

Seguridad Perimetral

(Firewall & Proxy)

Adrián Gómez Lois

Contenido

1. Obxectivos	3
2. Práctica A (Iptables)	4
3. Práctica B (Iptables).....	6
4. Práctica C (Iptables).....	10
5. Proxy - Squid.....	19
6. Conclusións	23

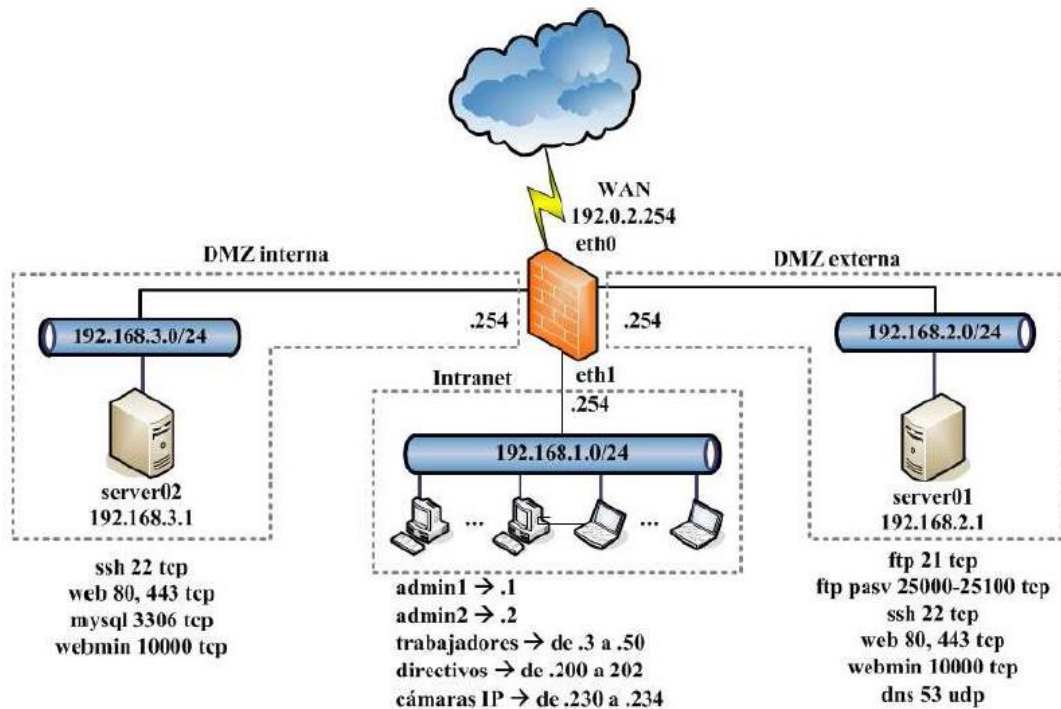
1. Obxectivos

Chagaráse a entender e traballar con regras iptables (netfilter) e o uso de Squid, un proxy de filtrado web e webcaché.

Distinguir os comentidos das cadeas que forman parte das taboas de iptables, crear diversas regras de filtrado, regras con estado. Iptables e extenso pero veremos o suficiente como para encamiñarse no seu uso básico.

Instalar e configurar de forma sinxela un proxy Squid e coñecer de este modo as diferencias entre un firewall e un proxy.

2. Práctica A (Iptables)



```
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Engadirase unha regra o final da cadea OUTPUT, que aceptará toda aquela conexión iniciada e establecida saínte.

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Engadirase unha regra o final da cadea INPUT, que aceptará toda aquela conexión iniciada e establecida entrante.

```
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 22 -j ACCEPT
```

Engadirase unha regra o final da cadea INPUT, que aceptará o tráfico novo aínda non establecido procedente da red 192.168.1.0/24 con destino o porto 22 de protocolo TCP (SSH por defecto).

```
iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -j ACCEPT
```

Engadirase unha regra o final da cadea INPUT, na que os paquetes recibidos pola interface **eth1** de tipo de protocolo ICMP con solicitudes echo sexan aceptados. (Habilita o echo entrante ICMP).

```
iptables -I INPUT 4 -s 192.168.3.0/24 -j REJECT --reject-with icmp-host-unreachable
```

Engade un número específico 4 na lista da cadea INPUT, que rechaze as solicitudes ICMP con un mensaxe "ICMP host unreachable" procedentes da rede 192.168.3.0/24.

```
iptables -A OUTPUT -p udp --dport 53 -d 80.58.32.97 -m state --state NEW -j ACCEPT
```

Engade unha regra o final da cadea OUTPUT, que permita todas as novas conexións de saída dirixidas a unha dirección IP concreta 80.58.32.97 polo porto 53 de protocolo UDP.

```
iptables -A OUTPUT -p tcp --dport 80 -d www.edu.xunta.es -j DROP
```

Engade unha regra o final da cadea OUTPUT, que descarte todas as conexións con destino a web “www.edu.xunta.es” polo porto 80 de protocolo TCP.

```
iptables -A FORWARD -p tcp --destination-port 80 -m iprange --src-range 192.168.1.3-192.168.1.50 -m state --state NEW -j ACCEPT
```

Engade unha regra o final da cadea FORWARD, que permita as conexións novas con destino o porto 80 en protocolo TCP que procedan dun determinado rango de rede 192.168.1.3-192.168.1.50.

```
iptables -A FORWARD -p tcp --destination-port 3306 -s 192.168.2.1 -d 192.168.3.1 -m state --state NEW -j ACCEPT
```

Engadirase unha regra o final da cadea FORWARD, que permita iniciar conexións novas que procedan da dirección IP 192.168.2.1 e se dirixan o destino 192.168.3.1 polo porto 3306 en protocolo TCP.

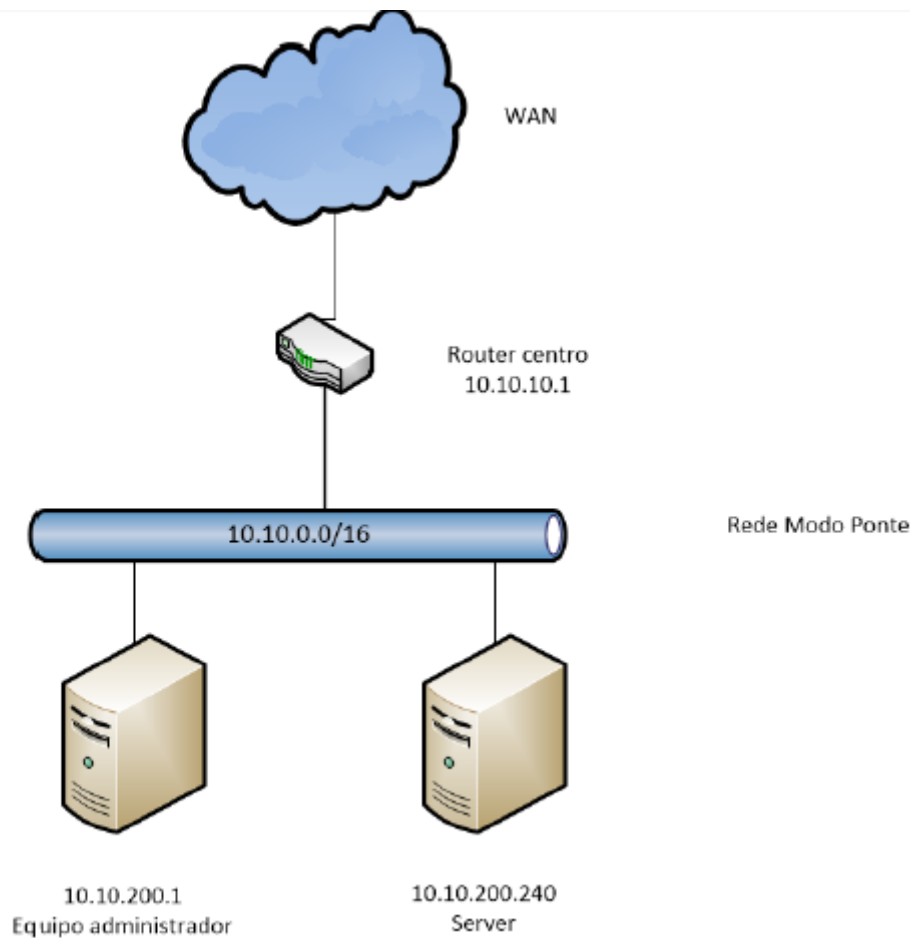
```
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.1.0/24 -j SNAT --to-source 192.0.2.254
```

Engadirase unha regra o final da cadea POSTROUTING dentro da taboa NAT, cambiará o orixen dos paquetes procedentes da rede 192.168.1.0/24, saíntes pola interface eth0 polo direccionamento 192.0.2.254. De forma que isto ocultará o direccionamento orixen da rede hacía o exterior.

