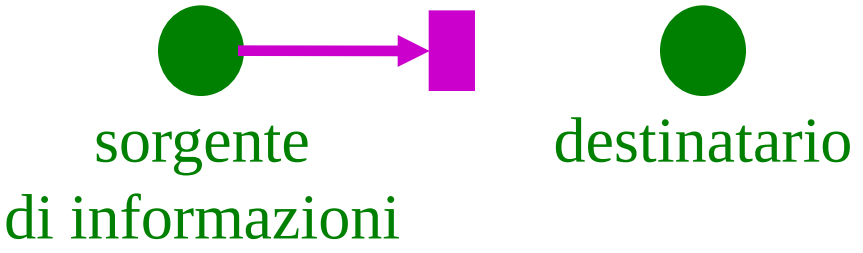
sicurezza delle reti

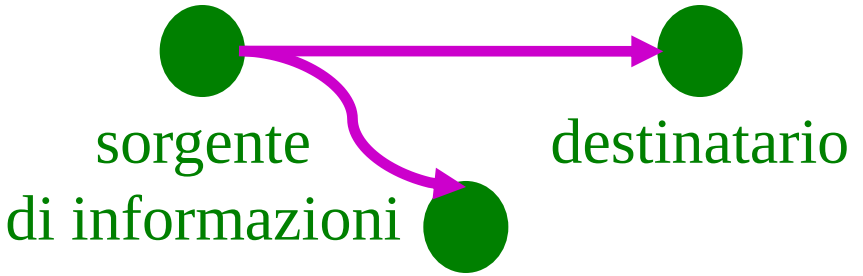
(metodi crittografici esclusi)

classificazione degli attacchi

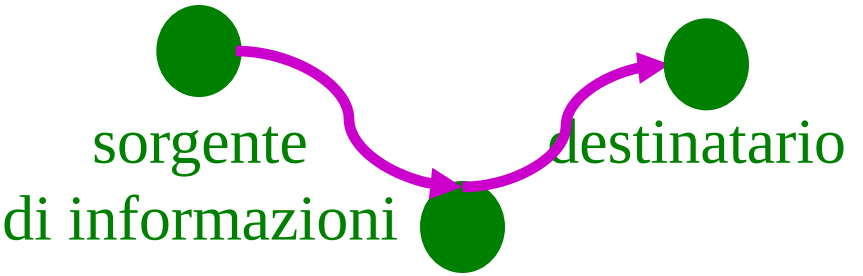
flusso normale



interruzione (DoS)



intercettazione (sniffing)



intercettazione (MiM passivo)

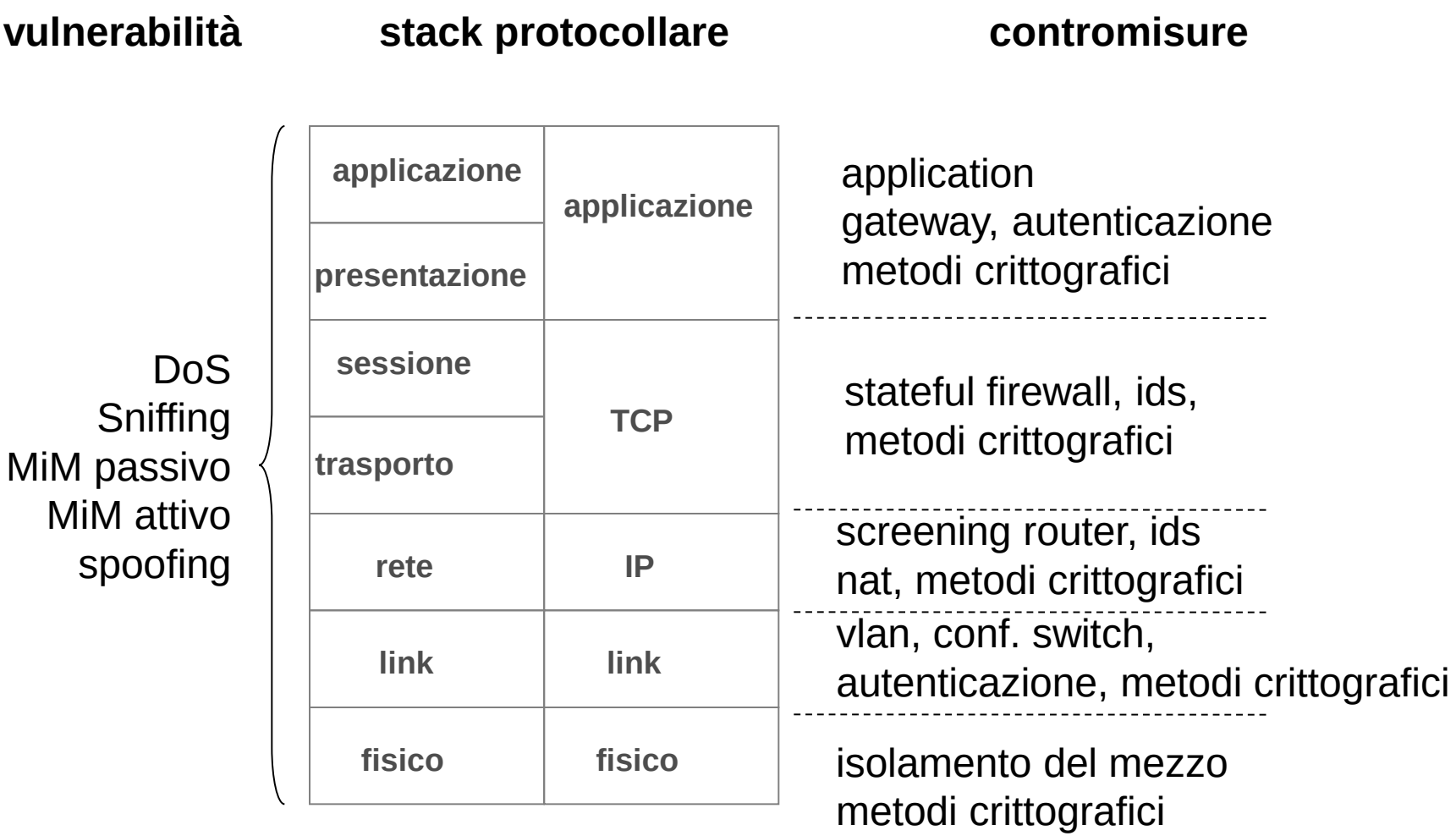
modifica (MiM attivo)

