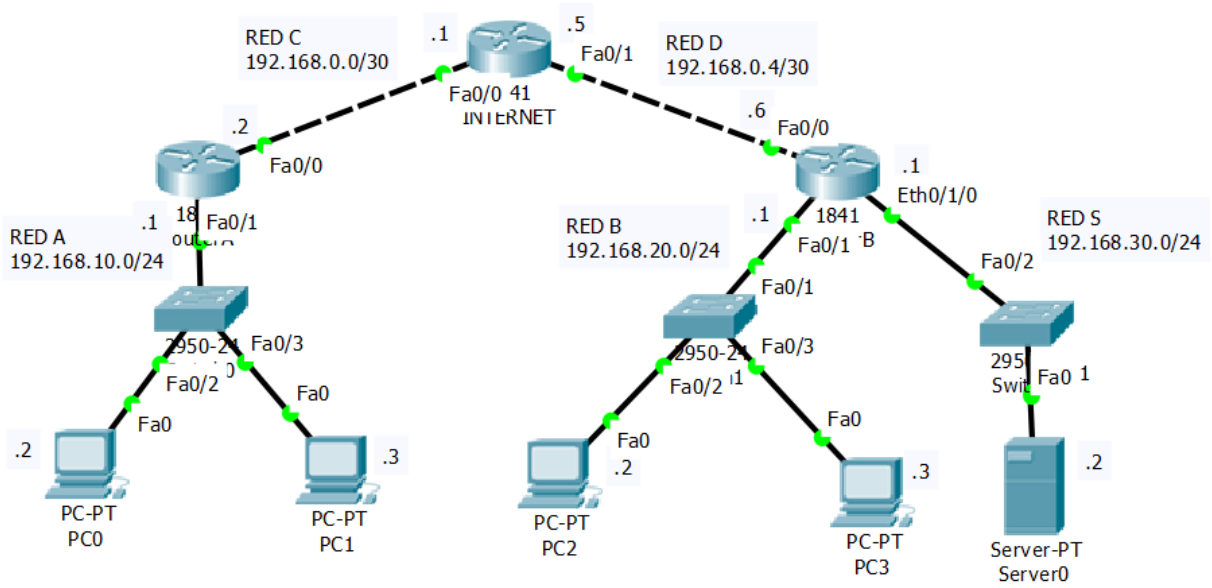
PECL5

Seguridad en redes IP

GII Redes de Computadores Laboratorio 08:00 a 10:00

Juan Casado Ballesteros 09108762A



Listas de acceso estándar

Una vez configurados los equipos según el esquema y comprobada su conectividad mediante el comando ping procedemos a configurar las listas de acceso estándar indicadas para ellos. Inicialmente podemos acceder al Server0 desde cualquiera de los equipos de la topología.

Este es un ejemplo de un ping desde PC2 a Server0

```
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.30.2: bytes=32 time=1ms TTL=125
Reply from 192.168.30.2: bytes=32 time=2ms TTL=125
Reply from 192.168.30.2: bytes=32 time<1ms TTL=125
Reply from 192.168.30.2: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Creamos una lista de acceso de la siguiente forma y se la aplicamos a la interface correspondiente (Eth0/1/0) en el ROUTER B de forma que los paquetes se rechacen a la salida de la interface, comprobamos como ahora solo podemos acceder al Server0 desde PC0.

```
Router(config)#access-list 1 permit host 192.168.10.2
Router(config)#interface Eth0/1/0
Router(config-if)#ip access-group 1 out
```

El ping se corresponde a PC2 intentando acceder a Server0 sin éxito.

```
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.0.6: Destination host unreachable.
Reply from 192.168.0.6: Destination host unreachable.
Reply from 192.168.0.6: Destination host unreachable.
Reply from 192.168.0.6: Destination host unreachable.

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Creamos ahora una nueva lista de acceso que aplicamos a la misma interface en el mismo router y también en su salida pero en este caso que permita a todos los equipos de la RED A acceder a Server0

```
Router(config)#access-list 2 permit 192.168.10.0 0.0.0.255
Router(config)#interface Eth0/1/0
Router(config-if)#ip access-group 2 out
```

Las listas de acceso se crean y se aplican sobre las interfaces, sobre una o sobre todas en las que sea necesario hacerlo, mostramos ahora como aplicar la lista de acceso 2 a otra interface del router, en este caso Fa0/1, con ello conseguimos que a los equipos de la RED B solo puedan acceder los de la RED A.

```
Router(config)#interface Fa0/1
Router(config-if)#ip access-group 2 out
```

Listas de acceso extendido

Creamos una lista de acceso extendida para bloquear el tráfico FTP en la RED A, esta lista de acceso la aplicamos al ROUTER B en la interface Eth0/1/0 en modo out.

```
Router(config)#access-list 101 deny tcp 192.168.10.0 0.0.0.255 any eq 21
Router(config)#access-list 101 deny tcp 192.168.10.0 0.0.0.255 any eq 20
Router(config)#access-list 101 permit ip any any
Router(config)#interface Eth0/1/0
Router(config-if)#ip access-group 101 out
```

permit ip any any hace que cualquier otro tráfico no referencia por el resto de instrucciones sea aceptado, de otra forma este no llegaría.

