Como ya he comentado en este mismo punto, las necesidades en prestaciones para estos servidores no son altas, por este motivo se ha buscado servidores económicos, de gama baja, con la única necesidad extra que la de tener dos adaptadores de red para poder realizar la configuración de ISA Server 2004.

De la simple comparación de los dos servidores encontrados con estas características podemos realizar la decisión.

Se aprecia claramente que HP ProLiant DL120 G5 está una generación por encima de DeLL PowerEdge SC1435, puesto que monta procesadores Quad-Core.
Pero no sería este el único motivo, puesto que ofrece mayores prestaciones y a un precio más competitivo.

Por tanto la elección es clara, el servidor de 1U HP ProLiant DL120 G5 resulta ideal para nuestra infraestructura informática, pudiendo soportar la única aplicación (ISA Server) que se le va a instalar.

6.6.1.1 Instalación de ISA Server 2004

Esta instalación se realiza sobre un servidor elegido anteriormente con un sistema Microsoft Windows Server 2003 instalado.

La versión instalada es ISA Server 2004 Standard Edition con un coste de licencia por procesador de 936,87 euros + 16% iva.

La elección de ISA Server 2004 viene dada porque contiene un firewall a nivel de aplicación con características que nos ayudan a protegernos frente a amenazas de intrusión, tanto internas como externas.

Otro motivo es que ISA Server 2004 realiza una inspección minuciosa de los protocolos de Internet, como el Protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol), lo cual nos permite detectar numerosas amenazas que se escapan a los firewalls tradicionales.

Además el firewall integrado y la arquitectura de VPN de ISA Server 2004 nos permiten el filtrado y la inspección de estado de todo el tráfico VPN.

Posibilitándonos la inspección de los clientes VPN de las delegaciones.

Para la instalación he utilizado el Asistente de instalación de Microsoft ISA Server 2004, siguiendo los siguientes pasos:

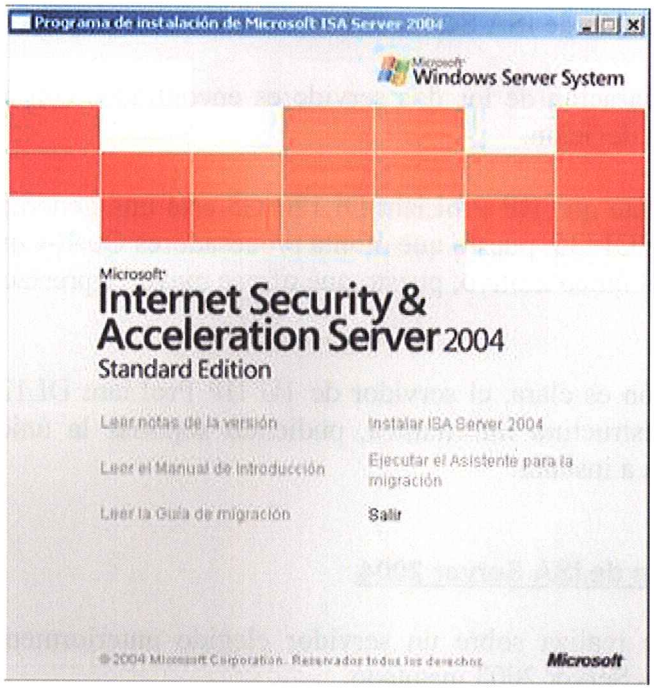


Ilustración 6-16: Instalación ISA Server 2004

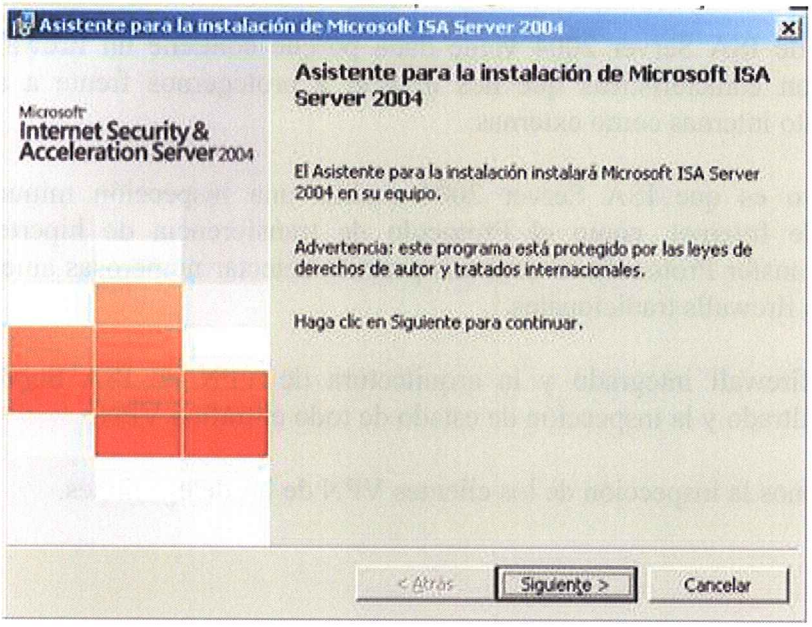


Ilustración 6-17: Asistente para la instalación ISA Server 2004 - 1

Voy a realizar una instalación con el **Tipo de instalación: "Instalación típica.** De esta manera se instalarán las características principales del programa.

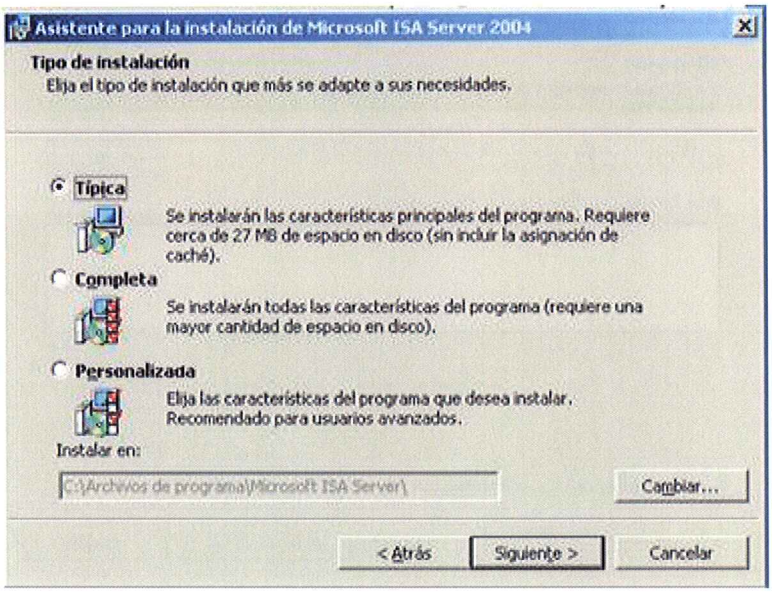


Ilustración 6-18: Asistente para la instalación ISA Server 2004 - 2

El asistente durante la instalación nos mostrará la **Red interna**, donde se deben especificar los rangos de direcciones que se desean incluir en la red interna del servidor ISA.

