VPN TUNEL SITIO A SITIO EN GNS3

Trabajo realizado por:

Brenda Marcela Tovar

Natalia Hernández

Yadfary Montoya

Sonia Deyanira Caratar G.

Administración de Redes

(Sena Antioquia)

Tutor: Julian Ciro

2012

VPN: red privada virtual

es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

El ejemplo más común es la posibilidad de conectar dos o mas sucursales de una empresa utilizando como vinculo internet.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública.

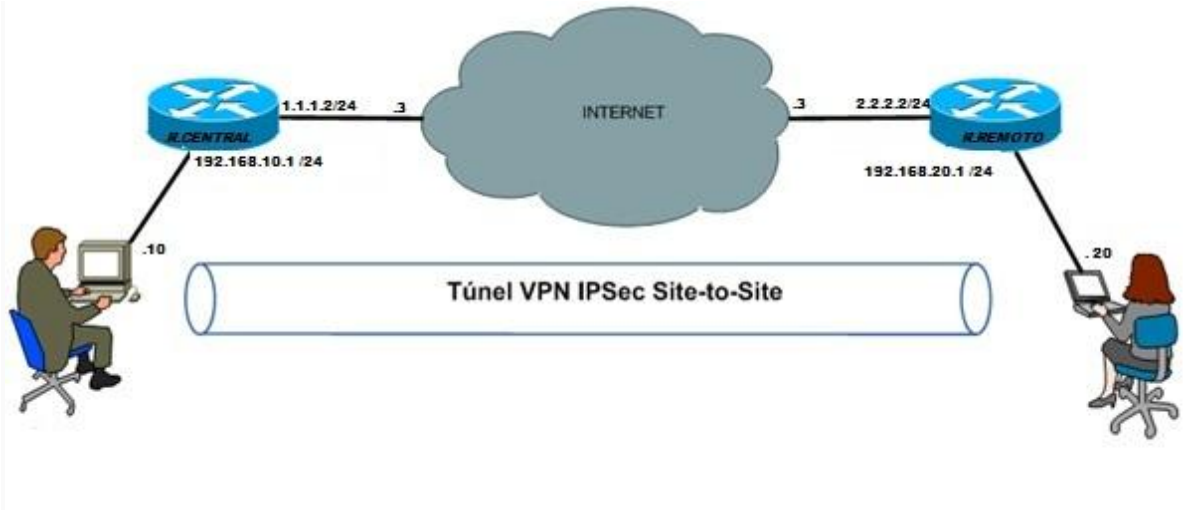
Como se usan redes públicas, en general Internet, es necesario prestar debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autentificación.

Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación.

Autenticación y Autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

Integridad : La garantía de que los datos enviados no han sido alterados.

Confidencialidad : Dado que los datos viajan a través de un medio hostil como Internet, los mismos son susceptibles de interceptación: por eso es fundamental el cifrado de los datos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma.



Para lograr subir la VPN se deben tener en cuenta los siguientes pasos:

<u>para cada nodo</u>

1. configurar las políticas IKE

-establecer la identidad ISAKMP de cada nodo (nombre o IP

-establecer el secreto compartido en cada nodo)

