

UD 4: “Instalación y configuración de cortafuegos”

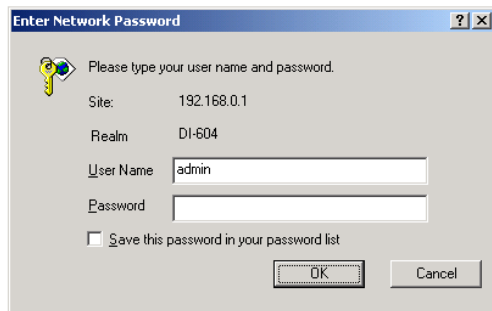
CORTAFUEGOS:

1. CONFIGURACIÓN ROUTER-FIREWALL

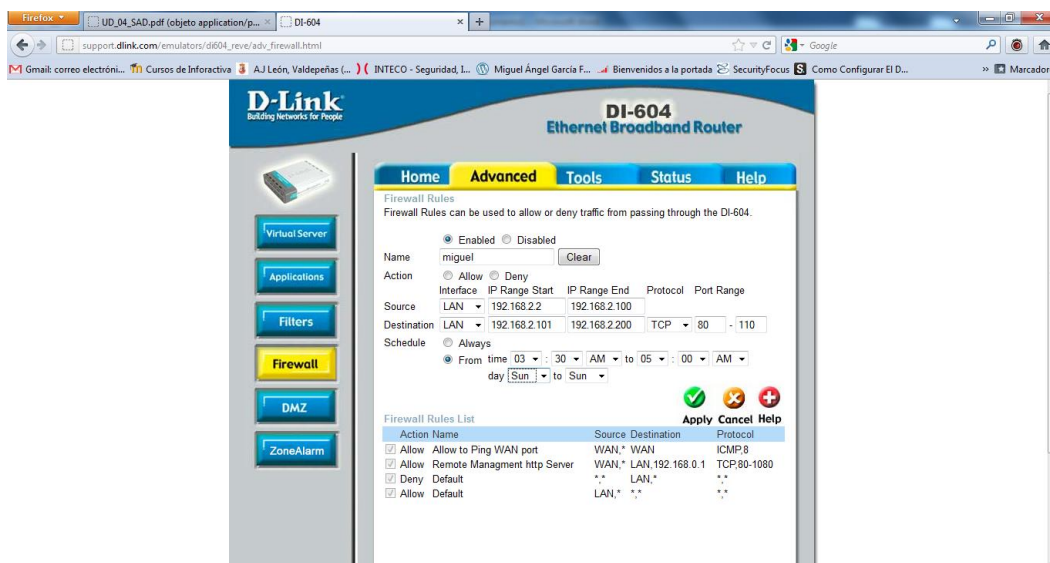
Configura un router-firewall utilizando los simuladores correspondientes:

a) Router *DLINK*:

Nos logueamos como administrador en el router.

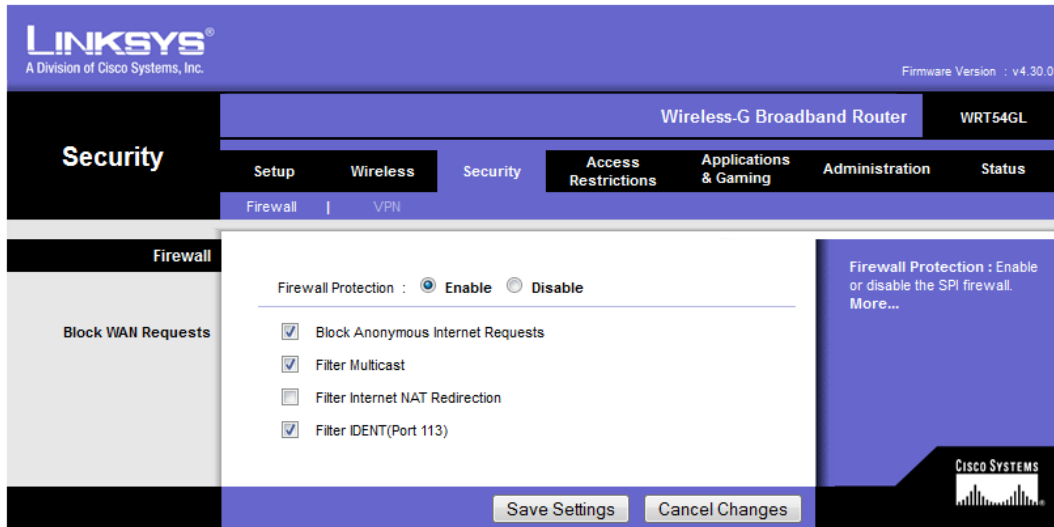


Denegamos el rango de direcciones de la 2-100 y de la 101 a la 200, pero éste último los puertos desde el 80 al 110. Además tienen un control horario de 3:30 AM a 5:00 AM.

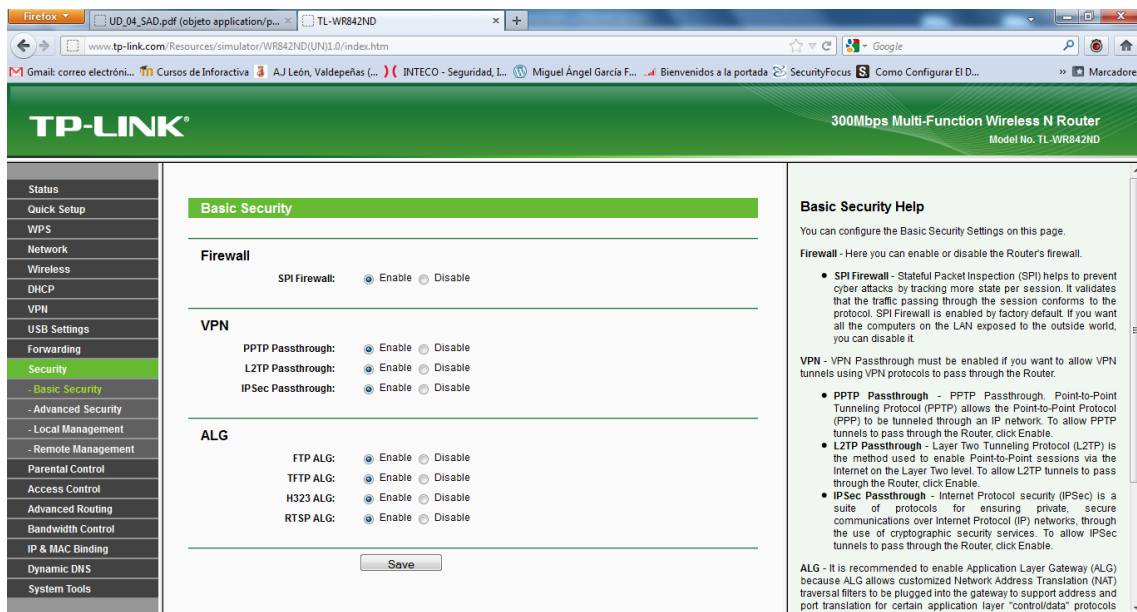


b) Router *LINKSYS*:

Podemos realizar un bloqueo de peticiones de anónimos, filtros multicast, filtrar el puerto 113 y un filtro de NAT.



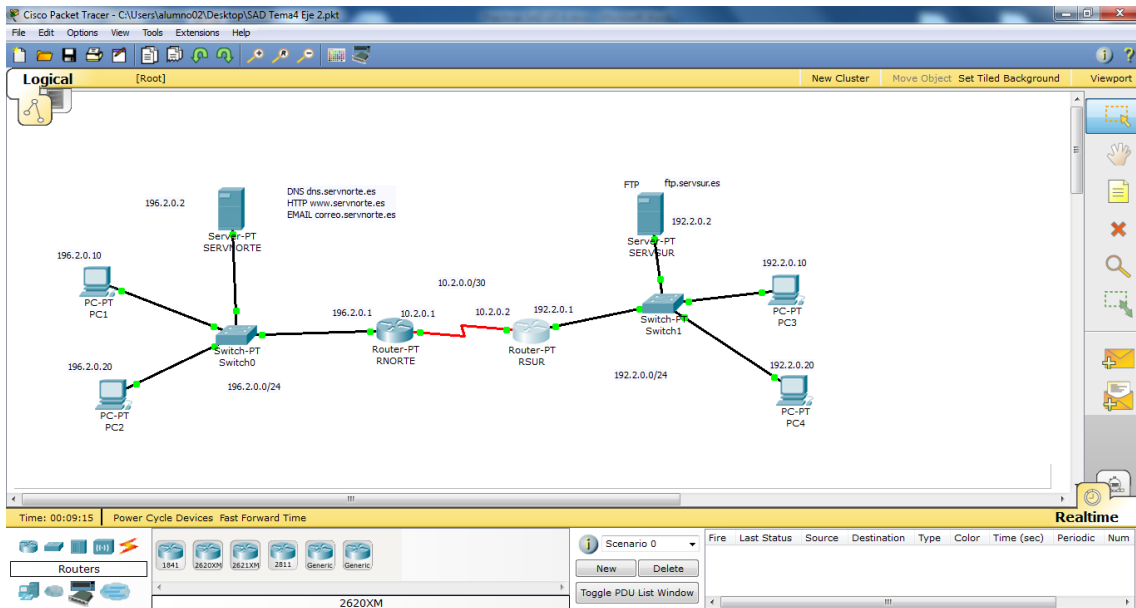
Este router, sólo tiene la opción de habilitar y deshabilitar el firewall.



2. ACL (CISCO)

a) Resolución de ejercicios.

b) Resolución escenario UD3-2.a. Router Frontera.



Uso de ACL estándar:

1) Elige el router adecuado para que los paquetes del PC1 no sean transmitido por la red 10.XX.0.0. Comprobar que si se permite los

```

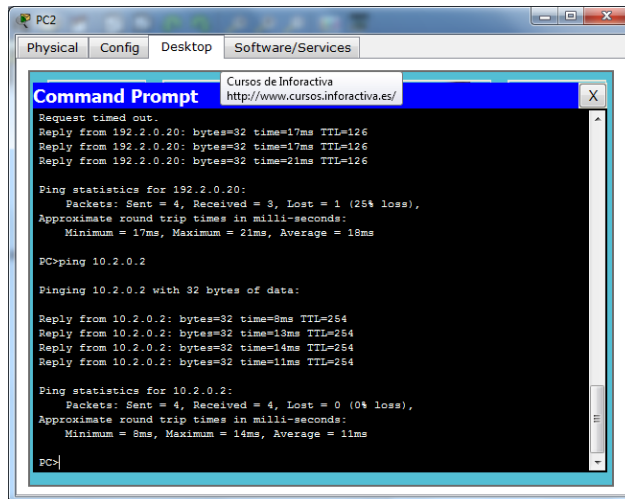
RNORTE
Physical Config CLI
IOS Command Line Interface
Sending 5, 100-byte ICMP Echos to 196.2.0.10, timeout is 2 seconds:
.....
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/7/10 ms

RNORTE#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RNORTE(config)#access-list 1 deny host 196.2.0.10
RNORTE(config)#access-list 1 permit any
RNORTE(config)#interface FastEthernet 0/0
RNORTE(config-if)#ip access-group 1 in
RNORTE(config-if)#
RNORTE(config-if)#end

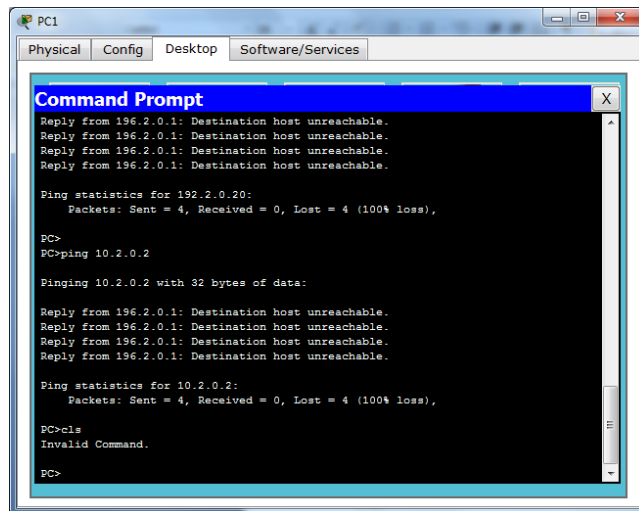
%SYS-5-CONFIG_I: Configured from console by console
RNORTE#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RNORTE#ping 196.2.0.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 196.2.0.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
    
```

Comprobamos que el PC2 puede mandar paquetes al RSUR

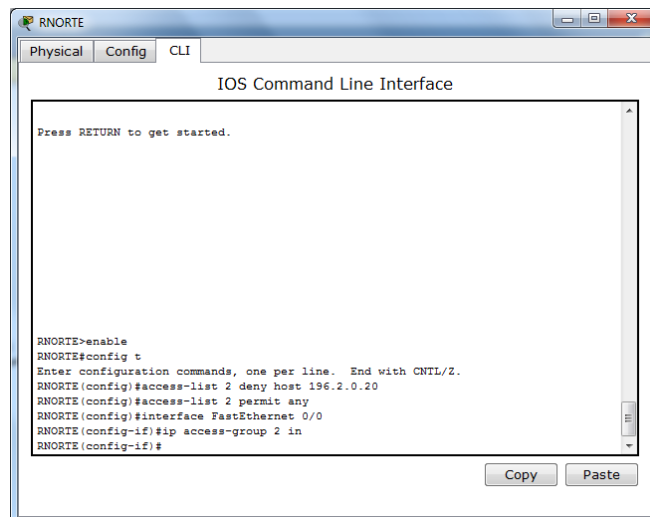


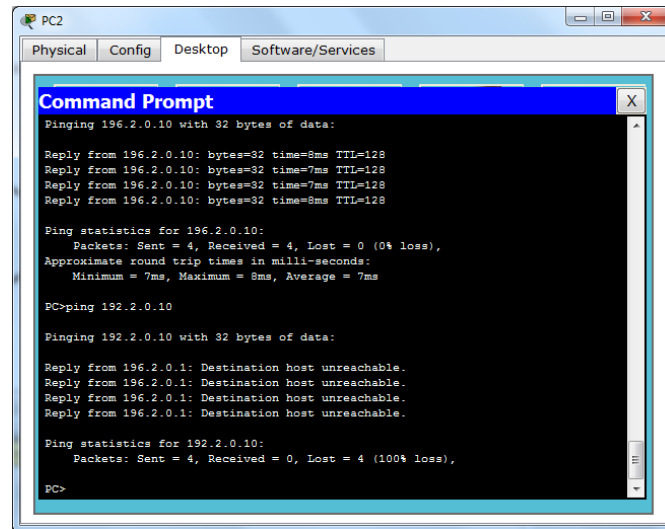
Sin embargo si hacemos lo mismo con el PC1 no permite mandar paquetes.



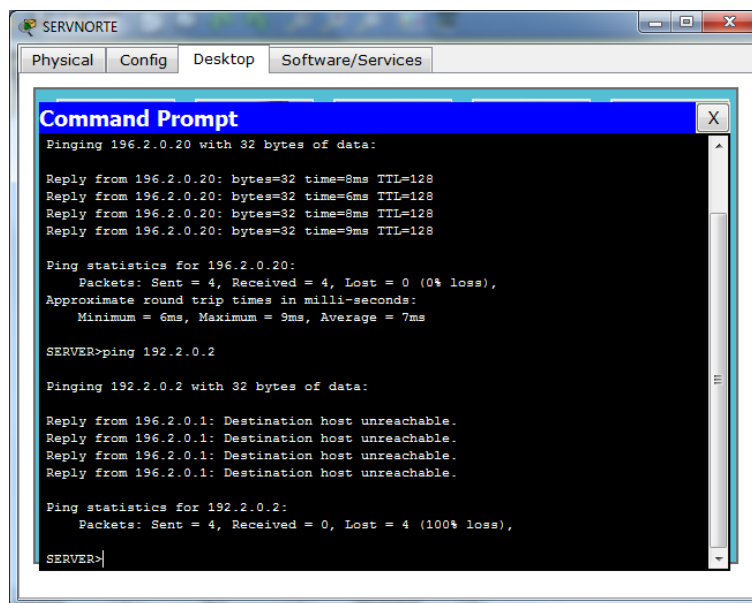
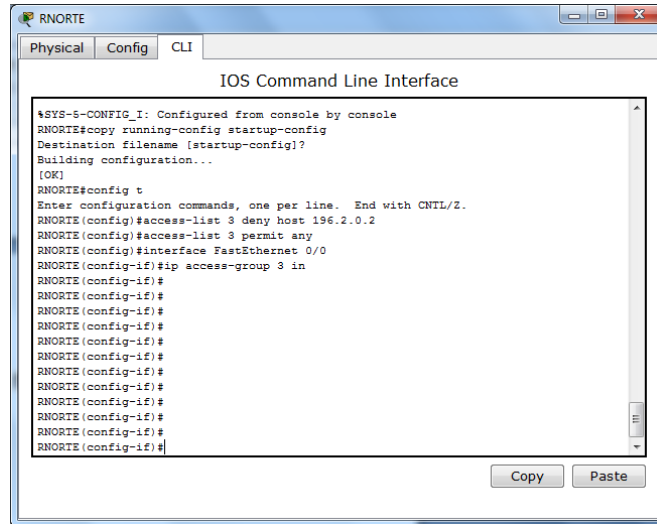
2) Configurar en la red 192.XX.0.0/24 un filtro “anti-spoofing” para que no sea enviado ningún paquete por la red 10.XX.0.0 que no coincida con su dirección de origen. Realizarlo también para la red 196.XX.0.20

Configuramos las acl para la IP 196.2.0.20.



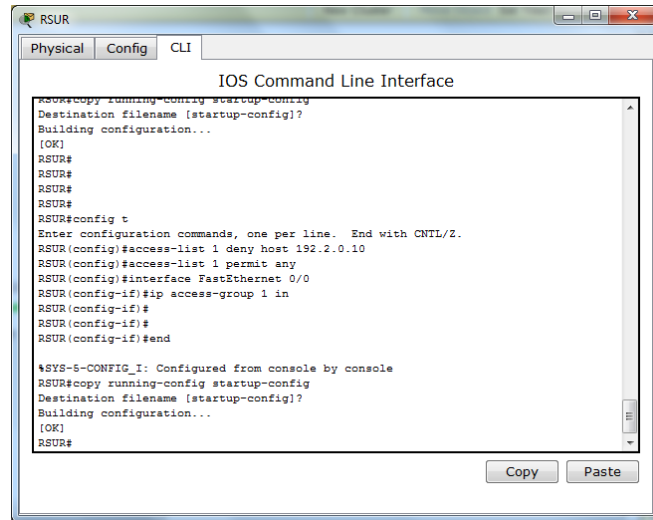


Configuramos las acl para la IP 196.2.0.2.



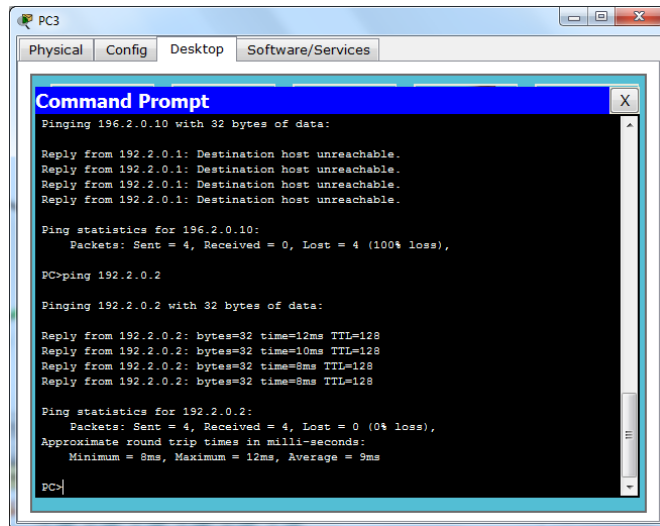
En la red 192.2.0.0:

Configuramos las acl para la IP 192.2.0.10



```
RSUR
Physical Config CLI
IOS Command Line Interface
RSUR#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RSUR#
RSUR#
RSUR#
RSUR#
RSUR#config t
Enter configuration commands, one per line. End with CNTL/Z.
RSUR(config)#access-list 1 deny host 192.2.0.10
RSUR(config)#access-list 1 permit any
RSUR(config)#interface FastEthernet 0/0
RSUR(config-if)#ip access-group 1 in
RSUR(config-if)#
RSUR(config-if)#
RSUR(config-if)#end

%SYS-5-CONFIG_I: Configured from console by console
RSUR#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RSUR#
```



```
PC3
Physical Config Desktop Software/Services
Command Prompt
Pinging 192.2.0.10 with 32 bytes of data:
Reply from 192.2.0.1: Destination host unreachable.
Reply from 192.2.0.1: Destination host unreachable.
Reply from 192.2.0.1: Destination host unreachable.
Reply from 192.2.0.1: Destination host unreachable.

Ping statistics for 192.2.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

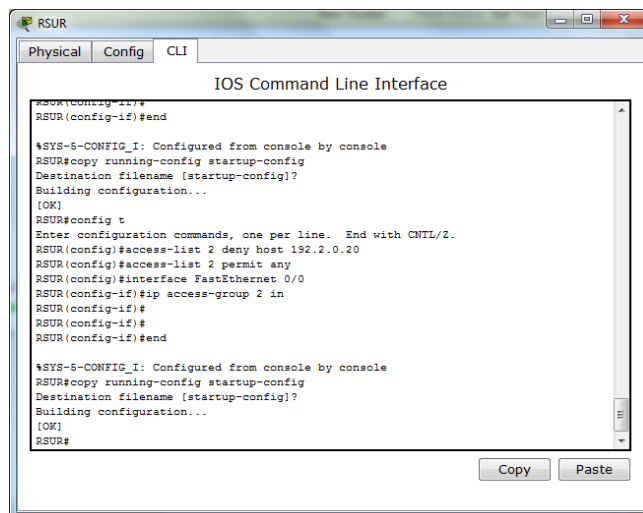
PC>ping 192.2.0.2

Pinging 192.2.0.2 with 32 bytes of data:
Reply from 192.2.0.2: bytes=32 time=12ms TTL=128
Reply from 192.2.0.2: bytes=32 time=10ms TTL=128
Reply from 192.2.0.2: bytes=32 time=8ms TTL=128
Reply from 192.2.0.2: bytes=32 time=8ms TTL=128

Ping statistics for 192.2.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 12ms, Average = 9ms

PC>
```

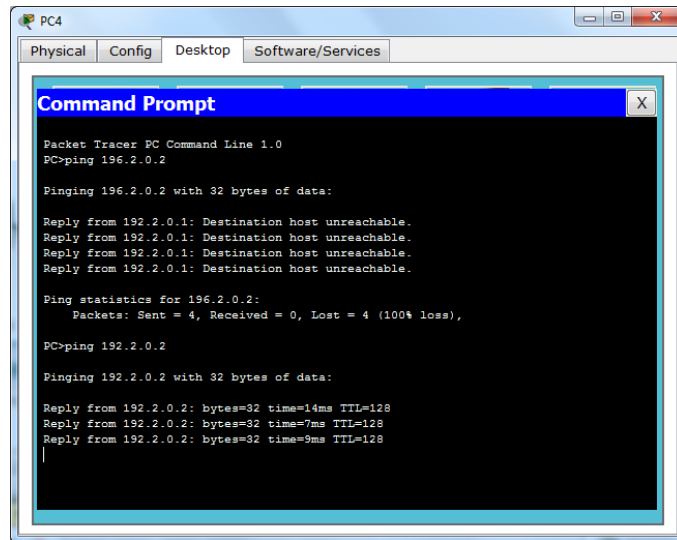
Configuramos las acl para la IP 192.2.0.20



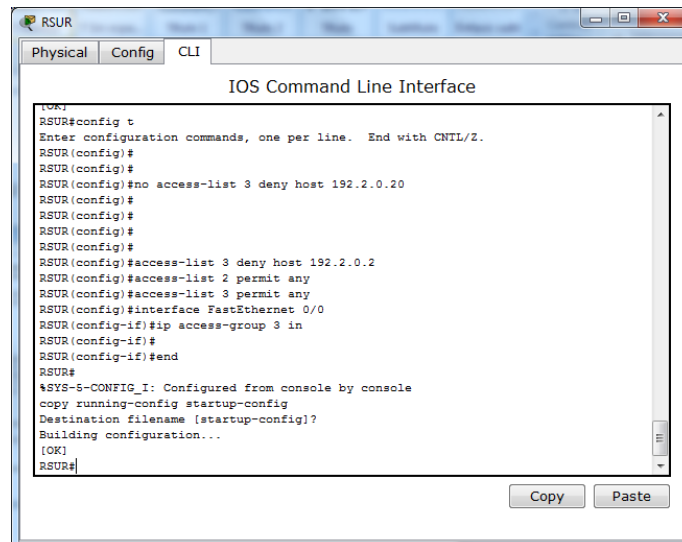
```
RSUR
Physical Config CLI
IOS Command Line Interface
RSUR(config-if)#end

%SYS-5-CONFIG_I: Configured from console by console
RSUR#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RSUR#config t
Enter configuration commands, one per line. End with CNTL/Z.
RSUR(config)#access-list 2 deny host 192.2.0.20
RSUR(config)#access-list 2 permit any
RSUR(config)#interface FastEthernet 0/0
RSUR(config-if)#ip access-group 2 in
RSUR(config-if)#
RSUR(config-if)#
RSUR(config-if)#end

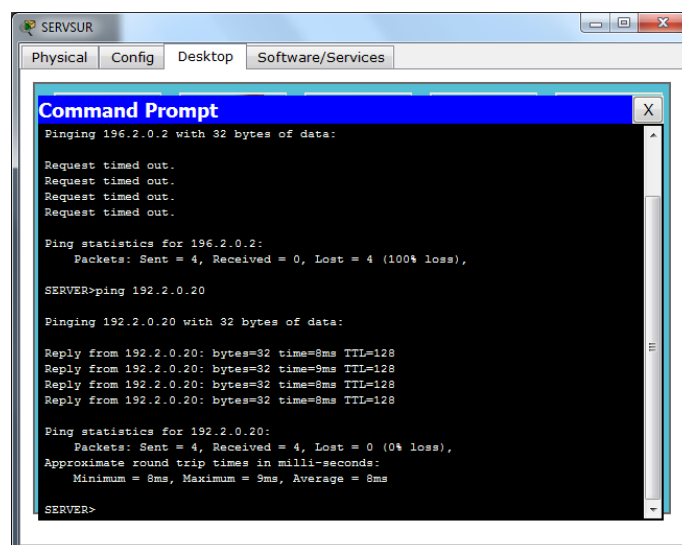
%SYS-5-CONFIG_I: Configured from console by console
RSUR#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RSUR#
```



Configuramos las acl para la IP 192.2.0.2

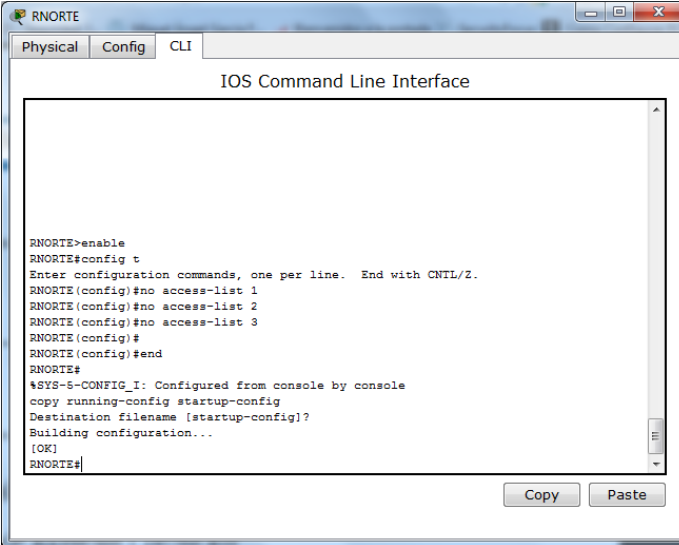


Comprobamos los resultados.



3) Borrar las ACLs definidas anteriormente.

Router Norte:

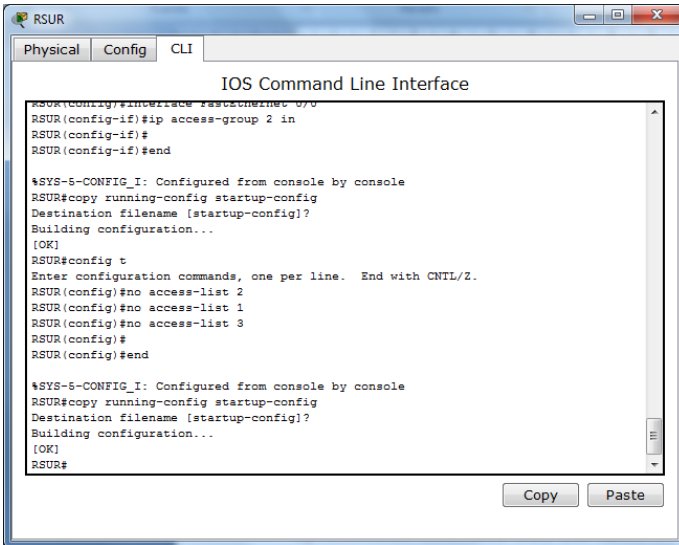


```

RNORTE
Physical Config CLI
IOS Command Line Interface

RNORTE>enable
RNORTE#config t
Enter configuration commands, one per line. End with CNTL/Z.
RNORTE(config)#no access-list 1
RNORTE(config)#no access-list 2
RNORTE(config)#no access-list 3
RNORTE(config)#
RNORTE(config)#end
RNORTE#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RNORTE#
```

Router Sur:



```

RSUR
Physical Config CLI
IOS Command Line Interface

RSUR(config-if)#no access-group 2 in
RSUR(config-if)#
RSUR(config-if)#end

%SYS-5-CONFIG_I: Configured from console by console
RSUR#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RSUR#config t
Enter configuration commands, one per line. End with CNTL/Z.
RSUR(config)#no access-list 2
RSUR(config)#no access-list 1
RSUR(config)#no access-list 3
RSUR(config)#
RSUR(config)#end

%SYS-5-CONFIG_I: Configured from console by console
RSUR#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RSUR#
```

Uso de ACL COMPLEJAS

4) Permitir que el equipo PC3 pueda utilizar el servidor HTTP de SERVNORTE y no pueda utilizar el resto de servicios de dicho servidor.


```

RSUR>enable
RSUR(config)#
RSUR(config)#
RSUR(config)#
RSUR(config)#
RSUR(config)#
RSUR(config)#
RSUR(config)#
RSUR(config)#access-list 101 deny tcp host 192.2.0.10 host 196.2.0.2 eq 2
RSUR(config)#access-list 101 deny udp host 192.2.0.10 host 196.2.0.2 eq 5
RSUR(config)#access-list 101 permit tcp any any
RSUR(config)#access-list 101 permit udp any any
RSUR(config)#interface fa0/0
RSUR(config-if)#ip access-group 101 in
RSUR(config-if)#
RSUR(config-if)#end

**SYS-5-CONFIG_I: Configured from console by console
RSUR#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RSUR#
    
```

5) Permitir que el equipo PC1 pueda utilizar el servidor FTP de SERVSUR y el PC2 no pueda utilizarlo dicho servicio.

Configuramos en el router NORTE, para agregar las ACLs.

```

RNORTE>enable
RNORTE(config)#
RNORTE(config)#access-list 102 permit tcp host 196.2.0.10 host 192.2.0.2 eq 21
RNORTE(config)#access-list 102 deny tcp host 196.2.0.20 host 192.2.0.2 eq 21
RNORTE(config)#access-list 102 permit any any
^
Invalid input detected at '^' marker.

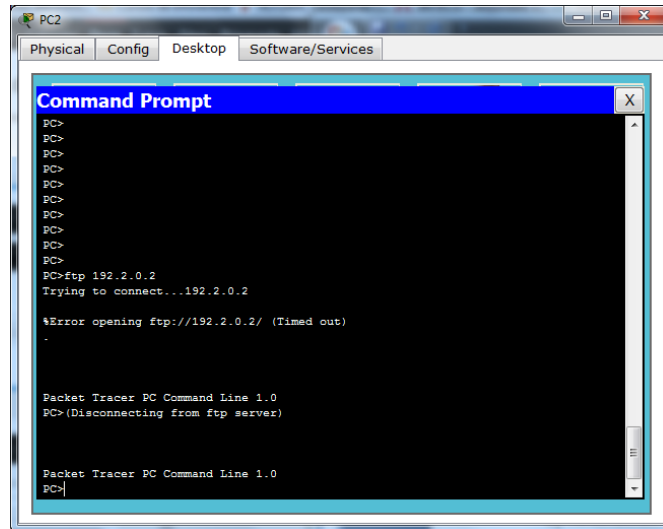
RNORTE(config)#access-list 102 permit tcp any any
RNORTE(config)#interface fa0/0
RNORTE(config-if)#ip access-group 102 in
RNORTE(config-if)#
    
```

Comprobamos que PC1 puede acceder vía FTP de SERVSUR

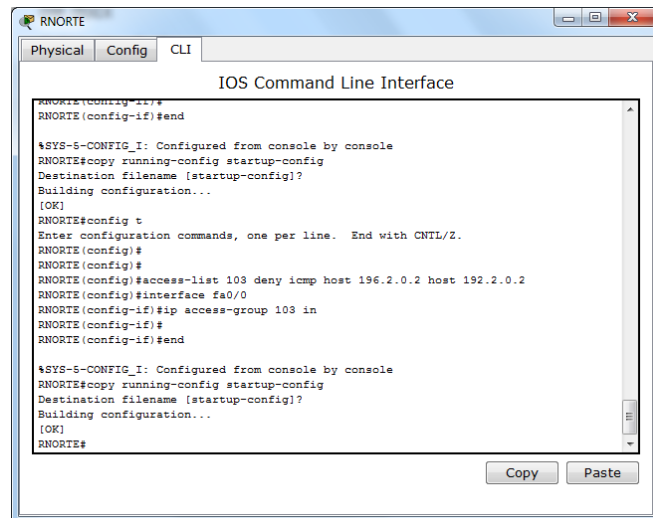
```

PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>ftp 192.2.0.2
Trying to connect...192.2.0.2
Connected to 192.2.0.2
220- Welcome to FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
    
```

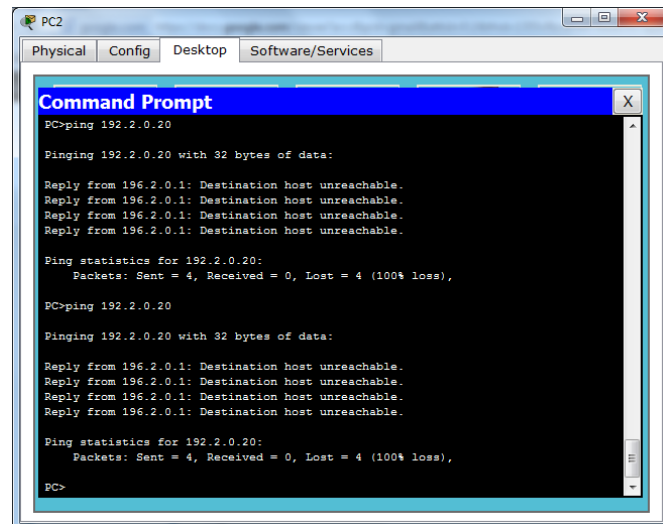
Comprobamos que el PC2 no puede acceder.



6) No permitir que el PC2 pueda comunicarse con el PC4.

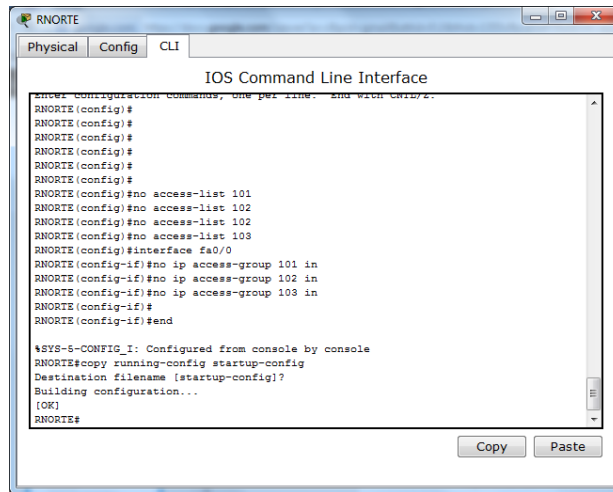


Comprobamos que ya no podemos acceder a PC4 desde PC2.

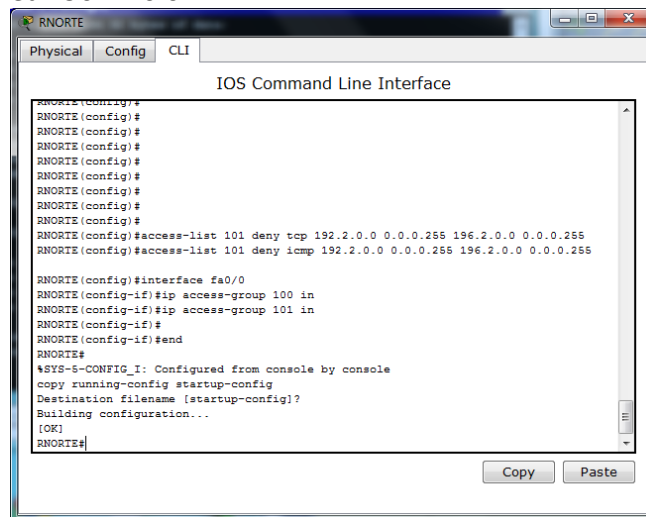


7) Borrar las ACLs anteriores.

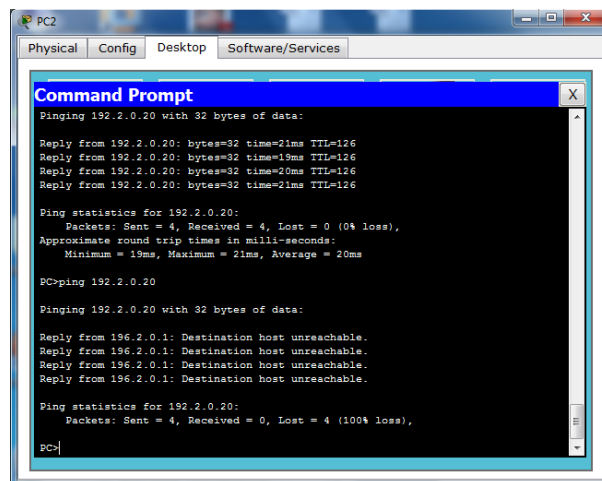
Borramos las ACLs.



