para ello se usa cifrado asimétrico.
- ➔ **Confidencialidad.** Todos los paquetes se encriptan para protegerlos de intercepciones de terceros no deseadas. Generalmente se usa cifrado simétrico (misma clave) para cifrar y descifrar los paquetes (por ejemplo, AES).
- ➔ **Integridad.** En el destino se verifica que todos los paquetes fueron recibidos íntegramente y que por lo tanto no se han modificado por el camino y no están corrompidos.
- ➔ **Protección de repetición.** Los paquetes enviados cuentan con una identificación única y que luego será descartada. Hecho que asegura que alguien que captura los paquetes no pueda volver a enviarlos al

receptor modificados con su dirección IP para conseguir información privilegiada.

- ➔ **Control de acceso.** Los extremos de la comunicación pueden filtrar mediante ACLs que solo los usuarios (clientes) autorizados se pueden conectar a la VPN.
- ➔ **Protección contra monitorización.** Todos los anteriores puntos dan como resultado una conexión muy segura que inhabilita a un man-in-the-middle saber quienes se están comunicando y con qué frecuencia.

PROTOCOLO ISAKMP

Es un protocolo criptográfico que constituye la base del protocolo de intercambio de claves IKE. ISAKMP define los procedimientos para la autenticación entre pares, creación y gestión de asociaciones de seguridad, técnicas de generación de claves, y la mitigación de la amenaza.

ISAKMP normalmente utiliza IKE para el intercambio de claves aunque pueden ser implementados otros métodos, además define los procedimientos y formatos de paquetes para establecer, negociar, modificar y eliminar las SA (asociaciones de seguridad).

Una Asociación de Seguridad contiene toda la información necesaria para la ejecución de diversos servicios de seguridad de red, como a nivel IP (IPsec AH o ESP), transporte o servicios de la capa de aplicación. ISAKMP define el formato para el intercambio de generación de claves y datos de autenticación.
También proporciona un marco coherente para la transferencia de claves y datos de autenticación, que es independiente de la técnica de generación de claves, el algoritmo de cifrado y el mecanismo de autenticación.

ESCENARIO

Se trata de la empresa **SOFTECK** que configuro una VPN para tener dos sucursales de su empresa conectada de forma segura y con transferencia de paquetes encriptados utilizando llaves en cada router que conecta a ambas LAN. Dicha conexión debe ser remota a través de Internet. Los dos segmentos a conectar, por un lado es la LAN general de la empresa la cual tiene los servidores WEB-DNS y SYSLOG de la empresa y por otro la LAN de la sucursal para los trabajadores del área de desarrollo . Además para mayor control de datos solo es posible conectar dispositivos terminales en los switches del lado de la sucursal remota para evitar que haya bucles en la red.

POLÍTICAS DE SEGURIDAD

Las Políticas de Seguridad Informática son una estrategia integral que desarrolla normas, técnicas y establece lineamientos para el buen funcionamiento y administración dentro de la organización de manera que en caso de presentarse algún imprevisto que pudiera afectar a la organización, su producción o su renombre esta pueda contrarrestar o minimizar este acto de manera que la organización, su trabajo o actividades así como su producción sea afectada lo menos posible.

Políticas de seguridad		
Sí son	**No son**	**Bienes a proteger**
1.Respuestas a las preguntas: ¿Qué es lo que se quiere proteger? ¿De quién o de qué se quiere proteger? ¿Cómo se quiere proteger? ¿Qué se debe proteger? 2. Restricciones que se deben tener en cuenta	1. Cómo implementar la seguridad especificando qué tipo de controles, medidas, mecanismos, para la protección de los bienes 2. Qué herramientas, sistemas, y equipos utilizar para la implementación de la seguridad	1. Instalaciones 2. Equipos 3. Edificios 4. Recursos humanos 5. Renombre o Reputación 6. Marca 7. Propiedad intelectual 8. Información de cualquier tipo y formato 9. Capacitación 10. Experiencia

Filosofía para las políticas

- **Prohibitiva:** Este tipo de filosofía maneja que todo aquello que no está permitido explícitamente está prohibido.
- **Permisiva:** En el caso de esta filosofía se maneja que todo aquello que no está prohibido de manera explícita está permitido.