1.1 verificar las políticas IKE

2. configurar el IPSec

-crear crypto ACL

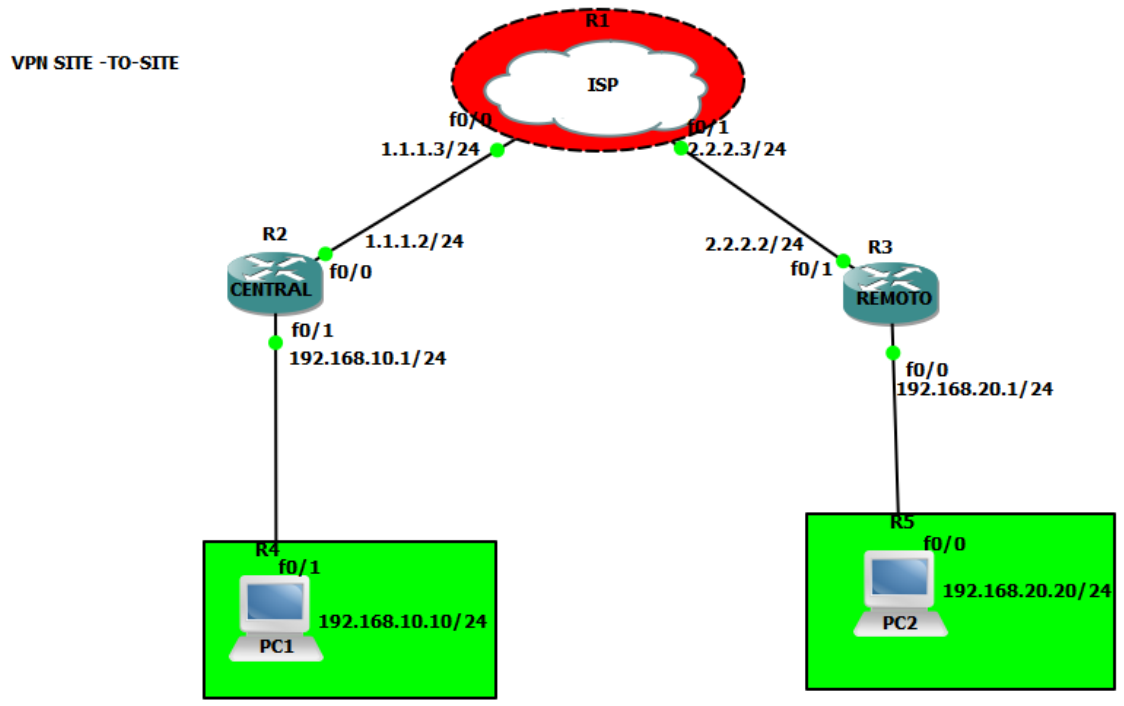
-Definir el transform Set

4.configurar el Crypto map

Un primer paso adicional es validar que los extremos donde vamos a crear la VPN tengan conectividad, para una red de internet es fácil ya que tenemos la ruta por defecto pero en otras situaciones hace falta configurar las rutas respectivas.

Para poder montar un laboratorio y probar este tipo de configuraciones hace falta tener los equipos ya que herramientas como packet tracer no tiene la funcionalidad (por lo menos el que yo tengo no me funciona), sin embargo con GNS3 y una IOS que soporte seguridad se puede montar.

La topología del laboratorio se muestra en la figura siguiente:



Configurar las políticas IKE

Paso	Comando	Objetivo
1	r1(config)# crypto isakmp policy 1	Crear una nueva política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la más prioridad más alta)
2	r1(config-isakmp)# encryption 3des	Especificar el algoritmo de cifrado a utilizar: 56-bit Data Encryption Standard (DES [des]) o 168-bit Triple DES (3des).
3	r1(config-isakmp)# hash sha	Elegir el algoritmo de hash a usar: Message Digest 5 (MD5 [md5]) o Secure Hash Algorithm (SHA [sha]).
4	r1(config-isakmp)# authentication pre-share	Determinar el método de autenticación: pre-shared keys (pre-share), RSA1 encrypted nonces (rsa-encr), o RSA signatures (rsa-slg).

Paso	Comando	Objetivo
5	r1(config-isakmp)# group 2	Especificar el identificador de grupo Diffie-Hellman: 768-bit Diffie-Hellman (1) o 1024-bit Diffie-Hellman (2)
6	r1(config-isakmp)# lifetime 86400	Determinar el tiempo de vide de la Asociación de Seguridad (SA) en segundos. 86400 segundos = 1 día
7	r1(config-isakmp)# exit	Volver al modo de configuración global
Op-cio-nal	r1(config)# cry isakmp keepalive 12 2	Elegir el intervalo de los paquetes hello (por defecto 10 segundos) y el tiempo de reintento cuando un paquete falla.

