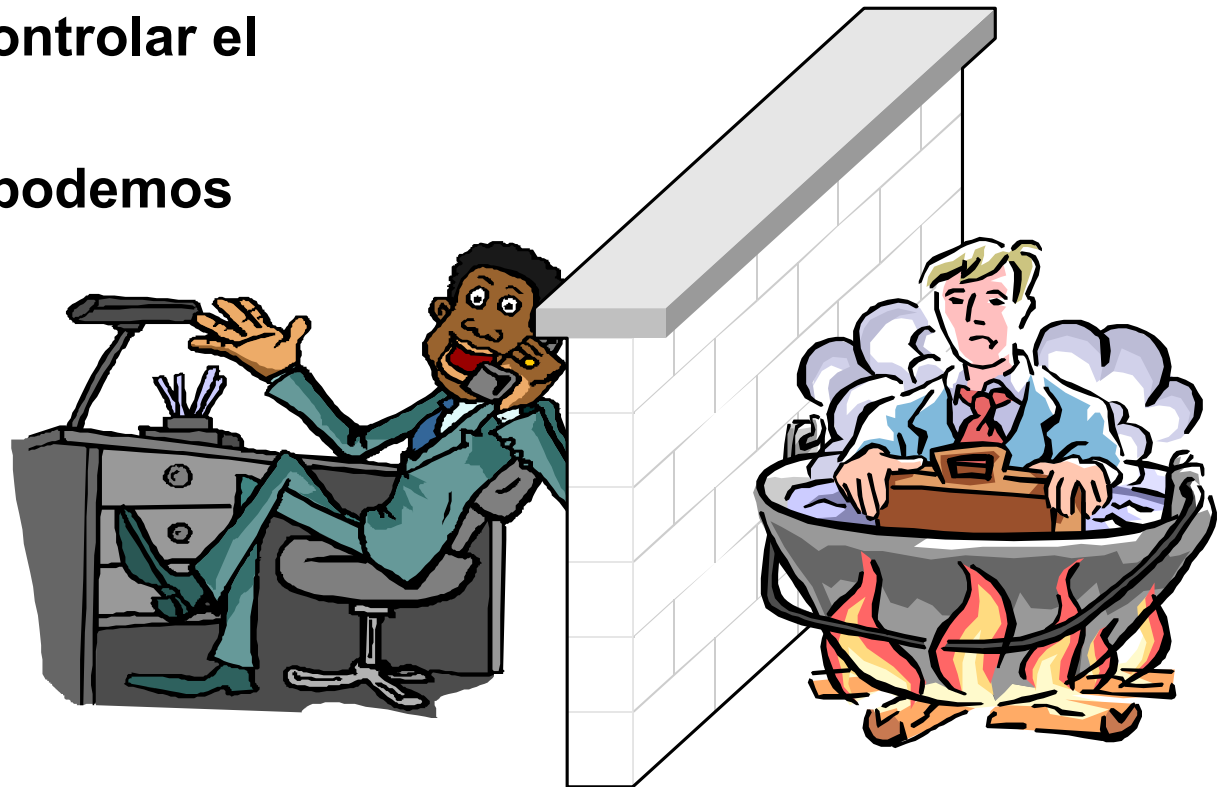


# Unidad 5

## Firewalls

# Introducción: Qué es un firewall

- Es una analogía con “Pared Cortafuego”
- Es un separador, permite controlar el tráfico que pasa por la red.
- Si ocurre una emergencia, podemos contenerla



# Introducción: Necesidad de un firewall

## Que queremos proteger?

- **Datos**
  - Confidencialidad
  - Integridad
  - Disponibilidad
- **Recursos**
  - Son míos
- **Reputación**
  - Lo que se haga con mis equipo parece provenir de mí
  - Ser vulnerado provoca desconfianza

- **Fines de los 80: routers que separan redes**
- **Principios de los 90: ACLs**
- **Bastion Hosts**
- **13 de Junio de 1991: primer “venta”**
- **1991-92: TCP-Wrapper**
- **1993: FWTK**
  - Stateful Inspection**
- **1994: Interfaces amigables**



# Tipos de Firewall

# Tipos de Firewalls

- **Filtrado de Paquetes**
- **Stateful Packet Inspection**
- **Gateways de Circuito**
- **Gateways de Aplicación**

- Cada paquete que entra o sale de la red es verificado y permitido o denegado dependiendo de un conjunto de reglas definidas por el usuario.
- Se basa en las direcciones de origen y destino
- Puede utilizar el protocolo y/o ports de origen y destino.
- Este tipo de filtros suelen utilizarse en los routers.
- Ventajas
  - Eficiencia.
  - Fácil implementación
- Desventajas
  - Complejidad de las reglas

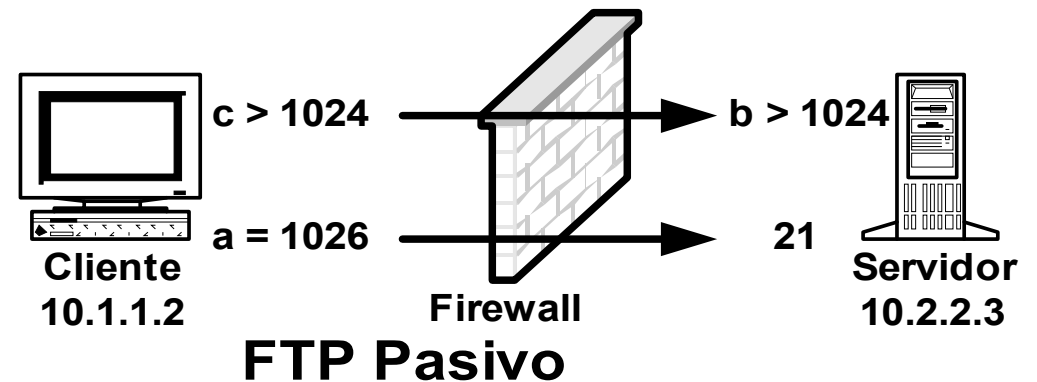
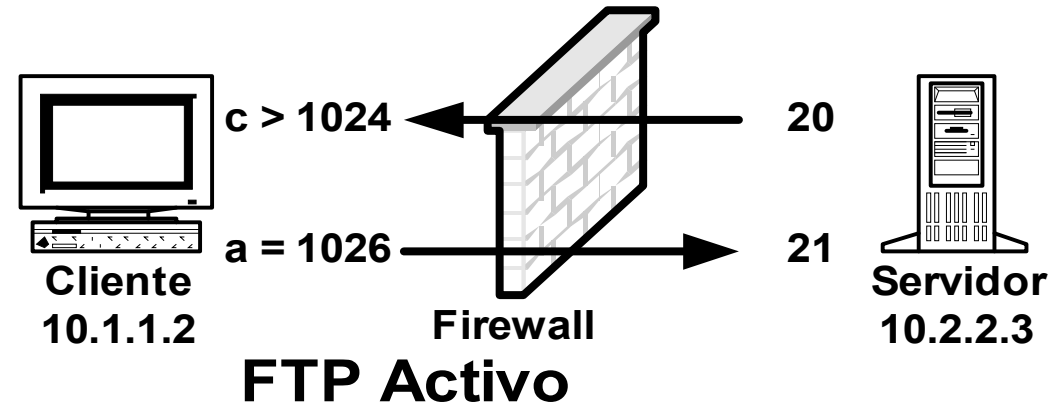
# Filtrado de paquetes estático