creazione (spoofing)

confinamento nelle reti

- il traffico è (o dovrebbe essere) ammesso solo tra sistemi e/o utenti con caratteristiche di sicurezza analoghe (principio di isolamento)
- esempi di classi di utenti
  - amministrazione
    - integrità e disponibilità: critiche per il business
    - confidenzialità: ciritica per legge
    - insieme di applicazioni ben definito
    - sistemi sotto controllo diretto
  - docenti
    - integrità e disponibilità: critiche per il business
    - confidenzialità: ciritica per certi aspetti particolari
    - richiesta alta flessibilità nelle applicazioni
    - il controllo dei sistemi è delegato ai gruppi di ricerca
  - studenti
    - best effort
    - sistemi non controllabili
  - utenti da internet di ricerca
    - servizi selezionati: web, email, siti di ricerca interni, login alle macchine di ricerca e a utenti da internet (altri)
    - servizi selezionati: web, email, siti di ricerca interni

la sicurezza nelle reti



sicurezza del mezzo trasmissivo

- cavi rame
  - vulnerabilità
    - wiretapping
    - taglio
    - emissione elettromagnetica
  - contromisure
    - protezione fisica
    - wiretapping detection
- fibra
  - vulnerabilità
    - wiretapping
    - taglio
  - contromisure
    - protezione fisica
    - wiretapping detection

sicurezza del mezzo trasmissivo

- wireless
  - vulnerabilità
    - copertura “ad area” non “a presa”
      - impossibile stabilire chi riceve il traffico
    - area di copertura varia con la sensibilità delle stazioni
      - antenne fortemente direzionali possono ricevere hot spot molto lontani
    - facile avere utenti “parassiti”
    - DoS elettrmagnetico
      - non adatto a sistemi la cui disponibilità è critica
    - banda molto limitata
  - contromisure
    - per la confidenzialità e gli utenti parassiti: meccanismi crittografici a livello data link (più o meno efficaci)

livello data link

switch

- vulnerabilità
  - mac spoofing/flooding
    - impatto su arp, spanning tree, e livelli superiori
  - e altri problemi mitigabili: bugs del firmware, errori di configurazione
- contromisure
  - switch sofisticati permettono di rilevare e contrastare attacchi basati su mac spoofing
  - autenticazione
    - mac lock
    - web based
      - al primo accesso funziona solo dhcp e dns
      - lo switch fa da web server e tramite http chiede username e password
    - **802.1X**
  - isolamento
    - **VLAN**
      - vulnerabilità: GVRP è abilitato di default per standard e permette la configurazione automatica di vlan, oramai obsoleto e deletereo.

virtual lan vs. real lan

- le “forze” che guidano il progetto della rete fisica e delle vlan sono diverse
- rete fisica, cioè switch e cablaggio
  - ha come obiettivo la rete economicamente più conveniente che soddisfi i seguenti vincoli
    - piena connettività tra le prese
    - prestazioni richieste
    - vincoli ambientali (es. posizione spazi adibiti agli impianti)
    - vincoli tecnologici (es. lunghezza dei cavi)
    - normative (es. materiali non infiammabili)
    - affidabilità (se richiesta, es. resiste al fault di uno switch)
- vlan, cioè configurazione ideale “desiderata”
  - ha come obiettivo la migliore configurazione che soddisfi…
    - le specifiche funzionali
      - chi deve essere connesso con chi? vedi strutture organizzative che occupano l’edificio (es. dipartimenti, reparti, ecc)
    - le specifiche di sicurezza basate sulle classi di utenti (vedi isolamento)
    - facilità di gestione (es. ciascuna vlan un amministratore)

vlan

- su un singolo switch
  - ciascuna porta è associata ad una vlan
  - uno “switch virtuale“ per ciascuna vlan
- su più switch: 802.1Q
  - tra uno switch e l’altro i pacchetti viaggiano taggati con l’identificatore della vlan (802.1p)
- comportamenti caratteristici
  - confinamento di broadcast e unicast
    - switch di scarsa qualità (non standard) confinavano solo il broadcast (vulnerabile)
  - la comunicazione tra vlan deve avvenire attraverso un router proprio come tra lan distinte
- argomenti correlati
  - vlan asimmetriche, vlan per protocollo, GVRP, multiple spanning tree

livelli rete, trasporto e applicazione

vulnerabilità e minacce

- veicolo per attacchi ai sistemi
- elemento umano
  - email, web, ecc. l'utente permette l'entrata di virus, trojan, ecc.
- molte vulnerabilità già viste all'inizio del corso
  - protocolli in chiaro e non autenticati: necessari metodi crittografici
  - DoS, DDoS

firewalls

- apparecchiature che confinano (filtrano) selettivamente il traffico di rete
- network (layer3+4) vs. application (layer7)
  - network: stateful vs. stateless
- hardware vs. software
- personal fw vs. network fw

- possono avere altre funzionalità
  - nat, virtual private network, autenticazione utenti

Unified Threat Management (UTM)

- evoluzione del concetto di firewall
- unisce molte delle funzionalità
  - firewall
  - network intrusion detection/prevention
  - sicurezza delle email
    - antivirus, anti-spam
  - VPN termination
  - applicative content inspection
  - load balancing
- semplicità di gestione e riduzione dei costi
- vedremo molte delle funzionalità come se fossero apparati separati

soggetti, oggetti e diritti in un fw

- soggetto: un pacchetto/messaggio in ingresso
- oggetto: solo il firewall
- accesso: richiesta al firewall di essere instradato verso la destinazione
- diritti: per ciascun tipo di traffico in ingresso le destinazioni ammesse

