

# **Proyecto 2**

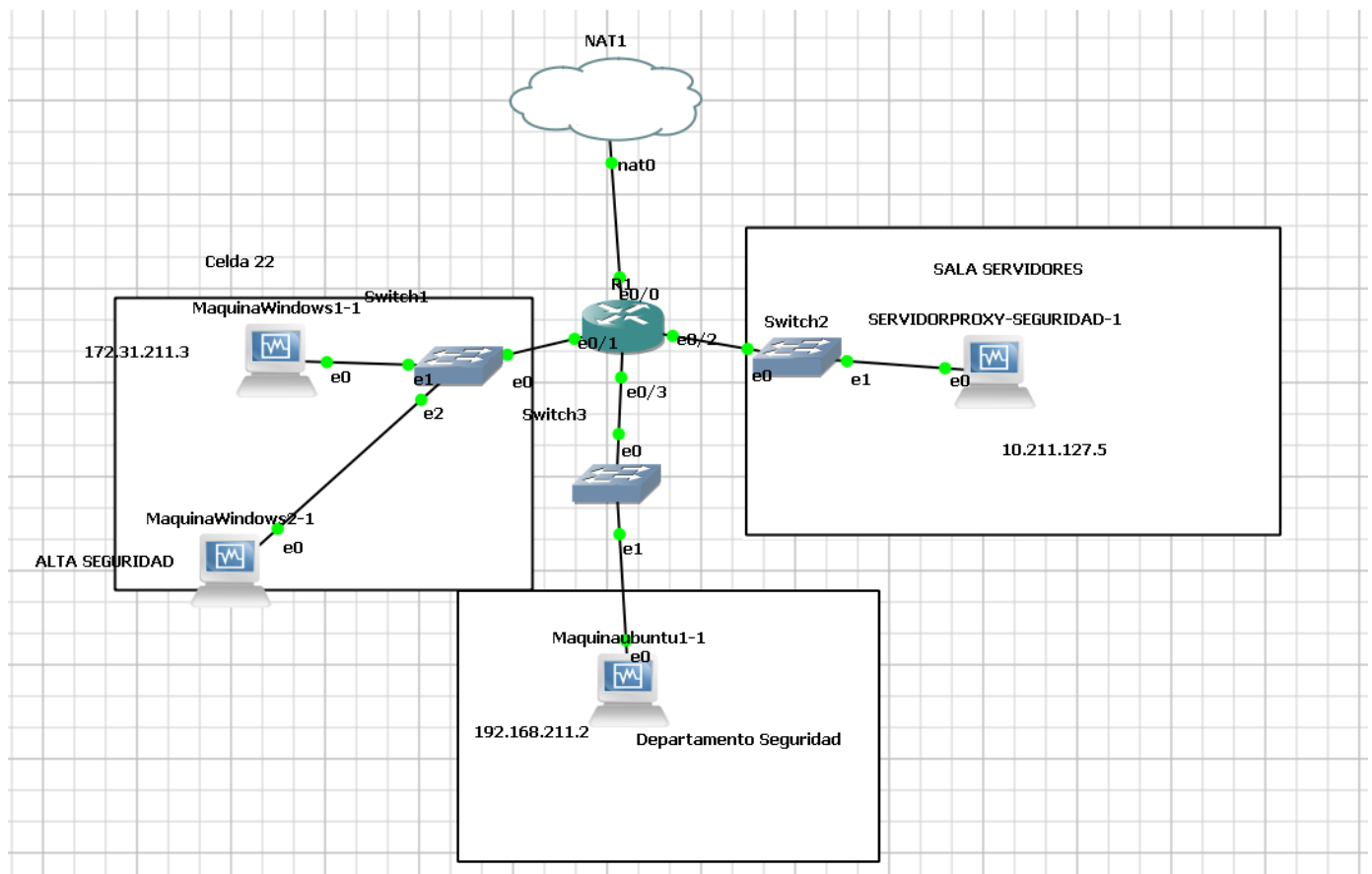
# **PROXY**

Sergi Moreno Piquer  
SMX2-B

# ÍNDICE

<u>1-Topologia Red</u> .....	3
<u>2-Configuración Router</u> .....	4
<u>3-Configuración SquidConf</u> .....	5
<u>4-Configuración SquidGuard</u> .....	7
<u>5-Comprobaciones SquidGuard</u> .....	8
<u>6-Comprobación SARG</u> .....	10
<u>7-Comprobación dominio</u> .....	11