## Ejemplo:

FTP

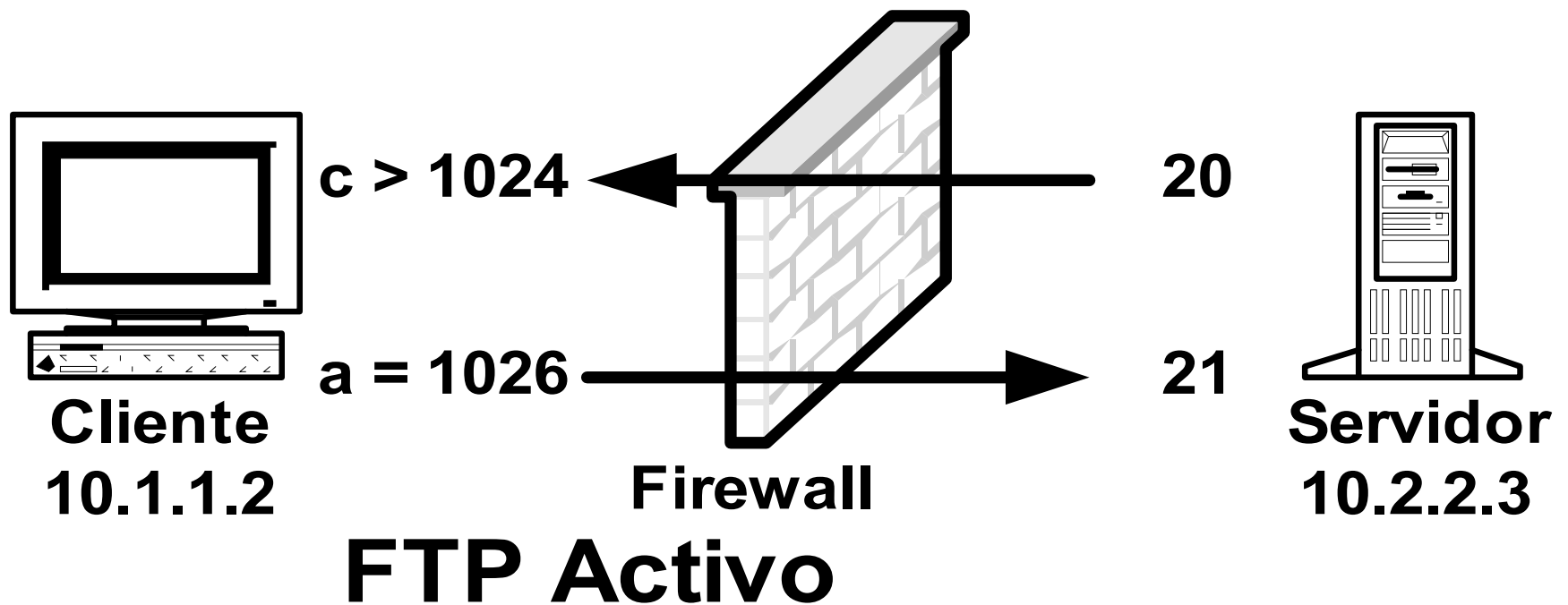
Origen: 10.1.1.2 port 1026

Destino: 10.2.2.3 port 21





# Filtrado de paquetes estático



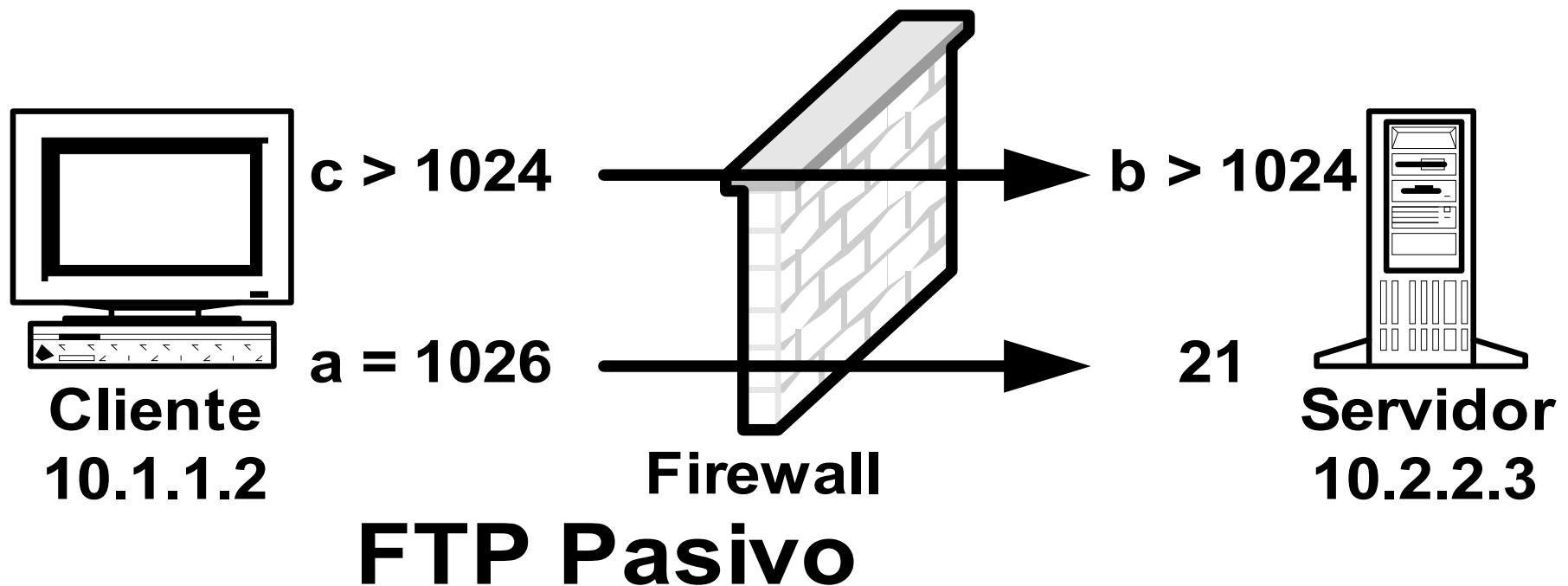
## Reglas para el servidor:

Permit any 1024:65535 to 10.2.2.3 21  
Permit 10.2.2.3 21 to any 1024:65535  
Permit 10.2.2.3 20 to any 1024:65535  
Permit any 1024:65535 to 10.2.2.3 20

## Reglas para el cliente:

Permit 10.1.1.0/24 1024:65535 to any 21  
Permit any 21 to 10.1.1.0/24 1024:65535  
Permit any 20 to 10.1.1.0/24 1024:65535  
Permit 10.1.1.0/24 1024:65535 to any 20

# Filtrado de paquetes estático



## Reglas para el servidor:

Permit any 1024:65535 to 10.2.2.3 21

Permit 10.2.2.3 21 to any 1024:65535

Permit any 1024:65535 to 10.2.2.3 1024:65535

Permit 10.2.2.3 1024:65535 to any 1024:65535

## Reglas para el cliente:

Permit 10.1.1.0/24 1024:65535 to any 21

Permit any 21 to 10.1.1.0/24 1024:65535

Permit 10.1.1.0/24 1024:65535 to any 1024:65535

Permit any 1024:65535 to 10.1.1.0/24 1024:65535

# Stateful Packet Inspection

- **Como el filtrado de paquetes pero stateful**
- Stateful se refiere a que pueden permitir o denegar sesiones entrantes o salientes tomando en cuenta el estado de las conexiones que el firewall maneja.
- El firewall mantiene información de las conexiones, del comienzo y del final de las sesiones, para dinámicamente poder controlar las decisiones de filtrado. Puede tener en cuenta los números de secuencia.
- El control se hace sobre la sesión y no sobre cada paquete individual.
- Puede analizar algunas partes del protocolo de nivel superior.
- **Ventajas:**
  - Mayor precisión en el filtrado
  - Más Facilidad para escribir reglas
- **Desventajas**
  - Mayor procesamiento

## **Regla para aceptar conexiones pre-establecidas:**

Permit any to any established,related

## **Reglas para el cliente (FTP pasivo):**

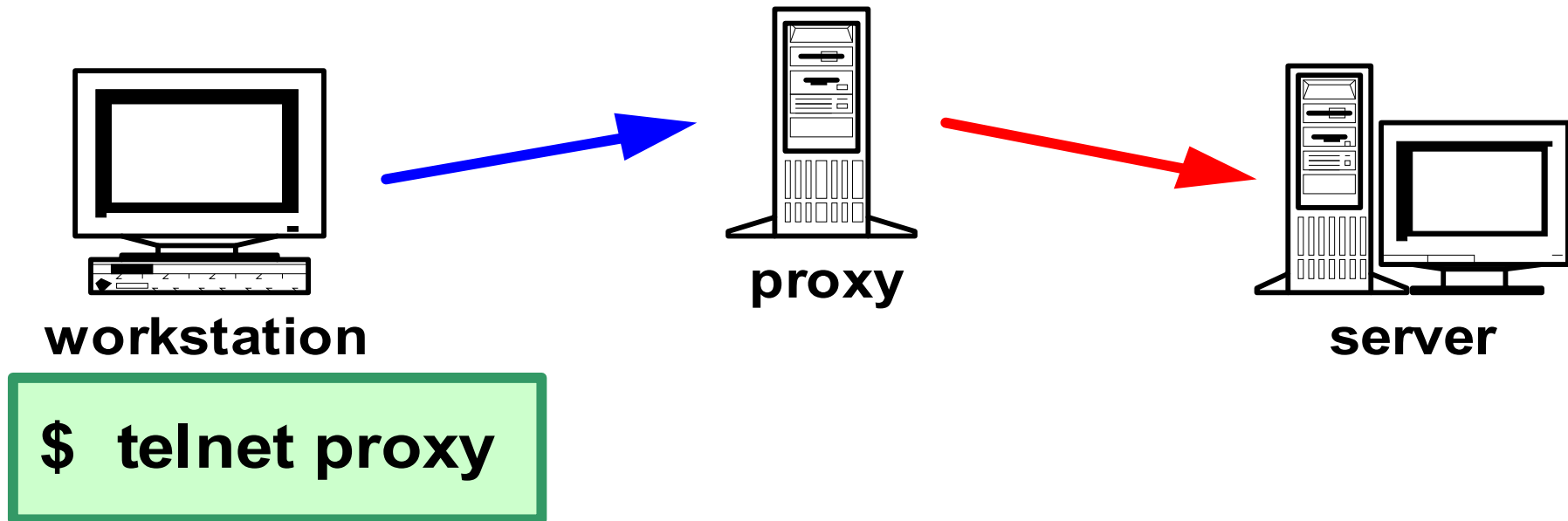
Permit 10.1.1.0/24 1024:65535 to any 21

## **Reglas para el servidor (FTP pasivo):**

Permit any 1024:65535 to 10.2.2.3 21

- **Son “proxys” no inteligentes.**
- **Simplemente generan una nueva conexión.**
- **El cliente debe conocerlo.**
- **Es independiente del protocolo.**
- **Se usan en combinación con políticas estrictas de filtrado.**
- **Ejemplo más conocido: SOCKS**