- è un modo di vedere il fw molto concreto ma poco utile

il firewall come reference monitor

- un firewall può essere visto come un reference monitor di rete
  - soggetto: l'host sorgente che ha inviato il pacchetto/messaggio
  - oggetto: l'host destinazione che riceverà il pacchetto/messaggio
  - accesso: richiesta all'host destinazione di processare il pacchetto/messaggio inviato dall'host sorgente
    - la semantica vera (cioè l'effetto sull'host destinazione) dell'accesso è data dal protocollo di rete e dal contesto in cui viene usato: il fw non ha bisogno di conoscerla
  - diritti: categorie di traffico ammesso per la coppia di host

packet filter firewall

- basati sulla quadrupla <saddr,sport,daddr,dport>
- in pratica è un router + access control list

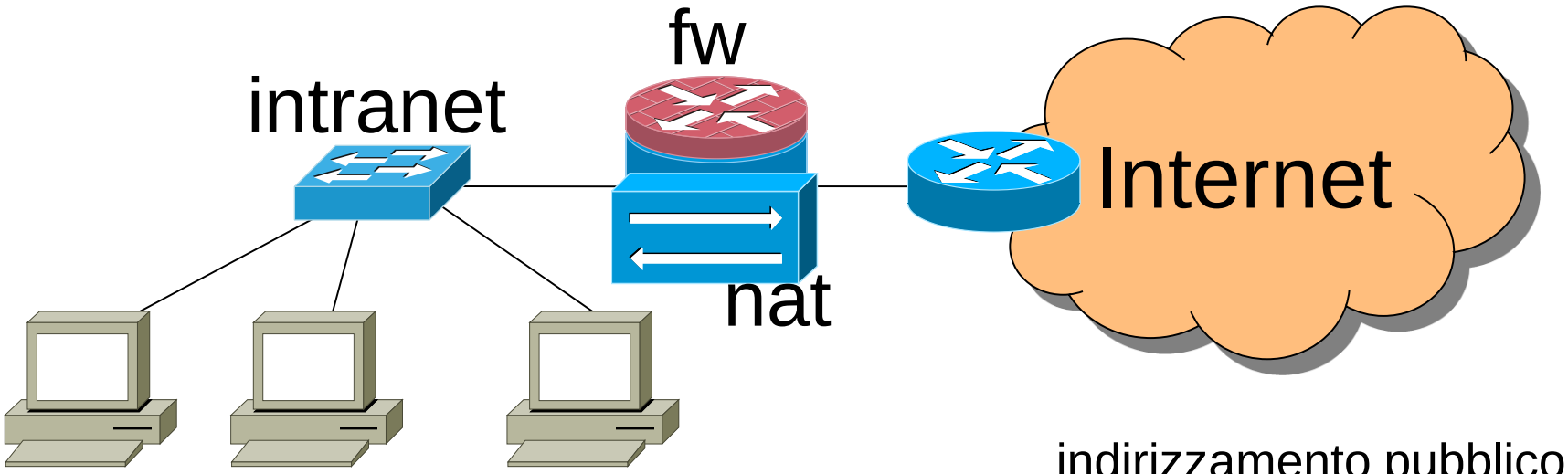
- detti anche “screening routers”
- sono firewall “stateless”
  - tipicamente quando si parla di firewall si fa riferiemento a firewall “stateful”

stateful packet filter firewall

- tengono traccia delle connessioni
  - solitamente tcp ma anche udp
  - stato della connessione: new, established, ecc.
- ciascun pacchetto è assegnato ad una connessione
  - filtrano in base allo stato della connessione
    - es. verso la rete interna solo se connessione è established
  - verificano la correttezza del protocollo
    - es. syn ammesso solo per connessioni nuove
  - **permettono regole in base allo stato della connessione**
- possono modificare il traffico
  - es. per implementare schemi anti-SYNflood

