

PROYECTO SAD

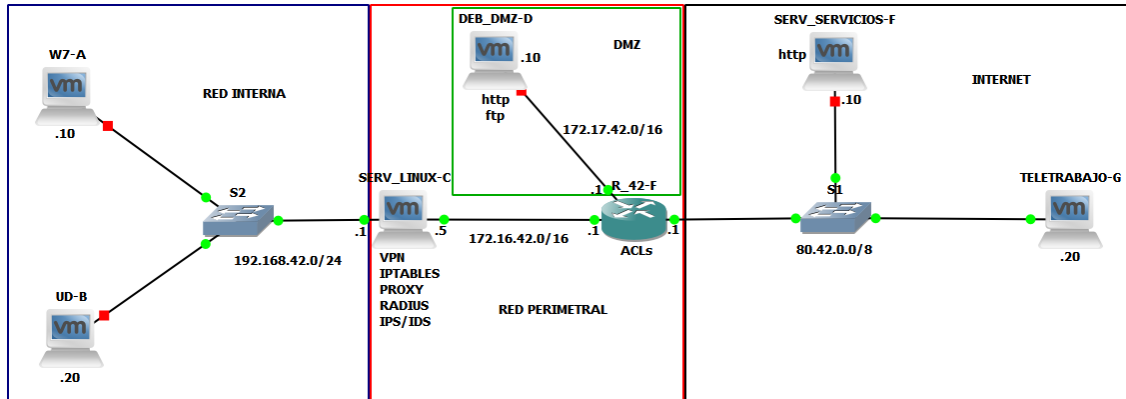
Eduardo de Lamo Téllez

ÍNDICE

UD1: Adopción de pautas de seguridad informática.	3
UD2: Implantación de mecanismos de seguridad activa.	7
UD 3.- Implantación de técnicas de acceso remoto. Seguridad perimetral.	14
UD 4.- Instalación y configuración de cortafuegos.	19
UD 5.- Instalación y configuración de servidores “proxy”.	22
UD 6.- Implantación de soluciones de alta disponibilidad.....	27

UD1: Adopción de pautas de seguridad informática.

1. Indica la red interna de la empresa, red perimetral, zona desmilitarizada e indica el tipo de arquitectura que está utilizando dicha empresa.



Este escenario cuenta con 4 zonas claramente diferenciadas; la red interna de la empresa a la izquierda, la red perimetral en el centro, dentro del perímetro se encuentra la DMZ y por último a la derecha del router frontera se encuentra Internet que ya está fuera de la empresa. Esta empresa está utilizando una arquitectura de tres patas.

2. Realizar una copia de seguridad del sitio web del equipo DMZ en el equipo B todos los días a las 23 horas.

Creo un script con el comando scp para realizar la copia de seguridad en remoto. Lo guardo en /usr/local/bin/copia_web.ssh.

```
#!/bin/bash
sshpas -p 'inves' scp -r /var/www/html/* edu@192.168.42.20:/copias
```

Le doy permisos de ejecución.

```
root@debian:~# chmod +x /usr/local/bin/copia_web.sh
root@debian:~#
```

Programo la copia con crontab.

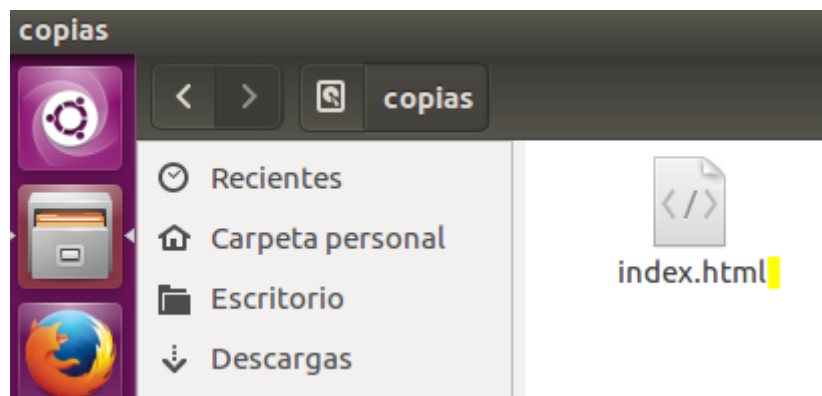
```
root@debian:~# crontab -e
no crontab for root - using an empty one

Select an editor. To change later, run 'select-editor'.
 1. /bin/nano      <---- easiest
 2. /usr/bin/vim.tiny

Choose 1-2 [1]: 1
```

```
GNU nano 2.7.4      Fichero: /tmp/crontab.2C4oXX/crontab      Modificado
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
* 23 * * * /usr/local/bin/copia_web.sh
```

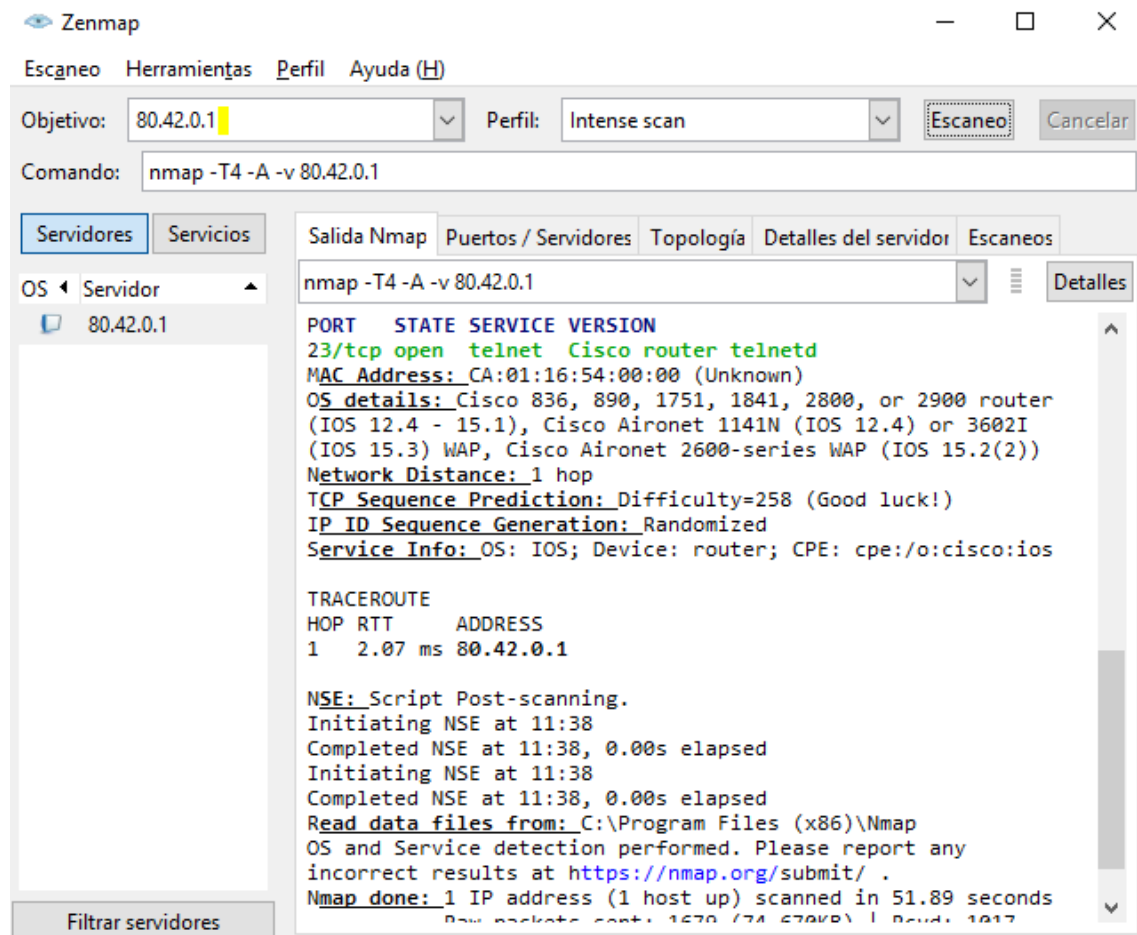
Vemos la copia realizada en el equipo B.