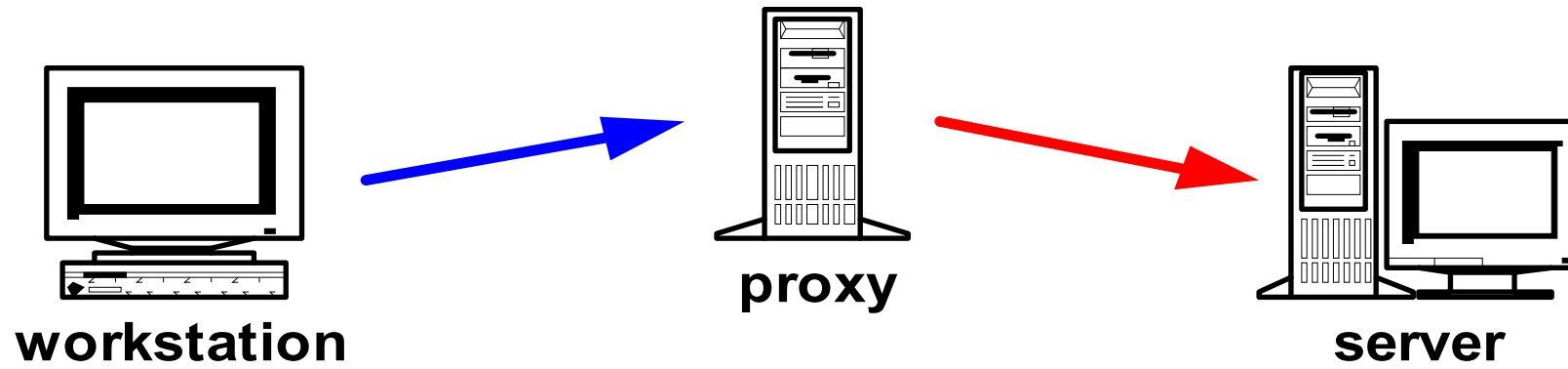
# Gateways de circuito





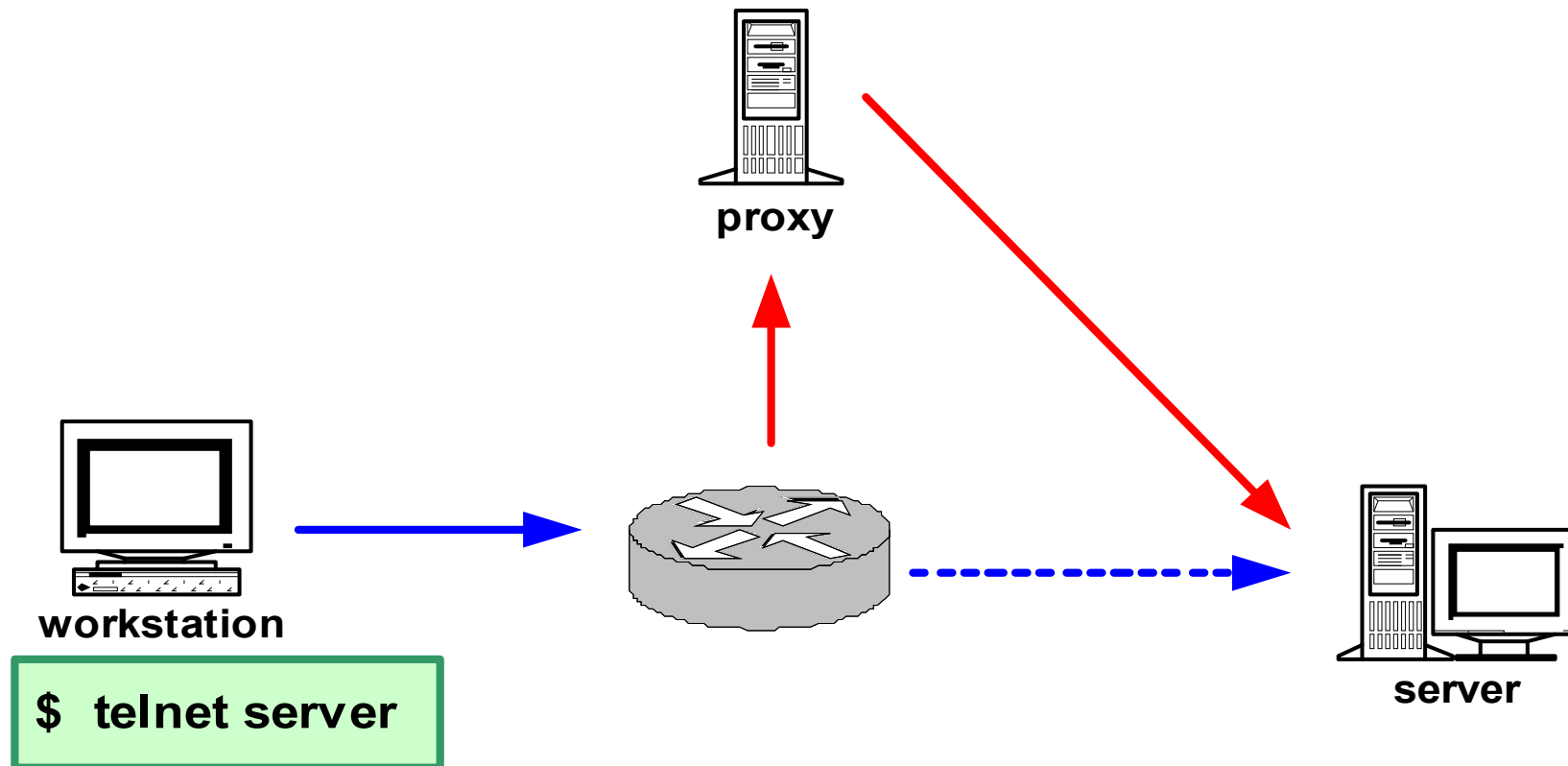
- **Conocidos como “Proxy”**
- **Entienden y manejan el protocolo en cuestión**
- **Generalmente el cliente debe conocerlo, y el protocolo debe permitir el uso de proxys.**
- **Permite manejar mejor la autenticación y el control del uso de los servicios.**
- **Provee mayores facilidades de generación de registros de auditoría.**
- **Pueden agregarse características adicionales, como el “cache”.**

# Gateways de aplicación



```
$ telnet proxy  
proxy> connect server
```

## Proxy Transparente



- Técnicas para evitar el IP spoofing.
- La técnica de Ingress filtering controla que no entren a mi red interna paquetes que vienen de una red externa pero que tienen como ip origen una ip de mi red.
- La técnica de Egress filtering asegura que paquetes con ip spoofeada no salgan de mi red.

- **Si pongo un Firewall estoy protegido.**
- **Con un Firewall protejo todo el perímetro.**
- **El vendedor es responsable de la seguridad del producto.**
- **Con este producto, usted estará completamente seguro.**
- **No somos interesantes para un Intruso.**