Como ya he comentado tendré que instalar un ISA por punto de conexión.
Por lo cual los rangos de IP internos serán diferentes en cada caso:
España

- Red Oficina Central he incluido el rango de IPs 10.10.1.1 – 10.10.198.254
- Red Oficina Delegación he incluido el rango de IPs 10.10.199.1 – 10.10.254.254

Rumania

- Red Oficina Rumania he incluido el rango de IPs 10.10.210.1 – 10.10.210.254
- Red Oficina Grupo he incluido el rango de IPs 10.10.1.1 – 10.10.200.254 y 10.10.220.1 – 10.10.239.254

Colombia

- Red Oficina Colombia he incluido el rango de IPs 10.10.210.1 – 10.10.220.254
- Red Oficina Grupo he incluido el rango de IPs 10.10.1.1 – 10.10.200.254 y 10.10.210.1 – 10.10.219.254 y 10.10.230.1 – 10.10.239.254

China

- Red Oficina China he incluido el rango de IPs 10.10.220.1 – 10.10.230.254
- Red Oficina Grupo he incluido el rango de IPs 10.10.1.1 – 10.10.200.254 y 10.10.210.1 – 10.10.229.254

He dejado el rango 10.10.199.1 – 10.10.200.254 como externo a todas las sedes porque va a ser dedicado a crear las VPN.

ISA Server cuando se refiere a red interna se esta refiriendo a la LAN, aquellas direcciones que consideramos privadas de cada oficina.

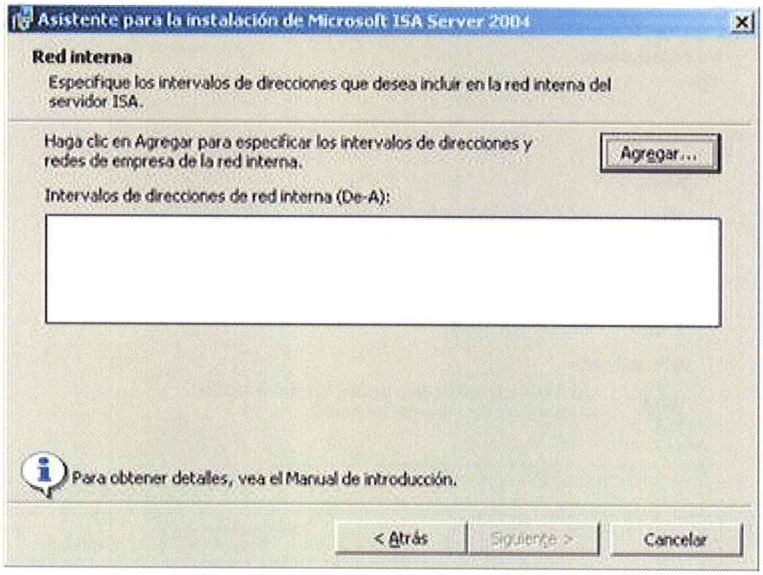


Ilustración 6-19: Asistente para la instalación ISA Server 2004 - Red interna -1

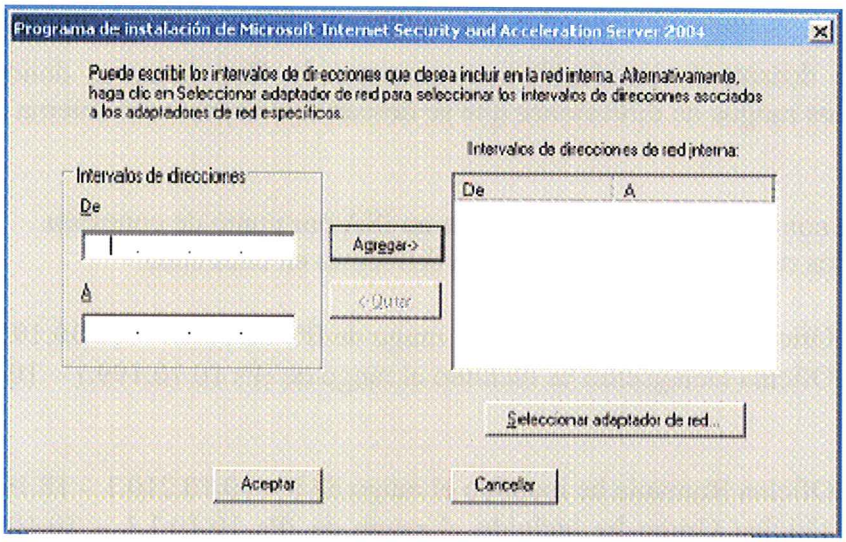
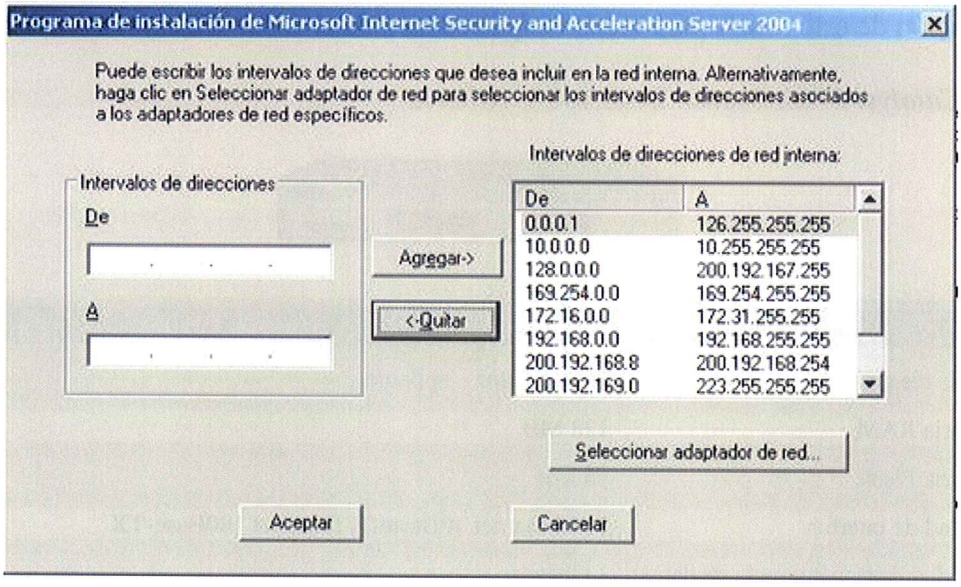


Ilustración 6-20: Asistente para la instalación ISA Server 2004 - Red interna -2

Para acaba la instalación de ISA Server solamente queda seleccionar el **Adaptador de Red,** como adaptador he seleccionado aquel o aquellos que forman parte de la red interna, es decir, los que están conectados a la sección en la que están las estaciones de trabajo.

Una vez seleccionado el adaptador el asistente incluye los intervalos de dirección de la red, redes internas. Estar realizando la instalación con un asistente de vez en cuando da problemas, como es el caso. Introduce intervalos que no nos interesa que estén dentro.

La solución es fácil, he quitado aquellos que no pertenecían a los intervalos de red interna con el botón **Quitar** desde Intervalos de direcciones de red interna.