8) No permitir que los ordenadores de la red 192.XX.0.0 se comuniquen con los ordenadores de la red 196.XX.0.0



Comprobamos el resultado



9) Borrar las ACL definidas anteriormente.

```
RNORTE(config)#
RNORTE(config)#no access-list 101
RNORTE(config)#
```

10) Impedir cualquier tráfico ICMP entrante excepto el “Destino Unreachable” y el “Echo Reply” en el router RNORTE.

3. IPTABLES (LINUX)

a) Resolución de ejercicios

1º) Ver la versión de Iptables:

```
root@miguel:/home/miguel# iptables -V
iptables v1.4.4
root@miguel:/home/miguel#
```

2º) Borrado de todas las reglas

```
root@miguel:/home/miguel# iptables -F
root@miguel:/home/miguel# iptables -X
root@miguel:/home/miguel# iptables -Z
root@miguel:/home/miguel# iptables -t nat -F
root@miguel:/home/miguel#
```

3º) Añadir una regla a la cadena INPUT para aceptar todos los paquetes que se originan desde la dirección 192.168.0.155.

```
root@miguel:/home/miguel# iptables -A INPUT -s 192.168.0.155 -j ACCEPT
root@miguel:/home/miguel# iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
ACCEPT    all  --  192.168.0.155         anywhere

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
root@miguel:/home/miguel#
```

Comprobamos.

```
C:\Documents and Settings>ping 192.168.0.10
Haciendo ping a 192.168.0.10 con 32 bytes de datos:
Respuesta desde 192.168.0.10: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.0.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.10: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.0.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 4ms, Media = 1ms

C:\Documents and Settings>
```

4º) Eliminar todos los paquetes que entren.

```
root@miguel:/home/miguel# iptables -A INPUT -j DROP
root@miguel:/home/miguel#
```

5º) Permitir la salida de paquetes.

```
root@miguel:/home/miguel# iptables -A OUTPUT -j ACCEPT
root@miguel:/home/miguel#
```

6º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155.

```
root@miguel:/home/miguel# iptables -A INPUT -s 192.168.0.155 -j DROP
root@miguel:/home/miguel#
```

7º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección de red 192.168.0.0.

```
root@miguel:/home/miguel# iptables -A INPUT -s 192.168.0.0/24 -j DROP
root@miguel:/home/miguel#
```

8º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155 y enviar un mensaje de error icmp.

```
root@miguel:/home/miguel# iptables -A INPUT -s 192.168.0.155 -j REJECT
root@miguel:/home/miguel#
```

9º) Permitir conexiones locales (al localhost), por ejemplo a mysql.

```
root@miguel:/home/miguel# iptables -A INPUT -i lo -p tcp --dport 3306 -j ACCEPT
root@miguel:/home/miguel#
```

10º) Permitir el acceso a nuestro servidor web (puerto TCP 80).

```
root@miguel:/home/miguel# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@miguel:/home/miguel#
```

11º) Permitir el acceso a nuestro servidor ftp (puerto TCP 20 y 21).

```
root@miguel:/home/miguel# iptables -A INPUT -p tcp --dport 20 -j ACCEPT
root@miguel:/home/miguel# iptables -A INPUT -p tcp --dport 21 -j ACCEPT
root@miguel:/home/miguel#
```

12º) Permitimos a la máquina con IP 192.168.0.155 conectarse a nuestro equipo a través de SSH.

```
root@miguel:/home/miguel# iptables -A INPUT -s 192.168.0.10 -p tcp --dport 22 -j
ACCEPT
root@miguel:/home/miguel#
```

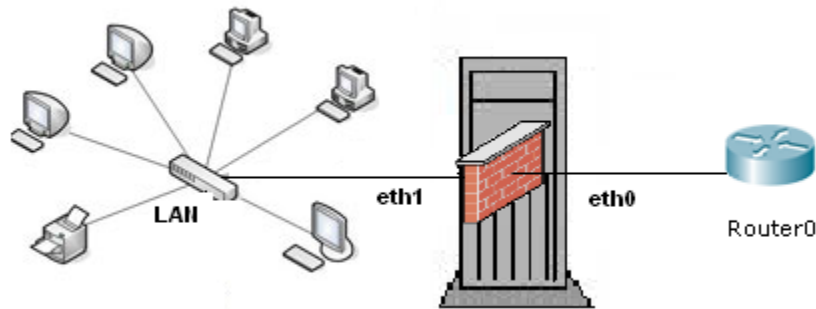
13º) Rechazamos a la máquina con IP 192.168.0.155 conectarse a nuestro equipo a través de Telnet.

```
root@miguel:/home/miguel# iptables -A INPUT -s 192.168.0.10 -p tcp --dport 23 -j
DROP
root@miguel:/home/miguel#
```

14º) Rechazamos las conexiones que se originen de la máquina con la dirección física 00:db:f0:34:ab:78.

```
root@miguel:/home/miguel# iptables -A INPUT -M 00:0c:29:de:dd:33 -i REJECT
root@miguel:/home/miguel#
```

Firewall de una LAN



15º) Rechazamos todo el tráfico que ingrese a nuestra red LAN 192.168.0.0 /24 desde una red remota, como Internet, a través de la interfaz eth0.

```
root@miguel:/home/miguel# iptables -A FORWARD -s 0.0.0.0/0 -i eth0 -d 192.168.0.0/24 -j DROP
root@miguel:/home/miguel#
```

16º) Cerramos el rango de puerto bien conocido desde cualquier origen:

```
root@miguel:/home/miguel# iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 1:1024 -j DROP
root@miguel:/home/miguel#
```

17º) Aceptamos que vayan de nuestra red 192.168.0.0/24 a un servidor web (puerto 80):

```
root@miguel:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -p tcp -dport 80 -j ACCEPT
root@miguel:/home/miguel#
```

18º) Aceptamos que nuestra LAN 192.168.0.0/24 vayan a puertos https:

```
root@miguel:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -p tcp -dport 443 -j ACCEPT
root@miguel:/home/miguel#
```

19º) Aceptamos que los equipos de nuestra red LAN 192.168.0.0/24 consulten los DNS, y denegamos todo el resto a nuestra red:

```
root@miguel:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -p tcp -dport 53 -j ACCEPT
root@miguel:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -p udp -dport 53 -j ACCEPT
root@miguel:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -j DROP
root@miguel:/home/miguel#
```

20º) Permitimos enviar y recibir e-mail a todos:

```
root@miguel:/home/miguel# iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 25 -j ACCEPT
root@miguel:/home/miguel# iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 110 -j ACCEPT
root@miguel:/home/miguel#
```

21º) Cerramos el acceso de una red definida 192.168.3.0/24 a nuestra red LAN 192.168.2.0/24:

```
root@miguel:/home/miguel# iptables -A INPUT -s 192.168.3.0/24 -d 192.168.0.0/24 -j DROP
root@miguel:/home/miguel#
```

22º) Permitimos el paso de un equipo específico 192.168.3.5 a un servicio (puerto 5432) que ofrece un equipo específico (192.168.0.5) y su respuesta:

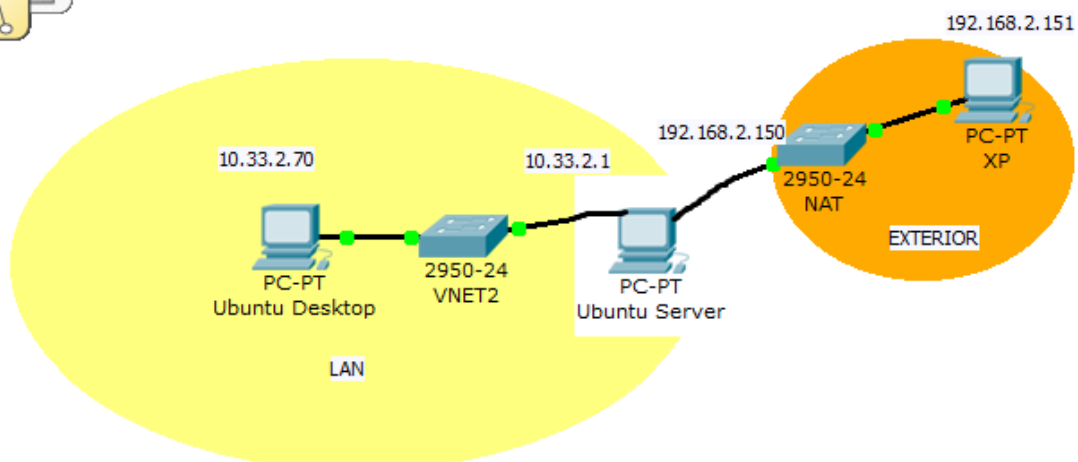
```
root@miguel:/home/miguel# iptables -A FORWARD -s 192.168.3.5/24 -d 192.168.0.5 -p tcp --dport 5432 -j ACCEPT
root@miguel:/home/miguel# iptables -A FORWARD -d 192.168.3.5/24 -s 192.168.0.5 -p tcp --dport 5432 -j ACCEPT
root@miguel:/home/miguel#
```

23º) Permitimos el paso de paquetes cuya conexión ya se ha establecido o es nueva pero está relacionada a una conexión ya establecida.

```
root@miguel:/home/miguel# iptables -A INPUT -n state --state ESTABLISHED,RELATED -j ACCEPT
```

b) Resolución escenario UD3-1.a. NAT.

Escenario



Establecemos la iptable, para que todo lo que salga por la interfaz eth1 salga por la eth0.

```

root@equipo02:~# iptables -t nat -F
root@equipo02:~# iptables -t nat -X
root@equipo02:~# iptables -t nat -Z
root@equipo02:~# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
root@equipo02:~# iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to-source 192.168.2.150
root@equipo02:~# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
SNAT all -- 0.0.0.0/0 0.0.0.0/0 to:192.168.2.150
root@equipo02:~#
    
```

Comprobamos la Ip del equipo que está dentro de la red.

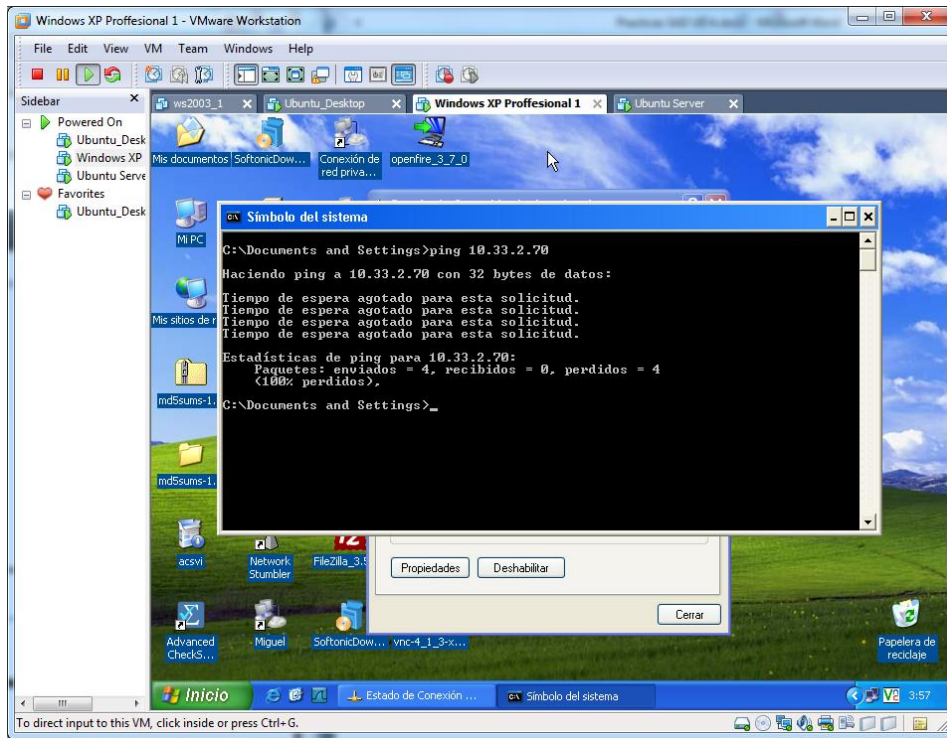
```

miguel@miguel:~$ ifconfig
eth1: Link encap:Ethernet direcciónHW 00:0c:29:90:9c:05
      Direc. inet:10.33.2.70 Difus.:10.33.2.255 Másc:255.255.255.0
      Dirección inet6: fe80::20c:29ff:fe90:9c05/64 Alcance:Enlace
      ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
      Paquetes RX:253 errores:0 perdidos:0 overruns:0 frame:0
      Paquetes TX:553 errores:0 perdidos:0 overruns:0 carrier:0
      colisiones:0 long.colaTX:1000
      Bytes RX:27544 (27.5 KB) TX bytes:35326 (35.3 KB)
      Interrupción:19 Dirección base: 0x2000

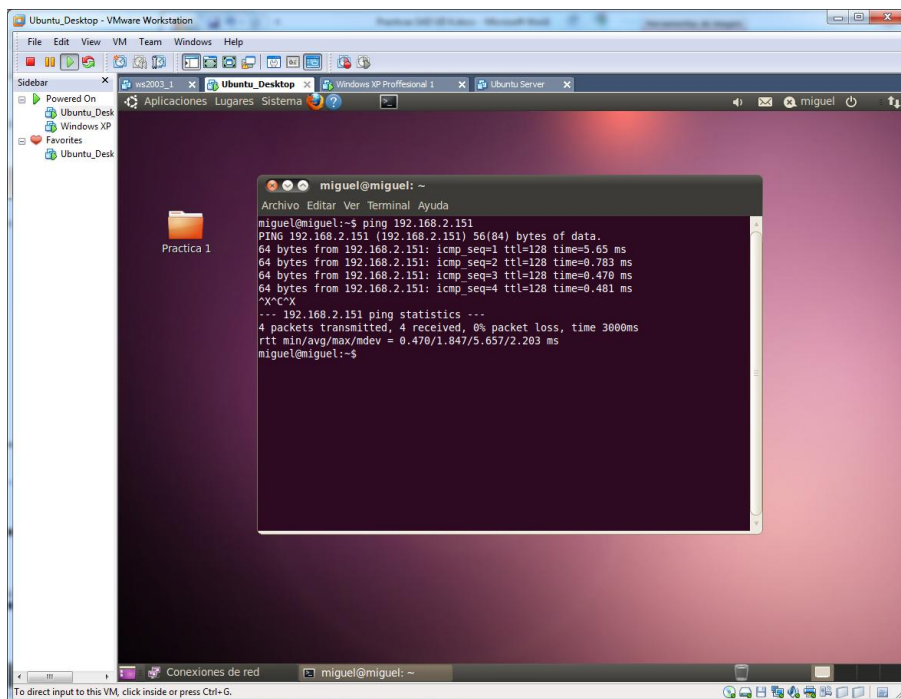
lo: Link encap:Bucle local
      Direc. inet:127.0.0.1 Másc:255.0.0.0
      Dirección inet6: ::1/128 Alcance:Anfitrión
      ACTIVO BUCLE FUNCIONANDO MTU:16436 Métrica:1
      Paquetes RX:203 errores:0 perdidos:0 overruns:0 frame:0
      Paquetes TX:203 errores:0 perdidos:0 overruns:0 carrier:0
      colisiones:0 long.colaTX:0
      Bytes RX:19124 (19.1 KB) TX bytes:19124 (19.1 KB)

miguel@miguel:~$
    
```

Comprobamos que el ordenador del exterior no puede conectar con el cliente de la lan.



Sin embargo el de dentro sí que puede conectar con el exterior.



CORTAFUEGOS:

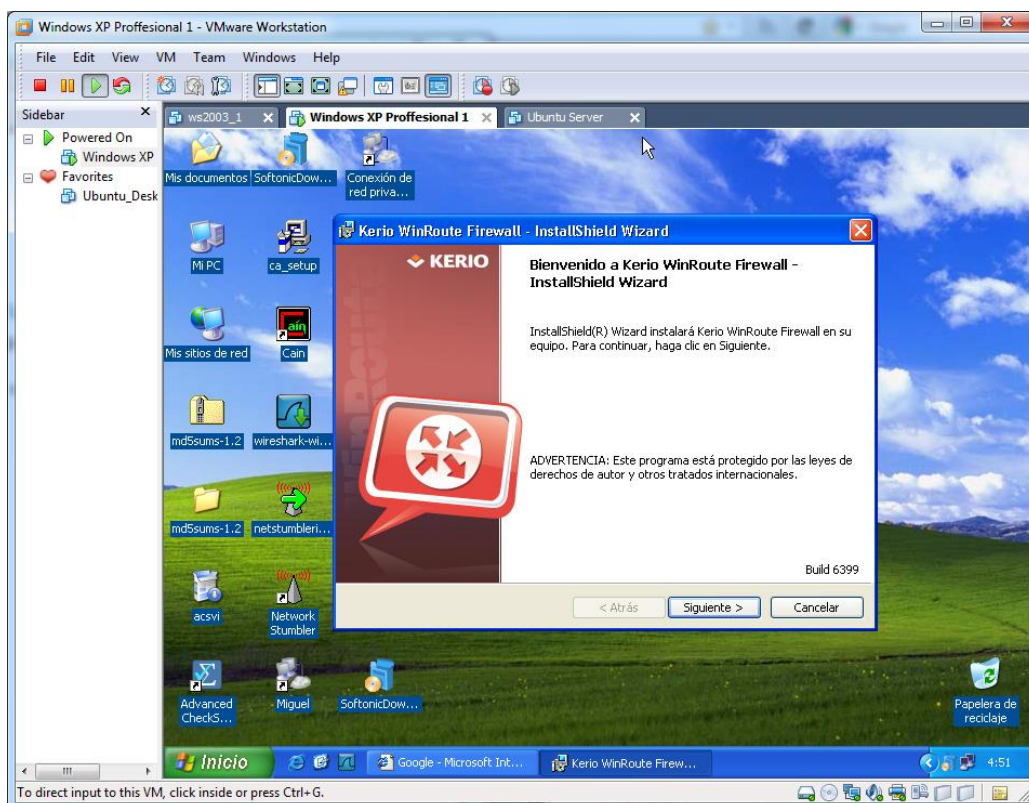
5. CORTAFUEGOS SOFTWARE.

a) Cortafuego integrado en Windows. Instalación de software de cortafuegos en Windows y Linux:

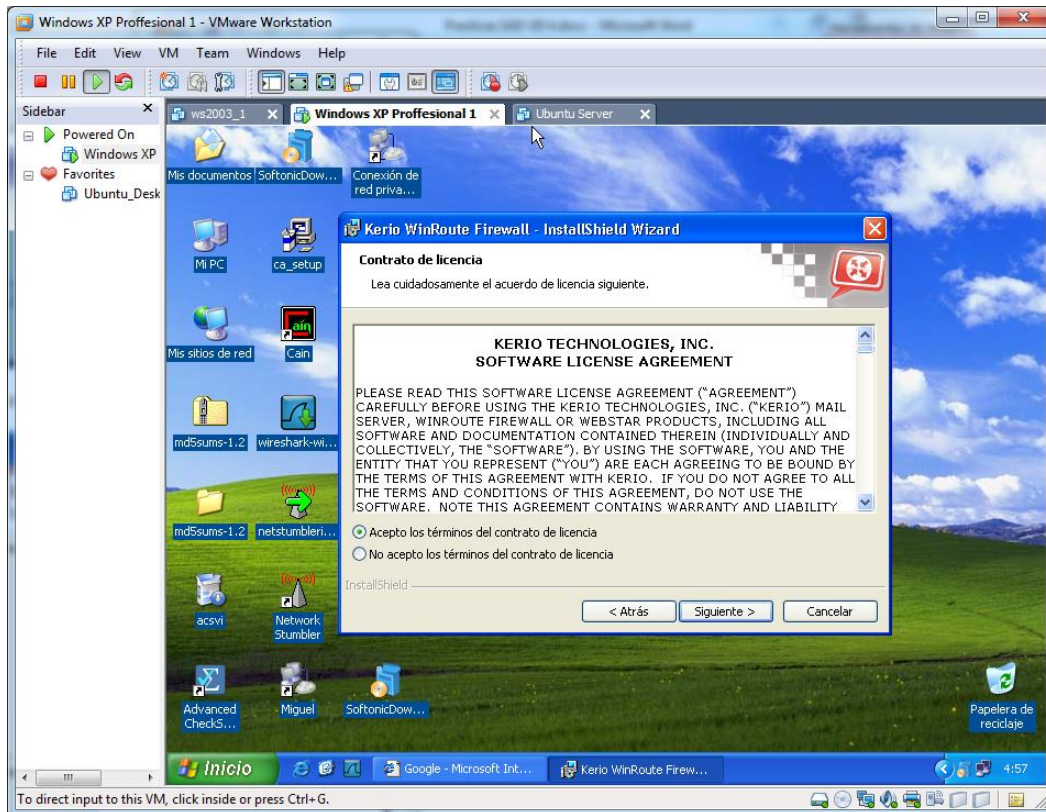
i) Instalar y configura el cortafuegos Kerio Winroute Firewall (Windows/Linux).

Nos descargamos la aplicación Kerio Winroute en nuestro equipo, que es un cortafuegos software muy potente para nuestro equipo (sólo entornos Windows.)

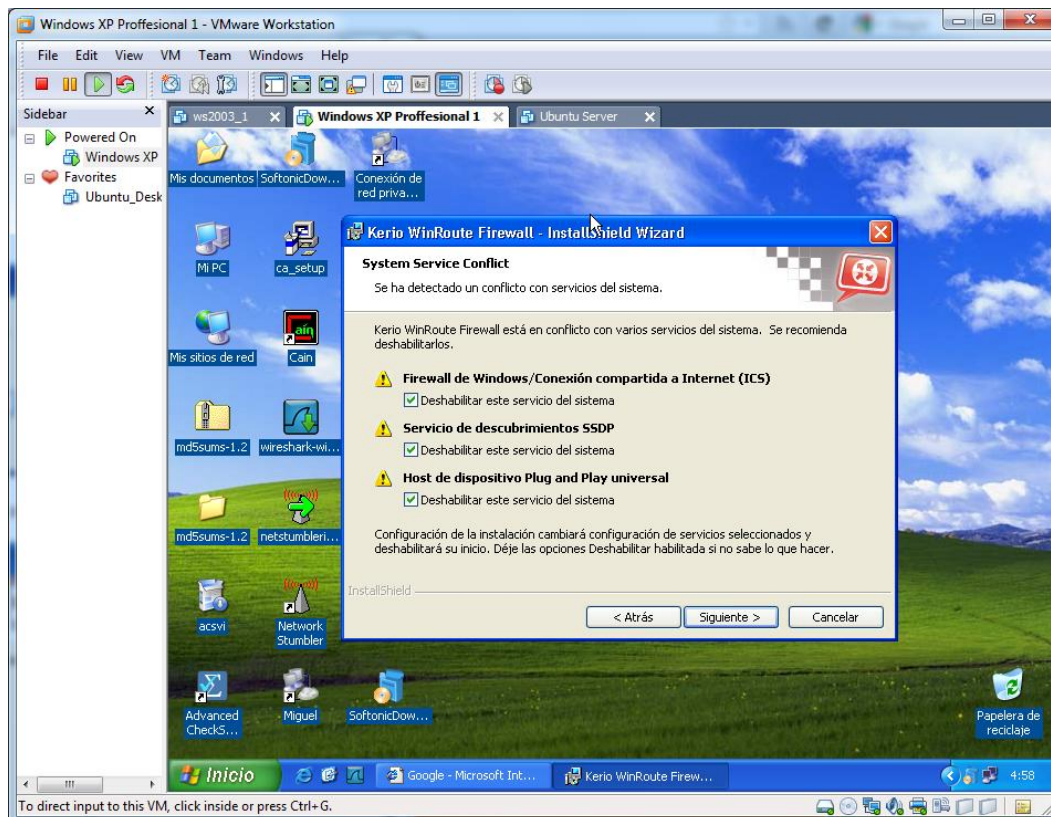
Comenzamos la instalación de la aplicación **Kerio WinRoute**.



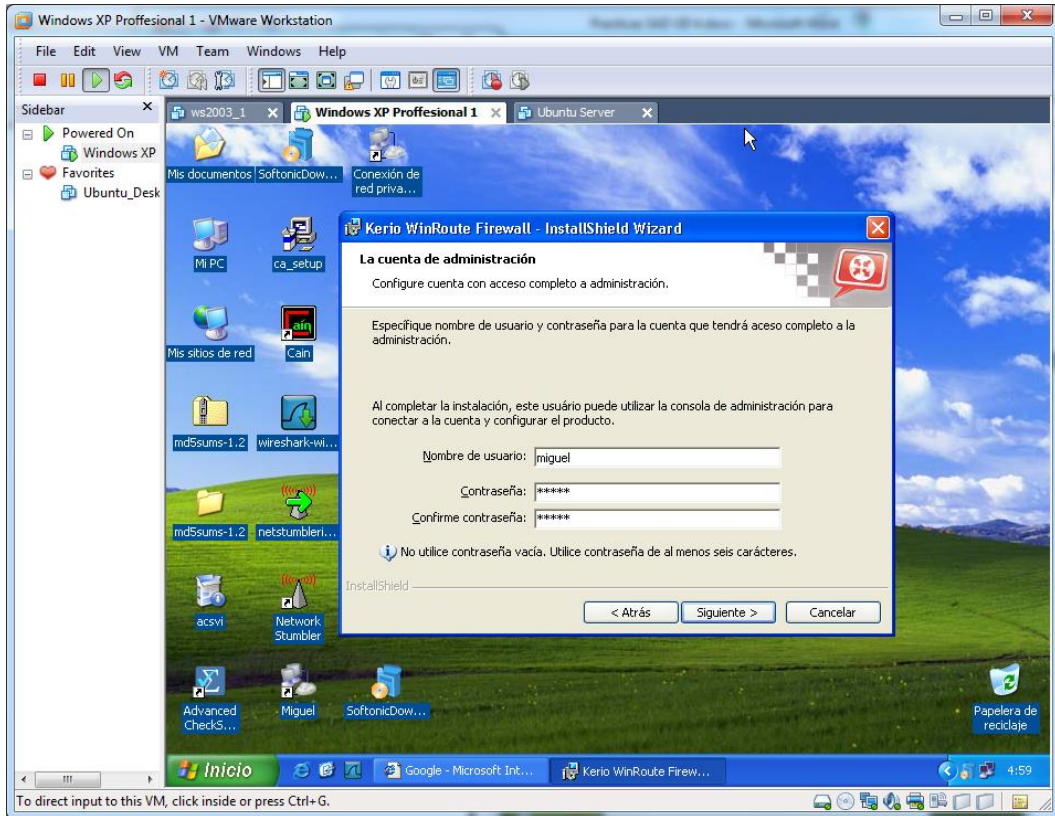
Aceptamos los términos de licencia.



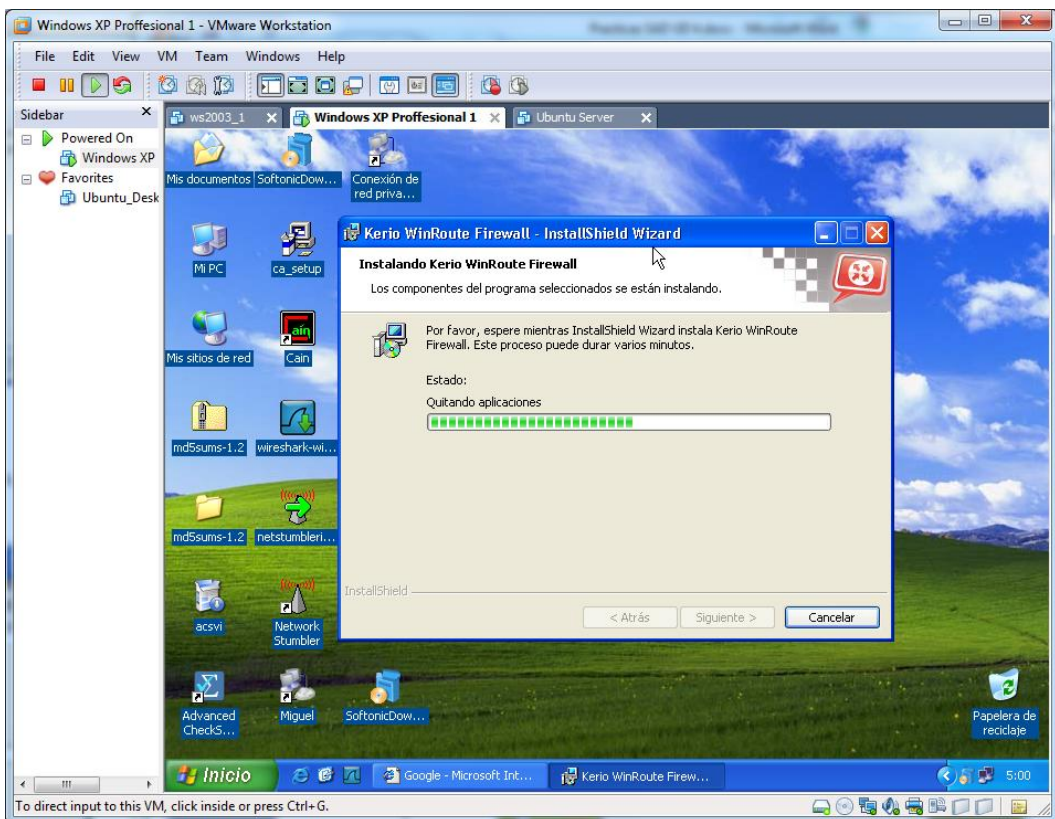
Marcamos las siguientes opciones para deshabilitar elementos como el firewall integrado de Windows y otros.



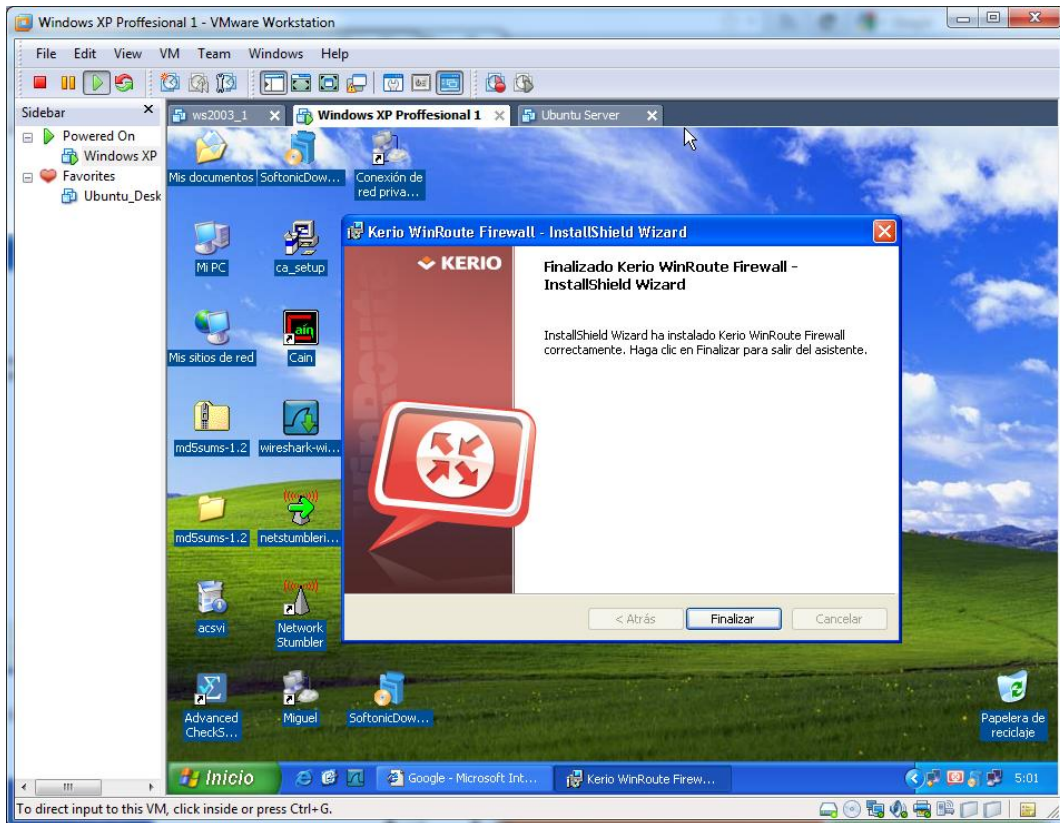
Introducimos el nombre de usuario y contraseña que usaremos para el administrador.



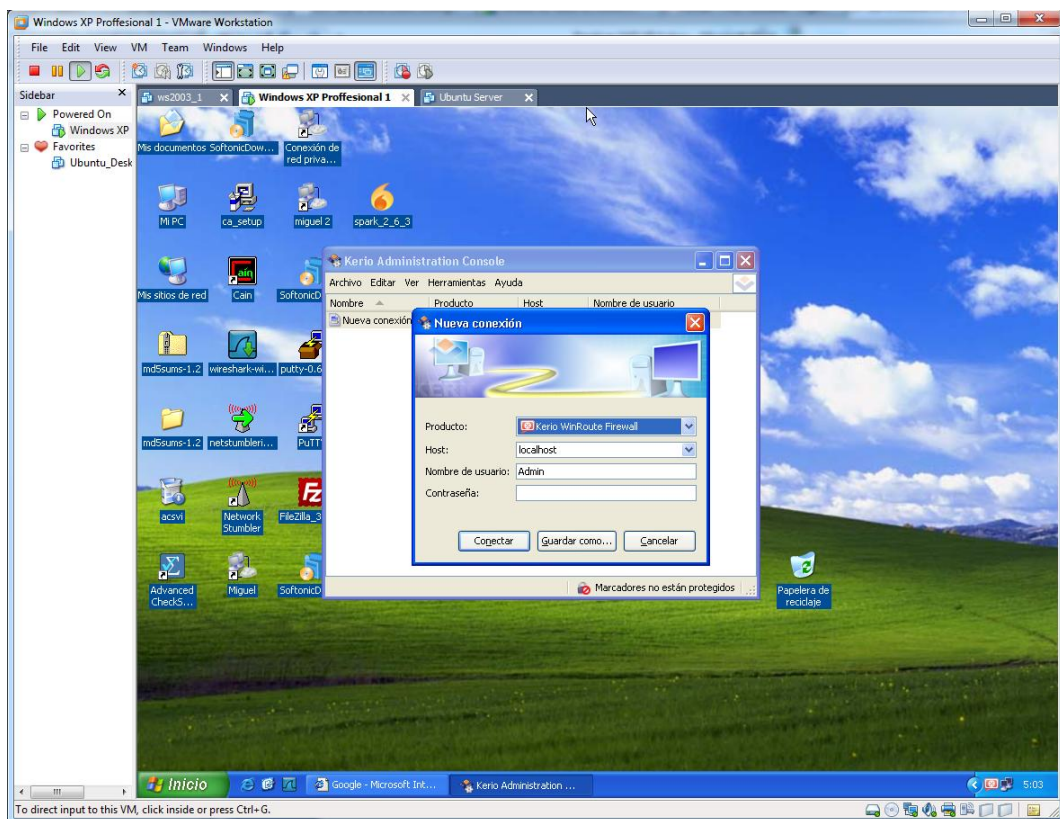
Comienza la instalación.



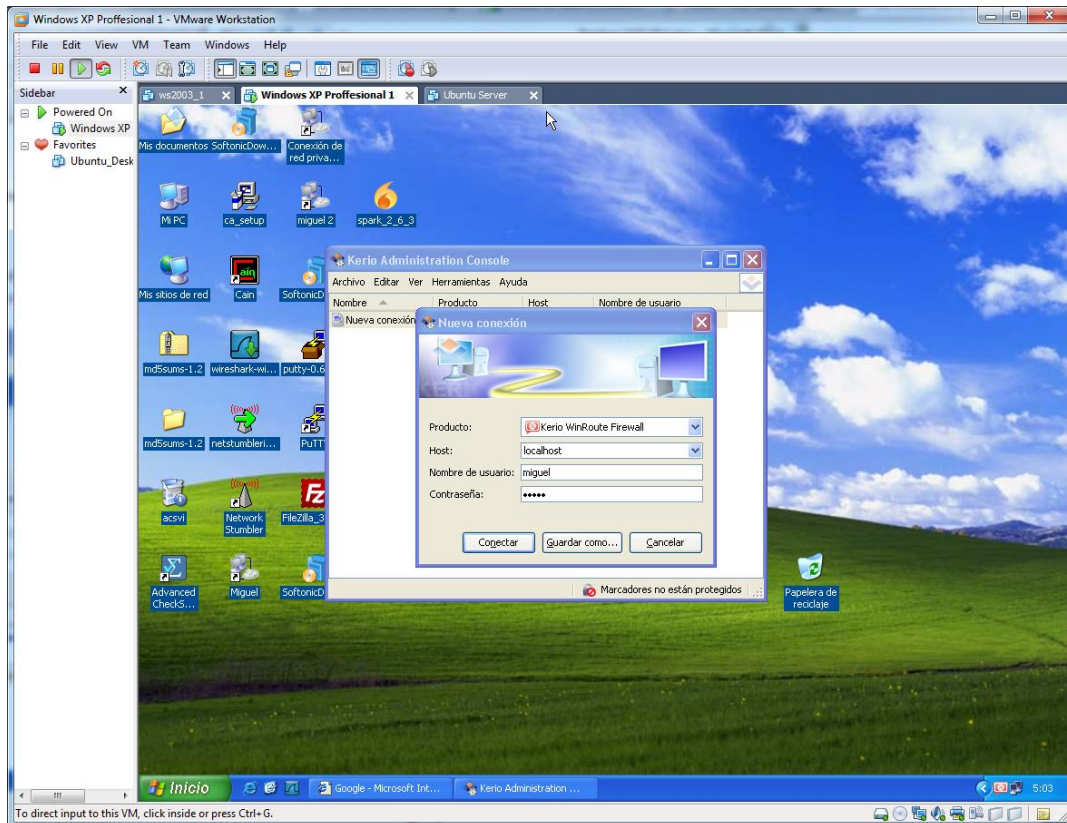
Una vez terminada la instalación finalizamos.