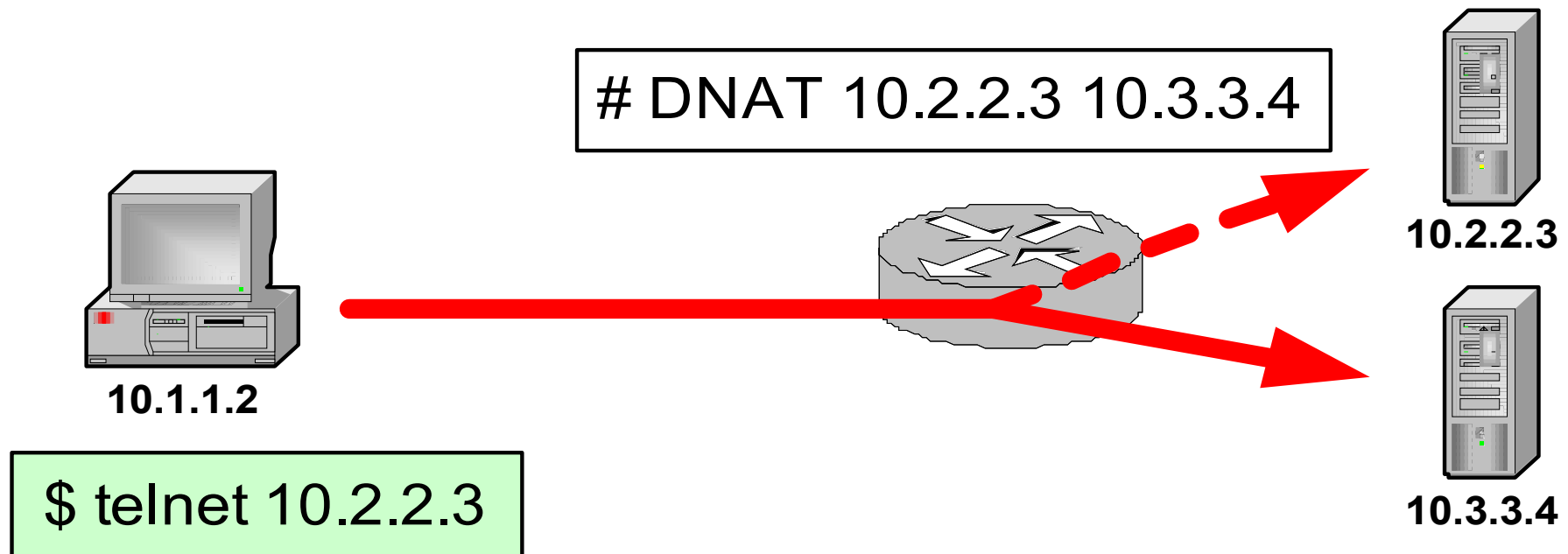


# NAT

*Network Address Translation*

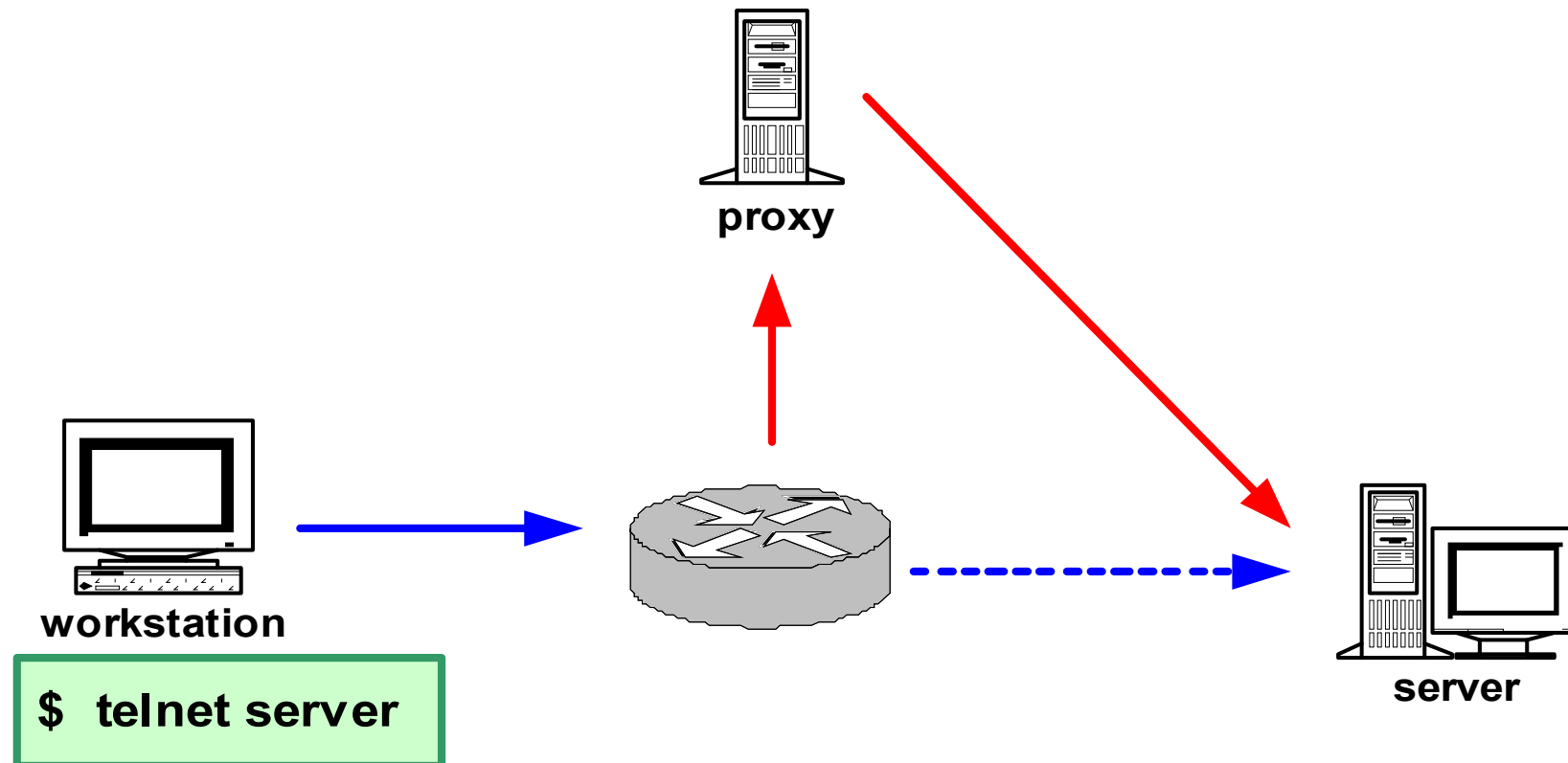
- **Network Address Translation**
- **RFC 1631 (1994)**
  - Falta de IPS
- **Oculto la topología de la Red**
- **RFC 1918**
  - Define rangos IP privados

- **DNAT**

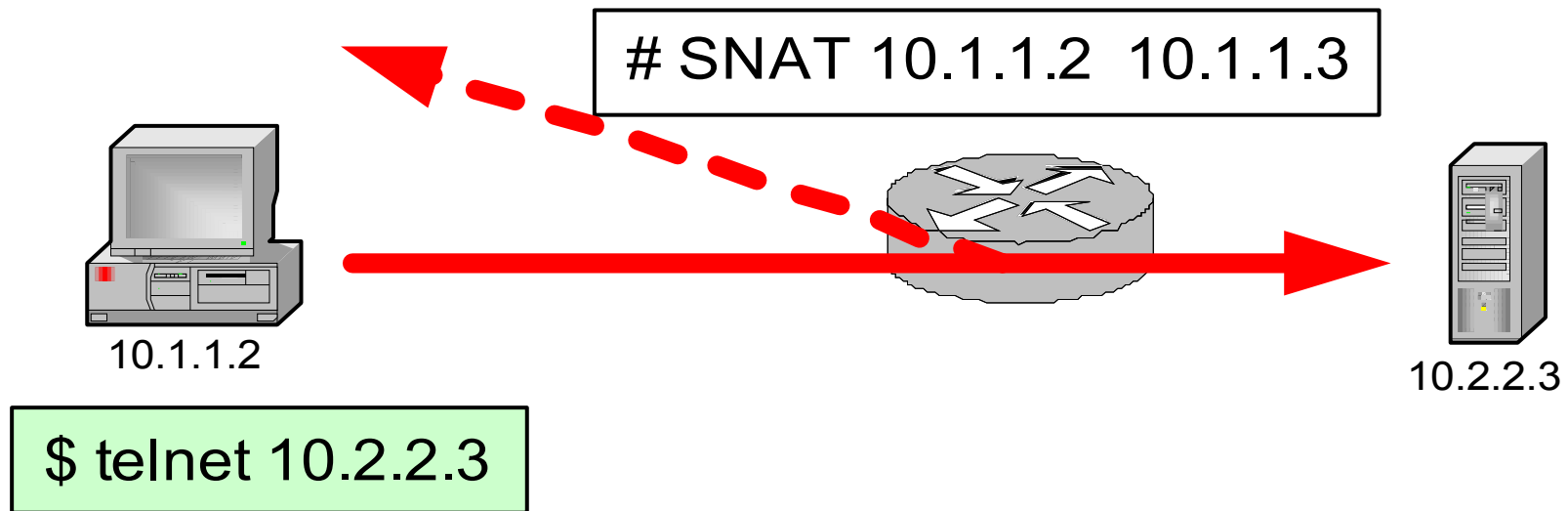




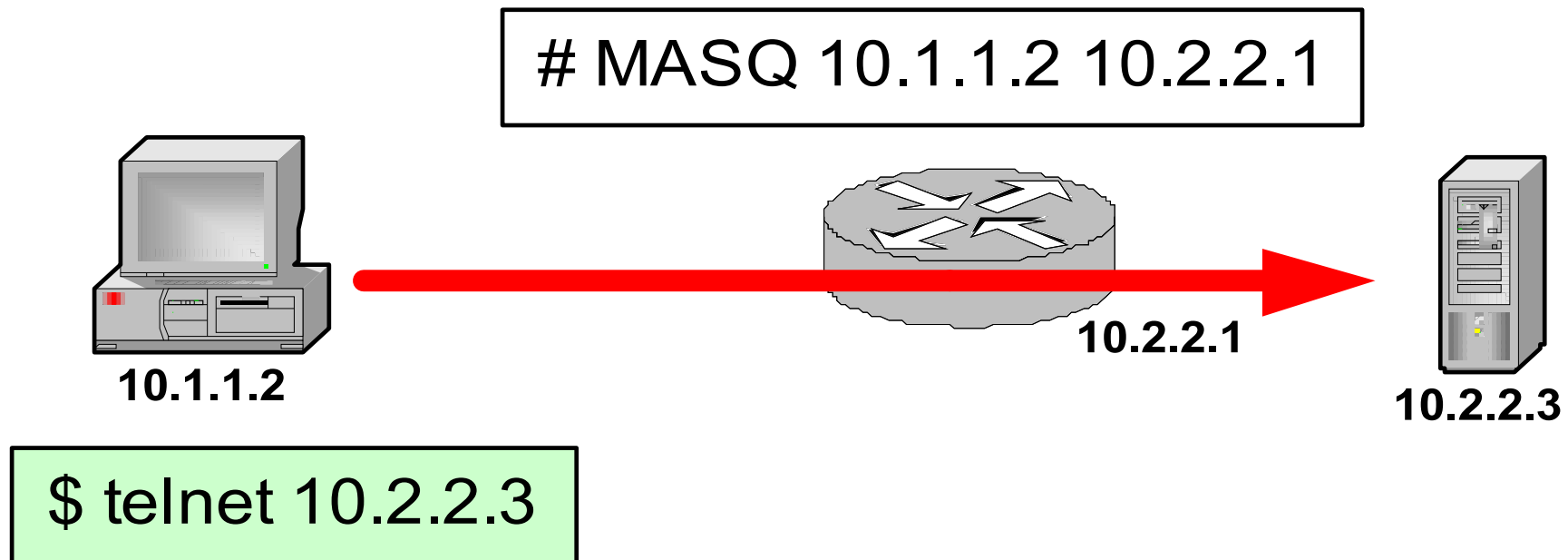
## Proxy Transparente



- **SNAT**




- **Masquerading**



- **Forma particular de SNAT**
- **Es la más usada**
- **Sirve para ocultar la topología de la red**

- **DNAT**
- **SNAT**
- **Masquerading**
- **PAT**

- **Todas se combinan con ACLs**
  - DNAT 10.1.1.1 >1024 any 80 to proxy 8080
- **Suelen combinarse entre sí**
- **Pueden ser stateful**
- **Pueden combinarse con packet inspection**
  - Por ejemplo, NAT específico para FTP