## 1-Topologia de la red:



Dispositivo	Interf ace	IPV4	MÁSCARA	GATEWAY
SERVIDO RPROXY	e0/2	10.211.127 .5	/24	10.211.127.1
Maquinaub untu	e0/3	192.168.21 1.2	/24	192.168.211. 1
MaquinaWi ndows	e0/1	172.31.211 .3	/24	172.31.211.1
NAT	e0/0	DHCP	/24	

## 2-Configuración del router:

```
R1(config)#do sh ip int br
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	192.168.112.118	YES	DHCP	up	up
Ethernet0/1	172.31.211.1	YES	NVRAM	up	up
Ethernet0/2	10.211.127.1	YES	NVRAM	up	up
Ethernet0/3	192.168.211.1	YES	NVRAM	up	up

```
interface Ethernet0/0
```

```
ip address dhcp
ip nat outside
ip virtual-reassembly in
duplex auto
```

```
!
```

```
interface Ethernet0/1
```

```
ip address 172.31.211.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
duplex auto
```

```
!
```

```
interface Ethernet0/2
```

```
ip address 10.211.127.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
duplex auto
```

```
!
```

```
interface Ethernet0/3
```

```
ip address 192.168.211.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
duplex auto
```

```
access-list 1 permit 192.168.211.0 0.0.0.255
```

```
access-list 1 permit 172.31.211.0 0.0.0.255
```

```
access-list 1 permit 10.211.127.0 0.0.0.255
```

```
!
```

### 3-Configuración squid.conf:

```
GNU nano 4.8 /etc/squid.conf
auth_param basic program "/usr/lib/squid/basic_ncsa_auth" "/etc/squid/usuarios.acl"
# al principio del fichero
url_rewrite_program /usr/bin/squidGuard -c /etc/squidguard/squidGuard.conf
url_rewrite_children 2

##### INICIO ACLs Y OTROS PARAMETROS #####

# activa el apagado en menos tiempo
shutdown_lifetime 3 seconds
# muestra las páginas de error en español
error_directory /usr/share/squid/errors/Spanish
# muestra un nombre del servidor proxy
visible_hostname MIPROXY
# oculta la versión de SQUID en cualquier página de error
httpd_suppress_version_string on
# oculta la versión de SQUID en las cabeceras de respuesta HTTP
via off

acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN)
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

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
```

```
# listas de control de acceso (ACLs)
acl subred1 src 10.211.127.0/24
acl subred2 src 192.168.211.0/24
acl subred3 src 172.31.211.0/24
acl HORARIO time MTWHF 17:45-21:45
acl USUARIOS proxy_auth REQUIRED
acl PALABRAS url_regex -i escapa escape sarg
acl DOMINIOS dstdomain .policia.es .mossos.gencat.cat
##### FIN ACLs Y OTROS PARAMETROS #####

http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

# ... (aquí existen otras líneas no modificar!!!)
http_access allow localhost manager
http_access deny manager
##### INICIO REGLAS #####
http_access allow subred1
http_access allow subred3 HORARIO !DOMINIOS !PALABRAS
http_access allow subred2 USUARIOS

# control de acceso (permitir o denegar)

include /etc/squid/conf.d/*
##### FIN REGLAS #####
http_access allow localhost
http_access deny all
http_port 3128

coredump_dir /var/spool/squid
refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:       1440      0%        1440
refresh_pattern -i (/cgi-bin/|\?) 0        0%         0
refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern \/(Release(|\.gpg))$ 0 0% 0 refresh-ims
refresh_pattern \/(InRelease$ 0 0% 0 refresh-ims
refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern .               0        20%      4320
```

## 4-Configuracion SquidGuard