POLÍTICAS DE USO DE VPN PARA SOFTECK

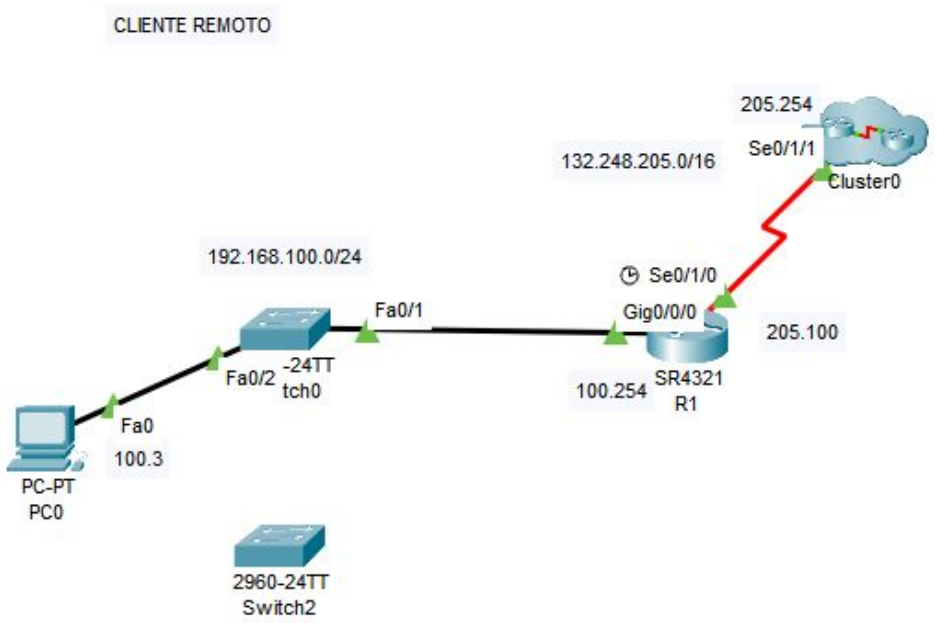
Las siguientes policías entran en vigor el día 30 de Enero del 2021 , siguen la filosofía y siguen la filosofía prohibitiva esto es : “Todo esta prohibido excepto lo que esté específicamente permitido”:

1. Solo los usuarios autorizados podrán utilizar los beneficios del sistema VPN, además serán los responsables del correcto uso de los recursos.
2. Utilizar contraseñas seguras, las cuales deben tener una longitud mínima de 8 caracteres, que deben incluir al menos una mayúscula, minúscula, número o carácter especial.

3. La implementación de un servidor syslog permite guardar mensajes y errores en la red, así se logra monitorear el tráfico de la red.
4. El usuario de la red externa a la red de internet deben ingresar únicamente host en las terminales de la interfaz del switch.
5. Las puertas de enlace VPN deben ser configuradas y administradas por el área de redes.
6. Todos los computadores provistos por la empresa conectados a las redes internas de la misma mediante VPN o cualquier otra tecnología deberán utilizar el software antivirus más actualizado, provisto por el área de soporte del respectivo organismo. Para los equipos personales es responsabilidad del usuario proveer este software antivirus a sus equipos.
7. El sistema VPN debe garantizar integridad, confidencialidad, autenticación y no repudio, para toda la red, su información y las sesiones activas.