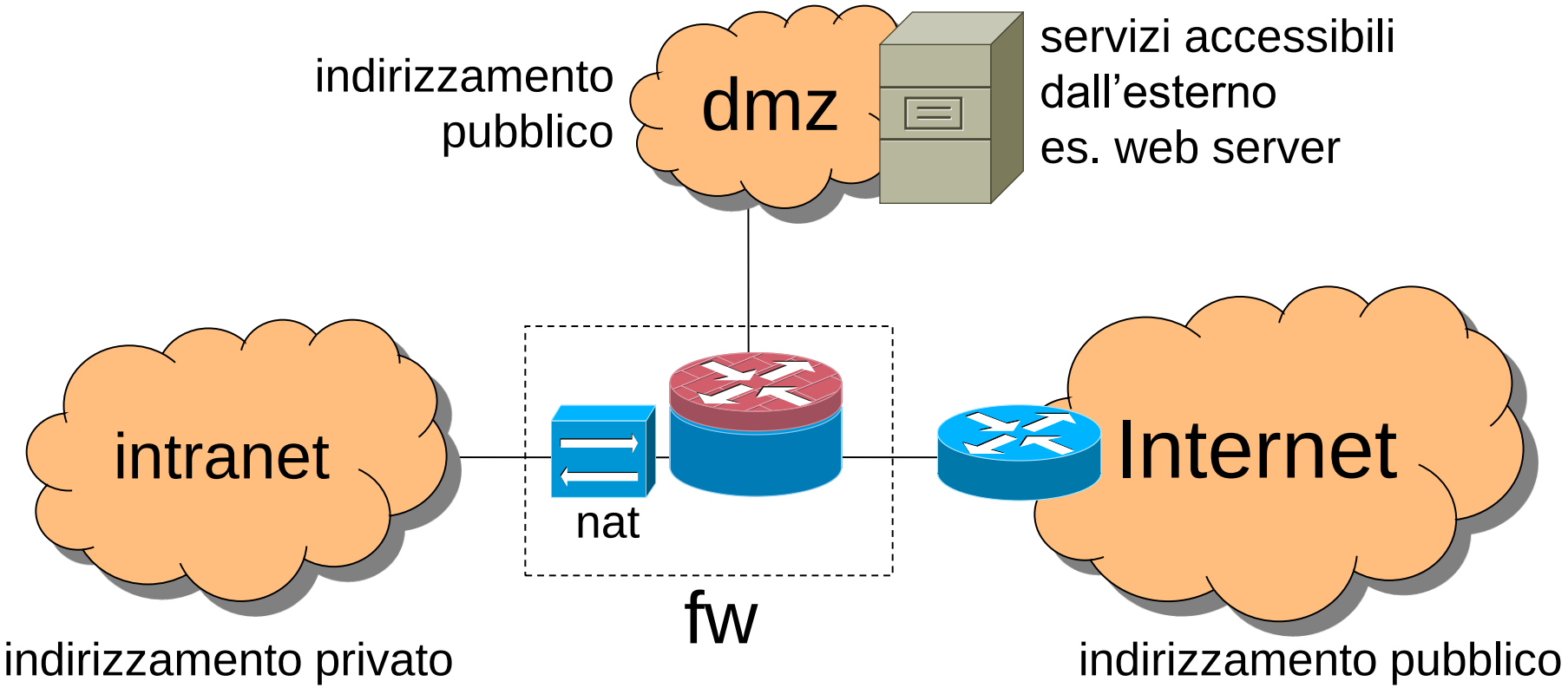
firewall, nat e intranet

- un semplice caso d'uso
  - isolare la intranet da Internet
  - in questa configurazione tipicamente il fw fa anche nat



dmz

- demiliterized zone (zona smilitarizzata) o perimeter network (rete perimetrale)
  - rete distinta sia da Internet che dalla intranet
  - gli host in tale rete sono in una classe di sicurezza distinta da quelli della intranet



dmz: esempio di policy

da \ a	host intranet	host dmz	host Internet
host intranet	all non si passa per il fw	richiesta dalla intranet si accede ai servizi della dmz	- dalla intranet non si accede a Internet
host dmz	risposta dalla dmz si risponde alle richieste della intranet	all non si passa per il fw	risposta dalla dmz si risponde alle richieste di Internet
host Internet	- da Internet non si accede alla intranet	richiesta da Internet si accede ai servizi della dmz	all non si passa per il fw

interpretazione per protocolli basati su tcp

- “richiesta”
  - un syn per una connessione NEW
- “risposta”
  - tutto ciò che è relativo ad una connessione ESTABLISHED (dopo il syn)

- facile da implementare in un firewall stateful

varianti

- intranet potrebbe dover accedere ad Internet
  - questo potrebbe rappresentare un grave problema di sicurezza perché Internet è una fonte di input non fidato
    - consigliato l'uso di application level gateway o application level packet inspection
- dmz potrebbe dover accedere a…
  - dns, per i log
    - fonte non fidata
  - servizi di altri fornitori
    - il grado di fiducia può variare

packet filtering: problemi

- la configurazione può essere molto complessa
  - facile fare errori
  - i firewall stateful sono un po' più semplici da configurare, ma la complessità rimane
  - configurazione fatta con indirizzi IP
    - non possiamo fidarci della risoluzione DNS

firewall e DDOS

- DDOS che saturano la banda
  - il firewall non aiuta
- DDOS che aprono tante connessioni
  - aging, white/black-list, etc.
- syn-flood: DDOS che inviano tanti syn da indirizzi spoofati => **syn proxy**
  - il fw risponde syn-ack e non inoltra il syn al server
  - quando arriva l'ack, si fa three-way-handshake con il server
  - raccordo dei numeri di sequenza come in certi nat
  - il fw è progettato per scalare sulle connessioni mezze aperte

syn cookies

- implementato su server o in fw (syn proxies)
- una delle poche soluzioni in grado di discriminare il traffico lecito da quello non lecito in maniera automatica
- chi risponde al syn non mantiene alcuno stato!
  - scalabilità non dipende dalla memoria riservata a connessioni mezze aperte
- lo stato è codificato nel sequence number
  - la codifica è firmata: tutto dentro 32 bits
- l'ack in risposta contiene il sequence number +1
  - cioè, per le connessioni «buone» il server ottiene lo stato che avrebbe dovuto mantenere
- limitato supporto a TCP options
- implementato in Linux

