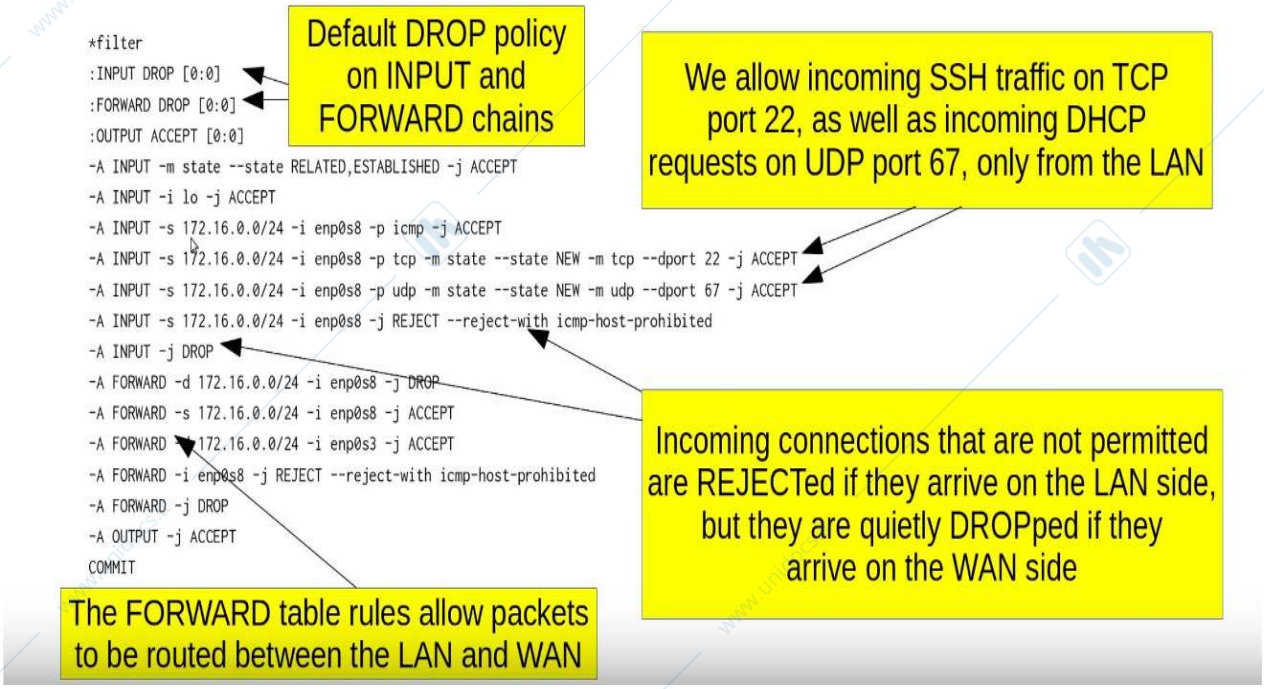
Appunti ed esercizi esame svolti - esercizi iptables di esami

Sicurezza dei sistemi e delle reti (Università degli Studi di Milano)

Example: Basic Router

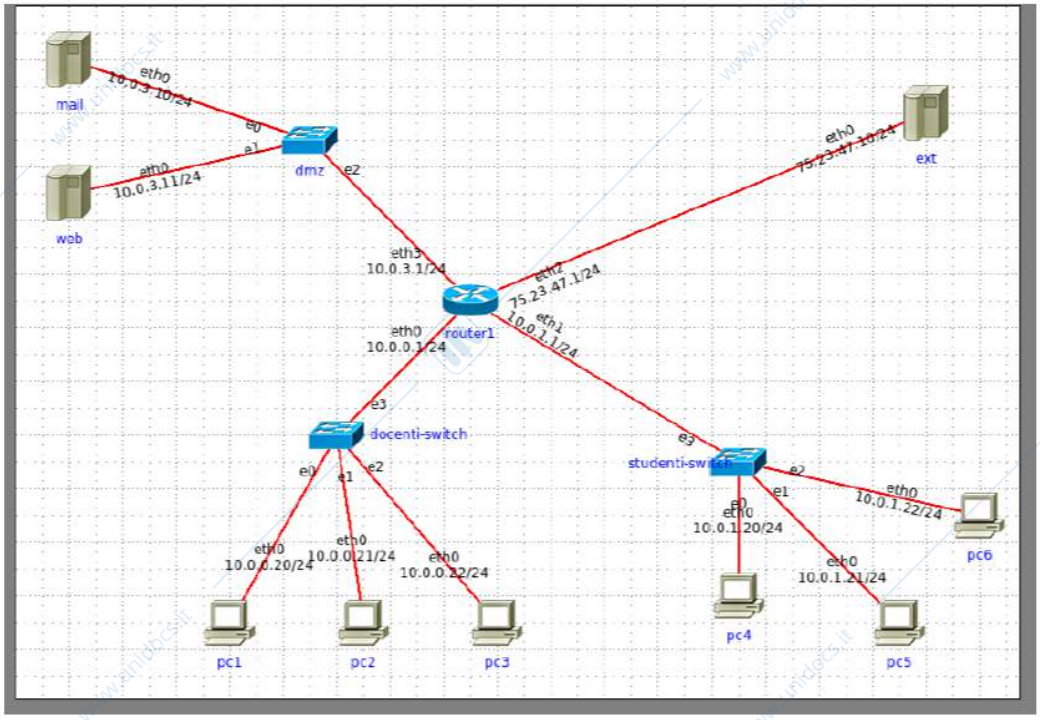


In generale:

PROF="10.0.0.0/24"
STUD="10.0.1.0/24"

SERVER="10.0.3.0/24"

*EXT="!$PROF, !$STUD, !$SERVER" (*Le variabili si dichiarano senza il $, il $ lo metti solo quando ne fai uso)