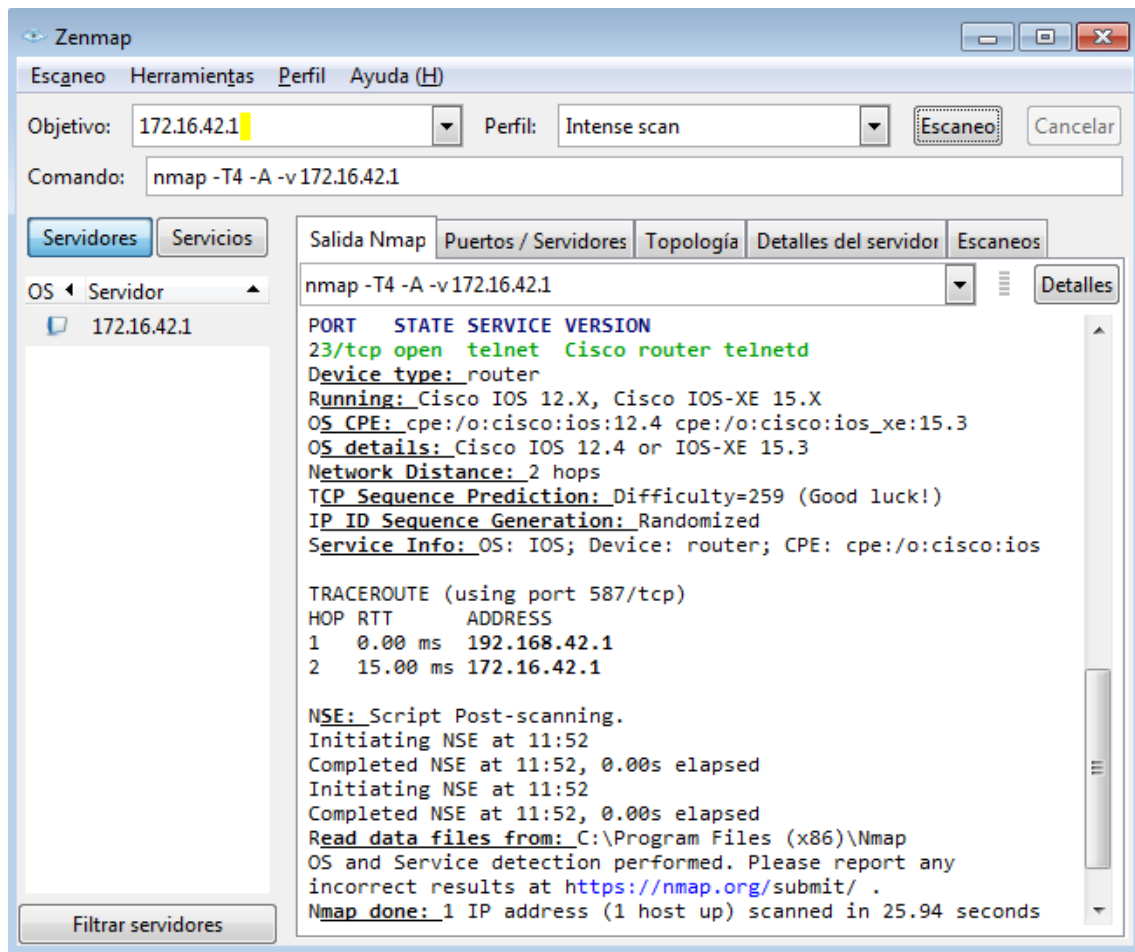
3. Detecta mediante NMAP las vulnerabilidades en el router frontera R_XX.

Utilizo la herramienta gráfica Zenmap tanto en la pata de la red interna como la pata de Internet.

Escaneo desde el PC TELETRABAJO-G.



Escaneo desde el PC W7-A.

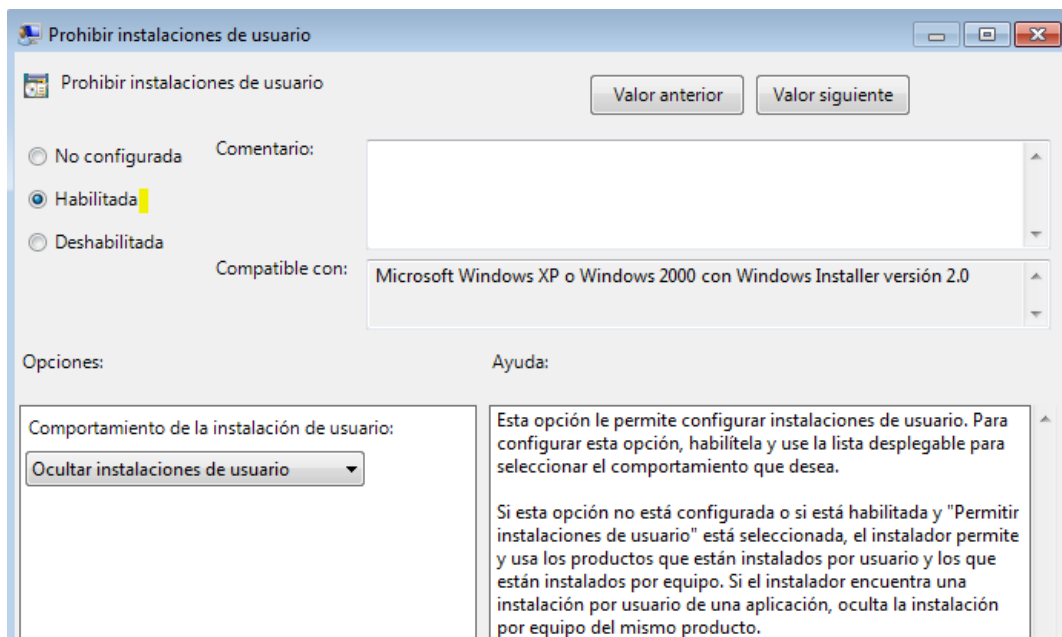
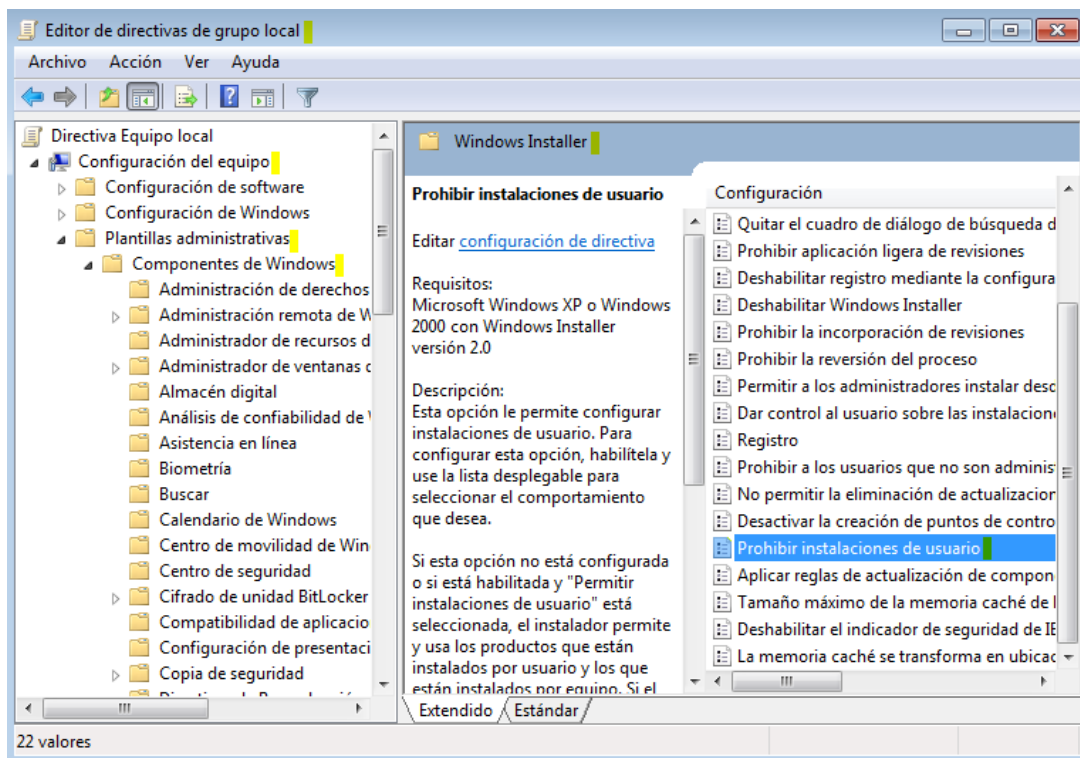
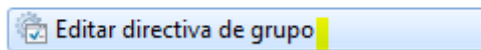


UD2: Implantación de mecanismos de seguridad activa.

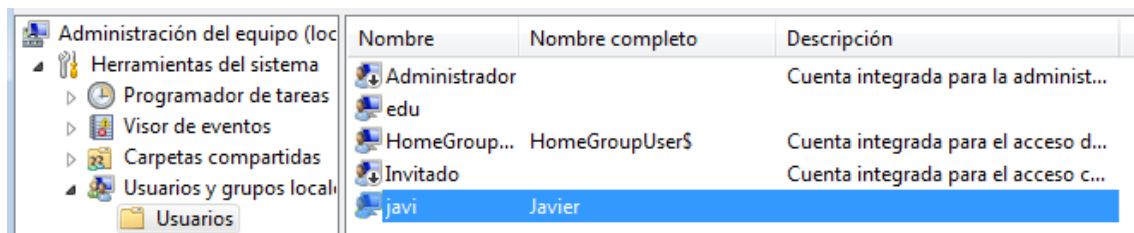
4. Evita que otros usuarios puedan instalar cualquier tipo de aplicación en el equipo A.

Edito la directiva de grupo local para prohibir la instalación de aplicaciones a usuarios que no sean el administrador.