```
iptables -t nat -A PREROUTING -p tcp -m tcp -m multiport -d 192.0.2.254 --dports 80,443 -j DNAT --to-destination 192.168.2.1
```

Engadirase unha regra o final da cadea PREROUTING dentro da taboa NAT, cambiará o direccionamento IP dirixido a rede 192.0.2.254 e que a súa vez usen os portos 80 e 443 (http e https) traballando en protocolo TCP, polo destino 192.168.2.1 antes de enrutar iste tráfico.

3. Práctica B (Iptables)



Comprobación de conexión previa hacía o servidor Apache iniciado.

IP Server: 10.0.0.17

IP Administración_1: 10.0.0.19

IP outro equipo da rede: 10.0.0.10

```

adrian@seadserver:~$ ifconfig
eth0: flags=4096<UP,BROADCAST,MULTICAST> mtu=1500
    Link encap:Ethernet  HWaddr 08:00:27:65:41:3d
    inet: 10.0.0.17  Bcast: 10.0.0.255  Mask: 255.255.255.0
    inet6: fe80::a00:27ff:fe65:413d/64  Scope: Link
    RX packets: 2220 errors: 0 dropped: 0 overruns: 0 frame: 0
    TX packets: 694 errors: 0 dropped: 0 overruns: 0 carrier: 0
    collisions: 0 long: 0 TX bytes: 1000
    RX bytes: 1429821 (1.4 MB)  TX bytes: 62339 (62.3 KB)

lo: flags=73<UP,LOOPBACK,RUNNING> mtu=65536
    Link encap: Bucle local
    inet: 127.0.0.1  Mask: 255.0.0.0
    inet6: ::1/128  Scope: Host
    RX packets: 32 errors: 0 dropped: 0 overruns: 0 frame: 0
    TX packets: 32 errors: 0 dropped: 0 overruns: 0 carrier: 0
    collisions: 0 long: 0 TX bytes: 2256 (2.2 KB)
    RX bytes: 2256 (2.2 KB)  TX bytes: 2256 (2.2 KB)

adrian@seadserver:~$
          
```

1. A política por defecto debe ser denegar todo o tráfico.

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

2. Debemos permitir as consultas DNS aos servidores DNS 8.8.8.8 e 8.8.4.4. ??

```
iptables -A OUTPUT -p udp --dport 53 -d 8.8.8.8,8.8.4.4 -m state --state NEW -j ACCEPT
iptables -A INPUT -p udp --sport 53 -s 8.8.8.8,8.8.4.4 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

3. Debemos permitir a navegación web tanto por http, como por https. ??

```
iptables -A OUTPUT -p tcp -m multiport --dport 80,443 -m state --state NEW -j ACCEPT
iptables -A INPUT -p tcp -m multiport --sport 80,443 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

4. Debemos permitir a administración do server por SSH para calquer equipo.

```
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

5. Debemos permitir a administración do server por SSH pero só ao equipo de Administración.

```
iptables -A INPUT -p tcp -s 10.0.0.19 --dport 22 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p tcp -d 10.0.0.19 --sport 22 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

6. Debemos permitir o acceso ás páxinas aloxadas no server.

```
iptables -A INPUT -p tcp -d 10.0.0.17 --dport 80 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p tcp -s 10.0.0.17 --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

7. Elimina a regra do punto 4, para que a do punto 5 faga efecto. ok

Listamos as regras polo número de lista:

```
iptables -L --line-numbers
```

Eliminamos a o número de orde correspondete a cadea en cuestión.

```
iptables -D INPUT 3
iptables -D OUTPUT 3
```

Mostrar todas as regras iptables de forma detallada (-v) e que mostre o número de liña (--line-numbers).

`iptables -L -v --line-numbers` | more

```

root@ubuntusead: /home/adrian
root@ubuntusead:/home/adrian# iptables -L -n -v --line-numbers
Chain INPUT (policy DROP 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
1      0      0 ACCEPT    udp  --  *      *       8.8.8.8              0.0.0.0/0          udp spt:
53 state RELATED,ESTABLISHED
2      0      0 ACCEPT    udp  --  *      *       8.8.4.4              0.0.0.0/0          udp spt:
53 state RELATED,ESTABLISHED
3      0      0 ACCEPT    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0          multipor
t sports 80,443 state RELATED,ESTABLISHED
4      0      0 ACCEPT    tcp  --  *      *       10.0.0.19            0.0.0.0/0          tcp dpt:
22 state NEW
5      0      0 ACCEPT    tcp  --  *      *       0.0.0.0/0            10.0.0.17          tcp dpt:
80 state NEW

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination

Chain OUTPUT (policy DROP 16 packets, 1072 bytes)
num  pkts bytes target    prot opt in     out     source               destination
1      0      0 ACCEPT    udp  --  *      *       0.0.0.0/0            8.8.8.8            udp dpt:
53 state NEW
2      0      0 ACCEPT    udp  --  *      *       0.0.0.0/0            8.8.4.4            udp dpt:
53 state NEW
3      0      0 ACCEPT    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0          multipor
t dports 80,443 state NEW
4      0      0 ACCEPT    tcp  --  *      *       0.0.0.0/0            10.0.0.19          tcp spt:
22 state RELATED,ESTABLISHED
5      0      0 ACCEPT    tcp  --  *      *       10.0.0.17            0.0.0.0/0          tcp spt:
80 state RELATED,ESTABLISHED
root@ubuntusead:/home/adrian#

```

Ficheiro /etc/iptables/rules.v4 (iptables-persistent).

```

root@ubuntusead: /home/adrian
GNU nano 2.2.6      Archivo: /etc/iptables/rules.v4
# Generated by iptables-save v1.4.21 on Wed May 25 19:29:49 2016
*nat
:PREROUTING ACCEPT [1:78]
:INPUT ACCEPT [1:78]
:OUTPUT ACCEPT [16:1072]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed on Wed May 25 19:29:49 2016
# Generated by iptables-save v1.4.21 on Wed May 25 19:29:49 2016
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT DROP [16:1072]
-A INPUT -s 8.8.8.8/32 -p udp -m udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 8.8.4.4/32 -p udp -m udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m multiport --sports 80,443 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 10.0.0.19/32 -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A INPUT -d 10.0.0.17/32 -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT
-A OUTPUT -d 8.8.8.8/32 -p udp -m udp --dport 53 -m state --state NEW -j ACCEPT
-A OUTPUT -d 8.8.4.4/32 -p udp -m udp --dport 53 -m state --state NEW -j ACCEPT
-A OUTPUT -p tcp -m multiport --dports 80,443 -m state --state NEW -j ACCEPT
-A OUTPUT -d 10.0.0.19/32 -p tcp -m tcp --sport 22 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -s 10.0.0.17/32 -p tcp -m tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Wed May 25 19:29:49 2016

^G Ver ayuda      ^O Guardar      ^R Leer Fich     ^Y RePág.      ^K Cortar Texto  ^C Pos actual
^X Salir          ^J Justificar   ^W Buscar        ^V Pág. Sig.    ^U PegarTxt      ^T Ortografía

