Un firewall realizzato con una ACL e un Proxy gateway.

Roberto Alfieri - INFN Parma

Secondo Incontro di GARR-B: La sicurezza in Rete

Napoli 17-18 Gennaio 2000

SOMMARIO:

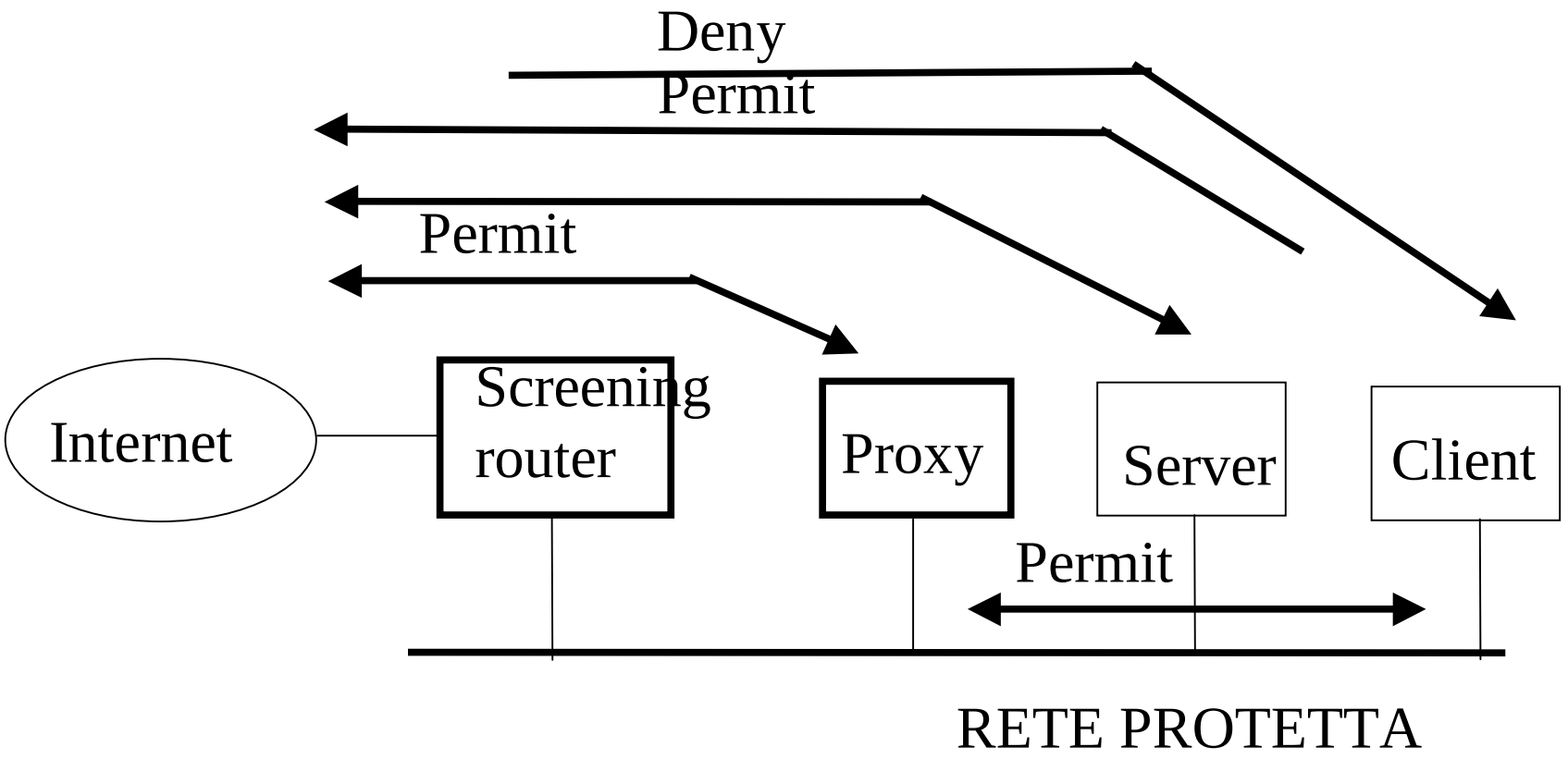
- Gli obiettivi
- Il progetto
- L'Access Control List
- La temporizzazione dell'ACL
- I proxy telnet e ftp
- Conclusioni

OBIETTIVI:

- Protezione della rete
- Criteri non eccessivamente restrittivi
- Massima trasparenza per l'utente della LAN
- Software pubblico dominio
- Senza hardware aggiuntivo