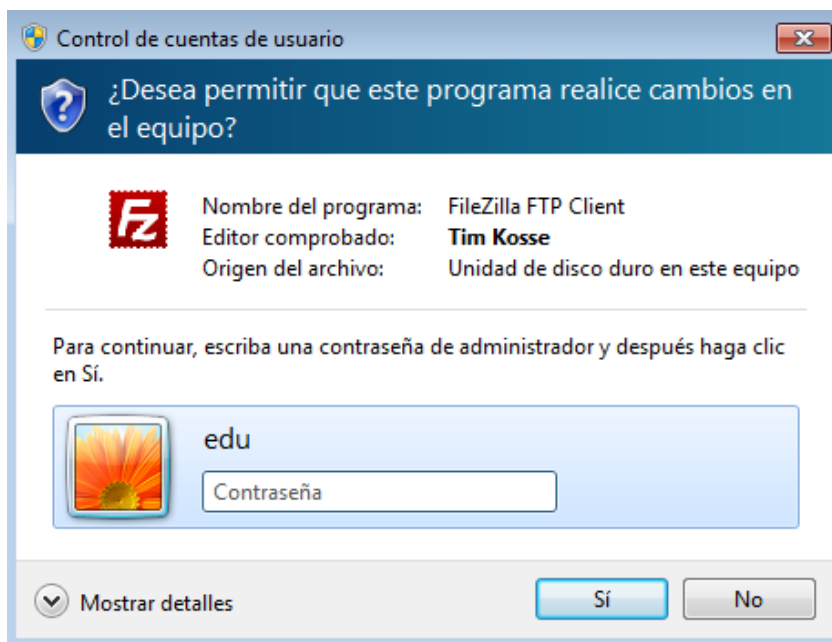
Panel de control (1)



Creo un usuario nuevo normal en el equipo.



Vemos como al intentar instalar una aplicación con dicho usuario se me piden credenciales de administrador.

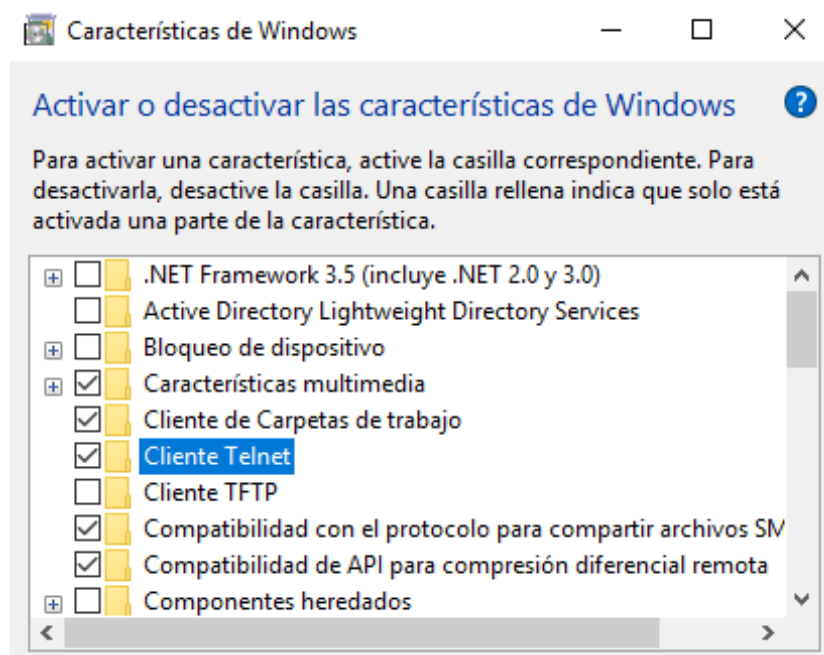


5. Instalar un modelo AAA en dicho router R_XX para permitir que otro usuario además del router pueda acceder con perfil de administrador desde el equipo de Teletrabajo. Dichos usuarios estarán autenticados de manera local en el propio router. Comprueba su funcionamiento.

Configuro la triple A en local y creo al usuario eduardo con nivel de privilegios 15 para acceder con él desde el equipo de TELETRABAJO-G.

```
R_42-F#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R_42-F(config)#aaa new-model
R_42-F(config)#aaa authentication login default local
R_42-F(config)#enable secret inves
R_42-F(config)#username eduardo privilege 15 secret inves
```


Instalo el cliente Telnet en el equipo y accedo al router con el usuario creado en el mismo.



```
C:\> Seleccíon Símboí del sistema

Microsoft Windows [Versíon 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\edu>telnet 80.42.0.1_
```

 Telnet 80.42.0.1

```
User Access Verification

Username: eduardo
Password:

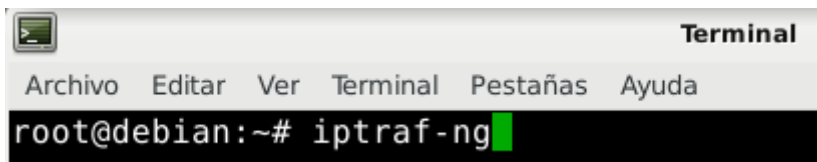
R_42-F>en
Password:
R_42-F#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_42-F(config)#
```

6. Instalar una herramienta de monitorización de la red en la zona DMZ de la empresa. Comprueba su funcionamiento.

Instalo iptraf.

```
root@debian:~# apt-get install iptraf
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  iptraf-ng
```

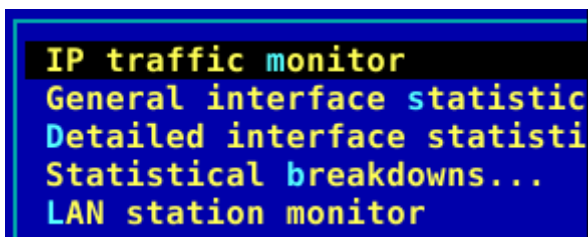
Empiezo a monitorizar.



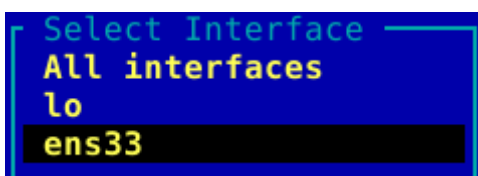
Terminal

Archivo Editar Ver Terminal Pestañas Ayuda

```
root@debian:~# iptraf-ng
```

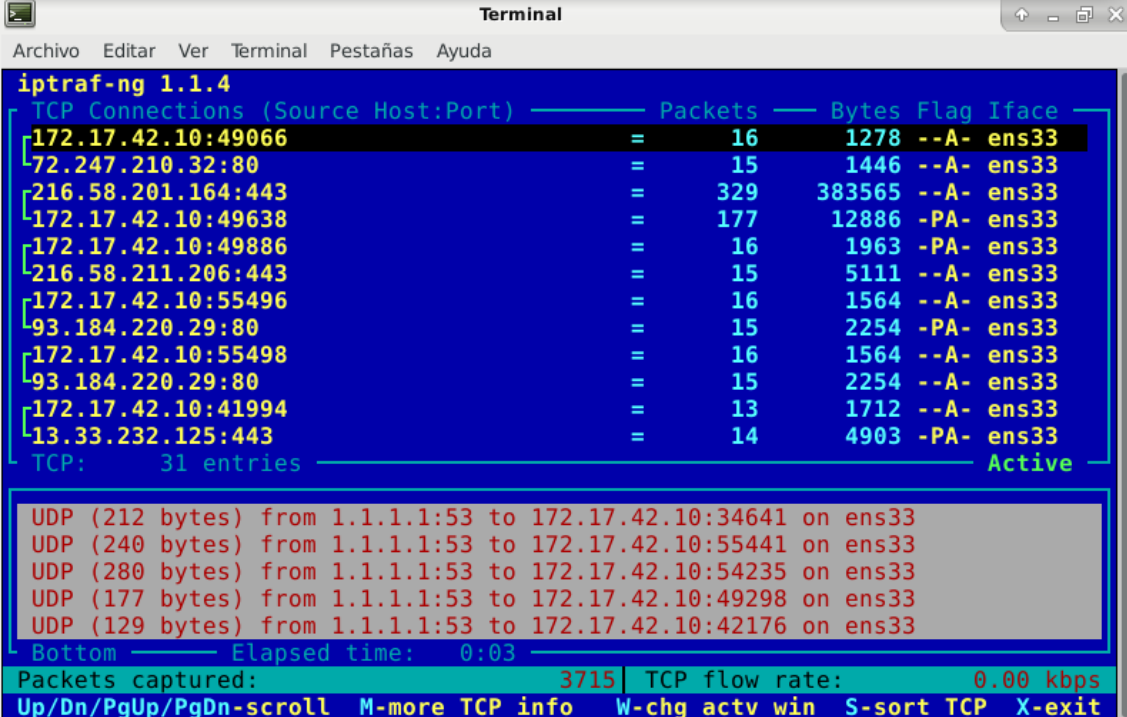


```
IP traffic monitor
General interface statistic
Detailed interface statisti
Statistical breakdowns...
LAN station monitor
```



```
Select Interface
All interfaces
lo
ens33
```

Vemos como detecta todo el tráfico.