```
GNU nano 4.8 /etc/squidguard/squidGuard.conf
# [see also in file dest-snippet.txt]

dest good {
}

dest local {
}

dest porn {
}

dest alcohol {
    domainlist alcohol/domains
    urllist alcohol/urls
    redirect http://localhost/alcohol-bloqueado.html
}

dest drugs {
    domainlist drugs/domains
    urllist drugs/urls
    redirect http://localhost/drugs-bloqueado.html
}

#dest adult {
#    domainlist      BL/adult/domains
#    urllist         BL/adult/urls
#    expressionlist  BL/adult/expressions
#    redirect http://admin.foo.bar.de/cgi-bin/blocked.cgi?clientaddr=%a&clientname=%n&clientuser=%i&clientgroup=%s&targetgroup=%t&url=%u
#}

#
# ACL RULES:
#

acl {
    admin {
        pass      any
    }

    foo-clients within workhours {
        pass      good !in-addr !porn any
    } else {
        pass any
    }
}
```

```
#dest adult {
#    domainlist      BL/adult/domains
#    urllist         BL/adult/urls
#    expressionlist  BL/adult/expressions
#    redirect http://admin.foo.bar.de/cgi-bin/blocked.cgi?clientaddr=%a&clientname=%n&clientuser=%i&clientgroup=%s&targetgroup=%t&url=%u
#}

#
# ACL RULES:
#

acl {
    admin {
        pass      any
    }

    foo-clients within workhours {
        pass      good !in-addr !porn any
    } else {
        pass any
    }

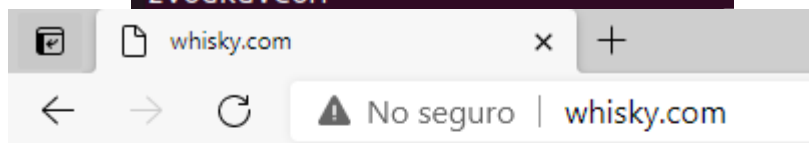
    bar-clients {
        pass      local none
    }

    default {
        pass      !alcohol !drugs all
        redirect http://localhost/content-to-be-quarantined.html
    }
}
```

## 5- Comprobaciones SquidGuard (alcohol, y drugs)

### Alcohol:

```
whisky.com  
whiskychallenge.com  
whiskylive.com  
whiskymag.com  
whiskymerchants.co.uk  
whitebeertravels.co.uk  
wildturkeybourbon.com  
wine-searcher.com  
wine-spirit.com  
wineandhospitalitynetwork.com  
winebeveragecenter.com  
winefront.com.au  
winelistaustralia.com.au  
winemaking.jackkeller.net  
winexmagazine.com  
winzerhof-zach.at  
wlvliquors.com  
wodka-gorbatschow.de  
wodka.de  
wolfberger.com  
wollastonwines.com  
woodstockwine.com.au  
worldofbeer.com  
wotanwodka.com  
wunschlikoer.de  
wychwood.co.uk  
xellent.ch  
xn--lsmagninger-fgb.dk  
xxxx.com.au  
youngsubrew.co.uk  
zvodka.com
```

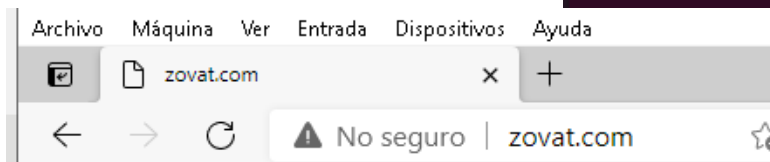


PAGINA BLOQUEADA



## Drugs:

znqwixpx.ru  
zocor.89.pl  
zodqagrb.at  
zokel.cn  
zoloft-info.us  
zoloft-klm.blogspot.com  
zoloft-qwq.blogspot.com  
zombiesarehere.info  
zonerx-med.ru  
zoolips.ru  
zoomhigh.com  
zoomhome.ru  
zoomjump.com  
zoompearl.com  
zoompiece.com  
zoomwealth.ru  
zovat.com  
ztbmedic.ru  
zu-dick-hier-klicken.org  
zugvpvo.ru  
zulozymkih.net  
zuluomster.net  
zupgaer.net  
zvymmogwu.net  
zwdoctor.ru  
zweisam69.net  
zwhmedic.ru  
zwipqubwu.net  
zxkaufvq.ru  
xztqkkdd.in  
zyban-klm.blogspot.com  
zyban-qwq.blogspot.com

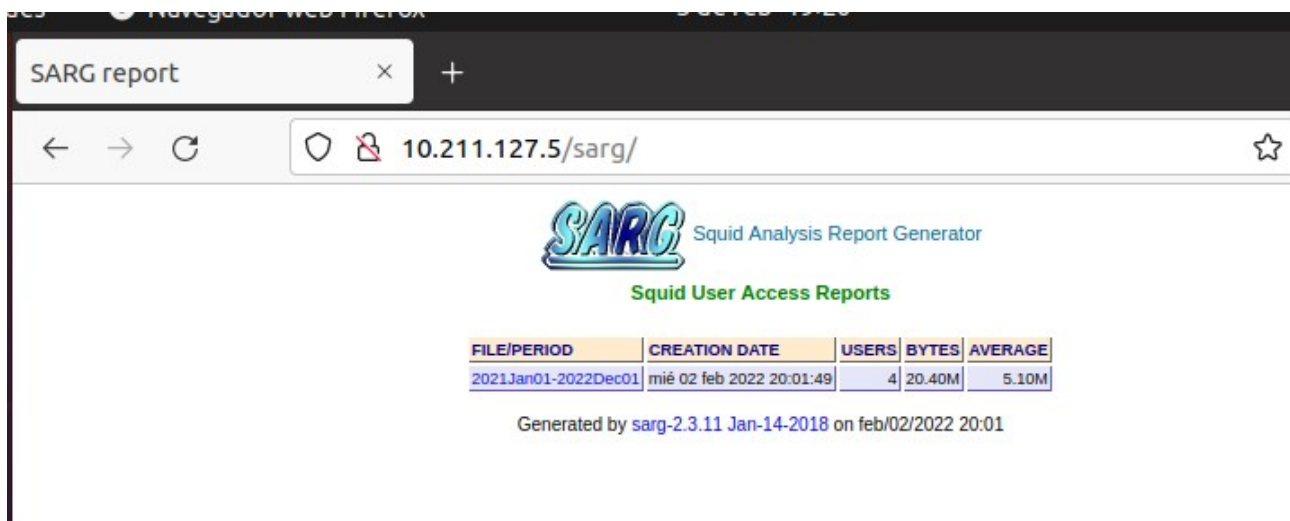


## 6-Aplicación de control de accesos de Internet

### Servidor



### Departamento Seguridad



### Celda




## 7-Comprobación dominio(policia y mossos):

Maquina Windows 1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

ERROR: El URL solicitado no se ha podido conseguir

No seguro | policia.es

 **ERROR**

**El URL solicitado no se ha podido conseguir**

Se encontró el siguiente error al intentar recuperar la dirección URL: <http://policia.es/>

**Acceso Denegado**

La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, contacte con su proveedor de servicios si cree que esto es incorrecto.

Su administrador del caché es [webmaster](#).


Generado Wed, 02 Feb 2022 20:09:37 GMT por MIPROXY (squid)

Maquina Windows 1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

ERROR: El URL solicitado no se ha podido conseguir

No seguro | mossos.gencat.cat

 **ERROR**

**El URL solicitado no se ha podido conseguir**

Se encontró el siguiente error al intentar recuperar la dirección URL: <http://mossos.gencat.cat/>

**Acceso Denegado**

La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, pcontacto con su proveedor de servicios si cree que esto es incorrecto.

Su administrador del caché es [webmaster](#).

Generado Wed, 02 Feb 2022 20:10:49 GMT por MIPROXY (squid)

## 8-Comprobación palabra ( escape , escapa)

