LA SICUREZZA NELL'USO DELLA RETE

13 maggio 2014 - Claudio Bizzarri

Modulo avanzato

MODULO AVANZATO
LA SICUREZZA NELLA PROGETTAZIONE DELLA RETE

- Firewall
  - architettura
  - vari tipi di firewall e loro caratteristiche
  - la scelta del firewall
  - installazione, programmazione e manutenzione
- Wireless
  - accesso sicuro a reti senza fili
  - prestazioni e limiti
  - architetture complesse: casi di studio
- Smaterializzazione
  - il cloud: minaccia o risorsa
  - Smaterializzazione documentale
  - Smaterializzazione dei computer
  - Smaterializzazione delle infrastrutture
  - IoT: Internet delle cose

FIREWALL

FIREWALL

- il firewall è solo uno strumento, se usato male (o non usato) non ha alcuna utilità

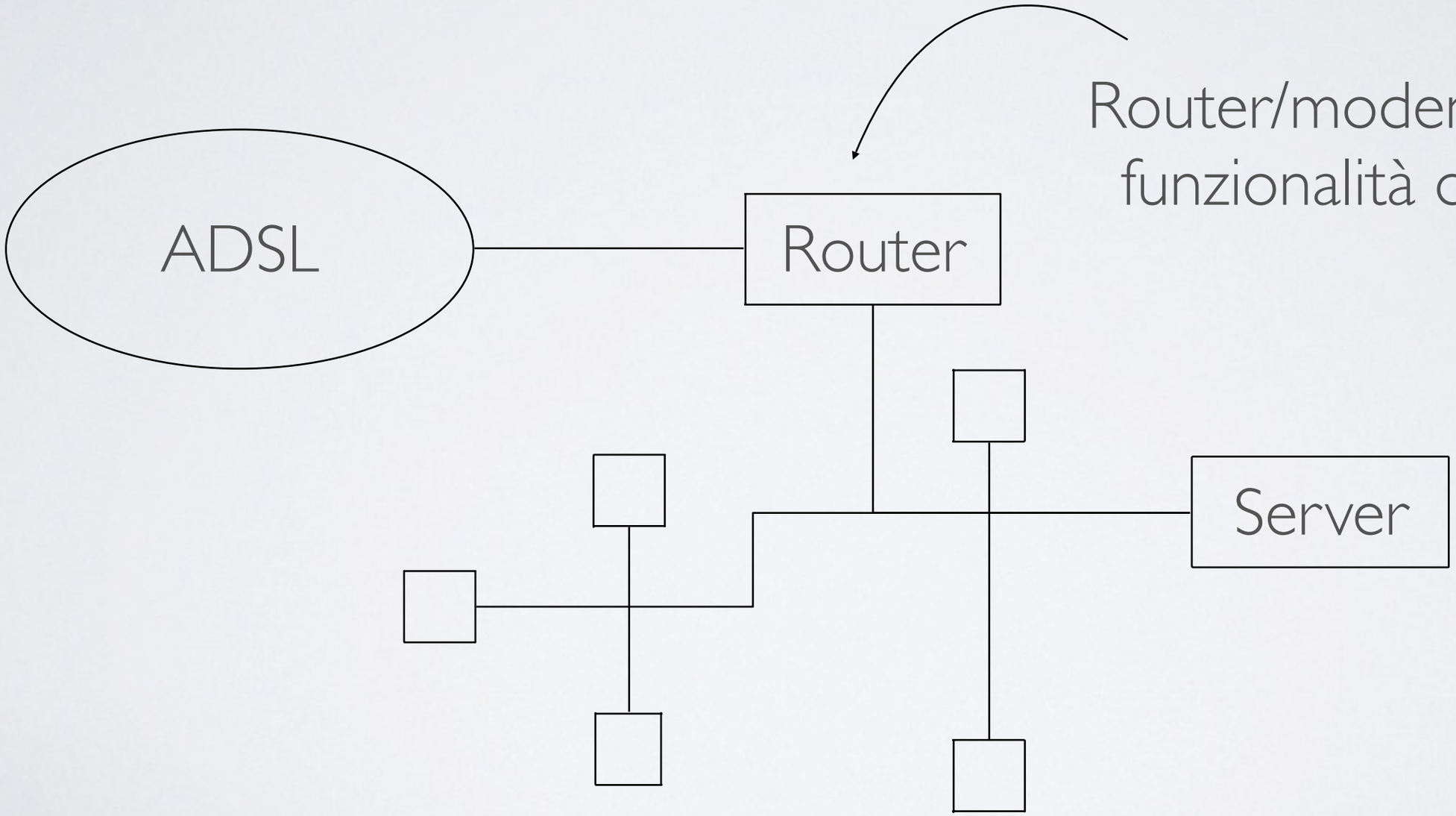
- la configurazione e la manutenzione sono più importanti della "scatola" vera e propria

ARCHITETTURA DEI FIREWALL

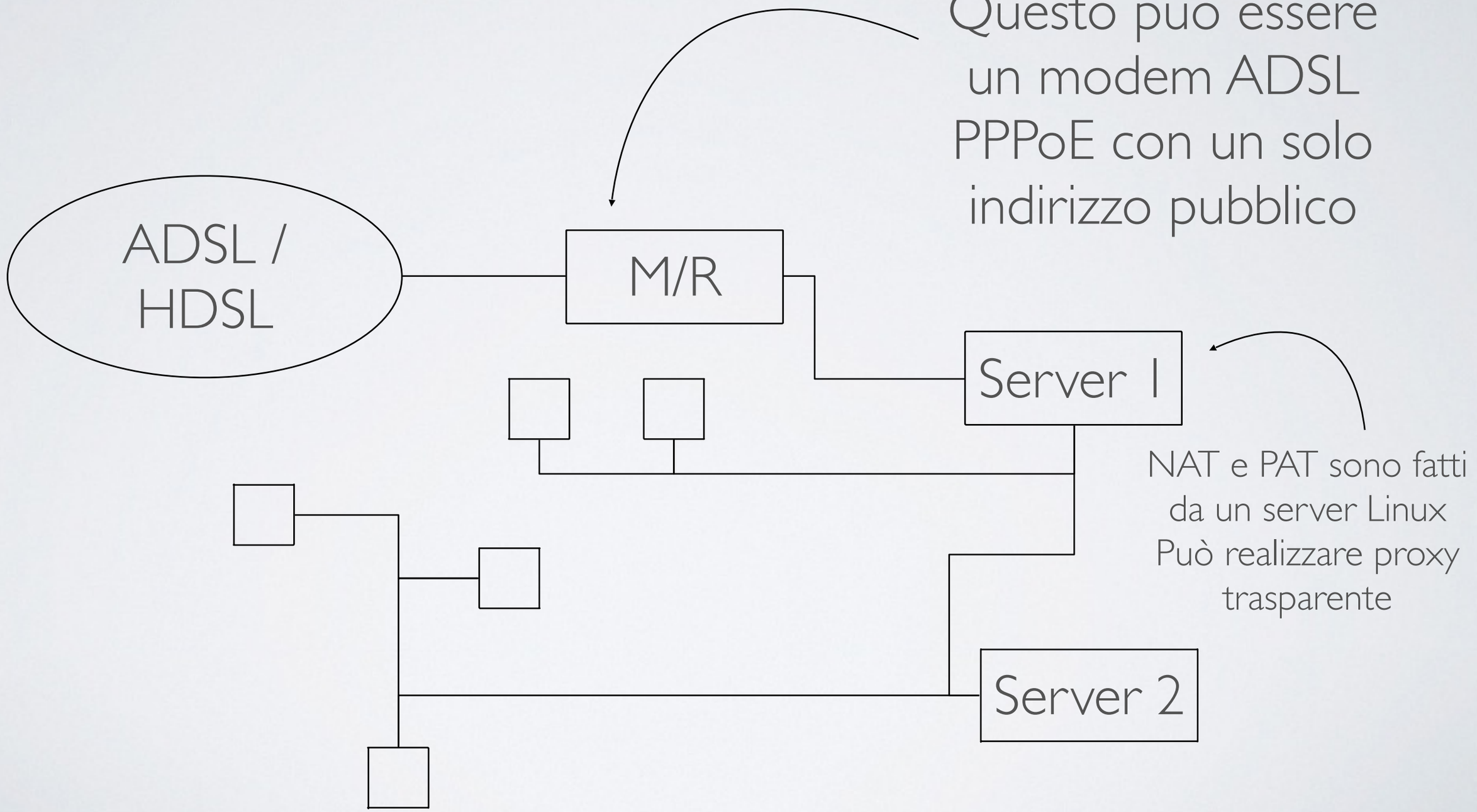
- Il firewall è un componente o un insieme di componenti per la restrizione di accessi ad una rete

- La struttura del sistema dipende fortemente dalle esigenze di sicurezza dell'organizzazione

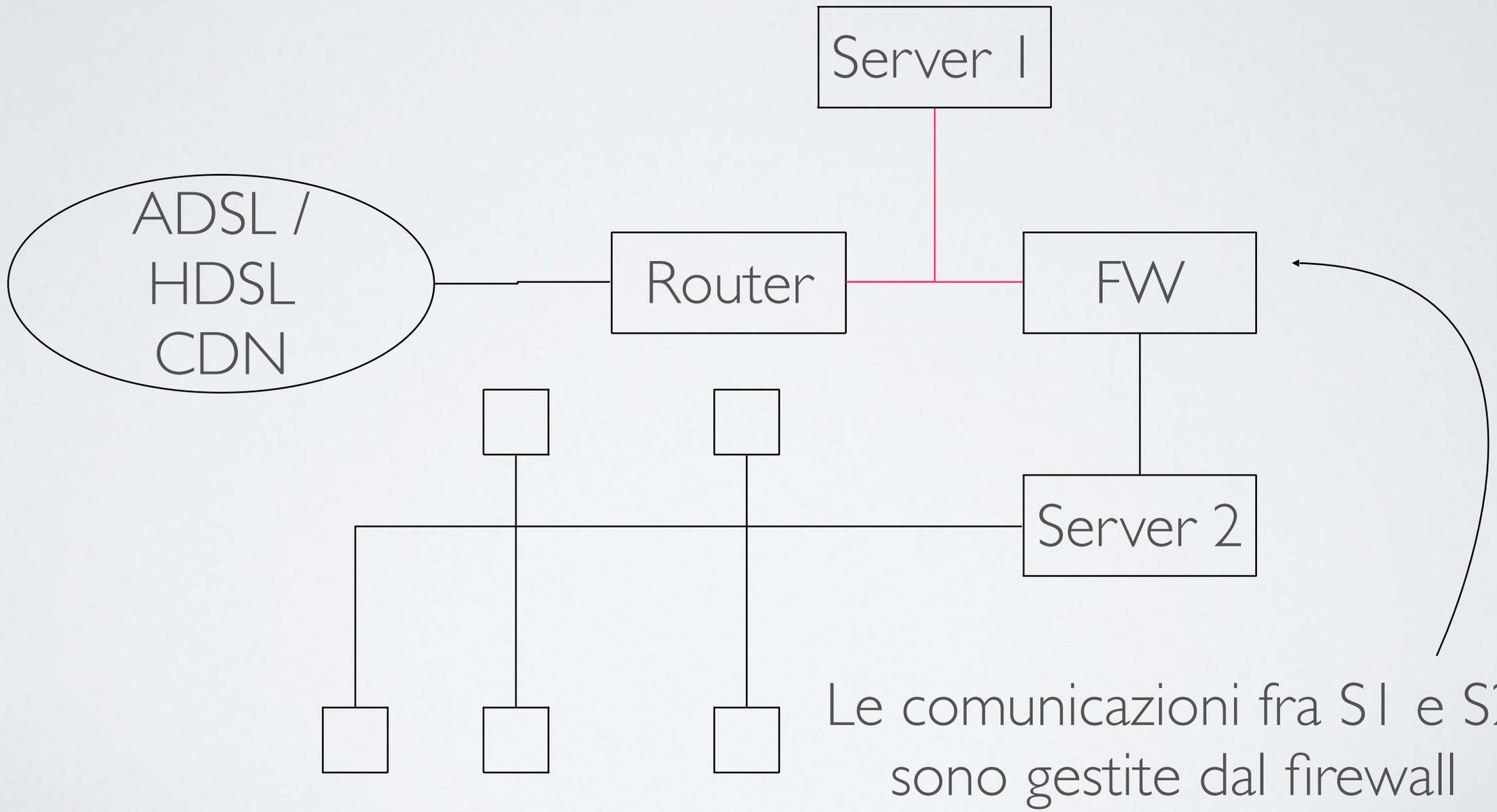
CONFIGURAZIONI DI RETE
I INDIRIZZO IP PUBBLICO