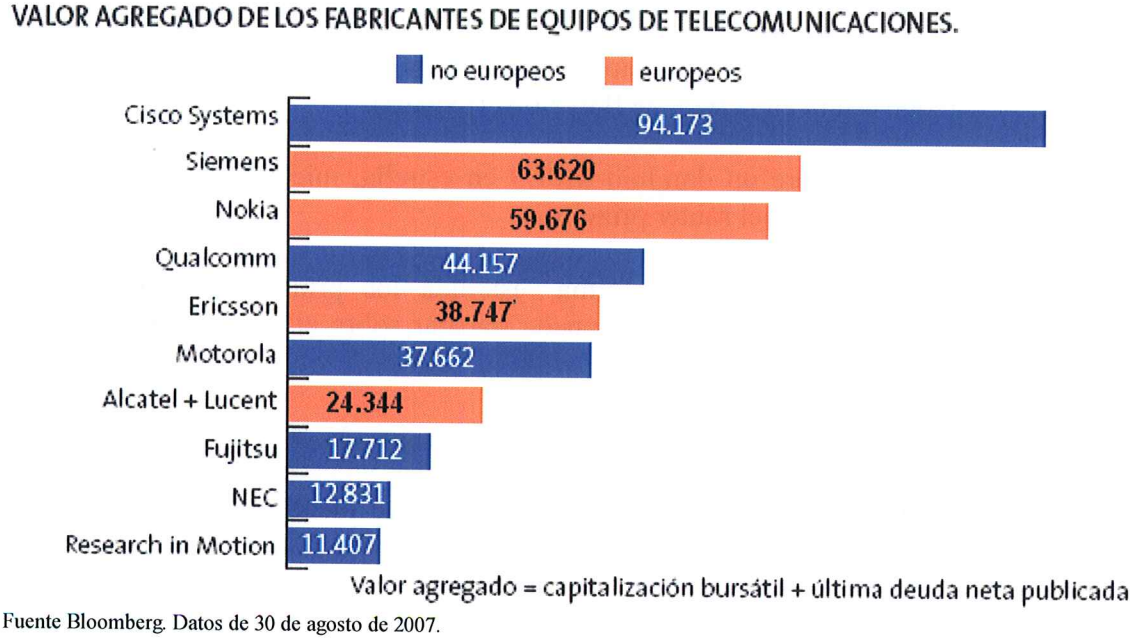
A partir de aquí solamente queda pulsar el botón **Instalar** para comenzar la instalación. Y **Finalizar** para finalizar el asistente de la misma.

Una vez elegidos los servidores e instalados voy a pasar al siguiente punto, elegir y configurar los routers que se van a interconectar sobre el domino MPLS.

6.6.2 Routers MPLS

Para implantar la solución MPLS elegida necesitamos de cuatro routers con la capacidad de soportar MPLS.

Referente a la elección de los routers no he tenido duda de decantarme directamente hacia Cisco Systems. Por dos motivos, la fiabilidad y la capacidad de soportar copias de seguridad de la configuración.



Fuente Bloomberg. Datos de 30 de agosto de 2007.

Ilustración 6-21: Valor agregado por los fabricantes de equipos de telecomunicaciones

La elección de este router para todos los países ha sido el Cisco Catalyst 3750.

Cisco Catalyst 3750: Precio: 2466,16€ + 16% iva

Especificación principal – Cisco Catalyst 3750	
Tipo de dispositivo	Conmutador – apilable
Memoria RAM	128 MB
Memoria Flash	16 MB
Cantidad de puertos	24x Ethernet 10Baste-T, Ethernet 100Base-TX
Velocidad de transferencia de datos	1 Gbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Ranuras vacías	2 x SFP (mini-GBIC)
Protocolo de gestión remota	SNMP 1, SNMP 2, SNMP 3, RMON, RMON 2, Telnet
Modo comunicación	Semidúplex, dúplex pleno
Características	Control de flujo, capacidad duplex, encaminamiento, auto sensor por dispositivo, soporte de DHCP, negociación automática, soporte ARP, concentración de enlaces, equilibrio de carga, soporte VLAN, snooping IGMP, activable, apilable
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
Alimentación	CA 120/230 V (50/60 Hz)
MTBF (tiempo medio entre errores)	294,928 hora(s)

Tabla 6-5: Especificación principal - Cisco Catalyst 3750

Se instalará un router en la sede principal de cada país, interconectando todos con el router principal que estará en la sede de Barcelona (España).

Se estructura una red sobre un dominio MPLS en estrella, iniciando la conexión las sedes que se conectan contra el router principal.

En este punto intento describir de forma resumida los principales comandos de configuración del router Cisco para que pueda trabajar sobre el dominio MPLS de la manera descrita.

Una vez realizada la configuración del primer router, gracias al sistema de backup y restore del cual disponen se puede configurar los demás volcando la información del primero y cambiando solamente aquellos parámetros que identifiquen las redes y el router.

En la siguiente ilustración se muestra lo descrito:

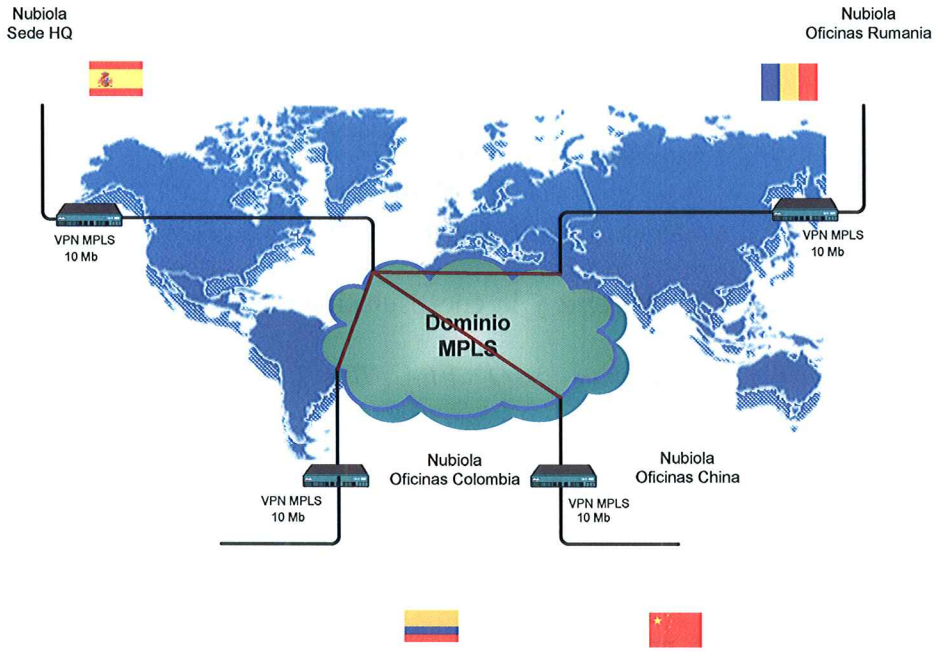


Ilustración 6-22: Implantación de routers MPLS

A continuación explico todos los puntos de configuración aplicados a los routers para un correcto funcionamiento con lo descrito. Lo explicaré de una manera genérica poniendo entre corchetes aquellos datos que dependan del router y de la situación geográfica del mismo.

6.6.2.1 Configuración de una interfaz loopback

La interfaz de loopback nos servirá para el identificador del router de cada país.
Para crear el interfaz de loopback lo he realizado de la siguiente manera:

cisco# configure terminal
cisco(config)# interface loopback 0
cisco(config-if)# ip address <dirección IP> 255.255.0.0

Configuro el interfaz de loopback porque más adelante en la configuración de OSPF [25] y de BGP [26] asociaré este interfaz a los procesos OSPF y BGP, asegurando de esta manera que no se van a perder las sesiones OSPF o BGP por cualquier problema físico en el interfaz puesto que las interfaces de loopback son interfaces lógicas.

[25] *OSPF: Open Shortest Path First.*
[26] *BGP: Border Gateway Protocol.*

6.6.2.2 Configuración de subinterfaces

La creación y configuración de subinterfaces la he realizado siguiendo los siguientes pasos:

cisco# configure terminal
cisco(config)# interface fastethernet0/0.100
cisco(config-subif)# encapsulation dot1Q <VLAN ID>
cisco(config-subif)# ip address 10.10.10.1 255.255.255.0

Una vez configurada la subinterfaz y la encapsulación para Levantar la interfaz física con no shutdown.
cisco(config-subif)# encapsulation dot1Q <VLAN ID>

6.6.2.3 Configuración básica de OSPF

Vamos a configurar OSPF como protocolo de routing dinámico en el futuro backbone MPLS.