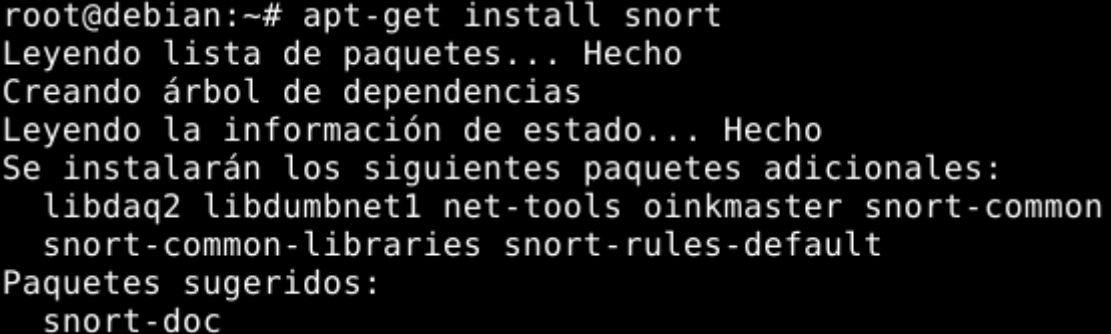


```
iptraf-ng 1.1.4
TCP Connections (Source Host:Port)  Packets  Bytes  Flag  Iface
172.17.42.10:49066                  =    16   1278  --A-  ens33
72.247.210.32:80                   =    15   1446  --A-  ens33
216.58.201.164:443                 =   329 383565 --A-  ens33
172.17.42.10:49638                 =   177  12886 -PA-  ens33
172.17.42.10:49886                 =    16   1963 -PA-  ens33
216.58.211.206:443                 =    15   5111 --A-  ens33
172.17.42.10:55496                 =    16   1564 --A-  ens33
93.184.220.29:80                   =    15   2254 -PA-  ens33
172.17.42.10:55498                 =    16   1564 --A-  ens33
93.184.220.29:80                   =    15   2254 --A-  ens33
172.17.42.10:41994                 =    13   1712 --A-  ens33
13.33.232.125:443                  =    14   4903 -PA-  ens33
TCP:      31 entries                Active

UDP (212 bytes) from 1.1.1.1:53 to 172.17.42.10:34641 on ens33
UDP (240 bytes) from 1.1.1.1:53 to 172.17.42.10:55441 on ens33
UDP (280 bytes) from 1.1.1.1:53 to 172.17.42.10:54235 on ens33
UDP (177 bytes) from 1.1.1.1:53 to 172.17.42.10:49298 on ens33
UDP (129 bytes) from 1.1.1.1:53 to 172.17.42.10:42176 on ens33
Bottom      Elapsed time:  0:03
Packets captured: 3715 | TCP flow rate: 0.00 kbps
Up/Dn/PgUp/PgDn-scroll  M-more TCP info  W-chg actv win  S-sort TCP  X-exit
```

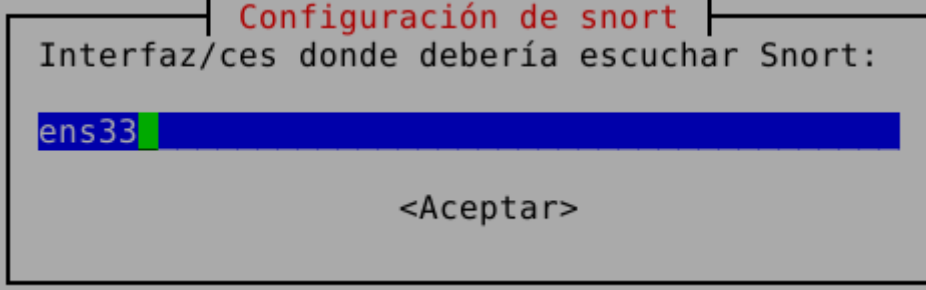
7. Instalar una herramienta IDS o IPS en el equipo indicado en el escenario. Comprueba su funcionamiento.

Instalo Snort en el equipo SERV-LINUX-C.

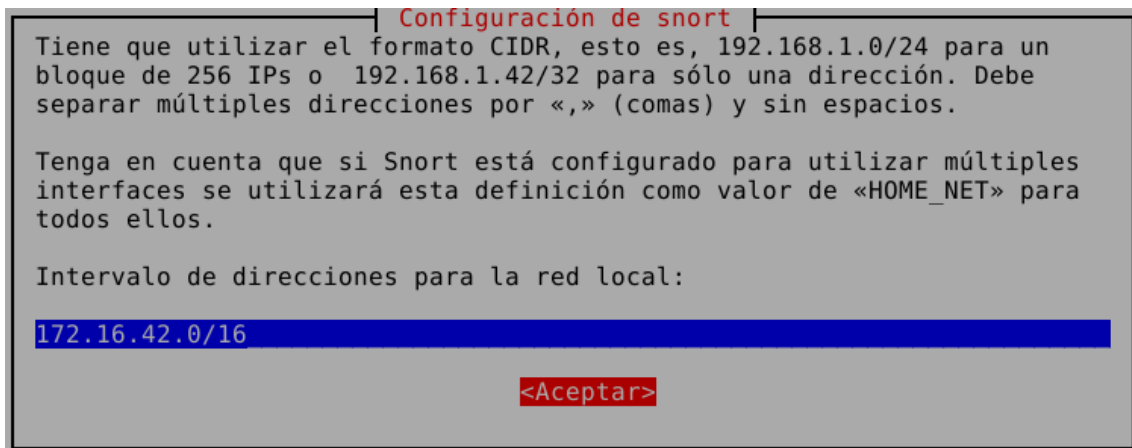


```
root@debian:~# apt-get install snort
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
 libdaq2 libdumbnet1 net-tools oinkmaster snort-common
 snort-common-libraries snort-rules-default
Paquetes sugeridos:
 snort-doc
```

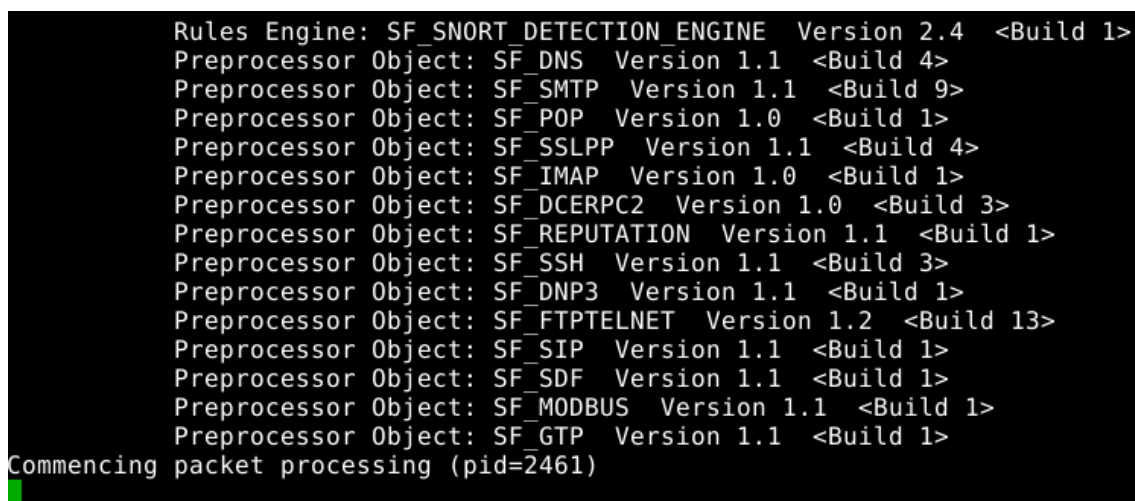
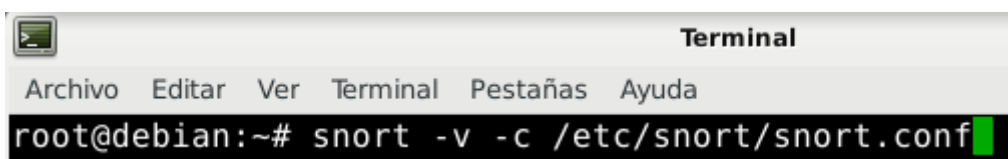
Escuchará por la interfaz que viene del exterior.



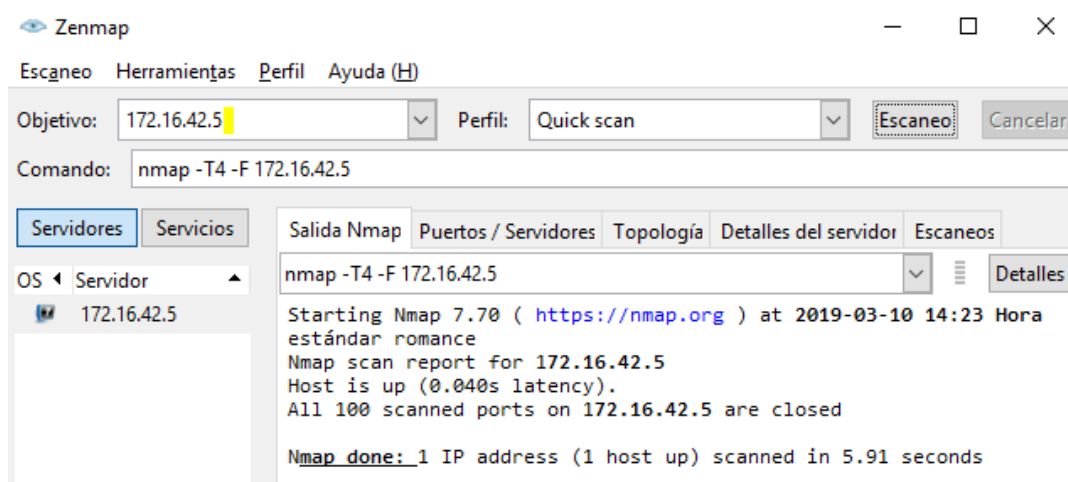
```
Configuración de snort
Interfaz/cas donde debería escuchar Snort:
ens33
<Aceptar>
```



Lo pongo en funcionamiento.



Hago un escaneo de puertos a SERV-LINUX-C desde el equipo TELETRABAJO-G.