Abbiamo:

- Router per la connettività internet

- Switch di DMZ con:

    - Mail server solo per uso interno

    - Server web per servizi universitari interni (portale studenti su 8080) ed esterni (sito web)

- Rete studenti con tre postazioni

- Rete docenti con tre postazioni

1. Scrivere le regole di firewalling (iptables) per garantire le seguenti situazioni:

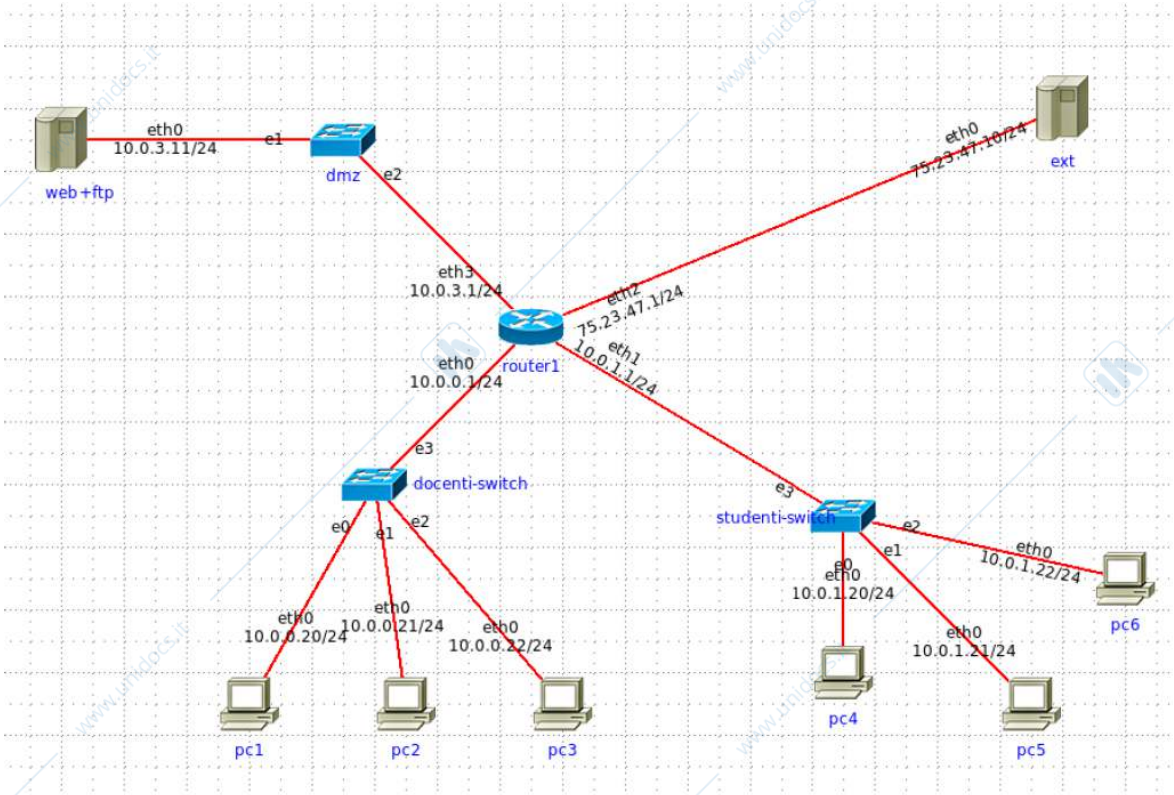
---

a. La rete dei professori può accedere al server mail sulle porte SMTP e IMAP, al server web (HTTP) e navigare in internet.
b. La rete degli studenti può accedere **SOLO** al server web sulla porta 8080, dove risiede il portale degli studenti, solo per uso interno.
c. Dall'esterno (ext) si può contattare solo il server web sulla porta HTTP.

Il restante traffico deve essere vietato.

La soluzione dell'esercizio è la trascrizione delle regole iptables. **E' possibile ma non obbligatorio utilizzare imunes per verificare la correttezza delle regole iptables [topologia fornita nell'apposito file .imn]**

```
PROF="10.0.0.0/24"
STUD="10.0.1.0/24"
SERVER="10.0.3.0/24"
EXT="!PROF,!STUD,!SERVER"

Firewall si router 1

#prof accede a mail su IMAP e SMTP, web http e internet (80,443)

iptables -t filter -A FORWARD -i eth0 -s $PROF -d 10.0.3.10/24 -p tcp --dport imap,smtp -j ACCEPT
iptables -t filter -A FORWARD -i eth3 -s 10.0.3.10/24 -p tcp --sport imap, smtp -d $PROF --dport 1024:65535 -m state --state
established,related -j ACCEPT

iptables -t filter -A FORWARD -i eth0 -s $PROF -d 10.0.3.11/24 -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -i eth3 -s 10.0.3.11/24 -p tcp --sport 80 -d $PROF --dport 1024:65535 -m state --state established,related
-j ACCEPT

iptables -t filter -A FORWARD -i eth0 -s $PROF -d $EXT -p tcp --dport 80,443 -j ACCEPT
iptables -t filter -A FORWARD -i eth2 -s $EXT -p tcp --sport 80,443 -d $PROF --dport 1024:65535 -m state --state established -j
ACCEPT

#stud solo 8080
iptables -t filter -A FORWARD -i eth1 -s $STUD -d 10.0.3.11/24 -p tcp --dport 8080 -j ACCEPT
iptables -t filter -A FORWARD -i eth3 -s 10.0.3.11/24 -p tcp --sport 8080 -d $STUD --dport 1024:65535 -m state --state
established,related -j ACCEPT

#ext solo http server web
iptables -t filter -A FORWARD -i eth2 -s $EXT -d 10.0.3.11/24 -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -i eth3 -s 10.0.3.11/24 -p tcp --sport 80 -d $EXT --dport 1024:65535 -m state --state established -j
ACCEPT

# Default Deny
iptables -t filter -A FORWARD -j DROP
```