```


Intento de conexión SSH dunha dirección IP SI permitida, equipo de “Administración”.

```

adrian@ubuntusead: ~
adrian@ubuntusead:~$ hostname
ubuntusead
adrian@ubuntusead:~$ ifconfig
eth0      link encap:Ethernet  direcciónHW 08:00:27:50:0b:9f
          Direc. inet:10.0.0.19  Difus.:10.0.0.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe50:b9f/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:3928 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:2839 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:2970932 (2.9 MB)  TX bytes:2825601 (2.8 MB)

lo
Link encap:Bucl
Direc. inet:127.0.0.1
Dirección inet6: ::1
ACTIVO BUCLE FU
Paquetes RX:288
Paquetes TX:288
colisiones:0 lo
Bytes RX:24495

adrian@ubuntusead:~$ ssh tecnico1@10.0.0.17
tecnico1@seadserver:~$
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 4.2.0-27-generic x86_64)
 * Documentation:  https://help.ubuntu.com/
System information as of Mon May 23 14:00:15 CEST 2016

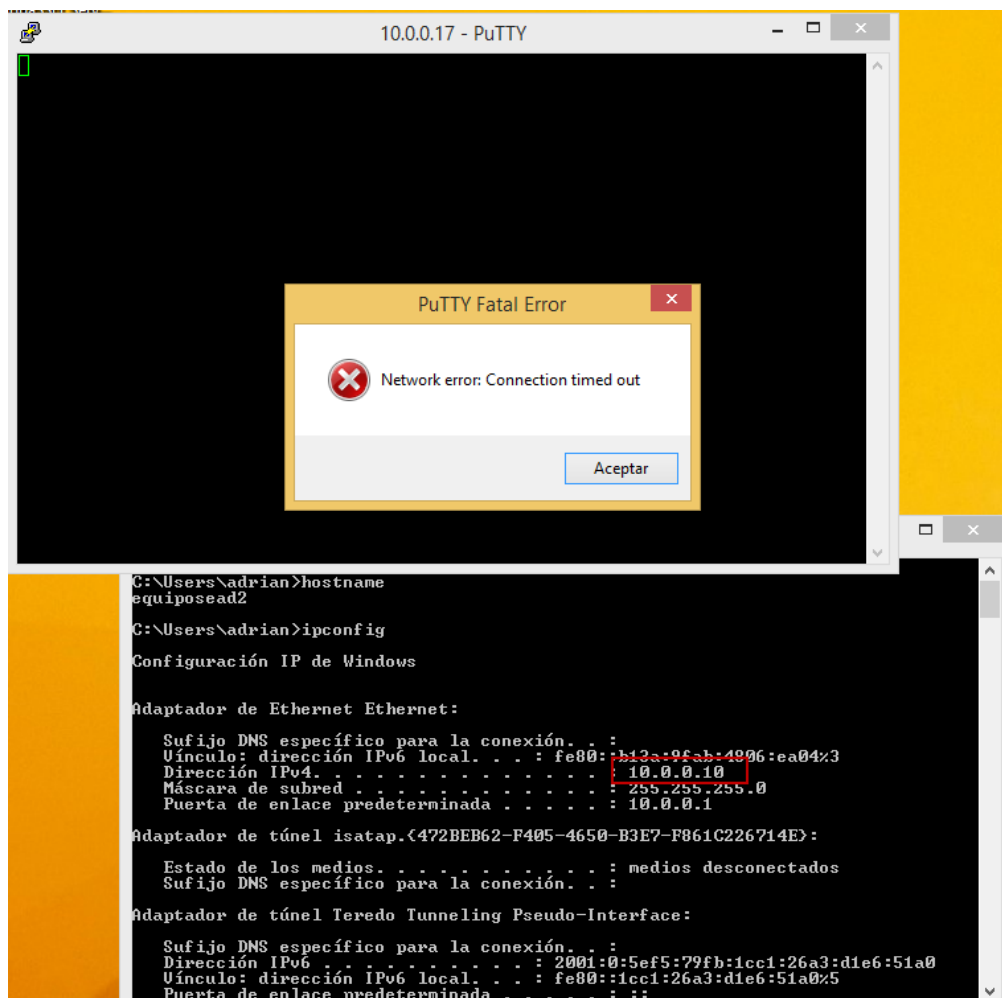
System load:  0.0          Processes:      87
Usage of /:   15.7% of 8.73GB Users logged in:   1
Memory usage: 8%          IP address for eth0: 10.0.0.17
Swap usage:  0%

Graph this data and manage this system at:
https://landscape.canonical.com/

Last login: Mon May 23 14:00:15 2016 from 10.0.0.19
tecnico1@seadserver:~$ whoami
tecnico1
tecnico1@seadserver:~$ hostname
seadserver
tecnico1@seadserver:~$

```

Intento de conexión SSH dunha dirección IP NON permitida.



```

10.0.0.17 - PuTTY
[
C:\Users\adrian>hostname
equiposead2
C:\Users\adrian>ipconfig
Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::b13a-9fab-4906:ea04%3
    Dirección IPv4. . . : 10.0.0.10
    Máscara de subred. . . : 255.255.255.0
    Puerta de enlace predeterminada. . . : 10.0.0.1

Adaptador de túnel isatap.{472BEB62-F405-4650-B3E7-F861C226714E}:

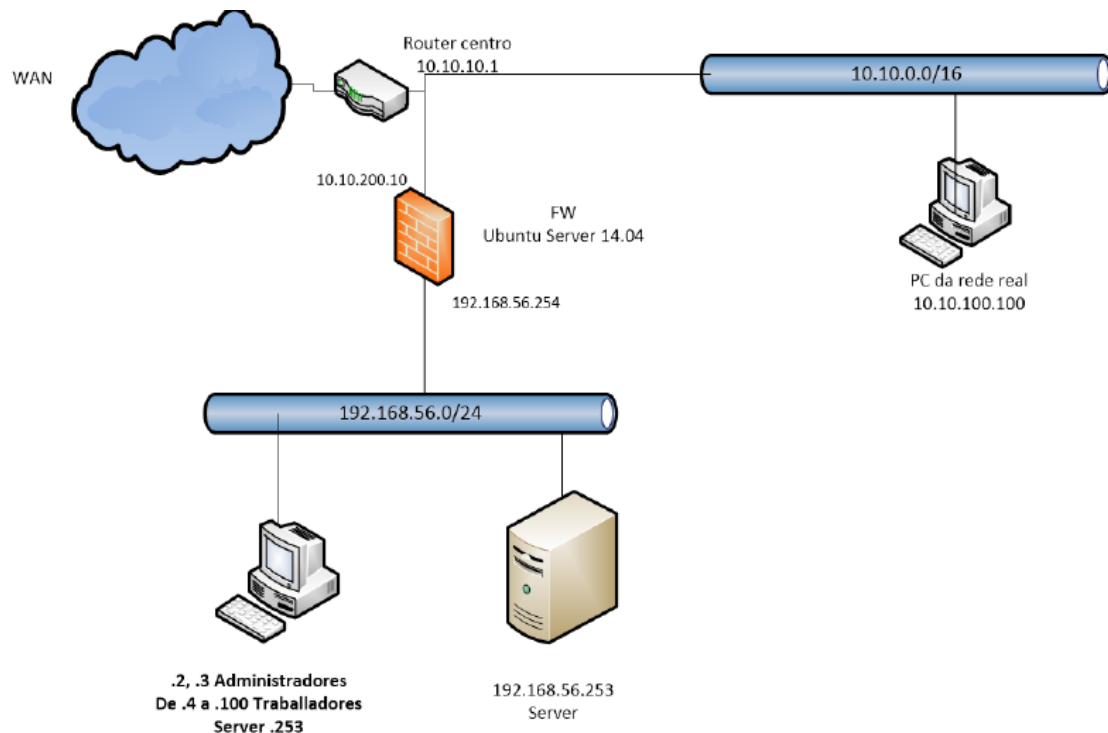
    Estado de los medios. . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de túnel Teredo Tunneling Pseudo-Interface:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv6. . . : 2001:0:5ef5:79fb:1cc1:26a3:d1e6:51a0
    Vínculo: dirección IPv6 local. . . : fe80::1cc1:26a3:d1e6:51a0%5
    Puerta de enlace predeterminada. . . :