Paso	Comando	Objetivo
9	r1(config)# crypto isakmp identity address	En la oficina central: elegir la identidad ISAKMP (address o hostname) que el router usará en las negociaciones IKE
10	r1(config)# crypto isakmp key misecretocompartido ip_oficina_remota	En la oficina central: establecer el secreto compartido que se usará con el router de la oficina remota

VERIFICAMOS LAS POLITICAS IKE

show crypto isakmp policy

comprobamos los valores de cada parámetro de seguridad de la política IKE.

```
CENTRAL#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   Three key triple DES
        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
CENTRAL#
```

2. configurar el IPSec

-crear crypto ACL

Paso	Comando	Objetivo
14	r1(config)# access-list 109 permit ip red_oficina_central red_oficina_remota	En la oficina central: cifrar todo el tráfico IP que salga de la oficina central hacia la oficina remota

aquí verificamos el crypto ACL EN CADA EXTREMO

```
REMOTO#show access-lists 109
Extended IP access list 109
    10 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 (43 matches)
REMOTO#
```

```
CENTRAL#show access-lists 109
Extended IP access list 109
    10 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 (34 matches)
CENTRAL#
```

-definir los transform-set

Paso	Comando	Objetivo
17	r1(config)# crypto ipsec transform-set STRONG esp-3des esp-sha-hmac	Esyablece las políticas de seguridad IPSEC que se usarán en las comunicaciones, eligiendo el modo transporte (AH) o túnel (ESP)
18	r1(config-isakmp)# exit	En la oficina remota: cifrar todo el tráfico IP que salga de la oficina remota hacia la oficina central

verificamos el transform set, que es la negociación del túnel.

```
CENTRAL#show crypto ipsec transform-set
Transform set STRONG: { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },


CENTRAL#
```

negociación del túnel

```
REMOTO#show crypto ipsec transform-set
Transform set STRONG: { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },


REMOTO#
```

4. CONFIGURAR EL CRYPTO MAP

20	r1(config)# crypto map NOMBRE 1 ipsec-isakmp	Crear un crypto map de nombre NOMBRE, y establecer el número de secuencia de esta entrada, obligando a usar IKE para establecer SAs.
21	r1(config-crypto-map)# set transform-set STRONG	De los transform sets que se hayan definido, especificar cuál se usara en esta entrada del crypto-map
22	r1(config-crypto-map)# set pfs group 2	Activar Perfect Forward Secrecy
23	r1(config-crypto-map)# set peer dirección-oficina-remota	Definir la dirección del host remoto

24	r1(config-crypto-map)# match address 109	Establecer el tráfico que se va a cifrar (definido previamente en una ACL)
25	r1(config-crypto-map)# ^Z	Volver al modo privilegiado

VERIFICAMOS LA CONFIGURACION DEL CRYPTO MAP

en esta imagen vemos la configuración del crypto map y la dirección de el host remoto en este caso para el router central será la 2.2.2.2 y para el remoto 1.1.1.2.

respectivamente. observamos también el nombre del mapa con su respectiva interface, lista de acceso la red que se está permitiendo.

```
CENTRAL#show crypto map
Crypto Map "REDES" 1 ipsec-isakmp
        Peer = 2.2.2.2
        Extended IP access list 109
            access-list 109 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.
255
        Current peer: 2.2.2.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): Y
        DH group:  group2
        Transform sets={
                STRONG,
        }
        Interfaces using crypto map REDES:
                FastEthernet0/0

CENTRAL#
```

```
REMOTO#show crypto map
Crypto Map "REDES" 1 ipsec-isakmp
        Peer = 1.1.1.2
        Extended IP access list 109
            access-list 109 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.
255
        Current peer: 1.1.1.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): Y
        DH group:  group2
        Transform sets={
                STRONG,
        }
        Interfaces using crypto map REDES:
                FastEthernet0/1

REMOTO#
```

APLICAR EL CRYPTO MAP A LA INTERFAZ FISICA

27	r1(config)# interface XXXX	Entrar al modo de configuración de la interfaz donde se aplicará el crypto map
28	r1(config-if)# crypto map NOMBRE	Aplicar el crypto map a la interfaz física.