Abbiamo:

- Router per la connettività internet

- Switch di DMZ con:

  - **Server web e ftp** per servizi universitari interni (portale studenti su 8080 e ftp docenti) ed esterni (solo sito web)

- Rete studenti con tre postazioni

- Rete docenti con tre postazioni

Scrivere le regole di firewalling (iptables) per garantire le seguenti situazioni:

- **Solo** la rete dei professori può accedere al server FTP

- I professori ***possono*** navigare su internet ma ***non possono*** accedere al portale web su 8080

- La rete degli studenti può **SOLO** accedere al portale web sulla porta 8080

- Dall'esterno (ext) si può contattare solo il server web sulla porta HTTP

Buongiorno,

per l'esame in oggetto, che allego, vorrei proporre la mia soluzione, non potendo semplicemente simularlo.

#default

iptables -P FORWARD DROP

iptables -P INPUT DROP

iptables -P OUTPUT DROP

#Professori

iptables -A FORWARD -p tcp -s $PROF_NET -d $INT_SERVER --dport 21 -j ACCEPT

iptables -A FORWARD -p tcp -s $INT_SERVER -d $PROF_NET --sport 20,21 -m state --state ESTABILISHED,RELATED -j ACCEPT

iptables -A FORWARD -p tcp -s $PROF_NET --dport 80,443 -d 75.23.47.10/24 -j ACCEPT

iptables -A FORWARD -p tcp -d $PROF_NET --sport 80,443 -m state --state ESTABILISHED,RELATED -j ACCEPT

#studenti

iptables -A FORWARD -p tcp -s $STUD_NET -d $INT_SERVER --dport 8080 -j ACCEPT

iptables -A FORWARD -p tcp -d $STUD_NET --sport 8080 -m state --state ESTABILISHED,RELATED -j ACCEPT

Grazie per ogni contributo e commento, sia da colleghi che - in particolare - dal tutor.

Appello-170213-Lab.pdf

Permalink | Rispondi

Re: Esame 13 febbraio 2017 - Iptables

di federico bidoggia - Wednesday, 8 August 2018, 19:30

Ciao Alessio,

ovviamente aspettiamo il parere del tutor ma provo comunque a dirti la mia, sperando di non fare ancora più confusione.

Io in tutte le regole, oltre che gli indirizzi sorgente e destinazione avrei aggiunto anche le interfacce di input e output.

Se ho interpretato bene le regole assumi di usare FTP attivo (domanda per il tutor: come dobbiamo comportarci in sede d'esame? possiamo assumere noi una delle due modalità FTP?).

Però nelle regole credo manchi quella che permette il traffico sulla connessione dati dagli host della rete dei docenti, al FTP server. Aggiungerei:

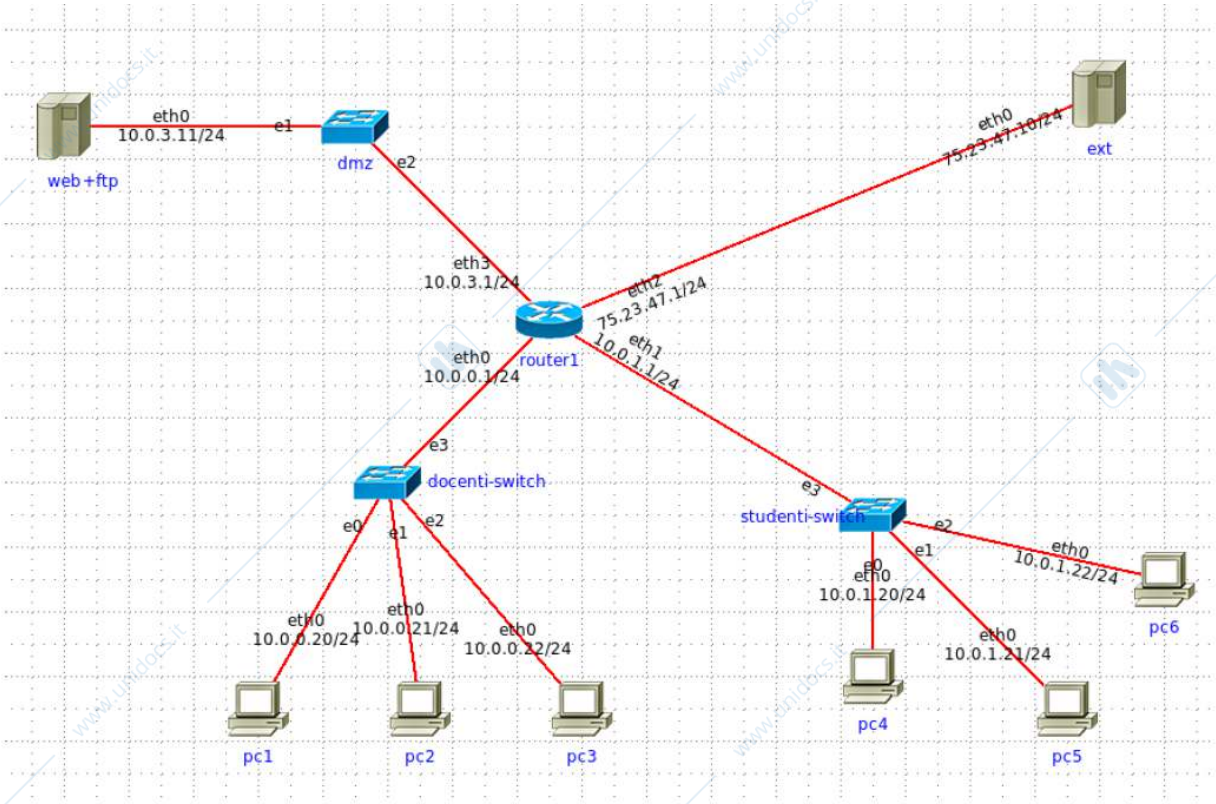
iptables -A FORWARD -p tcp -i eth0 -o eth3 -s $PROF_NET -d $INT_SERVER --dport 20 -m state --state ESTABILISHED -j ACCEPT

Come stato credo basti ESTABLISHED, visto che la connessione dati in FTP attivo è aperta dal server.