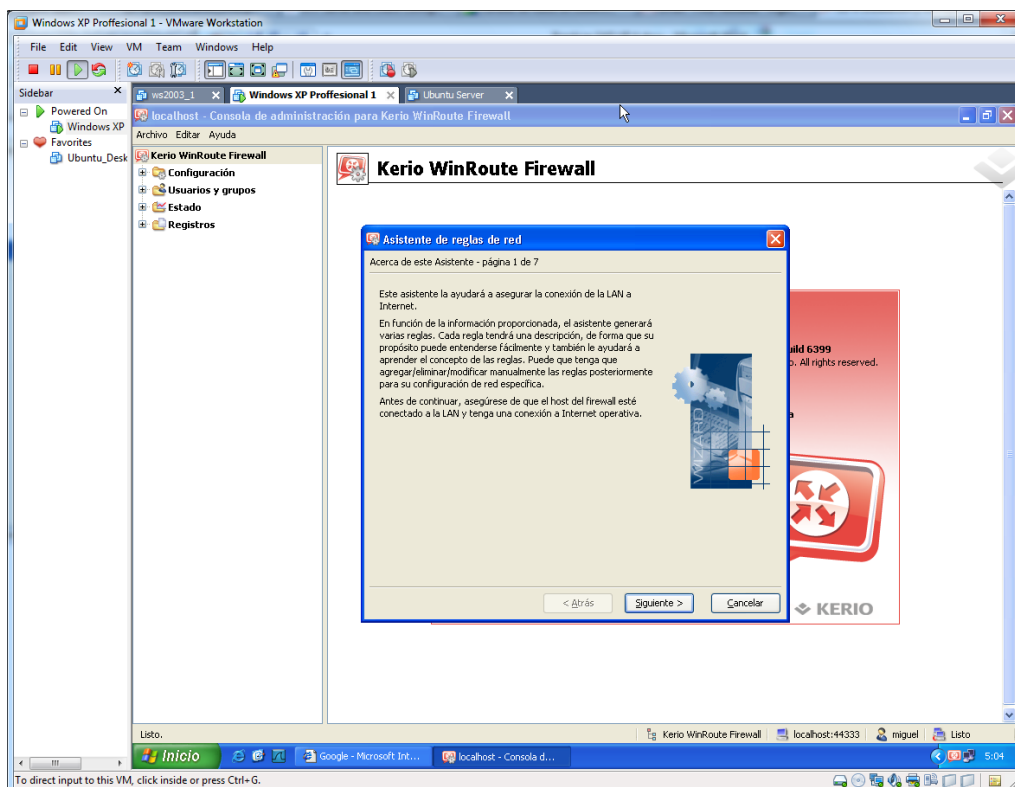
Ejecutamos la aplicación, y nos aparece esta ventana de autenticación.



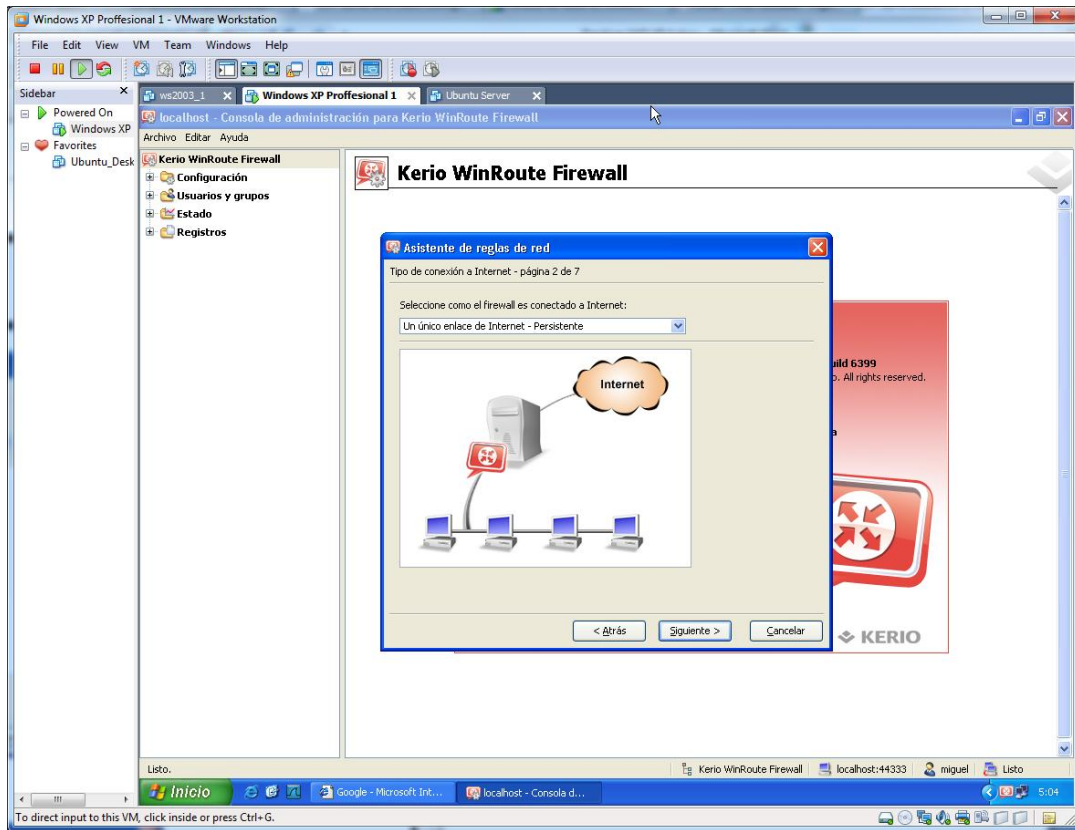
Accedemos con la cuenta que nos hemos creado anteriormente.



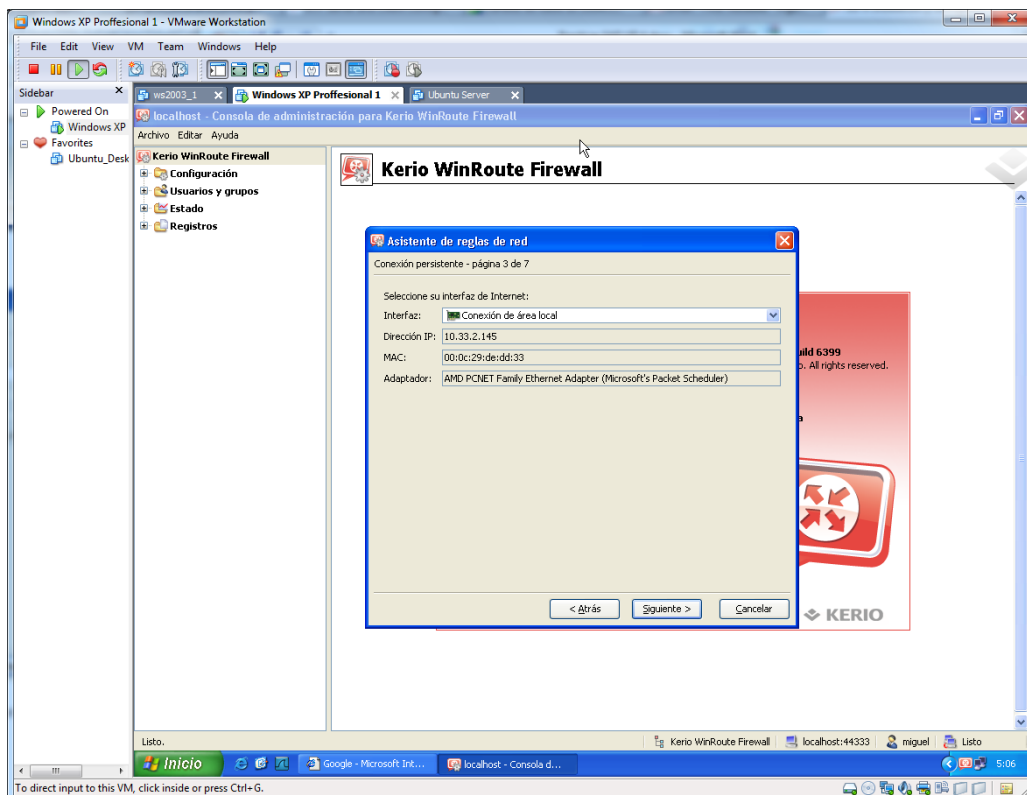
La primera vez que accedamos nos aparecerá este asistente de configuración.



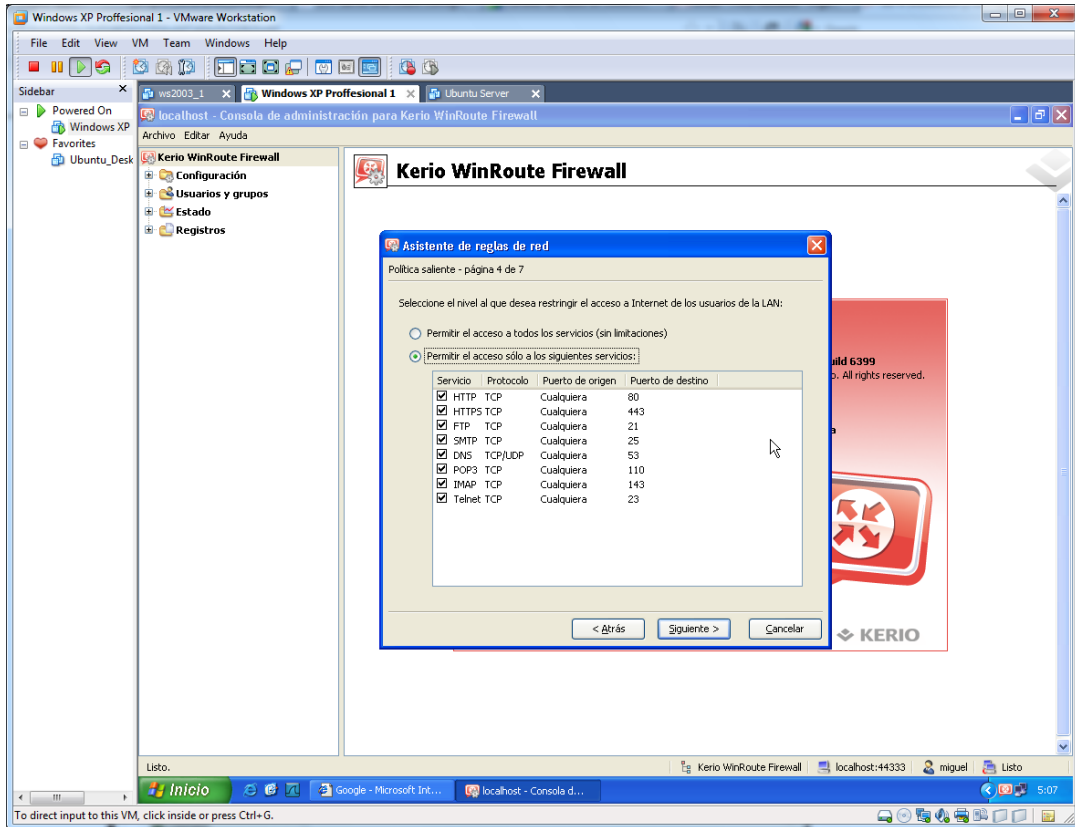
Elegimos la opción de **único enlace de Internet**.



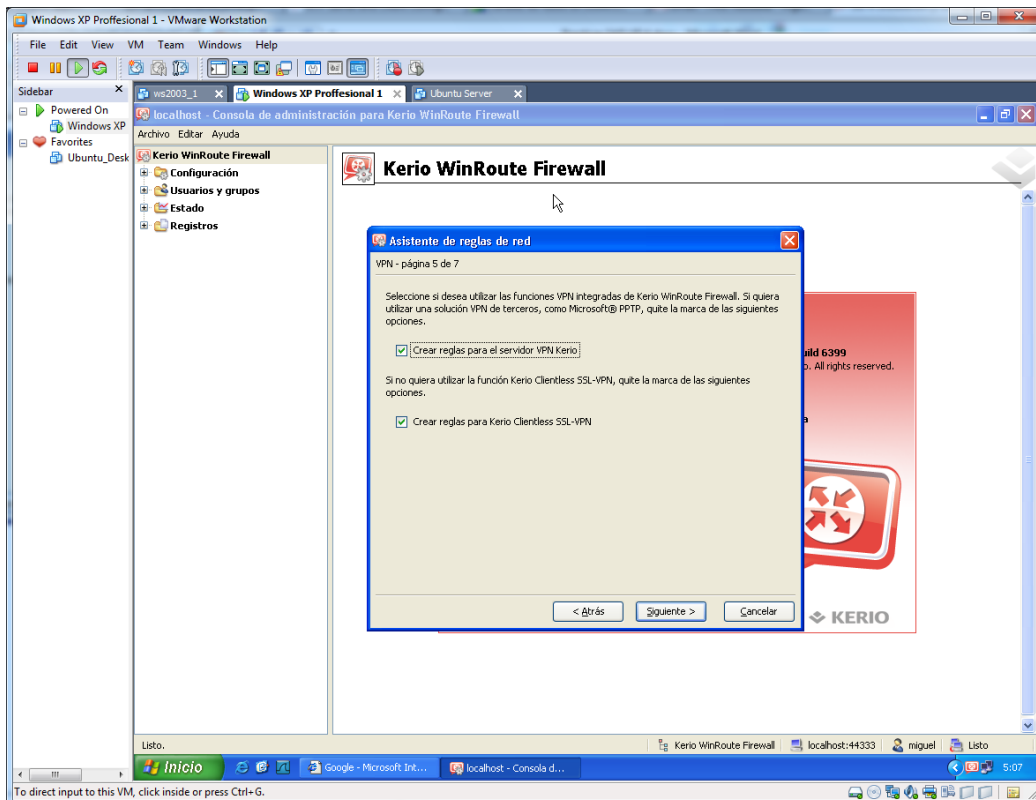
Elegimos nuestra tarjeta o interfaz de red.



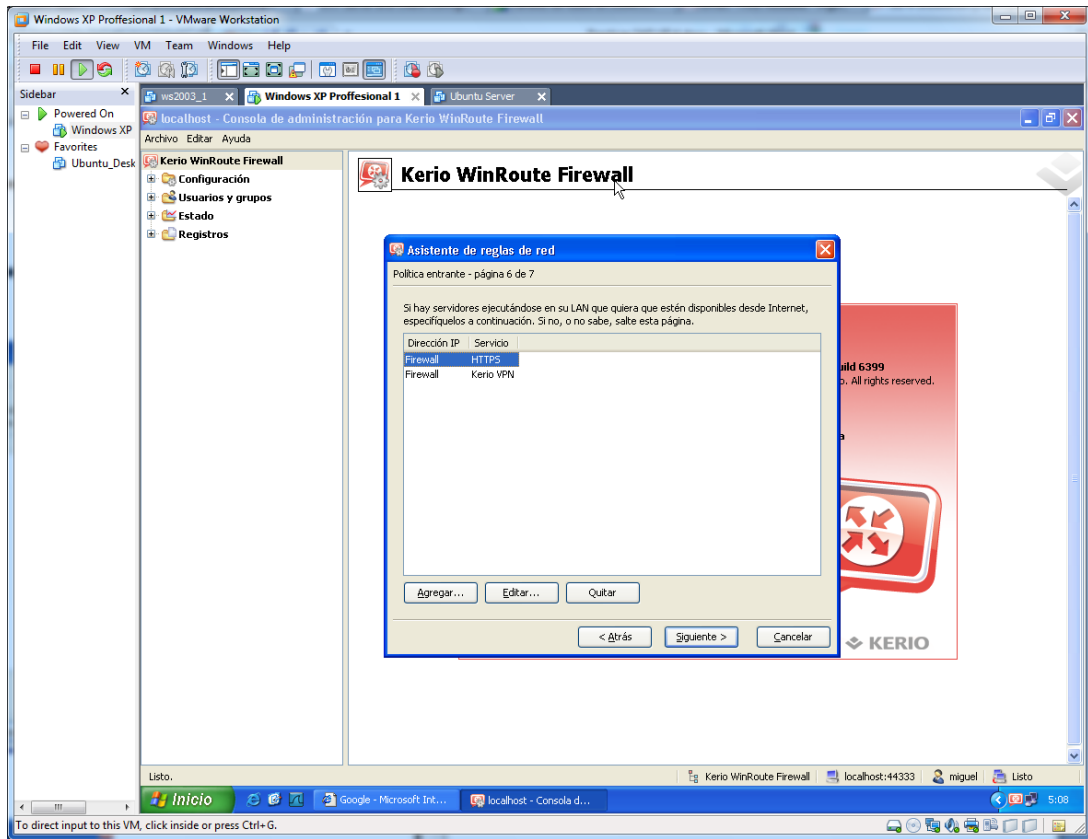
En esta pantalla, podemos escoger los protocolos a deshabilitar desmarcando el checkbox. Pero de momento, lo vamos a dejar como está.



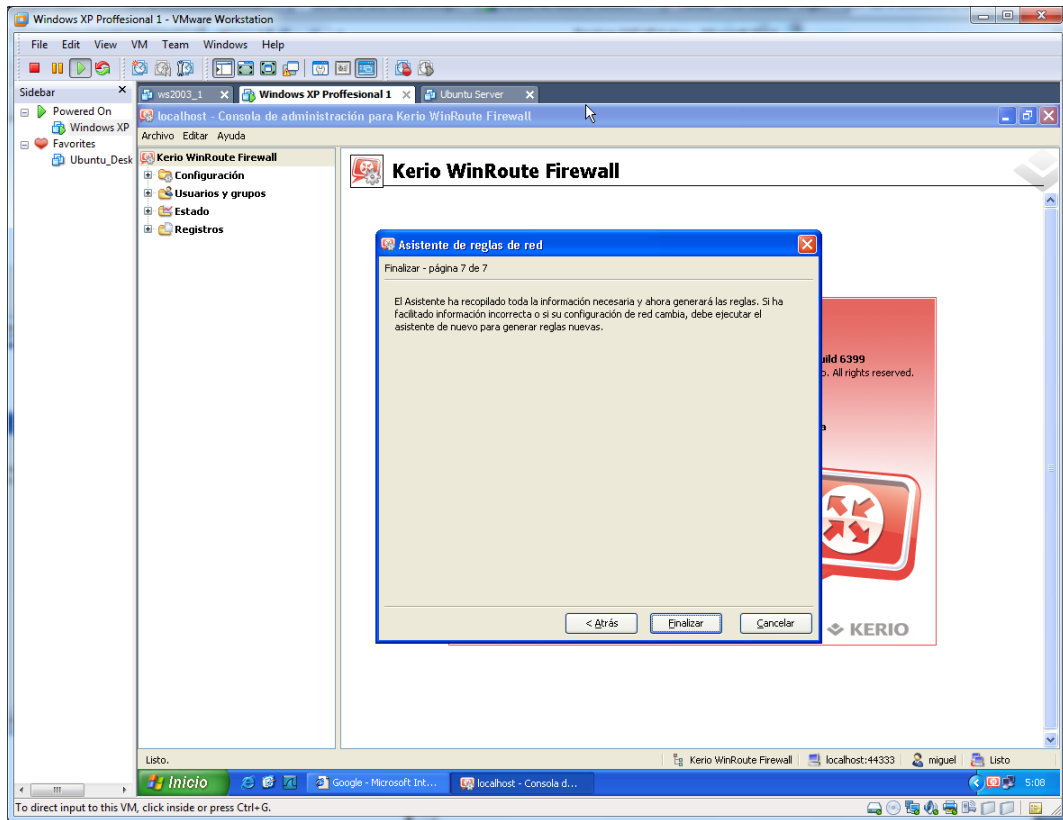
Dejamos marcadas estas opciones.



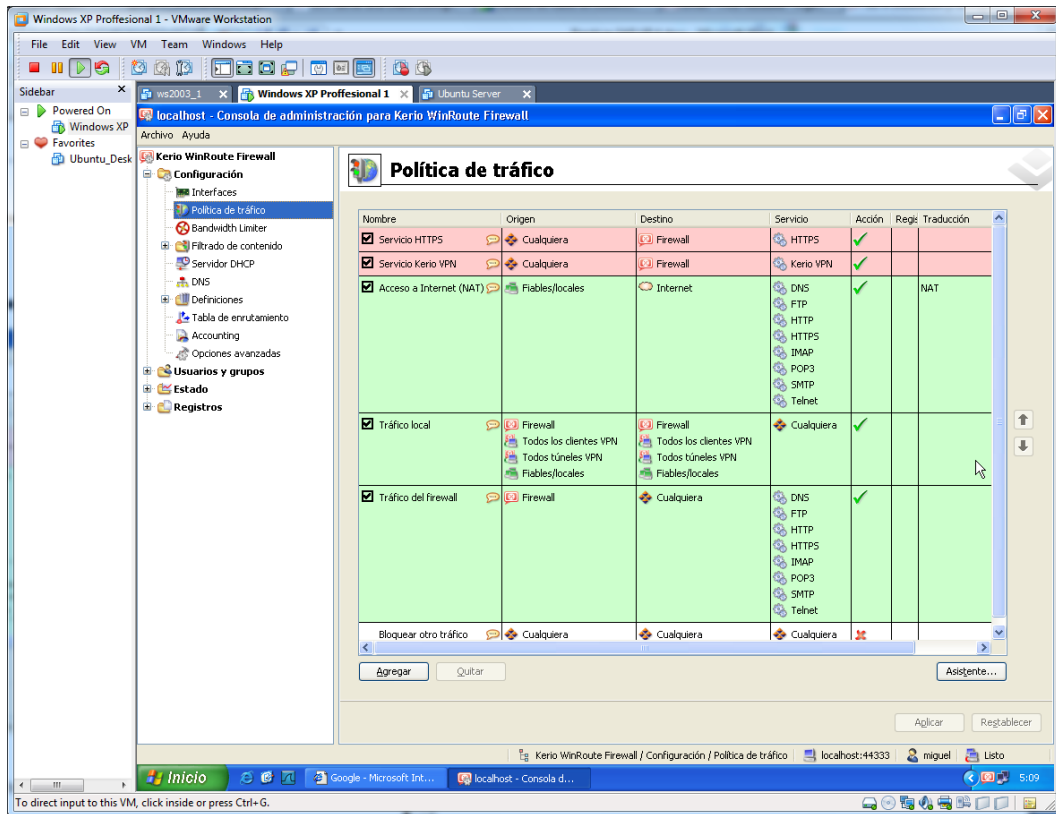
Dejamos estas reglas por defecto.



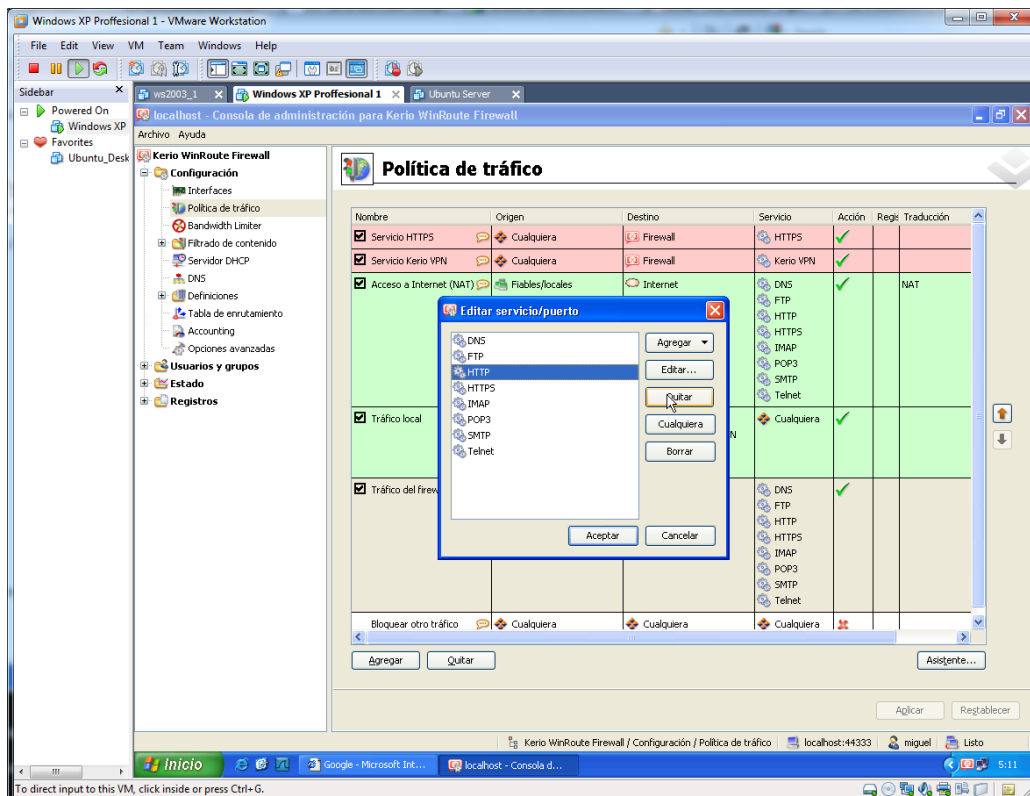
Por último finalizamos el asistente.



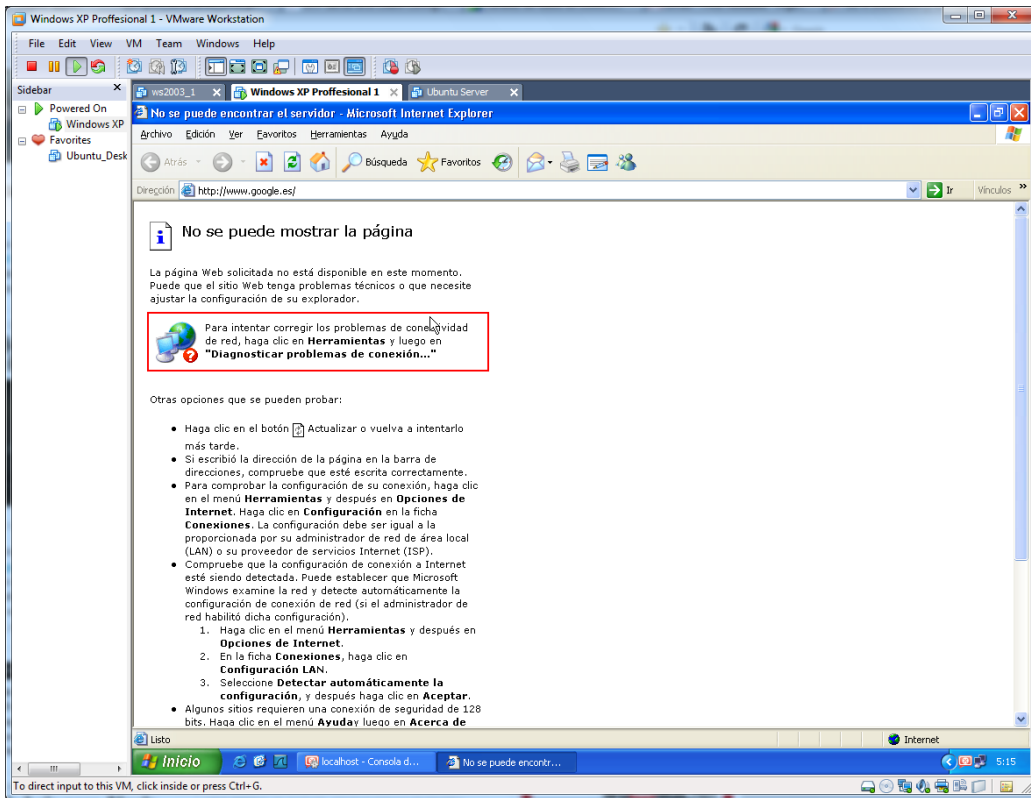
Nos situamos en política de tráfico. Donde podemos habilitar-deshabilitar diferentes protocolos de nuestro equipo.



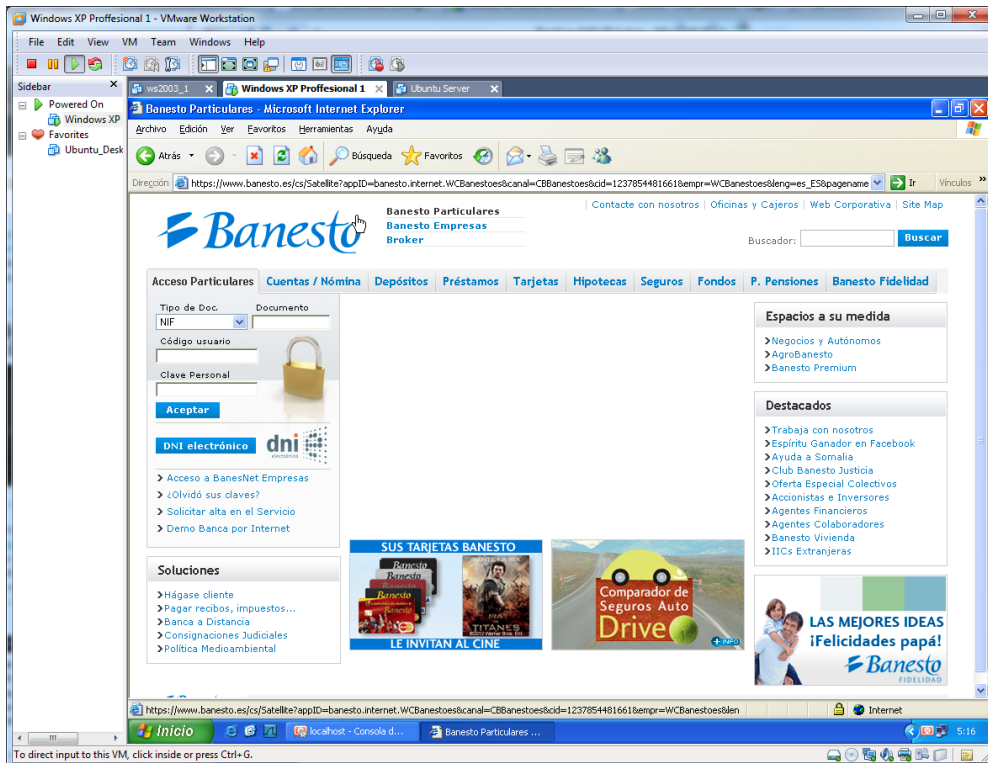
Nos situamos en acceso a internet, y pulsamos a la casilla servicio. Se desplegará la siguiente ventana, donde podemos deshabilitar protocolos como en éste caso el HTTP.



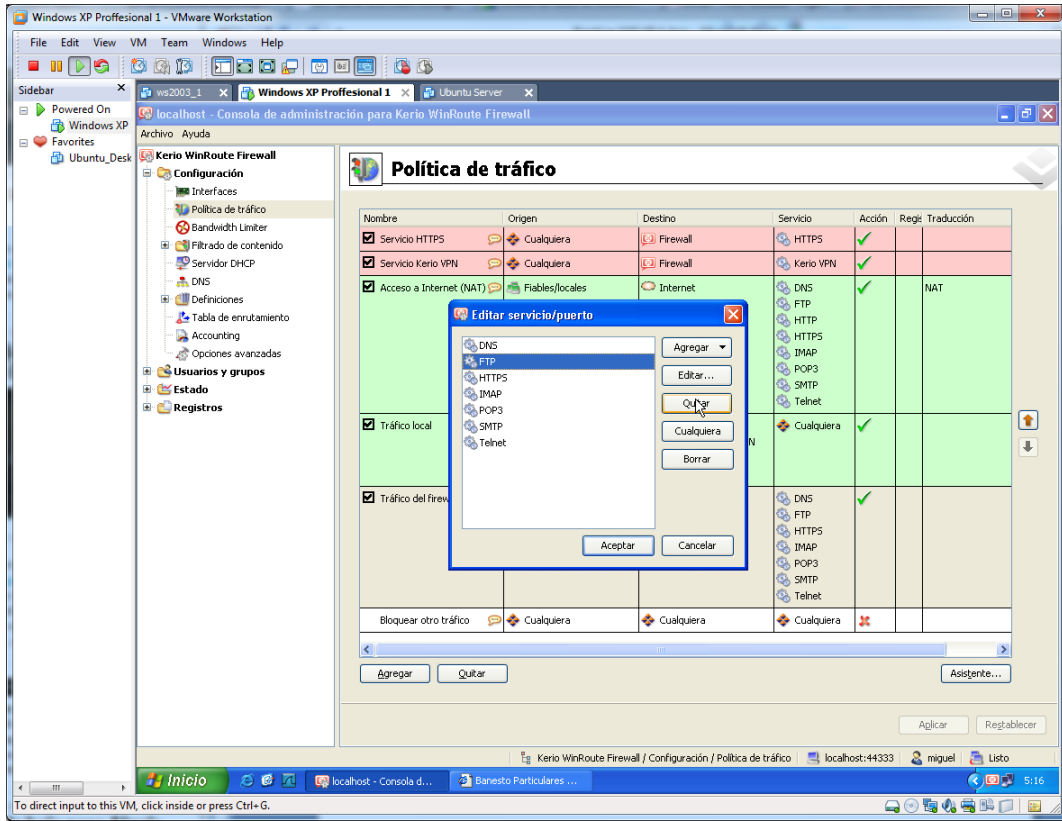
Comprobamos al acceso a internet a través de otro protocolo, donde el resultado será:



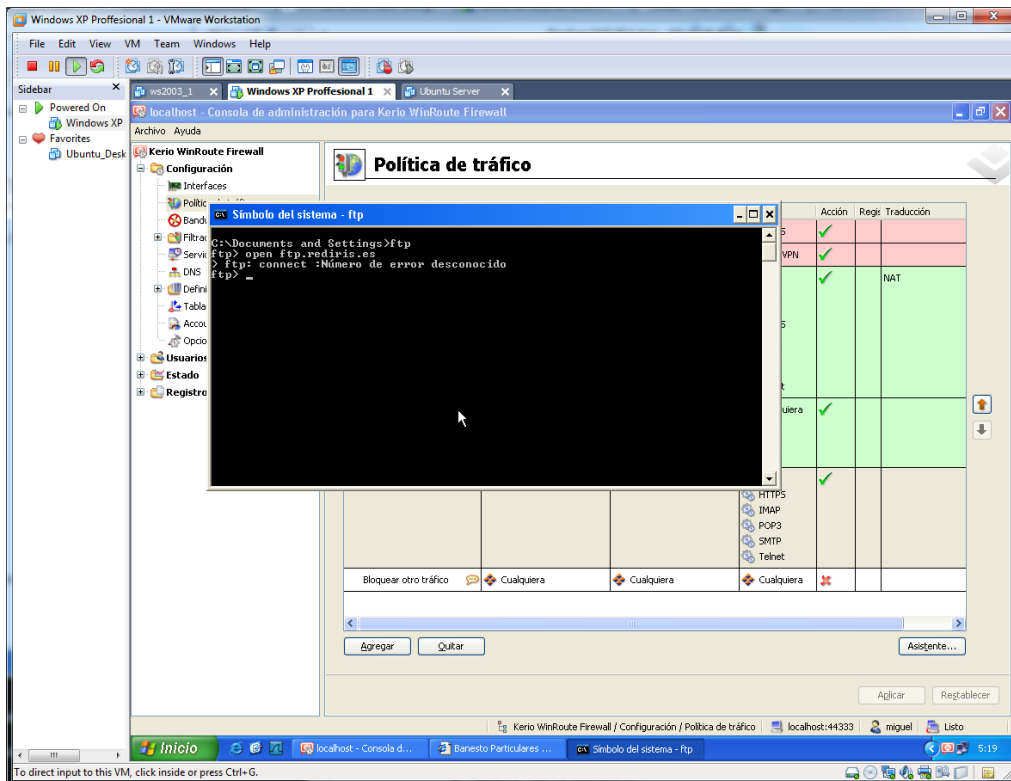
Comprobamos una página con protocolo HTTPS, para comprobar que a éstas sí que podemos acceder.



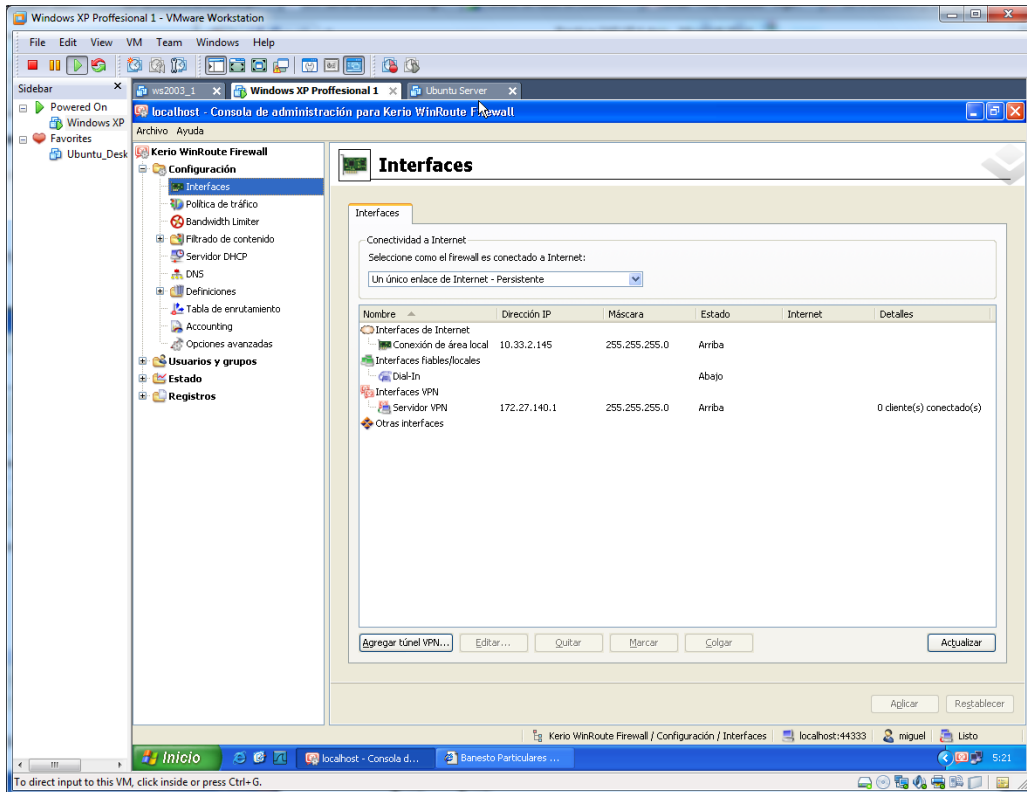
Si de la misma manera, deshabilitamos el protocolo FTP.



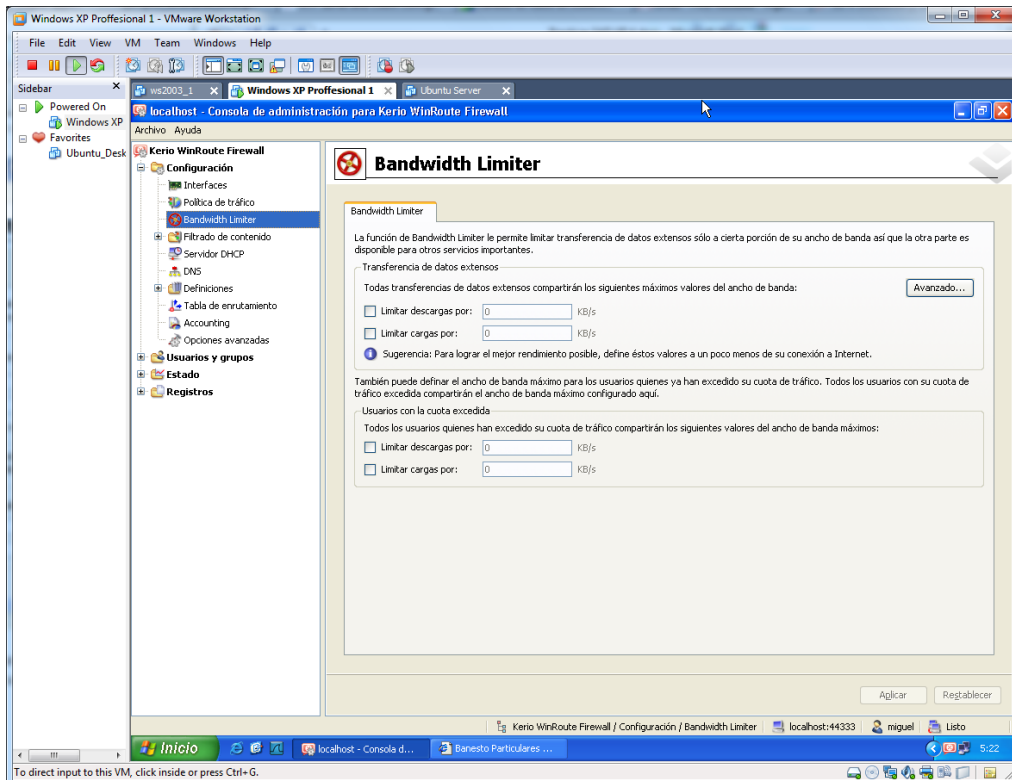
Comprobamos que no podemos establecer conexiones FTP a través de internet.