```

4. Práctica C (Iptables)



Configuración IP do server 192.168.56.253 + Iptables sen ningunha regra.

```

ubuntu_server_sead [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

root@seadserver:/home/adrian# ifconfig eth0
eth0      Link encap:Ethernet  direcciónHW 08:00:27:65:41:3d
          Direc. inet:192.168.56.253  Difus.:192.168.56.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe65:413d/64  Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:71 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:103 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:9489 (9.4 KB)  TX bytes:23679 (23.6 KB)

root@seadserver:/home/adrian# ip route show
default via 192.168.56.254 dev eth0
192.168.56.0/24 dev eth0  proto kernel  scope link  src 192.168.56.253
root@seadserver:/home/adrian# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@seadserver:/home/adrian# _

```

Servidores Apache e SSH correndo no equipo server 192.168.56.253.

```

1256/ssh
tcp        0      0 0.0.0.0:445          0.0.0.0:*          ESCUCHAR
589/smbd
tcp        0      0 0.0.0.0:139         0.0.0.0:*          ESCUCHAR
589/smbd
tcp6       0      0 :::80              :::*              ESCUCHAR
1298/apache2
tcp6       0      0 :::22              :::*              ESCUCHAR
1256/ssh
tcp6       0      0 :::445             :::*              ESCUCHAR
589/smbd
tcp6       0      0 :::139             :::*              ESCUCHAR
589/smbd
tcp6       0      0 192.168.56.253:80   192.168.56.10:1196 TIME_WAIT
tcp6       0      0 192.168.56.253:80   192.168.56.10:1197 TIME_WAIT
udp        0      0 192.168.56.255:137  0.0.0.0:*          ESCUCHAR
986/nmbd
udp        0      0 192.168.56.253:137  0.0.0.0:*          ESCUCHAR
986/nmbd
udp        0      0 0.0.0.0:137        0.0.0.0:*          ESCUCHAR
986/nmbd
udp        0      0 192.168.56.255:138  0.0.0.0:*          ESCUCHAR
986/nmbd
udp        0      0 192.168.56.253:138  0.0.0.0:*          ESCUCHAR
986/nmbd
udp        0      0 0.0.0.0:138        0.0.0.0:*          ESCUCHAR
986/nmbd
root@seadserver:/home/adrian#
  
```

Configuración IP e proba de conexións iniciais no equipo Administradores 192.168.56.10

tecnico1@seadserver: ~
login as: tecnico1
tecnico1@192.168.56.253's password:
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 4.2.0-27-generic x86_64)

* Documentation: <https://help.ubuntu.com/>

System information as of Tue May 24 10:34:08 CEST 2016
System load: 0.0 Processes: 81
Usage of /: 15.7% of 8.73GB Users logged in: 0
Memory usage: 7% IP address for eth0: 192.168.56.253
Swap usage: 0%

Graph this data and manage this system at:
<https://landscape.canonical.com/>

Last login: Mon May 23 14:11:21 2016 from 10.0.0.19
tecnico1@seadserver:~\$ hostname
seadserver
tecnico1@seadserver:~\$

C:\Windows\system32\cmd.exe
C:\Users\Adrian>ipconfig
Configuración IP de Windows
Adaptador de Ethernet Ethernet:
Sufijo DNS específico para la conexión. . . : fe80::b13a:9fab:4806:ea04x3
Vínculo de dirección IPv6 local. . . : fe80::b13a:9fab:4806:ea04x3
Dirección IPv4. : 192.168.56.10
Máscara de subred. : 255.255.255.0
Puerta de enlace predeterminada. : 192.168.56.254
Adaptador de túnel isatap.{472BEB62-F405-4650-B3E7-F861C226714E}:
Estado de los medios. : medios desconectados
Sufijo DNS específico para la conexión. . . :
Adaptador de túnel Teredo Tunneling Pseudo-Interface:
Estado de los medios. : medios desconectados
Sufijo DNS específico para la conexión. . . :
C:\Users\Adrian>

Apache2 Ubuntu Default Page...
192.168.56.253
Buscar

Apache2 Ubuntu Default Page
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Equipo router + firewall:

eth0=192.168.56.254 (rede interna).

eth1=10.0.0.15 (IP pública).

```

root@ubuntusead: /home/adrian# ifconfig
eth0      Link encap:Ethernet  direcciónHW 08:00:27:64:7d:2b
          Direc. inet:192.168.56.254  Difus.:192.168.56.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe64:7d2b/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:758 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:208 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colatX:1000
          Bytes RX:97478 (97.4 KB)  TX bytes:30301 (30.3 KB)

eth1      Link encap:Ethernet  direcciónHW 08:00:27:cb:45:1b
          Direc. inet:10.0.0.15  Difus.:10.0.0.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe64:451b/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:1163 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:181 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colatX:1000
          Bytes RX:80614 (80.6 KB)  TX bytes:23030 (23.0 KB)

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:65536 Métrica:1
          Paquetes RX:200 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:200 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colatX:0
          Bytes RX:14760 (14.7 KB)  TX bytes:14760 (14.7 KB)

root@ubuntusead: /home/adrian# ip route show
default via 10.0.0.1 dev eth1  proto static
10.0.0.0/24 dev eth1  proto kernel  scope link  src 10.0.0.15  metric 1
192.168.56.0/24 dev eth0  proto kernel  scope link  src 192.168.56.254
root@ubuntusead: /home/adrian# nano /etc/sysctl.conf
root@ubuntusead: /home/adrian# sysctl -p
net.ipv4.ip_forward = 1
root@ubuntusead: /home/adrian#

```

Imos aceptar todos os paquetes con destino/orixe (INPUT/OUTPUT) o FW que pertencen a unha conexión xa autorizada e coñecida.

```
iptables -A INPUT -m state --state NEW -j ACCEPT
```

```
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Aceptaremos todas as conexións o servidor para que sexa administrado por SSH só polos equipos dos administradores 192.168.56.2, 192.168.56.3. O resto de conexións rexéitanse (REJECT).

```
iptables -A INPUT -p tcp -s 192.168.56.2,192.168.56.3 --dport 22 -j ACCEPT
```

```
iptables -A OUTPUT -p tcp -d 192.168.56.2,192.168.56.3 --sport 22 -j ACCEPT
```

Permitiremos só as resolucións por DNS ás ips 8.8.8.8 e 8.8.4.4 e o resto bloquéanse (DROP).

```
iptables -A OUTPUT -p udp --dport 53 ! -d 8.8.8.8 -j DROP
iptables -A OUTPUT -p udp --dport 53 ! -d 8.8.4.4 -j DROP
iptables -A INPUT -p udp --sport 53 -s 8.8.8.8,8.8.4.4 -j ACCEPT
```

Só permitiremos o tráfico web para actualizar os repositorios de Ubuntu.

```
iptables -A OUTPUT -p tcp --dport 80 -m string --algo bm --string "es.archive.ubuntu.com" -j ACCEPT
iptables -A OUTPUT -p tcp --dport 80 -m string --algo bm --string "es.security.ubuntu.com" -j ACCEPT
iptables -A OUTPUT -p tcp --dport 80 -m string --algo bm --string "es.extras.ubuntu.com" -j ACCEPT
```

Definimos as políticas para INPUT e OUTPUT de descarte.

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

Crea unha regra NAT para permitir que os equipos da rede se enmascaren para saír á Internet a través do Firewall. Aplica SNAT ou MASQUERADE. Neste punto comproba que os clientes se poden conectar á Internet.