Infine credo manchino le regole per il punto "dall'esterno si può contattare solo il server web sulla porta HTTP". Io avrei aggiunto:

iptables -A FORWARD -p tcp -i eth2 -o eth3 -s $EXT -d $INT_SERVER --dport 80 -m state --state NEW, ESTABLISHED -j ACCEPT

iptables -A FORWARD -p tcp -i eth3 -o eth2 -s $INT_SERVER --sport 80 -m state --state ESTABLISHED -j ACCEPT



Abbiamo:

- Router per la connettività internet

- Switch di DMZ con:

    - **Server web e ftp** per servizi universitari esterni ed interni (portale studenti su 8080)

- Rete studenti con tre postazioni

- Rete docenti con tre postazioni

Scrivere le regole di firewalling (iptables) per garantire le seguenti situazioni:

- I professori ***possono*** navigare su internet ma ***non possono*** accedere al portale web su 8080

- La rete degli studenti può **solo** accedere al portale web sulla porta 8080 ed al server ftp

- Dall'esterno (ext) si può contattare **solo** il server web sulla porta http/https e il server ftp

Il restante traffico deve essere vietato.

Ciao a tutti,

io lo svolgerei cosi:

Facendo le seguenti assunzioni:
-firewall su router1, lo "snodo" di tutto il traffico
-variabili:
$PROF="10.0.0.0/24"
$STUD="10.0.1.0/24"
$SERVER="10.0.3.11/24"
$EXT="!$PROF,!$STUD,!$SERVER"
-le regole verrano scritte in successione e le regole attinenti ai diversi scenari saranno separate da uno spazio

iptables -A FORWARD -i eth0 -s $PROF -d $EXT -p tcp --dport 80,443 -j ACCEPT
iptables -A FORWARD -i eth2 -s $EXT --sport 80,443 -d $PROF --dport 1023:65553 -m state --state established -j ACCEPT
iptables -A FORWARD -i eth0 -s $PROF -d $SERVER -p tcp --dport 8080 -j DROP

iptables -A FORWARD -i eth1 -s $STUD -d $SERVER -p tcp --dport 8080,ftp
-j ACCEPT
iptables -A FORWARD -i eth3 -s $SERVER --sport 8080,ftp -d $STUD --dport 1023:65553 -m state --state established, related -j ACCEPT

iptables -A FORWARD -i eth2 -s $EXT -d $SERVER -p tcp --dport 80,443,ftp -j ACCEPT
iptables -A FORWARD -i eth3 -s $SERVER --sport 80,443,ftp -d $EXT --dport 1023:65553 -m state --state established, related -j ACCEPT

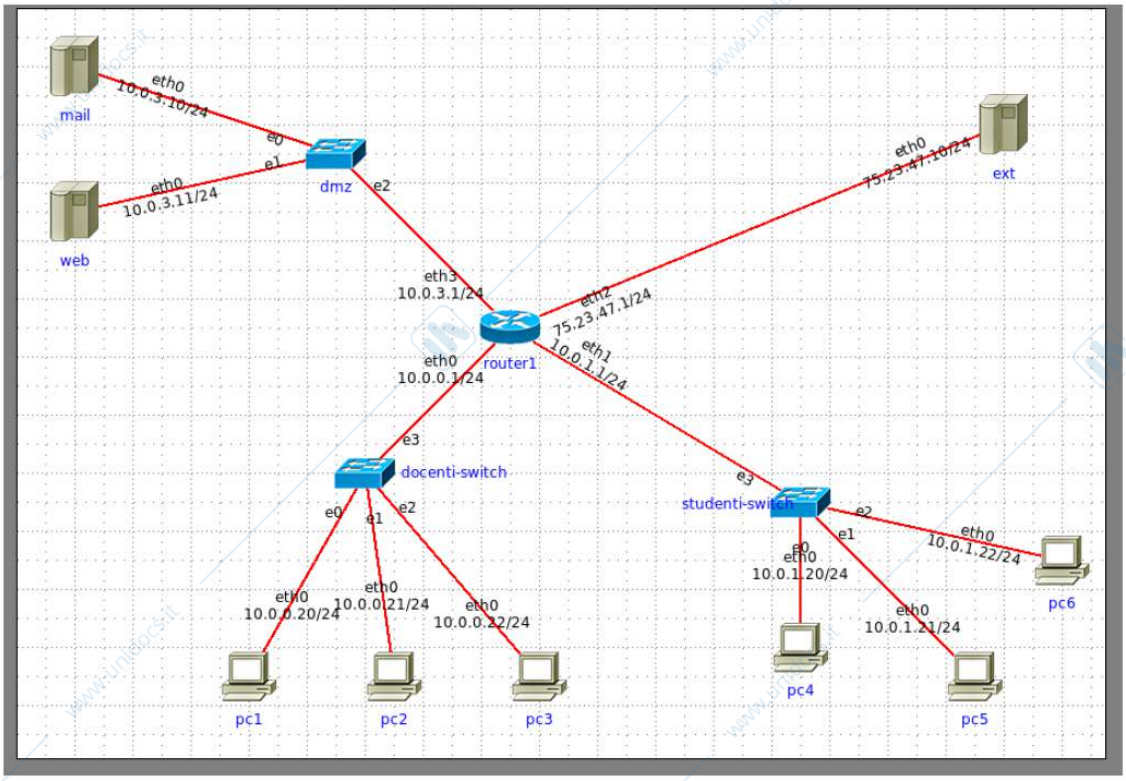
iptables -A FORWARD -j DROP

Trascurando le regole di nat, penso che qui l'obiettivo sia far capire di conoscere la sintassi iptables più che entrare fin nei minimi dettagli

cosa ne pensate? possono andare ?