Como podemos ver antes de aplicar la lista de acceso extendido podíamos conectarnos por FTP a Server0 desde PC0

```
C:\>ftp 192.168.30.2
Trying to connect...192.168.30.2
Connected to 192.168.30.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Una vez aplicada la lista de acceso extendido ya no podemos conectarnos a Server0 por medio de FTP desde PC0.

```
C:\>ftp 192.168.30.2
Trying to connect...192.168.30.2

%Error opening ftp://192.168.30.2/ (Timed out)
.



(Disconnecting from ftp server)
```

Podemos comprobar como con otros protocolos si podemos seguir accediendo a Server0 desde PC0

```
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.30.2: bytes=32 time<1ms TTL=125
Reply from 192.168.30.2: bytes=32 time=1ms TTL=125
Reply from 192.168.30.2: bytes=32 time<1ms TTL=125
Reply from 192.168.30.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

O inconcluso como otros equipos fuera de la RED A pueden hacerlo como PC2 de la RED B.

```
C:\>ftp 192.168.30.2
Trying to connect...192.168.30.2
Connected to 192.168.30.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

VPN con IPsec modo túnel

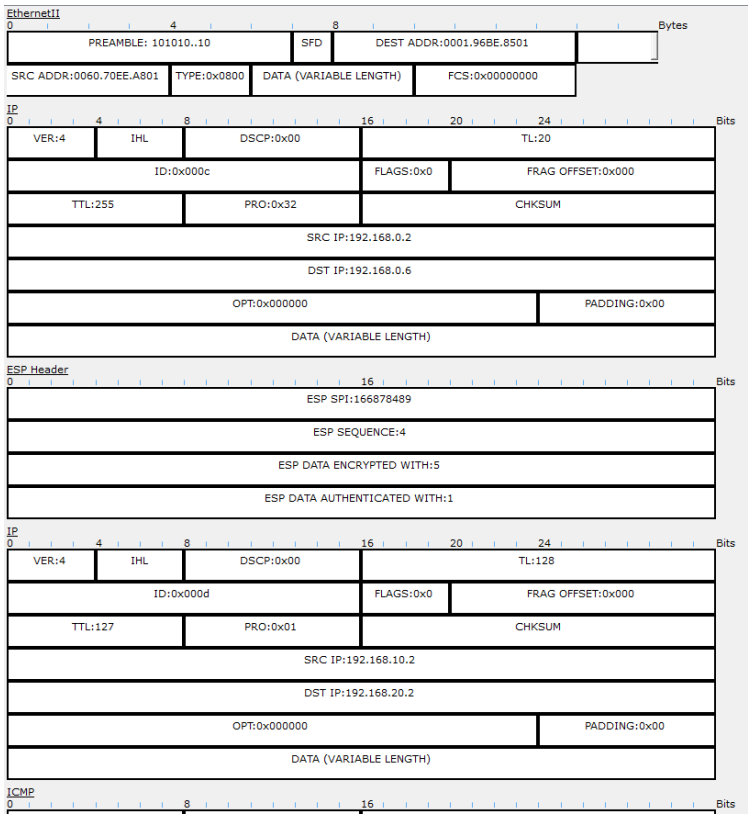
Para configurar el ROUTER B necesitamos introducir los siguientes comandos:

```
Router>enable
Router#config term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#exit
Router(config)#crypto isakmp key vpnuser address 192.168.0.2
Router(config)#crypto ipsec transform-set myset esp-des esp-md5-
hmac
Router(config)#crypto map mymap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#set peer 192.168.0.2
Router(config-crypto-map)#set transform-set myset
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#exit
Router(config)#interface fa0/0
Router(config-if)#crypto map mymap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
Router(config)#access-list 100 permit ip 192.168.20.0 0.0.0.255
192.168.10.0 0.0.0.255
Router(config)#exit
```

Los datos se encapsulan por **modo túnel** mediante una nueva cabecera IP y una cabecera ESP, dentro del encapsulado se encuentra la cabecera IP original y el resto de datos a transportar.

La autenticación de los datos se realiza por **pre-shared**, los routers comparten una clave que debe ser común y configurada en el router.

En la cabecera ESP destaca campo ESP SPI identifica a los parámetros de seguridad junto con la dirección IP y el campo ESP SEQUENCE va aumentando según se produce la transmisión de paquetes.



Comprobamos que el túnel creado funciona correctamente.

```
Router#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: mymap, local addr 192.168.0.6

   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 192.168.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
   #pkts decaps: 7, #pkts decrypt: 7, #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.: 192.168.0.6, remote crypto endpt.:
192.168.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x13700F67(326111079)

     inbound esp sas:
      spi: 0x09F25D19(166878489)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4525504/3560)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x13700F67(326111079)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2010, flow_id: FPGA:1, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4525504/3560)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Antes de poder realizar la autenticación de los datos ambos routers deben comprobar que han sido configurados con la misma clave, para ellos se comunican con paquetes ISAKMP.

Si ponemos claves no iguales en los router estos se darán cuenta y no podrán realizar la autenticación de los datos enviados.

Ya que la autenticación no puede realizarse la comunicación entre ambas redes no se podrá realizar.