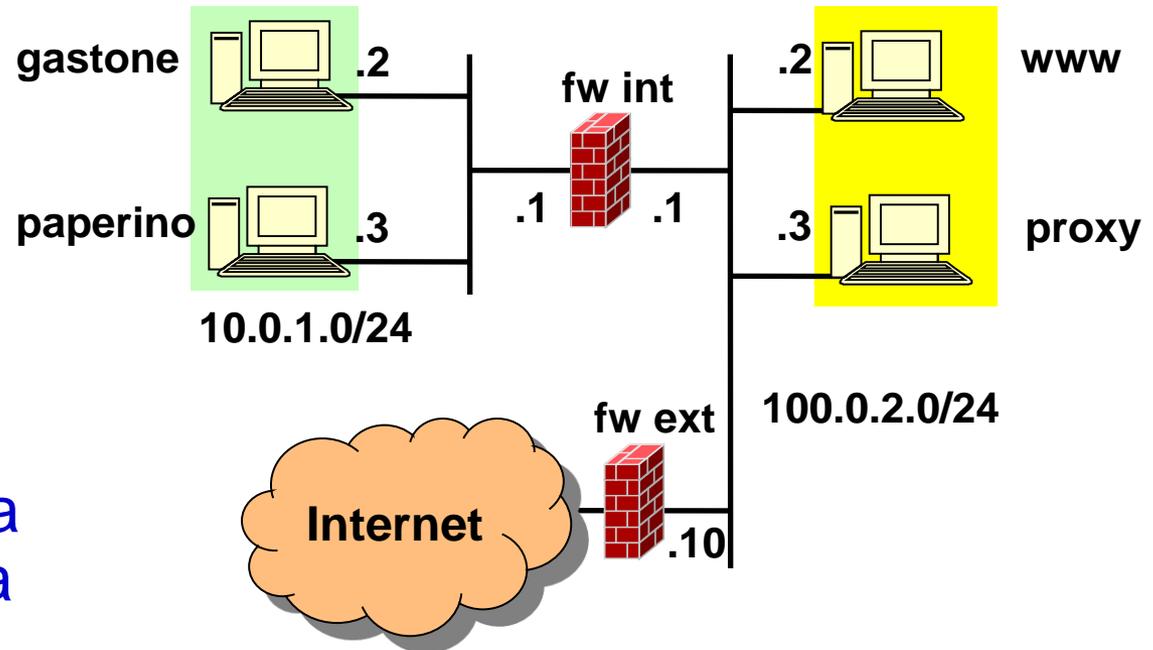


esercizi su sicurezza delle reti

screened subnet

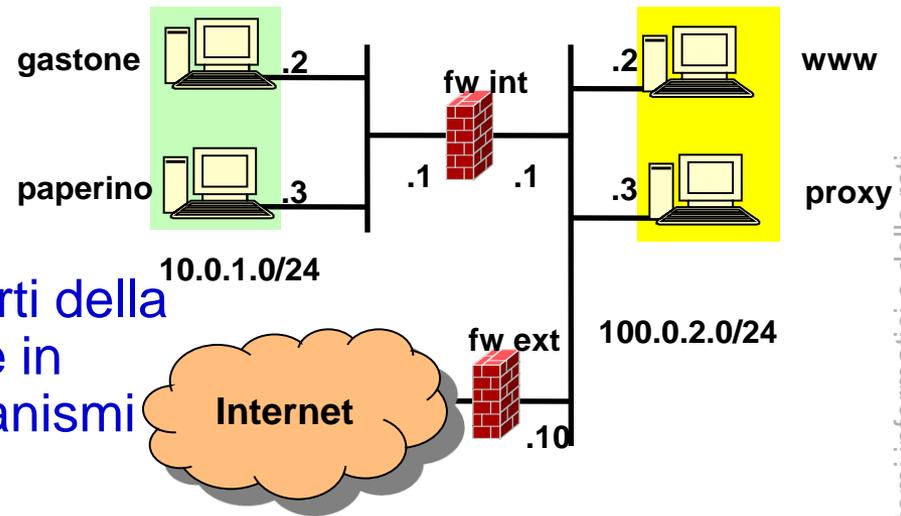


- supponi i fw siano linux con iptables
- dai una matrice di accesso che esprima la policy qui descritta