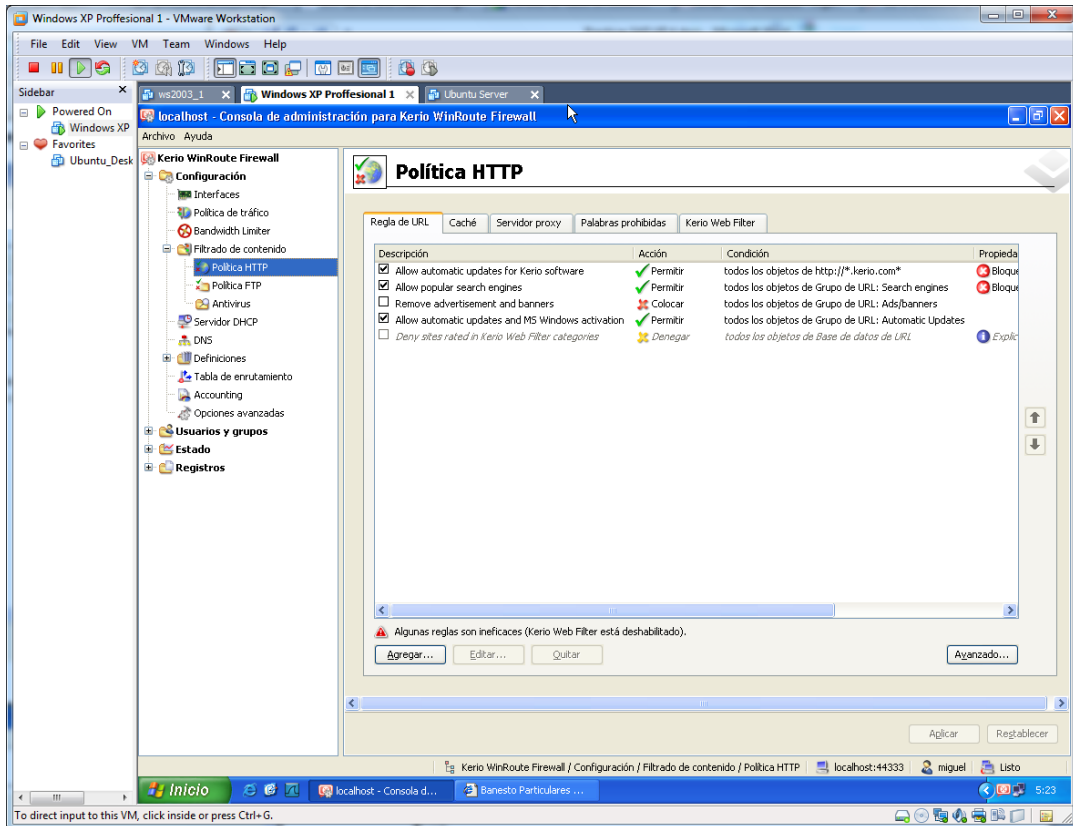
En la opción interfaces, podemos seleccionar la interfaz que queremos. O configurar VPN.



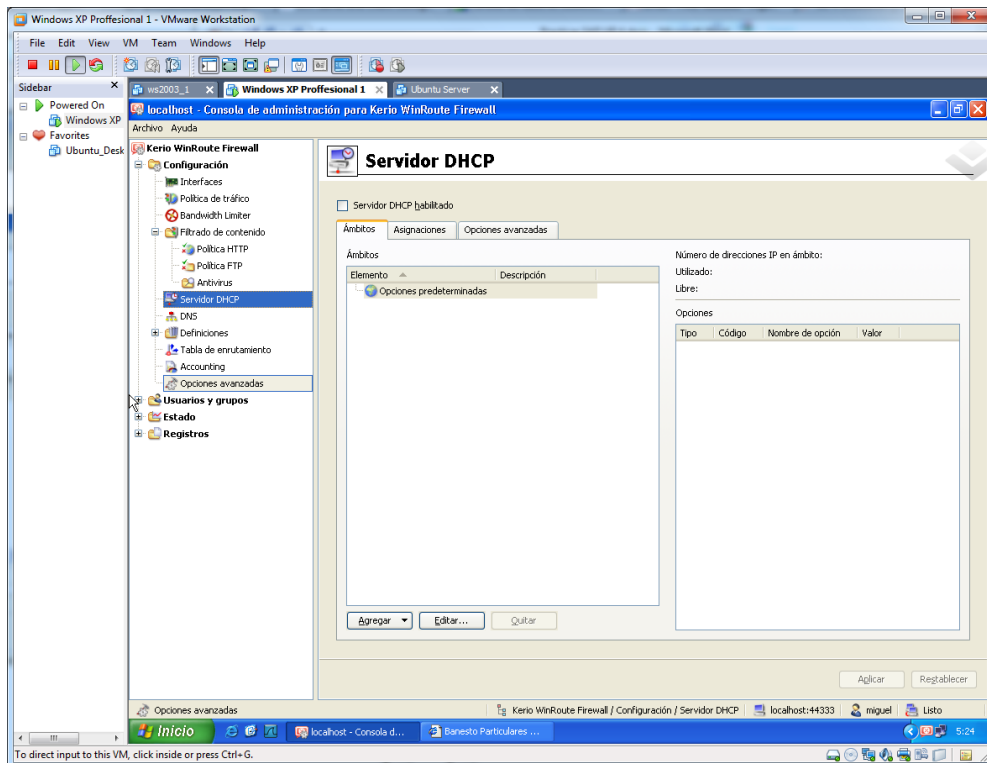
Aquí podemos controlar el ancho de bando, haciendo diferentes limitaciones.



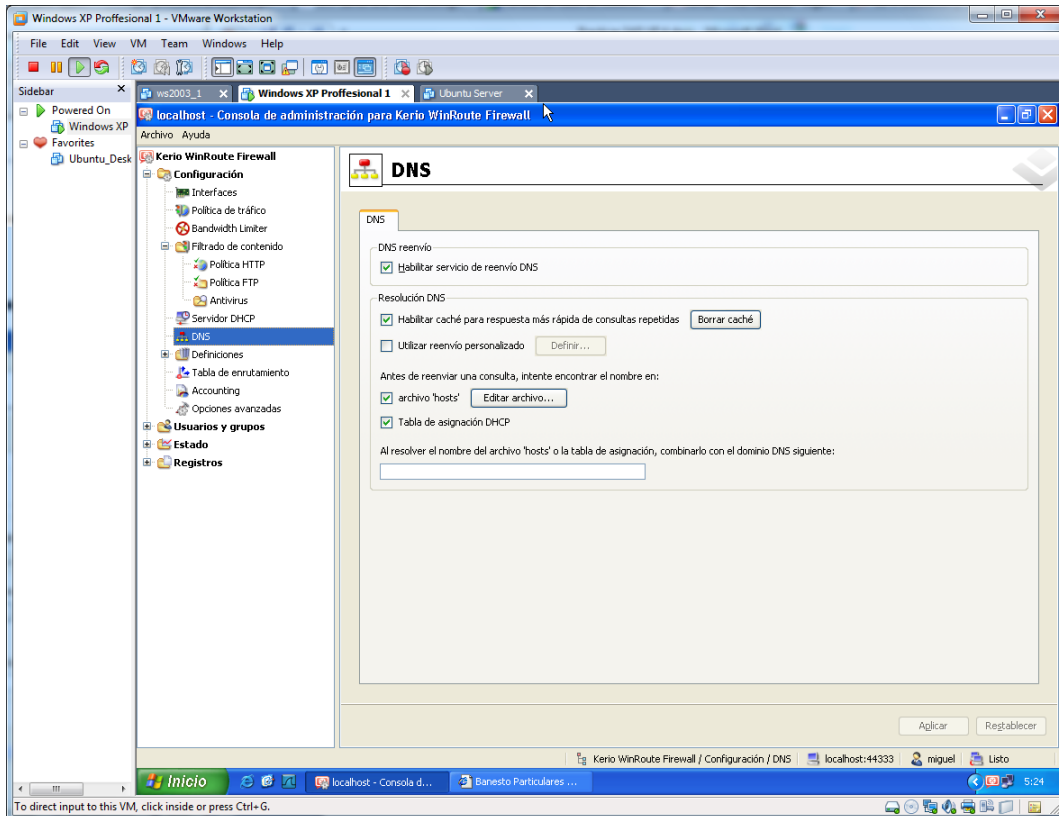
Aquí podemos realizar configuraciones, que por defecto ya realizan por defecto en el protocolo HTTP.



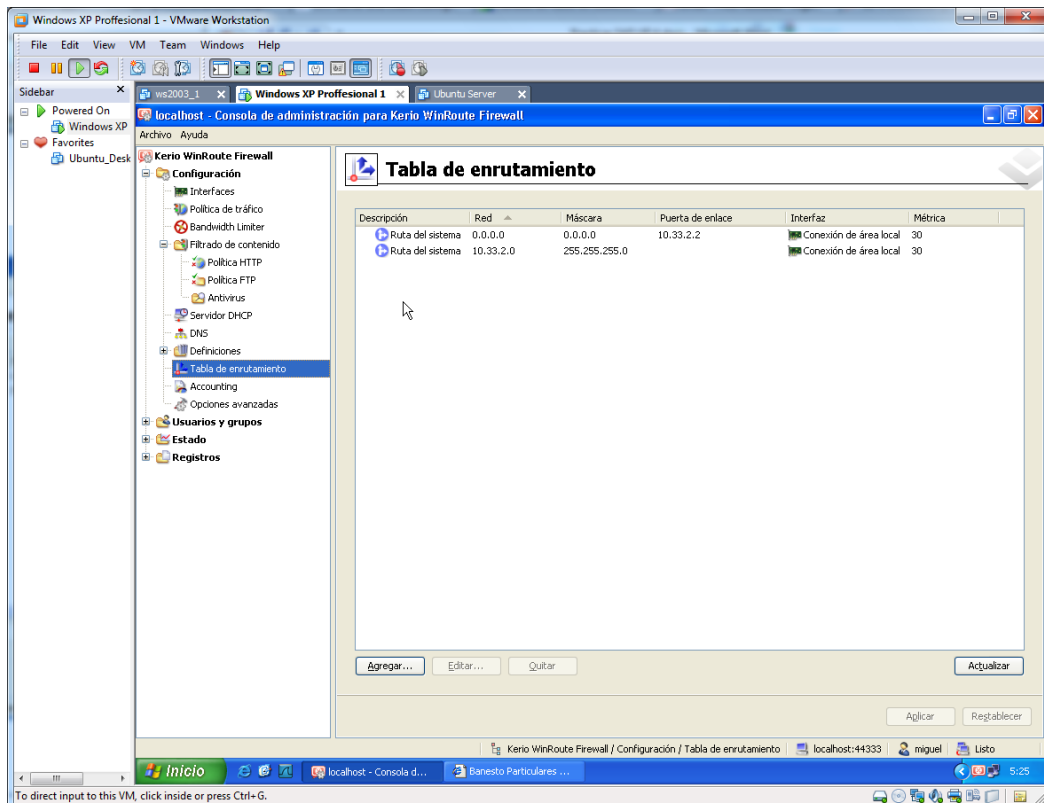
Hacemos configuraciones del DHCP.



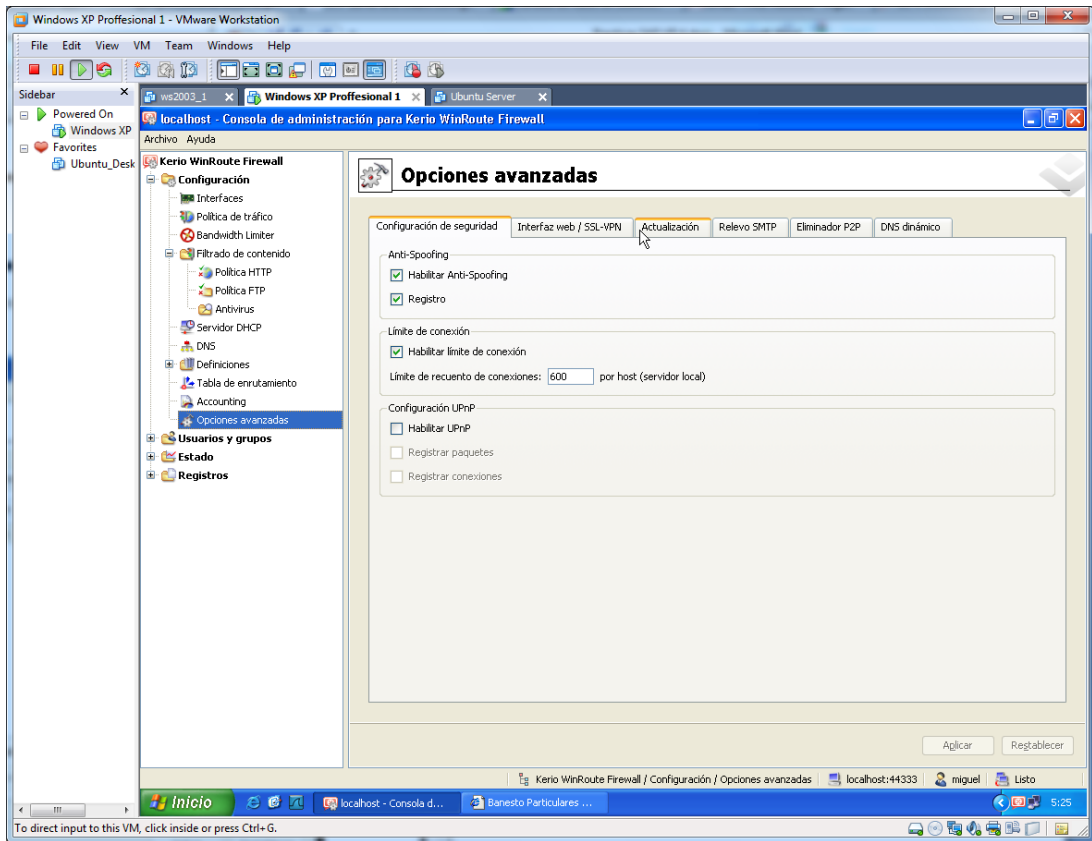
Configuramos opciones de DNS.



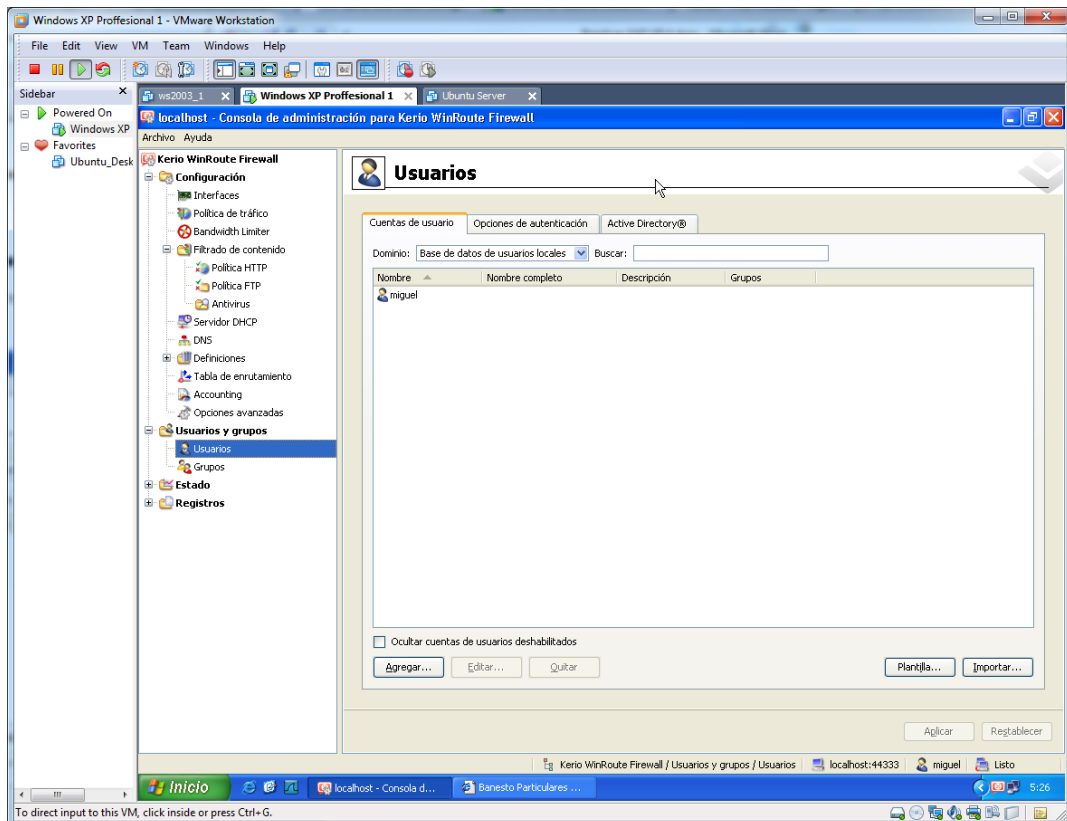
Podemos comprobar la tabla de enrutamiento en esta ventana.



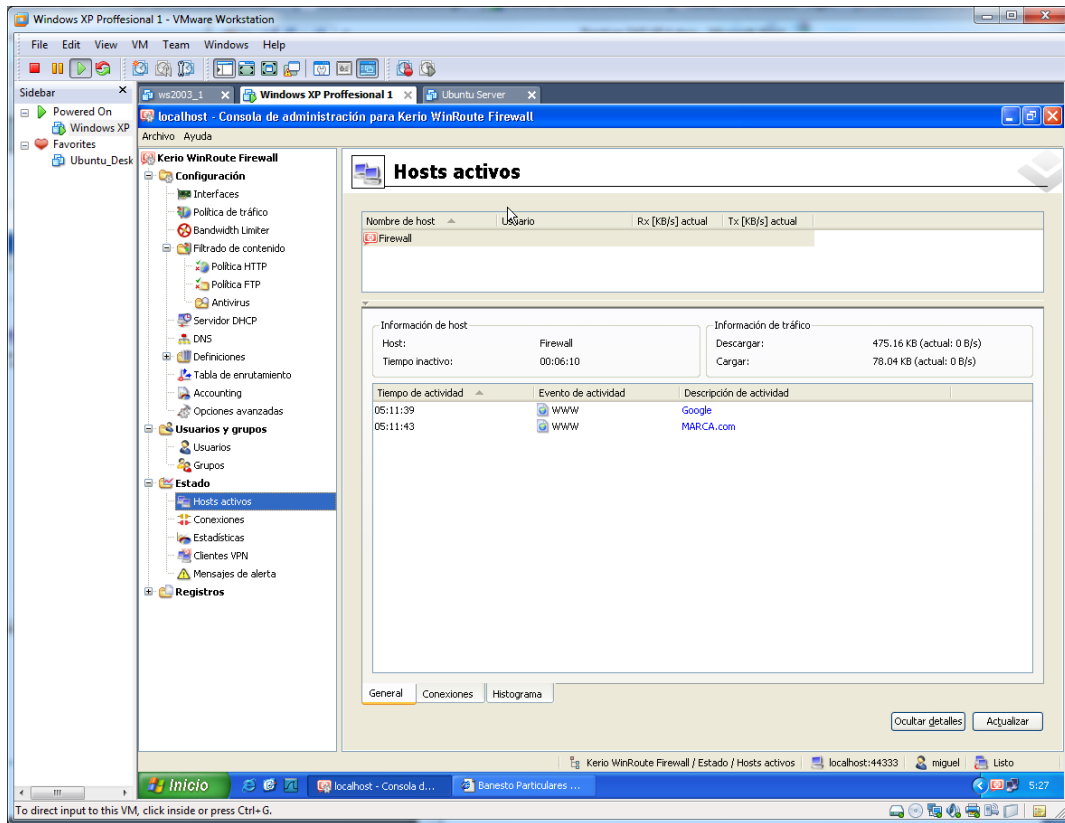
En opciones avanzadas, podemos realizar configuraciones más específicas del servicio.



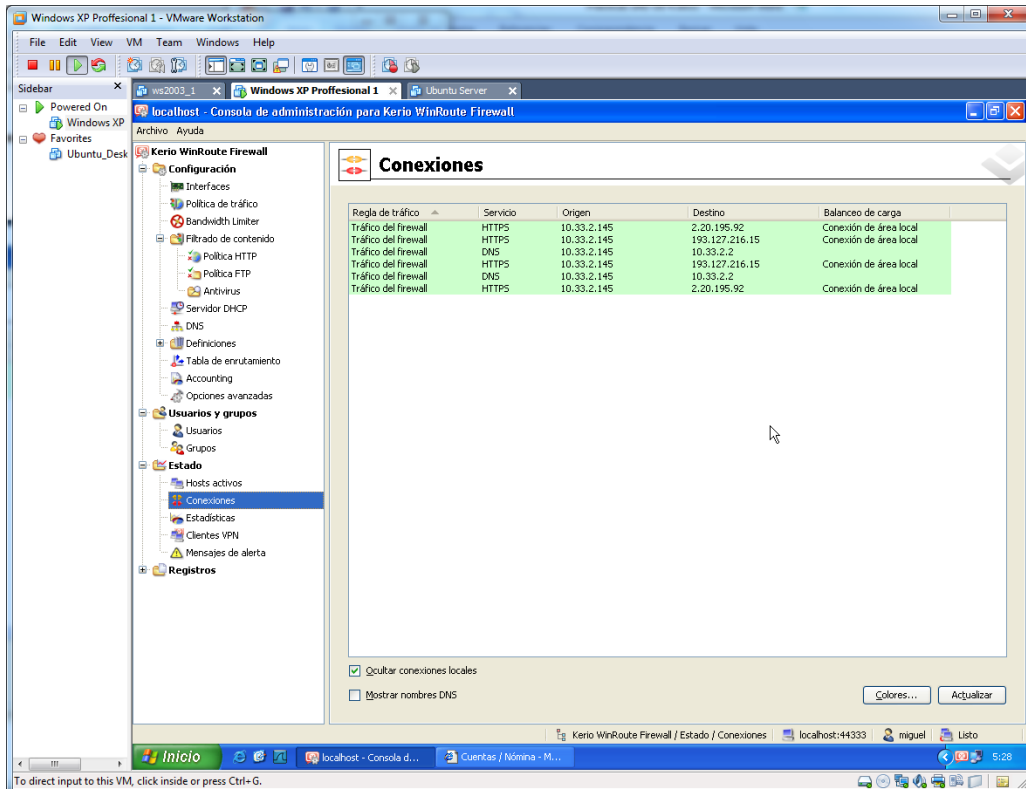
Aquí podemos agregar y configurar usuarios, además de crear respectivos grupos.



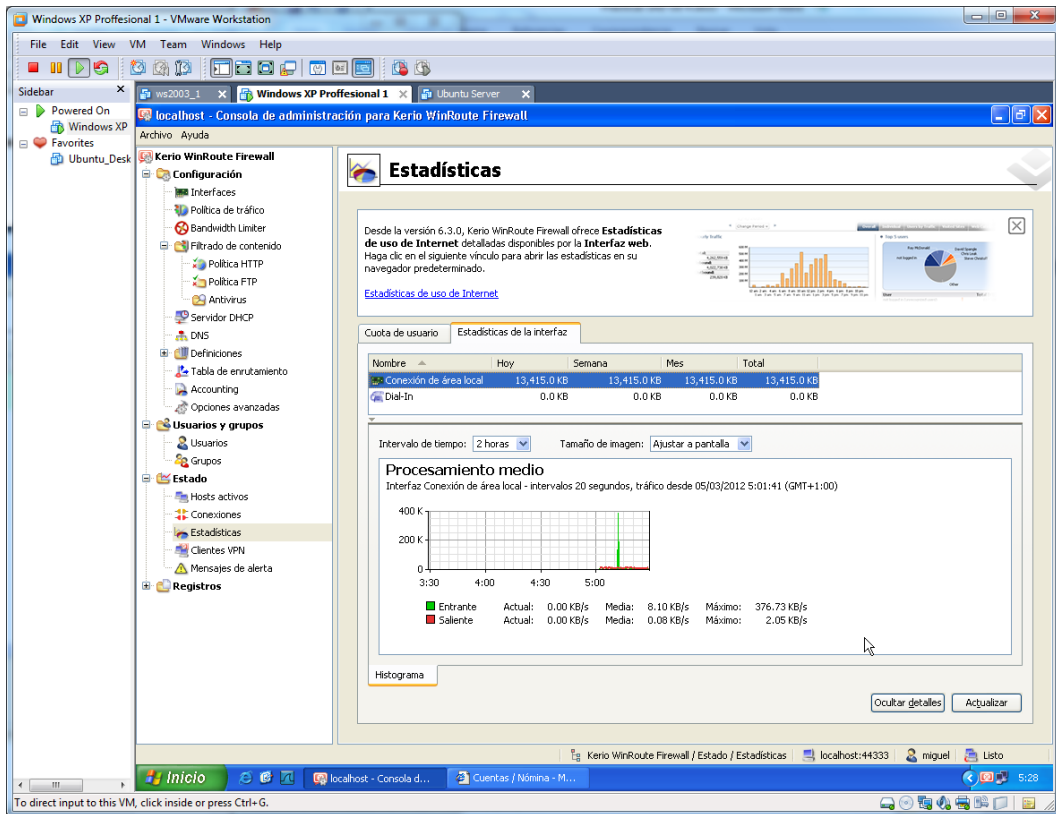
Aquí podemos auditar, los hosts a los que se ha accedido.



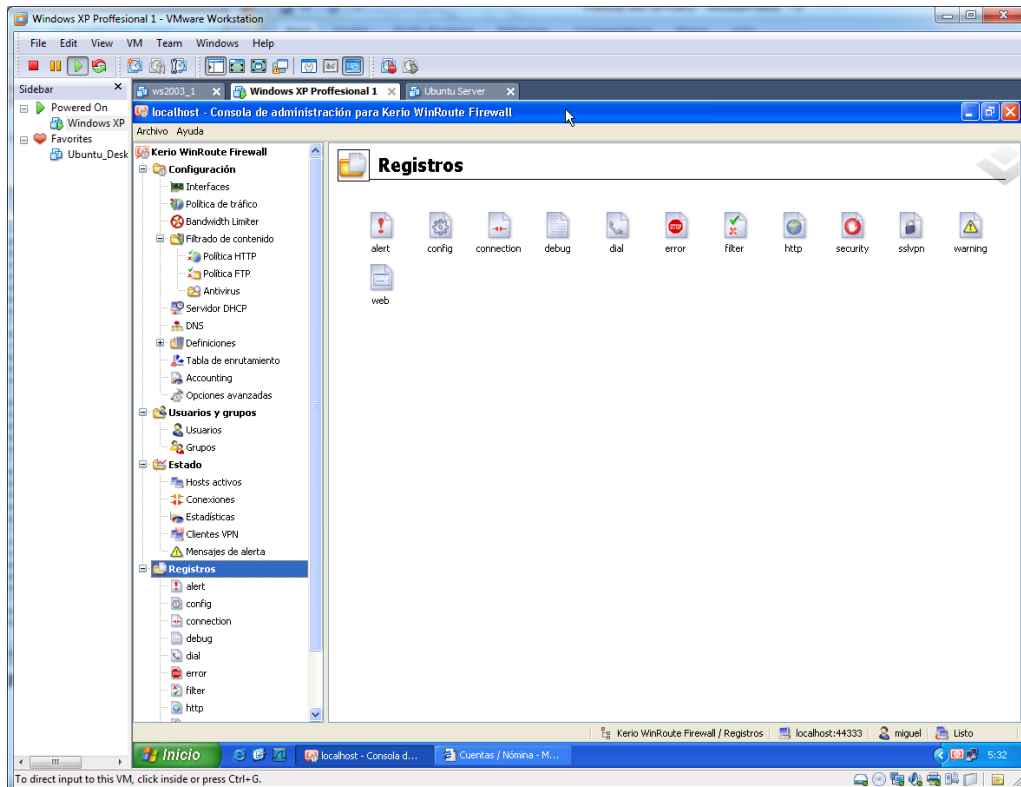
En esta pantalla, podemos auditar las conexiones realizadas entre el exterior y la propia red.



Podemos observar un pequeño gráfico con las estadísticas de procesamiento.



En los registros, el administrador de red, puede consultar diversos informes acerca de diferentes campos, a los que el firewall está controlando.



ii) Elabora un pequeño documento sobre Microsoft ForeFront y su funcionalidad en la empresa:

Microsoft Forefront: ¿Qué es Microsoft Forefront?

Microsoft Forefront es una completa línea de productos de seguridad que permite una mayor protección y control por medio de una excelente integración con su infraestructura de TI actual y una operación más sencilla de implantación, gestión y análisis. La línea de productos de seguridad Microsoft Forefront ofrece protección para las máquinas cliente, aplicaciones de servidor y la red perimetral.

Su completo conjunto de productos de seguridad, que se integran entre sí y con la infraestructura informática de su empresa, puede complementarse e interoperar con soluciones de terceros.

Una completa familia de productos

Microsoft Forefront ofrece una familia de productos de seguridad completa e integrada, que brindan protección para cliente, servidor y perímetro, de modo que su empresa esté a salvo de las amenazas que constantemente van evolucionando:

- Microsoft Forefront Client Security (anteriormente denominada Microsoft Client Protection).
- Microsoft Forefront Server for Exchange Server (anteriormente denominada Microsoft Antigen for Exchange).
- Microsoft Forefront Server for SharePoint® (anteriormente denominada Microsoft Antigen for SharePoint).
- Microsoft Forefront Security for Office Communications Server (anteriormente denominada Antigen for Instant Messaging).
- Microsoft Internet Security and Acceleration (ISA) Server 2006 (Descargue la información de este producto en XPS / PDF)
- Intelligent Application Gateway (IAG) 2007 (Descargue la información de este producto en XPS / PDF)
- Forefront Server Security Management Console.

Funcionalidades y ventajas

Todos ellos ofrecen una serie de funcionalidades y ventajas sobre los productos actuales de la competencia que podemos resumir en:

Protección para sistemas operativos

Forefront ayuda a proteger los sistemas operativos de clientes y servidores. Ofrece detección en tiempo real, programado o a demanda así como eliminación de virus, spyware, rootkits y otras amenazas emergentes.

Protección de aplicaciones de servidores críticas

Forefront ayuda a proteger los servidores de aplicaciones Microsoft a través de una estrategia de defensa en profundidad. ISA 2006 ofrece un sólido control de acceso e inspección de datos específicos de protocolo y de aplicaciones.

Acceso seguro y controlado

Forefront ofrece una amplia gama de tecnologías de firewall, VPN y encriptación, así como funcionalidades de administración de identidades que ayudan a asegurar que sólo los usuarios autorizados tengan acceso a los datos y recursos de TI especificados.

Protección de datos confidenciales

Los productos Forefront resguardan los datos confidenciales y protegen la propiedad intelectual. ISA 2006 proporciona una combinación de filtros específicos para cada aplicación en toda la red, como también tecnologías que garantizan la confidencialidad y autenticidad de los datos valiosos para su empresa.

Integración desde el diseño

Los productos Forefront ofrecen múltiples niveles de integración, de modo que se pueda lograr una mayor eficiencia y control en términos de seguridad de la red.

Integración con aplicaciones

Los productos anti-malware y de seguridad de acceso Microsoft Forefront están especialmente diseñados para proteger e integrarse con aplicaciones de servidores de misión crítica tales como Exchange, Outlook® Web Access y SharePoint.

Integración con la infraestructura informática

Esta infraestructura unificadora permite administrar sin inconvenientes la implementación, distribución, configuración y aplicación de los productos de seguridad, y permite hacerlo con un nivel de control detallado y minucioso.

Integración en Forefront

Los productos Forefront están diseñados para poder operar juntos, de modo que se puedan aprovechar sus funcionalidades y lograr una mayor cobertura de seguridad.

Administración simplificada y centralizada

Los productos Microsoft Forefront están diseñados de forma tal que permiten simplificar la implementación, configuración, administración, generación de informes y análisis. De esta forma, su empresa tiene mayor confiabilidad en cuanto a una excelente protección.

Implementación simplificada

Los utilitarios como ISA Server Best Practices Analyzer Tool y los asistentes de configuración ayudan a establecer una base sólida para una instalación de seguridad contundente. La integración de Forefront con Active Directory y los sistemas de actualizaciones como Systems Management Server proporcionan los cimientos comunes para la administración de configuraciones y cambios. Tanto los usuarios como los administradores se benefician con la distribución centralizada de

configuraciones y políticas actualizadas así como de actualizaciones de sistemas operativos o antivirus para clientes y servidores.

Unificación de generación de informes y análisis

Forefront centraliza la recopilación y el análisis de la información de administración de seguridad, dado que toda la información de seguridad se almacena en un único repositorio SQL Server™, que puede utilizar los servicios de generación de informes y análisis (SQL Server Reporting and Análisis Services) para identificar e interpretar los eventos de seguridad.

Administración simplificada

La administración y la generación de informes de seguridad están centralizadas en Forefront. Sus componentes se integran plenamente con los sistemas de administración existentes, incluyendo Microsoft Operations Manager, Microsoft Systems Management Server y Windows Server™ Update Services. Las consolas de administración integradas de Forefront ofrecen las conocidas interfaces de Microsoft y son, además, fáciles de utilizar; por otra parte, reducen el tiempo de capacitación necesaria y ayudan a controlar los costes.

Énfasis en la capacidad de "aseguramiento"

Al concentrar gran parte de sus esfuerzos en los aspectos relacionados con la integración y la administración de la seguridad –el "aseguramiento" de la infraestructura-, Forefront ayuda a su empresa a:

- Centralizar la administración de la seguridad.
- Evitar los errores en la configuración.
- Implementar la seguridad en toda la red.
- Obtener una visión unificada de la seguridad de la red.

Conclusión

En conclusión, nos encontramos ante una familia de productos que, tanto juntos como de manera independiente, nos ofrecen una solución:

Completa

A medida que los ataques aumentan, se tornan cada vez más costosos para su empresa, aumentando el tiempo de reposo necesario, la recuperación e impactando en forma negativa en la productividad y en la utilización de su software.

Integrada

En general, los productos de seguridad no se integran mucho entre sí ni con la infraestructura de TI existente de uno. Esta falta de sinergia en la infraestructura actual hace que sea más difícil de controlar, creando potencialmente brechas e ineficiencias en la seguridad de su red.

Microsoft Forefront integra capacidades de seguridad en toda la línea de productos, con aplicaciones de servidor Microsoft y con su infraestructura de TI existente, de modo que usted puede lograr mayor eficiencia y control sobre la seguridad de su red.

Simplificada

Puede ser difícil obtener visibilidad crítica acerca del estado de seguridad de su red, especialmente sin una herramienta de administración central. Sin este tipo de visibilidad, implementar y administrar la seguridad es más difícil, ineficiente, propicia al error y consume más tiempo.

Microsoft Forefront mejora su capacidad para mantener la seguridad de su organización al simplificar la administración, instalación y uso de los productos de seguridad, con lo que aumentará su confianza en que su organización está bien protegida.

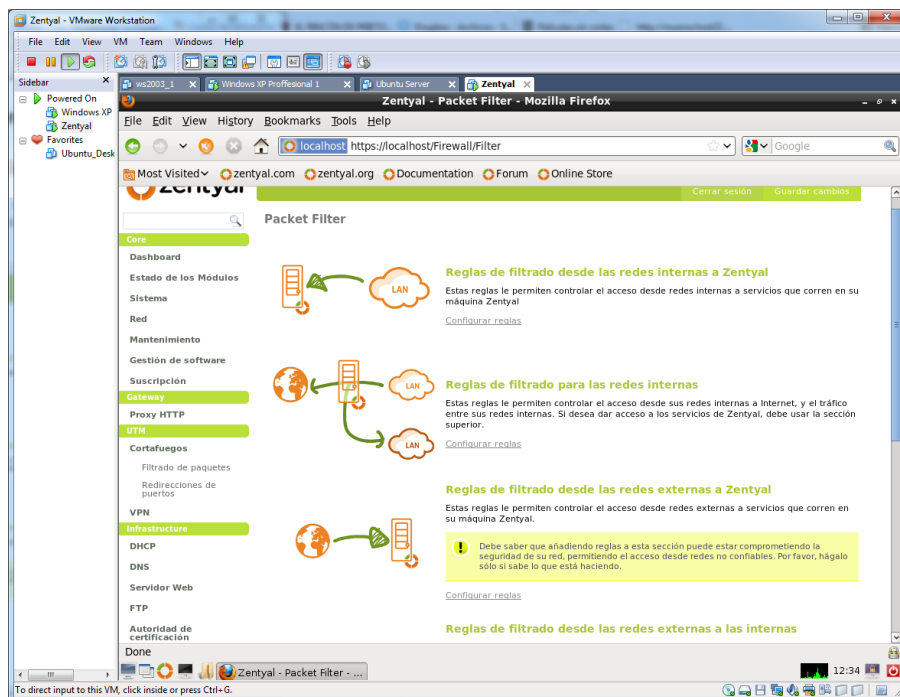
Forefront aumenta la visibilidad en el estado de seguridad de su red al brindar una vista individual de la red, permitiendo una administración y una mitigación de amenazas mejor y más informadas.