Vemos como es detectado por la herramienta.

```
03/10-14:23:49.491299 80.42.0.20:54007 -> 172.16.42.5:465
TCP TTL:39 TOS:0x0 ID:17973 IpLen:20 DgmLen:44
*****S* Seq: 0xDCB92BC5 Ack: 0x0 Win: 0x400 TcpLen: 24
TCP Options (1) => MSS: 1460

03/10-14:23:49.491308 172.16.42.5:465 -> 80.42.0.20:54007
TCP TTL:64 TOS:0x0 ID:64513 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0 Ack: 0xDCB92BC6 Win: 0x0 TcpLen: 20

03/10-14:23:49.524574 fe80::6c88:b03e:b051:a06c:546 -> ff02::1:2:547
UDP TTL:1 TOS:0x0 ID:0 IpLen:40 DgmLen:134
Len: 86

03/10-14:23:50.718218 172.16.42.5:56161 -> 178.255.228.77:123
UDP TTL:64 TOS:0x10 ID:59460 IpLen:20 DgmLen:76 DF
Len: 48
```

Cuando pulsamos Control + C vemos las estadísticas de todo el tráfico que ha detectado.

```
Stream statistics:
    Total sessions: 206
    TCP sessions: 202
    UDP sessions: 4
    ICMP sessions: 0
    IP sessions: 0
    TCP Prunes: 0
    UDP Prunes: 0
    ICMP Prunes: 0
    IP Prunes: 0
TCP StreamTrackers Created: 202
TCP StreamTrackers Deleted: 202
```

UD 3.- Implantación de técnicas de acceso remoto. Seguridad perimetral.

8. Instalar y configurar un servidor de acceso VPN en el equipo indicado en el escenario. Elegir un protocolo seguro a nivel de enlace o de red.

Instalo PPTP en el equipo indicado.

```
root@debian:~# apt-get install pptpd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Configuro la IP local del servidor y las que voy a dar a los clientes en el fichero /etc/pptpd.conf.

```
localip 192.168.42.1
remoteip 192.168.42.50,192.168.42.55
```

Nombre de la conexión en el fichero /etc/ppp/pptpd-options.

```
# Authentication

# Name of the local system for authentication purposes
# (must match the second field in /etc/ppp/chap-secrets entries)
name PPTP-EMPRESA
```

Creo a los usuarios que se podrán conectar a la VPN en el fichero /etc/ppp/chap-secrets.

```
# Secrets for authentication using CHAP
# client      server      secret  IP addresses

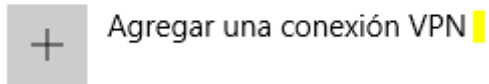
eduardo      PPTP-EMPRESA  inves   *
pepe         PPTP-EMPRESA  inves   *
```

Reinicio el servicio y ya está configurado.

```
root@debian:~# service pptpd restart
root@debian:~# service pptpd status
● pptpd.service - PoPToP Point to Point Tunneling Server
   Loaded: loaded (/lib/systemd/system/pptpd.service; disabled; vendor preset:
   Active: active (running) since Mon 2019-03-11 10:57:38 CET; 4s ago
```

Agrego la conexión VPN en el equipo de TELETRABAJO-G.

VPN



Agregar una conexión VPN

Proveedor de VPN
Windows (integrado) ▼

Nombre de conexión
PPTP-EMPRESA

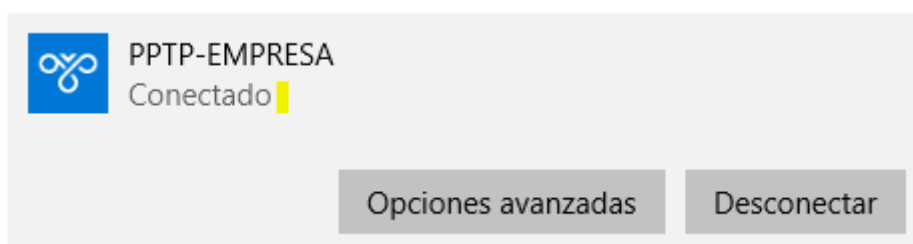
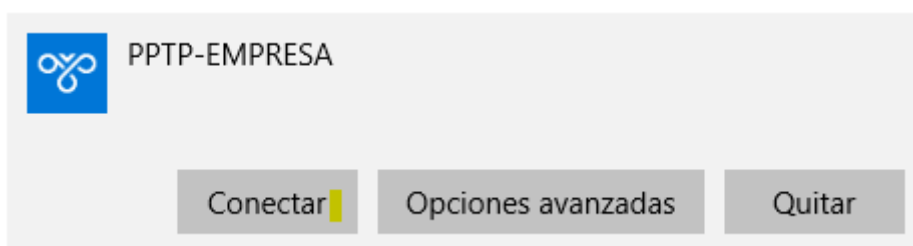
Nombre de servidor o dirección
192.168.42.1

Tipo de VPN
Protocolo de túnel punto a punto (PPTP) ▼


Tipo de información de inicio de sesión
Nombre de usuario y contraseña ▼

Nombre de usuario (opcional)
eduardo

Me conecto.



Observamos la IP que se me ha asignado.

 Símbolo del sistema

```
Adaptador PPP PPTP-EMPRESA:

  Sufijo DNS específico para la conexión. . . :
  Descripción . . . . . : PPTP-EMPRESA
  Dirección física. . . . . :
  DHCP habilitado . . . . . : no
  Configuración automática habilitada . . . : sí
  Dirección IPv4. . . . . : 192.168.42.50(Preferido)
  Máscara de subred . . . . . : 255.255.255.255
  Puerta de enlace predeterminada . . . . . : 0.0.0.0
  Servidores DNS. . . . . : 1.1.1.1
                               1.0.0.1
  NetBIOS sobre TCP/IP. . . . . : habilitado
```

Vemos cómo podemos hacer ping al equipo A situado en la red interna de la empresa.

```
C:\Users\edu>ping 192.168.42.10

Haciendo ping a 192.168.42.10 con 32 bytes de datos:
Respuesta desde 192.168.42.10: bytes=32 tiempo=18ms TTL=127
Respuesta desde 192.168.42.10: bytes=32 tiempo=15ms TTL=127
Respuesta desde 192.168.42.10: bytes=32 tiempo=16ms TTL=127
Respuesta desde 192.168.42.10: bytes=32 tiempo=18ms TTL=127

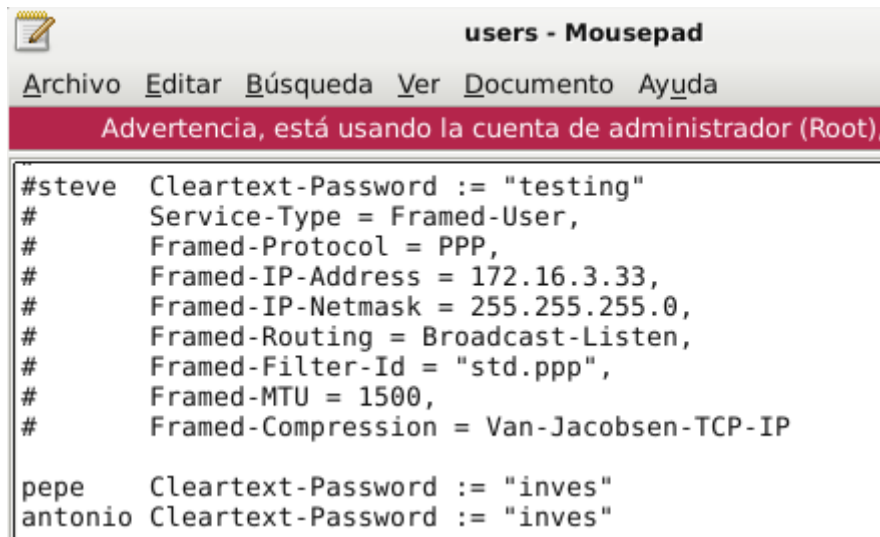
Estadísticas de ping para 192.168.42.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 15ms, Máximo = 18ms, Media = 16ms
```


9. Instalar y configurar un servidor de autenticación RADIUS en el equipo indicado en el escenario.

Instalo FreeRadius en el equipo indicado.

```
root@debian:~# apt-get install freeradius
```

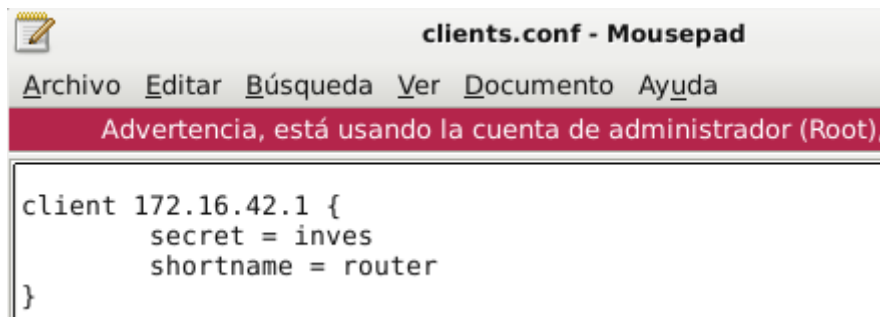
Configuro a los usuarios en el fichero /etc/freeradius/3.0/users



```
#steve Cleartext-Password := "testing"
#      Service-Type = Framed-User,
#      Framed-Protocol = PPP,
#      Framed-IP-Address = 172.16.3.33,
#      Framed-IP-Netmask = 255.255.255.0,
#      Framed-Routing = Broadcast-Listen,
#      Framed-Filter-Id = "std.ppp",
#      Framed-MTU = 1500,
#      Framed-Compression = Van-Jacobson-TCP-IP

pepe  Cleartext-Password := "inves"
antonio Cleartext-Password := "inves"
```

Configuro /etc/freeradius/3.0/clients.conf para poner la IP del router que será el cliente Radius.