IMPLEMENTACIÓN

Topología



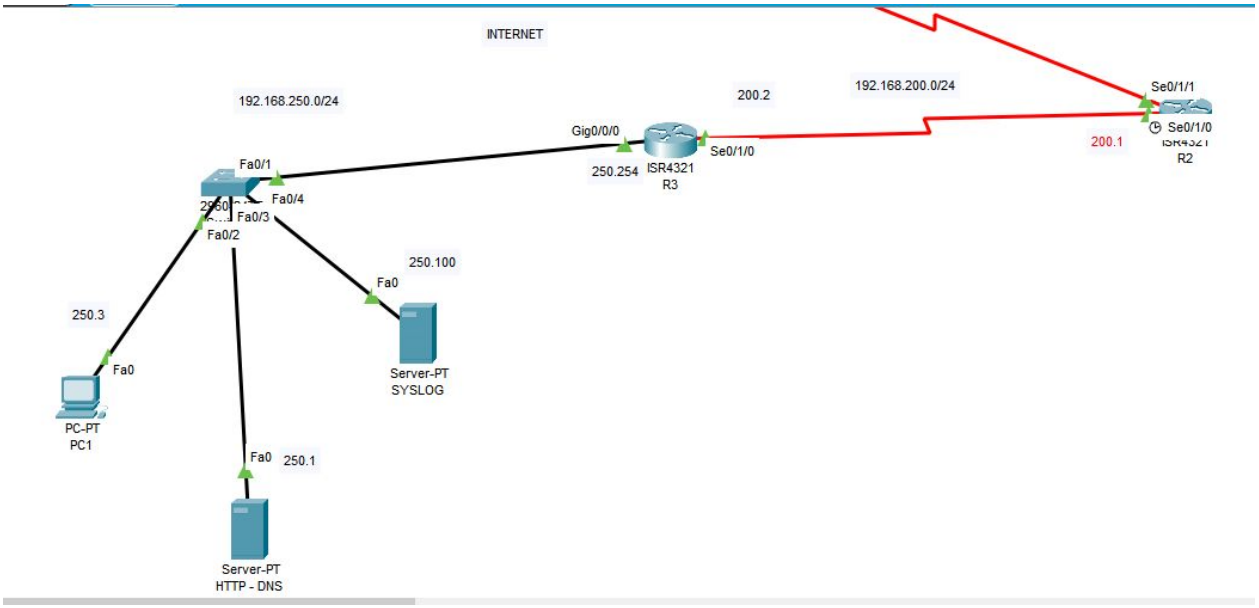


Tabla de Direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Gateway predeterminado
R1	Se 0/1/ 0	132.248.205.100	255.255.0.0	NA
	Gi 0/0/0	192.168.100.254	255.255.255.0	NA
R2	Se 0/1/1	132.248.205.254	255.255.0.0	NA
	Se 0/1/0	192.168.200.1	255.255.255.0	NA
R3	Se 0/1/0	192.168.200.2	255.255.255.0	NA
	Gi 0/0/0	192.168.250.254	255.255.255.0	NA
PC0	Fa 0/0	192.168.100.3	255.255.255.0	192.168.100.254
PC1	Fa 0/0	192.168.250.3	255.255.255.0	192.168.250.254
HTTP - DNS	Fa 0/0	192.168.250.1	255.255.255.0	192.168.250.254
SYSLOG	Fa 0/0	192.168.250.100	255.255.255.0	192.168.250.254

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	DH2	DH2
Vida útil de SA IKE	86 400 segundos o menos	86400	86400
ISAKMP Key (Llave USB)		jFfExO&!#ZHf	jFfExO&!#ZHf

Parámetros de política de fase 2 de IPsec

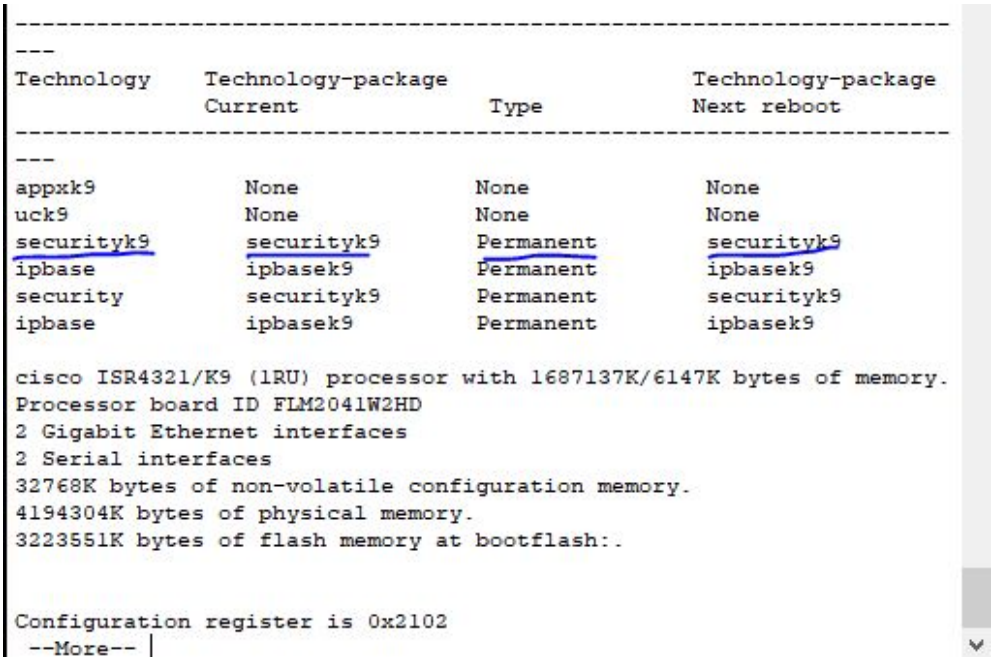
Parámetros	R1	R3
Conjunto de transformaciones	VPN -SET	VPN-SET
Nombre de host del peer	R3	R1
Dirección IP del peer	192.168.200.2	132.248.205.100
Red para cifrar	192.168.250.0	192.168.100.0
Nombre de la asignación criptográfica	VPN-MAP	VPN-MAP
Establecimiento de SA	ipsec-isakmp	ipsec-isakmp

Parte 1: Habilitar las características de seguridad

Activar el módulo securityk9.