Grazie

Marcello



Abbiamo:

- Router per la connettività internet

-DMZ con **Server web e mail**

-Il portale interno studenti è attivo su porta 8000

- il sito web pubblico è attivo solo su https

- Rete studenti

- Rete docenti

1. Scrivere le regole di firewalling (iptables) per garantire le seguenti situazioni:
- Solo i docenti possono inviare e ricevere email (definire quali protocolli di posta si usano)
- Gli studenti possono navigare all'esterno solo su siti che supportano https
- Le reti docenti e studenti non possono scambiarsi comunicazioni
- Solo il pc3 della rete docenti può connettersi in telnet alle macchine della dmz

---

Il restante traffico deve essere vietato.

La soluzione dell'esercizio è la trascrizione delle regole iptables

PROF="10.0.0.0/24"

STUD="10.0.1.0/24"

SERVER="10.0.3.0/24"

EXT="!PROF, !STUD, !SERVER"

#PROF SOLO inviare e ricevere mail

//traffico SMTP (porta 25) dai prof al server mail (invio mail)

iptables –t filter –A FORWARD –i eth0 –o eth3 –s $PROF –sport 1024:65535 –d 10.0.3.10/24 –p tcp –dport 25 –j ACCEPT

// traffico IMAP (porta 143) dai prof al server mail e viceversa (ricezione email)

iptables –t filter –A FORWARD –i eth0 –o eth3 –s $PROF –sport 1024:65535 –d 10.0.3.10/24 -p tcp –dport 143 –j ACCEPT

iptables –t filter –A FORWARD –i eth3 –o eth0 –s 10.0.3.10/24 –p tcp –sport 143 –d $PROF --dport 1024:65535 –m state –state established, related –j ACCEPT

#STUD navigare in Internet SOLO http (porta 443)

iptables –t filter –A FORWARD –i eth1 –o eth2 –s $STUD –p tcp –sport 1024:65535 –d $EXT --dport 443 –j ACCEPT

iptables –t filter –A FORWARD –i eth2 –o eth1 –s $EXT –p tcp –sport 443 –d $STUD --dport 1024:65535 –m state –state ESTABLISHED –j ACCEPT

#PROF e STUD no comunicazione

iptables –t filter –A FORWARD –i eth0 –o eth1 –s $PROF –p tcp –sport 1024:65535 -d $STUD –dport 1024:65535 –j DROP

iptables –t filter –A FORWARD –i eth1 –o eth0 –s $STUD –p tco –sport 1024:65535 -d $PROF –dport 1024:65535 –J DROP

#PC3 TELNET (porta 23) alla DMZ

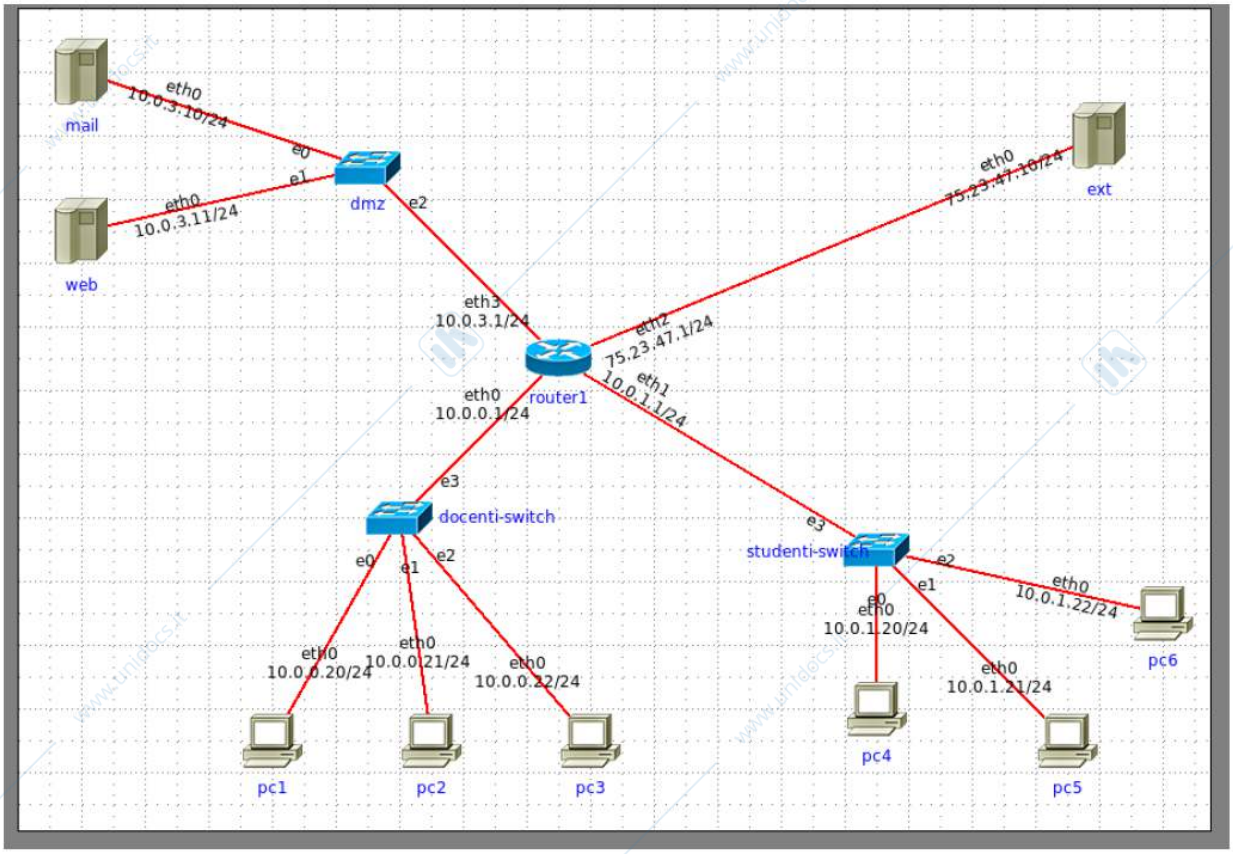
iptables –t filter –A FORWARD –i eth0 –o eth3 –s 10.0.0.22/24 –p tcp –sport 1024:65535 -d $SERVER –dport 23 –j ACCEPT