```
client 172.16.42.1 {
    secret = inves
    shortname = router
}
```

Una vez configurado reinicio el servicio.

```
root@debian:~# service freeradius restart
root@debian:~# service freeradius status
● freeradius.service - FreeRADIUS multi-protocol policy server
   Loaded: loaded (/lib/systemd/system/freeradius.service; disabled; vendor
   Active: active (running) since Mon 2019-03-11 12:04:12 CET; 4s ago
```

10. Comprobar que un usuario situado en el equipo Teletrabajo puede acceder a la red empresarial.

Configuro el router para la autenticación de acceso mediante Radius.

```
R_42-F(config)#aaa new-model
R_42-F(config)#aaa authentication login default group radius local
R_42-F(config)#aaa authentication enable default group radius enable
R_42-F(config)#ip radius source-interface fa1/0
R_42-F(config)#radius-server host 172.16.42.5 auth-port 1812 key inves
R_42-F(config)#end
```

```
R_42-F(config)#aaa authorization exec default local
R_42-F(config)#username pepe privilege 15 password 0 inves
R_42-F(config)#username antonio privilege 15 password 0 inves
```

Accedo a la administración del router desde el equipo TELETRABAJO-G mediante Telnet con los usuarios configurados en el servidor Radius.

CA: Seleccionar Símbolo del sistema

```
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.
C:\Users\edu>telnet 172.16.42.1
```

CA: Telnet 172.16.42.1

```
User Access Verification
Username: antonio
Password:
R_42-F>
```

CA: Telnet 172.16.42.1

```
User Access Verification
Username: pepe
Password:
R_42-F>
```

UD 4.- Instalación y configuración de cortafuegos.

11. No permitir a los usuarios situados en el equipo DMZ acceder a la zona interna de la red ni a Internet.

Configuro la ACL en el router y la aplico a la interfaz adecuada.

```
R_42-F(config)#access-list 1 deny 172.17.42.0 0.0.255.255
R_42-F(config)#access-list 1 permit any
R_42-F(config)#int fa1/1
R_42-F(config-if)#ip access-group 1 in
```

Vemos como desde el equipo de la DMZ no puedo hacer ping hacia Internet ni hacia la red interna de la empresa.

```
root@debian:~# ping 80.42.0.10
PING 80.42.0.10 (80.42.0.10) 56(84) bytes of data.
From 172.17.42.1 icmp_seq=1 Packet filtered
From 172.17.42.1 icmp_seq=2 Packet filtered
From 172.17.42.1 icmp_seq=3 Packet filtered
From 172.17.42.1 icmp_seq=4 Packet filtered
^C
--- 80.42.0.10 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3007ms

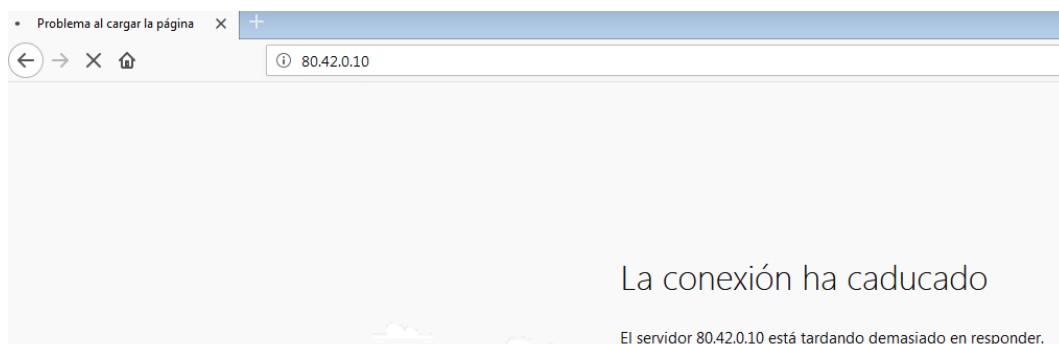
root@debian:~# ping 192.168.42.10
PING 192.168.42.10 (192.168.42.10) 56(84) bytes of data.
From 172.17.42.1 icmp_seq=1 Packet filtered
From 172.17.42.1 icmp_seq=2 Packet filtered
From 172.17.42.1 icmp_seq=3 Packet filtered
From 172.17.42.1 icmp_seq=4 Packet filtered
^C
--- 192.168.42.10 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3006ms
```

12. Permitir a los usuarios situados en el equipo A no acceder a Internet y permitir a los usuarios situados en el equipo B sólo realizar http en Internet.

Regla IPTABLES en SERV_LINUX-C para el equipo A.

```
root@debian:~# iptables -A FORWARD -s 192.168.42.10/24 -d 80.42.0.0/24 -j DROP
```

Vemos como este equipo no puede salir a Internet.



```
cmd - Acceso directo
Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\System32>ping 80.42.0.10

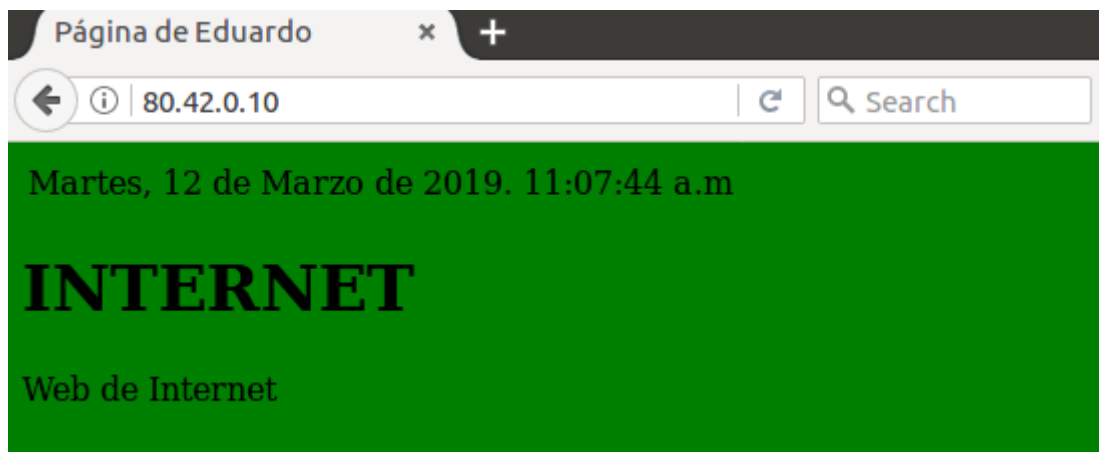
Haciendo ping a 80.42.0.10 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 80.42.0.10:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

Reglas IPTABLES en SERV_LINUX-C para el equipo B.

```
root@debian:~# iptables -A FORWARD -s 192.168.42.20/24 -i ens37 -p tcp
--dport 80 -j ACCEPT
root@debian:~#
root@debian:~# iptables -A FORWARD -s 192.168.42.20/24 -i ens37 -j DROP
```

Vemos cómo este equipo puede acceder a la página Web de Internet.



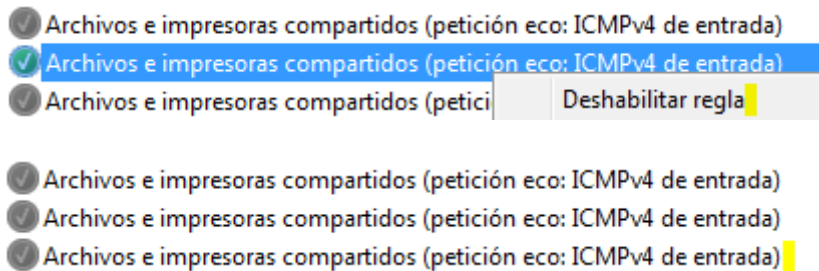
Pero no puede hacer por ejemplo ping.

```
edu@ubuntu: ~
edu@ubuntu:~$ ping 80.42.0.10
PING 80.42.0.10 (80.42.0.10) 56(84) bytes of data.
```

13. No permitir el protocolo ICMP en los equipos A y B de la red interna (utiliza su cortafuegos personal).

Equipo A.

Deshabilito la regla que permite el ICMP en las opciones avanzadas del Firewall de Windows.



Este equipo ya no responde al ICMP.

```
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
root@debian:~# ping 192.168.42.10
PING 192.168.42.10 (192.168.42.10) 56(84) bytes of data.
■
```

Equipo B.