<http://www.microsoft.com/business/es-es/content/paginas/article.aspx?cbcid=225>

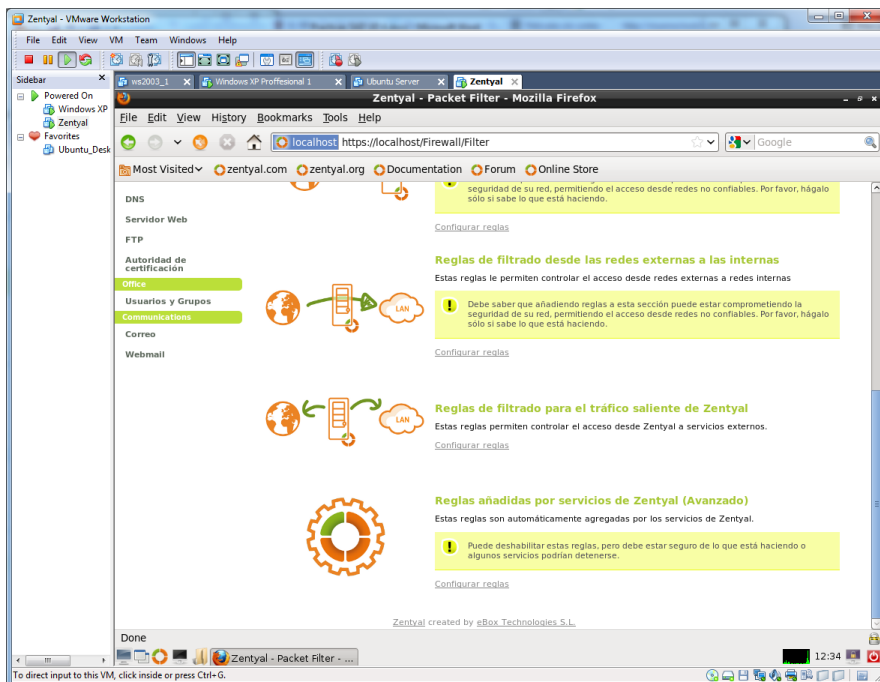
b) Distribuciones libres para implementar cortafuegos en máquinas dedicadas.

i) Instalación y configuración del cortafuegos “Firewall Zentyal”.

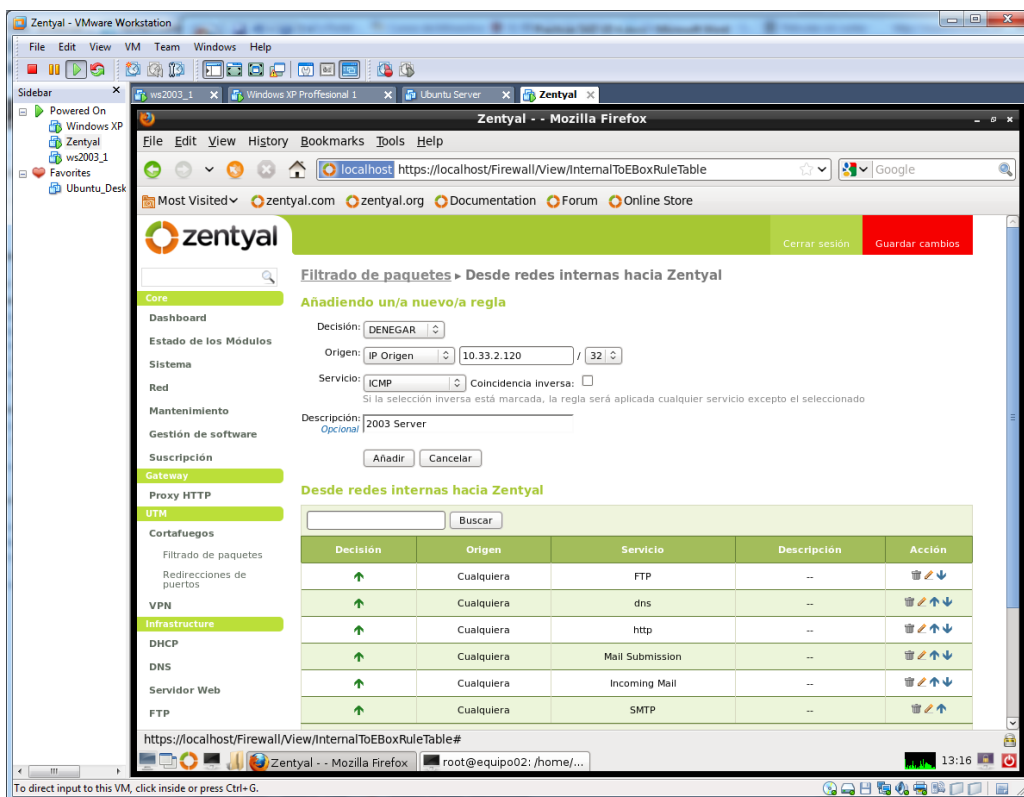
Tenemos el cortafuegos instalado por defecto en nuestro sistema, si nos situamos en cortafuegos, podemos configurar los siguientes escenarios.



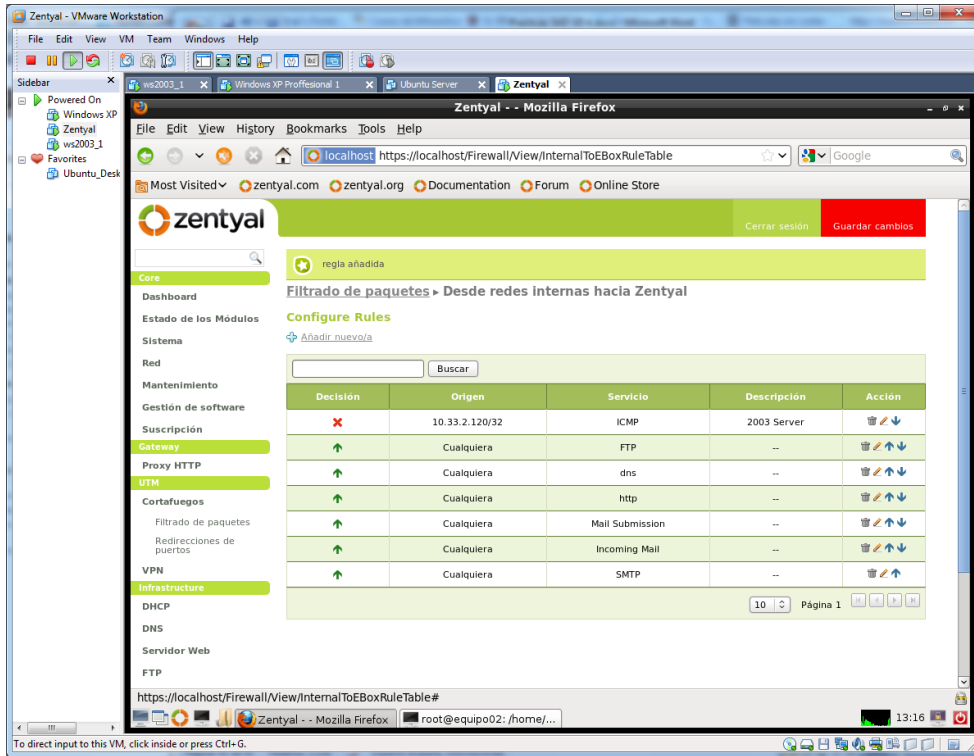
O en cambio éstos otros.



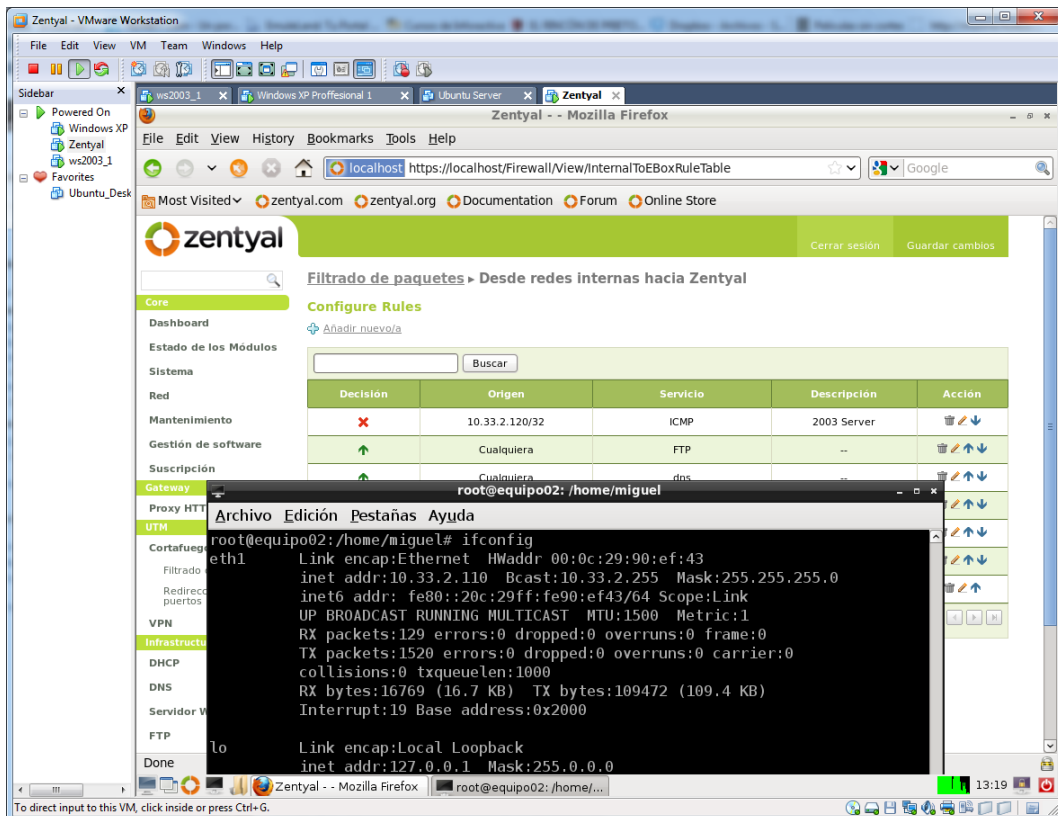
Escogemos la primera opción, ya que vamos a denegar un servicio a un PC de nuestra LAN para comprobar el resultado de nuestro cortafuegos.



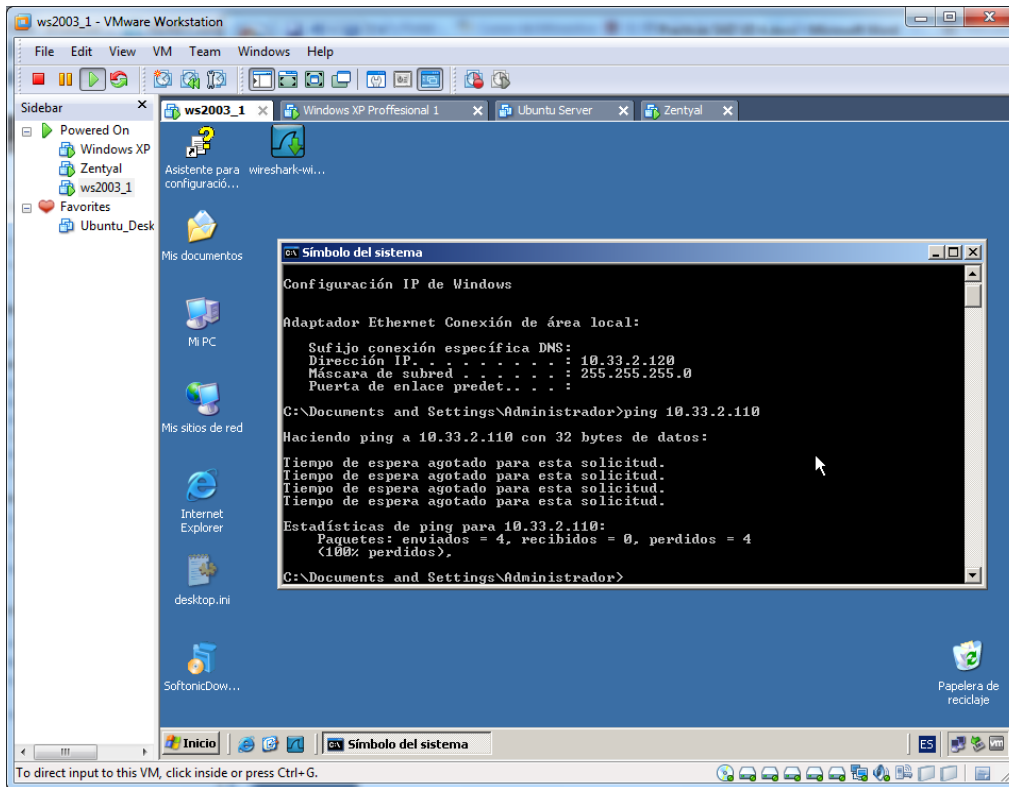
Una vez configurado guardamos los cambios. Hemos denegado el protocolo ICMP para el equipo 10.33.2.120.



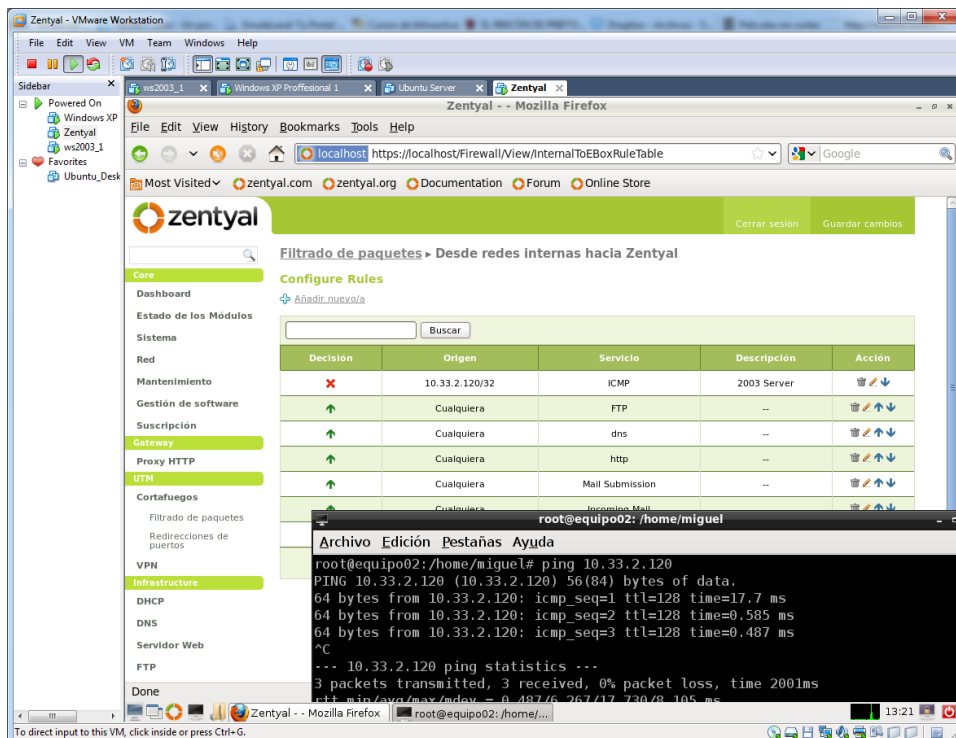
Comprobamos nuestra IP de Zentyal.



Comprobamos la IP del cliente denegado, y comprobamos que no puede conectar con el Zentyal, por el cortafuegos.

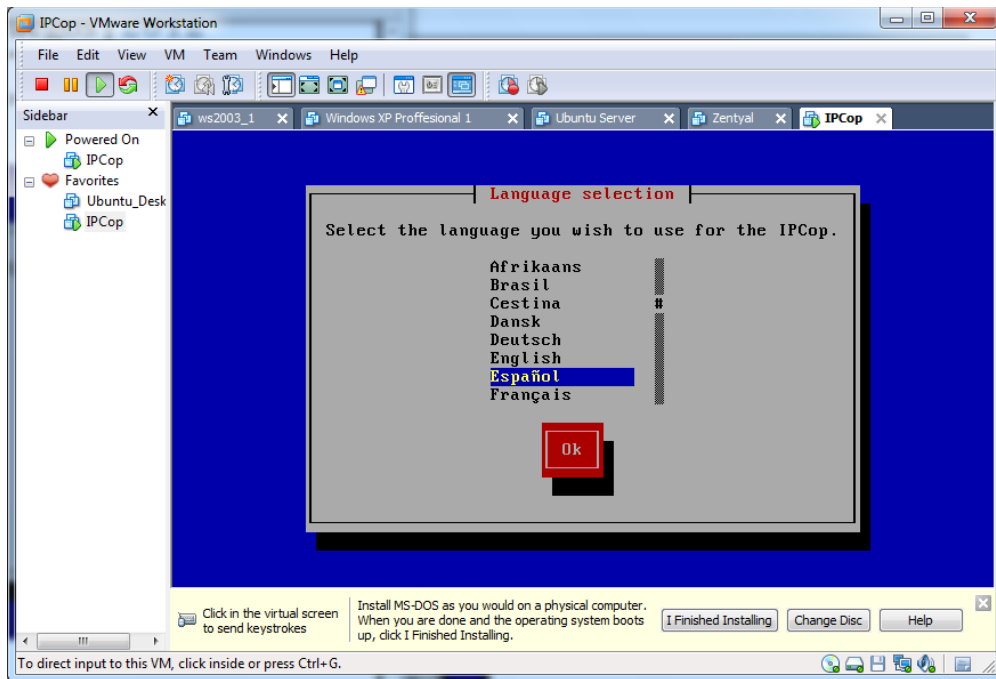


Sin embargo, a la inversa sí que podemos.

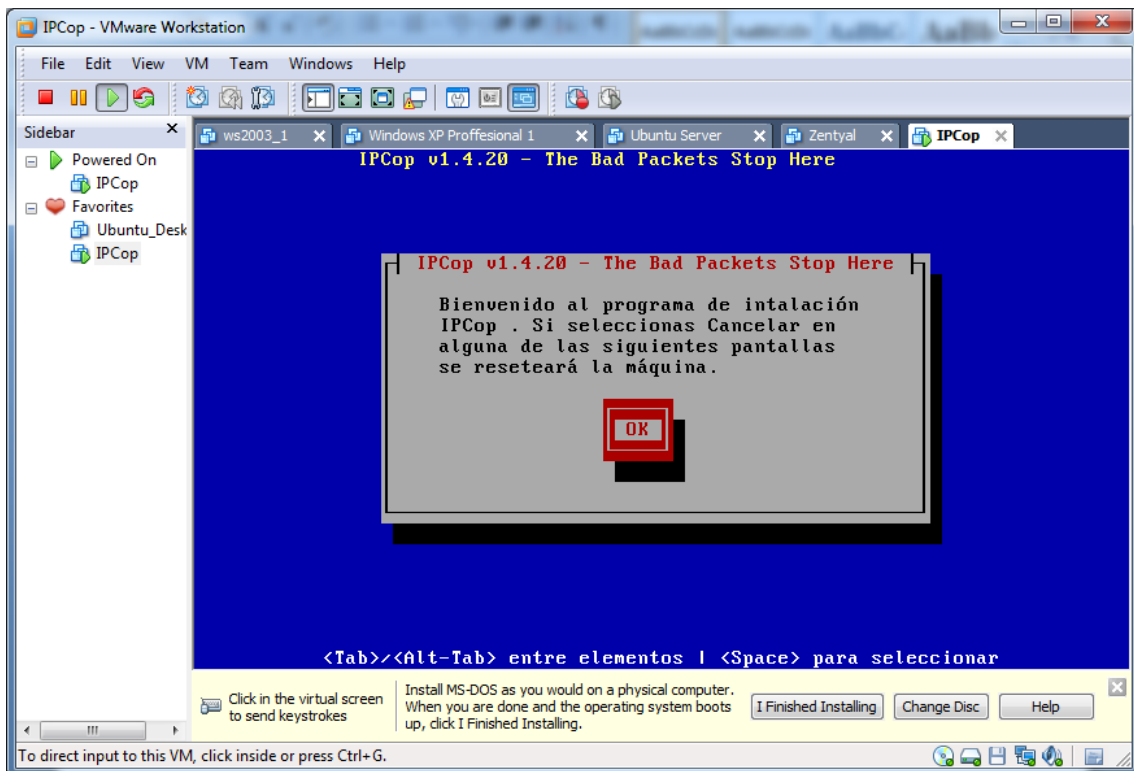


ii) Instalación y configuración del cortafuegos “Firewall IpCop”.

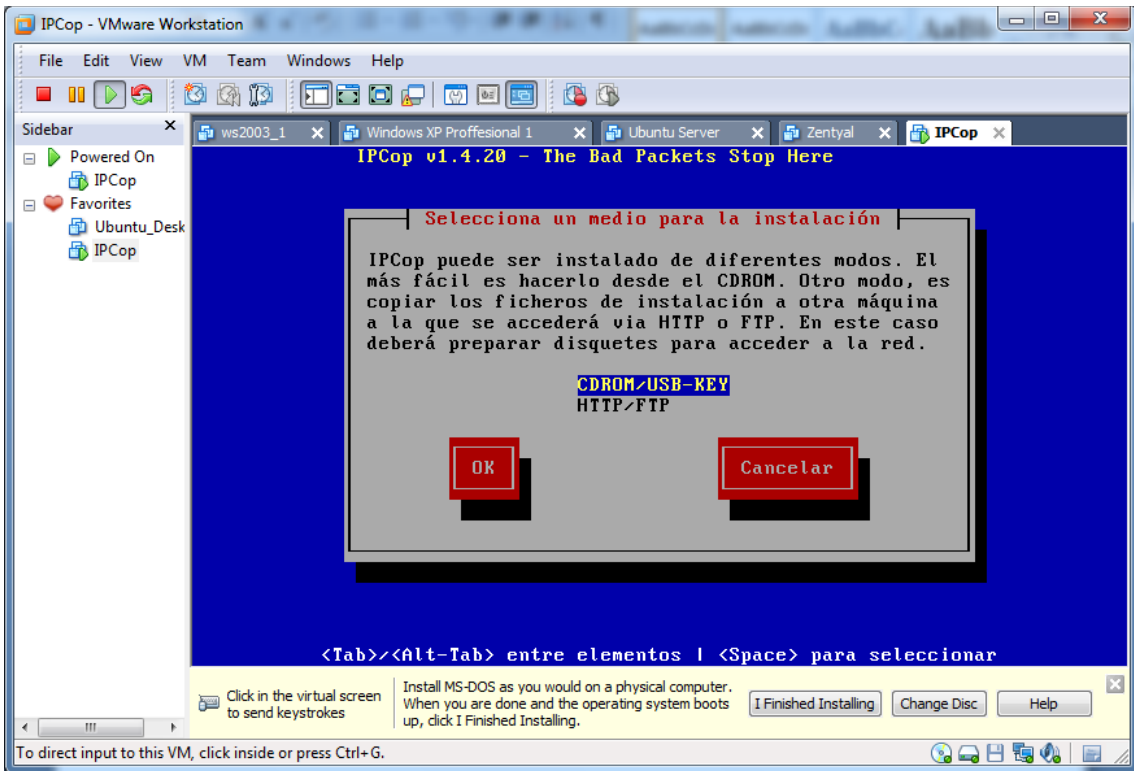
Introducimos la ISO de la aplicación, y arrancamos la máquina virtual, una vez arrancado, procedemos a instalarlo en nuestro idioma.



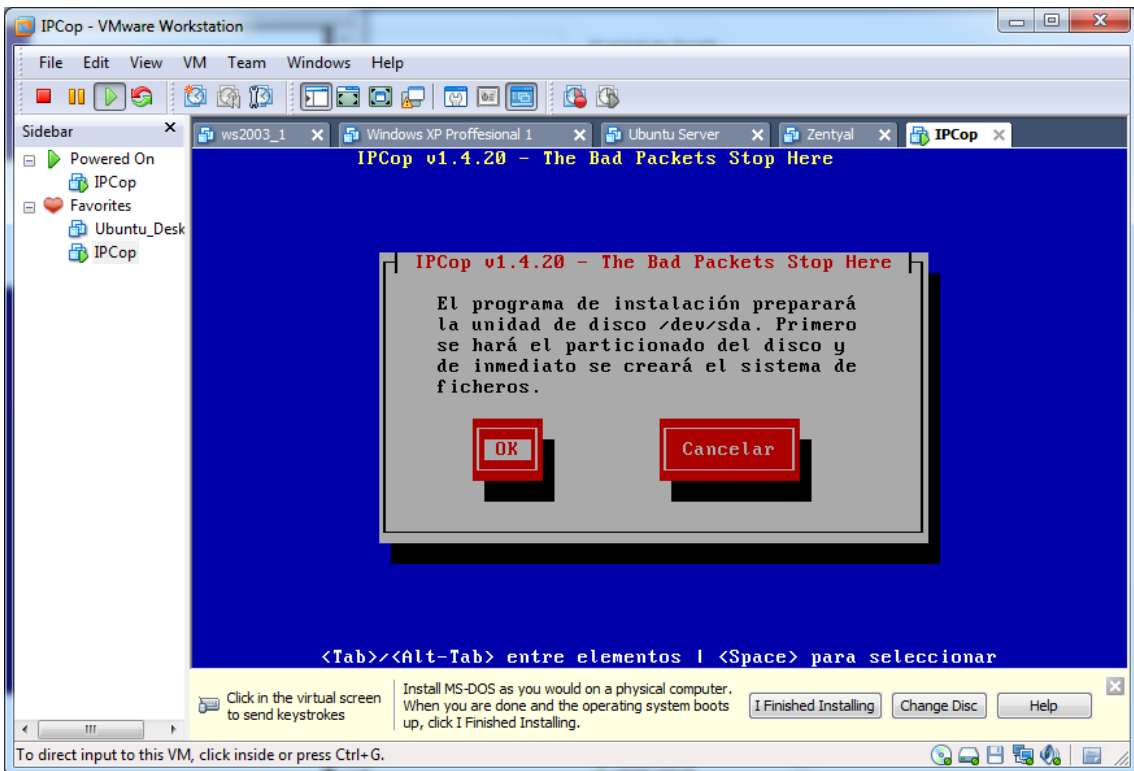
Confirmamos el siguiente mensaje.



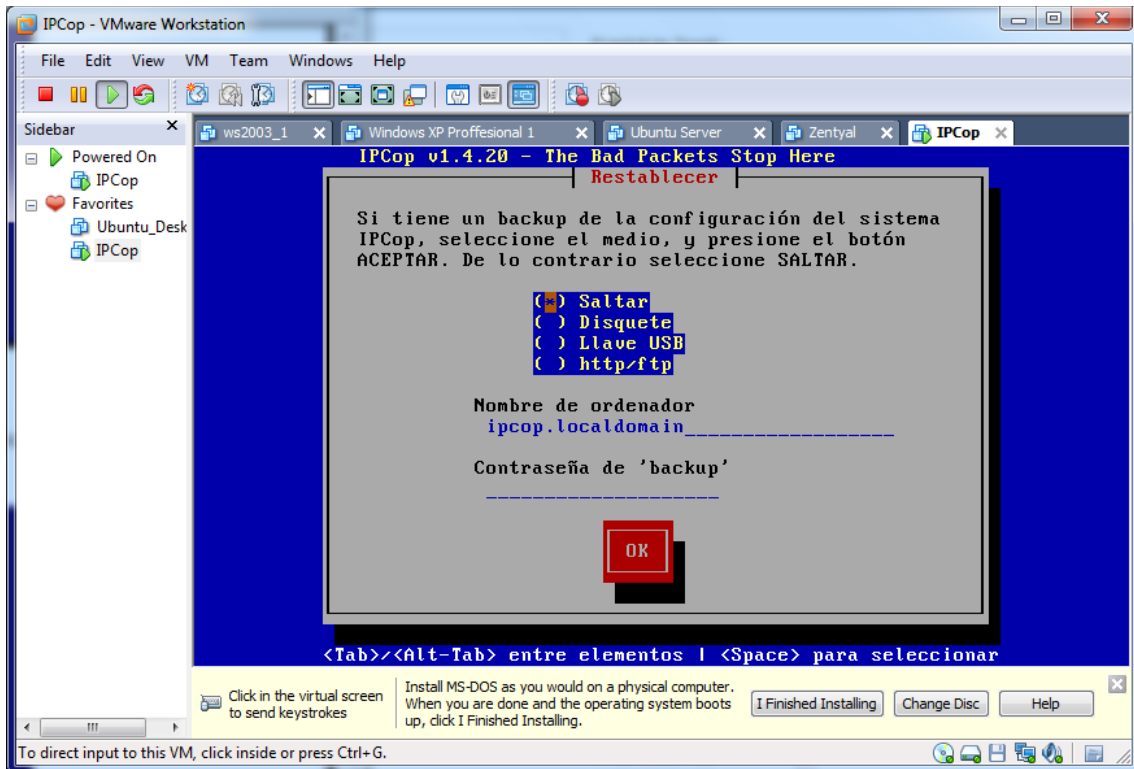
Elegimos instarlo desde la primera opción.



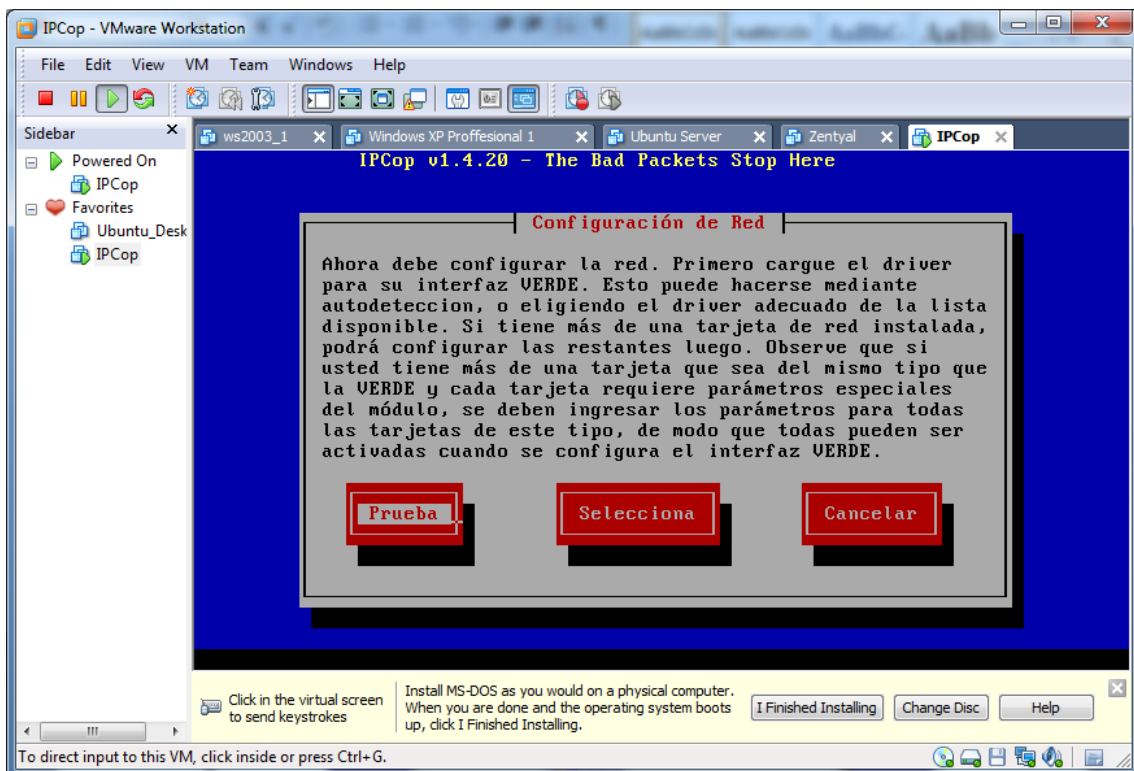
Nos indica el disco donde se llevara a cabo la instalación, que en este caso es /dev/sda



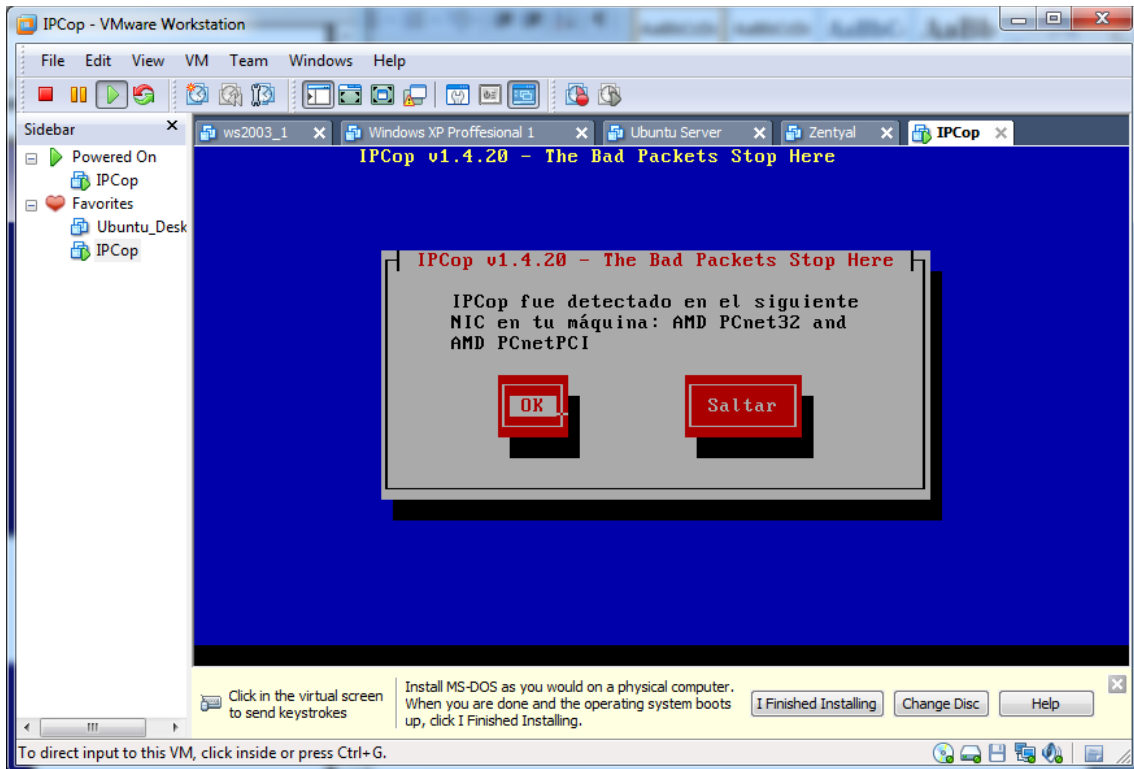
Nos saltamos el proceso de backup.



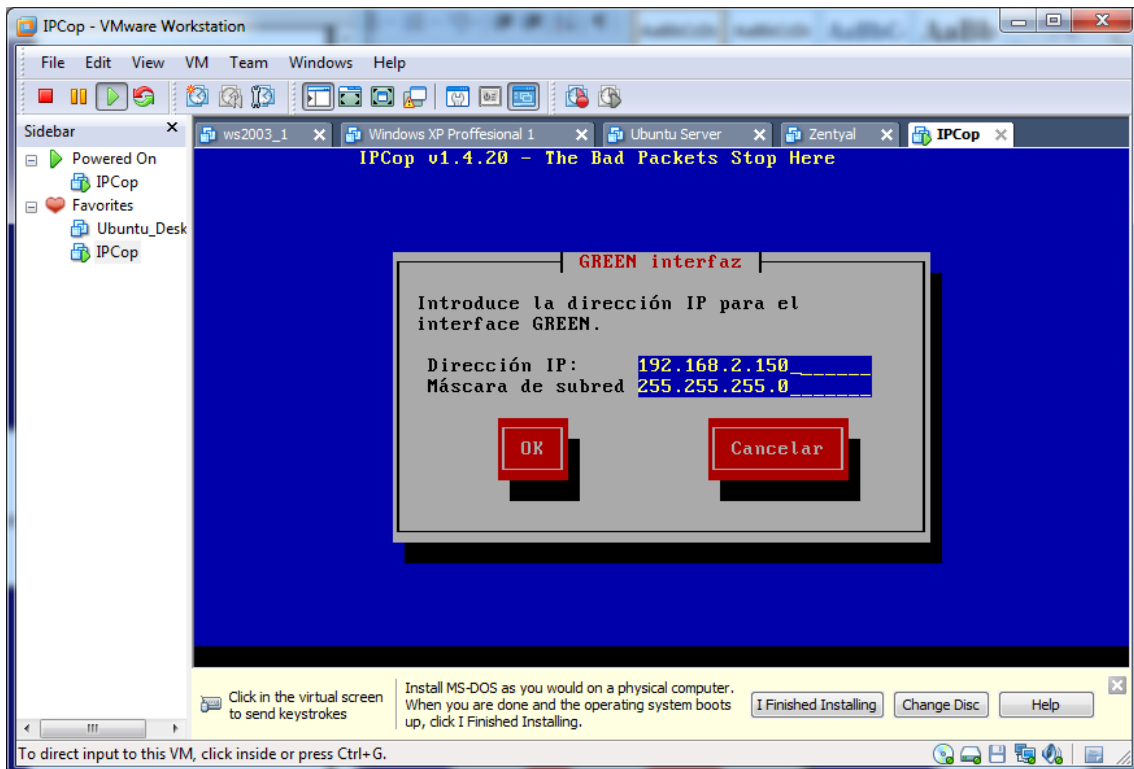
Comprobamos nuestras tarjetas, con la opción **prueba**.



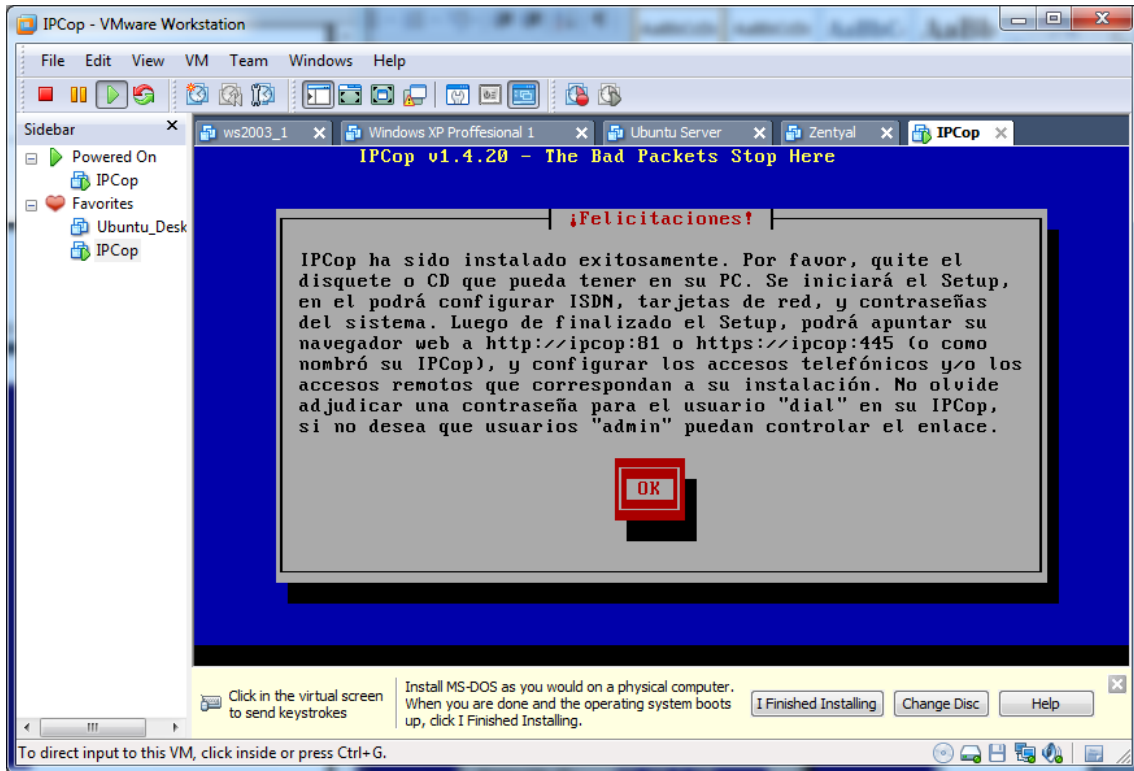
Una vez nos detecte las tarjetas de red, aceptamos.