CONFIGURAZIONI DI RETE
1-2 (1-4) INDIRIZZI IP PUBBLICI



CONFIGURAZIONI DI RETE
3 O PIÙ INDIRIZZI IP PUBBLICI (8 O PIÙ)

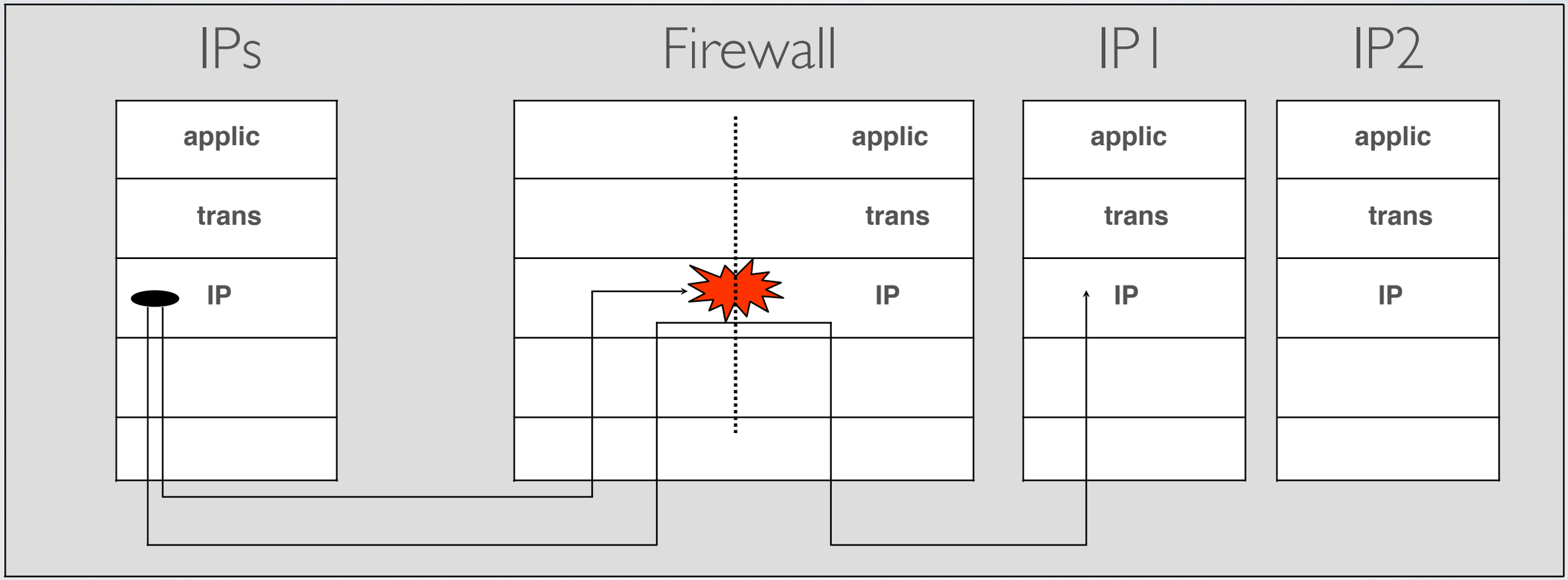


IL SISTEMA FIREWALL

Le funzioni di un sistema firewall sono:

- autorizzazione
- monitoraggio
- modifica

FIREWALL LIVELLO RETE



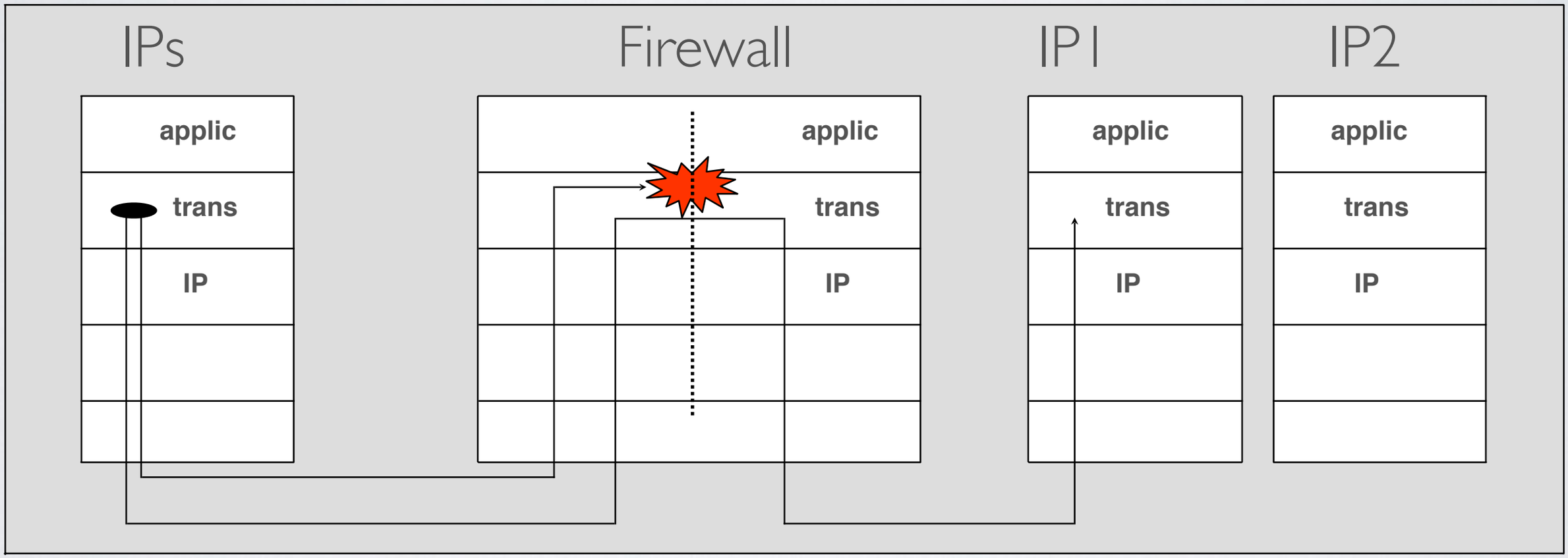
FIREWALL LIVELLO RETE

- Le operazioni vengono svolte basandosi sull'intestazione IP

- Sono possibili filtraggi basati sull'IP mittente e destinatario, sulla frammentazione e sulle opzioni

- Questo tipo di firewall viene chiamato anche **PACKET FILTER**

FIREWALL LIVELLO TRASPORTO



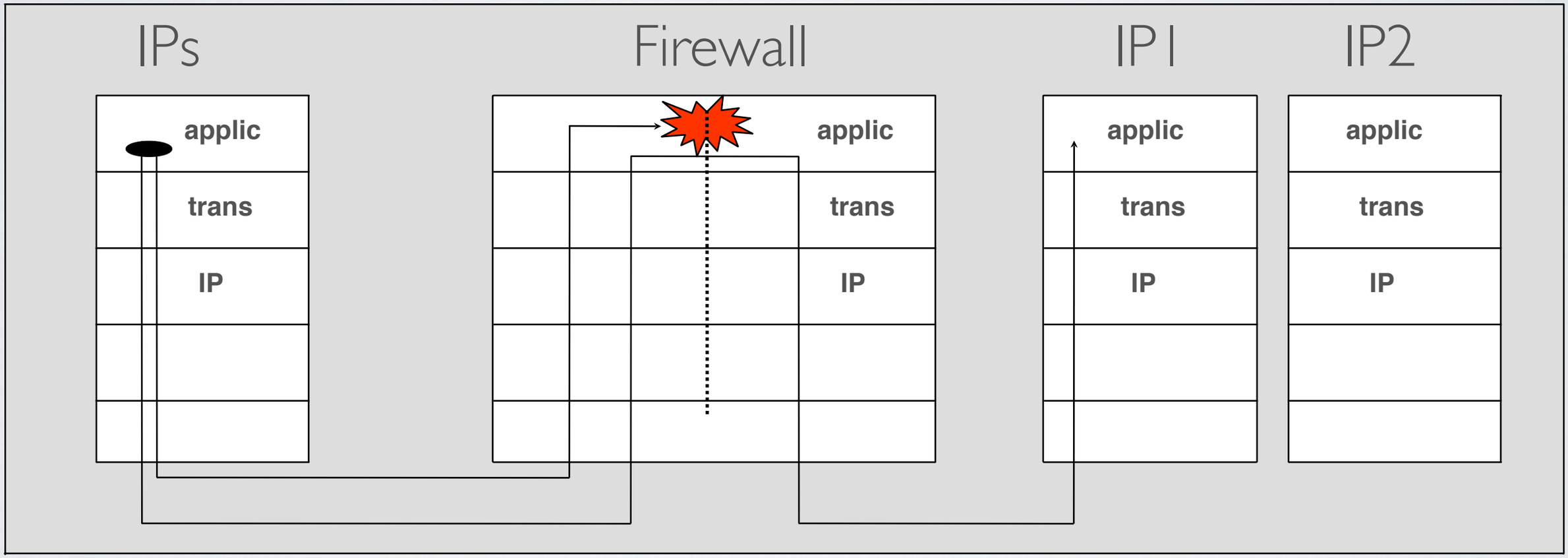
FIREWALL LIVELLO TRASPORTO

- Le operazioni vengono svolte basandosi sull'intestazione TCP e UDP

- Sono possibili filtraggi sofisticati, basati sulle quadruple IP/porta mittente/destinatario, sui flag TCP e sui valori delle finestre

- Possono essere anche **STATEFULL**

FIREWALL LIVELLO APPLICATIVO



FIREWALL LIVELLO APPLICATIVO

- Le operazioni vengono svolte basandosi sull'analisi del contenuto del livello applicativo

- Firewall di questo tipo debbono avere potenze di calcolo e memoria notevoli, soprattutto al crescere della rete che debbono controllare

- Necessitano di frequenti aggiornamenti software o addirittura di licenze e abbonamenti

AUTORIZZAZIONE

RETE: packet filter

TRASPORTO: packet filter, filtraggio sulle porte o sullo stato di sessione

APPLICATIVO: content filter, application filter

MONITORAGGIO

RETE: P2P

TRASPORTO: sessioni

APPLICATIVO: analisi del traffico web, email, ecc.