Se debe activar la licencia del paquete de tecnología de seguridad para completar esta actividad, para la topología usamos un modelo router que ya tiene la licencia activada, este es el ISR4321 , para asegurarnos que si se tiene el modulo

securityk9 activado a, correr el comando **show version** nos debe mostrar una salida parecida a esta:



```
------------------------------------------------------------------------
---
Technology    Technology-package                  Technology-package
              Current                Type         Next reboot
------------------------------------------------------------------------
---
appxk9           None              None             None
uck9             None              None             None
securityk9       securityk9        Permanent        securityk9
ipbase           ipbasek9          Permanent        ipbasek9
security         securityk9        Permanent        securityk9
ipbase           ipbasek9          Permanent        ipbasek9

cisco ISR4321/K9 (1RU) processor with 1687137K/6147K bytes of memory.
Processor board ID FLM2041W2HD
2 Gigabit Ethernet interfaces
2 Serial interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3223551K bytes of flash memory at bootflash:.


Configuration register is 0x2102
 --More--
```

Parte 2: Configurar los parámetros de IPsec en el R1

Probar la conectividad.

Para esta topología , utilizamos enrutamiento RIPv2 para las redes LAN y ya a la hora de salir a internet , se ocupó enrutamiento estático por defecto activando el **default information originate** para que este enrutamiento se propague por toda nuestra red.

Identificar el tráfico interesante en el R1.

Configuramos 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. por lo que ejecutamos lo siguiente:

R1(config)# access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.250.0 0.0.0.255

Configurar las propiedades de la fase 1 de ISAKMP en el R1.

Configuramos las propiedades de la política criptográfica ISAKMP 10 en el R1 junto con la clave criptográfica compartida cisco. , para ello ejecutamos los siguientes comandos en R1:

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
R1(config)# crypto isakmp key jFfExO&!#ZHf **address 192.168.200.2**

Configurar las propiedades de la fase 2 de ISAKMP en el R1.

Creamos el conjunto de transformaciones VPN-SET para usar esp-3des y esp-sha-hmac. A continuación mostramos los comandos para la asignación criptográfica VPN-MAP que vincula todos los parámetros de la fase 2. Y usamos el número de secuencia 10 cómo 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 192.168.200.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit

Configurar la asignación criptográfica en la interfaz de salida.

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

R1(config)# interface S0/1/0
R1(config-if)# crypto map VPN-MAP

Parte 3: Configurar los parámetros de IPsec en el R3

Para configuración del Router 3 son exactamente los mismos comandos a excepción: el de la configuración de ACL , el origen del peer para el envío de tráfico interesante y con qué dirección se va a asociar la clave compartida.

Parte 4: Verificar la VPN con IPsec

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

0, esto es porque aún no generamos tráfico interesante entre las redes, pero si enviamos un ping de PC0 a PC1, obtenemos lo siguiente

```
Router#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 132.248.205.100

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(192.168.100.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port):
(192.168.250.0/255.255.255.0/0/0)
   current_peer 192.168.200.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 1, #pkts decrypt: 1, #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.: 132.248.205.100, remote crypto endpt.:
192.168.200.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0xEF23A27A(4012089978)

     inbound esp sas:
      spi: 0x8EB11D88(2393972104)
 --More--
```

Podemos observar que la cantidad de paquetes es superior a 0, lo que indica que el túnel VPN con IPsec funciona y nos podemos cerciorar que los dos segmentos de red que están siendo encriptados corresponden a lo que configuramos.
Adicionalmente a esta forma de mantener nuestro tráfico seguro de forma remoto, nos dimos la tarea de implementar un Servidor SYSLOG cómo una forma de monitoreo de nuestra red ,este nos va a ayudar a tener la bitácora o los mensajes que envíen todos nuestros dispositivos de red, adicional a ello debemos configurar un protocolo NTP el cual nos va a servir para poder actualizar la hora o la fecha del dispositivo.