**Your IP Is**

**157.92.27.1, 10.0.0.2**

**WhatIsMyIP.com is the fastest and easiest way  
to determine your IP address.**

Courtesy of WhatIsMyIP.com

[IP Command Lines](#) [IP Addresses Explained](#)

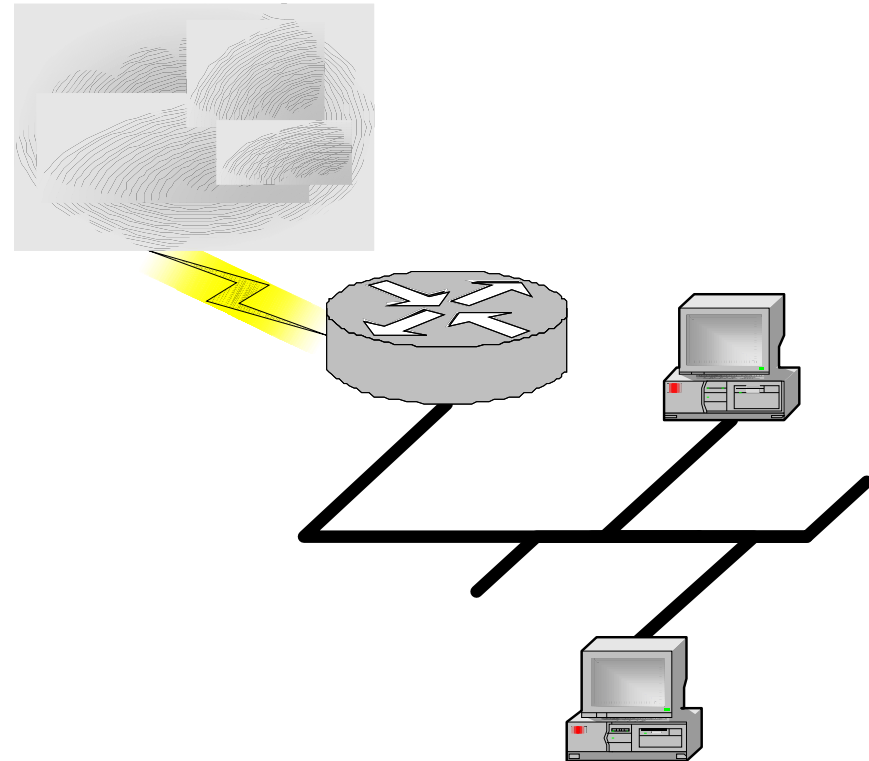


# Esquemas de redes



## Screening Router

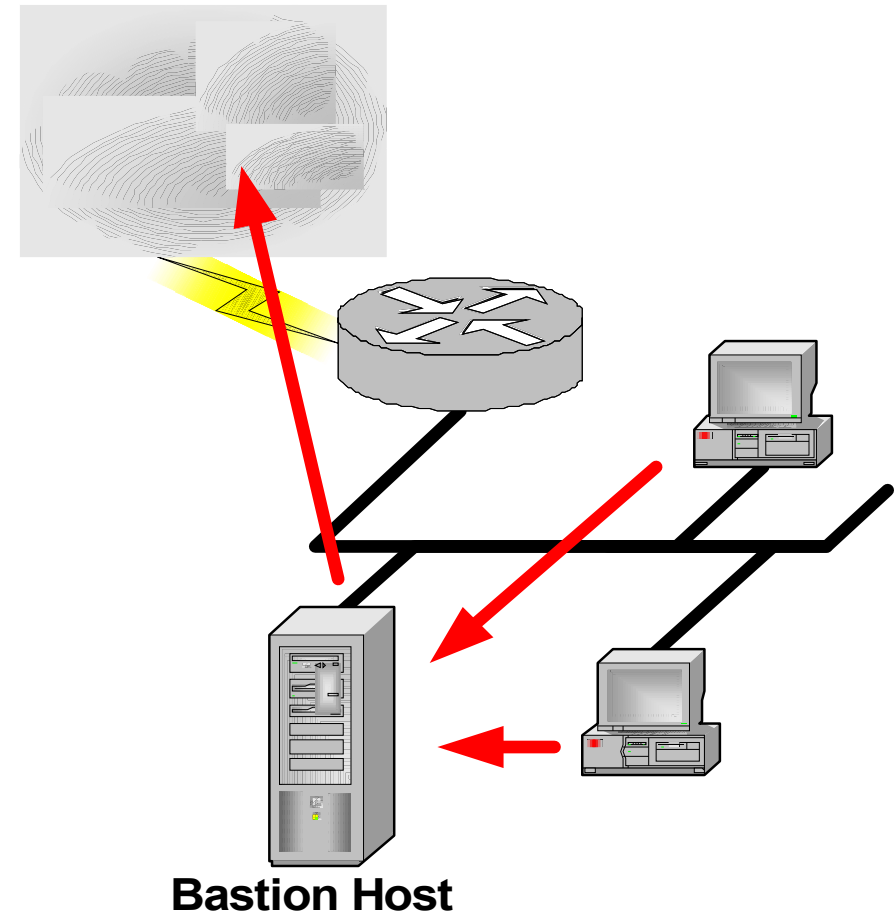
- **Filtra paquetes**
- **Reglas complejas**
- **Poca inteligencia**
- **Generalmente asociado a filtrado estático**



# Esquemas de redes con firewalls

## Screened Host (Bastion Host)

- Solo permite paquetes al bastion host
- Reglas más simples
- El BH debe ser seguro
- Suele tener Proxies