MODIFICA

RETE: rare applicazioni

TRASPORTO: Captive Portal, NAT/PAT

APPLICATIVO: applicazioni sofisticate (aziendali)

NAT

192.168.1.0/24

Sadd: 10
SP: 4521
Dadd: 1.2.3.4
DP: 80

Sadd: 11
SP: 5623
Dadd: 1.2.3.4
DP: 80

Sadd: 12
SP: 2121
Dadd: 1.2.3.4
DP: 80

Tabella

Sadd 10	SP 4521	SP 9000
Sadd 11	SP 5623	SP 9001
Sadd 12	SP 2121	SP 9002

Timeout: 120s

Internet

80.121.23.21

PAT

192.168.1.0/24

add: 10

add: 11

add: 12

Tabella

Dport 80	Dadd 10	Dport2 80
Dport 110	Dadd 11	Dport2 110
Dport 8080	Dadd 12	Dport2 80

Tabella dinamica

Sadd 1.2.3.4	Dport 80	Res 10:80
Sadd 3.4.5.6	Dport 110	Res 11:110
Sadd 7.8.9.1	Dport 8080	Res 12:80

Timeout: 120s

Internet

80.121.23.21

L'ANTICIPO E IL MODELLO T

L'ANTICIPO E IL MODELLO T

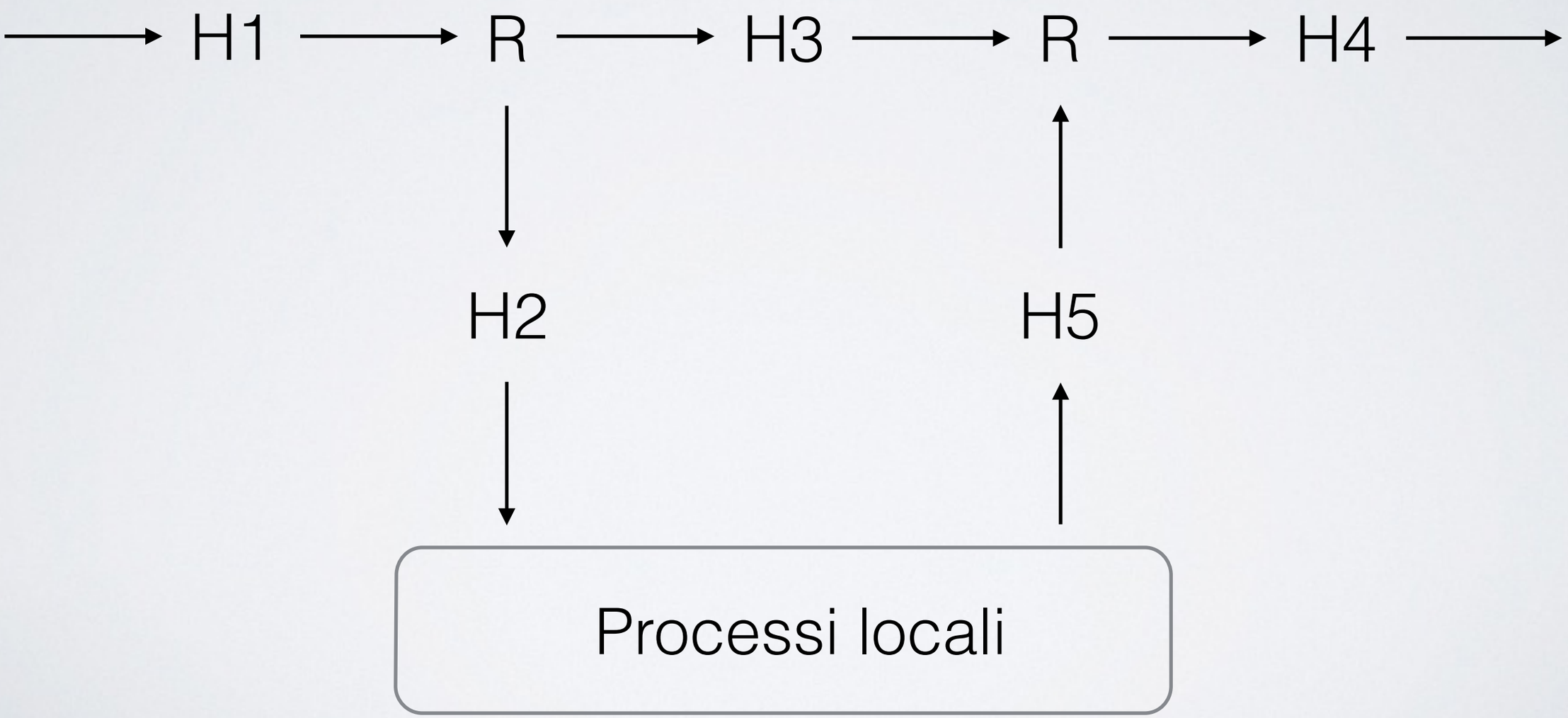
- La Ford modello T è un'auto prodotta dal 1908 al 1928
- A sinistra del piantone del volante c'è una levetta per la regolazione dell'anticipo, da usare al variare della pressione atmosferica o dell'altitudine ma anche al variare dei giri del motore
- Nei motori moderni l'anticipo c'è ancora, completamente automatizzato e nascosto all'utente

NETFILTER

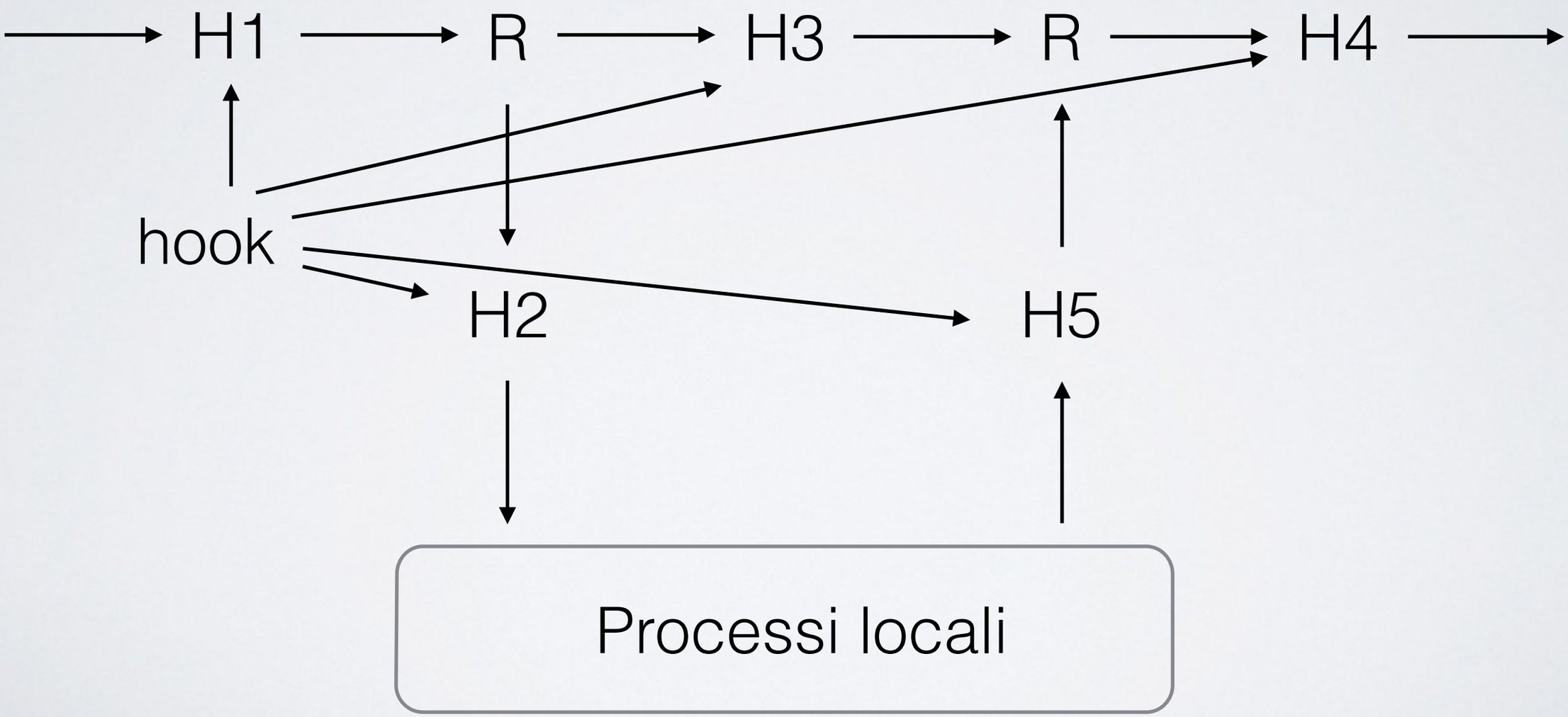
- netfilter è un framework per la manipolazione dei pacchetti, esterno alla normale interfaccia socket Berkeley

- i pacchetti attraversano dei punti (hook) definiti da netfilter in cui posso specificare azioni da eseguire sul pacchetto stesso