Para configurar la hora actual de forma manual en nuestro dispositivo usamos el comando :

R1#clock set 05:50:20 27 JANUARY 2021

Además NTP nos da la posibilidad de tener un router con router o switch con la hora exacta lo pongamos como ntp master, este comando nos ayuda a definir dicho router o switch cómo nuevo servidor NTP y cualquier otro dispositivo que apunte hacia una ip que esté arriba del router o switch master va a actualizar la fecha y la hora.

R1#ntp master

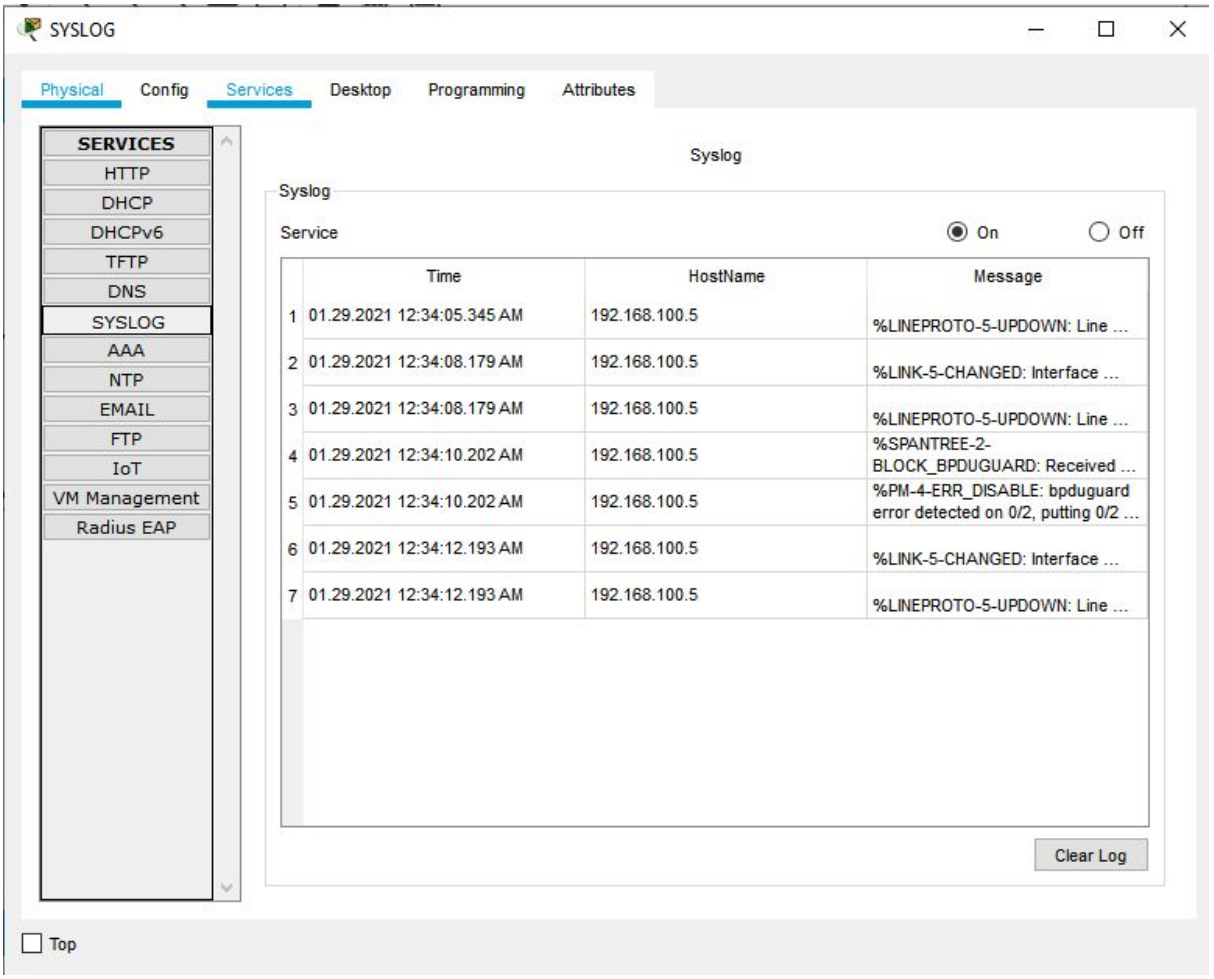
Finalmente para configurar a que cuando el router o switch presenten algún inconveniente o falla , se le notifique a nuestro servidor syslog , ejecutamos el siguiente comando en modo de configuración global.