```
iptables -t nat -A POSTROUTING -s 192.168.56.0/24 -j SNAT --to-source 10.0.0.1
```

Sería o mesmo que esta outra regra, MASQUERADE “enmascara” a red orixe coa IP pública de router.

```
iptables -t nat -A POSTROUTING -s 192.168.56.0/24 -j MASQUERADE
```

Establece a política por defecto para Forward de descarte.

```
iptables -P FORWARD DROP
```

Imos aceptar todos os paquetes a enrutar polo FW que pertencen a unha conexión xa autorizada e coñecida (cadea FORWARD).

```
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Agora imos permitir só a resolución de dns para os equipos dos traballadores.

```
iptables -A FORWARD -p udp -s 192.168.56.0/24 --dport 53 -d 8.8.8.8,8.8.4.4 -j ACCEPT
```

Agora imos permitir só a navegación web para os equipos dos traballadores.

```
iptables -A FORWARD -p tcp -s 192.168.56.0/24 -m multiport --dport 80,443 -j ACCEPT
```

Crea unha regra NAT para permitir que un equipo fóra da rede poida interactuar co servidor Web da rede local.

```
iptables -t nat -A PREROUTING -d 10.0.0.1 -p tcp --dport 80 -j DNAT --to-destination 192.168.56.254  
iptables -t nat -A POSTROUTING -s 192.168.56.254 -p tcp --sport 80 -j SNAT --to-source 10.0.0.1
```

Para que funcione tamén debes crear unha regra FORWARD que permita este tipo de tráfico.

```
iptables -A FORWARD -p tcp -d 192.168.56.254 --dport 80 -j ACCEPT
```

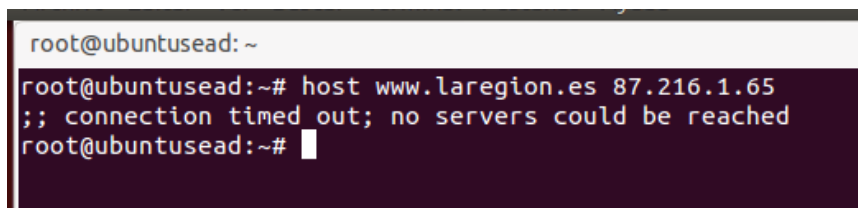
Crea unha regra NAT para permitir que un equipo fóra da rede poida administrar o servidor mediante SSH. Aplica DNAT.

```
iptables -t nat -A PREROUTING -d 10.0.0.1 -p tcp --dport 22 -j DNAT --to-destination 192.168.56.254  
iptables -t nat -A POSTROUTING -s 192.168.56.254 -p tcp --sport 22 -j SNAT --to-source 10.0.0.1
```

Para que funcione tamén debes crear unha regra FORWARD que permita este tipo de tráfico.

```
iptables -A FORWARD -p tcp -d 192.168.56.254 --dport 22 -j ACCEPT
```

A saída do comando host `www.laregion.es` 87.216.1.65 dende o equipo cliente.

A terminal window with a dark background and light text. The prompt is 'root@ubuntusead: ~'. The user enters the command 'host www.laregion.es 87.216.1.65'. The output is ';; connection timed out; no servers could be reached'. The prompt returns to 'root@ubuntusead:~#'.

```
root@ubuntusead: ~  
root@ubuntusead:~# host www.laregion.es 87.216.1.65  
;; connection timed out; no servers could be reached  
root@ubuntusead:~#
```

A saída do comando `cat /etc/iptables/rules.v4`

```

root@ubuntu: /home/adrian
GNU nano 2.2.6      Archivo: /etc/iptables/rules.v4

# Generated by iptables-save v1.4.21 on Thu Jun  2 19:23:29 2016
*nat
:PREROUTING ACCEPT [1:78]
:INPUT ACCEPT [1:78]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -d 10.0.0.1/32 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.56.254
-A PREROUTING -d 10.0.0.1/32 -p tcp -m tcp --dport 22 -j DNAT --to-destination 192.168.56.254
-A PREROUTING -d 10.0.0.1/32 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.56.254
-A PREROUTING -d 10.0.0.1/32 -p tcp -m tcp --dport 22 -j DNAT --to-destination 192.168.56.254
-A PREROUTING -d 10.0.0.1/32 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.56.254
-A PREROUTING -d 10.0.0.1/32 -p tcp -m tcp --dport 22 -j DNAT --to-destination 192.168.56.254
-A POSTROUTING -s 192.168.56.0/24 -j SNAT --to-source 10.0.0.1
-A POSTROUTING -s 192.168.56.0/24 -j MASQUERADE
-A POSTROUTING -s 192.168.56.254/32 -p tcp -m tcp --sport 80 -j SNAT --to-source 10.0.0.1
-A POSTROUTING -s 192.168.56.254/32 -p tcp -m tcp --sport 22 -j SNAT --to-source 10.0.0.1
-A POSTROUTING -s 192.168.56.0/24 -j SNAT --to-source 10.0.0.1
-A POSTROUTING -s 192.168.56.0/24 -j MASQUERADE
-A POSTROUTING -s 192.168.56.254/32 -p tcp -m tcp --sport 80 -j SNAT --to-source 10.0.0.1
-A POSTROUTING -s 192.168.56.254/32 -p tcp -m tcp --sport 22 -j SNAT --to-source 10.0.0.1
-A POSTROUTING -s 192.168.56.0/24 -j SNAT --to-source 10.0.0.1
-A POSTROUTING -s 192.168.56.0/24 -j MASQUERADE
-A POSTROUTING -s 192.168.56.254/32 -p tcp -m tcp --sport 80 -j SNAT --to-source 10.0.0.1
-A POSTROUTING -s 192.168.56.254/32 -p tcp -m tcp --sport 22 -j SNAT --to-source 10.0.0.1
COMMIT
# Completed on Thu Jun  2 19:23:29 2016
# Generated by iptables-save v1.4.21 on Thu Jun  2 19:23:29 2016
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -m state --state NEW -j ACCEPT
-A INPUT -s 192.168.56.2/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 192.168.56.3/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 8.8.8.8/32 -p udp -m udp --sport 53 -j ACCEPT
-A INPUT -s 8.8.4.4/32 -p udp -m udp --sport 53 -j ACCEPT
-A FORWARD -s 192.168.56.0/24 -p tcp -m tcp --dport 80 -m string --string "es.archive.ubuntu.com" -j ACCEPT
-A FORWARD -s 192.168.56.0/24 -p tcp -m tcp --dport 80 -m string --string "es.security.ubuntu.com" -j ACCEPT
-A FORWARD -s 192.168.56.0/24 -p tcp -m tcp --dport 80 -m string --string "es.extras.ubuntu.com" -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -s 192.168.56.0/24 -d 8.8.8.8/32 -p udp -m udp --dport 53 -j ACCEPT
-A FORWARD -s 192.168.56.0/24 -d 8.8.4.4/32 -p udp -m udp --dport 53 -j ACCEPT
-A FORWARD -s 192.168.56.0/24 -p tcp -m multiport --dports 80,443 -j ACCEPT
-A FORWARD -d 192.168.56.254/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -d 192.168.56.254/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 10.0.0.74/32 -m time --timestart 20:00:00 --timestop 10:00:00 --weekdays Mon,Tue,Wed -j DROP
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -d 192.168.56.2/32 -p tcp -m tcp --sport 22 -j ACCEPT
-A OUTPUT -d 192.168.56.3/32 -p tcp -m tcp --sport 22 -j ACCEPT
-A OUTPUT ! -d 8.8.8.8/32 -p udp -m udp --dport 53 -j DROP
-A OUTPUT ! -d 8.8.4.4/32 -p udp -m udp --dport 53 -j DROP
COMMIT
# Completed on Thu Jun  2 19:23:29 2016

^G Ver ayuda      ^O Guardar      ^R Leer Fich     ^Y RePág.      ^K Cortar Texto ^C Pos actual
^X Salir          ^J Justificar   ^W Buscar       ^V Pág. Sig.   ^U PegarTxt    ^T Ortografia