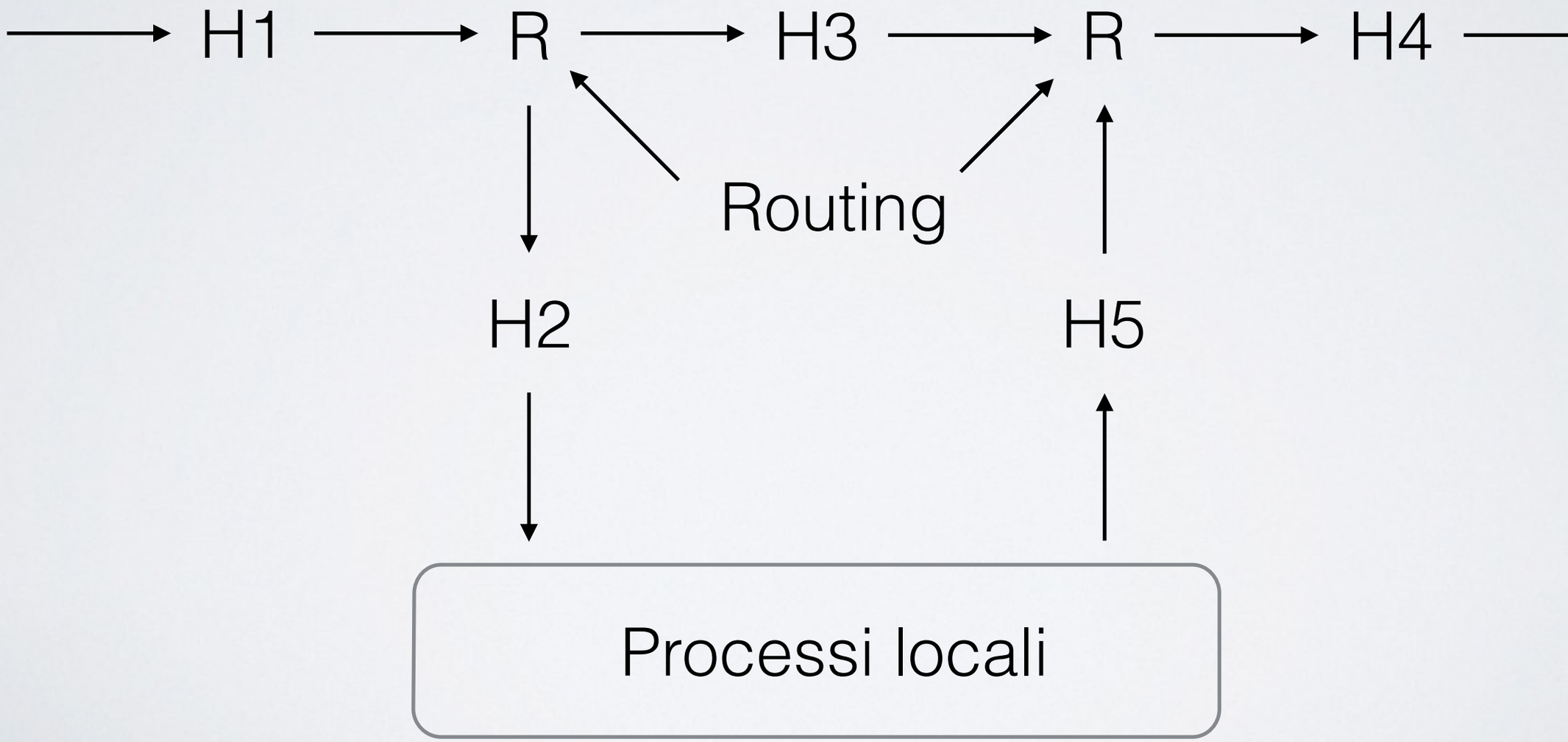
NETFILTER



NETFILTER

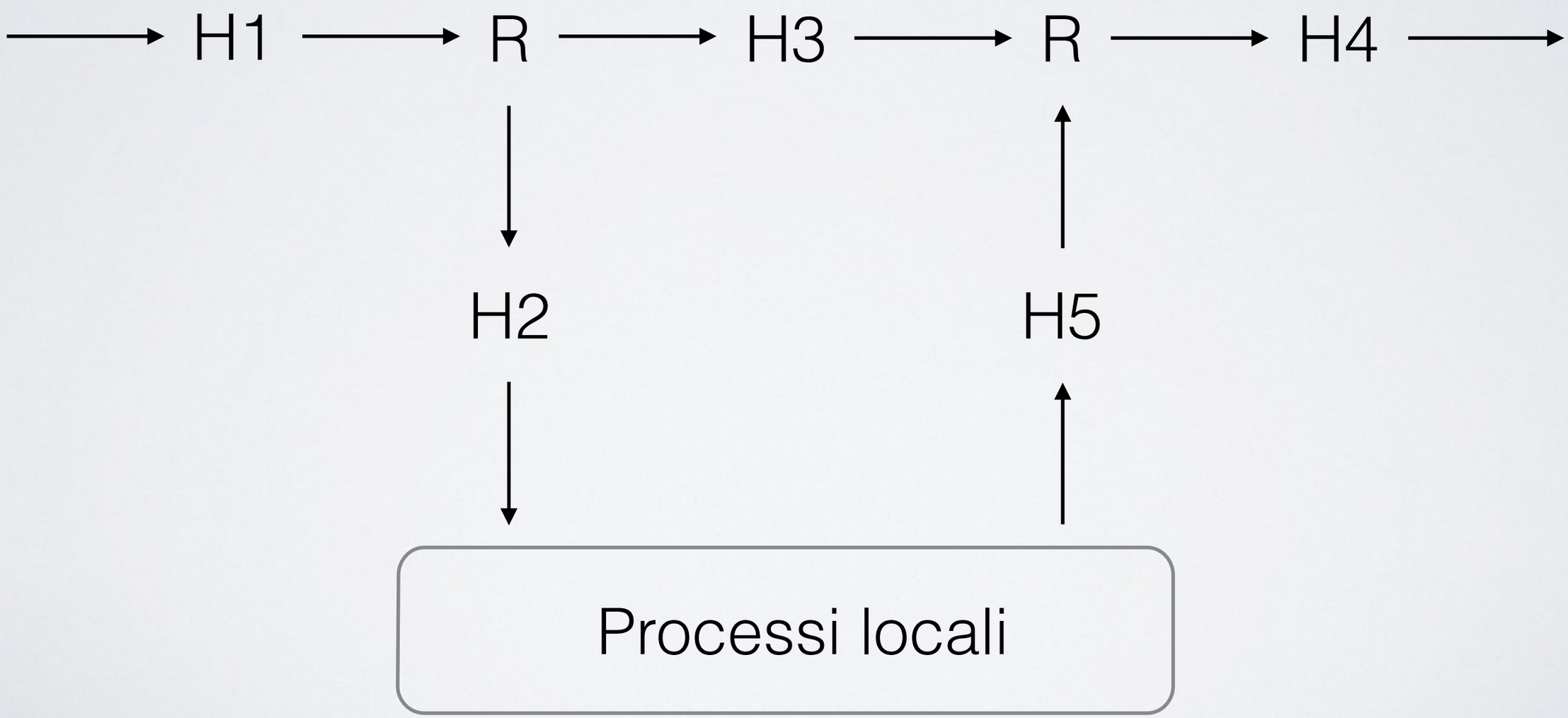


NETFILTER



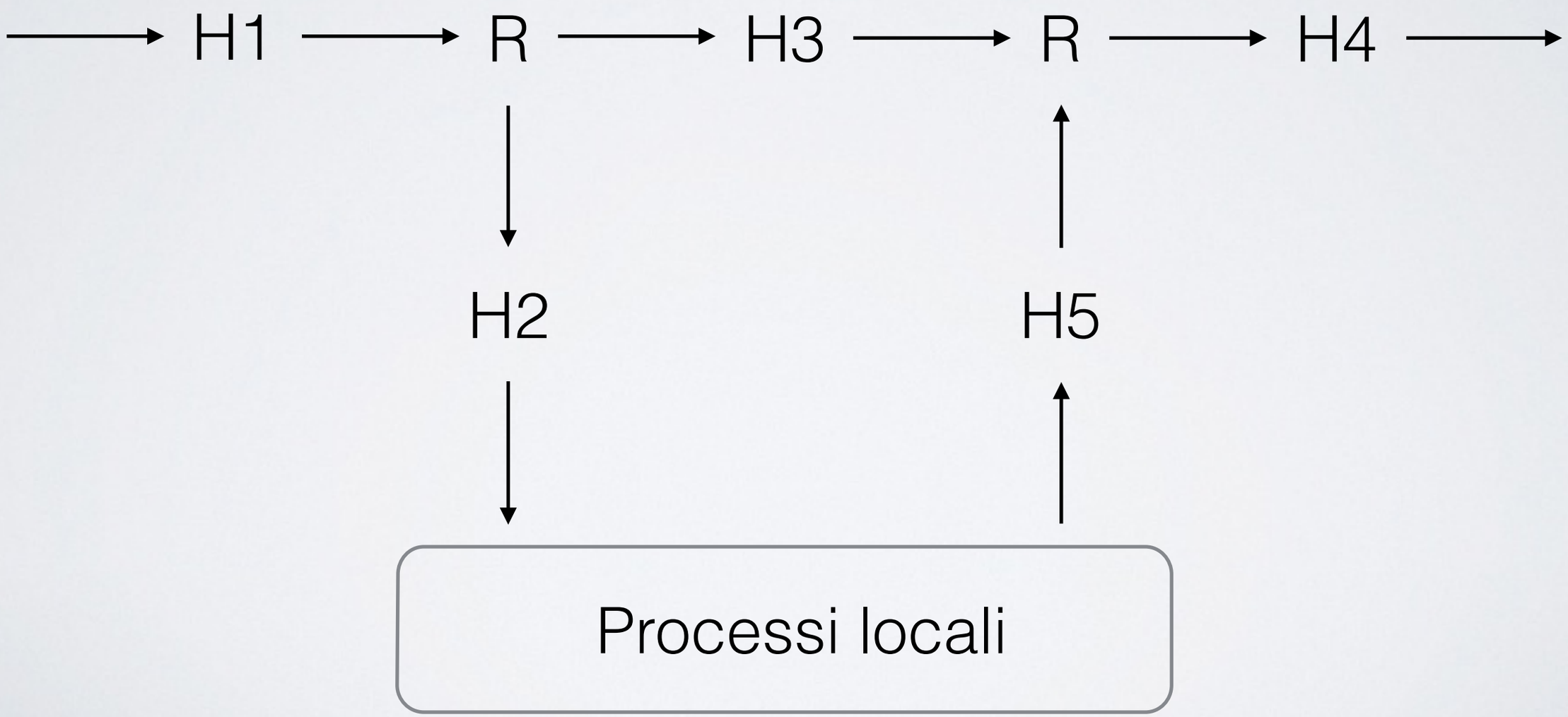
NETFILTER

H1: pre routing



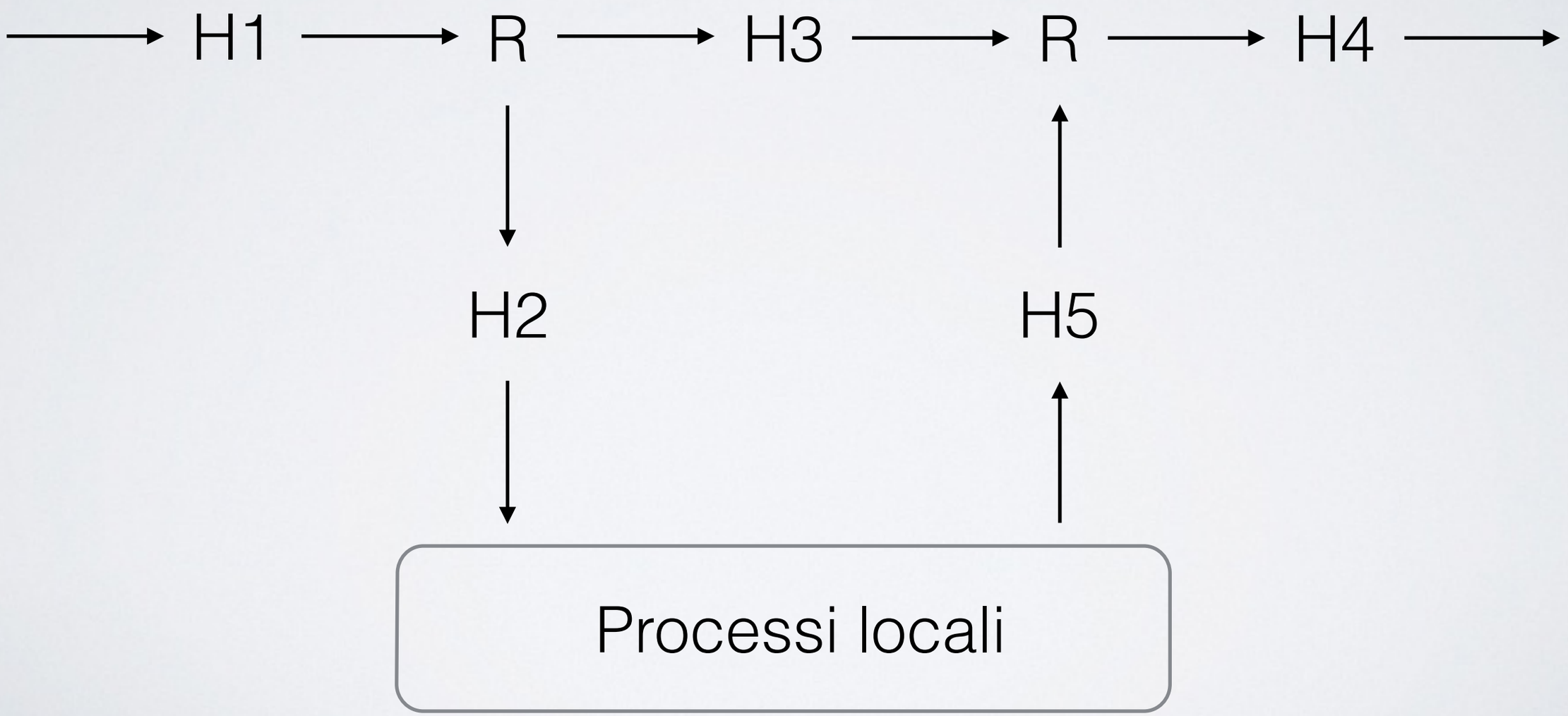
NETFILTER

H2: local IN



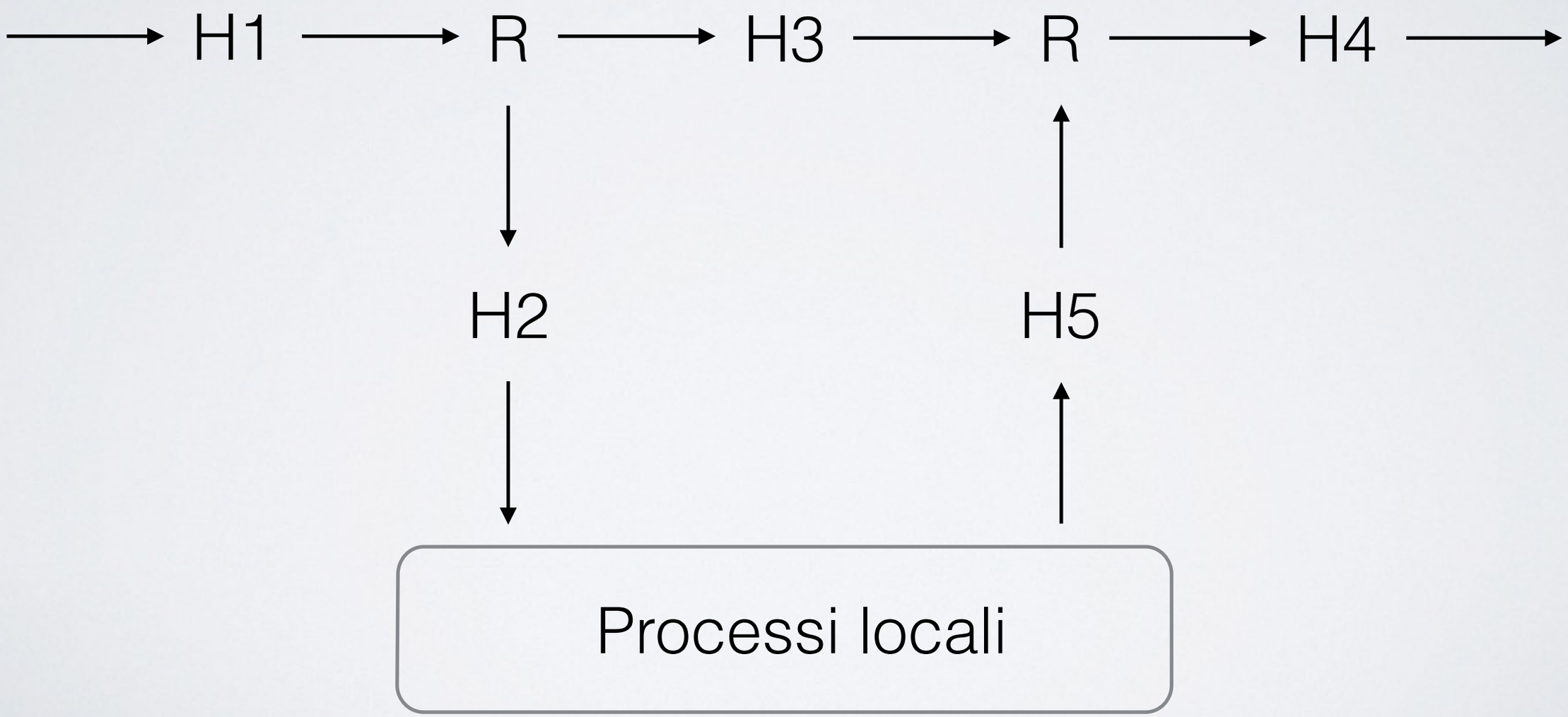
NETFILTER

H3: forward



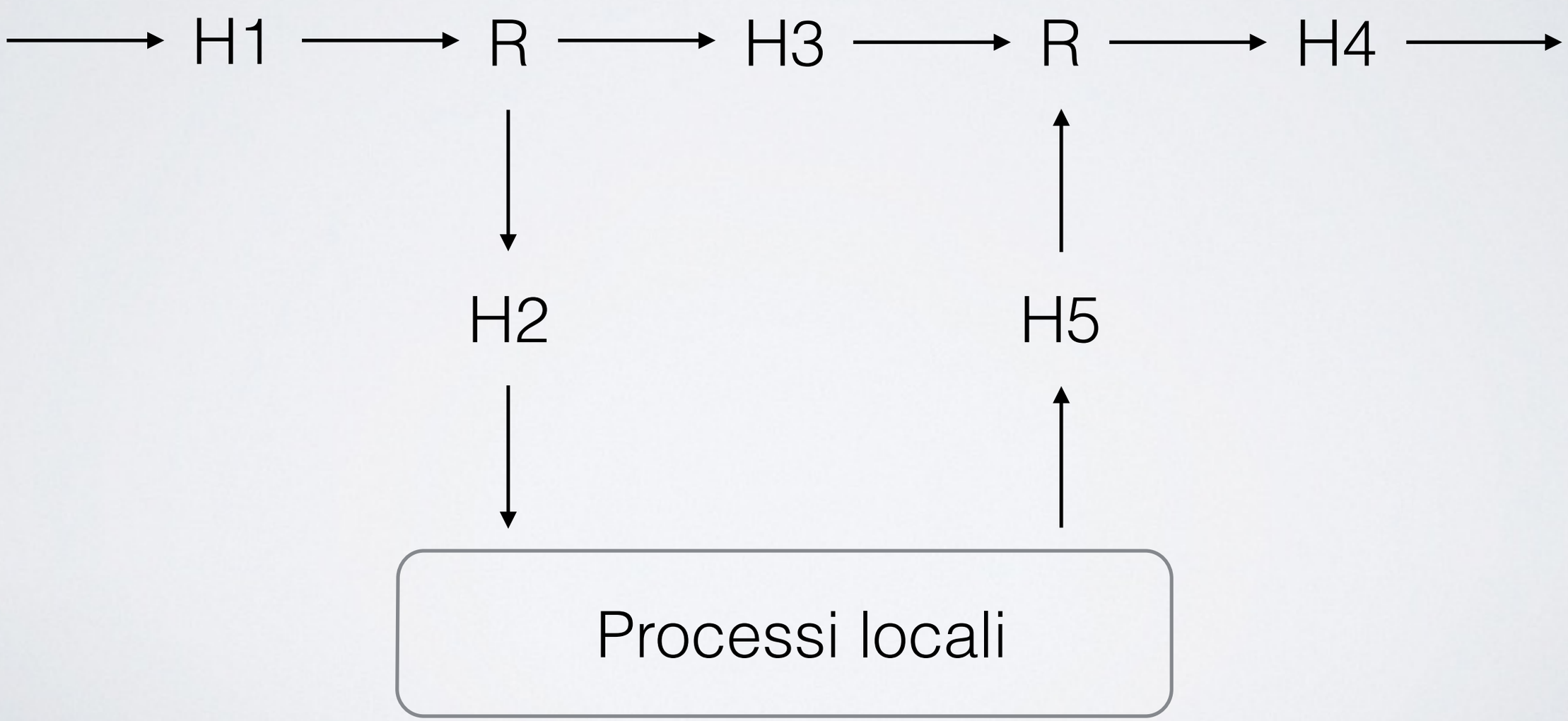
NETFILTER

H4: post routing

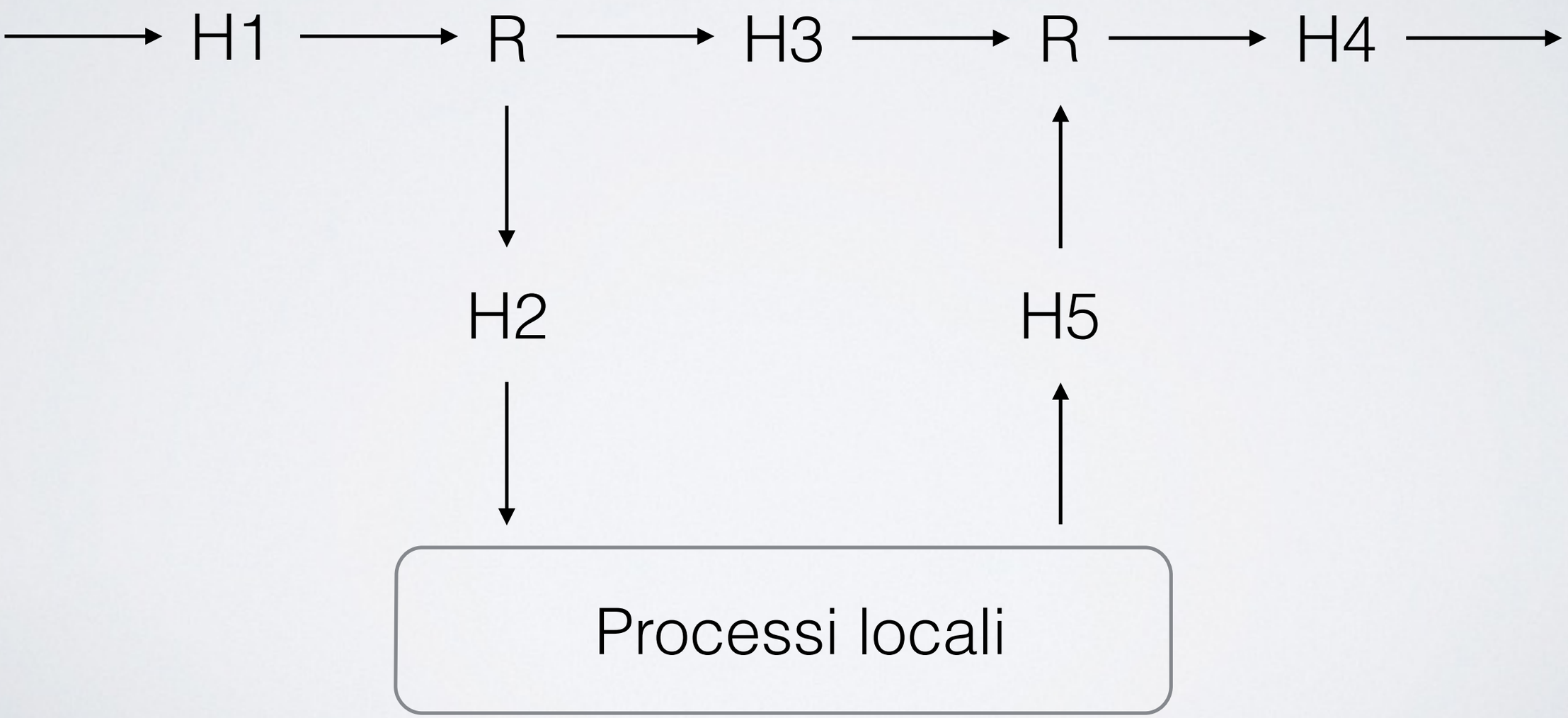


NETFILTER

H5: local out



NETFILTER



NETFILTER: AZIONI

NETFILTER: AZIONI

NF_ACCEPT: continua la traversata normalmente

NETFILTER: AZIONI

NF_ACCEPT: continua la traversata normalmente

NF_DROP: scarta il pacchetto; non continuare la traversata

NETFILTER: AZIONI

NF_ACCEPT: continua la traversata normalmente

NF_DROP: scarta il pacchetto; non continuare la traversata

NF_STOLEN: ho prelevato il pacchetto; non continuare

NETFILTER: AZIONI

NF_ACCEPT: continua la traversata normalmente

NF_DROP: scarta il pacchetto; non continuare la traversata

NF_STOLEN: ho prelevato il pacchetto; non continuare

NF_QUEUE: accoda il pacchetto (di solito userspace)

NETFILTER: AZIONI

NF_ACCEPT: continua la traversata normalmente

NF_DROP: scarta il pacchetto; non continuare la traversata

NF_STOLEN: ho prelevato il pacchetto; non continuare

NF_QUEUE: accoda il pacchetto (di solito userspace)

NF_REPEAT: chiama di nuovo questo hook.

IPTABLES

- è l'interfaccia utente per l'impostazione di filtri eseguiti da netfilter a livello di Kernel (disponibile in tutte le distribuzioni di GNU/Linux)
- crea un array di regole in memoria (da cui il nome) per dirigere i pacchetti provenienti dai vari hook
- attualmente (aprile 2014) la versione disponibile e' la 1.4.21 da usare su kernel >= 2.4.x
- è in grado di effettuare filtering su protocolli IPv4, IPv6, Decnet, etc.