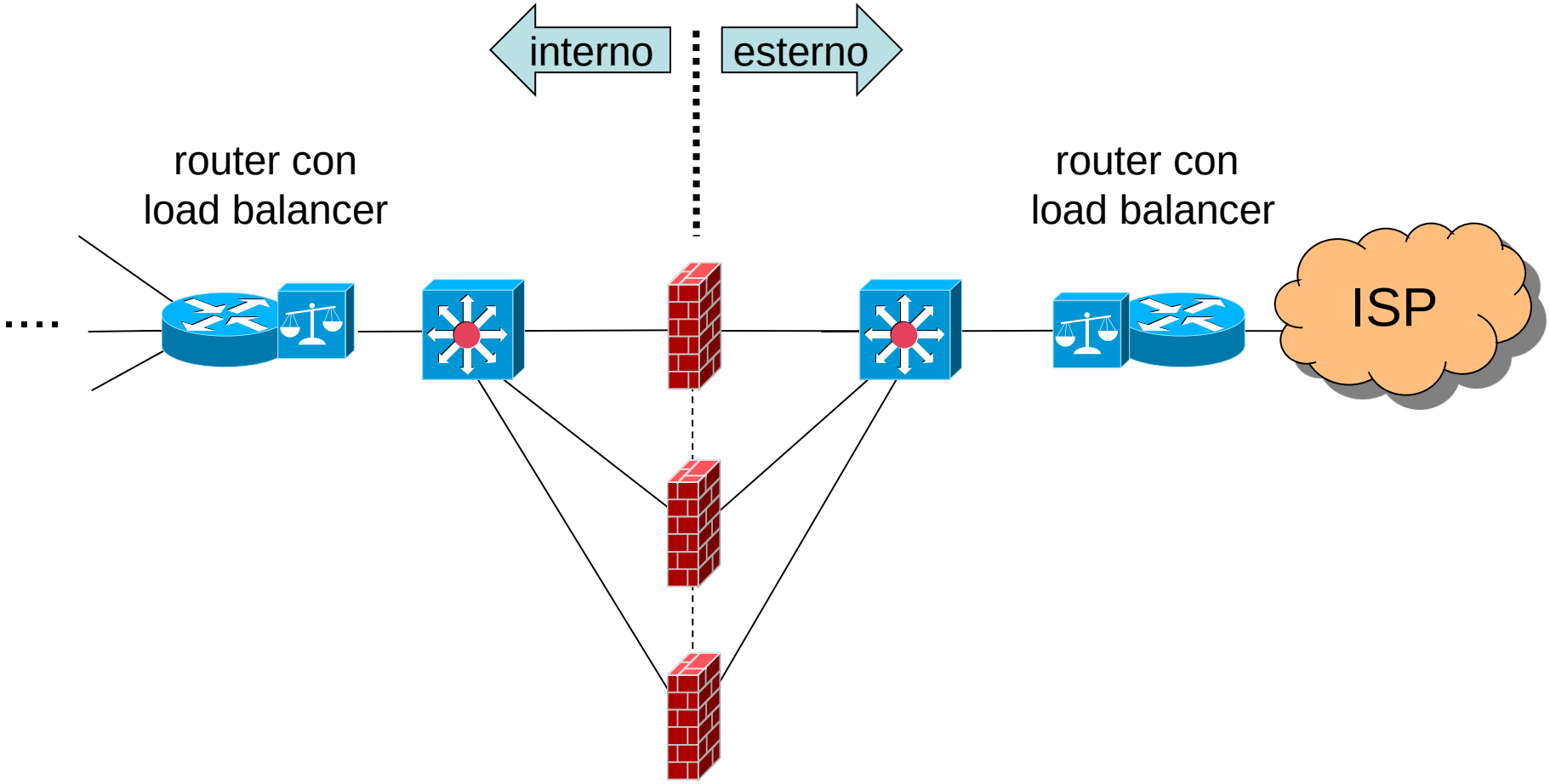
  echo 1 > /proc/sys/net/ipv4/tcp_syncookies

prestazioni e affidabilità

- i fw spesso sono
  - un collo di bottiglia per le prestazioni
  - un single point of failure
- spesso utilizzati in configurazione “cluster” con tutti gli elementi attivi
  - bilanciamento del carico
  - ridondanza
- load balancer
- i fw si scambiano lo stato (soluzioni proprietarie)

prestazioni e affidabilità

- una architettura d'esempio



load balancer

- più difficile che scegliere un server
- ciascun fw deve vedere il traffico di una sessione in entrambe le direzioni
- due possibilità
  - i load balancer tengono traccia delle sessioni esplicitamente
  - I load balancer sanno da che parte stanno e si comportano di conseguenza

    al ritorno l'ordine con cui si calcola l'hash è l'inverso poiché src e dest sono scambiate

    interno: fw=hash(src_ip, dest_ip)

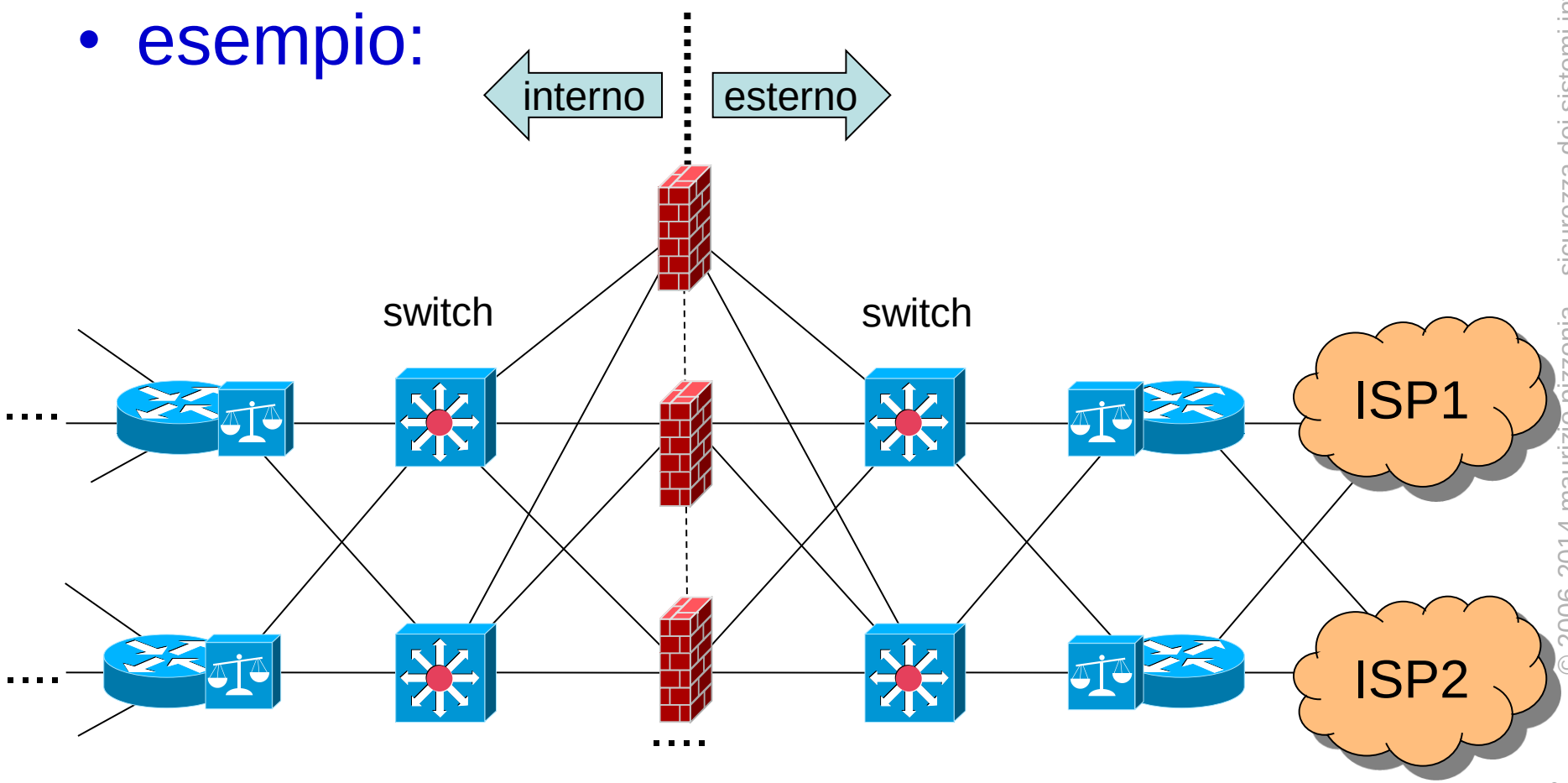
    esterno: fw=hash(dest_ip,src_ip)
- caveat
  - load balancer assegna l'intera connessione ad un fw, ma…
  - non così ovvio: alcuni protocolli coinvolgono più sessioni tcp (es. ftp)