Deshabilito el ICMP con una regla IPTABLES.

```
edu@ubuntu: ~
edu@ubuntu:~$ sudo iptables -A INPUT -i ens33 -p icmp -j DROP
```

El equipo ya no responde al ICMP.

```
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
root@debian:~# ping 192.168.42.20
PING 192.168.42.20 (192.168.42.20) 56(84) bytes of data.
■
```

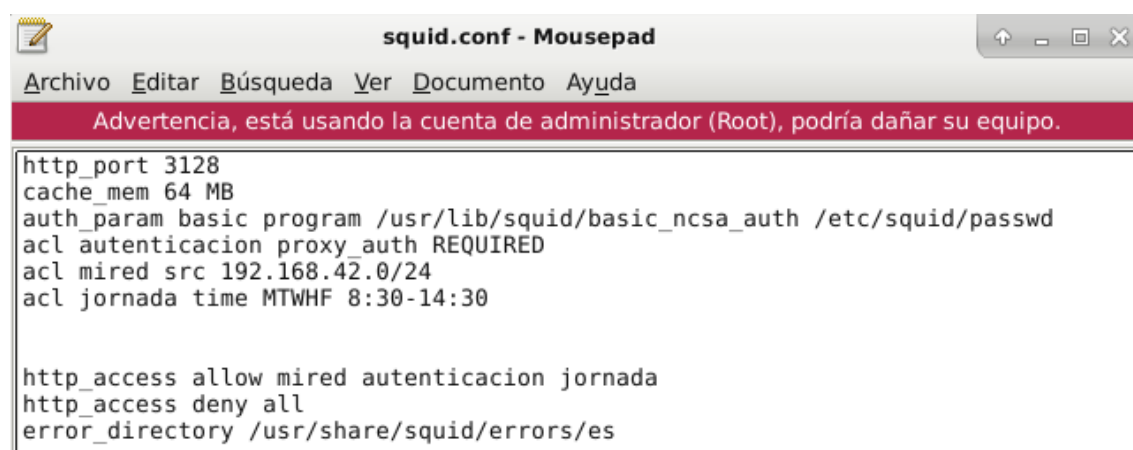
UD 5.- Instalación y configuración de servidores “proxy”.

14. Permitir en el servidor “proxy-caché” del escenario navegar en Internet sólo la jornada de mañana de lunes a viernes. Autenticarse en dicho “proxy-caché” para poder navegar por Internet. Asimismo crear una auditoria del uso del servidor “proxy-caché” y monitoriza su actividad.

Instalo Squid en el equipo correspondiente.

```
root@debian:~# apt-get install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Configuro su archivo de configuración /etc/squid/squid.conf con las reglas pertinentes.



```
squid.conf - Mousepad
Archivo Editar Búsqueda Ver Documento Ayuda
Advertencia, está usando la cuenta de administrador (Root), podría dañar su equipo.
http_port 3128
cache_mem 64 MB
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwd
acl autenticacion proxy_auth REQUIRED
acl mired src 192.168.42.0/24
acl jornada time MTWHF 8:30-14:30

http_access allow mired autenticacion jornada
http_access deny all
error_directory /usr/share/squid/errors/es
```

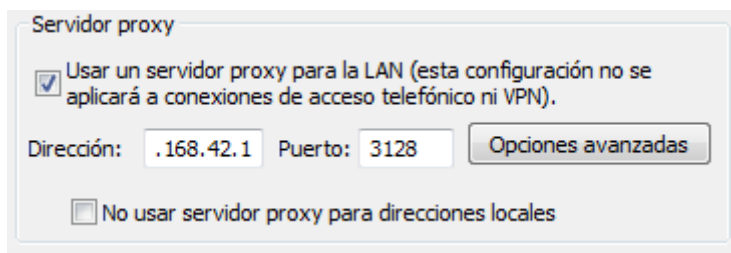
Creo al usuario que tendrá permisos de acceso al proxy.

```
root@debian:~# htpasswd -c /etc/squid/passwd eduardo
New password:
Re-type new password:
Adding password for user eduardo
```

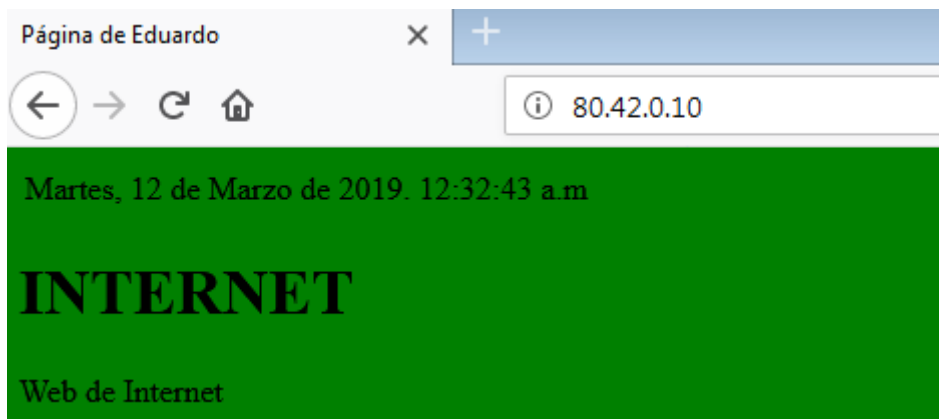
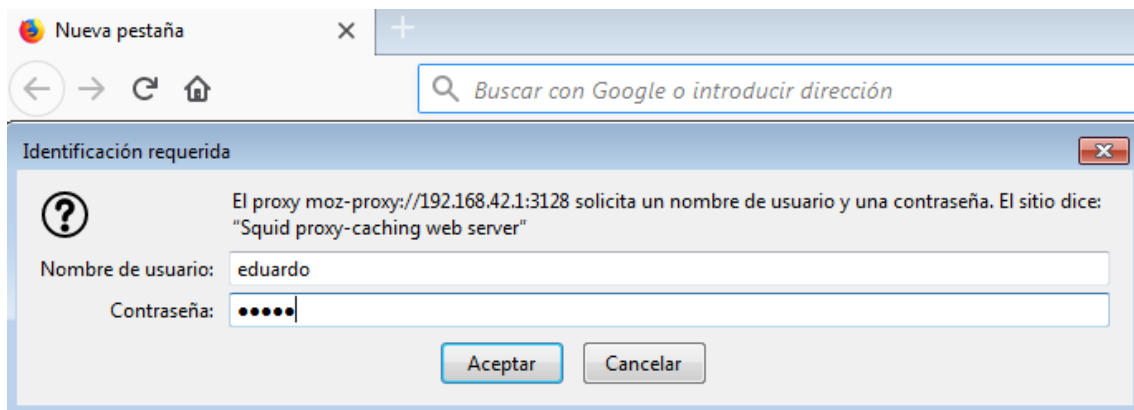
Reiniciamos el servicio.

```
root@debian:~# service squid restart
root@debian:~# service squid status
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated; vendor preset: enabled)
   Active: active (running) since Tue 2019-03-12 12:25:33 CET; 17s ago
```

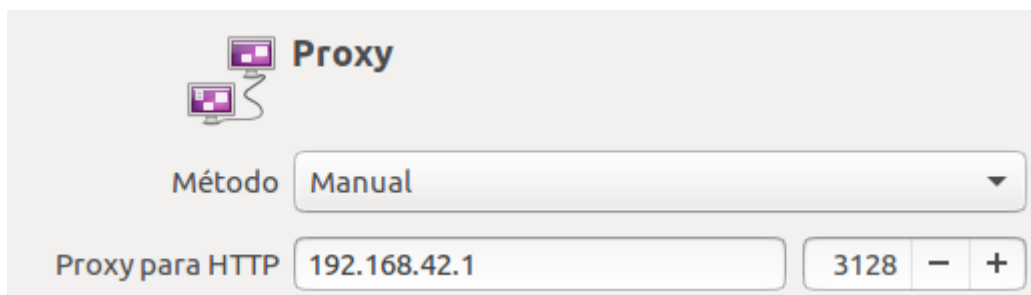
Configuración del cliente A para utilizar el proxy.



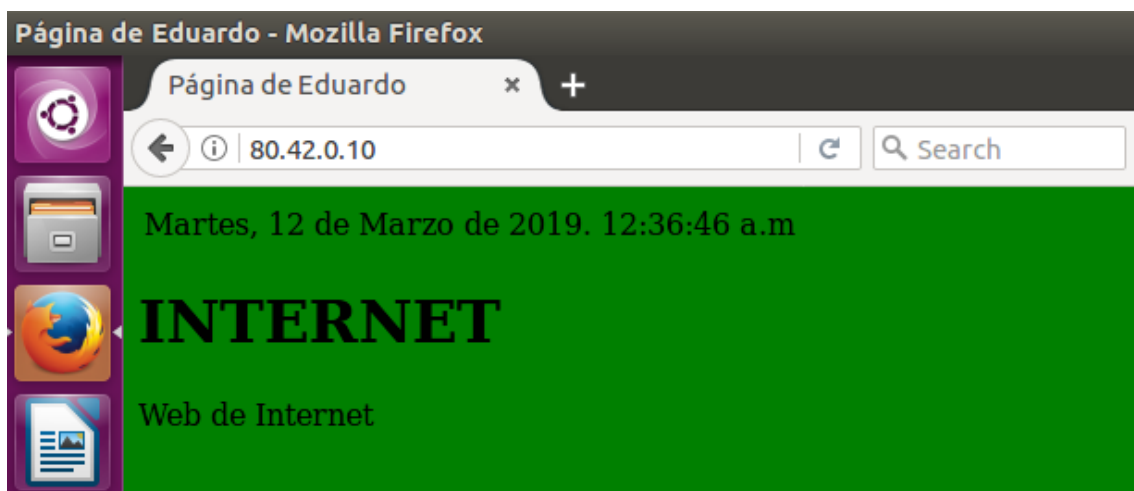
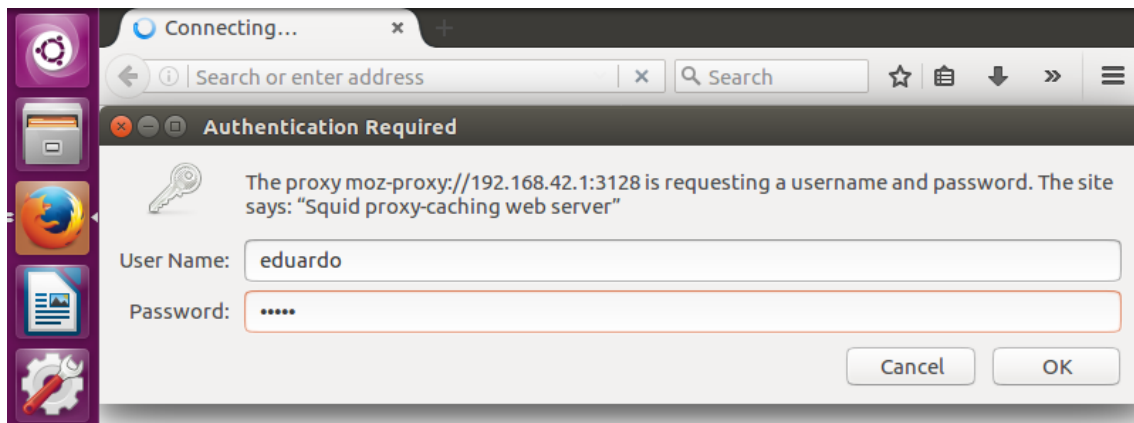
Vemos como al acceder al navegador ya se nos solicitan las credenciales.



Configuración del cliente B para utilizar el proxy.



Vemos como al acceder al navegador ya se nos solicitan las credenciales.



Auditoría de acceso al proxy.

Instalo Sarg.