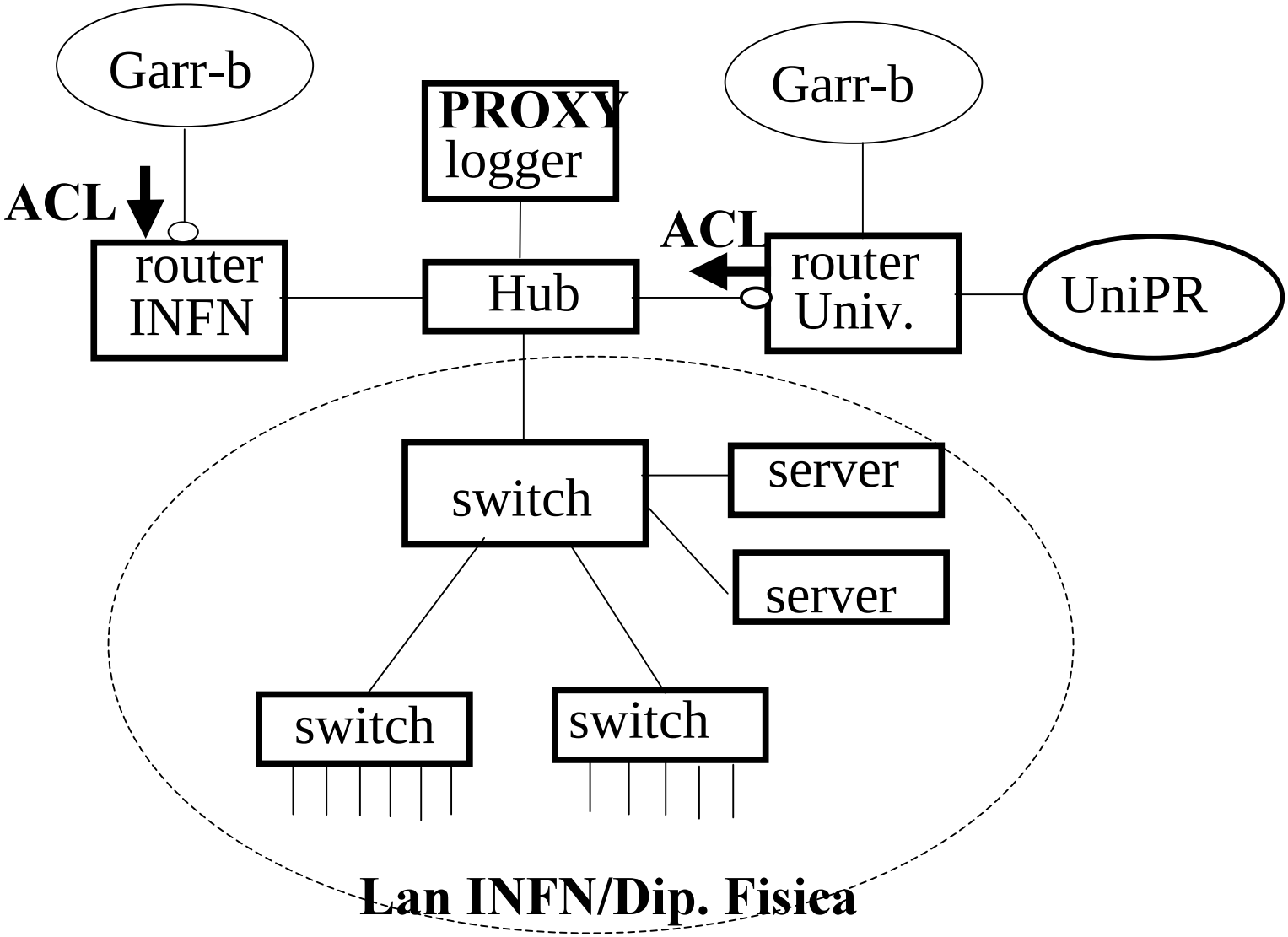
IL PROGETTO:

- Collaborazione con il CCE dell'Univ. Di Parma.
- Utilizzo delle principali tipologie di firewall:
  Packet screeneng e Proxy Gateway.
- Il packet screening, realizzato con ACL sul router Cisco, permette l'accesso ai proxy o direttamente ai servizi.
- I proxy, realizzati con FWTK, regolamentano l'accesso ai servizi piu' critici (es. telnet e ftp).
- ACL temporizzate per avere maggiore sicurezza quando la rete non e' presidiata (notte e festivi).


Deny
Permit
Permit
Internet
Screening
router
Proxy
Server
Client
Permit
RETE PROTETTA

IL CONTESTO:

- INFN Parma
- 3 reti di classi C : INFN, Dip. Fisica, Didattica (priv.)
- Circa 500 nodi IP
- 1 Linea Frame Relay 2 Mbyte INFN-GARRB
- 1 Router Cisco 4000
- 1 Peering in Ethernet con l’Universita’


Garr-b
PROXY
logger
Garr-b
ACL
ACL
router
INFN
Hub
router
Univ.
UniPR
switch
server
server
switch
switch
Lan INFN/Dip. Fisica

REGOLE PRINCIPALI DEL FILTRO:

- Nessuna restrizione sulle connessioni TCP uscenti
- Telnet e ftp permessi solo verso il proxy-gateway
- SSH e ICMP senza restrizioni
- SMTP POP3 IMAP HTTP FTP (…) solo verso i server interni
- Domain (53/tcp, tutte/udp) verso server DNS
- X11 non passa (incapsulato in ssh o proxy-telnet)
- FTP download: abilitazione tcp>1023 o Pasv e Proxy
- Tutto il resto non passa

ACL (1/3):

```
! Comunicazione tra eventuali LAN interne, necessario
! in caso di ACL sulla interfaccia interna (lato LAN)
access-list 140 permit ip "net1" 0.0.0.255 any
access-list 140 permit ip "net2" 0.0.0.255 any
!
! abilitazione connessioni tcp stabilite dall'interno
access-list 140 permit tcp any any established
!
! (continua)
```

ACL (2/3):

```
!
access-list 140 permit tcp any any eq ssh
access-list 140 permit tcp any any eq ftp-data
access-list 140 permit icmp any any
access-list 140 permit tcp any host "webserver" eq www
access-list 140 permit tcp any host "smtpserver" eq smtp
access-list 140 permit tcp any host "mailserver" eq pop3
access-list 140 permit tcp any host "mailserver" eq imap
access-list 140 permit tcp any host "telnet-gw" eq telnet
access-list 140 permit tcp any host "ftp-gw" eq ftp
access-list 140 permit tcp any host "dnsserver" eq domain
access-list 140 permit udp any host "dnsserver”
!
! (continua)
```

ACL (3/3):

```
!
! abilitazione (con logging) delle porte "alte" per ftp
! in alternativa al proxy-ftp e PASV
! Viene inoltre bloccata la connessione X11 (entrante)
access-list 140 deny   tcp any any range 6000 6063
access-list 140 permit tcp any any gt 1023 log
!
! Eventuali abilitazioni locali
!
! tutto il resto non passa
access-list 140 deny   ip any any log
```

LA TEMPORIZZAZIONE DELL'ACL:

- ACL permissiva o inesistente durante le ore lavorative (LAN presidiata)
- ACL restrittiva durante la notte e i fine settimana (LAN non presidiata)
- Script enable/disable via CRON

LA TEMPORIZZAZIONE DELL'ACL: CONFIGURAZIONE DEL ROUTER

```
! host abilitato a lanciare lo script
access-list 23 permit "cron-server"

! abilitazione sul terminale virtuale numero 6
line vty 6
 access-class 23 in
 access-class 23 out
 login local
 rotary 6
```

LA TEMPORIZZAZONE DEL'ACL: LO SCRIPT IN CRON

```
(echo 'username xxx';  sleep 2;
echo 'password yyy';  sleep 2;
echo 'ena';  sleep 2;
echo 'username xxx';  sleep 2;
echo 'password yyy';  sleep 2;
echo 'terminal monitor';  sleep 2;
echo 'configure terminal';  sleep 2;
echo 'int eth zzz';  sleep 2;
echo 'ip access-group 140 out';  Sleep 2;
!!!!!! echo 'no ip access-group 140 out';
echo 'exit';)
| telnet router-name 3006
```

FireWall ToolKit (FWTK):

- Fwtk 2.1 (www.fwtk.org)
- Red Hat 6.1 , Ppro200, 64MB
- Proxy telnet, rlogin, X, ftp, smtp, http
- Logging
- Autenticazione (password, S/key, ..)

/etc/inetd.conf

```
ftp     stream tcp nowait root /usr/local/etc/ftp-gw ftp-gw
telnet  stream tcp nowait root /usr/local/etc/tn-gw tn-gw
authsrv stream tcp nowait root /usr/local/etc/authsrv authsrv
```

/etc/services

```
authsrv 7777/tcp
```

/usr/local/etc/netperm-table (esempio):

```
ftp-gw: welcome-msg /usr/local/etc/ftp-welcome.txt
ftp-gw: permit-hosts *
tn-gw: authserver localhost 7777
tn-gw: welcome-msg /usr/local/etc/tn-welcome.txt
tn-gw: xforwarder /usr/local/etc/x-gw
tn-gw: permit-hosts *.infn.it -xok
tn-gw: permit-hosts * -auth
authsrv: hosts 127.0.0.1
authsrv: database /usr/local/etc/fw-authdb
authsrv: permit-hosts localhost
x-gw: permit-hosts *
```

Esempio di connessione al tn-gw:

```
> Telnet tn-gw.pr.infn.it
Username: User
Password: *****
##########################################
  Dipartimento di Fisica di Parma - INFN Parma
  Benvenuti al telnet-gateway tn-gw.pr.infn.it
 Per utilizzare Xwindow:  x clientname
 Per connettersi ad un host: c hostname
##########################################
tn-gw-> c archimede.pr.infn.it
```

CONCLUSIONI:

- Un filtro temporizzato e' attivo dal marzo 1998
- Da aprile 1999 e' attivo un filtro (non temporizzato) con proxy
- Il carico sulla CPU del Cisco e' trascurabile
- Alcune richieste di utenti (all'inizio) per "aperture" verso PC con ftp o web server