IPTABLES: TIPOLOGIE DI FILTRI

- Controlla e verifica 5 tipi diversi di flussi attraverso la definizione di altrettante tabelle o chains: **Input, Output, Forward, Prerouting, Postrouting**
- Oltre alle tabelle citate se ne possono creare altre personalizzate per scopi specifici
- È in grado di effettuare i LOG

IPTABLES: FUNZIONI DELLE CODE

Filter	FORWARD	Filters packets to servers accessible by another NIC on the firewall.
	INPUT	Filters packets destined to the firewall.
	OUTPUT	Filters packets originating from the firewall

IPTABLES: FUNZIONI DELLE CODE

Nat	PREROUTING	Address translation occurs before routing. Facilitates the transformation of the destination IP address to be compatible with the firewall's routing table. Used with NAT of the destination IP address, also known as destination NAT or DNAT.
	POSTROUTING	Address translation occurs after routing. This implies that there was no need to modify the destination IP address of the packet as in pre-routing. Used with NAT of the source IP address using either one-to-one or many-to-one NAT. This is known as source NAT, or SNAT.
	OUTPUT	Network address translation for packets generated by the firewall. (Rarely used in SOHO environments)

IPTABLES: FUNZIONI DELLE CODE

Mangle	FORWARD	Modification of the TCP packet quality of service bits before routing occurs. (Rarely used in SOHO environments)
	INPUT	
	OUTPUT	
	PREROUTING	
	POSTROUTING	

IPTABLES: TIPOLOGIA DEI FILTRI

All'interno di ciascuna tabella effettua il controllo su:

- Input e Output Interface
- Source MAC Address
- Source e destination IP Address
- Invalid Packets (CRC error, frammenti, etc)
- Protocol (IP, TCP, UDP, ICMP, etc.)
- Source e destination port (TCP e UDP)
- Flag TCP (SYN, FIN, ACK, RST, URG, PSH, ALL, NONE)
- Rate limit
- Etc.