con CRL Z volvemos al modo privilegiado, y luego verificamos la asociación de la interfaz 0/0 y el crypto map.

```
CENTRAL#show crypto map interface fastEthernet 0/1
No crypto maps found.

CENTRAL#show crypto map interface fastEthernet 0/0
Crypto Map "REDES" 1 ipsec-isakmp
        Peer = 2.2.2.2
        Extended IP access list 109
            access-list 109 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.
255
        Current peer: 2.2.2.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): Y
        DH group:  group2
        Transform sets={
                STRONG,
        }
        Interfaces using crypto map REDES:
                FastEthernet0/0

CENTRAL#
```

en esta imagen observamos la aplicación del crypto map a la interfaz 0/1 en el router remoto

```
REMOTO#SHow crypto map interface fastEthernet 0/0
No crypto maps found.

REMOTO#SHow crypto map interface fastEthernet 0/1
Crypto Map "REDES" 1 ipsec-isakmp
        Peer = 1.1.1.2
        Extended IP access list 109
            access-list 109 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.
255
        Current peer: 1.1.1.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): Y
        DH group:  group2
        Transform sets={
                STRONG,
        }
        Interfaces using crypto map REDES:
                FastEthernet0/1

REMOTO#
```

COMPROBAR EL FUNCIONAMIENTO DE LAS FACE (1,2,3) EN CADA ROUTER

FACE 1 ROUTER

con el comando **show crypto isakmp sa**

CENTRAL

```
CENTRAL#show crypto isakmp sa
dst             src             state          conn-id slot status
2.2.2.2         1.1.1.2         QM_IDLE              1    0 ACTIVE

CENTRAL#
```

REMOTO

```
REMOTO#show crypto isakmp sa
dst             src             state          conn-id slot status
2.2.2.2         1.1.1.2         QM_IDLE              1    0 ACTIVE

REMOTO#
```

FACE 2

show crypto ipsec sa

he resaltado el proceso de encapsumiento y des encapsulamiento de los paquetes que es uno de los procesos más importantes de esta face2.

CENTRAL

```
CENTRAL#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: REDES, local addr 1.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   current_peer 2.2.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
    #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.: 1.1.1.2, remote crypto endpt.: 2.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x8F261465(2401637477)

     inbound esp sas:
      spi: 0x439A6EC(70887148)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2003, flow_id: SW:3, crypto map: REDES
        sa timing: remaining key lifetime (k/sec): (4570919/1870)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x8F261465(2401637477)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2004, flow_id: SW:4, crypto map: REDES
        sa timing: remaining key lifetime (k/sec): (4570919/1858)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
CENTRAL#
```

REMOTO

```
REMOTO#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: REDES, local addr 2.2.2.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 1.1.1.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19
    #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
    #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.: 2.2.2.2, remote crypto endpt.: 1.1.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:
REMOTO#
```

FACE 3

con el comando **show crypto map**

en esta imagen vemos la configuración del crypto map y la dirección de el host remoto en este caso para el router central será la 2.2.2.2 y para el remoto 1.1.1.2. respectivamente. observamos también el nombre del mapa con su respectiva interface, lista de acceso la red que se está permitiendo.

```
CENTRAL#show crypto map interface fastEthernet 0/0
Crypto Map "REDES" 1 ipsec-isakmp
        Peer = 2.2.2.2
        Extended IP access list 109
            access-list 109 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.
255
        Current peer: 2.2.2.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): Y
        DH group:  group2
        Transform sets={
                STRONG,
        }
        Interfaces using crypto map REDES:
                FastEthernet0/0

CENTRAL#
```

vemos la combinación de los parámetros de seguridad (cifrado, hash, autenticación y DH) que serán usados durante la negociación IKE.

```
CENTRAL#show run | section crypto
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key misecretocompartido address 2.2.2.2
crypto isakmp keepalive 122
crypto ipsec transform-set STRONG esp-3des esp-sha-hmac
crypto map REDES 1 ipsec-isakmp
 set peer 2.2.2.2
 set transform-set STRONG
 set pfs group2
 match address 109
 crypto map REDES
CENTRAL#
```

```
REMOTO#show run | section crypto
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key misecretocompartido address 1.1.1.2
crypto isakmp keepalive 122
crypto ipsec transform-set STRONG esp-3des esp-sha-hmac
crypto map REDES 1 ipsec-isakmp
 set peer 1.1.1.2
 set transform-set STRONG
 set pfs group2
 match address 109
 crypto map REDES
REMOTO#
```

COMPROBACIÓN DE RUTAS ESTATICAS

Podemos comprobar la configuración y el funcionamiento de las rutas estáticas mediante el comando ping. Para comprobar la configuración en caso de fallas usar el comando **show ip route** para ver las tablas de enrutamiento. Las marcadas con "C" son las redes directamente conectadas y las marcadas con "S" son las rutas estáticas.