Arrancaremos primero el proceso OSPF:

cisco(Config)# router ospf 1

Definiremos el área en la cual se encuentra cada interfaz del router, lo realizaré con el comando "network", con el cual especificaré la asociación entre direcciones de interfaces e identificadores de área.

cisco(config-router)# network <dirección IP> <mascara> area <ID area>
cisco(config-router)# network <dirección IP> <mascara> area <ID area>

En nuestro caso sería:

cisco(config-router)# network 10.10.10.0 0.0.0.255 area 0
cisco(config-router)# network 10.10.210.0 0.0.0.255 area 1
cisco(config-router)# network 10.10.220.0 0.0.0.255 area 2
cisco(config-router)# network 10.10.230.0 0.0.0.255 area 3

La primera línea especifica que los interfaces del router que comienza por 10.10.10.0/24 pertenecen al área 0. De la misma manera, la segunda declara que los interfaces cuya dirección comience por 10.10.200.0 pertenecen al área 1. Y de la misma manera las demás.

Como son routers frontera de área (ABR), debo definir como se realizará el flujo de información de encaminamiento entre las áreas y el backbone:

En caso de no especificar nada en el ABR, los prefijos de las áreas se redistribuirían al backbone y viceversa sin modificaciones por lo que no habría ni agregación ni rutas por defecto.

Para crear la agregación desde las áreas hacia le backbone lo realizo de la siguiente forma:

cisco(config)# router ospf 10
cisco (config-router)# area 1 range 10.10.210.0 255.255.255.0

OSPF es un protocolo de routing interno del tipo estado de enlace.
Los equipos de nuestra red anunciarán toda la información al arrancar el protocolo. Se enviarán entre sí paquetes link state cuando se detectan fallos en algún enlace. Entonces, todos los routers actualizan la base de datos topológica, se copian los link state e inundan a los vecinos. (Sólo se van enviando las nuevas actualizaciones de rutas y no la tabla completa).

Vamos a verificar el estado de OSPF por interfaz así como los vecinos OSPF que tenemos en un interfaz, mediante los comandos siguientes:

show ip ospf interface
show ip ospf neighbors

```
cisco# show ip ospf interface ethernet 0
Ethernet0 is up, line protocol is up
  Internet Address 10.10.10.1/24, Area 0
  Process ID 1, Router ID 192.168.45.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.10.10.1, Interface address 10.10.10.2
  Backup Designated router (ID) 10.10.10.1, Interface address 10.10.10.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.10.210.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

6.6.2.4 Configuración básica de BGP

Antes de configurar MPLS en la red, deberé establecer un full-mesh de sesiones BGP en nuestro backbone y así dejar preparado el escenario de red para la configuración final de MPLS en los routers.

Para realizar la configuración de BGP he tenido que pasar por los siguientes pasos:

Configurar el proceso de routing BGP:

cisco# configure terminal
cisco(config)# router bgp <número de proceso BGP>

El número de proceso BGP que generalmente se pone es el 65000, para un entorno de pruebas, ya que hay otras numeraciones que están reservadas.
Con este comando estamos configurando el sistema autónomo con el que queremos que se "hable" BGP.

Configurar para cada pareja de routers que estén enfrentados lo siguiente (España-China, España-Colombia, España-Rumania):

Selecciono uno de los routers y le especifico el router vecino, posteriormente le indico que actualice el encaminamiento a través de la interfaz de loopback que he configurado anteriormente:

cisco(config-router)# neighbor <dir IP de la interfaz del vecino que tiene enfrentada> remote-as <número de proceso BGP >

cisco(config-router)# neighbor <dir IP de la interfaz del vecino que tiene enfrentada > update-source loopback<número de la interfaz>

En el caso del router de España esta configuración la he tenido que repetir tres veces, una por cada vecino.

Vamos a verificación el estado de BGP

show ip bgp neighbor

```
cisco# show ip bgp neighbors
BGP neighbor 10.10.210.1 using remote AS 100
router ID: 10.10.210.0 version: 4
state: Active time: 0:34:41
def orignat: False ebgp multihop: False
n hop self: False route ref client: False
send comm: False soft reconfig: False
hold time: 180 sec keepalive time: 60 sec
advertisement interval: 5 sec
# notf rcvd: 0 # msg rcvd: 0 # updates rcvd: 0
# notf sent: 0 # msg sent: 0 # updates sent: 0
number of prefixes received: 0
            inbound AS-path filter: filt_list_in
           outbound AS-path filter: filt_list_out
            inbound network filter: dist_list_in
           outbound network filter: dist_list_out
                 inbound route-map: routemap_in
                outbound route-map: routemap_out
Address Family IPv4 Unicast: activated advertised
Routes Dropped : 0
Time Since First Dropped : 0:00:00
Reason for dropping first Route : No Routes Dropped number
```

show ip bgp summary

```
cisco# show ip bgp summary
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.210.1     4 20976  183034  183123  5723690    0    0 1d06h           4
10.10.220.1     4 20976  183037  183197  5723690    0    0 1w3d            3
10.10.230.1     4 20834       0       0        0    0    0 never         Active
```

Muestra los routers que mantienen una relación de vecindad con el router en el que se ejecuta el comando, y el estado en el que se encuentran.

6.6.2.5 Configuración de MPLS

Una vez establecidos los protocolos de routing pasaré a establecer las funcionalidades MPLS en los routers. Para ello tengo que arrancar el protocolo de distribución de etiquetas en las distintas interfaces por las que queremos "hablar MPLS".

La configuración de MPLS requiere los siguientes pasos:

Configurar el CEF [27] en todos los routers con la funcionalidad "PE [28]" y "P [29]".

Para activar CEF en los routers he utilizado el siguiente comando:

cisco# configure terminal
cisco(config)# ip cef

Activar el protocolo de distribución de etiquetas LDP [30]:
Esta configuración la tendré que hacer en cada interfaz que vaya a hablar MPLS en un mismo router:

cisco(config)# interface fastethernet0/0.100
cisco(config-if # mpls ip
cisco(config-if)# mpls label protocol ldp

Vamos a verificar el funcionamiento de MPLS en la red

Para realizar la verificación del funcionamiento de MPLS utilizaré los siguientes comandos:

1. *show mpls interfaces*
Muestra las interfaces en las que está funcionando MPLS-LDP.

```
cisco# show mpls interface
Interface         State       Administrative groups
so-0/0/0.0        Up          Rumania
so-0/0/1.0        Up          Colombia
so-0/0/2.0        Up          China
```

2. *show mpls ldp parameters*
Muestra los parámetros que está utilizando el protocolo en el equipo donde se ejecuta el comando.

```
cisco# show mpls ldp parameters
Protocol version: 1
Downstream label pool: min label 16; max label 100000
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 180 sec; interval: 5 sec
LDP for targeted sessions; peer acl: 1
LDP initial/maximum backoff: 30/240 sec
```

3. *show mpls ldp neighbor*
Muestra los routers que mantienen una relación de vecindad con el router en el que se ejecuta el comando.

---

[27] *CEF: Cisco Express Forwarding:* conjunto de funcionalidades que reúnen los equipos Cisco para poder trabajar en un entorno MPLS entre otras funciones.
[28] *PE's: Provider Edge routers.*
[29] *P's: Provider backbone routers.*
[30] *LDP: Label Distribution Protocol:* protocolo estándar entre routers MPLS para negociar las etiquetas (direcciones) que se utiliza para avanzar los paquetes.