- policy

- www è il web server della ditta
- proxy è il bastion host da cui passano le richieste web dalla intranet per i siti di Internet e le richieste da Internet per www
- paperino può accedere solo a www direttamente
- gastone può a www direttamente e ad internet tramite il proxy

AM e FW



- per la seguente AM individua quali parti della matrice possono essere implementate in quali FW e quali richiedono altri meccanismi

da	a	gastone	paperino	internet	www	proxy
gastone		non pertinente	-	-	http (richieste)	http (richieste)
paperino		-	non pertinente	-	http (richieste)	-
internet		-	-	non pertinente	-	http (richieste e risposte) dns (risposte)
www		http (risposte)	http (risposte)	-	non pertinente	http (risposte)
proxy		http (risposte)	-	http (richieste e risposte) dns (richieste)	http (richieste)	non pertinente

classi di sicurezza e fw

richiede un fw sulle macchine gastone e paperino, non richiesto

da a	gastone	paperino	internet	www	proxy
gastone	non pertinente	-	- fw int/ext	http (richieste) fw int	http (richieste)
paperino	-	non pertinente	-	http (richieste)	-
internet	- fw int/ext	-	non pertinente	-	http (richieste e risposte) dns (risposte) fw ext
www	http (risposte) fw int	http (risposte)	-	non pertinente	http (risposte) fw ext
proxy	http (risposte)	-	http (richieste e risposte) dns (richieste)	http (richieste)	non pertinente

richiede un fw sulle macchine www e proxy, non richiesto

screened subnet: una soluzione

- fw int

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A FORWARD -p tcp -s gastone -d proxy --dport www -m state --state NEW -j ACCEPT
-A FORWARD -p tcp -s gastone -d www --dport www -m state --state NEW -j ACCEPT
-A FORWARD -p tcp -s paperino -d www --dport www -m state --state NEW -j ACCEPT
-A FORWARD -m state --state ESTABLISHED -j ACCEPT
COMMIT
```

- fw ext

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A FORWARD -p tcp -s proxy --dport www -m state --state NEW -j ACCEPT
-A FORWARD -p udp -s proxy --dport domain -m state --state NEW -j ACCEPT
-A FORWARD -p tcp -d proxy --dport www -m state --state NEW -j ACCEPT
-A FORWARD -m state --state ESTABLISHED -j ACCEPT
COMMIT
```

- analizza la soluzione, e considera il suo comportamento nei confronti di un attacco di spoofing

vulnerabilità a ip spoofing

- minaccia

- da Internet un syn per la porta 80 con indirizzo sorgente di proxy viene fatto passare da fw ext verso qualsiasi indirizzo (anche www)

- contromisura

- specificare esplicitamente l'interfaccia

```
-A FORWARD -i eth0 -p tcp -s proxy --dport www -m state --state NEW -j ACCEPT
```

```
-A FORWARD -i eth0 -p udp -s proxy --dport domain -m state --state NEW -j ACCEPT
```

- filtri anti spoofing

- sorgenti interne non possono venire dall'esterno

```
-A FORWARD -i eth1 -s 100.0.2.0/24 -j DROP
```