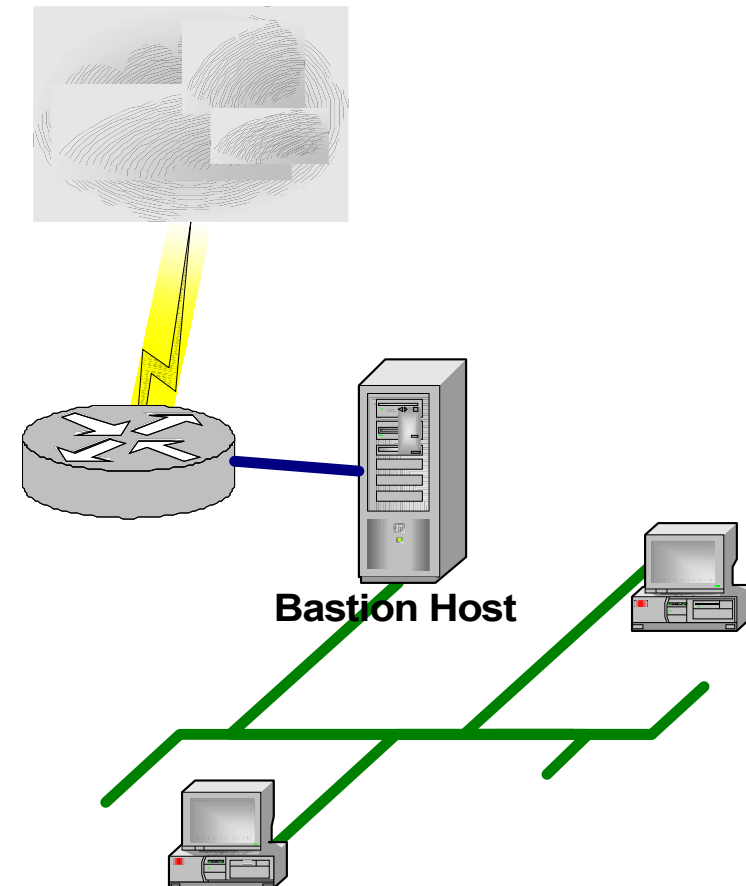


# Esquemas de redes con firewall

## Screened Host

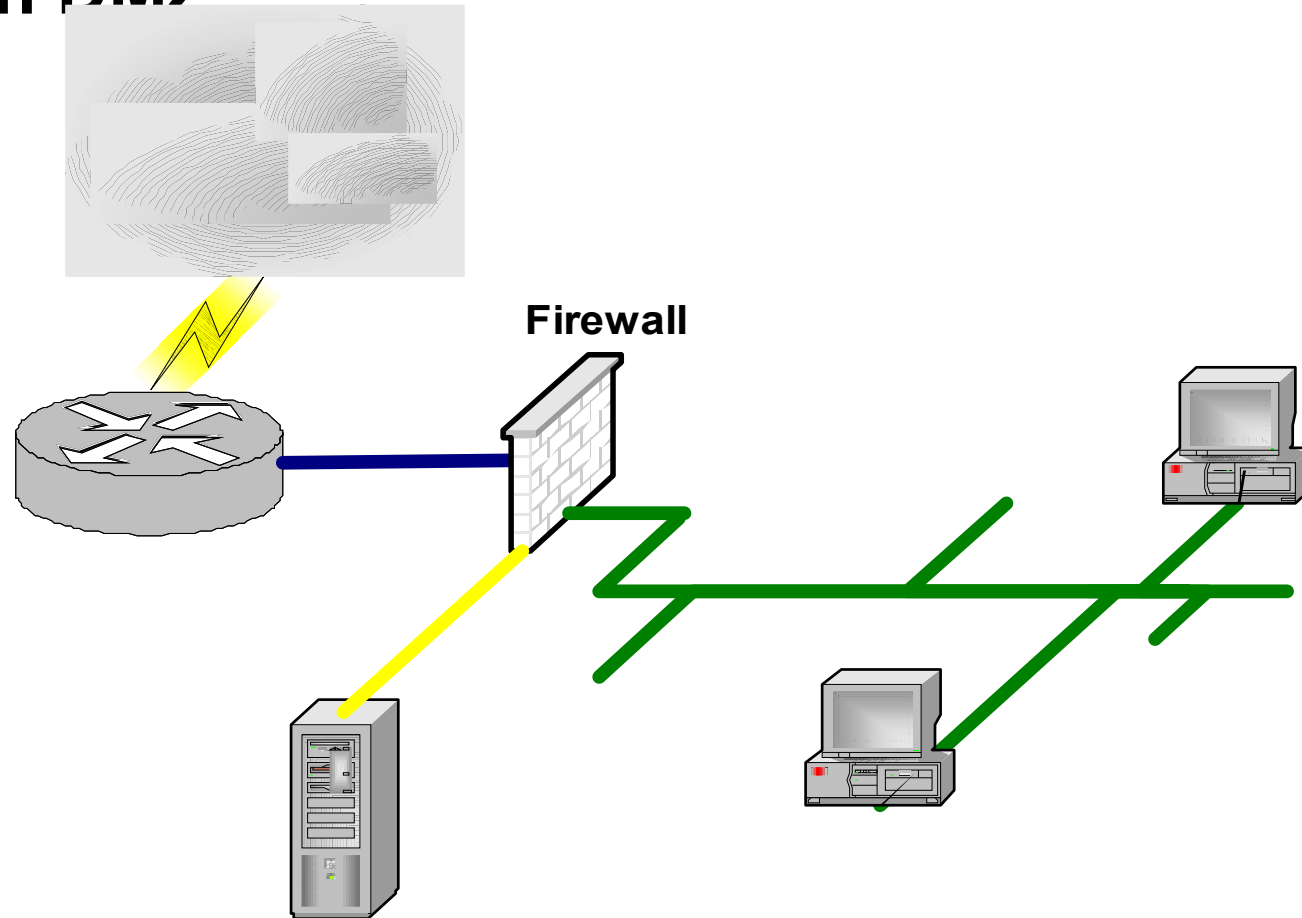
### (Dual homed Bastion Host)

- Sin ruteo a través del BH
- BH con Proxies
- Muy Robusto
- El BH debe ser seguro
- No se necesita NAT



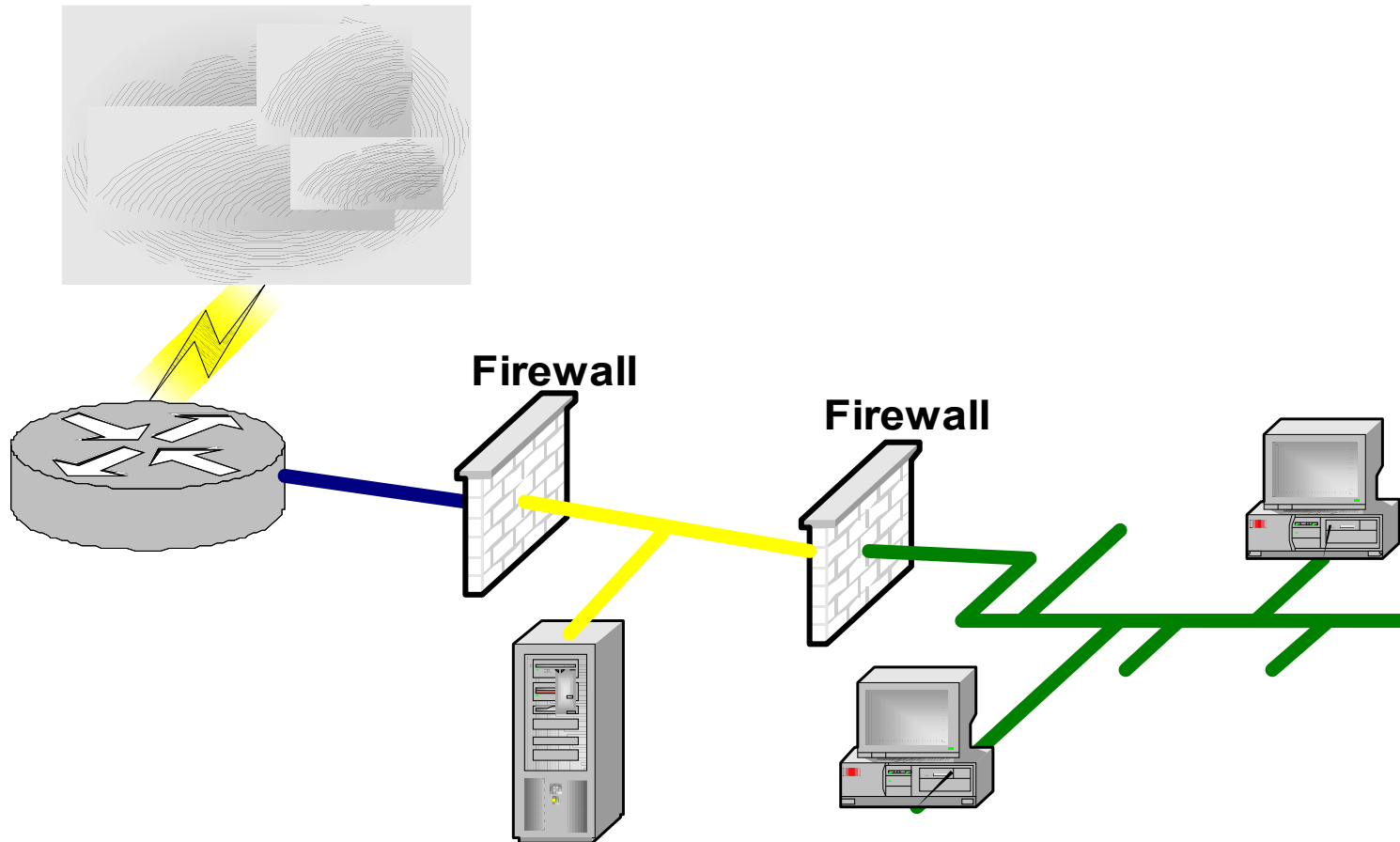
# Esquemas de redes con firewalls

## Firewall con DMZ



# Esquemas de redes con firewall

## Firewall con DMZ



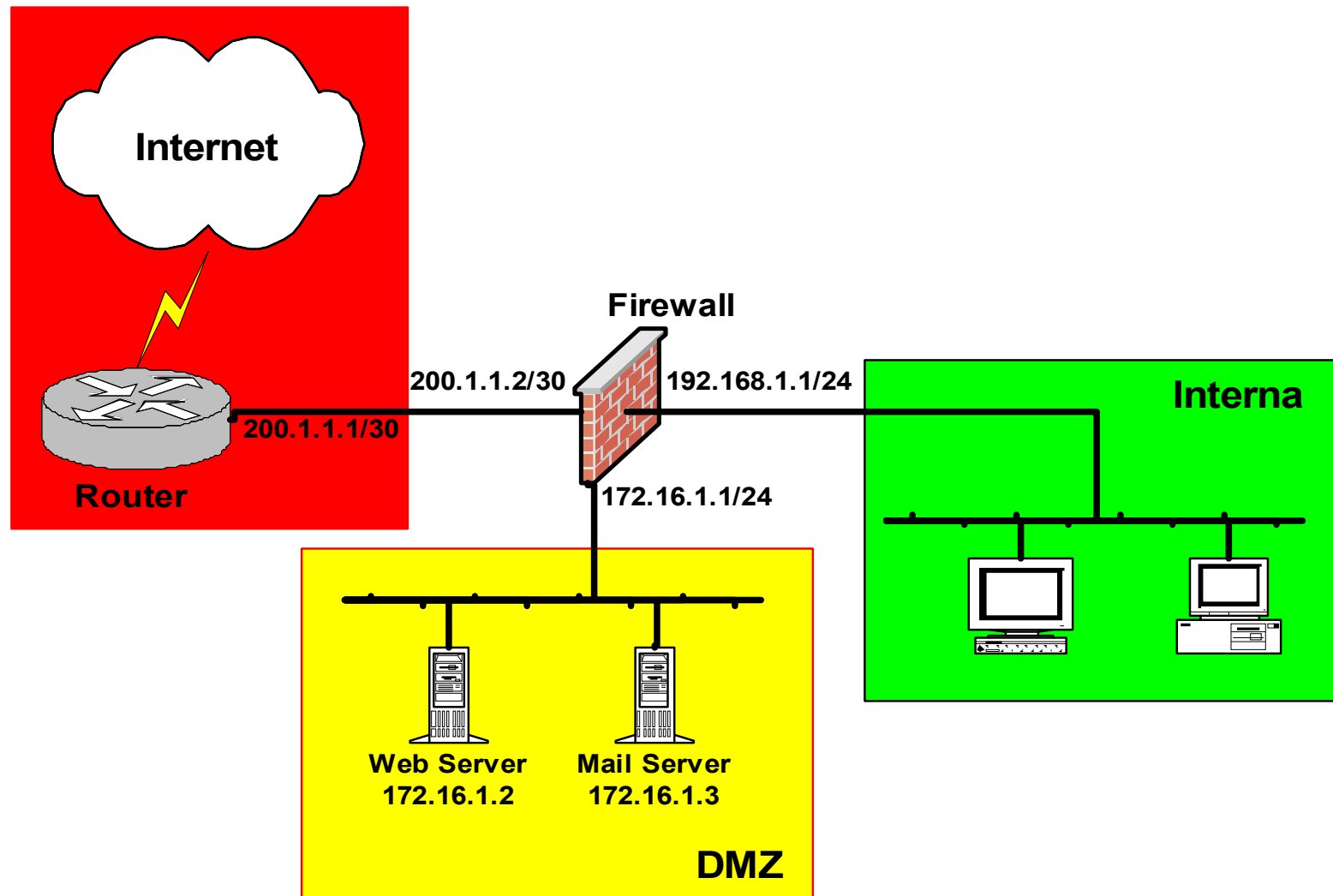
**Default Permit:** Permito todo salvo algunos protocolos, como por ejemplo telnet, rlogin, etc.