```


A listaxe numerada de regras iptables para a táboa filter.

```

root@ubuntusead: /home/adrian
root@ubuntusead:/home/adrian# iptables -L -t filter -n -v --line-numbers
Chain INPUT (policy DROP 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source         destination
1      0      0 ACCEPT    all  --  *      *       0.0.0.0/0      0.0.0.0/0
    state NEW
2      0      0 ACCEPT    tcp  --  *      *       192.168.56.2   0.0.0.0/0
    tcp dpt:22
3      0      0 ACCEPT    tcp  --  *      *       192.168.56.3   0.0.0.0/0
    tcp dpt:22
4      0      0 ACCEPT    udp  --  *      *       8.8.8.8        0.0.0.0/0
    udp spt:53
5      0      0 ACCEPT    udp  --  *      *       8.8.4.4        0.0.0.0/0
    udp spt:53

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source         destination
1      0      0 ACCEPT    tcp  --  *      *       192.168.56.0/24 0.0.0.0/0
    tcp dpt:80 STRING match "es.archive.ubuntu.com" ALGO name bm TO 65535
2      0      0 ACCEPT    tcp  --  *      *       192.168.56.0/24 0.0.0.0/0
    tcp dpt:80 STRING match "es.security.ubuntu.com" ALGO name bm TO 65535
3      0      0 ACCEPT    tcp  --  *      *       192.168.56.0/24 0.0.0.0/0
    tcp dpt:80 STRING match "es.extras.ubuntu.com" ALGO name bm TO 65535
4      0      0 ACCEPT    all  --  *      *       0.0.0.0/0      0.0.0.0/0
    state RELATED,ESTABLISHED
5      0      0 ACCEPT    udp  --  *      *       192.168.56.0/24 8.8.8.8
    udp dpt:53
6      0      0 ACCEPT    udp  --  *      *       192.168.56.0/24 8.8.4.4
    udp dpt:53
7      0      0 ACCEPT    tcp  --  *      *       192.168.56.0/24 0.0.0.0/0
    multiport dports 80,443
8      0      0 ACCEPT    tcp  --  *      *       0.0.0.0/0      192.168.56.254
    tcp dpt:80
9      0      0 ACCEPT    tcp  --  *      *       0.0.0.0/0      192.168.56.254
    tcp dpt:22

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source         destination
1      0      0 ACCEPT    all  --  *      *       0.0.0.0/0      0.0.0.0/0
    state RELATED,ESTABLISHED
2      0      0 ACCEPT    tcp  --  *      *       0.0.0.0/0      192.168.56.2
    tcp spt:22
3      0      0 ACCEPT    tcp  --  *      *       0.0.0.0/0      192.168.56.3
    tcp spt:22
4      0      0 DROP      udp  --  *      *       0.0.0.0/0      !8.8.8.8
    udp dpt:53
5      0      0 DROP      udp  --  *      *       0.0.0.0/0      !8.8.4.4
    udp dpt:53
root@ubuntusead:/home/adrian#

```


A listaxe numerada de regras iptables para nat.

```

root@ubuntusead: /home/adrian
root@ubuntusead:/home/adrian# iptables -L -t nat -n -v --line-numbers
Chain PREROUTING (policy ACCEPT 1 packets, 78 bytes)
num  pkts bytes target    prot opt in     out     source         destination
1      0      0 DNAT      tcp  --  *      *       0.0.0.0/0       10.0.0.1
    tcp dpt:80 to:192.168.56.254
2      0      0 DNAT      tcp  --  *      *       0.0.0.0/0       10.0.0.1
    tcp dpt:22 to:192.168.56.254
3      0      0 DNAT      tcp  --  *      *       0.0.0.0/0       10.0.0.1
    tcp dpt:80 to:192.168.56.254
4      0      0 DNAT      tcp  --  *      *       0.0.0.0/0       10.0.0.1
    tcp dpt:22 to:192.168.56.254

Chain INPUT (policy ACCEPT 1 packets, 78 bytes)
num  pkts bytes target    prot opt in     out     source         destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source         destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source         destination
1      0      0 SNAT      all  --  *      *       192.168.56.0/24  0.0.0.0/0
    to:10.0.0.1
2      0      0 MASQUERADE all  --  *      *       192.168.56.0/24  0.0.0.0/0
3      0      0 SNAT      tcp  --  *      *       192.168.56.254   0.0.0.0/0
    tcp spt:80 to:10.0.0.1
4      0      0 SNAT      tcp  --  *      *       192.168.56.254   0.0.0.0/0
    tcp spt:22 to:10.0.0.1
5      0      0 SNAT      all  --  *      *       192.168.56.0/24  0.0.0.0/0
    to:10.0.0.1
6      0      0 MASQUERADE all  --  *      *       192.168.56.0/24  0.0.0.0/0
7      0      0 SNAT      tcp  --  *      *       192.168.56.254   0.0.0.0/0
    tcp spt:80 to:10.0.0.1
8      0      0 SNAT      tcp  --  *      *       192.168.56.254   0.0.0.0/0
    tcp spt:22 to:10.0.0.1
root@ubuntusead:/home/adrian#

```

Un posible comando de iptables para a cadea FORWARD que só permitise aos equipos dos traballadores ter tráfico web de 11.00 a 12.00 horas todos os días.

```
iptables -A FORWARD -p tcp -s 192.168.56.0/24 -m multiport --dport 80,443 -m time --timestart 11:00 --timestop 12:00 --weekdays Mon,Tue,Wed,Thu,Fri,Sat,Sun -j ACCEPT
```

```

root@ubuntusead: /home/adrian
root@ubuntusead:/home/adrian# iptables -A FORWARD -d 10.0.0.74 -m time --timestart 20:00 --timestop 10:00 --weekdays Sun,Mon,Tue,Wed,Thu,Fri -j DROP
root@ubuntusead:/home/adrian# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination

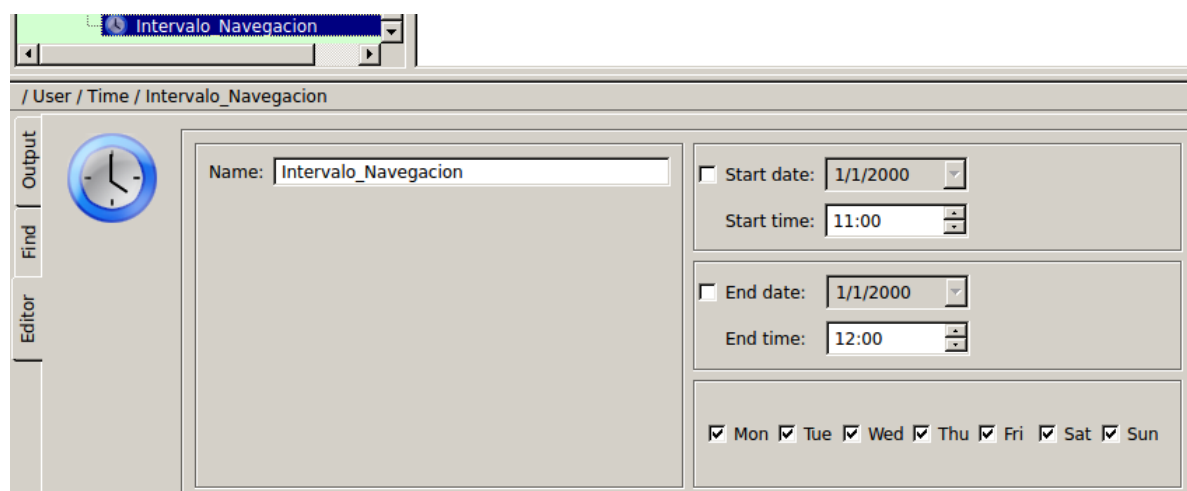
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination

    0    0 DROP      all  --  *      *        0.0.0.0/0         10.0.0.74
    TIME from 20:00:00 to 10:00:00 on Mon,Tue,Wed,Thu,Fri,Sun UTC

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination

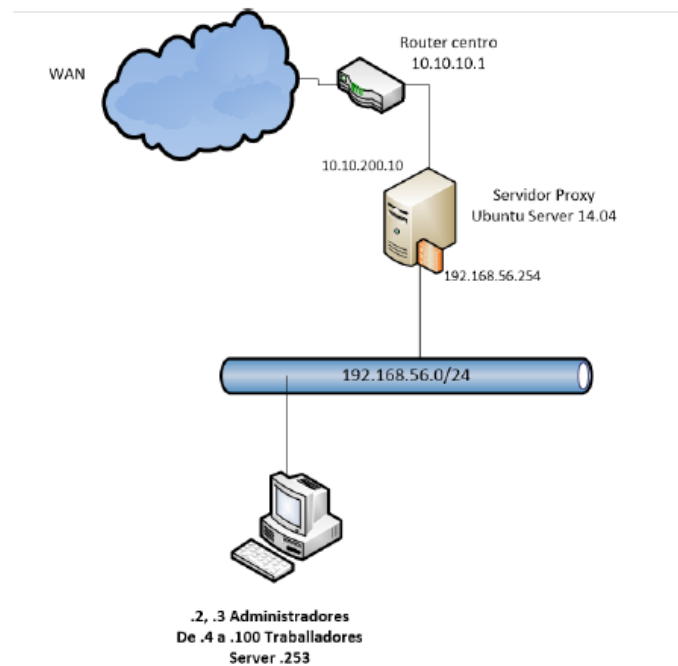
root@ubuntusead:/home/adrian#