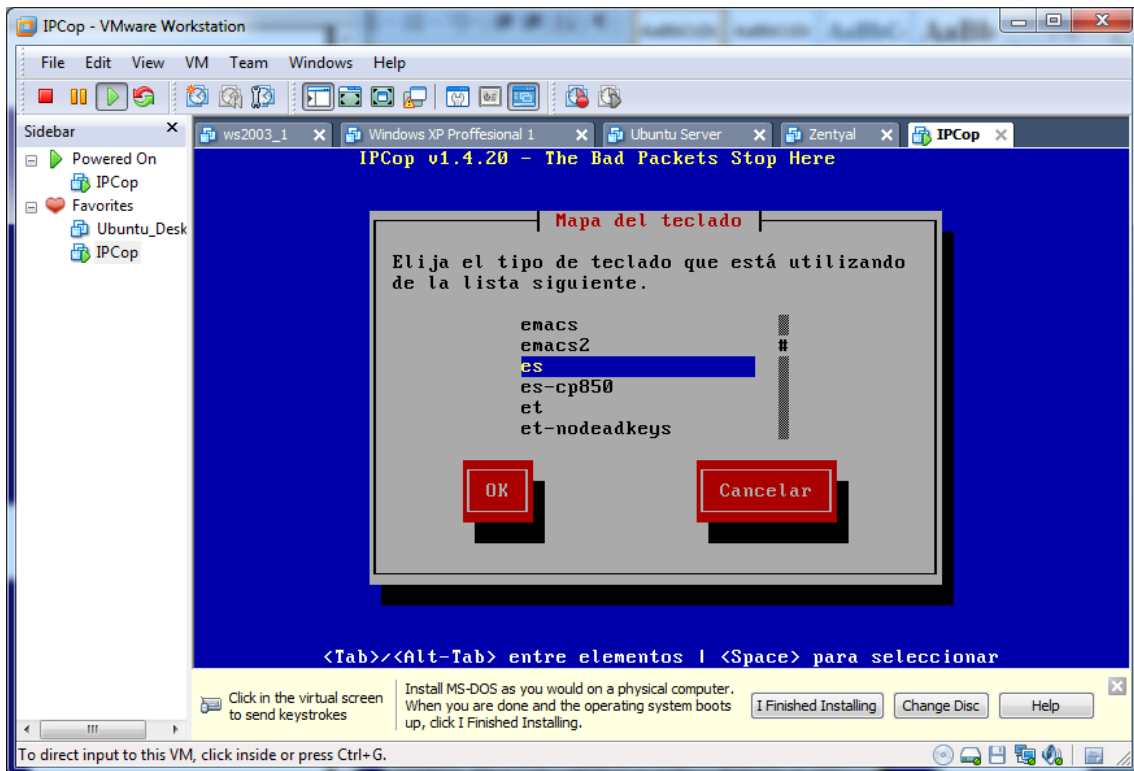
Elegimos la primera interfaz, que será **green**, y configuramos la direcciones IP de la siguiente manera.



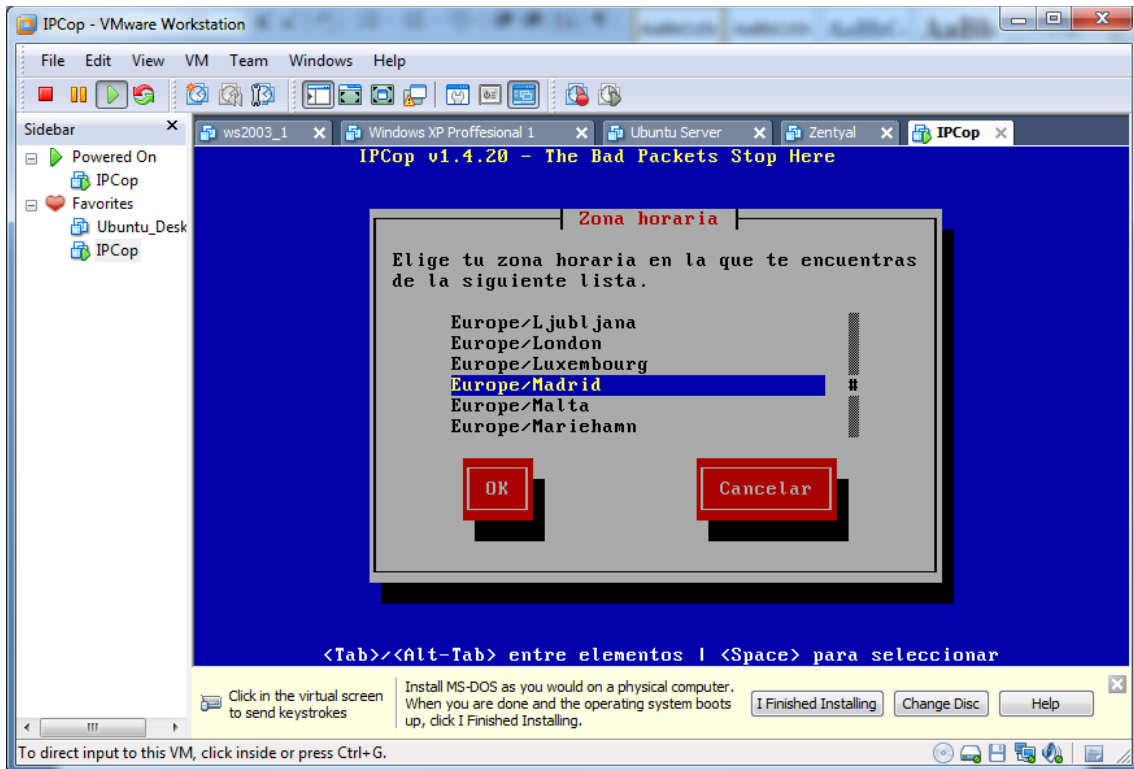
Una vez las tengamos pulsamos OK.



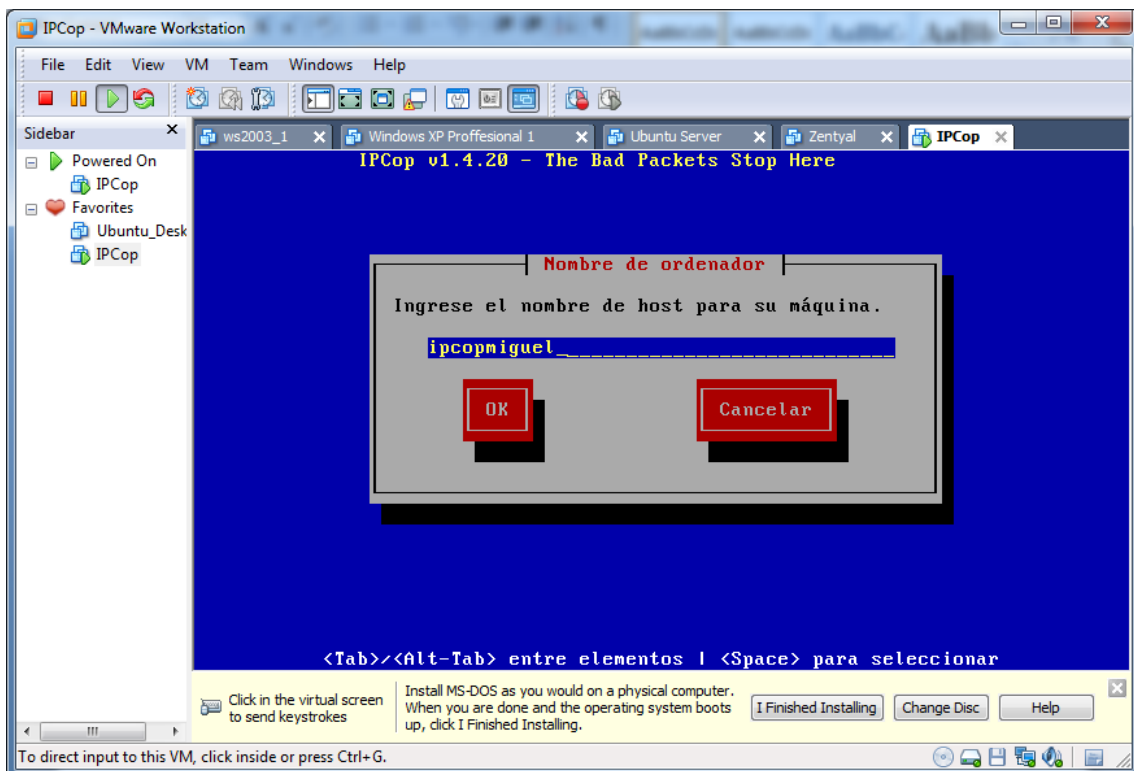
Elegimos nuestro mapa de teclado, que es en nuestro caso es.



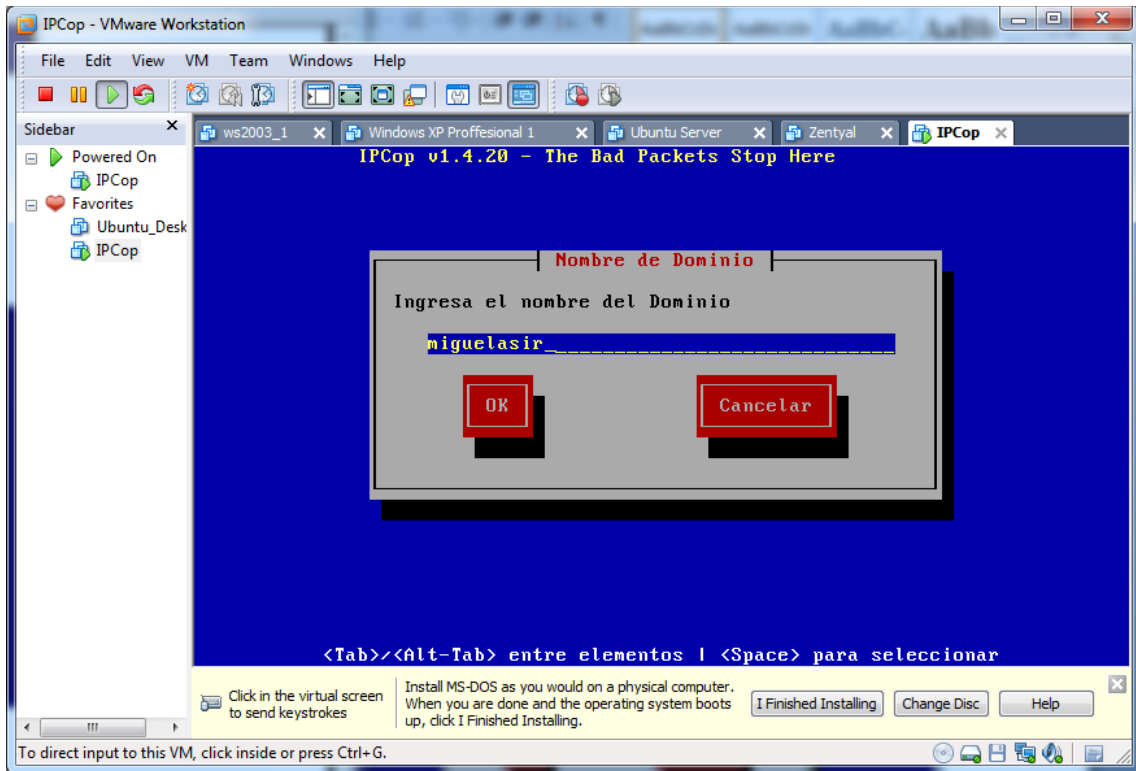
Elegimos nuestra zona horaria, **Europe/Madrid**



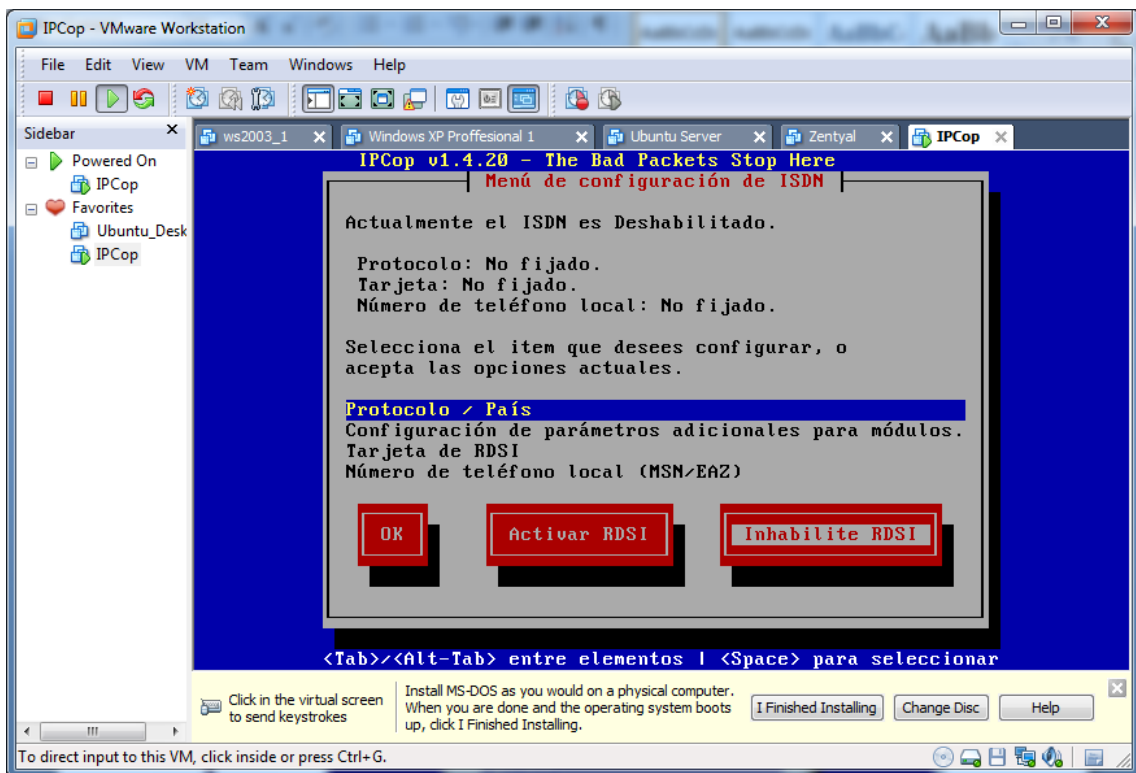
Introducimos el nombre de la máquina, **ipcopmiguel**



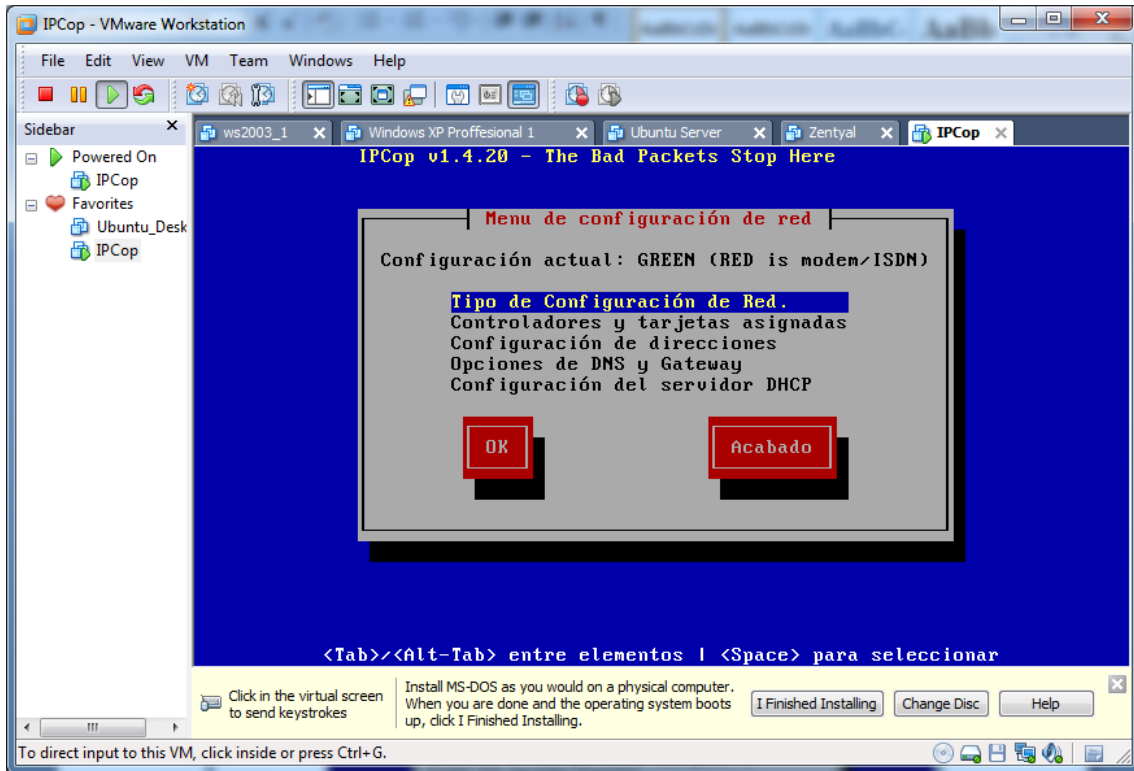
Ingresamos el nombre de nuestro dominio, **miguelasir**.



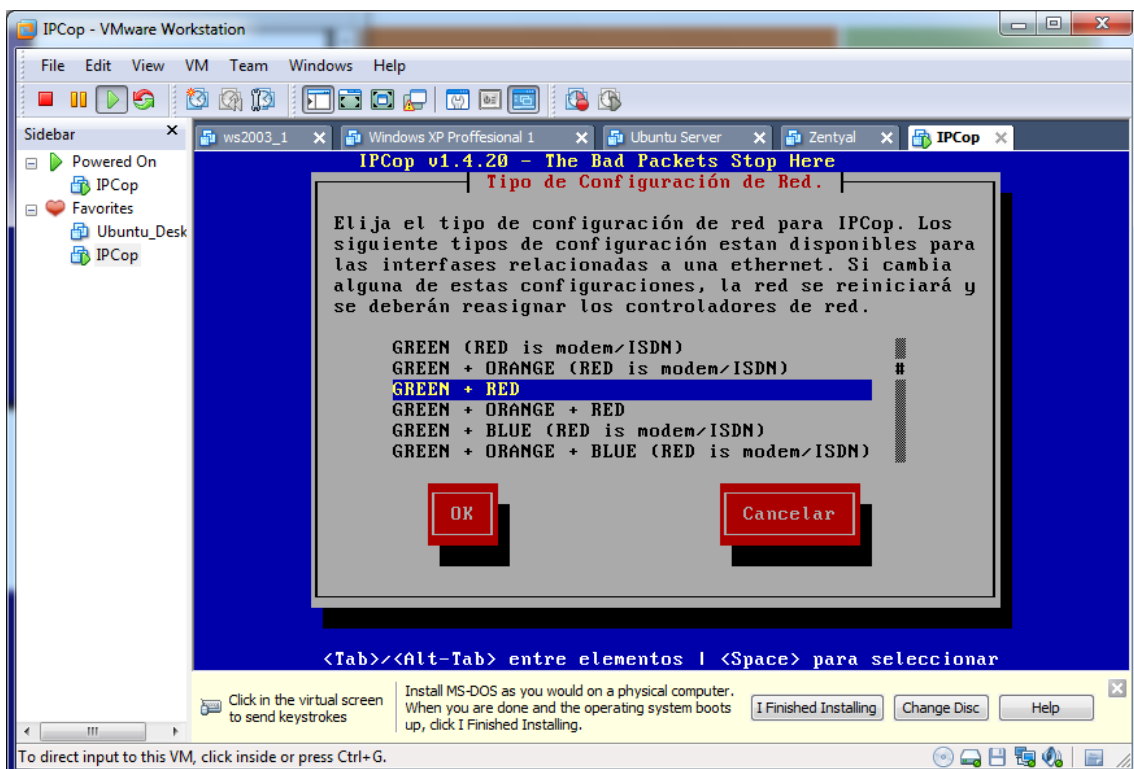
Inhabilitamos la configuración de RDSI.



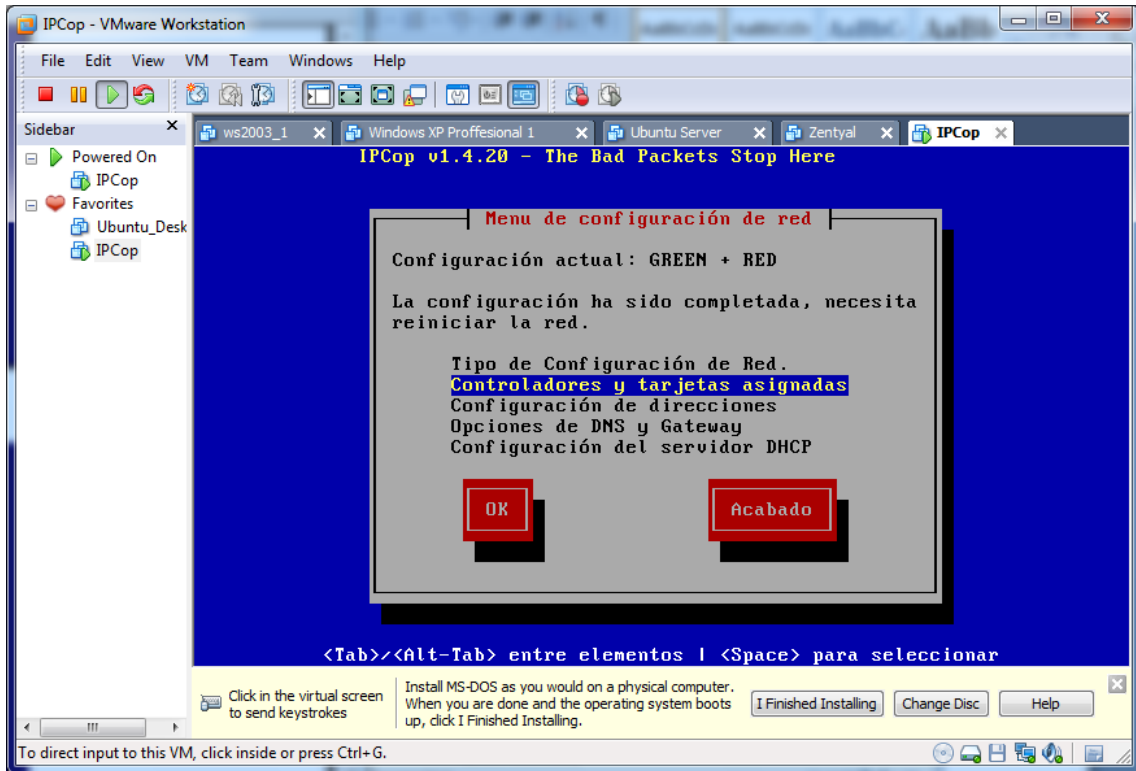
Una vez realizados los pasos anteriores, accedemos a este menú de configuración, que configuramos uno a uno.



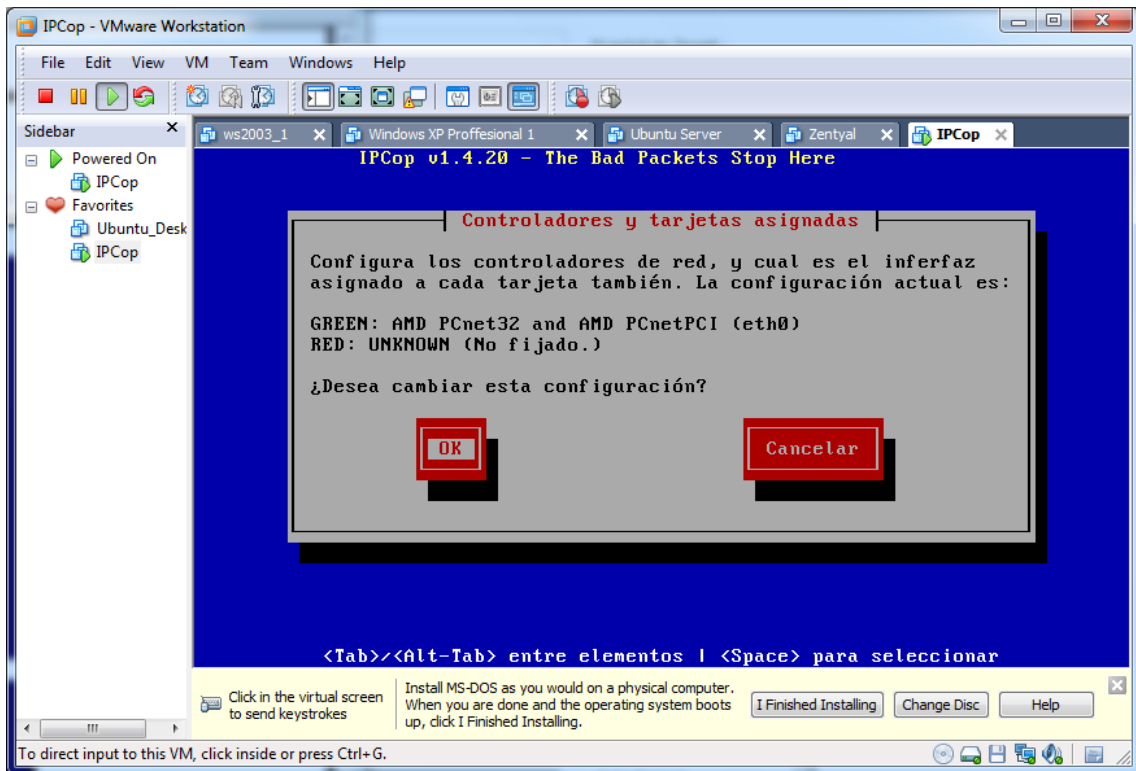
Elegimos el tipo de configuración **GREEN + RED**, que corresponden a nuestras 2 tarjetas de red instaladas en la máquina.



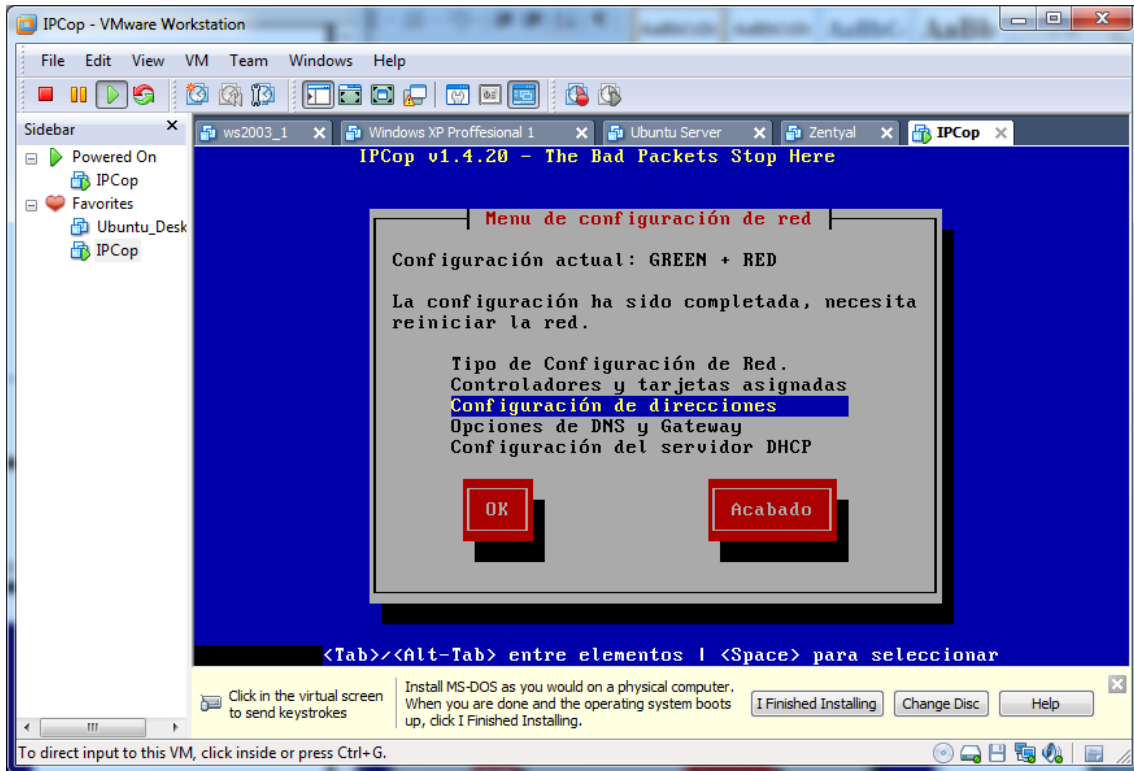
Pulsamos la opción controladores y tarjetas asignadas.



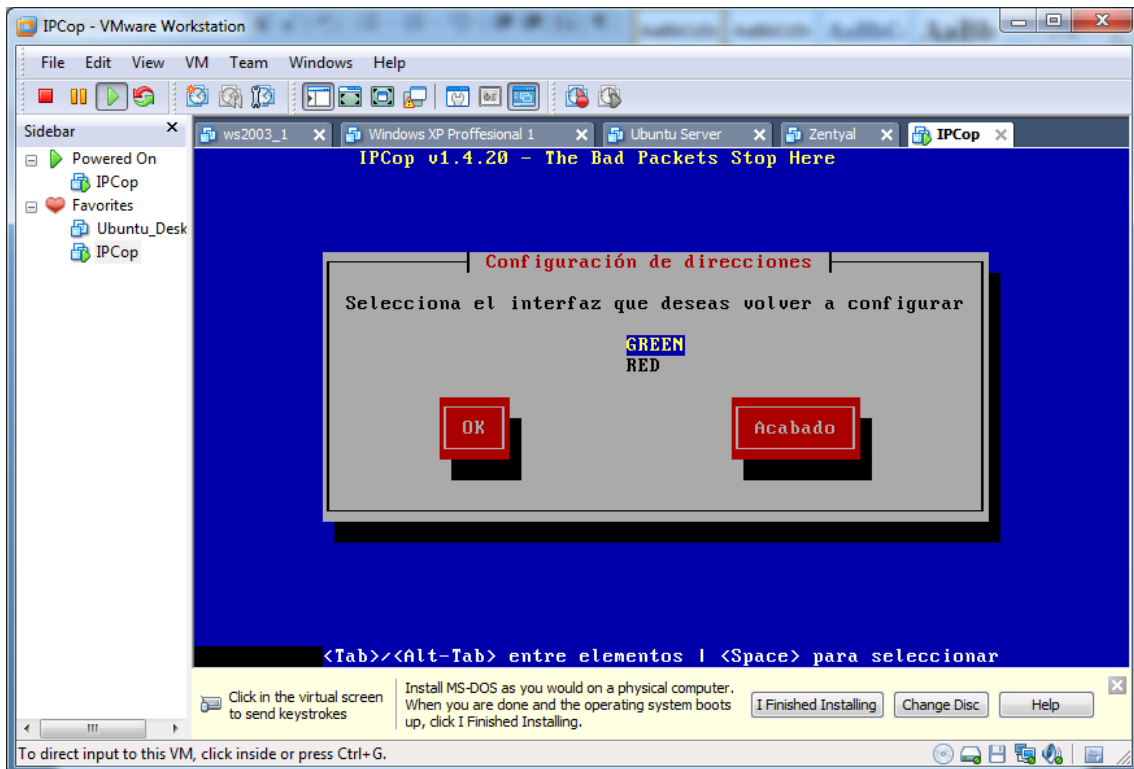
Pulsamos OK para habilitar la segunda tarjeta de red, RED.



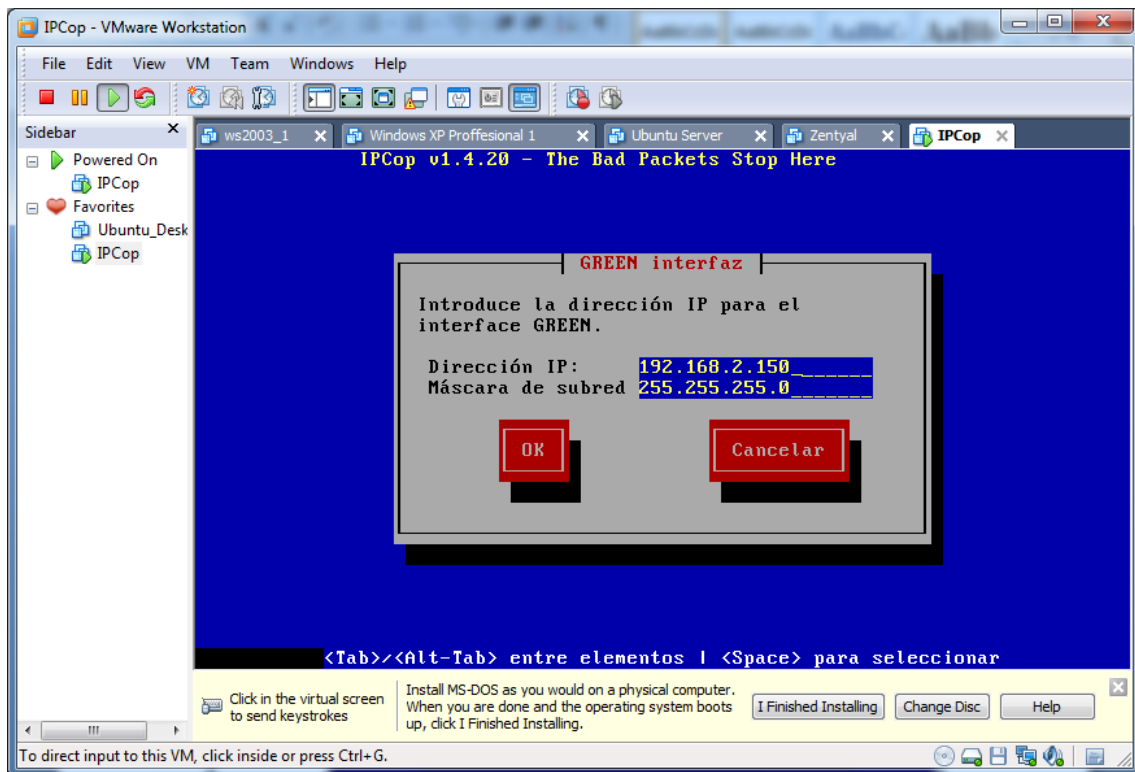
Configuramos las direcciones de nuestra tarjeta.



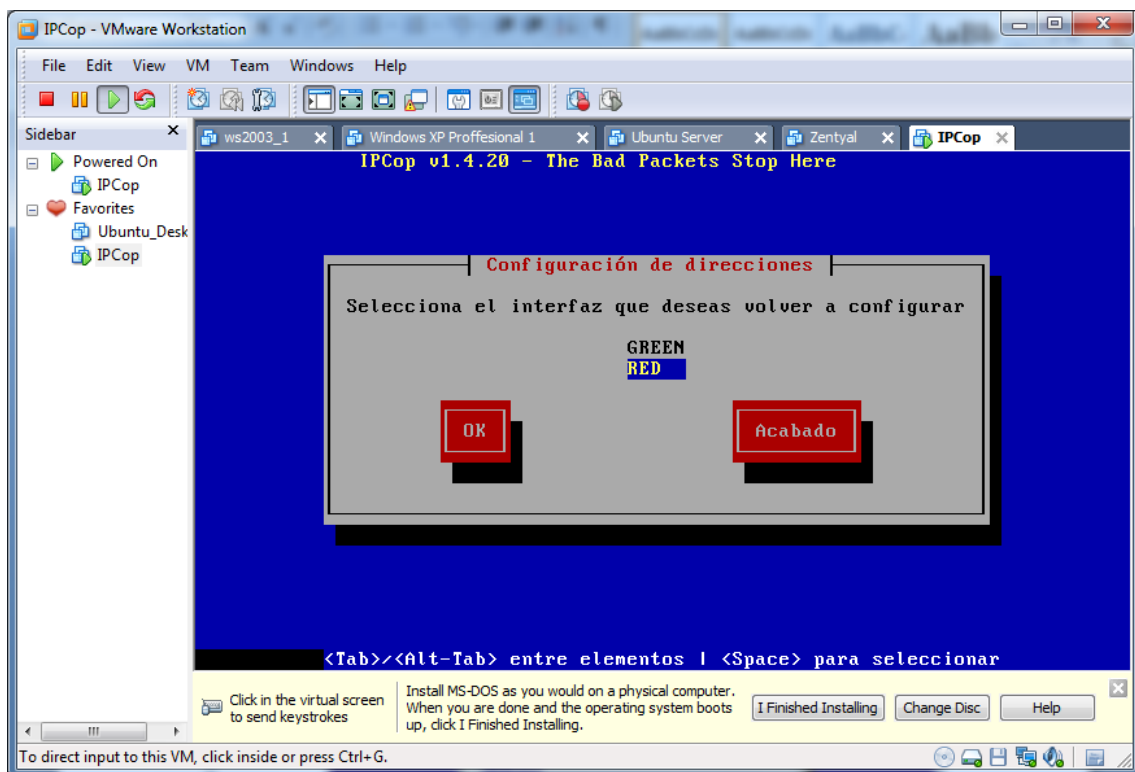
Elegimos la interfaz **GREEN** o tarjeta número 1.