IPTABLES: POLITICHE APPLICABILI

Per ogni pacchetto analizzato iptables è in grado di applicare le seguenti politiche:

ACCEPT (accetta il pacchetto)

DROP e REJECT (scarta il pacchetto)

QUEUE (passa il pacchetto allo userspace)

RETURN (esce dalla access list della attuale tabella e passa il controllo alla successiva tabella)

La sintassi è di tipo command line per la costruzione di ACL sequenziali (per ciascun pacchetto l'esecuzione termina al primo match).

DUE ESEMPI APPLICATIVI

- Accesso SSH su richiesta

- Firewall ACME SpA

APRIRE UN ACCESSO SSH SU RICHIESTA

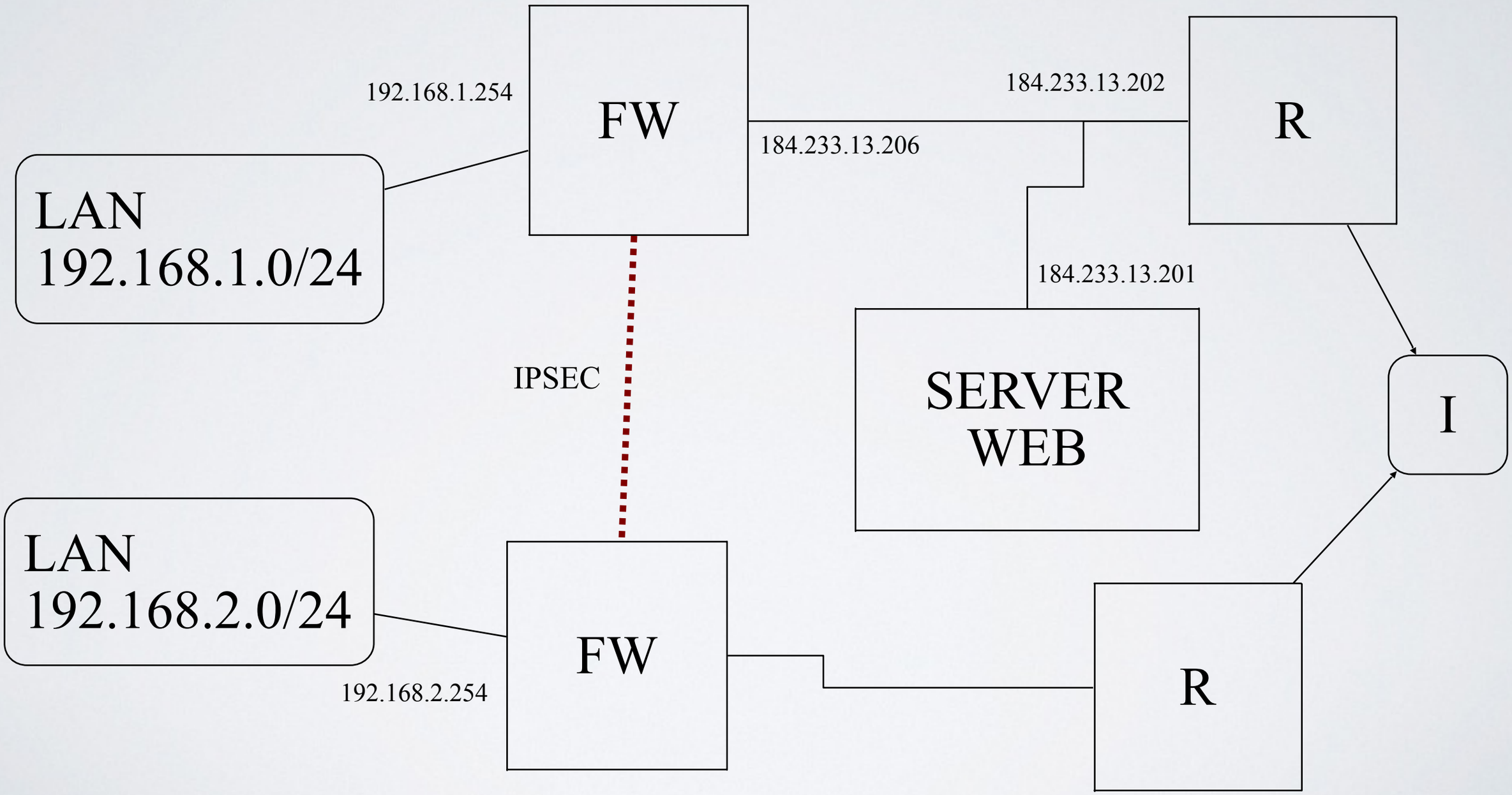
- Si richiede di poter effettuare login SSH sul server iptables (porta 22 TCP) solo dopo una procedura di autorizzazione

- Può essere utile per diminuire l'efficacia degli attacchi a forza bruta quando è necessario consentire l'accesso da indirizzi ip variabili

```
#
# definisco la politica della catena di INPUT
#
iptables -P INPUT DROP
#
# mi assicuro che eventuali connessioni aperte non siano
bloccate
#
iptables -A INPUT -m conntrack --ctstate
ESTABLISHED,RELATED -j ACCEPT
#
# controllo l'accesso alla porta 22
#
iptables -A INPUT -m state --state NEW -m tcp -p tcp --
dport 22 -m recent --rcheck --name SSH -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --
dport 5566 -m recent --name SSH --remove -j DROP
iptables -A INPUT -m state --state NEW -m tcp -p tcp --
dport 5567 -m recent --name SSH --set -j DROP
iptables -A INPUT -m state --state NEW -m tcp -p tcp --
dport 5568 -m recent --name SSH --remove -j DROP
```

FIREWALL ACME SPA (ESEMPIO SOHO)

ACME S.P.A.


192.168.1.254
FW
184.233.13.202
R
184.233.13.206
LAN
192.168.1.0/24
184.233.13.201
IPSEC
SERVER
WEB
I
LAN
192.168.2.0/24
FW
R
192.168.2.254

ACME S.P.A.

```
#!/bin/bash
#
service iptables stop
#
#
# Variabili generali
#
CLIENT_GOOD=$(cat /etc/sysconfig/fw_tabelle/fw_good_client)
CLIENT_STD=$(cat /etc/sysconfig/fw_tabelle/fw_std_client)
CLIENT_MAIL=$(cat /etc/sysconfig/fw_tabelle/fw_mail_client)
I_ETH=eth1
O_ETH=eth0

NS1="194.243.23.201"
NS2="151.99.125.2"
NS3="151.99.125.3"

LAN="192.168.1.0/24"
REMOTELAN="192.168.2.0/24"

#Regole generali delle 3 catene per la tabella "filter"
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

#Regole per interfaccia Loopback:
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

ACME S.P.A. (2)

```
#
# Masquerade
#
iptables -t nat -A POSTROUTING -s 192.168.1.0/255.255.255.0 -o $O_ETH -j MASQUERADE

#
# Abilito il port forwarding per Gabriele
#
iptables -A FORWARD -i $O_ETH -o $I_ETH -p tcp --dport 4662 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A PREROUTING -t nat -p tcp -d 184.233.13.206 --dport 4662 -j DNAT --to
192.168.1.3:4662
iptables -A FORWARD -i $O_ETH -o $I_ETH -p udp --dport 4672 -j ACCEPT
iptables -A PREROUTING -t nat -p udp -d 184.233.13.206 --dport 4672 -j DNAT --to
192.168.1.3:4672
iptables -A FORWARD -i $O_ETH -o $I_ETH -p tcp --dport 4771 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A PREROUTING -t nat -p tcp -d 184.233.13.206 --dport 4771 -j DNAT --to
192.168.1.3:4771
#
# Abilito il port forwarding per poter montare su webserver almeno un volume samba
di mexal
#
iptables -A FORWARD -i $O_ETH -o $I_ETH -s 184.233.13.201 -p tcp --dport 139 -m
state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A PREROUTING -t nat -p tcp -d 184.233.13.206 --dport 139 -j DNAT --to
192.168.1.1:139
```

ACME S.P.A. (3)

```
#-------------------------------------------------------------------
# SEZIONE INPUT
#-------------------------------------------------------------------
#
# allow IPsec
#
iptables -I INPUT  -p udp --sport 500 --dport 500 -j ACCEPT
iptables -I INPUT  -p 50 -j ACCEPT
iptables -I INPUT  -p 51 -j ACCEPT
#
# Devo aprire un po' di porte:
#       22              SSH (solo da www.acmespa.com)
#       53 (udp)        DNS SERVER
#
iptables -A INPUT -p tcp -s 184.233.13.201 --dport 22 -j ACCEPT
iptables -A INPUT -p UDP -s $NS1 -j ACCEPT
iptables -A INPUT -p UDP -s $NS2 -j ACCEPT
iptables -A INPUT -p UDP -s $NS3 -j ACCEPT
#
# Devo fare mysql con www.acmespa.com
# e posta con telemat
#
iptables -A INPUT -i $O_ETH -p tcp -s 184.233.13.201 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -i $O_ETH -p tcp -s 150.217.8.42   -m state --state ESTABLISHED -j ACCEPT
#
# Verso le macchine interne posso fare tutte le connessioni che voglio
#
iptables -A INPUT -i $I_ETH -p tcp -s 192.168.1.0/24 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -i $I_ETH -p udp -s 192.168.1.0/24 -j ACCEPT
#
# Accetto le connessioni dhcp
#
iptables -A INPUT -i $I_ETH -p udp --dport 67 -j ACCEPT
iptables -A INPUT -i $I_ETH -p tcp --dport 67 -j ACCEPT
#
```

ACME S.P.A. (4)