(config)#logging host 192.168.250.100

Para visualizar que nuestro servidor SYSLOG funciona y cómo medida de seguridad remota ,en el switch que se tiene fuera de la red de la empresa, vamos a configurar el switch para que no exista el STP y además vamos a bloquear sus interface que está en portfast en caso de que esté en un dispositivo intermediario, es decir que si conectamos algún switch a la interfaz automáticamente se apagará y nos lo notificara

Eso se realiza con los siguientes comandos en el Switch0

Switch0(config)# interface vlan 1
Switch0(config-if)# ip address 192.168.100.5 255.255.255.0
Switch0(config-if)# no shutdown
Switch0(config-if)#exit
Switch0(config)#ip default-gateway 192.168.100.254
Switch0(config)#logging host 192.168.250.100
Switch0(config)#service timestamp log datetime msec
Switch0(config)#interface fa 0/2
Switch0(config-if)#spannig-tree portfast
Switch0(config-if)#spannig-tree bpduguard enable
Switch0(config-if)#exit



La imagen anterior muestra los logs generados a intentar conectar un dispositivo intermediario a Switch de la red remota.

Cabe mencionar que todos los dispositivos Router y Switch cuentan con contraseña de acceso y esta tiene un nivel 5 de cifrado , el cual no es tan fácil de vulnerar. Esto lo configuramos usando el comando:

R1(config)#enable secret 5 cisco123

NOTA

Para la simulación de esta política se usaron contraseña fáciles de recortar, pero si llevamos este escenario a la vida real es necesario cumplir con la política número dos.

CONCLUSIÓN

Con la implementación del proyecto se comprobó que se pueden comunicar dos segmentos de red a través de Internet de forma segura, ya que con VPN se mantienen aisladas del resto. Se implementó VPN con cifrado, con ayuda de IPSec, que es un protocolo sencillo con un marco de estándares detallados para comunicaciones con características para fortalecer la seguridad, autenticación del origen y la encriptación del flujo de datos que se mueven a través del túnel. El IPSec no se limita a ningún tipo de algoritmo específico de cifrado, lo que permite mejorar o implementar nuevos algoritmos para proteger los paquetes. Ayudándonos también para mayor seguridad con la implementación de ISAKMP el cual define los procedimientos para la autenticación entre pares, creación y gestión de asociaciones de seguridad, técnicas de generación de claves, y la mitigación de la amenaza, por lo que definimos calves seguros en ambos routers. Además que recordamos cuales son los fundamentos para el buen diseño de las políticas de seguridad y porque son importantes en una empresa. Pudimos reforzar conocimientos de redes , lo que es enrutamiento , enrutamiento estático por defecto , protocolo ntp el cual nos sirve para poder actualizar la hora o la fecha del dispositivo , implementar un servidor SYSLOG el cual nos va a ayudar a tener la bitácora o los mensajes que envíen todos nuestros dispositivos de red , DNS y WEB. Conceptos cómo STP y bpduguard para el control de nuestro switch.

ENLACE DEL VIDEO

★ https://youtu.be/RuzwgG4mJks
★ https://www.youtube.com/watch?v=RuzwgG4mJks

REFERENCIAS

- *[PDF] VPN - Free Download PDF*. (s. f.). VPN. Recuperado enero de 2021,de https://docuri.com/download/vpn_59bf3aaff581716e46c4e555_pdf
- colaboradores de Wikipedia. (2019, 12 julio). *Internet Security Association and Key Management Protocol*. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Internet_Security_Association_and_Key_Management_Protocol
- Plataforma de Javiace Curso Adm. Redes Recuperado en enero del 2021 http://javiace.softgot.com/moodle/pluginfile.php/1749/mod_resource/content/1/scfacls.pdf
- Plataforma de Javiace Curso Adm. Redes Recuperado en enero del 2021 de http://javiace.softgot.com/moodle/mod/resource/view.php?id=452&redirect=1
- Políticas de cómputo y sistemas Recuperado en enero del 2021 de http://www.dirac.mx/documents/dirac-politicas-de-sistemas.pdf
- Informática docuri Recuperado en enero del 2021 de https://docuri.com/download/vpn_59bf3aaff581716e46c4e555_pdf