```
cisco#show mpls ldp neighbor
Peer LDP Ident: 10.10.210.1:0; Local LDP Ident 10.10.210.1:0
TCP connection: 10.10.210.1.646 - 10.10.210.1.11000
State: Oper;
Msgs sent/rcvd: 3117/3112; Downstream;
Last TIB rev sent2
Up time: 2w4d; UID: 4; Peer Id 0;
LDP discovery sources:
Serial0/0; Src IP addr: 10.10.10.1
holdtime: 15000 ms, hello interval: 5000 ms
Addresses bound to peer LDP Ident:
10.10.210.1 10.10.220.1 10.10.230.1
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer
state: estab
show mpls ldp neighbor detail
```

4. *show mpls ldp binding*

Muestra la tabla de etiquetas que está utilizando el router donde se ejecuta el comando.

```
cisco#show mpls ldp binding
10.10.210.1/16, rev 29
local binding: label: 26
remote binding: lsr: 172.27.32.29:0, label: 26
10.10.220.1/32, rev 32
local binding: label: 27
remote binding: lsr: 82.231.42.16:0, label: 28
10.10.230.1/32, rev 33
local binding: label: 28
remote binding: lsr: 24.223.91.74:0, label: 29
```

5. *show mpls forwarding-table*

Muestra la tabla de *forwarding* del router donde se ejecuta el comando.