```
#-----------------------------------------------------------------------
# SEZIONE FORWARD
#-----------------------------------------------------------------------
#
# Creo una catena per l'accounting di tutta la LAN
#
iptables -N 192.168.1.254
iptables -A FORWARD -i $O_ETH -d 192.168.1.0/24  -j 192.168.1.254
iptables -A FORWARD -o $O_ETH -s 192.168.1.0/24 -j 192.168.1.254
iptables -A 192.168.1.254 -i $O_ETH -d 192.168.1.0/24
iptables -A 192.168.1.254 -o $O_ETH -s 192.168.1.0/24
#
# creo le catene di forward per l'accounting di ogni IP address
#
NET="192.168.1"
START=1
STOP=253
COUNT=$START;
while [ $COUNT -le $STOP ]; do
        iptables -N $NET.$COUNT
        iptables -A FORWARD -i $O_ETH -d $NET.$COUNT -j $NET.$COUNT
        iptables -A FORWARD -o $O_ETH -s $NET.$COUNT -j $NET.$COUNT
        iptables -A $NET.$COUNT -i $O_ETH -d $NET.$COUNT
        iptables -A $NET.$COUNT -o $O_ETH -s $NET.$COUNT
        let COUNT=$COUNT+1;
done;
```

ACME S.P.A. (6)

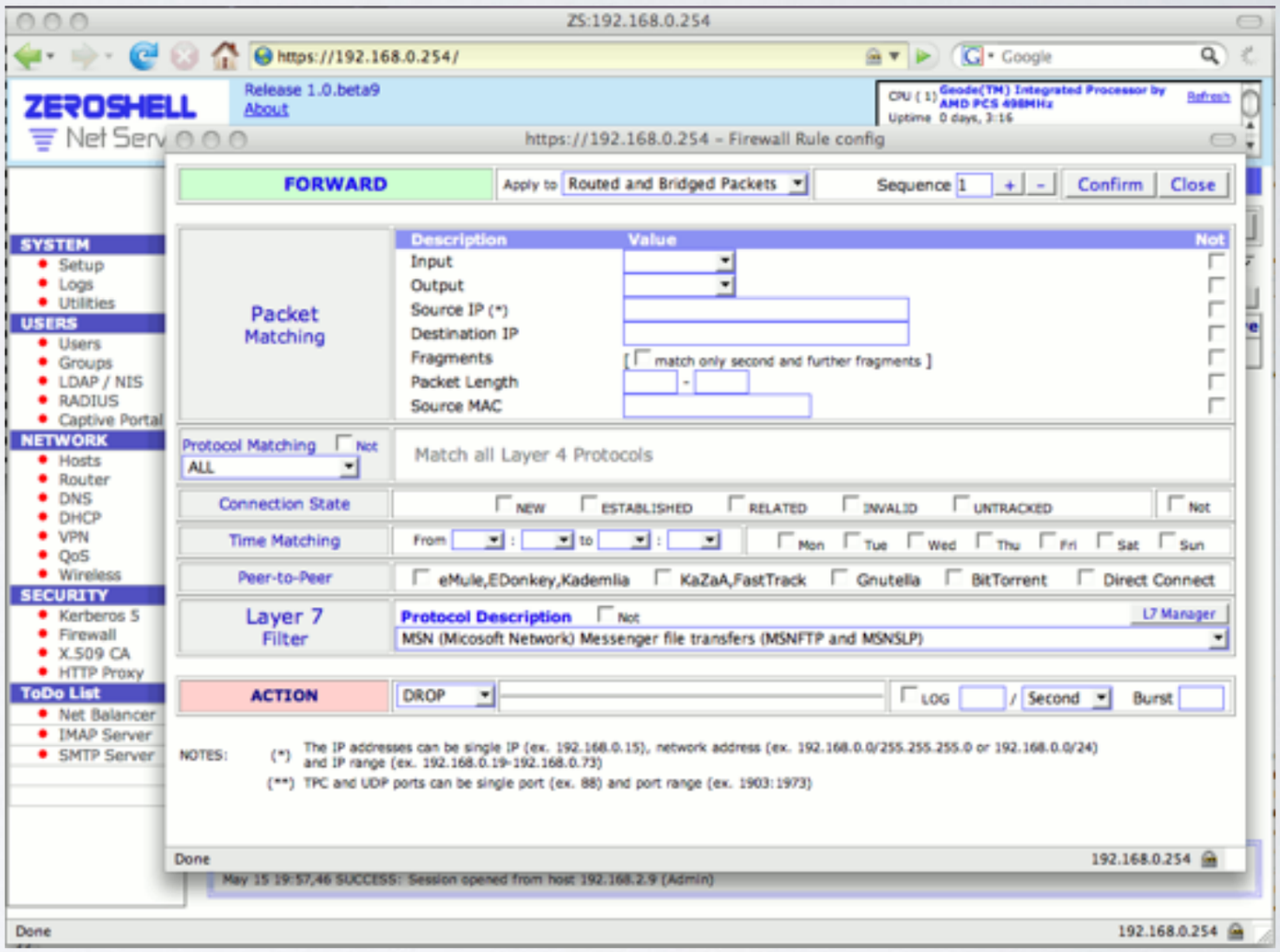
```
#
# I client possono richiedere connessioni all'esterno, ma non possono
# accettarne di nuove
#
for client in ${CLIENT_GOOD}; do
 iptables -A FORWARD -p TCP -i $I_ETH -o $O_ETH -s ${client} -j ACCEPT
 iptables -A FORWARD -p TCP -i $O_ETH -o $I_ETH -d ${client} -m state --state
ESTABLISHED -j ACCEPT
 iptables -A FORWARD -p UDP -i $I_ETH -o $O_ETH -s ${client} -j ACCEPT
 iptables -A FORWARD -p UDP -i $O_ETH -o $I_ETH -d ${client} -m udp --dport
1024:65535 -j ACCEPT
 iptables -A FORWARD -p udp -i $I_ETH -o $O_ETH -s ${client} -d $NS1 -j ACCEPT
 iptables -A FORWARD -p UDP -i $O_ETH -o $I_ETH -d ${client} -m udp -s $NS1 -j
ACCEPT
 iptables -A FORWARD -p udp -i $I_ETH -o $O_ETH -s ${client} -d $NS2 -j ACCEPT
 iptables -A FORWARD -p UDP -i $O_ETH -o $I_ETH -d ${client} -m udp -s $NS2 -j
ACCEPT
done
```

ACME S.P.A. (6)