```
root@debian:~# apt-get install sarg
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```


Configuro el fichero de configuración /etc/sarg/sarg.conf.

```
sarg.conf - Mousepad
Archivo Editar Búsqueda Ver Documento Ayuda
Advertencia, está usando la cuenta de administrador (Root),

# TAG:  output_dir
#      The reports will be saved in that directory
#      sarg -o dir
#
# output_dir /var/lib/sarg
output_dir /var/www/html/squid-reports
```

Genero el informe.

```
root@debian:~# /usr/bin/sarg
```

Lo podemos visualizar desde un cliente.

SARG report for 12 mar 2019

192.168.42.1/squid-reports/12Mar2019-12Mar2019/index.html

SARG Squid Analysis Report Generator

Squid User Access Reports
Period: 12 mar 2019
Sort: bytes, reverse
Top users

Top sites
Sites & Users
Denied accesses
Authentication Failures

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILLISEC	%TIME
1	eduardo	150	466.85K	60.56%	87.82% 12.18%	01:04:52	3,892,471	100.00%
2	192.168.42.10	46	185.56K	24.07%	100.00% 0.00%	00:00:00	2	0.00%
3	192.168.42.20	29	118.42K	15.36%	100.00% 0.00%	00:00:00	5	0.00%
TOTAL		225	770.83K		92.62% 7.38%	01:04:52	3,892,478	
AVERAGE		75	256.94K			00:21:37	1,297,492	

Generated by sarg-2.3.10 Apr-12-2015 on 12/mar/2019-13:14

Monitorización de la actividad.

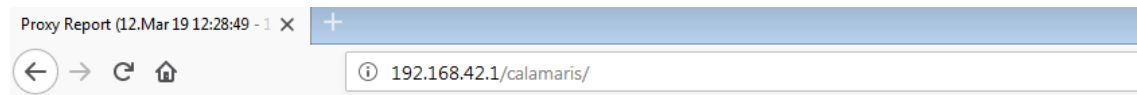
Instalo Calamaris.

```
root@debian:~# apt-get install calamaris
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Genero el informe.

```
root@debian:~# cat /var/log/squid/access.log | calamaris -a -F html > /var/www/html/calamaris/index.html
```

Ya podemos verlo desde un cliente.



Proxy Report

Report period: 12.Mar 19 12:28:49 - 12.Mar 19 13:15:04
Generated at: 12.Mar 19 13:20:38

Table of Content / Overview			
Summary	-	-	-
Incoming requests by method	most requested method	GET	152 Requests
Incoming UDP-requests by status	-	-	no requests found
Incoming TCP-requests by status	most incoming request by status to	ERROR	157 Requests
Outgoing requests by status	most outgoing request to	DIRECT Fetch from Source	156 Requests
Outgoing requests by destination	most requested destination	DIRECT	156 Requests
Request-destinations by 2nd-level-domain	most requested 2nd-level-domain	<error>	160 Requests
Request-destinations by toplevel-domain	most requested toplevel-domain	<error>	160 Requests
TCP-Request-protocol	most requested protocol	<error>	160 Requests
Requested content-type	most requested content-type	<error>	160 Requests
Requested extensions	most requested extension	<error>	160 Requests
Incoming UDP-requests by host	-	-	no requests found
Incoming TCP-requests by host	most active host	192.168.42.10	245 Requests
Size Distribution Diagram	most requested object_size	1000-9999	204 Requests

UD 6.- Implantación de soluciones de alta disponibilidad.

15. Realiza un informe a entregar a la dirección de la empresa de cómo puedes mejorar la alta disponibilidad de la empresa, indicando su coste económico.

Podríamos mejorar la alta disponibilidad de la empresa implantando las siguientes medidas:

- El equipo de la DMZ podríamos sustituirlo por un NAS con 2 HD's en espejo mediante RAID.



Synology DS218J Servidor NAS Blanco
182€ SIN IVA 150,41€
★★★★★ 17 Opiniones | Review
Vendido por PcComponentes - 7 nuevos


Marca: Synology - P/N: DS218J | Cod. Artículo: 159404
Envío: Desde 5,25€ GRATIS con PcComponentes Premium
Cantidad: - 1 +
Disponibilidad: ¡En stock! ¡Recíbelo mañana! >
¿Recoges en tienda? Comprueba disponibilidad >
Financiación: 6, 12, 20, 30 y 40 meses. (Calcular cuota)

♥ Añadir al carrito Haz tu pregunta Comprar ?

☐ Extensión de garantía +3 años por 29,00 € info

- El servidor más fundamental de la empresa que es SERV_LINUX-C debe estar replicado, por si este cae que no nos quedemos sin servicios en la red interna. Con lo cual configuramos un bonding en las tarjetas de red de los servidores para que actúen conjuntamente, y si uno cae el otro nos siga ofreciendo salida hacia Internet.

Para ello podemos comprar 2 de estos servidores.



HP ProLiant MicroServer Gen10 AMD Opteron X3216/8GB
385€ SIN IVA 318,18€
★★★★★ 9 Opiniones | Review
Vendido por PcComponentes - 3 nuevos

Marca: HP - P/N: 873830-421 | Cod. Artículo: 139138
Envío: Desde 6,25€ GRATIS con PcComponentes Premium
Cantidad: - 1 +
Disponibilidad: ¡En stock! ¡Recíbelo mañana! >
¿Recoges en tienda? Comprueba disponibilidad >
Financiación: 6, 12, 20, 30 y 40 meses. (Calcular cuota)

♥ Añadir al carrito Haz tu pregunta Comprar ?

Twitter Facebook Google+ Email

Además debemos configurarle los discos duros replicados con un sistema RAID-1 para tener bien salvaguardados los datos en caso de caída de alguno de ellos.



Seagate BarraCuda 3.5" 1TB SATA3
44,03€ SIN IVA 36,39€
★★★★★ 2512 Opiniones | Review
Vendido por PcComponentes - 4 nuevos


Marca: Seagate - P/N: ST1000DM010 | Cod. Artículo: 111412
Envío: Desde 3,95€ GRATIS con PcComponentes Premium
Cantidad: - 1 +
Disponibilidad: ¡En stock! ¡Recíbelo mañana! >
¿Recoges en tienda? Comprueba disponibilidad >

☐ Recuperación de datos +1 año por 9,95 €+ Info

[Haz tu pregunta](#)

Añadir LG GH24NSD1 Grabadora DVD 24x Negra

- Por último debemos proteger los equipos de la empresa con un SAI por los posibles picos de tensión o cortes eléctricos.



APC Back-UPS 1400VA 230V
159€ SIN IVA 131,40€
★★★★★ 80 Opiniones | Review
Vendido por PcComponentes - 2 nuevos

Marca: APC - P/N: BX1400U-GR | Cod. Artículo: 80560
Envío: Desde 7,25€ GRATIS con PcComponentes Premium
Cantidad: - 1 +
Disponibilidad: ¡En stock! ¡Recíbelo mañana! >
¿Recoges en tienda? Comprueba disponibilidad >

Financiación: 6, 12, 20, 30 y 40 meses. (Calcular cuota)

☐ Extensión de garantía +3 años por 29,00 €+ Info

[Haz tu pregunta](#)

Añadir Kingston A400 SSD 120GB

Por lo tanto NAS 182 € + 2 Servidores 770 € + 6 Discos Duros 264.18 € + SAI 159 €; el coste económico de la alta disponibilidad en la empresa es de 1375,18 €.