```
cisco#show mpls forwarding-table
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
70 Pop tag 10.10.200.1/16 0 Se0/0 point2point
MAC/Encaps=4/4, MTU=1400, Tag Stack{}
0F008847
No output feature configured
Per-packet load-sharing
71 Pop tag 10.10.210.1/32 0 Se0/0 point2point
MAC/Encaps=4/4, MTU=1400, Tag Stack{}
0F008847
No output feature configured
Per-packet load-sharing
72 Pop tag 10.10.210.1/32 0 Se0/0 point2point
MAC/Encaps=4/4, MTU=1400, Tag Stack{}
0F008847
No output feature configured
Per-packet load-sharing
```

Una vez configurados los routers correctamente los cuatro routers vamos a juntar los routers con los servidores instalados para crear las VPN y con ello la red de comunicaciones internacional.

6.6.3 Implantación VPN – MPLS internacional

En este punto explico la implantación de las VPN sobre MPLS creadas mediante ISA Server 2004.

El siguiente esquema expresa en que punto de la implantación nos encontramos:

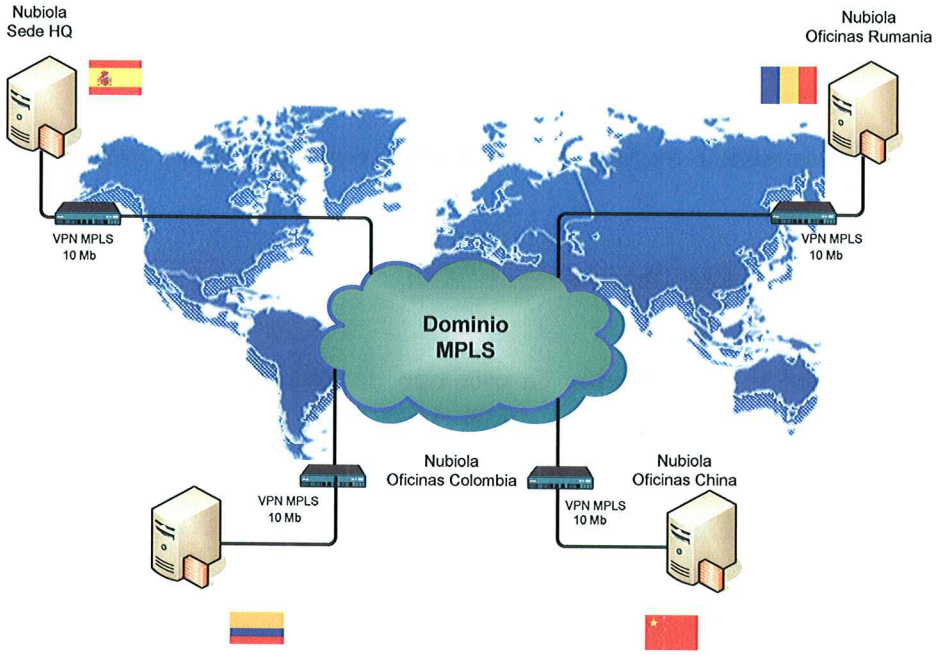


Ilustración 6-23: Implantación de la red VPN - MPLS

Para realizar la conexión VPN entre dos sedes se ha escogido hacerlo mediante la tecnología Site to Site aportada por ISA Server 2004.

La instalación de Windows ISA Server 2004 Standard se ha realizado sobre un Windows Server 2003 con la finalidad de proteger la red VPN y brindar un acceso seguro a Internet.

La única necesidad que se requiere para la configuración de la VPN en los servidores es la de tener dos adaptadores de red, esta necesidad ya ha sido cubierta en la compra del mismo.

El siguiente esquema muestra el escenario donde la red se encuentra protegida a través de un servidor Windows Server 2003 con ISA Server 2004:

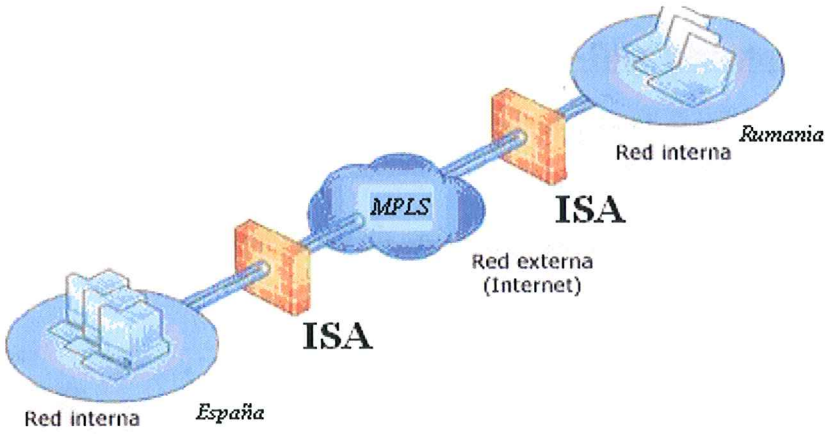


Ilustración 6-24: Esquema de red creada con Microsoft ISA Server

6.6.3.1 Routing and Remote Access (RRAS)

Para llevar a cabo la implantación en este tipo de escenario he tenido que instalar y activar el servicio de Routing and Remote Access que tiene interno el propio sistema operativo.

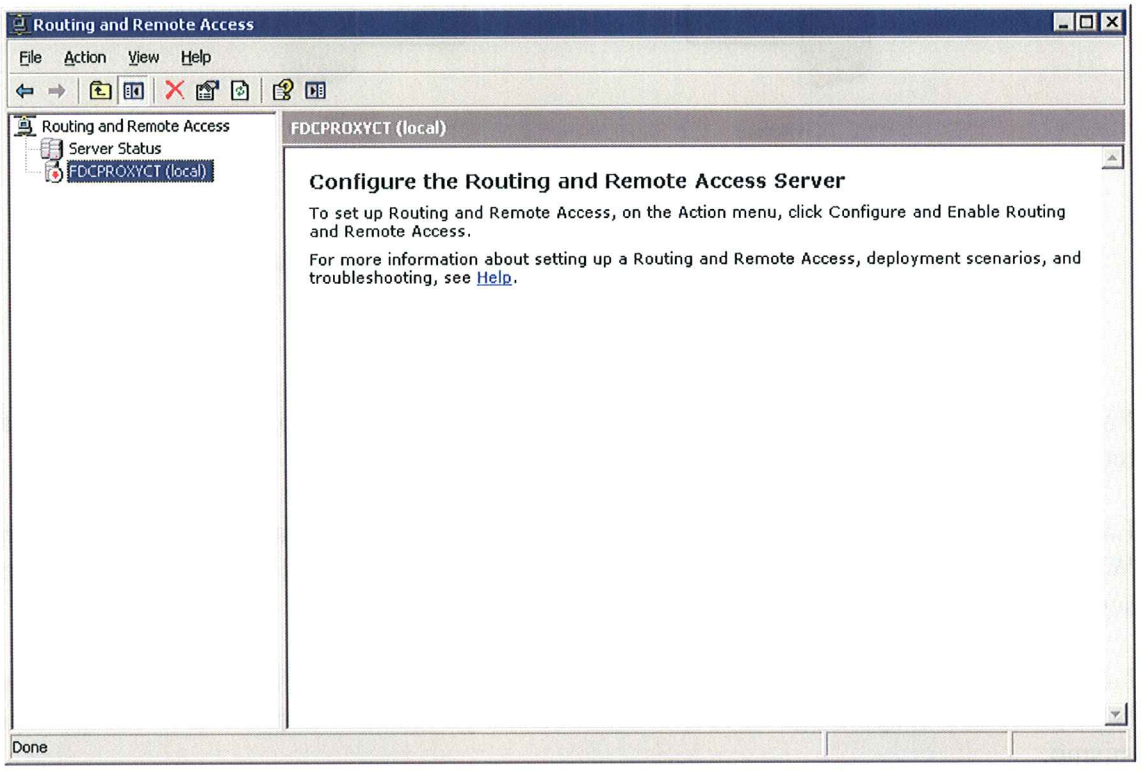


Ilustración 6-25: Configuración Routing and Remote Access Server - 1

Deberé configurarlo con la capacidad de Virtual Prinate Network (VPN) acces and NAT (Network Addesss Translation). Esto se debe configurar porque RRAS es utilizado por ISA Server para gestionar las conexiones VPN.

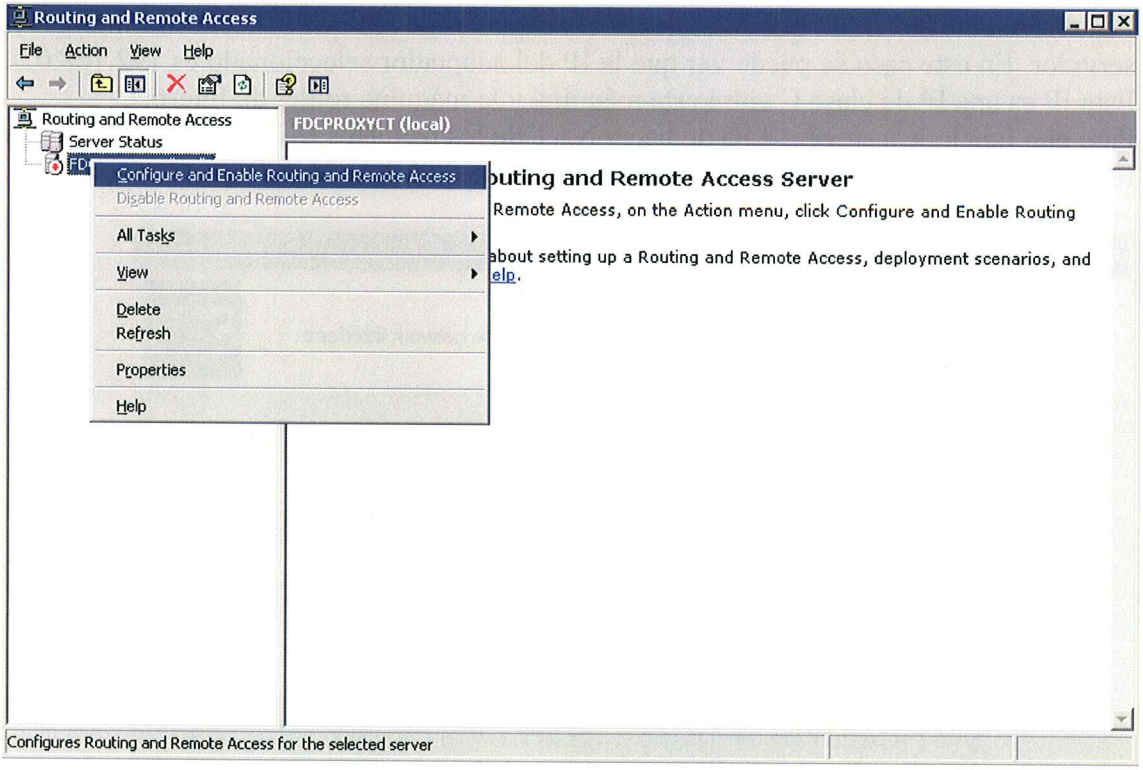


Ilustración 6-26: Configuración Routing and Remote Access Server - 2

He seleccionado Virtual Private Network and NAT.