```
#
# Client BAD: Abilitati solo sulle porte 25, 80, 110, 443 e relative risposte
# Traffico UDP Bloccato
#
for client in ${CLIENT_STD}; do
 iptables -A FORWARD -p TCP -i $I_ETH -o $O_ETH -s ${client} -m tcp --dport 25 -j ACCEPT
 iptables -A FORWARD -p TCP -i $I_ETH -o $O_ETH -s ${client} -m tcp --dport 80 -j ACCEPT
 iptables -A FORWARD -p TCP -i $I_ETH -o $O_ETH -s ${client} -m tcp --dport 110 -j ACCEPT
 iptables -A FORWARD -p TCP -i $I_ETH -o $O_ETH -s ${client} -m tcp --dport 443 -j ACCEPT
 iptables -A FORWARD -p TCP -i $O_ETH -o $I_ETH -d ${client} -m state --state ESTABLISHED -j ACCEPT
 iptables -A FORWARD -p udp -i $I_ETH -o $O_ETH -s ${client} -d $NS1 -j ACCEPT
 iptables -A FORWARD -p UDP -i $O_ETH -o $I_ETH -d ${client} -m udp -s $NS1 -j ACCEPT
 iptables -A FORWARD -p udp -i $I_ETH -o $O_ETH -s ${client} -d $NS2 -j ACCEPT
 iptables -A FORWARD -p UDP -i $O_ETH -o $I_ETH -d ${client} -m udp -s $NS2 -j ACCEPT
done
##
# Client MAIL: Abilitati solo sulle porte 25, 110, (posta) e relative risposte
# Traffico UDP Bloccato
#
for client in ${CLIENT_MAIL}; do
 iptables -A FORWARD -p TCP -i $I_ETH -o $O_ETH -s ${client} -m tcp --dport 25 -j ACCEPT
 iptables -A FORWARD -p TCP -i $I_ETH -o $O_ETH -s ${client} -m tcp --dport 110 -j ACCEPT
 iptables -A FORWARD -p TCP -i $O_ETH -o $I_ETH -d ${client} -m state --state ESTABLISHED -j ACCEPT
 iptables -A FORWARD -p udp -i $I_ETH -o $O_ETH -s ${client} -d $NS1 -j ACCEPT
 iptables -A FORWARD -p UDP -i $O_ETH -o $I_ETH -d ${client} -m udp -s $NS1 -j ACCEPT
 iptables -A FORWARD -p udp -i $I_ETH -o $O_ETH -s ${client} -d $NS2 -j ACCEPT
 iptables -A FORWARD -p UDP -i $O_ETH -o $I_ETH -d ${client} -m udp -s $NS2 -j ACCEPT
done
#
```

FIREWALL PER TUTTI

- ZeroShell
- pfSense
- IPcop
- Sonicwall (Dell)
- Cisco
- …e tanti altri



COME SCEGLIERE UN FIREWALL

- Tipologia: hardware/software
- Banda
- Connettività
- Prestazioni

FIREWALL HARDWARE DEDICATO

- Installazione semplificata
- Affidabilità
- Espandibilità limitata dal costruttore
- Costo elevato ma certo

FIREWALL SOFTWARE

- Installazione non sempre facilissima
- Supporto non sempre sufficiente
- Espandibilità teoricamente illimitata
- Costo basso ma variabile

INSTALLAZIONE, PROGRAMMAZIONE E MANUTENZIONE

- Decidere una policy
- Scegliere il tipo di firewall da installare
- Impostare le regole per rispettare la policy scelta
- Verificare periodicamente la rispondenza alla policy

5 CONSIGLI PRATICI

- Documentare i cambiamenti di configurazione
- Concedere sempre il minimo dei diritti
- Verificare che qualunque modifica sia coerente con la policy stabilita
- Rimuovere immediatamente le regole inutilizzate dal firewall
- Effettuare una revisione completa delle regole ogni sei mesi

FINE PRIMA PARTE

WIRELESS

ACCESSO SICURO SENZA FILI

- open: nessuna sicurezza
- WEP: vulnerabile
- WPA+TKIP
- WPA+TKIP/AES
- WPA+AES
- WPA2+AES

OPEN

- Nessuna gestione
- Il traffico è visibile a tutti i client
- Qualunque tipo di attacco è possibile: DOS, MITM, sinffing, ecc.
- **NESSUNA SICUREZZA**

WEP

- WEP: Wired Equivalent Privacy
- Algoritmo RC4 con due chiavi, 40bit e 104bit, più 24bit di vettore di inizializzazione
- Definito nel 1999, nel 2003 è stato violato per una implementazione debole di RC4
- Attualmente con aircrack si ottiene l'accesso in 60 secondi
- **SICUREZZA DEBOLISSIMA**

WPA+TKIP

- WPA: Wi-Fi Protected Access
- Compatibile con vecchie schede WEP (aggiornamento firmware)
- Algoritmo RC4 con chiave a 128bit, più 48bit di vettore di inizializzazione
- Il TKIP (Temporal Key Integrity Protocol) protegge da attacchi tipo WEP cambia la chiave in uso nel tempo
- Nel 2008/2009 si è dimostrato possibile violare WPA+TKIP
- **SICUREZZA DEBOLE**

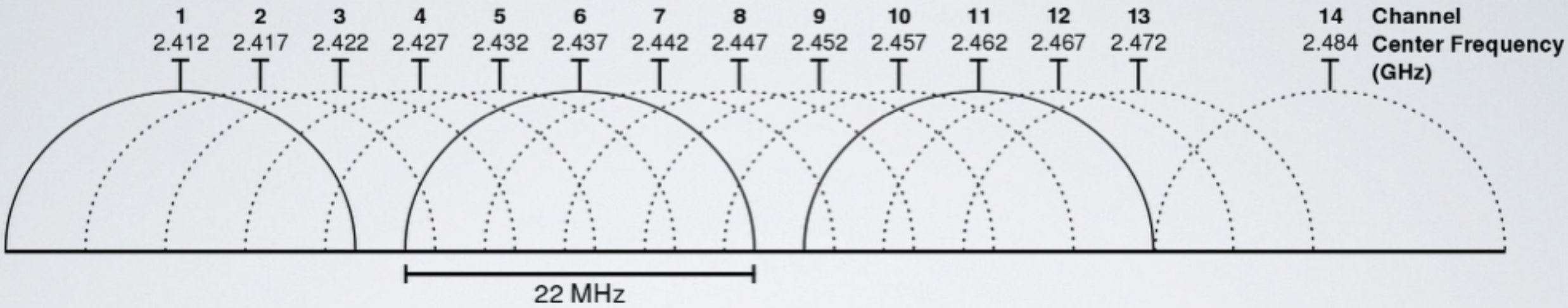
WPA2+AES

- WPA2: incompatibile con vecchie schede WEP
- AES: Advanced Encryption Standard è attualmente molto sicuro
- Attacco forza bruta su chiave a 64 bit ha impiegato quasi 5 anni con migliaia di CPU
- **SICUREZZA ELEVATA**

WPA2+AES+WPS

- WPS: Wi-Fi Protected Setup (mercato SOHO)
- Metodo semplificato per inserire la chiave
- PIN 8 cifre (7+1) con messaggio di errore
- 2 ore per provare tutte le combinazioni
- Alcuni apparati hanno WPS con PIN abilitato per default
- **SICUREZZA DEBOLISSIMA**

PRESTAZIONI E LIMITI



- 802.11b: fino a 11Mb/s, 2.4GHz, 22MHz per canale

- 802.11g: fino a 54Mb/s, stesse frequenze di 802.11b

PRESTAZIONI E LIMITI

- 802.11n: fino a 300Mb/s, 2.4GHz e 5.4GHz, 24 e 40MHz per canale

- 802.11ac: fino a 866.7Mb/s, 5.4GHz, da 20 a 160MHz per canale, MIMO fino a 8

5GHZ VS 2GHZ

- Nella banda dei 2.4GHz ci sono sovrapposizioni: i canali da usare sono solo 1, 6, 11 e 14
- Nella banda dei 5GHz non ci sono sovrapposizioni. In Europa sono disponibili i canali 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140

CASO DI STUDIO: ITIS FEDI

- AS2007/2008: introduzione registro elettronico
- Necessità della rete wireless in ogni aula
- Gestione centralizzata (esami di stato)
- Sicurezza (rete segreteria fisicamente connessa)

CASO DI STUDIO: ITIS FEDI

CASO DI STUDIO: ITIS FEDI

CASO DI STUDIO: ITIS FEDI

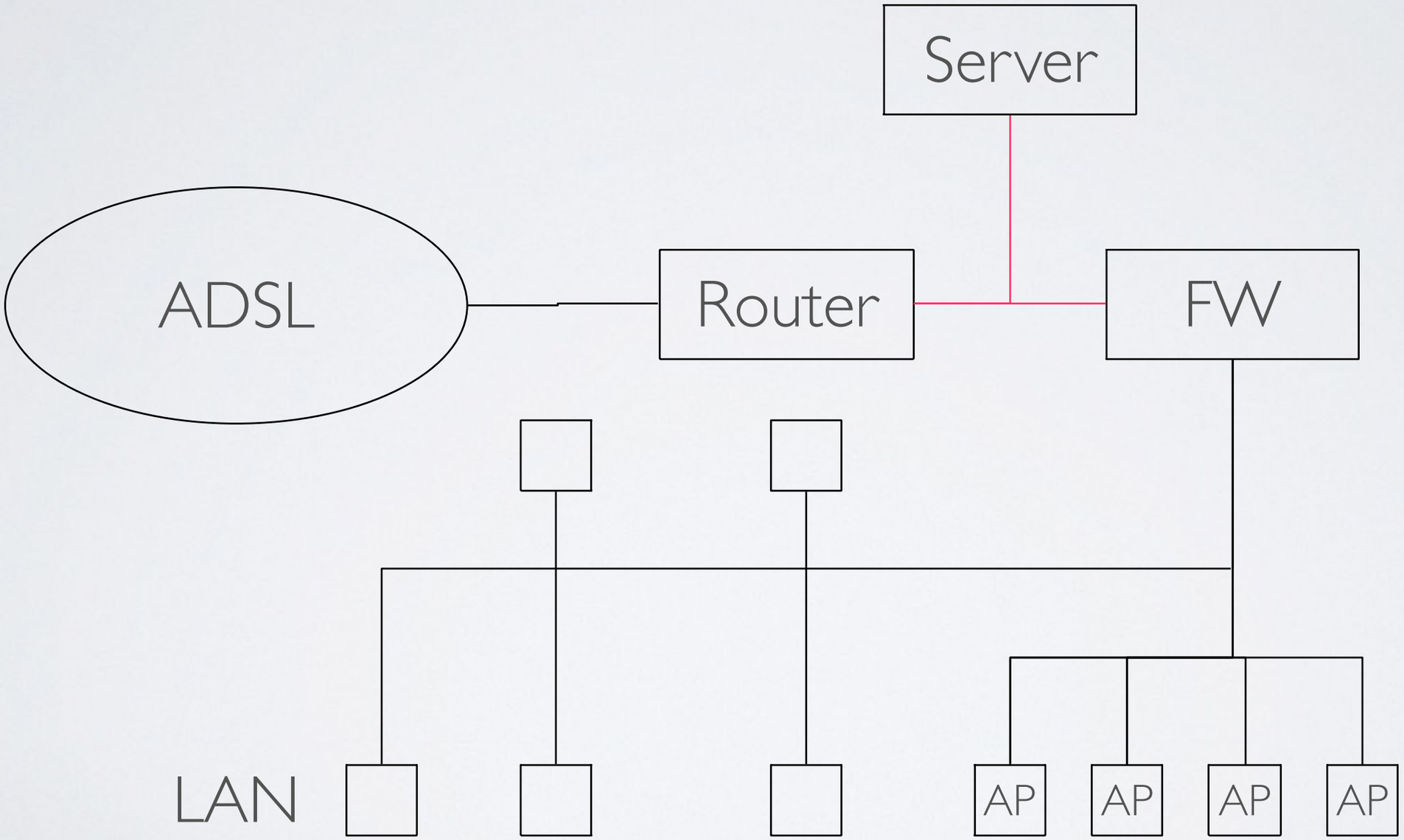
CASO DI STUDIO: ITIS FEDI

- Sostituzione del firewall Linux a gestione manuale con Sonicwall pro 2040

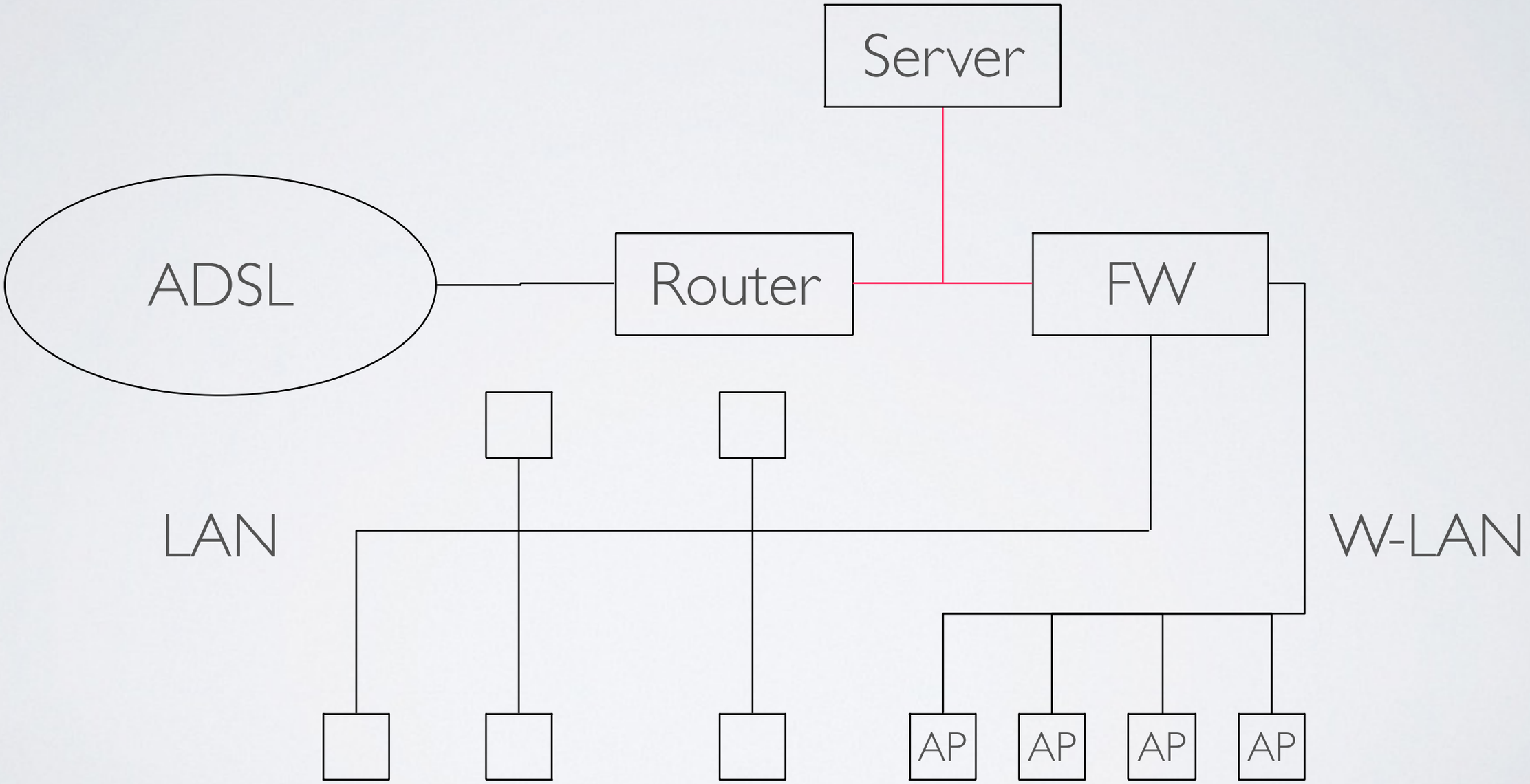
- Sostituzione dei vari access point "casalinghi" e installazione dei nuovi punti di accesso con 16 Sonicpoint G

- Installazione di 3 switch PoE HP ProCurve (managed) per eliminare la necessità degli alimentatori a muro (e gli impianti elettrici corrispondenti) e per le VLAN

CASO DI STUDIO: ITIS FEDI



CASO DI STUDIO: ITIS FEDI



CASO DI STUDIO: ITIS FEDI PRIMA

- shared key praticamente non sostituibile
- gestione complessa
- roaming non funzionante
- nessuna divisione fra client LAN e client wireless

CASO DI STUDIO: ITIS FEDI DOPO

- policy di accesso completamente gestita
- gestione da unico pannello di controllo
- roaming funzionante
- divisione fisica fra client LAN e client wireless

SMATERIALIZZAZIONE

CONSERVAZIONE SOSTITUTIVA

Eliminare il cartaceo è possibile

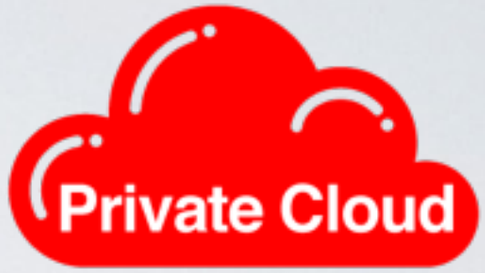
CONSERVAZIONE SOSTITUTIVA

- Spazio e conservazione
- Ricerca e organizzazione
- Il server in azienda non è sempre la soluzione migliore

ARCHIVIAZIONE SOSTITUTIVA

Sistemi di archiviazione in locale

VS



Publically Shared
Virtualised Resources

Privately Shared
Virtualised Resources

Supports multiple
customers

Cluster of dedicated
customers

Supports connectivity
over the internet

Connectivity over
internet, fibre and private network

Suited for less
confidential information

Suited for secured
confidential information
& core systems

ARCHIVIAZIONE SOSTITUTIVA

Sistemi di archiviazione in cloud privati e pubblici

CLOUD
MINACCIA O RISORSA

- Bancomat o contanti?
- Sicurezza
- Riservatezza
- Fruibilità

IT IN AZIENDA

Tanti apparati per gestire ogni aspetto dell'IT

SMATERIALIZZAZIONE DELLE INFRASTRUTTURE

- Occorrono davvero le infrastrutture locali?
- Amazon, Google, Microsoft (ma anche altri!) possono fornire la soluzione

SMATERIALIZZAZIONE DEL COMPUTER

- Serve davvero un PC?
- AWS Workspace: in Europa da maggio 2014, da 37$ a 79$ mensili

IL FUTURO: IOT

- IPV6 e tutto sarà raggiungibile
- Internet in qualunque dispositivo
- Industrial Internet: un futuro da miliardi di dollari
- Le implicazioni sulla sicurezza sono al di là di ogni immaginazione

CONCLUSIONI

GRAZIE PER L'ATTENZIONE!
DOMANDE?

CLAUDIO@BIZZARRI.NET