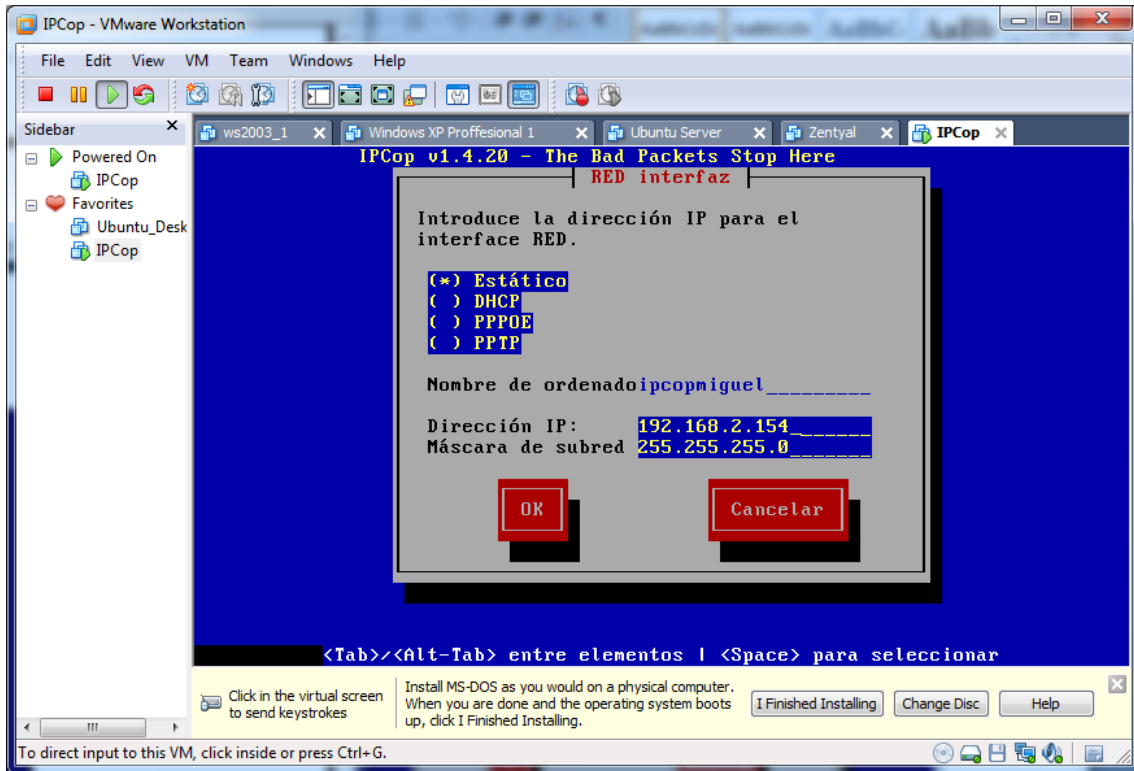
Establecemos las direcciones IP si no las tuviéramos, pero ya las hemos configurado anteriormente.



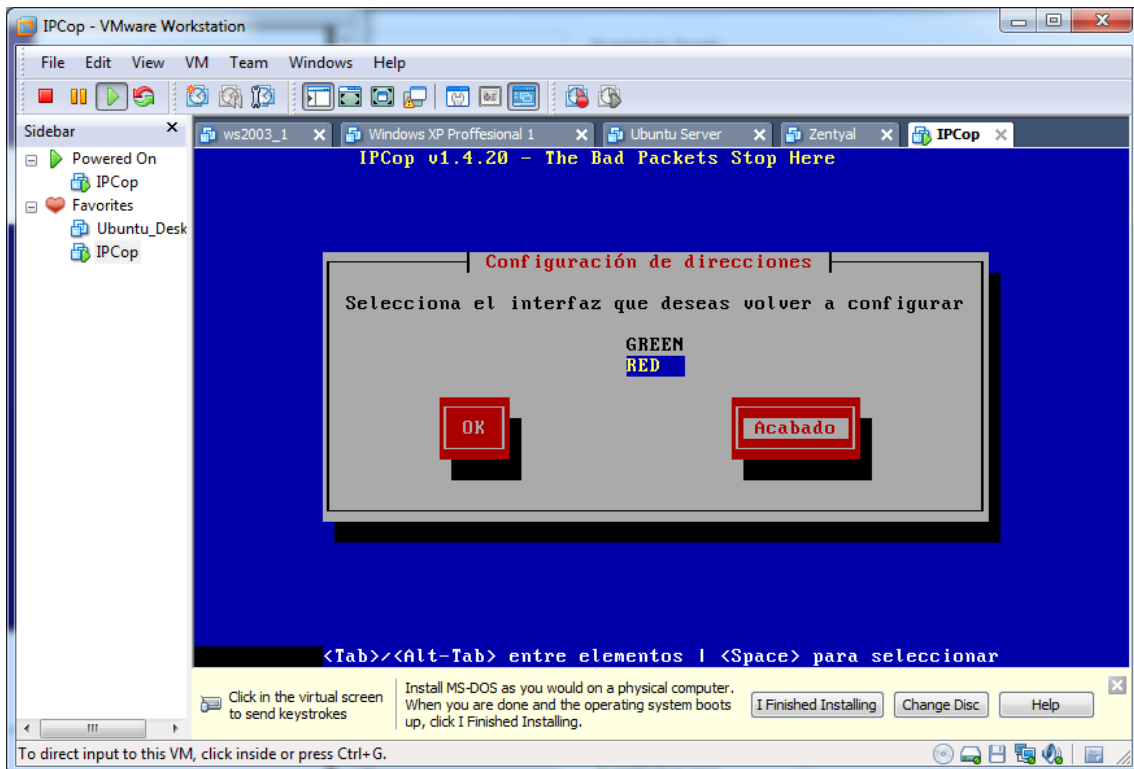
Elegimos la interfaz RED o tarjeta número 2.



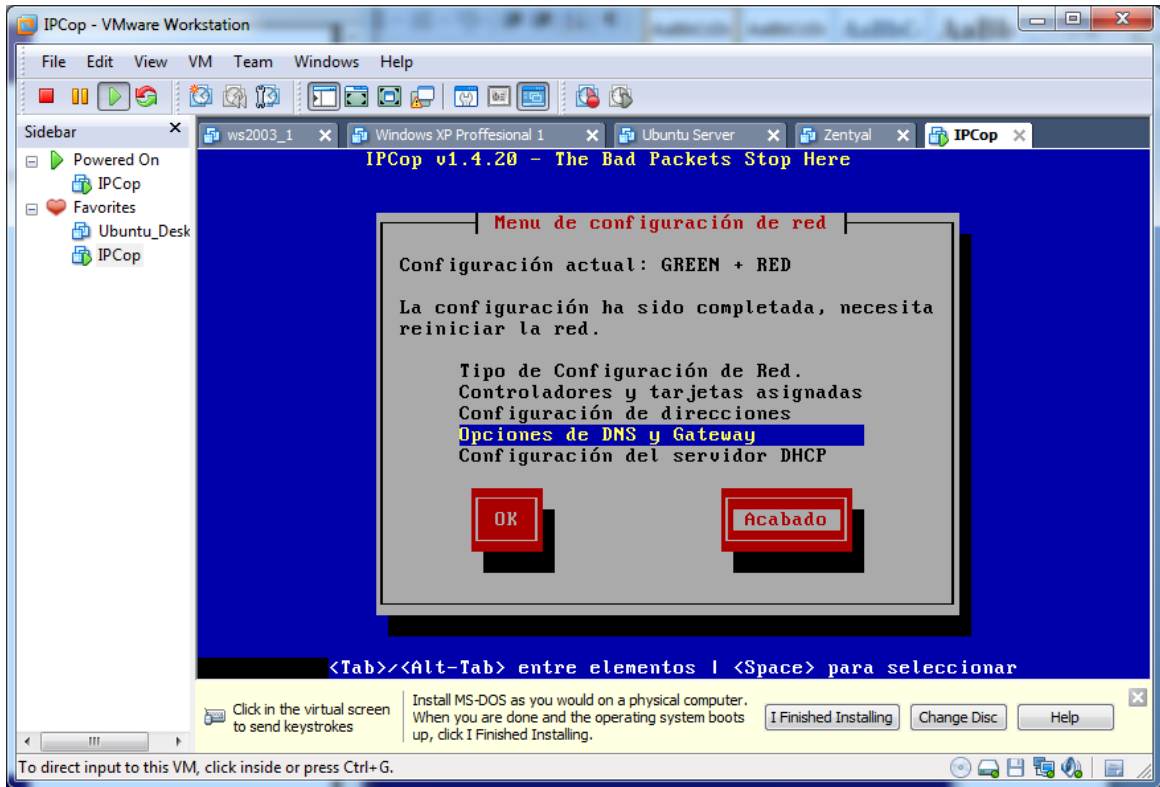
Establecemos la dirección IP de esta interfaz.



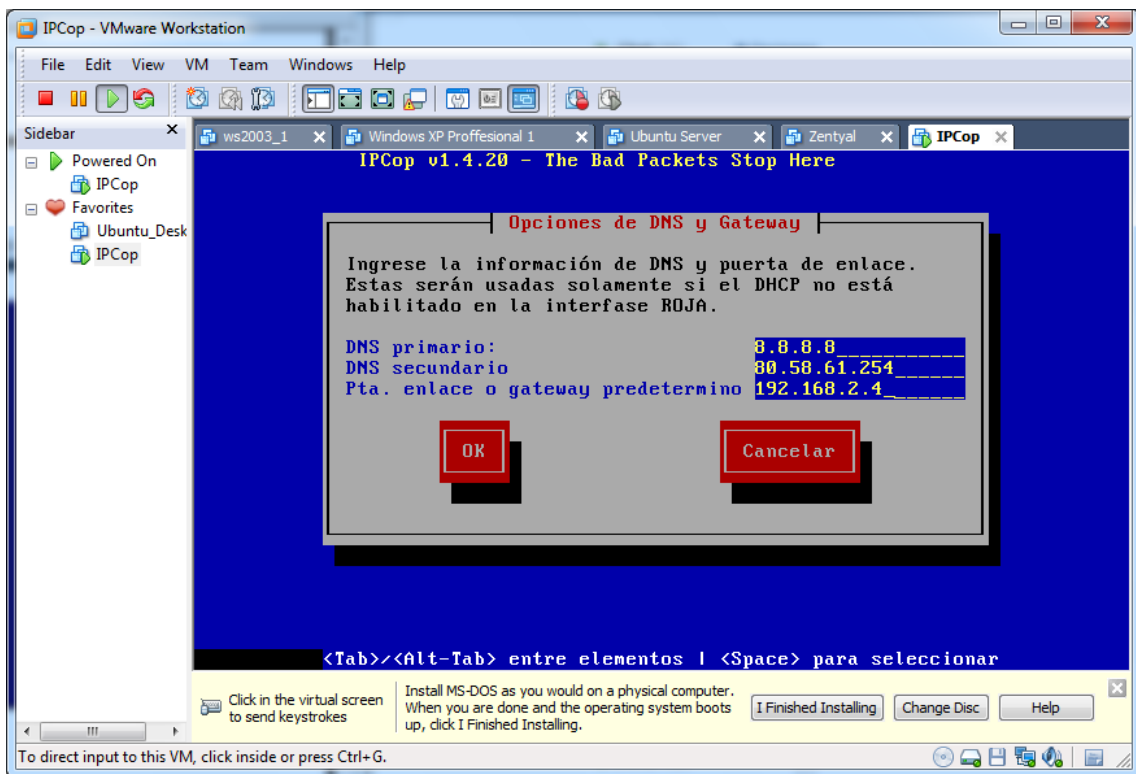
Como ya hemos configurado las dos interfaces, acabamos el proceso.



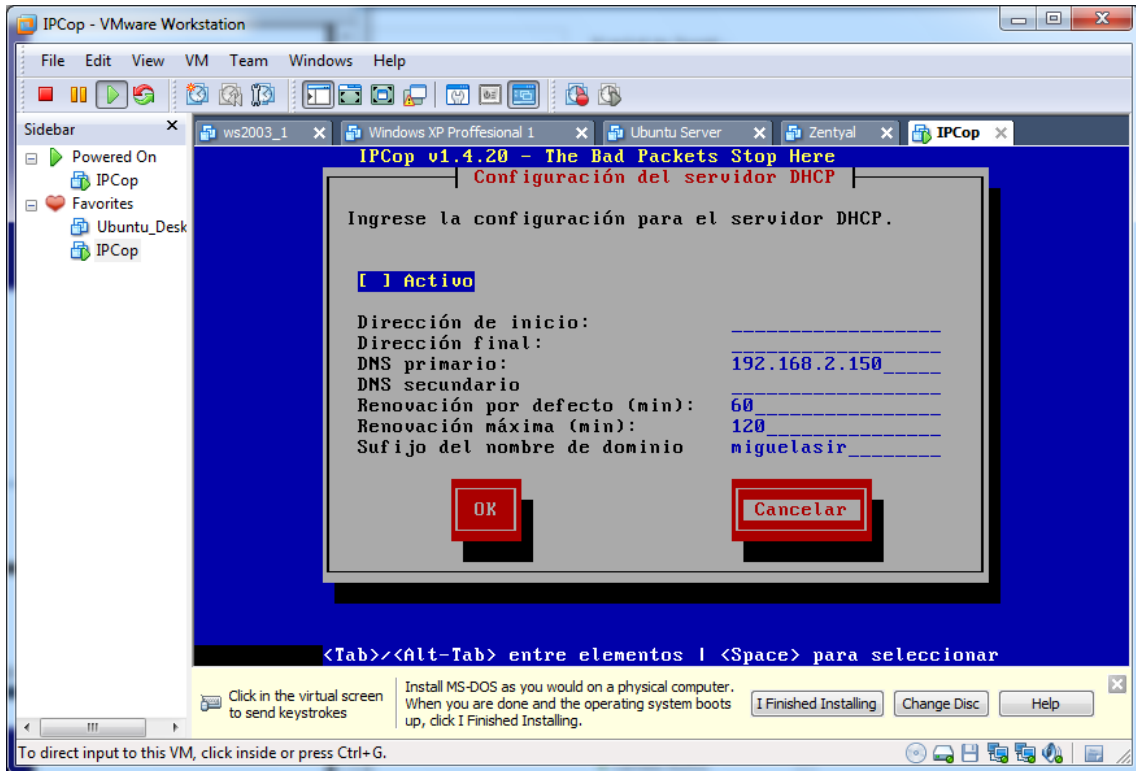
Accedemos a las opciones de DNS y puerta de enlace.



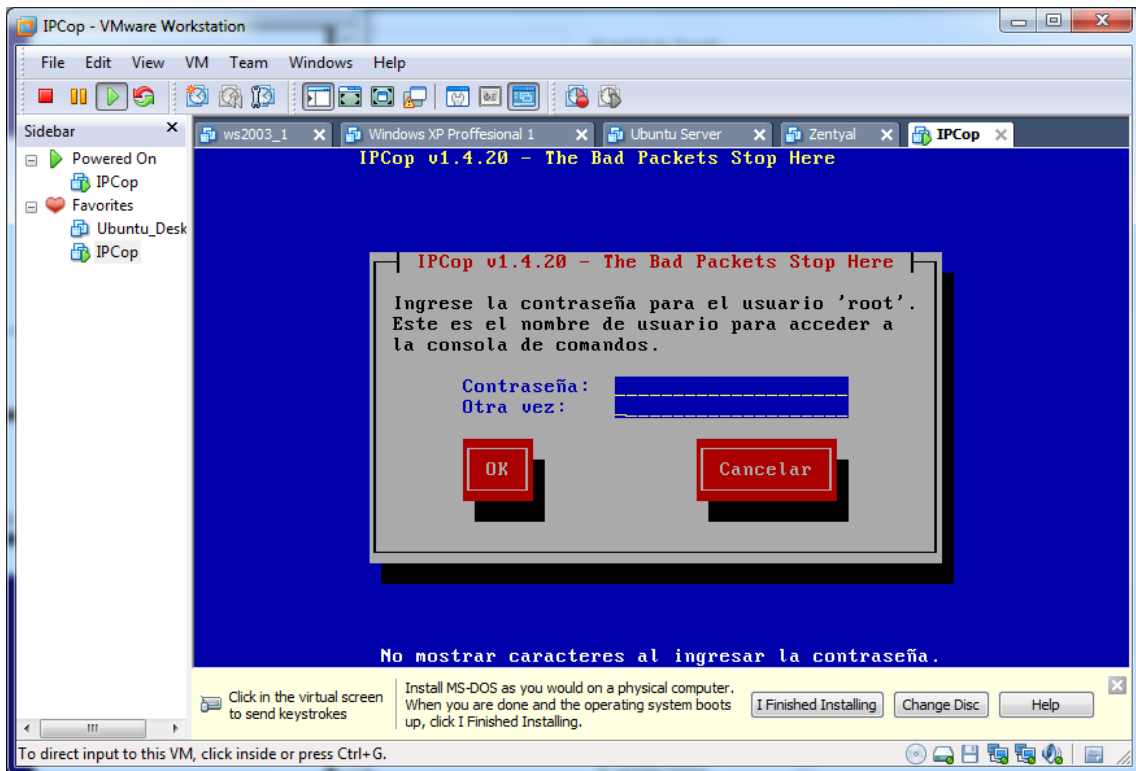
Ingresamos la información de las DNS y la puerta de enlace a internet.



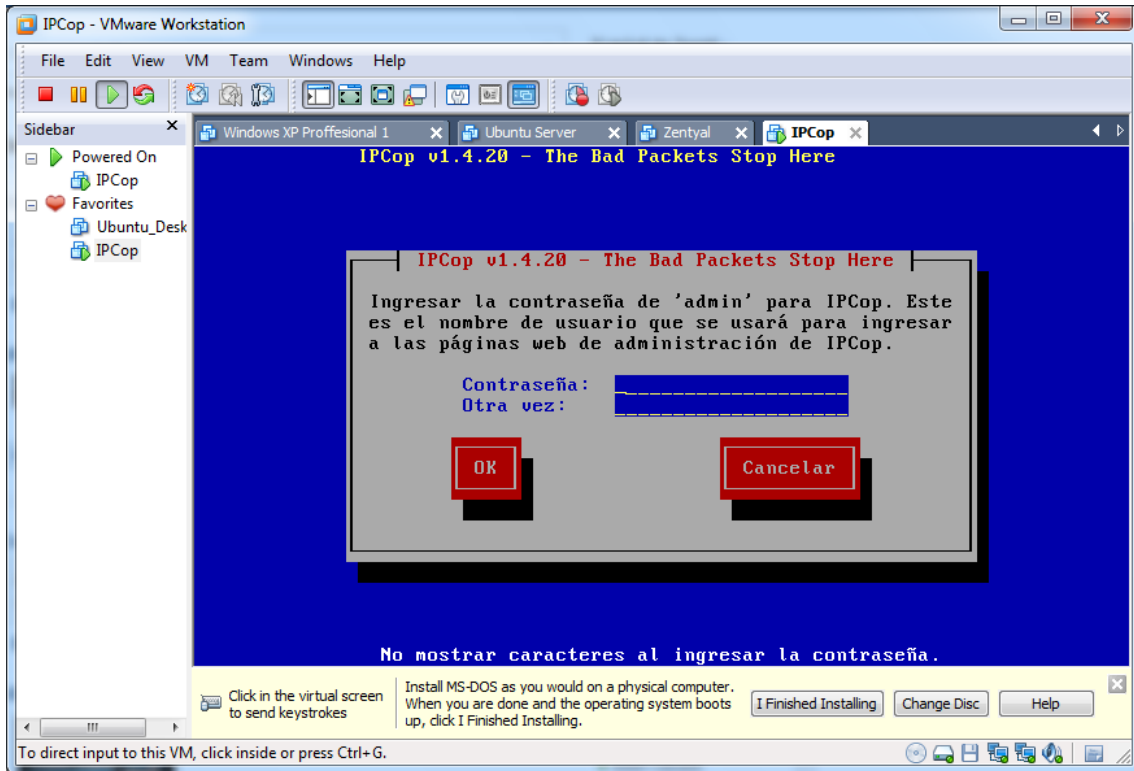
Por, último si queremos, hacemos la configuración del servidor DHCP, seguidamente pulsamos OK, y finalizamos la configuración.



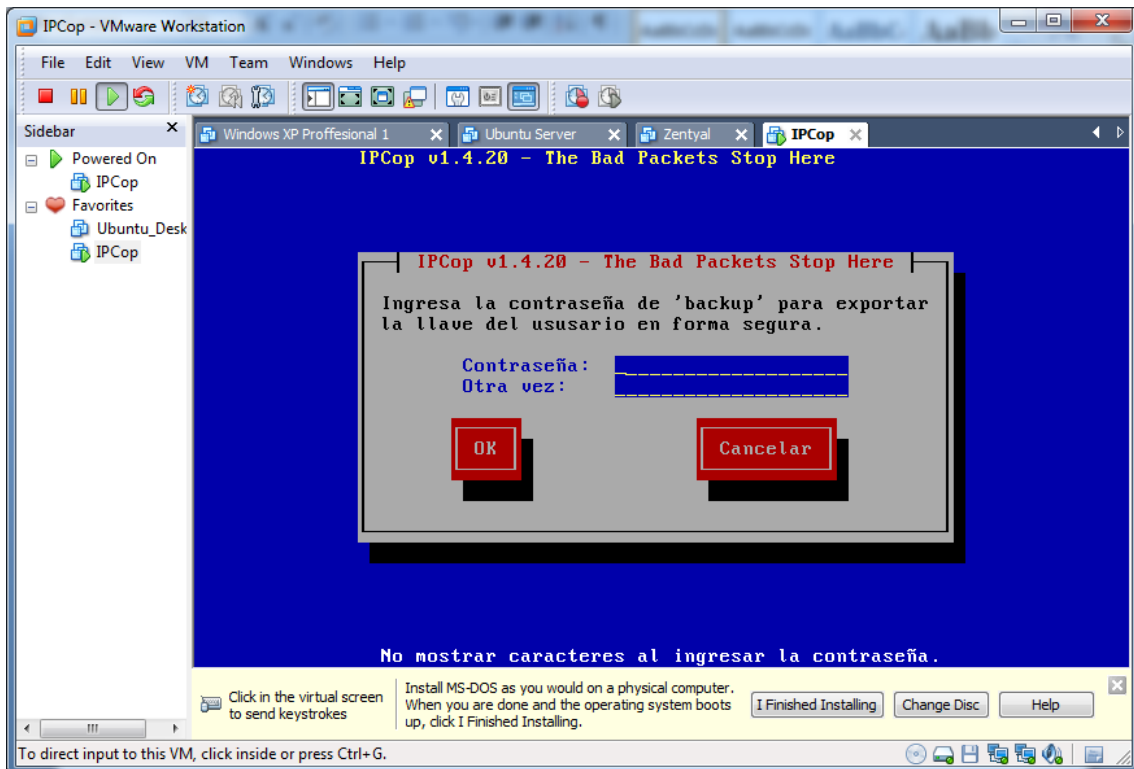
Ingresamos la contraseña para el usuario **root**, que será "invesinves".



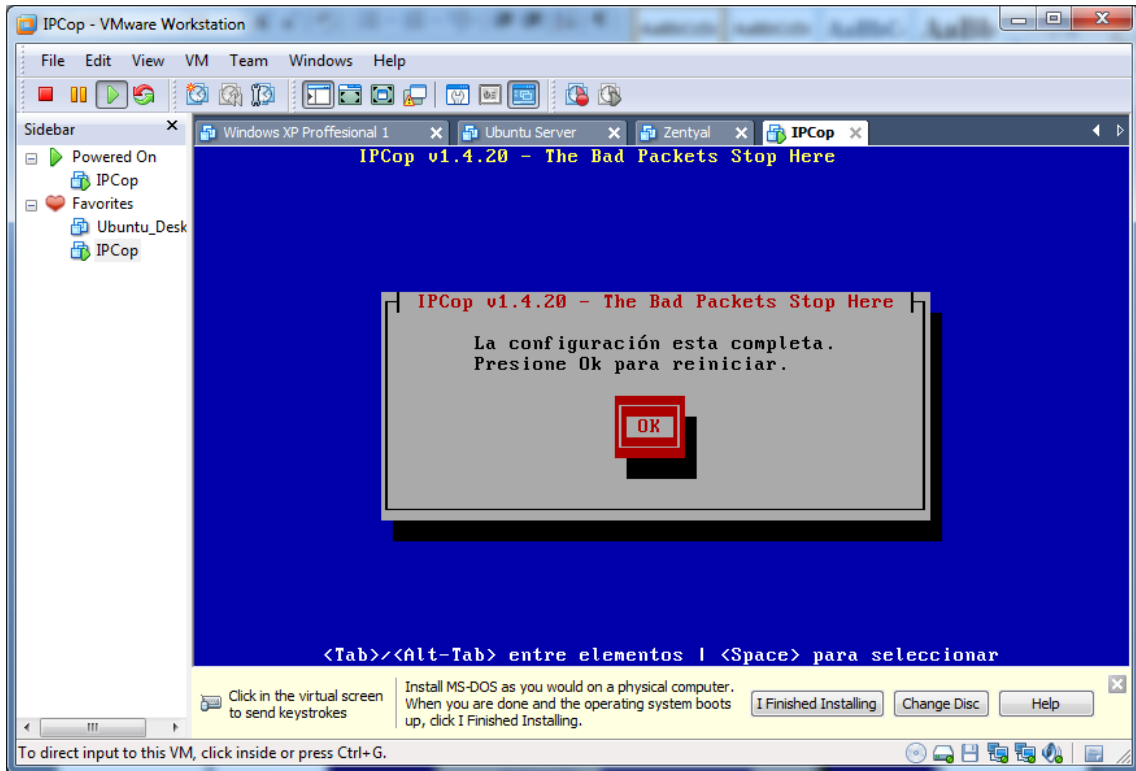
Ingresamos la contraseña para el administrador de IPCot.



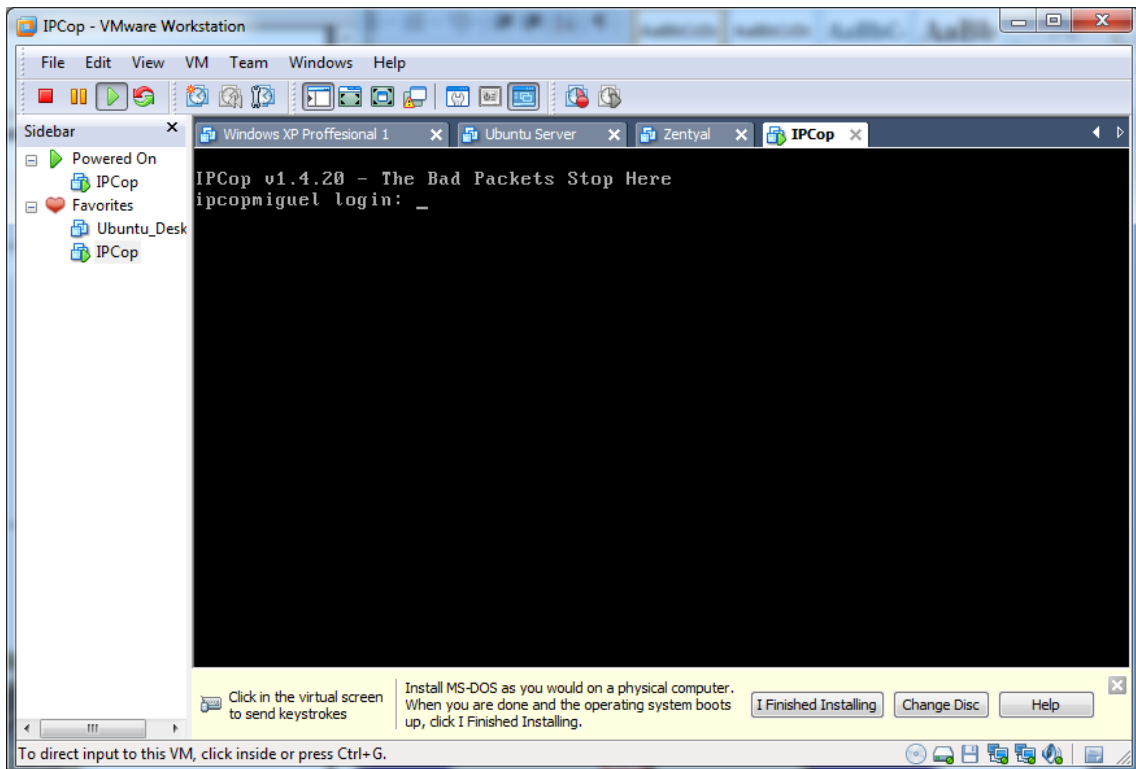
Además ingresamos una contraseña para la realización de backups de forma segura.



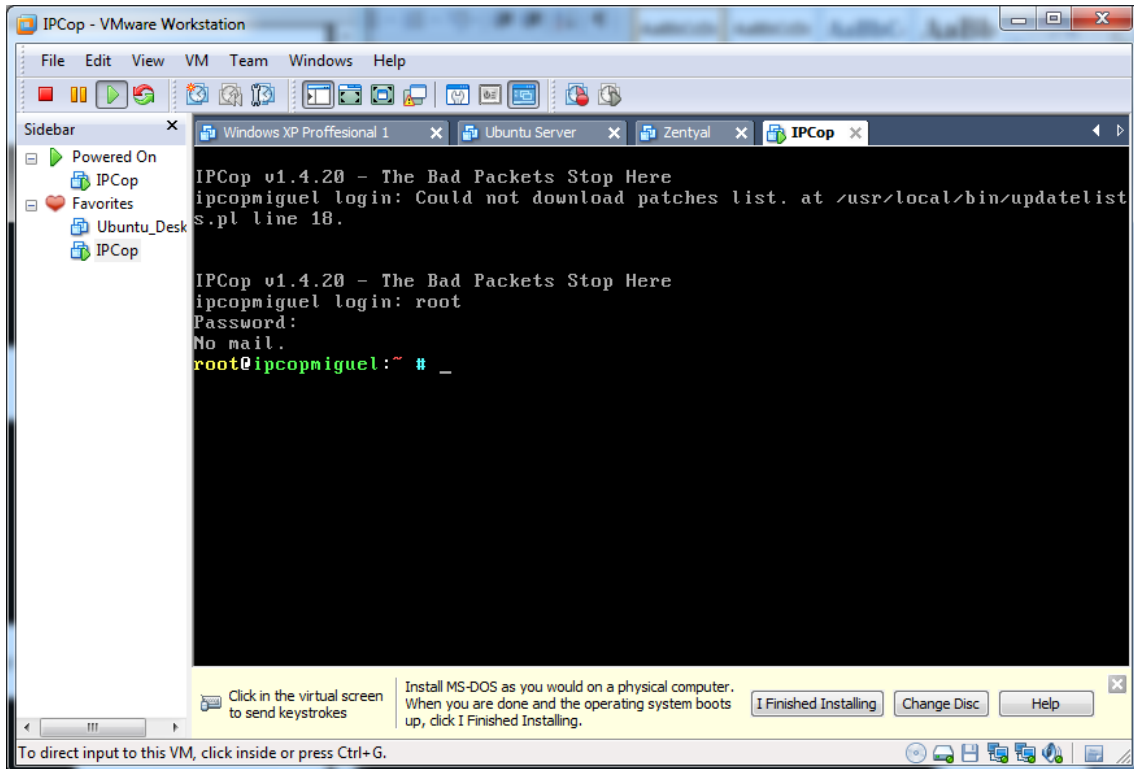
Una vez configurado todo perfectamente, pulsamos OK en esta pantalla y reiniciamos la máquina.



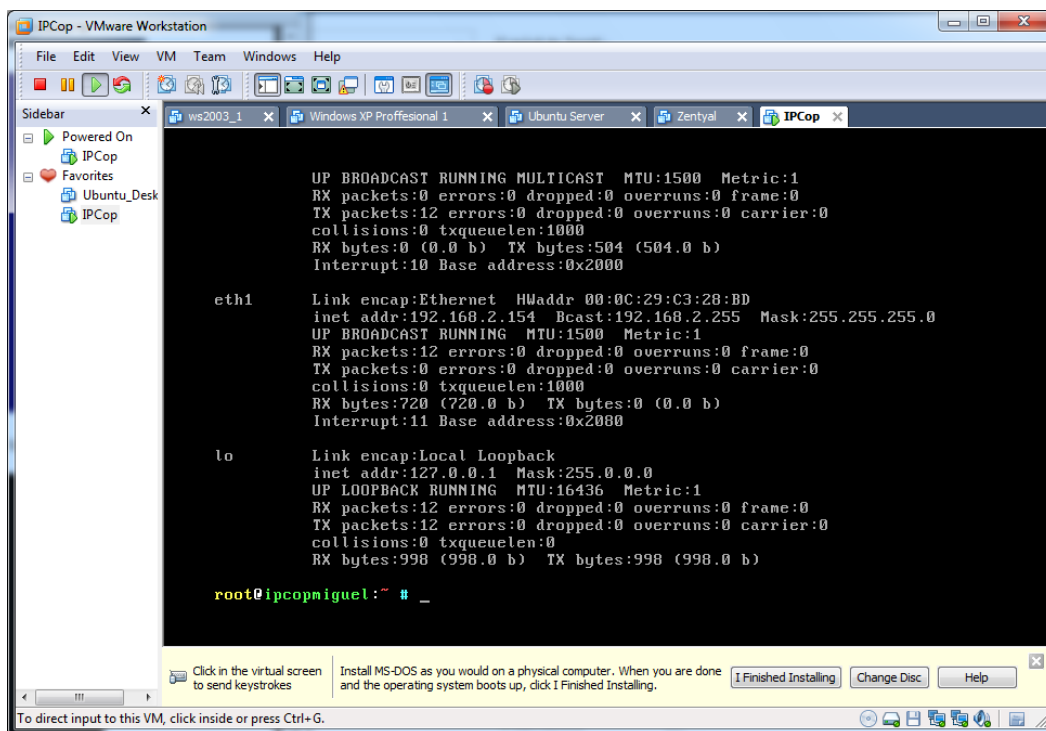
Arrancamos el sistema, y apreciamos un arranque similar a otros sistemas Linux.



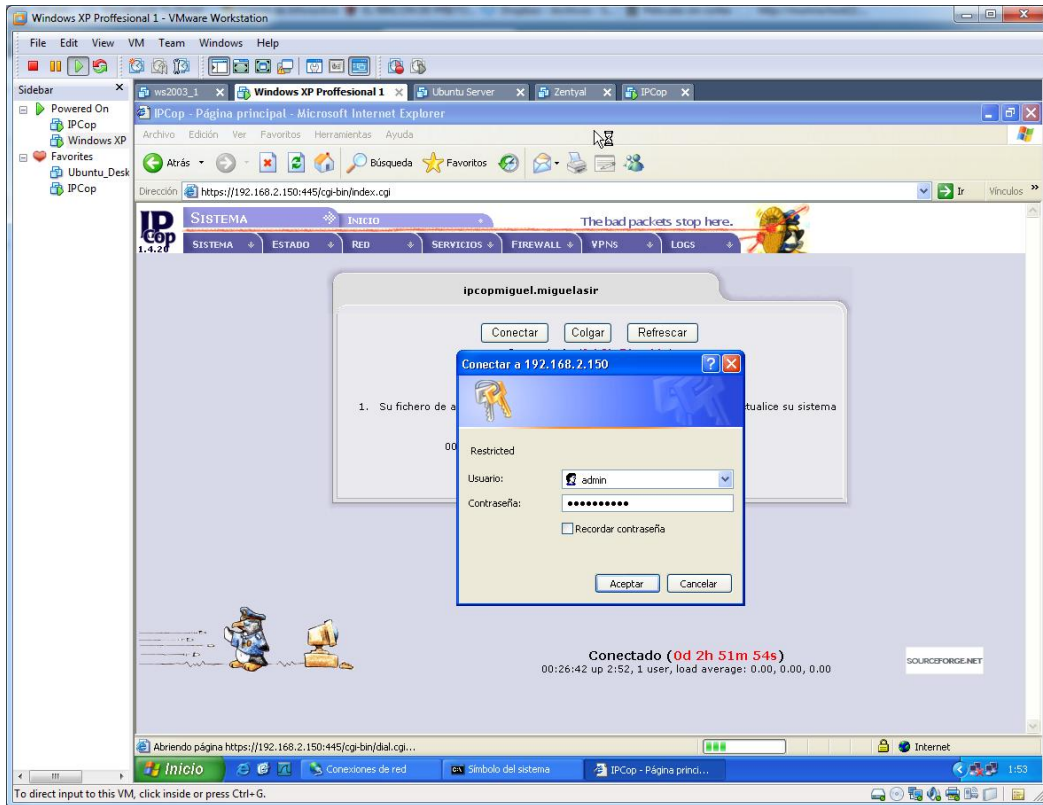
Nos logueamos como **root**.



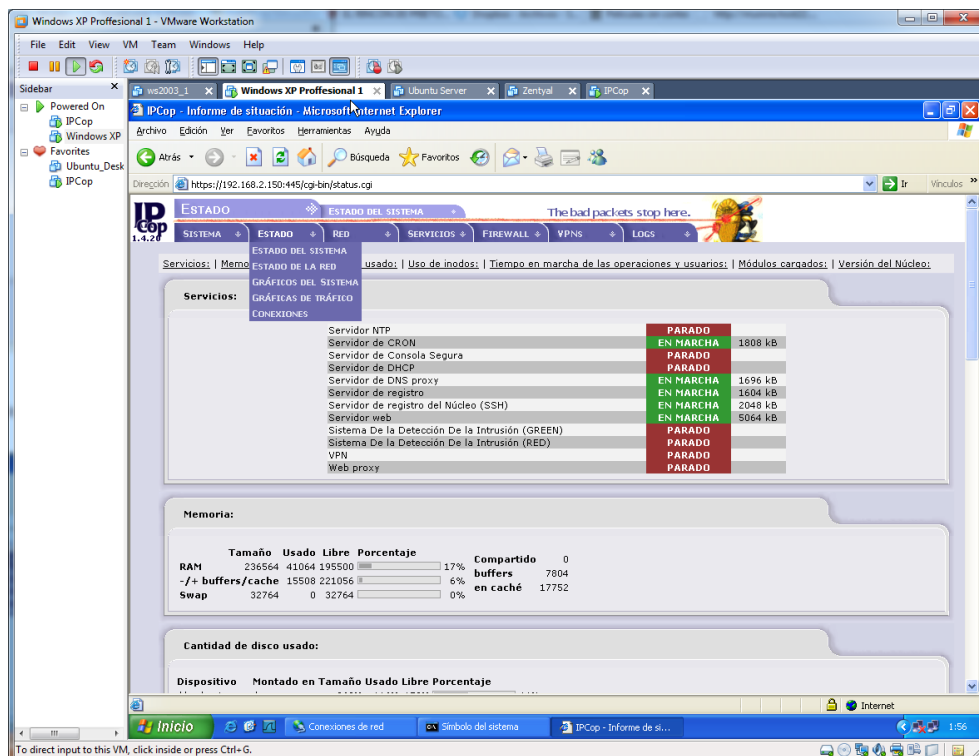
Ejecutamos un **ipconfig** para comprobar que nos ha almacenado el valor de las tarjetas de red.