TABLAS DE ENRUTAMIENTO EN CADA ROUTER

ROUTER REMOTO

```
REMOTO#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 2.2.2.3 to network 0.0.0.0

     2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, FastEthernet0/1
C    192.168.20.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 2.2.2.3
REMOTO#
```

ROUTER CENTRAL

```
CENTRAL#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 1.1.1.3 to network 0.0.0.0

     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, FastEthernet0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 1.1.1.3
CENTRAL#
```

en las próximas imágenes observamos la configuración de cada una de las interfaces en los respectivos routers ubicados en los extremos de la topología realizada en este pequeño tutorial .

```
REMOTO#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 97 bytes
!
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
end

REMOTO#show running-config interface fastEthernet 0/1
Building configuration...

Current configuration : 110 bytes
!
interface FastEthernet0/1
 ip address 2.2.2.2 255.255.255.0
 duplex auto
 speed auto
 crypto map REDES
end

REMOTO#
```

vemos las direcciones ip configuradas de manera estática en sus respectivas interfaces.

una ip privada y la otra publica con mascara 24 respectivamente

```
CENTRAL#show running-config interface fastEthernet 0/1
Building configuration...

Current configuration : 97 bytes
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
end

CENTRAL#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 110 bytes
!
interface FastEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 duplex auto
 speed auto
 crypto map REDES
end

CENTRAL#
```

en la siguiente imagen observamos la política de seguridad creada anteriormente con un nivel de seguridad alto como es el 1, también vemos el algoritmo de cifrado 3DES, siendo mas precisa vemos la combinación de los parámetros de seguridad (cifrado, hash, autenticación y DH) que
serán usados durante la negociación IKE. que fueron creadas en los 2 extremos en este caso solo muestro la de un extremo como es el remoto.

```
REMOTO#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   Three key triple DES
        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
REMOTO#
```

PING ENTRE ROUTERS

observamos la conectividad que es exitosa dando un ping a la interface fastethernet 0/1, del ISP y la 2.2.2.2 del router remoto.

nota: no olvidar configurar la ruta por defecto en cada router

0.0.0.0 0.0.0.0 direccion del otro router por donde va a salir (inside)

```
CENTRAL#ping 2.2.2.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/41/76 ms
CENTRAL#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/56/92 ms
CENTRAL#
```

```
REMOTO#ping 1.1.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/35/48 ms
REMOTO#ping 1.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/66/88 ms
REMOTO#
```

PING ENTRE LOS PC 1-2

```
PC1#ping 192.168.20.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/125/192 ms
PC1#
```

```
PC2#ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/126/172 ms
PC2#
```