```



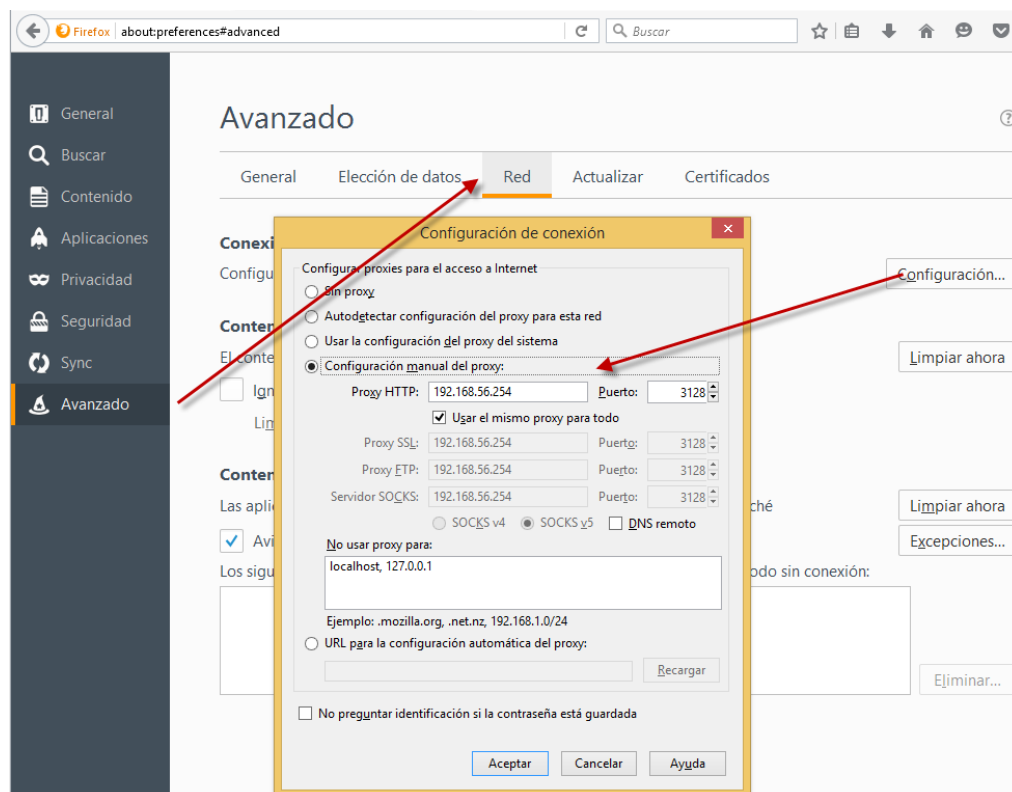
5. Proxy - Squid

O escenario podería ser o seguinte:

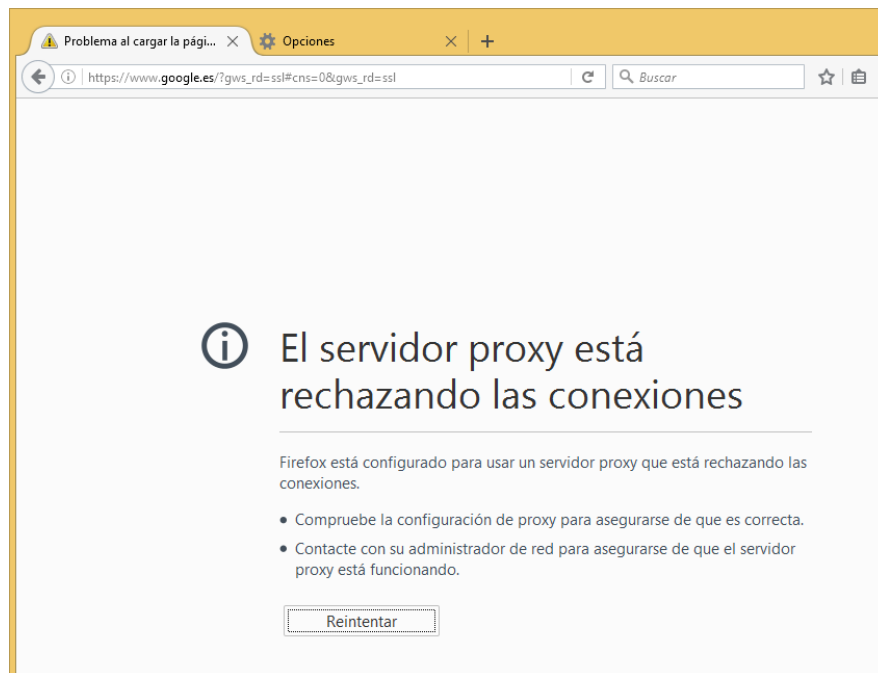


No equipo cliente non sería necesario establecer unha dirección IP xa que o encamiñamento hacía a navegación de Internet verase afectada e establecida polo servidor proxy. A dirección IP do equipo cliente, neste caso e a 192.168.56.10.

Configuramos o navegador web Mozilla Firefox ca dirección IP do servidor proxy.



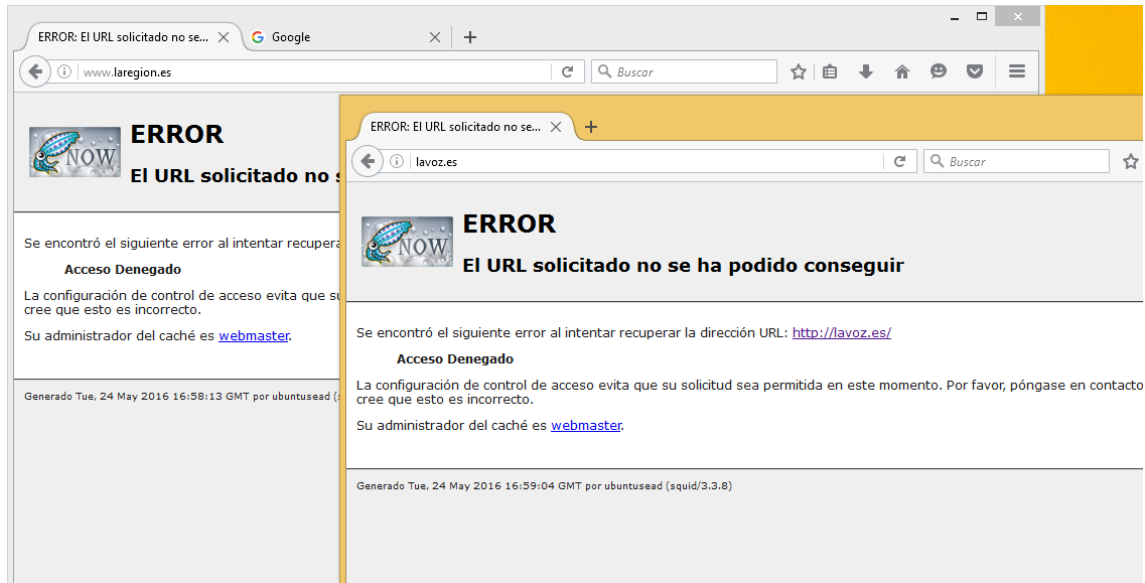
Por defecto, este negará todas as conexións.