iptables –t filter –A FORWARD –i eth3 –o eth0 –s $SERVER –p tcp –sport 23 –d 10.0.0.22/24 --dport 1024:65535 –m state –state ESTABLISHED, RELATED –j ACCEPT

#DEFAULT DENY

iptables –t filter –A FORWARD –J DROP

Le regole iptables in generale van bene. Suggerimento: puoi scriverle in modo più compatto facendo un unica regola per traffico "estrablished+related" come discusso qui.



Abbiamo:

- - **Server web e ftp** per servizi universitari interni (portale studenti su 8080 e ftp docenti) ed esterni (solo sito web)

-

1. Scrivere le regole di firewalling (iptables) per garantire le seguenti situazioni:
    a. - **Solo** la rete dei professori può accedere al server FTP (solo modalità passiva)
    b. - I professori *possono* navigare su internet ma *non possono* accedere al portale studenti
    c. - La rete degli studenti può **SOLO** accedere al portale studenti
    d. - Solo il PC1 è in grado di connettersi al server interno in ssh
    e. Dall'esterno (ext) si può contattare solo il server web sulla porta HTTP o HTTPS
    f. - I professori possono usare i principali di posta elettronica collegandosi **solo** al server con indirizzo IP 159.149.70.53

Il restante traffico deve essere vietato.

```
PROF="10.0.0.0/24"
STUD="10.0.1.0/24"
SERVER="10.0.3.0/24"
EXT="!PROF, !STUD, !SERVER"
```

a) *iptables -t filter -A FORWARD -i eth0 -o eth3 -s $PROF --sport 1024:65535 -d 10.0.3.11/24 --dport 21 -p tcp -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT*

iptables -t filter -A FORWARD -i eth3 -o eth0 -s 10.0.3.11/24 --sport 21 -d $PROF --dport 1024:65535 -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -t filter -A FORWARD -i eth0 -o eth3 -s $PROF --sport 1024:65535 -d 10.0.3.11/24 --dport 1024:65535 -p tcp -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

iptables -t filter -A FORWARD -i eth3 -o eth0 -s 10.0.3.11/24 --sport 1024:65535 -d $PROF --dport 1024:65535 -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

#PROF accedere ad Internet, ma NON al portale studenti

> iptables –t filter –A FORWARD –i eth0 –o eth2 –s $PROF –sport 1024:65535 –d $EXT –p tcp –dport 80, 443 –j ACCEPT

> iptables –t filter –A FORWARD –i eht2 –o eth0 –s $EXT –p tcp –sport 80,443 –d $PROF --dport 1024:65535 –m state –state established –j ACCEPT

- Ok (vedi commenti sopra per evitare ridondanza)

> iptables –t filter –A FORWARD –i eth 0 –o eth3 –s $PROF –sport 1024:65535 –d 10.0.3.11/24 –p tcp –dport 8080 -j DROP

> iptables –t filter –A FORWARD –i eth 3 –o eth0 –s 10.0.3.11/24 –p tcp –sport 8080 –d $PROF --dport 1024:65535 –m state –state established, related –j DROP

- Queste sono ridondanti poichè "drop" è già il default.

#PROF posta elettronica solo con ip 159.149.70.53

//traffico SMTP (porta 25) dai prof al server mail (invio mail)

> iptables –t filter –A FORWARD –i eth0 –o eth3 –s $PROF –sport 1024:65535 –d 10.0.3.10/24 –p tcp –dport 25 –j ACCEPT

// traffico IMAP (porta 143) dai prof al server mail e viceversa (ricezione email)

> iptables –t filter –A FORWARD –i eth0 –o eth3 –s $PROF –sport 1024:65535 –d 10.0.3.10/24 -p tcp –dport 143 –j ACCEPT

> iptables –t filter –A FORWARD –i eth3 –o eth0 –s 10.0.3.10/24 –p tcp –sport 143 –d $PROF --dport 1024:65535 –m state –state established, related –j ACCEPT

- Qui hai fatto riferimento al server email segnato nella rete interna. A mio parere c'è un errore nel testo: il server mail è in realtà il server ftp. Queste regole dovresti invece scriverle per un ipotetico server si posta esterno con ip 159.149.70.53.

#STUD solo portale studenti

> iptables –t filter –A FORWARD –i eth1 –o eth3 –s $STUD –sport 1024:65535 –d 10.0.3.11/24 –p tcp –-dport 8080 -j ACCEPT

> iptables –t filter –A FORWARD –i eth3 –o eth1 –s 10.0.3.11/24 –p tcp –sport 8080 –d $STUD --dport 1024:65535 -m state –state established, related –j ACCEPT

- Ok (vedi commento sopra per evitare ridondanza).