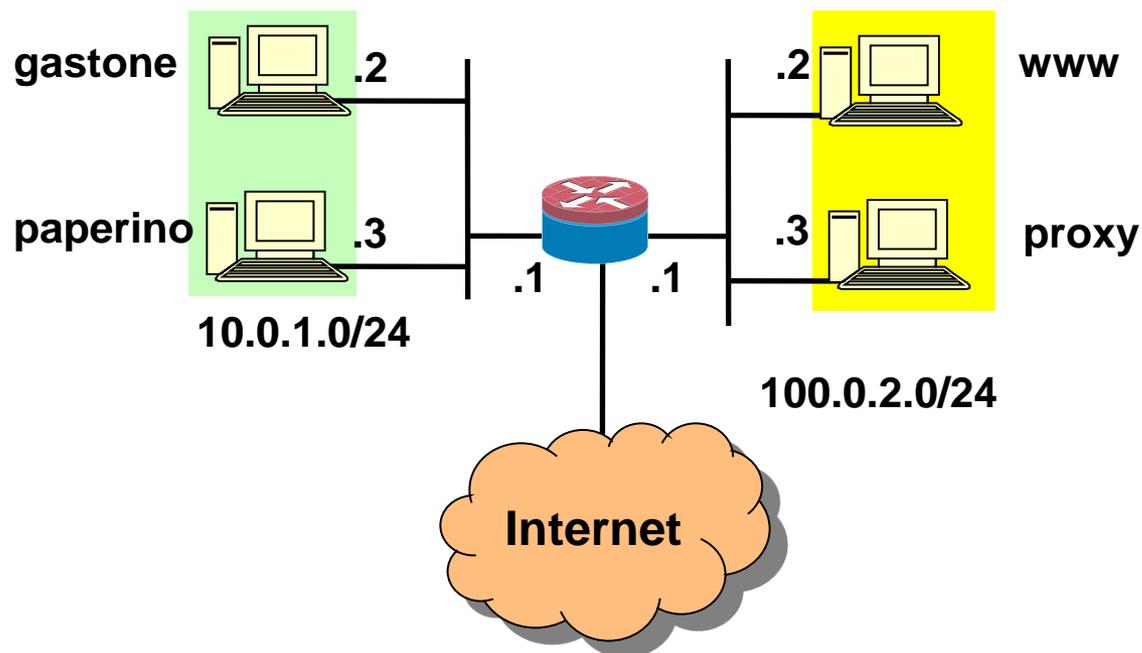
linux: antispoofing

- linux può verificare che ciascun pacchetto sull'interfaccia X abbia un ip sorgente atteso su quella interfaccia
- controllato da
 - `/proc/sys/net/ipv4/conf/X/rp_filter`
- sfrutta la tabella di instradamento
 - quella visualizzabile con “ip route” o “route”
 - attenzione la tabella deve contenere tutte le rotte interessanti (ad esempio anche quella della rete interna)
- attivazione su tutte le interfacce

```
for i in /proc/sys/net/ipv4/conf/*/rp_filter; do
    echo 1 > $i
done
```

firewall con tre interfacce

- per motivi economici si può optare per un firewall con tre interfacce
- dai la configurazione del firewall per la policy vista e la topologia sottostante
- elenca almeno tre potenziali problemi di questa soluzione rispetto a quella con due firewall



stateful vs. stateless

- semplice firewall stateful (eth0 sulla rete interna)

```
*filter
```

```
:FORWARD DROP [0:0]
```

```
-A FORWARD -i eth0 -o eth1 -m state --state NEW -j ACCEPT
```

```
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
COMMIT
```

- mostra una configurazione stateless che sfrutti il fatto che i pacchetti tcp danno informazioni sullo stato della connessione (syn, ack)
 - --syn significa SYN=1 e ACK=0

esercizio

- se il firewall è stateless si può sfruttare il fatto che i pacchetti tcp danno informazioni sullo stato della connessione

```
*filter
```

```
:FORWARD DROP [0:0]
```

```
-A FORWARD -i eth0 -o eth1 -p tcp --syn -j ACCEPT
```

```
-A FORWARD -p tcp ! --syn -j ACCEPT # SYN+ACK è accettato
```

```
COMMIT
```

- l'implementazione stateless proposta non è equivalente a quella stateful
 - quale traffico è **accettato** dalla stateful e **non** è **accettato** dalla stateless?
 - è traffico fidato o no? utile o no?
 - quale traffico è **accettato** dalla stateless e **non** è **accettato** dalla stateful?
 - è traffico fidato o no? utile o no?