affidabilità dei componenti di contorno

- i router possono essere un single point of failure
  - quanto down-time siamo disposti a sopportare?
  - le configurazioni tolleranti ai guasti per mezzo di elementi ridondati si dicono in “fail over” o “high-availability”
- le configurazioni che prevedono tutti gli elementi ridondati possono essere molto complesse
  - costose
  - difficili da gestire
- high-availability è necessaria quando gli SLA (service level agreement) non prevedono il tempo per la sostituzione di uno degli elementi

full high-availability

- ciascun elemento dell'architettura deve essere ridondato
- esempio:



(intermezzo: gw ridondato)

- principio: no single point of failure!
- soluzioni per il default gateway di una lan
  - quando si rompe corri ad accendere il fail-over (!)
  - fai partecipare ciascuna macchina della lan al protocollo di routing (!!!!)
  - Virtual Routing Redoundancy Protocol, rfc 5798
- VRRP
  - un indirizzo ip V per un router virtuale
  - il router virtuale è composto da, almeno, due router
  - solo uno solo risponde all'arp request per V: il master
  - il master manda un heartbeat periodico agli altri router
  - quando il master muore uno degli altri prende il suo posto
    - meccanismo di elezione (tipo root bridge negli spannin tree)
- HSRP: analogo, proprietario cisco

linux netfilter

- sistema di moduli Linux che realizza un fw
  - packet filter
  - stateful
  - nat
  - sistema di access list (chains) organizzate per funzionalità (tables)
  - tables
    - filter
      - chains: INPUT, OUTPUT, FORWARD
    - nat
      - chains: PREROUTING, POSTROUTING, OUTPUT
  - si possono definire delle “user-defined chain”
  - ciascuna tabella viene gestita da un modulo del kernel

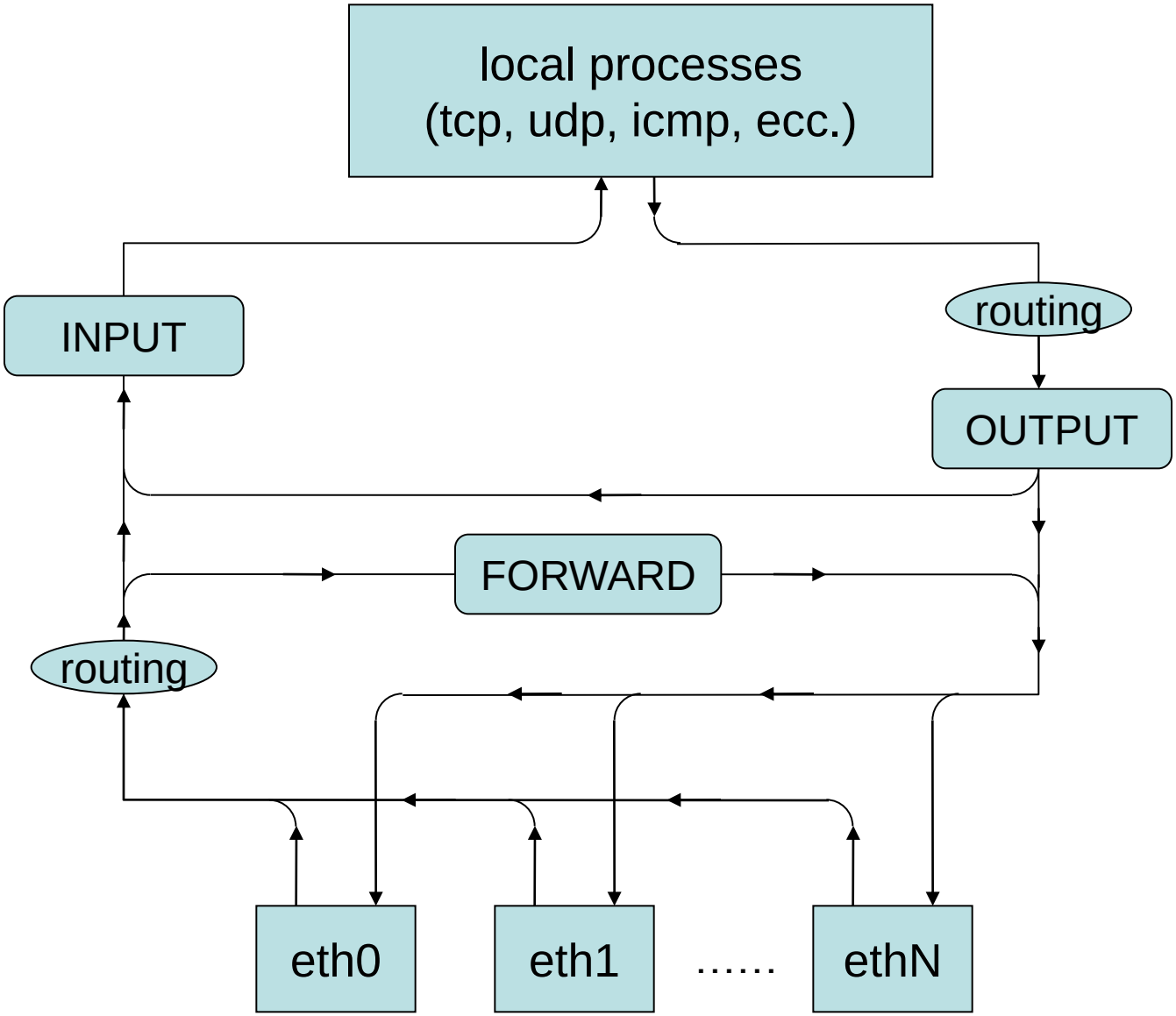
linux netfilter: chains (acl)