Debe ser con esta configuración puesto que tenemos que crear una conexión VPN y posteriormente enrutar por ella el tráfico saliente que vaya destino hacia las IPs del lado contrario.

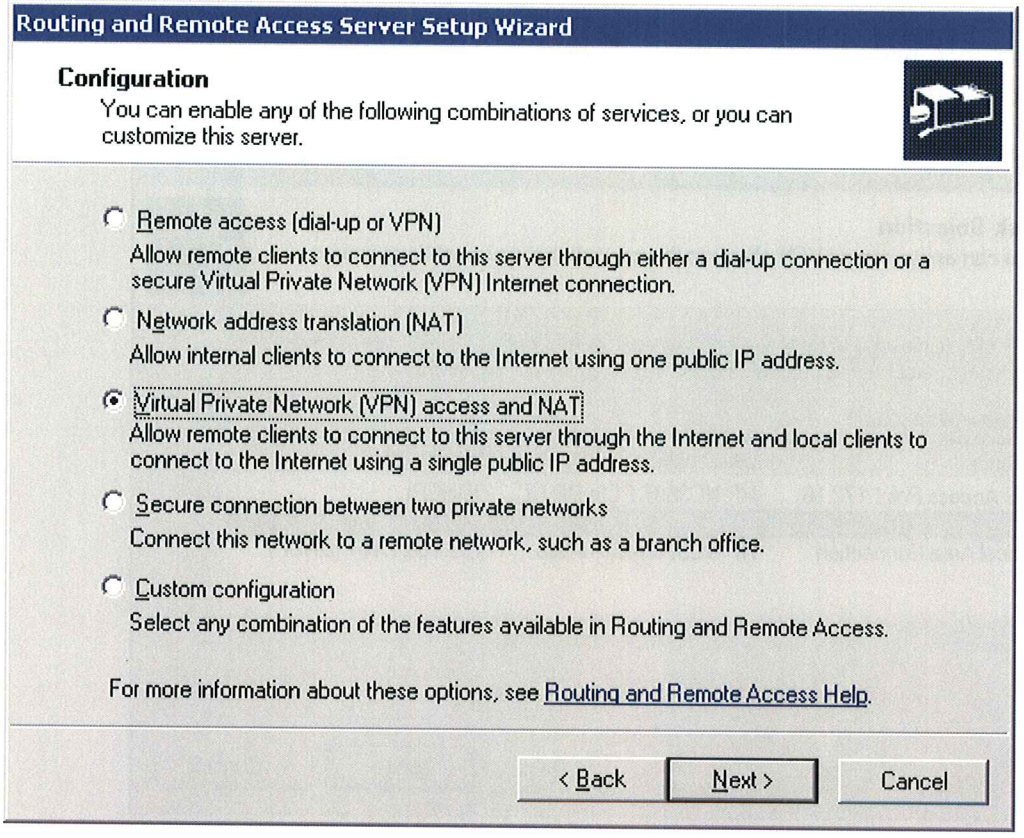


Ilustración 6-27: Configuración Routing and Remote Access Server - 3

Posteriormente he tenido que seleccionar el adaptador de red que conecta con Internet el servidor. En este caso se puede ver que la IP del adaptador seleccionado es 192.168.0.5. Esta IP es una IP de clase C entre esta máquina y la máquina router de Internet.
Para que funcione a su vez se ha de hacer NAT de los paquetes IKE, L2TP e IPSec de la IP pública hacia esta IP interna. (lo explicaré mejor en el Punto 6.6.3.2).

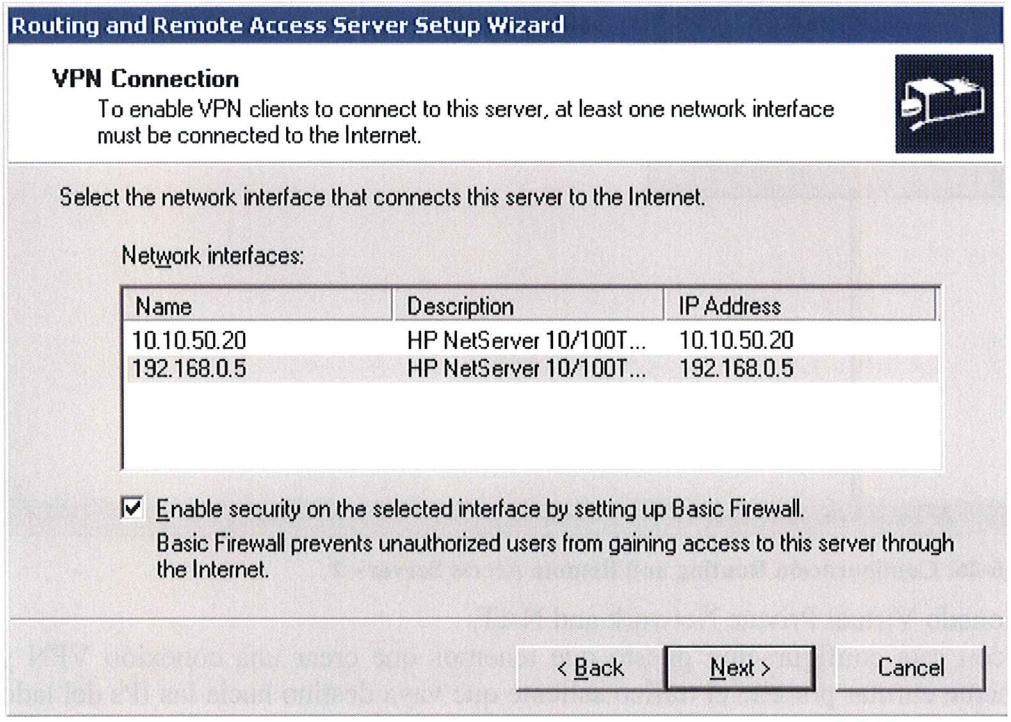


Ilustración 6-28: Configuración RRAS - Selección de Adaptadores de Red externo

Una vez seleccionada la red externa de la que vendrán las conexiones deberé marcar la red a la que tendrán acceso los usuarios VPN, en este caso es la interna.

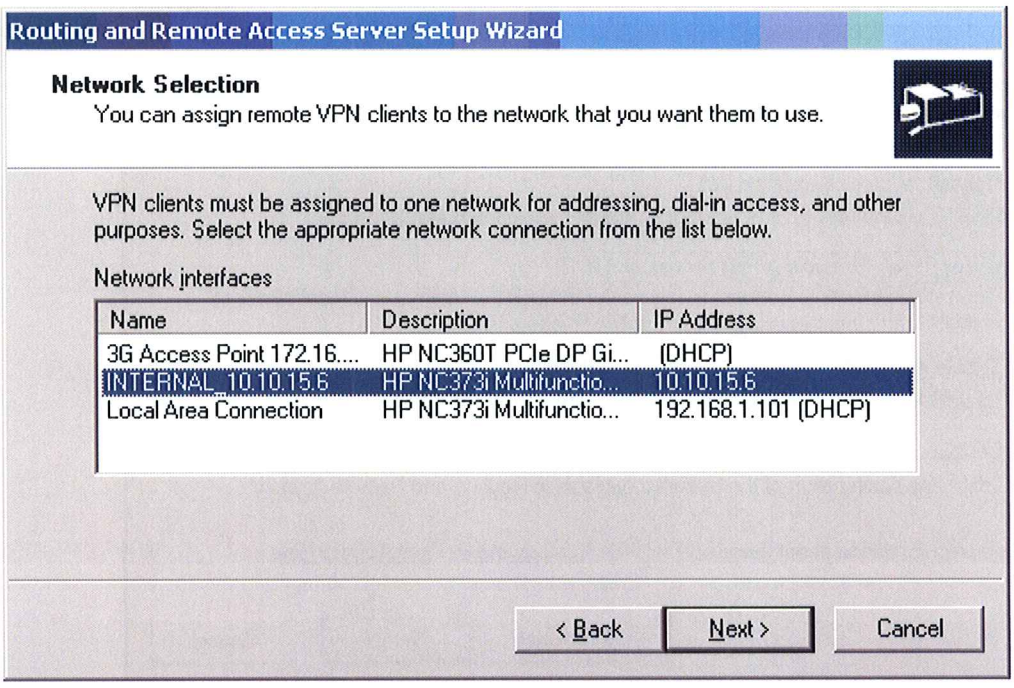


Ilustración 6-29: Configuración RRAS - Selección de Adaptadores de Red interno

Esta conexión puede utilizar Radius, para autentificar a los diferentes clientes. No lo he activado porque solamente vamos a tener como clientes a las delegaciones que se conecten.

Una vez llegado este punto ya tengo Routing and Remonte Access configurado con las necesidades que requerimos.

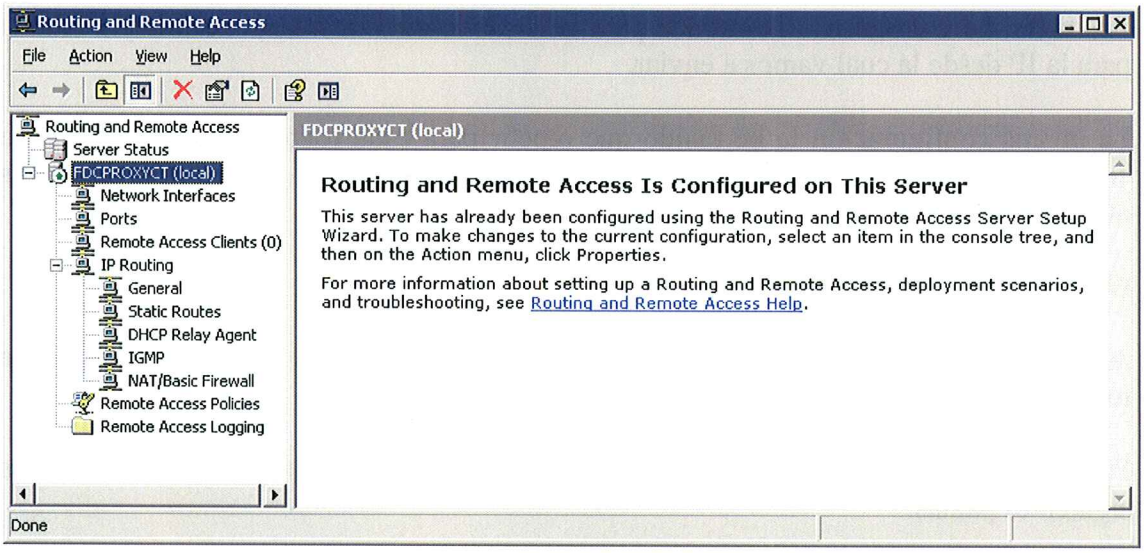


Ilustración 6-30: RRAS - Configurado con las necesidades requeridas.

6.6.3.2 Enrutamiento de los paquetes del router hacia el servidor ISA

Llegado este punto tenemos configurado el RRAS y el dominio MPLS con los routers entendiéndose entre ellos. Ahora deberemos marcar la pauta para que los paquetes que lleguen vía la MPLS lleguen al ordenador que los va a gestionar.

Para ello deberé configurar en el router las políticas de entrada y salida y posteriormente las políticas sobre NAT.

Políticas a configurar:

He tenido que configurar el tráfico L2TP, IKE e IKE_NAT_TRAVERSAL en los dos sentidos. Puesto que estos son los protocolos que se utilizarán en la creación de la VPN que explicaré más adelante en el punto 6.6.3.3.

SOURCE	DESTINATION	VPN	SERVICE	ACTION
ISA_213.201.59.3	ISA_213.201.59.7	Any Traffic	L2TP IKE IKE_NAT_TRAVERSAL	accept
ISA_213.201.59.7	ISA_213.201.59.3	Any Traffic	L2TP IKE IKE_NAT_TRAVERSAL	accept

Ilustración 6-31: Políticas de enrutamiento del tráfico entre router y servidor VPN