Accedemos o arquivo de configuración de Squid: `/etc/squid3/squid.conf` e xeramos as seguinte listas de control de acceso (ACLs).

```
root@ubuntusead: /home/adrian
root@ubuntusead:/home/adrian# cat /etc/squid3/squid.conf | grep -v '^#' | awk NF
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
acl filtro_periodico dstdomain .laregion.es .lavo.es
http_access deny filtro_periodico
http_access allow localhost
acl ip_rede src 192.168.56.10
http_access allow ip_rede
acl rango_ips_permitidas src 192.168.56.0/255.255.255.0
http_access allow rango_ips_permitidas
http_access deny all
http_port 3128
coredump_dir /var/spool/squid3
refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:      1440      0%       1440
refresh_pattern -i (/cgi-bin/|\?) 0       0%       0
refresh_pattern (Release|Packages(.gz)*)$ 0      20%     2880
refresh_pattern .              0        20%     4320
root@ubuntusead:/home/adrian#
```

Comprobamos que agora xa temos saída a Internet no equipo cliente, excepto as páxinas webs: “laregion.es” e “lavoz.es”.



Por defecto ao usuario móstraselle a mensaxe da captura anterior, pero esta pódese modificar según o tipo de erro.

No directorio: /usr/share/squid3/errors/es. Veremos os disintos arquivos que se interpretarán en HTML polo navegador os cales podemos editar o noso antoxo e personalizalos no caso de estar nunha organización.

Neste caso a modo de práctica editarei o arquivo oportuno que nos mostra a imaxe anterior, ERR_ACCESS_DENIED.

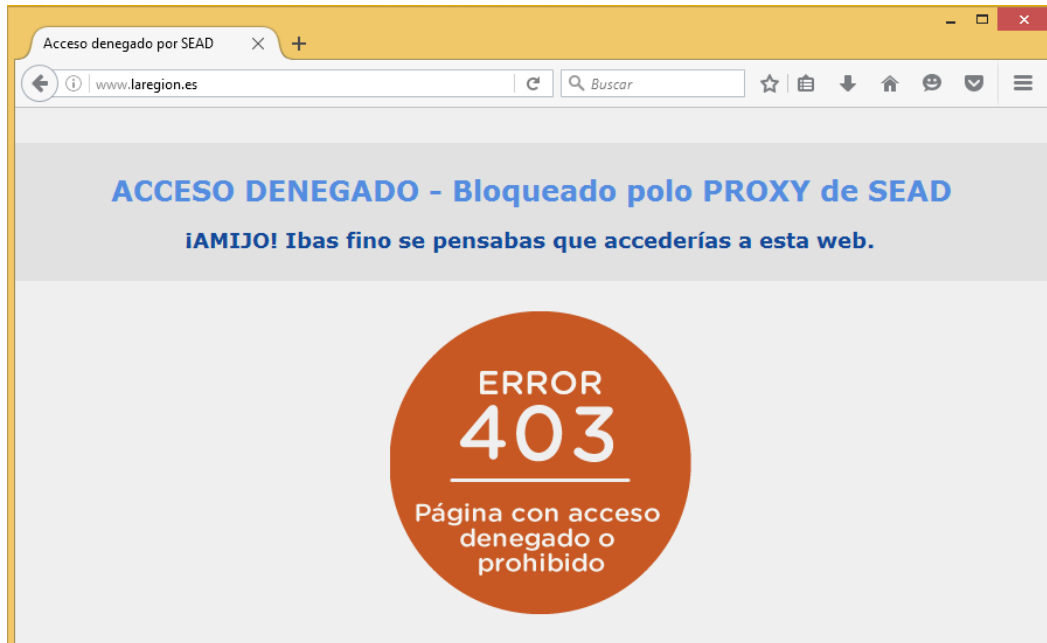
```

root@ubuntusead: /home/adrian
root@ubuntusead:/home/adrian# ls /usr/share/squid3/errors/es
ERR_ACCESS_DENIED      ERR_FTP_FAILURE        ERR_ONLY_IF_CACHED_MISS
ERR_ACL_TIME_QUOTA_EXCEEDED  ERR_FTP_FORBIDDEN      error-details.txt
ERR_AGENT_CONFIGURE      ERR_FTP_NOT_FOUND      ERR_PRECONDITION_FAILED
ERR_AGENT_WPAD           ERR_FTP_PUT_CREATED    ERR_READ_ERROR
ERR_CACHE_ACCESS_DENIED   ERR_FTP_PUT_ERROR      ERR_READ_TIMEOUT
ERR_CACHE_MGR_ACCESS_DENIED ERR_FTP_PUT_MODIFIED    ERR_SECURE_CONNECT_FAIL
ERR_CANNOT_FORWARD        ERR_FTP_UNAVAILABLE    ERR_SHUTTING_DOWN
ERR_CONFLICT_HOST         ERR_GATEWAY_FAILURE    ERR_SOCKET_FAILURE
ERR_CONNECT_FAIL          ERR_ICAP_FAILURE       ERR_TOO_BIG
ERR_DIR_LISTING           ERR_INVALID_REQ         ERR_UNSUP_HTTPVERSION
ERR_DNS_FAIL              ERR_INVALID_RESP        ERR_UNSUP_REQ
ERR_ESI                   ERR_INVALID_URL         ERR_URN_RESOLVE
ERR_FORWARDING_DENIED     ERR_LIFETIME_EXP        ERR_WRITE_ERROR
ERR_FTP_DISABLED          ERR_NO_RELAY            ERR_ZERO_SIZE_OBJECT
root@ubuntusead:/home/adrian# nano /usr/share/squid3/errors/es/ERR_ACCESS_DENIED

root@ubuntusead:/home/adrian# service squid3 restart
squid3 stop/waiting
squid3 start/running, process 4246
root@ubuntusead:/home/adrian#

```

Unha vez editado o HTML do arquivo e reiniciado o servicio do Squid, temos a nosa personalización actualizada.



Sen embargo cas ACLs establecidas anteriormente **podemos “eludir” este tipo de proxy a través dun proxyweb** dispoñible nunha sinxela búsqueda que podería facer o usuario final.

Habería que filtrar máis regras a máis explícitas para “pulir” máis as restriccións do Proxy.

Existen infinidade proxys nos que podemos establecer configuracións máis personalizadas, incluso filtrar polas cabeceiras dos paquetes, e saber si se trata dunha petición http a través dun protocolo ssh (conexión con un add-on dende o navegador por exemplo), así como o tipo de protocolos a filtrar, peticións de portos lóxicos, etc.



6. Conclusións

Coñecemos as diferentes formas de sistemas de filtrado de tráfico de rede como foi o Firewall con iptables (netfilter) e proxy web como Squid.

Os cales permitíronos tomar decisións en que tráfico pode entrar e saír (“a groso modo”) da nosa rede, tendo así unha comunicación máis controlada e explícita.