- ciascuna chain ha una sequenza di regole e un target
  - il target specifica cosa fare del pacchetto se questo non ha attivato alcuna regola
- target possibili
  - ACCEPT (pacchetto ok, lascia passare)
  - DROP (pacchetto droppato)
  - REJECT (come drop ma invia un icmp di errore al mittente)
  - <chain name> (salta alla chain specificata, come una chiamata a procedura, utile con “user-defined chain”)
  - RETURN (ritorna alla chain chiamante)
  - ...

linux netfilter: firewall rules

- una regola ha dei parametri e un target
  - i parametri specificano per quali pacchetti la regola viene attivata
  - il target specifica cosa fare
- parametri
  - protocollo (-p ip/tcp/udp/)
  - source/destination address (-s/-d [!]x.x.x.x/x)
  - source/destination port (--sport/--dport port)
  - input/output interface (-i/-o ethN)
  - tcp flags syn=1 e ack=0 (--syn)
  - e altri

linux netfilter: filter table



linux netfilter: connection tracking

- netfilter tiene traccia delle “connessioni”
  - per tcp e udp: coppia (non ordinata) di coppie {<addr, port>, <addr, port>}
  - per icmp echo: coppia di indirizzi {addr, addr}
- a ciascun pacchetto è associata una connessione (eventualmente ne viene creata una nuova)
  - questo viene fatto appena un pacchetto entra in netfilter da una interfaccia o dai processi locali
  - le connessioni muoiono per timeout o per protocollo (fin/ack, rst)
- stato del pacchetto
  - NEW: primo pacchetto della connessione
  - ESTABLISHED: pacchetto di una connessione già esistente
  - RELATED: nuova connessione associata ad una precedente (ftp, icmp errors)
  - INVALID: impossibile associare una connessione (es. icmp error non associati ad alcuna connessione)

linux netfilter: extended matches

- l'opzione -m <nome> permette di attivare molti altri tipi di regole
  - **state**: filtro in base allo stato (NEW, ESTABLISHED, RELATED, INVALID)
    - **conntrak** è una versione estesa
  - **mac**: filtro in base agli indirizzi mac di livello 2
  - **limit**: filtro in base alla frequenza di arrivo
    - anti DoS, anti scanning ecc.
  - **iprange**: es. 192.168.1.13-192.168.2.19
  - e molti altri

netfilter: comandi

- iptables
  - modifica e mostra la configurazione
    - -L mostra la configurazione
    - --flush cancella la configurazione
    - -A <chain> aggiunge in coda a <chain> un regola
    - ecc.
- iptables-save
  - dump della configurazione attuale
- iptables-restore
  - carica la configurazione da un dump fatto con iptables-save (più efficiente che molte chiamate a iptables)

esempio: nessun filtro

- **iptables --flush**
- **iptables-save**

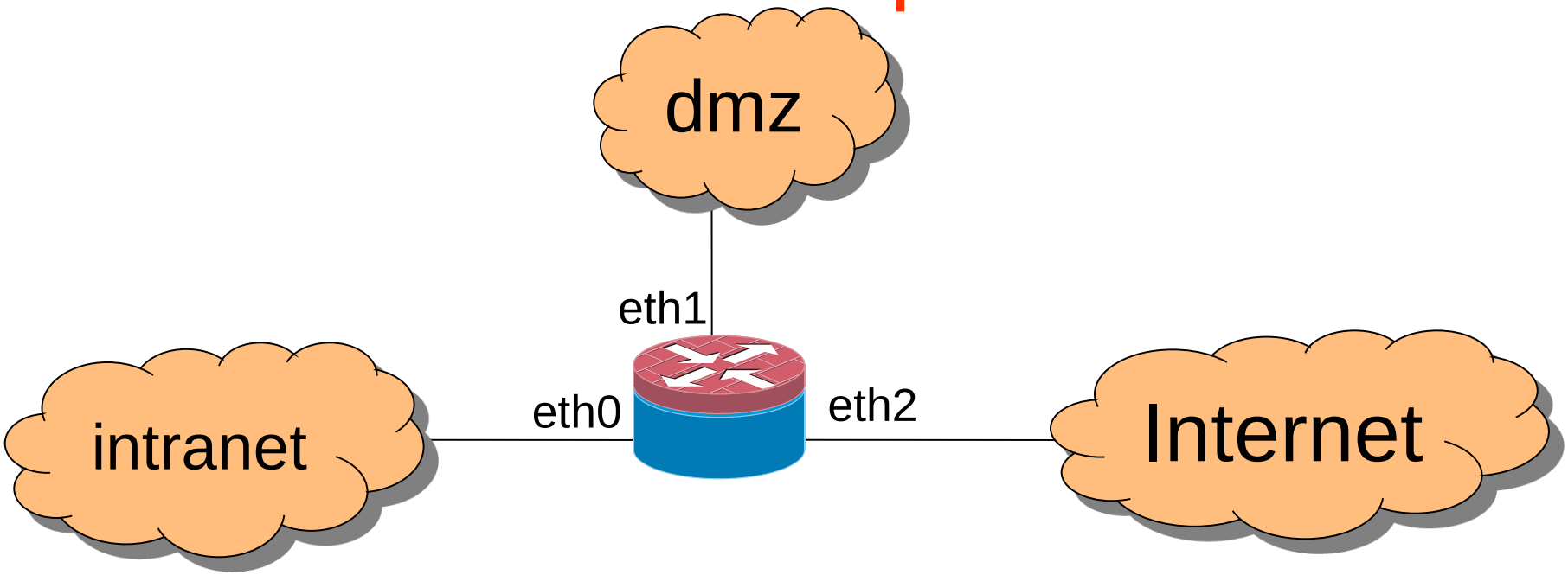
```
# Generated by iptables-save v1.3.3 on Fri Dec  8 17:58:19 2006
*filter
:INPUT ACCEPT [37:4620]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [19:1352]
COMMIT
# Completed on Fri Dec  8 17:58:19 2006
```