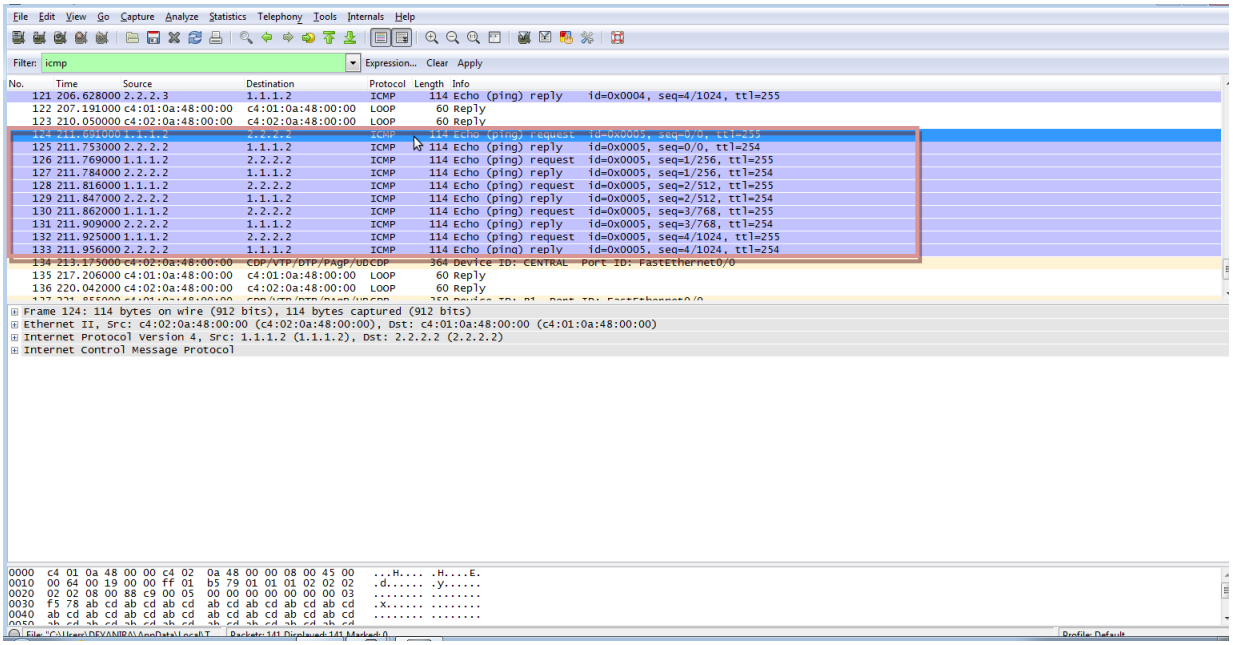
CAPTURA DEL TRAFICO EN WIRESHARK

Aquí en esta imagen capturamos el trafico ICMP en este caso capturas de paquetes de ping; Esta imagen corresponde con la lista de visualización de todos los paquetes del ping.

que se están capturando en tiempo real. (tipo de protocolo, números de secuencia,

flags, marcas de tiempo, puertos, etc.) nos va a permitir, en ciertas ocasiones,

deducir el problema sin tener que realizar una auditoría minuciosa.



ARCHIVO DE CONFIGURACION DE ROUTER CENTRAL:

CENTRAL#SHOW RUNning-config

Building configuration...

Current configuration : 1484 bytes

!

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CENTRAL
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
```

```
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key misecretocompartido address 2.2.2.2
crypto isakmp keepalive 122
```

```
!
!
crypto ipsec transform-set STRONG esp-3des esp-sha-hmac
!
crypto map REDES 1 ipsec-isakmp
 set peer 2.2.2.2
 set transform-set STRONG
 set pfs group2
 match address 109
!
!
!
!
interface FastEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 duplex auto
 speed auto
 crypto map REDES
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
```

```
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 1.1.1.3
!
!
```

```
no ip http server
no ip http secure-server
!
access-list 109 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
```

```
!
!
end

CENTRAL#
```

ARCHIVO DE CONFIGURACION DE ROUTER REMOTO:

```
REMOTO#SHOW RUNning-config
Building configuration...

Current configuration : 1483 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname REMOTO
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
```

```
ip cef
!
!
!
!
no ip domain lookup
ip auth-proxy  max-nodata-conns  3
ip admission max-nodata-conns  3
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key misecretocompartido address 1.1.1.2
crypto isakmp keepalive 122
!
!
crypto ipsec transform-set STRONG esp-3des esp-sha-hmac
!
crypto map REDES 1 ipsec-isakmp
 set peer 1.1.1.2
 set transform-set STRONG
 set pfs group2
 match address 109
!
!
!
!
```

```
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 2.2.2.2 255.255.255.0
 duplex auto
 speed auto
 crypto map REDES
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
```

```
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 2.2.2.3
!
!
no ip http server
no ip http secure-server
!
access-list 109 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
!
!
!
control-plane
!
!
!
!
!
```

```
!
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
end

REMOTO#
```

ARCHIVO DE CONFIGURACION DEL ISP

```
R1#show running-config
Building configuration...

Current configuration : 1022 bytes
!
version 12.4
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 1.1.1.3 255.255.255.0
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 ip address 2.2.2.3 255.255.255.0
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
```

```
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
```

```
line aux 0
line vty 0 4
 login
!
!
end

R1#
```