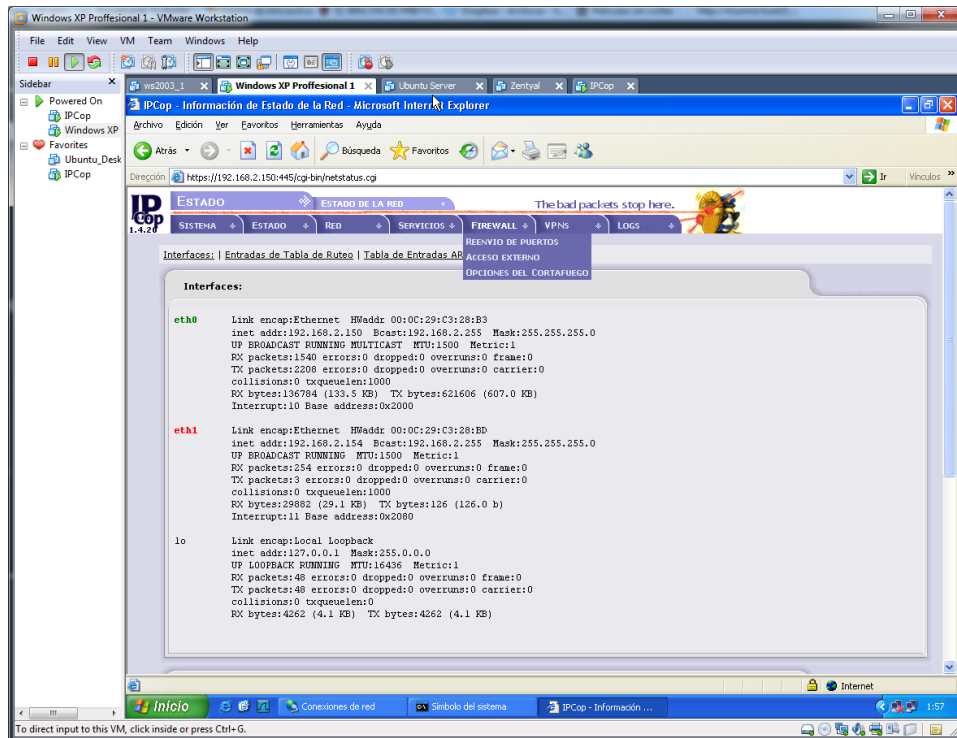
Desde un cliente, accedemos a la máquina vía web. Nos logueamos con la cuenta de administrador.



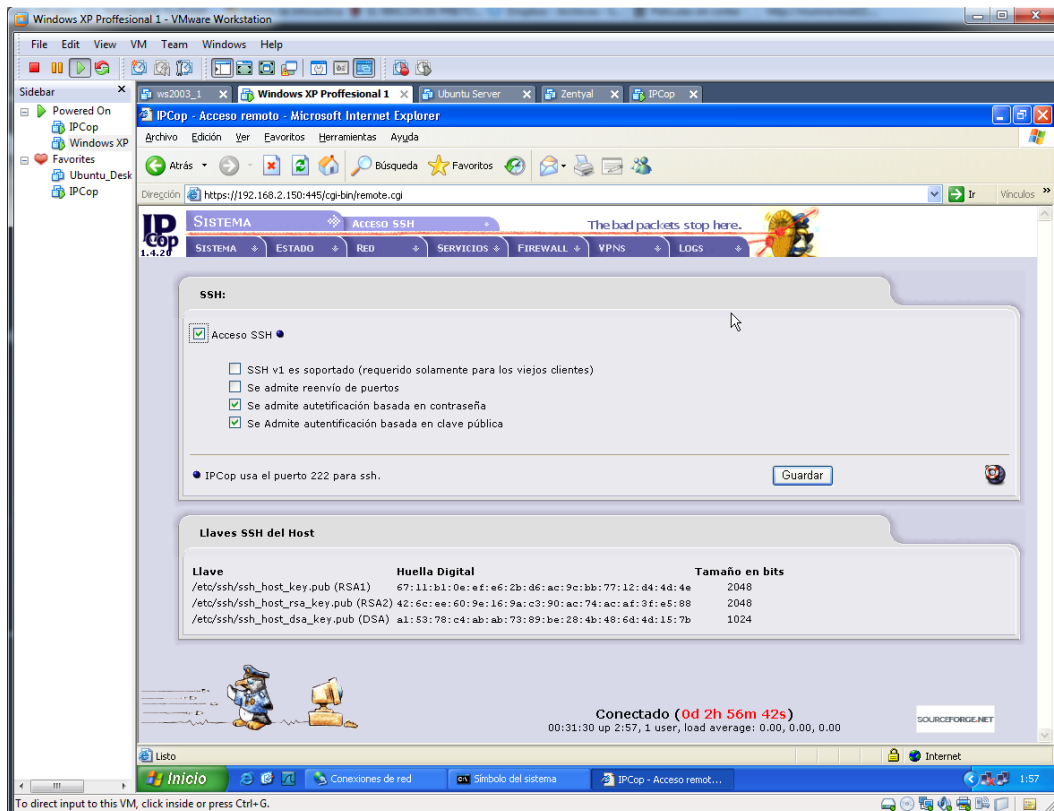
Podemos realizar diversas tareas con esta aplicación, como por ejemplo mirar el estado del sistema.



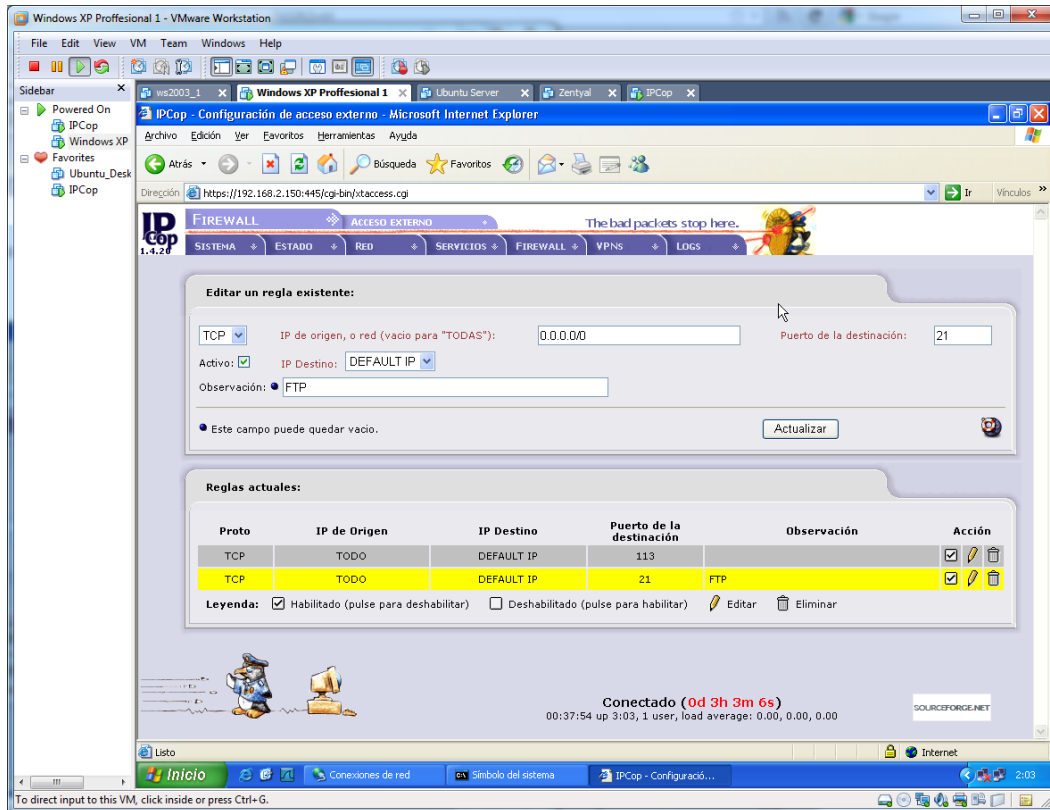
Podemos comprobar el estado de las interfaces de la máquina, que hemos configurado anteriormente.



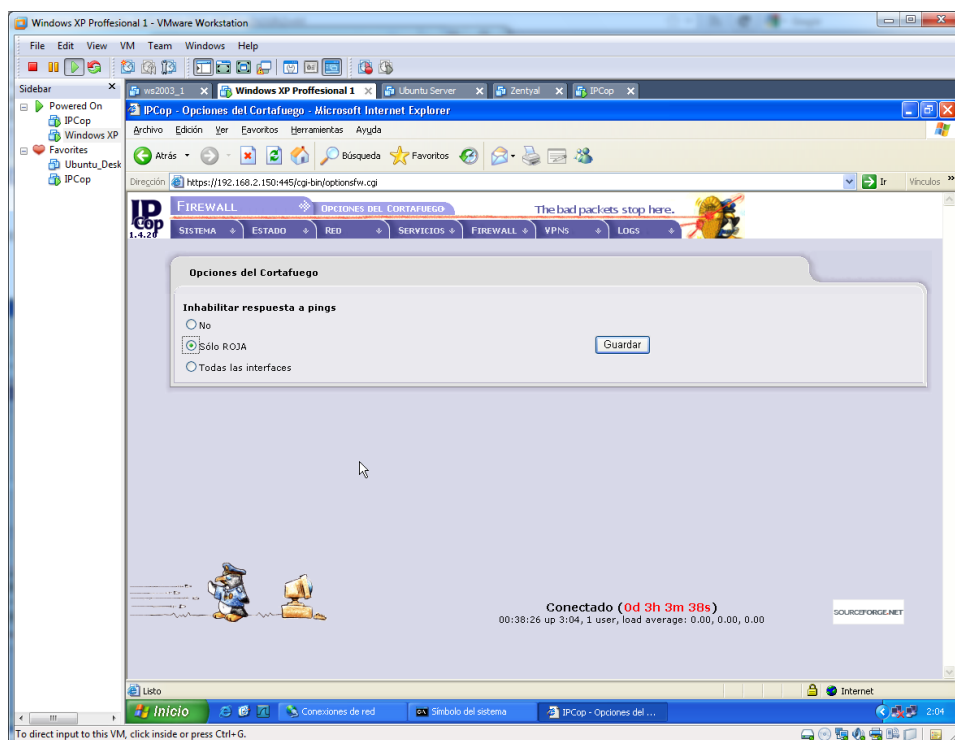
Podemos habilitar el acceso ssh a la máquina.



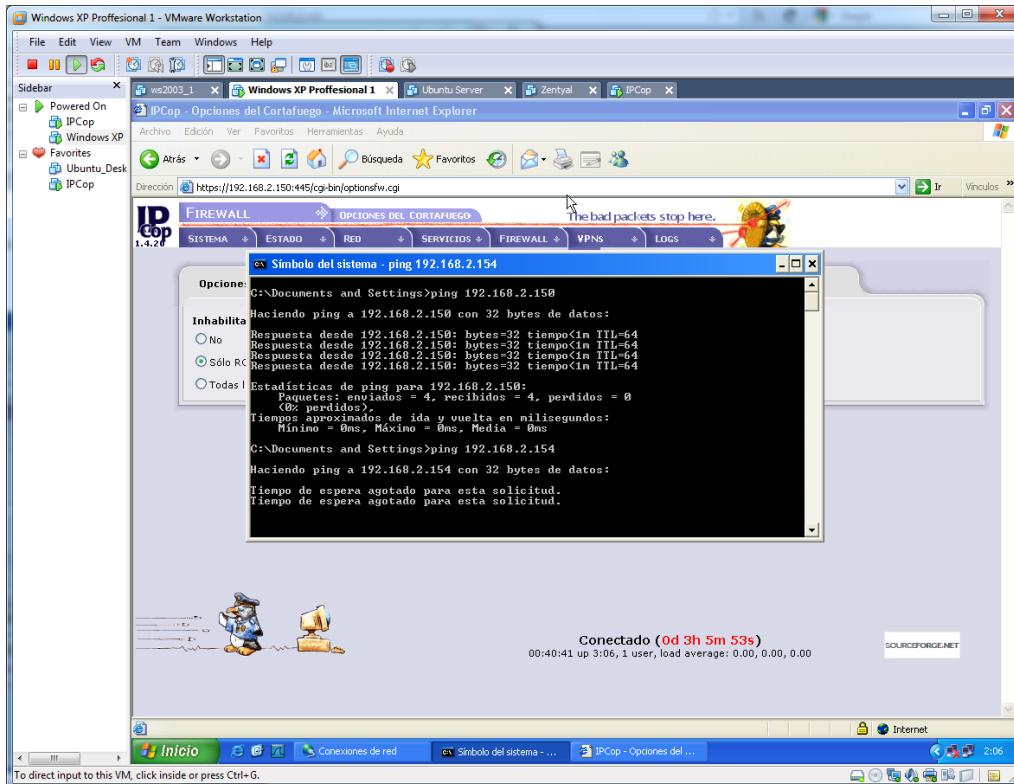
En acceso externo, deshabilitamos el servicio FTP por el puerto 21



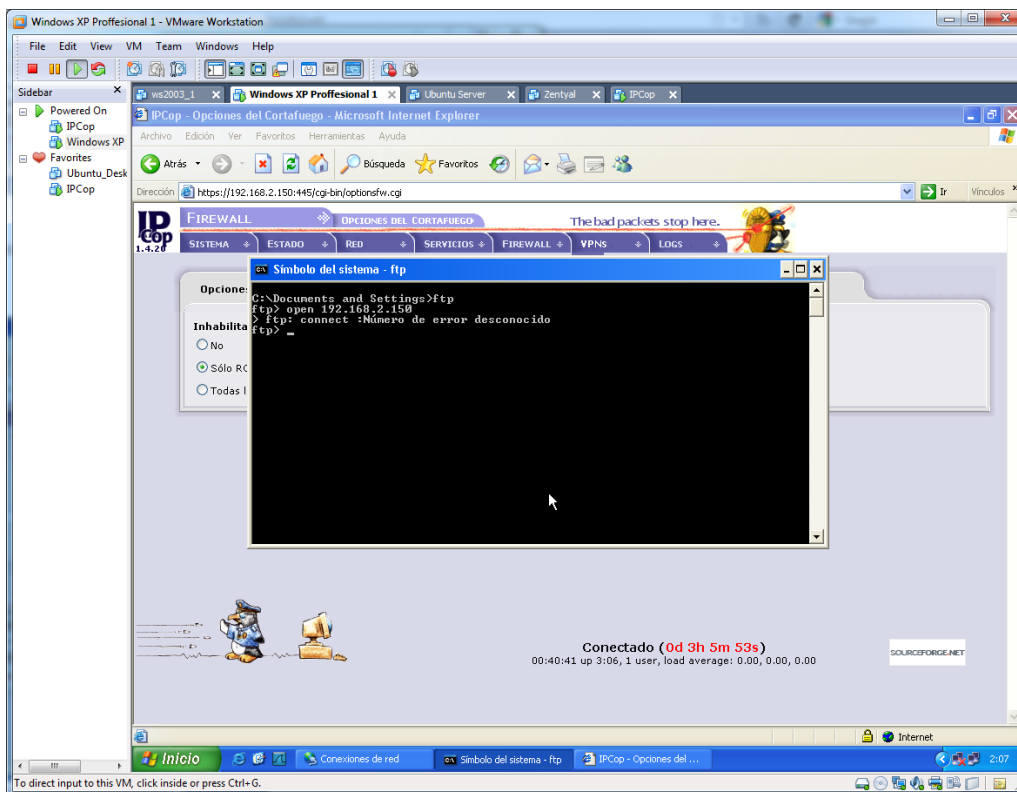
También podemos denegar las respuestas de ping a las interfaces, aquí por ejemplo denegamos la tarjeta roja o 2º interfaz.



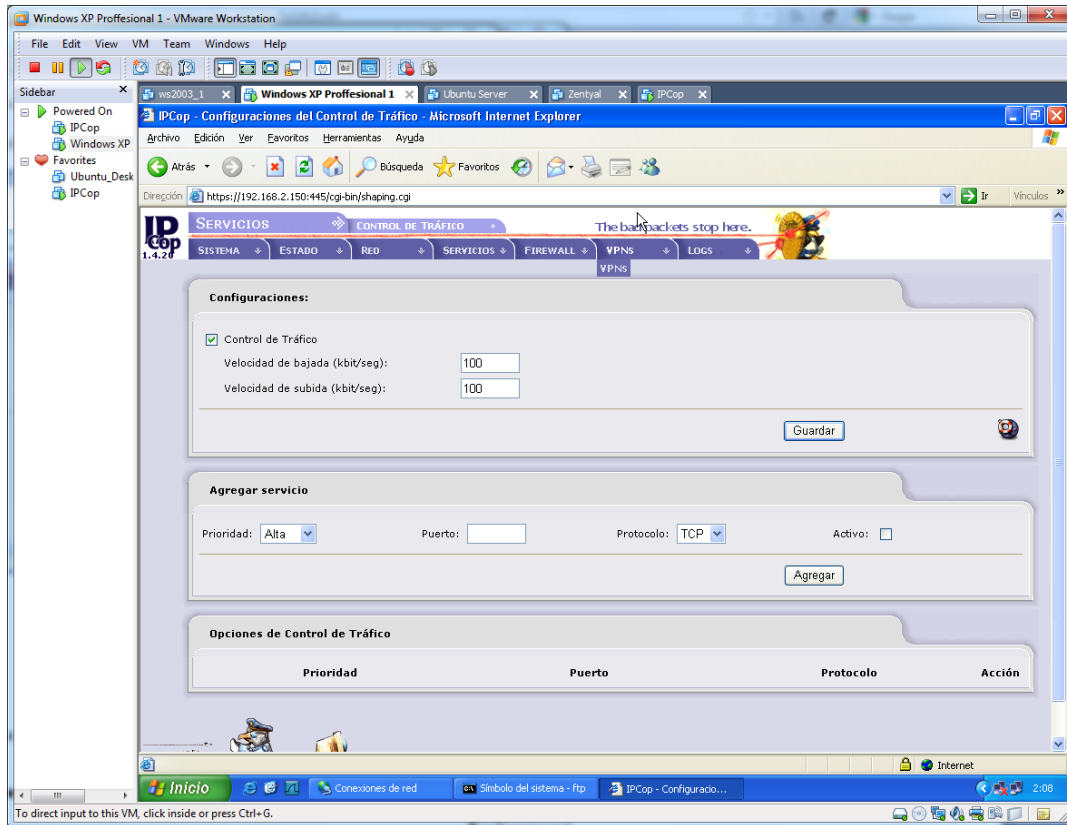
Comprobamos que podemos hacer ping con el cliente a la tarjeta verde, pero no a la roja.



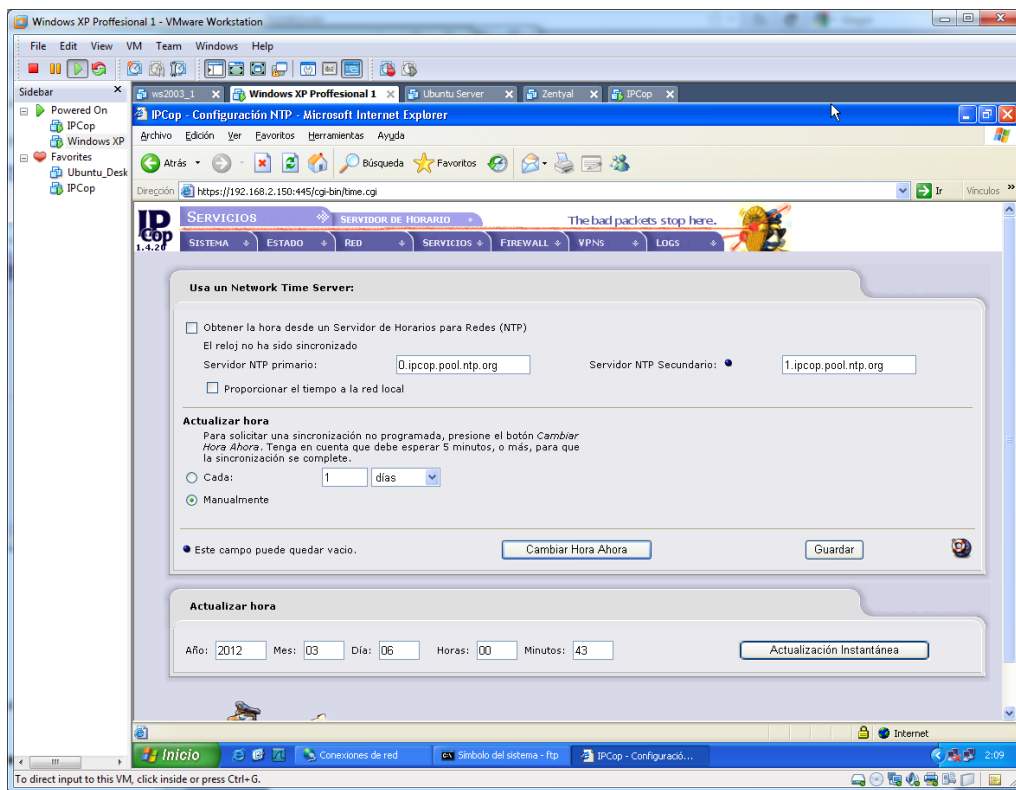
Comprobamos también que no podemos acceder al servicio FTP.



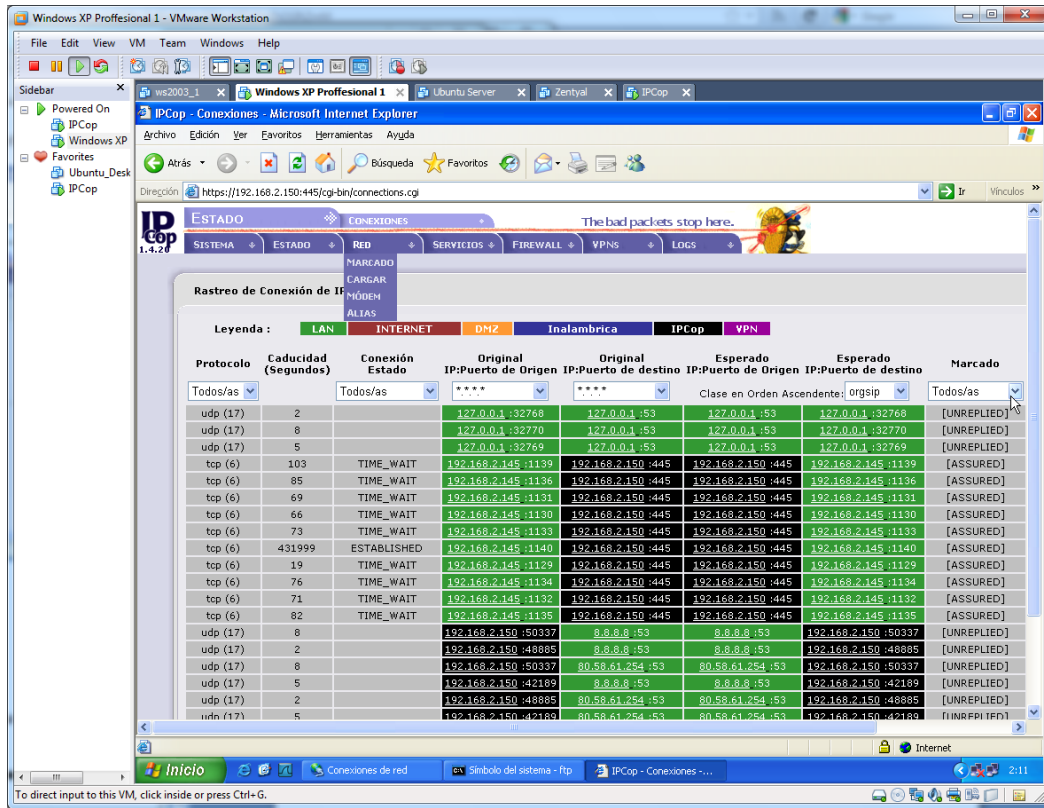
Podemos realizar en control de tráfico un control del mismo.



Podemos configurar en servidor de horario un servidor NTP.



También podemos destacar el estado de las conexiones, para auditar todas las conexiones con la máquina.



6. CORTAFUEGOS HARDWARE.

a) Elabora un informe sobre los cortafuegos hardware Cisco PIX (Private Internet Exchange) y la tecnología ASA de Cisco. Comenta en detalle algún producto Cisco PIX.

Cisco PIX (Private Internet Exchange)

PIX es el acrónimo de Private Internet EXchange.

Esta sigla es utilizada por el fabricante tecnológico Cisco, para referirse a sus modelos de equipos Cortafuegos (FireWalls).

Se trata de un firewall completamente hardware: a diferencia de otros sistemas cortafuegos, PIX no se ejecuta en una máquina Unix, sino que incluye un sistema operativo empujado denominado Finesse que desde espacio de usuario se asemeja más a un router que a un sistema Unix clásico.



El cortafuegos PIX utiliza un algoritmo de protección denominado *Adaptive Security Algorithm* (ASA): a cualquier paquete *inbound* (generalmente, los provenientes de redes externas que tienen como origen una red protegida) se le aplica este algoritmo antes de dejarles atravesar el firewall, aparte de realizar comprobaciones contra la información de estado de la conexión (PIX es *stateful*) en memoria; para ello, a cada interfaz del firewall se le asigna un nivel de seguridad comprendido entre 0 (la interfaz menos segura, externa) y 100 (la más segura, interna). La filosofía de funcionamiento del Adaptive Security Algorithm se basa en estas reglas:

- Ningún paquete puede atravesar el cortafuegos sin tener conexión y estado.
- Cualquier conexión cuyo origen tiene un nivel de seguridad mayor que el destino (outbound) es permitida si no se prohíbe explícitamente mediante listas de acceso.
- Cualquier conexión que tiene como origen una interfaz o red de menor seguridad que su destino (inbound) es denegada, si no se permite explícitamente mediante listas de acceso.
- Los paquetes ICMP son detenidos a no ser que se habilite su tráfico explícitamente.
- Cualquier intento de violación de las reglas anteriores es detenido, y un mensaje de alerta es enviado a syslog.
- Cuando a una interfaz del cortafuegos llega un paquete proveniente de una red con menor nivel de seguridad que su destino, el firewall le aplica el *adaptive security algorithm* para verificar que se trata de una trama válida, y en caso de que lo sea comprobar si del host origen se ha establecido una conexión con anterioridad; si no había una conexión previa, el firewall PIX crea una nueva entrada en su tabla de estados en la que se incluyen los datos necesarios para identificar a la conexión.

El cortafuegos PIX puede resultar muy complejo de gestionar, especialmente a los que provienen del mundo Unix, ya que como hemos dicho se asemeja más a un router que a un servidor con cualquier flavour de Unix; es por tanto recomendable consultar bibliografía adicional antes de trabajar con estos equipos. Una buena referencia puede ser [JF01], así como la documentación sobre el producto que está disponible a través de la web de Cisco Systems

Tecnología ASA de Cisco

Los dispositivos Cisco ASA 5505 y 5550 son componentes centrales de la estrategia Self-Defending Network de Cisco Systems. Ambos dispositivos forman parte de una familia de dispositivos de seguridad de red multifunción que ofrece la amplitud y profundidad necesarias para proteger empresas de cualquier tamaño. Su defensa proactiva frente a amenazas evita que los ataques se extiendan por toda la red de la empresa, permitiendo a las empresas proteger varios segmentos de una red al mismo tiempo, lo que consolida la inversión en seguridad y minimiza la complejidad de las instalaciones y reduce los costes operativos.



Diseñado para proporcionar servicios de seguridad de alto rendimiento para entornos de ancho de banda de nueva generación, Cisco ASA 5505 ofrece una rendimiento de firewall de 150 Megabits por segundo (Mbps) y una rendimiento de VPN encriptado de 100 Mbps. También ofrece flexibilidad y protección de la inversión significativa mediante su diseño modular único,

ofreciendo una ranura de expansión para capacidades futuras. Además, el Cisco ASA 5505 puede funcionar como un cliente VPN de hardware para simplificar la gestión. Ofrece servicios VPN SSL acelerados a través de hardware, un switch de 8 puertos 10/100 integrado compatible con la creación de múltiples “zonas” de seguridad y dos puertos integrados de Power-over-Ethernet (PoE). Entre sus diversos usos, dichos puertos PoE ofrecen una instalación intuitiva y sencilla para teléfonos Cisco IP y puede proporcionar energía a puntos de acceso Cisco con la que se mejora la movilidad del usuario.

El Cisco ASA 5550 incluye el firewall de Cisco, líder del sector y los servicios IPsec/SSL VPN dirigidos a entornos de red para grandes empresas. Puede proporcionar más de 1,2 gigabits por segundo (Gbps) de rendimiento de firewall y da soporte a 200 redes de área local virtuales (VLAN), de modo que las empresas pueden segmentar su red en numerosas zonas de alto rendimiento para mejorar la seguridad. También ofrece servicios VPN escalables, que soportan hasta 5.000 clientes IPsec y SSL VPN por aplicación. Mediante sus capacidades de agrupación de VPN y de balanceo de carga, las empresas pueden agrupar hasta 10 dispositivos Cisco ASA 5550, dando servicio a 50.000 usuarios simultáneos de IPsec y SSL VPN.

Al ampliar el alcance de la familia Cisco ASA y aprovecharse de los nuevos servicios Cisco ASA Software 7.2, las empresas pueden ampliar la aplicación de seguridad a través de su red. Ofrece más de 50 nuevas opciones de seguridad que refuerzan el firewall de capa de aplicaciones de la familia Cisco ASA, VPN de acceso remoto, alta disponibilidad, integración de redes y capacidades de gestión.

De estas mejoras, algunas de las más significativas son los servicios de firewall en la capa de aplicaciones y la integración de servicios con Cisco Network Admission Control (NAC). Los servicios de firewall en la capa de aplicaciones de Cisco proporcionan a las empresas un mayor control sobre sus dispositivos y ayudan a prevenir que las amenazas accedan a las redes empresariales. Además, mejoran la protección de protocolos de aplicaciones como web, correo electrónico, voz sobre Protocolo Internet (VoIP), mensajería instantánea, transferencia de archivos y protocolos de red Microsoft. El soporte de Cisco ASA para las soluciones NAC de Cisco administra evaluaciones integrales para usuarios y dispositivos que accedan a la red mediante conexiones IPsec y SSL VPN. Esta evaluación incluye la comprobación de las actualizaciones correspondientes de software de seguridad y sistemas operativos antes de conceder acceso a los privilegios en red.

b) Elabora un informe sobre productos comerciales que implemente Gestión Unificada de Amenazas **“Firewall UTM”** (Unified Threat Management).

D-Link Firewall UTM NETDEFEND

Firewall UTM para delegaciones

El firewall UTM DFL-260 ofrece una potente solución de seguridad para las oficinas de pequeño o medio tamaño, con hasta 50 usuarios, contra una amplia variedad de amenazas para la red en tiempo real. Al integrar un sistema de prevención de intrusos (IPS), un gateway antivirus (AV) y el filtrado de contenidos web (WCF) en un diseño industrial de tamaño de sobremesa, este dispositivo está dirigido a las empresas que buscan seguridad para la red a un precio competitivo.



Gestión de amenazas unificada

El DFL-260 integra un sistema de prevención de intrusos (IPS), un gateway antivirus (AV) y el filtrado de contenidos/URL web para una mejor protección con inspección de contenido de nivel 7.

Está disponible un servicio opcional de suscripciones para mantener actualizadas en tiempo real cada una de estas defensas.

Potente prevención de intrusos

El DFL-260 sigue una única tecnología IPS, firmas de virus basadas en componente, que se integra para reconocer todas las variedades de ataques conocidos y desconocidos y proteger contra ellas, y que puede tratar todos los aspectos críticos de un ataque o potencial ataque, incluidos la carga, NOP sled, infección y exploits. En cuanto a la cobertura de las firmas de virus, la base de datos IPS incluye informaciones y datos de ataque procedentes de una parrilla de sensores global y, además, exploits recopilados de sitios públicos, tales como la National Vulnerability Database y Bugtrax. El DFL-260 cuenta con firmas de virus IPS de alta calidad porque constantemente crea y optimiza las firmas de virus NetDefend por medio del sistema sensor de autofirma de D-Link (Auto-Signature Sensor System). Sin sobrecargar el dispositivo, estas firmas garantizan una alta tasa de precisión de detección y la menor tasa de falsos positivos.

Escaneado de virus basado en el flujo

El DFL-260 escanea archivos de cualquier tamaño utilizando una tecnología de escaneo de virus basada en el flujo que no requiere almacenamiento temporal. Este método de escaneado mejora el rendimiento de inspección al mismo tiempo que elimina los cuellos de botella en la red. El dispositivo usa firmas de virus de la respetada compañía antivirus Kaspersky Labs para proporcionar a los usuarios unas firmas antivirus precisas y fiables, así como comunicar las actualizaciones de firmas. Por consiguiente, se pueden bloquear con eficacia los virus y el malware antes de que lleguen a los dispositivos móviles o de sobremesa de la red.

Filtrado de contenido web

El filtrado de contenido web ayuda a los administradores a monitorizar, gestionar y controlar el uso que los empleados hacen de internet. El DFL-260 implementa varios servidores de índice global con millones de URL e información de sitios web en tiempo real para mejorar la capacidad de rendimiento y maximizar la disponibilidad del servicio. El firewall usa políticas granulares y explícitas listas blancas y listas negras para permitir o denegar el acceso a determinados tipos de sitios web para cada combinación de usuarios, interfaces y redes IP. Puede desmontar los potenciales objetos maliciosos, como applets de Java, JavaScripts/VBScripts, objetos ActiveX y cookies, para tratar activamente el contenido de internet.

Acelerador por hardware

El DFL-260 usa un acelerador por hardware para llevar a cabo las funciones de escaneado antivirus e IPS simultáneamente, sin que se degrade el rendimiento del firewall ni el de la red privada virtual.

Este potente acelerador le permite al firewall trabajar con un rendimiento muy superior al de los firewall UTM con función antivirus del mercado.

Potente rendimiento de la red privada virtual

El DFL-260 dispone de un motor de red privada virtual basado en hardware para soportar y gestionar hasta 100 túneles VPN. Admite los protocolos IPSec, PPTP y L2TP en modo cliente/servidor y también puede manejar el tráfico que pasa a través de él. La autenticación de usuario puede llevarse a cabo por medio de un servidor RADIUS externo o a través de la base de datos interna del firewall, que admite hasta 150 cuentas.

Monitorización y gestión

El DFL-260 puede gestionarse remotamente a través de la interfaz basada en web, la interfaz de línea de comandos por el puerto consola RS-232 o una conexión SSH (Secure Shell). La configuración es rápida gracias a un asistente de instalación que incluye características avanzadas para monitorizar la red y conservarla en buen estado y con total seguridad, tales como avisos por correo electrónico, registro del sistema, comprobaciones regulares y estadísticas en tiempo real.

Clavister Extended UTM

Desde el principio, el requerimiento mínimo UTM era un Firewall, Detección de Intrusión de red (IDS) y funcionalidad de Prevención de Intrusiones (IPS), y Antivirus de Entrada (AV Perimetral). El último producto de Clavister ofrece esta funcionalidad junto con capacidades VPN, Control de Tráfico y Gestor de Filtrado de Contenidos, todos con capacidad de multi-gigabit. Lo llamamos xUTM. La demanda de dispositivos, al contrario de software, se explica por el aumento del requerimiento de la conveniencia plug & play, son de fácil instalación y de administración centralizada. Los dispositivos son más fáciles de desplegar que las soluciones de software, ya que incluyen su hardware y software pre-integrados. Son generalmente muy confiables y pueden resistir gran volumen de tráfico. La mayoría pueden tener más escala agregando más dispositivos. Cuando una maquina falla, es más fácil cambiarla que localizar el problema. Este proceso pone al nodo en línea más rápido, y puede realizarse por personal no técnico. Esto es especialmente importante para oficinas remotas o para las PYMES con poco personal capacitado.



Integridad

Oferta producto completo

Incluye todos los componentes necesarios para despliegue, administración y apoyo de su infraestructura de seguridad de por vida.

El conjunto más variado

Incluye Firewall, VPN, Anti-virus, Prevención y Detección de Intrusión, Administración de tráfico, Control de Aplicación, Failover, Control P2P, Routing avanzado y mucho más.

Ximark UTM/Firewall

La administración de Firewalls y UTM's es intensiva en recursos y requiere un alto nivel de conocimientos. Debido a la complejidad asociada a estas tareas, la mayoría de las violaciones son causadas por la incorrecta configuración de reglas y políticas de firewall.



Ximark UTM/Firewall Administrado es un servicio de administración de dispositivos de seguridad de perímetro, conocidos también como “Administradores de Amenazas Unificadas” que protegen a las organizaciones con herramientas integrales como: anti-spam, anti-virus, sistema de prevención de intrusos (IPS), filtro de contenido web, control de “peer-to-peer” (P2P) y control de chat, entre otros.

El registro de eventos, la administración de la configuración y los reportes centralizados son fundamentales de acuerdo a las mejores prácticas de seguridad modernas. Con Ximark UTM/Firewall Administrado las organizaciones pequeñas y medianas pueden cumplir con estas prácticas. Con nuestro modelo de seguridad “On-Demand” las empresas de todos los tamaños pueden beneficiarse de una solución centralizada de administración y monitoreo de sus dispositivos de seguridad perimetral de varios fabricantes líderes. No hay requerimientos adicionales de hardware, software o facilidades, lo cual provee un costo competitivo.

Funcionalidades del Servicio

- **Monitoreo**

Administración de registros (logs). Revise registros en tiempo real o históricamente. Para diagnóstico o análisis de seguridad.

Monitoreo de la disponibilidad del dispositivo. Sea notificado cuando el dispositivo presenta problemas de desempeño o conectividad.

- **Reportes**

Servicio "On-demand". Acceda al servicio desde cualquier ubicación vía Internet vía un browser.

Reportes pre-configurados. Vea reportes de actividades como los hosts más activos, servicios más usados, sitios más visitados y otra información útil para diagnóstico y control.

- **Administración**

Administración de la configuración. La ejecución de cambios programados se incluye dentro Ximark UTM/Firewall Administrado.

Mantenimiento. Las tareas de mantenimiento como actualización de firmware y otras.

Actualización de servicios de protección. Los servicios de protección UTM como anti-spam, anti-virus, IPS y filtrado de contenido web se actualizan.

- **Mesa de Servicio**

Mesa de servicio vía Web. Puede abrir casos 24x7x365 días al año vía web y por teléfono. Como un sólo punto de contacto para todas sus necesidades de soporte, nuestros ingenieros que atienden vía nuestra plataforma web, tienen experiencia en soportar redes y ayudar a diagnosticar problemas y proveer soluciones. La mesa de servicio permite que Ximark responda tan rápido como sea posible o de acuerdo a los acuerdos de niveles de servicio (SLA) establecidos con el cliente. Para ellos es posible manejar escalamientos y alertas a los gerentes del área de soporte. La mesa de servicio es basado en Web y en tecnologías de última generación. El sistema posee una base de datos conocimiento, calendario, manejo de SLAs, y otras funcionalidades que permiten brindar un servicio de soporte avanzado.

- **Niveles de Servicio**

Ximark UTM/Firewall Administrado ofrece niveles de acuerdo de servicio (SLA) para garantizar la disponibilidad y confiabilidad.