#PC1 connette al server interno con SSH (porta 22)

> iptables –t filter –A FORWARD –i eth0 –o eth3 –s 10.0.0.20/24 –sport 1024:65535 -d 10.0.3.11/24 –p tcp –dport 22 –j ACCEPT

> iptables –t filter –A FORWARD –i eth3 –o eth0 –s 10.0.3.11/24 –sport 22 –d 10.0.0.20/24 -p tcp –dport 1024:65535 –m state –state established, related –j ACCEPT

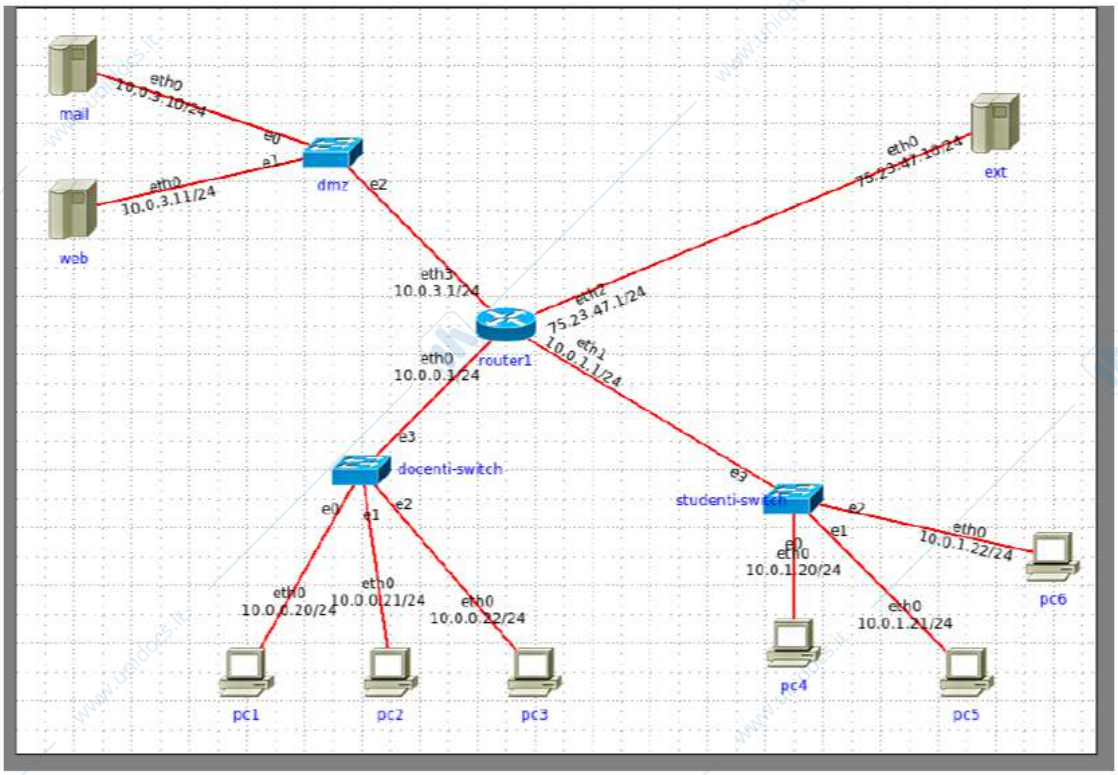
- Ok (vedi commento sopra per evitare ridondanza).

#EXT solo server web con http o https

> iptables –t filter –A FORWARD –i eth2 –o eth3 –s $EXT –d 10.0.3.11/24 –p tcp –dport 80,443 -j ACCEPT

> iptables –t filter –A FORWARD –i eth3 –o eth2 –s 10.0.3.11/24 –p tcp –sport 80,443 –d $EXT --dport 1024:65535 –m state –state established –j ACCEPT

- Ok (vedi commento sopra per evitare ridondanza).



Abbiamo:

- Router per la connettività internet

-DMZ con **Server web e ftp**

-Il portale interno studenti è attivo su porta 8080

- il sito web pubblico è attivo solo su https

- Rete studenti

- Rete docenti

1. Scrivere le regole di firewalling (iptables) per garantire le seguenti situazioni:
   a. Solo le reti dei professori e degli studenti possono accedere al server FTP (solo modalità passiva)
   b. il portale interno è accessibile solo dalla rete studenti
   c. il sito web pubblico è accessibile ovunque solo con https

---

   d. Professori e studenti possono navigare su internet
   e. Solo la rete professori può utilizzare i protocolli di posta.
   f. Solo pc1 può connettersi in ssh ai server su dmz
   g. Dall'esterno (ext) si può contattare solo il server web sulla porta HTTPS

Il restante traffico deve essere vietato.

#Assegno singoli indirizzi o sottoreti a costanti. Sono indicate correttamente?

DOC="10.0.0.0/24"
STUD="10.0.1.0/24"
FTP="10.0.1.10"
WEB="10.0.3.11"
SERV="10.0.3.0/24"
EXT="!DOC,!STUD,!SERV"

1. Scrivere le regole di firewalling (iptables) per garantire le seguenti situazioni:
   1. Solo le reti dei professori e degli studenti possono accedere al server FTP (solo modalità passiva)

      #controllo della connessione FTP

      iptables -A FORWARD -p tcp -i eth0,eth1 -o eth3 -s $DOC,$STUD -d $FTP --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT
      iptables -A FORWARD -p tcp -i eth3 -o eth0,eth1 -s $FTP --sport 21 -d $DOC,$STUD -m state --state ESTABLISHED -j ACCEPT

      #FTP PASSIVO

      iptables -A FORWARD -p tcp -i eth0,eth1 -o eth3 -s $DOC,$STUD --sport 1024: -d $FTP --dport 1024: -m state --state ESTABLISHED -j ACCEPT
      iptables -A FORWARD -p tcp -i eth3 -o eth0,eth1 -s $FTP --sport 1024: -d $DOC,$STUD --dport 1024: -m state --state RELATED,ESTABLISHED -j ACCEPT