**Default Deny:** Deniego todo y luego voy habilitando únicamente lo que necesito en forma explícita.

**OJO!!! El “Default Permit” no es recomendable!! Si surge una vulnerabilidad en un servicio innecesariamente abierto y que no había filtrado, me pueden atacar!**

- **Diseño de la red.**
- **Definición de Políticas**
- **Implementación de las reglas**
- **Mantenimiento**

# Implementación: Diseño





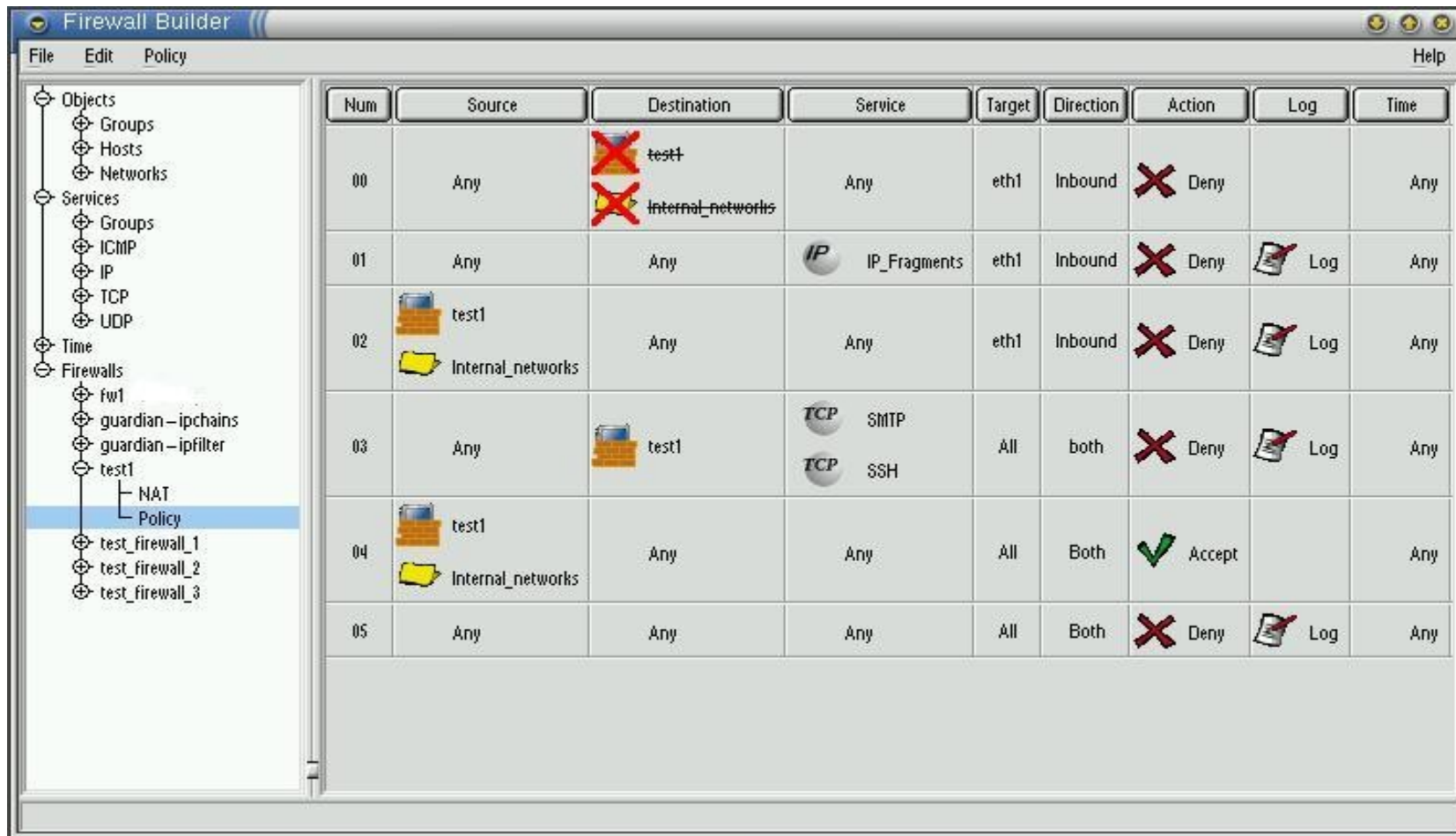
# Implementación: Políticas

	Internet	DMZ	Interna
Internet (eth0) 200.1.1.2/30		ws:http ms:smtp	NO
DMZ (eth1) 172.16.1.1/24	ms:dns ms:smtp		NO
Interna (eth2) 192.168.1.1/24	-:http	ms:smtp ms:dns ms:pop3 ws:http	

- **Configurar un firewall puede no ser una tarea sencilla. Para facilitar dicha tarea, existen aplicaciones que permiten escribir reglas con interfaces gráficas o abstracciones para escribir la configuración de forma más sencilla.**
- **Ej: FWbuilder, shorewall, etc.**

# Netfilter: fwbuilder

- <http://www.fwbuilder.org/>



- **Mantener las reglas actualizadas**
- **Actualizar el SO y el software**
- **Revisar los LOGS**
  - <http://sourceforge.net/projects/lila/>
  - <http://tud.at/programm/fwalog>
  - <http://www.gege.org/iptables>

# Logs

Sep 26 00:11:10 rodito Shorewall:net2all:DROP: IN=ppp0 OUT= MAC= SRC=200.59.11.154 DST=200.59.77.76  
LEN=48 TOS=00 PREC=0x00 TTL=122 ID=57566 CE DF PROTO=TCP SPT=3645 DPT=3306 SEQ=3134956685 ACK=0  
WINDOW=64240 SYN URGP=0

Sep 26 13:40:48 rodito Shorewall:net2all:DROP: IN=ppp0 OUT= MAC= SRC=200.59.11.245 DST=200.59.77.76  
LEN=48 TOS=00 PREC=0x00 TTL=122 ID=10710 DF PROTO=TCP SPT=2336 DPT=3306 SEQ=301533607 ACK=0  
WINDOW=64240 SYN URGP=0

Sep 26 15:46:43 rodito Shorewall:net2all:DROP: IN=ppp0 OUT= MAC= SRC=200.59.47.80 DST=200.59.77.76 LEN=48  
TOS=00 PREC=0x00 TTL=121 ID=33520 CE DF PROTO=TCP SPT=4151 DPT=3306 SEQ=1991646254 ACK=0  
WINDOW=16384 SYN URGP=0

Sep 26 17:38:25 rodito Shorewall:net2all:DROP: IN=ppp0 OUT= MAC= SRC=200.59.11.171 DST=200.59.77.76  
LEN=48 TOS=00 PREC=0x00 TTL=122 ID=15676 DF PROTO=TCP SPT=4905 DPT=3306 SEQ=3858843027 ACK=0  
WINDOW=64240 SYN URGP=0

Sep 26 19:33:34 rodito Shorewall:net2all:DROP: IN=ppp0 OUT= MAC= SRC=200.59.11.225 DST=200.59.77.76  
LEN=48 TOS=00 PREC=0x00 TTL=122 ID=19885 DF PROTO=TCP SPT=4387 DPT=3306 SEQ=3943226625 ACK=0  
WINDOW=16384 SYN URGP=0

Sep 26 19:35:52 rodito Shorewall:net2all:DROP: IN=ppp0 OUT= MAC= SRC=200.59.11.154 DST=200.59.77.76  
LEN=48 TOS=00 PREC=0x00 TTL=122 ID=16769 DF PROTO=TCP SPT=4023 DPT=3306 SEQ=1221701610 ACK=0  
WINDOW=64240 SYN URGP=0

Sep 26 19:56:54 rodito Shorewall:net2all:DROP: IN=ppp0 OUT= MAC= SRC=200.59.11.137 DST=200.59.77.76  
LEN=48 TOS=00 PREC=0x00 TTL=122 ID=32755 DF PROTO=TCP SPT=4077 DPT=3306 SEQ=2552478340 ACK=0  
WINDOW=64240 SYN URGP=0

Sep 26 21:13:02 rodito Shorewall:net2all:DROP: IN=ppp0 OUT= MAC= SRC=200.59.106.201 DST=200.59.77.76  
LEN=48 TOS=00 PREC=0x00 TTL=128 ID=63037 CE DF PROTO=TCP SPT=2039 DPT=3306 SEQ=3066055685 ACK=0  
WINDOW=16384 SYN URGP=0

Sep 26 21:46:55 rodito Shorewall:net2all:DROP: IN=ppp0 OUT= MAC= SRC=200.59.76.88 DST=200.59.77.76 LEN=48  
TOS=00 PREC=0x00 TTL=128 ID=2758 DF PROTO=TCP SPT=3746 DPT=3306 SEQ=1348136531 ACK=0  
WINDOW=16384 SYN URGP=0GP=0

# Implementación: Mantenimiento - Logs



## iptables logs

Current chain : DROP  
Nb packets / page : 20  
Packets date : 2 days  
Packet filter

Last packets filtered by chain DROP younger than 2 days :