soluzione

- **quale traffico è accettato dalla stateful e non non è accettato dalla stateless?**
 - qualsiasi protocollo diverso da tcp riconosciuto dal connection tracker del kernel per connessioni iniziate dal lato di eth0
 - es.: udp, icmp echo
 - le connessioni “related”
 - es.: ftp data channel da eth1 a eth0
- si tratta in ogni caso di traffico che tipicamente è considerato fidato perché iniziato da eth0 o relativo a connessioni iniziate da eth0
- tale traffico andrebbe accettato

soluzione

- quale traffico è **accettato dalla stateless** e **non è accettato dalla stateful**?
 - i pacchetti tcp con bit SYN e ACK settato in direzione eth1→eth0 anche al di fuori del 3-way-handshake
 - i pacchetti tcp con bit SYN e ACK settato in direzione eth1→eth0 anche all'inizio del 3-way-handshake
- si tratta di traffico che non rispetta il protocollo non è considerato fidato perché viene da eth1
- tale traffico non dovrebbe essere accettato

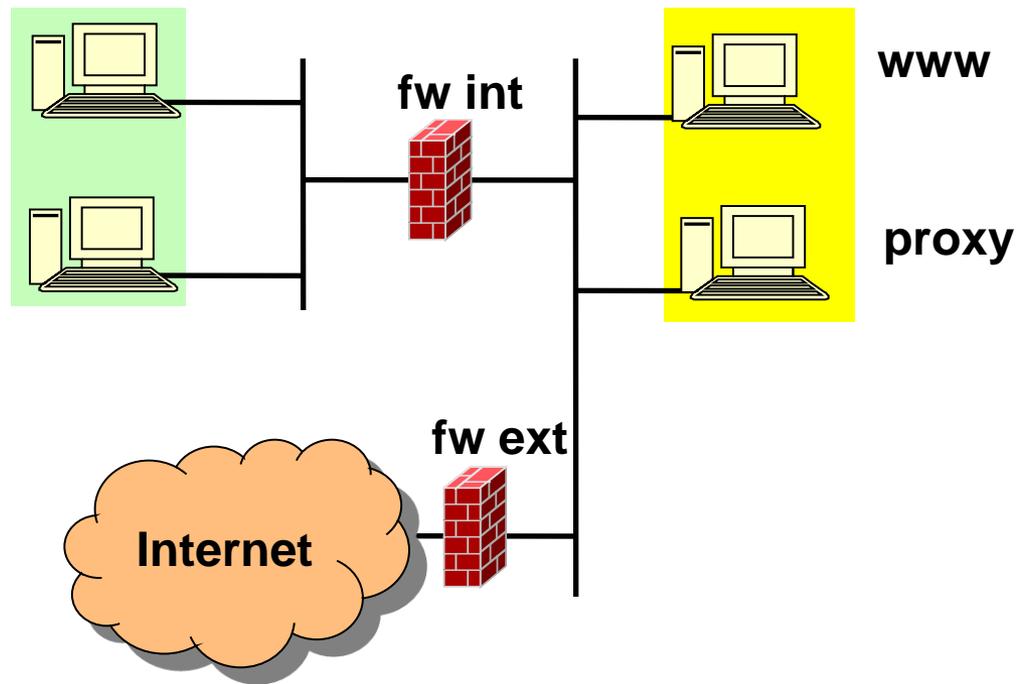
esercizio

- prova a dare una configurazione stateless che approssimi meglio quella stateful

proxy web

- una piccola azienda vuole dare ai dipendenti accesso al web e **nient'altro**
- listino prezzi
 - proxy web + content analysis sw 800 euro
 - proxy web 2 schede di rete + content analysis sw 820 euro
 - router dotato di interfaccia xDSL per accesso a internet e 1 interfaccia ethernet 400 euro
 - firewall stateful (livelli 3+4) 2 interfacce ethernet 600 euro
 - firewall stateful (livelli 3+4) 3 interfacce 700 euro
 - UTM 1000 euro
- progetta la rete che abbia “buone” caratteristiche di sicurezza, rispetto ai requisiti, e basso costo

nids



- dove metteresti dei nids? perché?
- supponi che la intranet sia piccola ma il sito web sia molto acceduto da Internet
- quali sono i bottleneck prestazionali
- come possono essere risolti?
- introduci ridondanza piena sulle apparecchiature critiche per il sito web