El router deberá aceptar los protocolos que he comentado antes solamente si vienen de la IP del otro lado.
Por ejemplo la IP fija de España es la 213.201.59.3, la de China l 213.201.59.7. Deberé configurar como se ve en la ilustración anterior que todo lo que venga de china con destino mi IP sea aceptado. Y todo lo que va de España destino a China sea aceptado su envío.

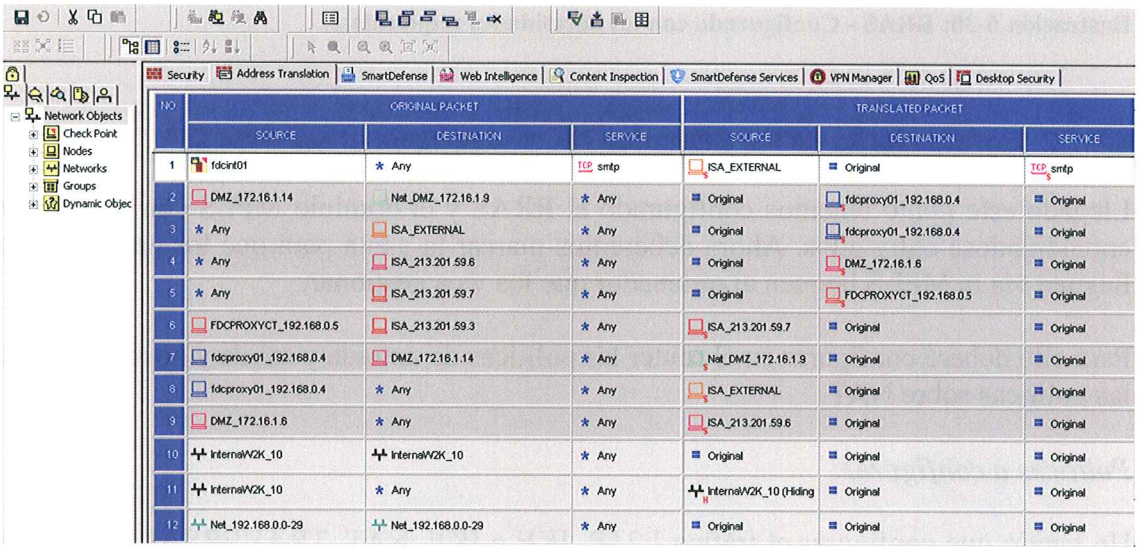
Por tanto, he configurado la entrada para la IP de la cual deseamos recibir y la salida para la IP desde la cual vamos a enviar.

La misma configuración la he tenido que repetir para cada router, creando 3 veces la configuración en el router de España, puesto que este recibirá las conexiones de los otros tres routers.

Configuración del NAT:

Ahora voy a configurar que estos paquetes que entran o salen se envíen al servidor que los va a tratar.

Para ello tengo que configurar el Network Address Translation (NAT) con las siguientes pautas:



NO.	ORIGINAL PACKET			TRANSLATED PACKET		
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
1	fdcint01	Any	smtp	ISA_EXTERNAL	Original	smtp
2	DMZ_172.16.1.14	Net_DMZ_172.16.1.9	Any	Original	fdcproxy01_192.168.0.4	Original
3	Any	ISA_EXTERNAL	Any	Original	fdcproxy01_192.168.0.4	Original
4	Any	ISA_213.201.59.6	Any	Original	DMZ_172.16.1.6	Original
5	Any	ISA_213.201.59.7	Any	Original	FDCPROXYCT_192.168.0.5	Original
6	FDCPROXYCT_192.168.0.5	ISA_213.201.59.3	Any	ISA_213.201.59.7	Original	Original
7	fdcproxy01_192.168.0.4	DMZ_172.16.1.14	Any	Net_DMZ_172.16.1.9	Original	Original
8	fdcproxy01_192.168.0.4	Any	Any	ISA_EXTERNAL	Original	Original
9	DMZ_172.16.1.6	Any	Any	ISA_213.201.59.6	Original	Original
10	InternalW2K_10	InternalW2K_10	Any	Original	Original	Original
11	InternalW2K_10	Any	Any	InternalW2K_10 (Hiding	Original	Original
12	Net_192.168.0.0-29	Net_192.168.0.0-29	Any	Original	Original	Original

Ilustración 6-32: Configuración Network Address Translation

Pauta de Salida:
Todo lo que venga desde la IP interna A: 192.168.0.5 destino hacia la IP pública B: 213.201.59.3 (IP del otro lado de la VPN) envíalo como si la fuente fuera la IP pública C: 213.201.59.7 (IP pública del router).

Pauta de Entrada:
Todo lo que venga hacia la IP pública A: 213.201.59.7 (IP pública del router) envíalo hacia la IP interna A: 192.168.0.5 (IP del Servidor ISA).

Podría haber marcado que servicios queremos que sean trasladados por el NAT. No lo he realizado porque la IP de conexión esta destinada solamente al servicio VPN.