Chain	Date	Host	Interf.	Proto.	IP	Dest. port
DROP	2002-10-06 21:06:03	nuage	ppp0	UDP	p5082C792.dip0.t-ipconnect.de	137(netbios-ns)
DROP	2002-10-06 21:00:54	nuage	ppp0	UDP	dup-200-65-6-111.prodigy.net.mx	137(netbios-ns)
DROP	2002-10-06 21:00:54	nuage	ppp0	UDP	bgrcvx038228.prexar.com	137(netbios-ns)
DROP	2002-10-06 21:00:37	nuage	ppp0	UDP	host217-39-63-27.in-addr.btopenworld.com	137(netbios-ns)
DROP	2002-10-06 20:58:35	nuage	ppp0	UDP	wkm53-01-p128.fs.saix.net	137(netbios-ns)
DROP	2002-10-06 20:37:57	nuage	ppp0	UDP	200-161-6-88.dsl.telesp.net.br	137(netbios-ns)
DROP	2002-10-06 20:32:53	nuage	ppp0	UDP	211.229.201.148	137(netbios-ns)
DROP	2002-10-06 20:13:15	nuage	ppp0	UDP	N623P014.adsl.highway.telekom.at	137(netbios-ns)
DROP	2002-10-06 20:01:57	nuage	ppp0	UDP	a213-22-193-57.netcabo.pt	137(netbios-ns)
DROP	2002-10-06 19:41:41	nuage	ppp0	UDP	216.6.110.192	137(netbios-ns)
DROP	2002-10-06 19:20:17	nuage	ppp0	UDP	hbt-a17.carrollswb.com	137(netbios-ns)
DROP	2002-10-06 19:16:36	nuage	ppp0	UDP	async219.starlinx.com	137(netbios-ns)
DROP	2002-10-06 19:05:08	nuage	ppp0	UDP	GR149096.Griffin.PeachNet.EDU	137(netbios-ns)
DROP	2002-10-06 18:57:50	nuage	ppp0	UDP	Ace21.pppool.de	137(netbios-ns)
DROP	2002-10-06 18:54:30	nuage	ppp0	UDP	bds1.66.13.220.210.gte.net	137(netbios-ns)
DROP	2002-10-06 18:46:03	nuage	ppp0	UDP	ANice-101-1-1-106.abo.wanadoo.fr	137(netbios-ns)
DROP	2002-10-06 18:31:25	nuage	ppp0	UDP	pdf7c35.kngwnt01.ap.so-net.ne.jp	137(netbios-ns)
DROP	2002-10-06 18:31:25	nuage	ppp0	UDP	pdf7c35.kngwnt01.ap.so-net.ne.jp	137(netbios-ns)
DROP	2002-10-06 18:28:45	nuage	ppp0	UDP	p3E9E88AD.dip0.t-ipconnect.de	137(netbios-ns)
DROP	2002-10-06 18:28:45	nuage	ppp0	UDP	p3E9E88AD.dip0.t-ipconnect.de	137(netbios-ns)

Records 0 to 20 of 478



### Database stats

4587 packets in database  
478 packets younger than 2 days  
219 packets today  
First was at 2002-09-10 03:24:20  
Last was at 2002-10-06 21:06:03

### Top Hosts [DROP] [2 days]

Host	Nb
80-25-180-170.uc.nombres.ttd.es	54
dup-200-65-245-77.prodigy.net.mx	37
nexus.adsl.nerim.net	36
ABoulogne-107-1-1-216.abo.wanadoo.fr	15
193-153-29-18.uc.nombres.ttd.es	12
pool34-tch-1.Sofia.Orbitel.net	9
AAubervilliers-104-1-4-86.abo.wanadoo.fr	9
montpellier-1-a7-62-147-81-154.dial.proxad.net	8
debian.proxad.net	6
195.24.216.1	6

### Top Proto [ALL] [2 days]

Proto	Nb
TCP	252
UDP	226

### Top Ports [2 days]

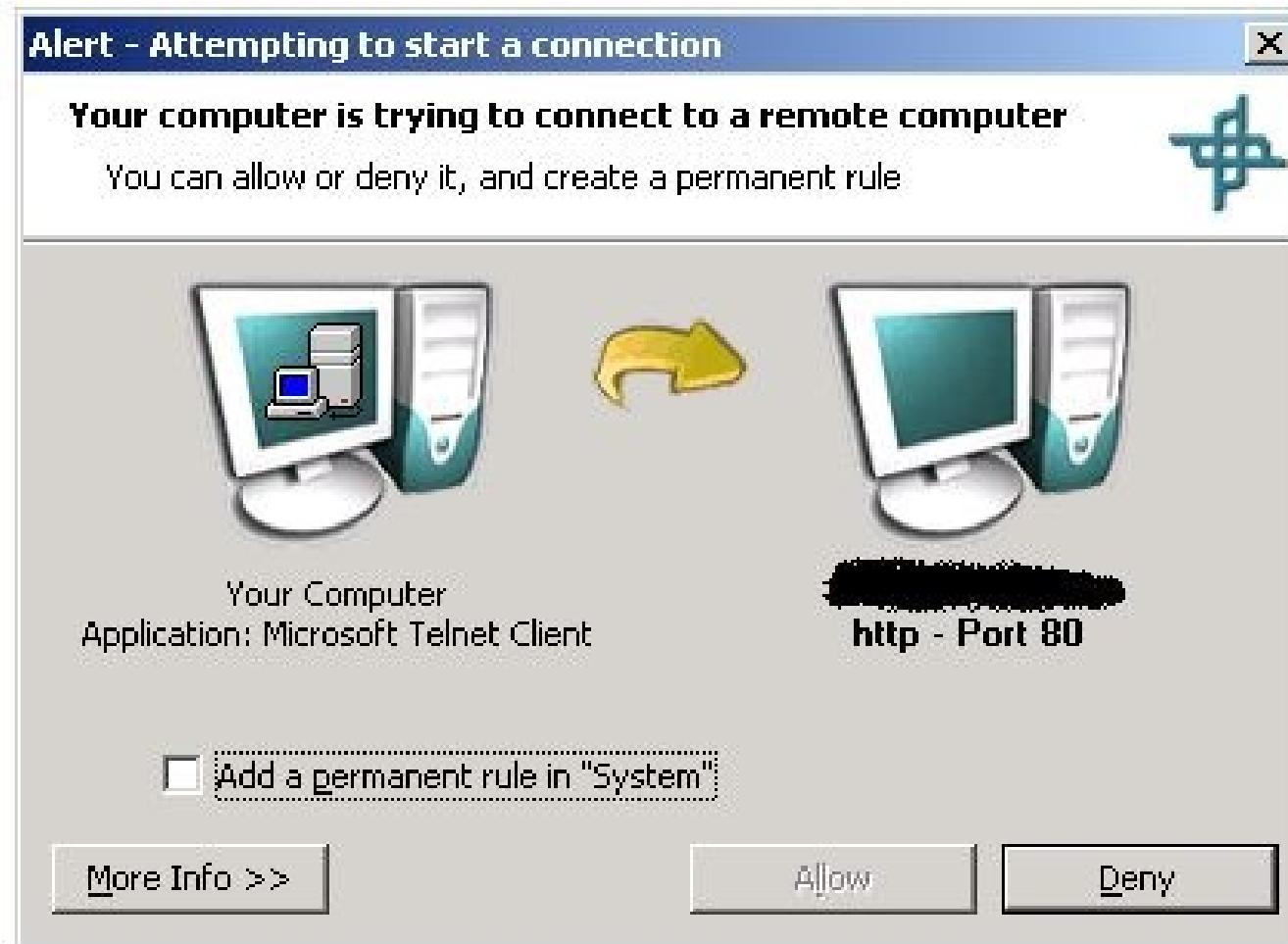
Port	Number	Nb
netbios-ns	137	213
unknown	4662	99
kazaa	1214	95
unknown	4668	13
ms-sql-s	1433	9
ftp	21	8
netbios-ssn	139	7
unknown	6761	7
ident	113	6
unknown	23424	6

Un firewall personal es un software instalado en un sistema, generalmente la estación de trabajo de un usuario, que controla la comunicación de y hacia ese equipo.

En el caso de los productos para windows, generalmente brindan la posibilidad de filtrar las comunicaciones en base a la aplicación local que intenta iniciarlas, permitiendo definir que aplicaciones pueden acceder a internet, y consultandolo cuando una aplicación desea establecer una nueva comunicación.



# Firewall Personal





# Unified Threat Management (UTM)

- **Solución que incluye varios componentes (no siempre todos):**
- **Firewall de red stateful inspection**
- **Antivirus de red**
- **Anti-spam**
- **Filtrado de contenidos**
- **IDS/IPS**
- **Data leak prevention (DLP)**
- **VPN**

# Next-Generation Firewall

- **Firewall que contiene mayor funcionalidad, y que inspecciona el tráfico con más nivel de detalle:**
- **Detección de protocolo de aplicación, independiente del puerto de comunicaciones.**
- **User Role Firewalling**
- **IPS**
- **SSL Proxy**
- **Manejo de redundancia y alta disponibilidad.**
- **Para algunos, más orientado a soluciones enterprise.**
- **En general, el nombre es una cuestión comercial. A nivel técnico, en algunos casos, UTM = NGFW**

- **Cheswick, W., Bellovin, S. and Rubin, A. D.,** Firewalls and Internet Security: Repelling the Wily Hacker, 2nd Edition, **ISBN 0-201-63466-X, Addison-Wesley, 2003.**
- **1st edition online:** <http://www.wilyhacker.com/1e/>
- **Shimonski, R., Shinder, T,** The Best Damn Firewall Book Period, **ISBN 1-931836-90-6, Syngress, 2003.**