   2. il portale interno è accessibile solo dalla rete studenti

      iptables -A FORWARD -p tcp -i eth1 -o eth3 -s $STUD -d $WEB--dport 8080 -m state --state NEW,ESTABLISHED -j ACCEPT
      iptables -A FORWARD -p tcp -i eth3 -o eth1 -s $WEB --sport 8080 -d $STUD -m state --state RELATED,ESTABLISHED -j ACCEPT

   3. il sito web pubblico è accessibile ovunque solo con https

      iptables -A FORWARD -p tcp -o eth3 -d $WEB--dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
      iptables -A FORWARD -p tcp -i eth3 -s $WEB --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT

   4. Professori e studenti possono navigare su internet

      iptables -A FORWARD -p tcp -i eth0,eth1 -o eth2 -s $DOC,$STUD -d $EXT --dport 80,443 -m state --state NEW,ESTABLISHED -j ACCEPT
      iptables -A FORWARD -p tcp -i eth2 -o eth0,eth1 -s $EXT --sport 80,443 -d $DOC,$STUD -m state --state RELATED,ESTABLISHED -j ACCEPT

   5. Solo la rete professori può utilizzare i protocolli di posta. (*RISPOSTA INCERTA)*

      **
      #ho supposto che il server mail non fosse nella DMZ, ma esterno alla rete (in EXT). Le mie principali perplessità sono relative a come ho specificato le porte le quali includono SMTP, IMAP, POP3 anche in versione sicura e se vada specificato uno stato (-m state). Dato che i tre protocolli citati hanno funzioni diverse (SMTP per posta in uscita e IMAP e POP3 per posta in entrata) non sono sicuro circa la possibilità di raggrupare i tre protocolli in sole due regole con relativi stati e se --sport e--dport siano corretti.
      **
      Quale è un metodo efficace per definire regole iptables per i principali protocolli di posta?

      iptables -A FORWARD -p tcp -i eth0 -o eth2 -s $DOC -d $EXT --dport 25,446,110,995,143,993 -j ACCEPT
      iptables -A FORWARD -p tcp -i eth2 -o eth0 -s $EXT --sport 25,446,110,995,143,993 -d $DOC -j ACCEPT

   6. Solo pc1 può connettersi in ssh ai server su dmz

      iptables -A FORWARD -p tcp -i eth0 -o eth3 -s 10.0.0.20 -d $SERV --dport 22 -m state --state NEW, ESTABLISHED -j ACCEPT
      iptables -A FORWARD -p tcp -i eth3 -o eth0 -s $SERV --sport 22 -d 10.0.0.20 -m state --state RELATED,ESTABLISHED -j ACCEPT

   7. Dall'esterno (ext) si può contattare solo il server web sulla porta HTTPS

      #Queste due regoli sono ridondanti perché credo siano incluse nella regola numero 3. Corretto?

      iptables -A FORWARD -p tcp -i eth2 -o eth3 -s $EXT -d $WEB --dport 443 -m state --state NEW, ESTABLISHED -j ACCEPT
      iptables -A FORWARD -p tcp -i eth3 -o eth2 -s $WEB --sport 443 -d $EXT -m state --state RELATED,ESTABLISHED -j ACCEPT

Il restante traffico deve essere vietato.

iptables -A FORWARD -j DROP
iptables -A INPUT -j DROP
iptbles - A OUTPUT -j DROP

In alternativa il traffico restante potrebbe essere vietato con delle regole di default:

iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP

Altra domanda:
In qualche regola qui sopra ho omesso --sport o --dport quando queste venivano scelte casualmente per identificare la connessione (funzione tipica di una porta sorgente che inzia una connessione).
Mi chiedevo: è sempre meglio specificare in sede d'esame i generici --sport 1024: o --dport 1024: per porte casuali oltre la 1024?

Ringrazio chiunque potrà dedicare del tempo ai miei quesiti

Ciao

Re: Esercizio su firewall (iptables) - appello 12 gennaio 2018
di matteo camilli - Friday, 8 February 2019, 19:32

Come scritto sotto puoi fare delle assunzioni, ad esempio IMAP + SMTP.

Porte usate:
- IMAP porta 143
- SMTP porta 25

Quindi lascerei passare verso ext connessioni verso le porte 143 e 25 + connessioni da ext dalla porta 143.

Permalink | Visualizza intervento genitore | Rispondi

Re: Esercizio su firewall (iptables) - appello 12 gennaio 2018
di matteo camilli - Friday, 8 February 2019, 19:08

DMZ con Server web e ftp (*e non Mail come indicato nell'immagine?*)

- direi che c'è un errore nel testo: nella figura il server è FTP (non Mail)

#Assegno singoli indirizzi o sottoreti a costanti. Sono indicate correttamente?

- EXT="!$DOC,!$STUD,!$SERV", per il resto è ok

Risposte 1, 2, 3, 4

- In generale le regole che hai scritto per il traffico NEW van bene. Io però farei invece un unica regola generale per il traffico RELATED e ESTABLISHED per evitare regole ridondanti (vedi discussione qui).

Risposta 5

- Direi che è corretto considerare il server di posta come esterno. Se non specificato puoi fare delle assunzioni sui protocolli usati, l'importante è far capire che sai come funziona il meccanismo. Ad esempio qui potresti assumere che i protocolli usati siano IMAP e SMTP, dopodiché aggiungere le relative regole.

Risposte 6, 7

- Vale lo stesso commento dato per le risposte 1, 2, 3, 4

In alternativa il traffico restante potrebbe essere vietato con delle regole di default

- Bene usando queste regole di default.

Mi chiedevo: è sempre meglio specificare in sede d'esame i generici --sport 1024: o --dport 1024: per porte casuali oltre la 1024?

- Si, va bene come hai fatto qui.

Permalink | Visualizza intervento genitore | Rispondi