esempio: un semplice personal firewall

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

```
# Generated by iptables-save v1.3.3 on Fri Dec  8 18:26:51 2006
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [14735:2397896]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Fri Dec  8 18:26:51 2006
```

implementazione della politica dmz di esempio




```
*filter
:INPUT ACCEPT [64:3448]
:FORWARD DROP [13:858]
:OUTPUT ACCEPT [409:37987]
-A FORWARD -i eth0 -o eth1 -m state --state NEW -j ACCEPT
-A FORWARD -i eth2 -o eth1 -m state --state NEW -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

proxy applicativi

- due sessioni di trasporto
  - S ↔ Proxy ↔ D
- permettono verifiche di sicurezza a livello applicativo
  - devono conoscere i protocollo applicativo o almeno parte di esso
- **spesso usati per prevenire comportamenti insicuri degli utenti della intranet**
- protocolli
  - http, https
  - smtp, pop3, imap
  - ftp, dns, sql

- circuit level proxies (SOCKS)
  - proxy generico, indipendente dal protocollo applicativo
  - utile per forzare una autenticazione a livello tcp

web proxy: obiettivi

- **autenticazione, controllo di accesso al servizio**
- **test per codice malevolo**
- anonimità
- prestazioni: caching
- modifica contenuto
  - censura
  - riformattazione per schermi piccoli (cellulari, PDA)
- reverse proxy: un proxy in prossimità di un web server che riceve le richieste da Internet
  - sicurezza (bastion host), load balancing, encryption acceleration, cache del contenuto statico
- open source: squid, privoxy, spikeproxy

transparent web proxy

- un web proxy regolare richiede la configurazione del browser
  - scomodo
  - la presenza del proxy è palese
- un proxy “transparent” intercetta richieste http qualsiasi
  - non richiede configurazione del browser
  - il proxy c’è ma non si vede
- esercizio: configurare linux netfilter per un transparent proxy

web proxy: vulnerabilità

- il protocollo http prevede il metodo CONNECT
- tale metodo viene interpretato dai proxy come un comando per lasciare passare connessioni arbitrarie
  - usato per connessioni http criptate
    - https (http su secure socket layer)
  - se connessione è criptata il proxy non può conoscerne il contenuto
- disabilitare CONNECT comporta l'impossibilità di usare https

network based IDS (NIDS)

- verifica la presenza sulla rete di traffico riconducibile ad attività sospette
- si avvale di uno sniffer
  - particolari precauzioni per reti switched
- riconosce il traffico malevolo tramite
  - regole contenuto in un db
  - tecniche statistiche per anomaly detection
- open source: snort (http://www.snort.org/)
  - supportato sia sotto Windows che sotto Linux

NIDS e reti switched

- il nids è innanzi tutto uno sniffer
- sniffare reti swithced è complesso
- supporto degli switch
  - port mirroring
  - multi-port mirroring
  - vlan mirroring
- caveat
  - la banda della destination port può essere insufficiente anche se lo switch è full speed

NIDS: azioni

- può generare un log delle attività sospette
- può riconfigurare automaticamente un firewall
  - attività di contrasto automatica
  - detti anche intrusion prevention systems (IPS)
  - un NIDS–IPS è tipicamente in configurazione in-line con firewall incorporato
    - in sostanza un firewall con due interfacce che analizza il traffico da cui è attraversato

NIDS e connessioni tcp

- un NIDS non si può limitare a verificare ciascun pacchetto ip
- gran parte degli attacchi sono a livello applicativo e incapsulati in tcp
- è necessario seguire la sessione tcp e applicare le regole al flusso di bytes
  - molto oneroso!

NIDS: scalabilità

- un NIDS dovrebbe essere in grado di elaborare tutto il traffico della rete
  - ogni pacchetto un lookup nel db
    - db in memoria
  - perdita di pacchetti $\rightarrow$ perdita di accuratezza
    - falsi negativi
  - le risorse necessarie dipendono da
    - numero di pacchetti
    - quantità di flussi tcp e desequenziamento

NIDS: load balancing

- è possibile mettere più NIDS in parallelo
- è necessario che ciascun flusso venga analizzato dallo stesso NIDS
  - flusso: pacchetti con la stessa quadrupla <saddr, sport, daddr, dport>
    - altra definizione di flusso possibile: stessa coppia <saddr, daddr>
  - in questo modo ciascun NIDS mantiene un insieme di connessioni tcp

switches e link aggregation (lag)

- gli switch permettono di aggregare più link in un solo link logico (lag)
  - utile per utilizzare due link paralleli senza spanning tree
  - autoconfigurato con il Link Aggregation Control Protocol, ieee 802.3ad
- bilanciamento del traffico sui vari link
  - ciscun flusso sullo stesso link
    - fondamentale per non desequenziare i pacchetti di un flusso – tcp inefficiente al risequenziamento massivo
  - tecnica dell'hash: link=hash(src,dst)

NIDS load balancing = ½ lag

- il lag è spesso configurabile anche staticamente
  - noi lo useremo con un solo switch!
- dietro a ciascuna porta del lag un NIDS
- mirroring di VLAN su un lag
- i lag mandano flussi identici su porte identiche e quindi sugli stessi NIDS.

HIDS vs. NIDS

- controllano aspetti diversi
  - host based
    - legittimtà del comportamento del software (integrità del sistema)
    - legittimità del traffico di rete da/per un host specifico
  - network based:
    - legittimità di tutto il traffico nella rete
- approcci complementari