Subject: Aiuto per configurazione iptables
Posted by Michele Barbato on Sun, 24 Jul 2011 07:30:17 GMT
View Forum Message <> Reply to Message

Server ubuntu con doppia scheda di rete. Tale server ha IP 192.168.1.115
verso il router e 192.168.0.2 verso la LAN.

Devo impostare un portforward su iptable in modo che tutto il traffico che
entra nella porta 9001 lato router vada a finire sempre nella porta 9001 di
una telecamera ip che sta nella lan ed ha indirizzo 192.168.0.7.

Chiedo cortesemente aiuto per la corretta definizione del comando iptables.

Grazie.
Mik

Subject: Re: Aiuto per configurazione iptables
Posted by Alessandro Selli on Sun, 24 Jul 2011 08:48:43 GMT
View Forum Message <> Reply to Message

Michele Barbato ha scritto:
> Server ubuntu con doppia scheda di rete. Tale server ha IP 192.168.1.115
> verso il router e 192.168.0.2 verso la LAN.
>
> Devo impostare un portforward su iptable in modo che tutto il traffico che
> entra nella porta 9001 lato router vada a finire sempre nella porta 9001 di
> una telecamera ip che sta nella lan ed ha indirizzo 192.168.0.7.
>
> Chiedo cortesemente aiuto per la corretta definizione del comando iptables.

  Nella supposizione che l'interfaccia che collega il server con il
router sia eth0 e che il protocollo usato dalla porta 9001 sia TCP, si
puÃ² fare cosÃ¬ (una volta attivato il forwarding):

iptables -t nat -I PREROUTING -p tcp -i eth0 --dport 9001 -j DNAT \
--to-destination 192.168.0.7

  Un controllo sullo stato della connessione sarebbe un'aggiunta
opzionale ma intelligente:

-m state --state NEW,RELATED,ESTABLISHED

  Ciao,

--

Alessandro Selli http://alessandro.route-add.net
AVVERTENZA: i messaggi inviati a "trappola" non mi arriveranno.
WARNING: messages sent to "trappola" will never reach me.

Subject: Re: Aiuto per configurazione iptables
Posted by Michele Barbato on Sun, 24 Jul 2011 09:18:36 GMT
View Forum Message <> Reply to Message

"Alessandro Selli" <trappola@route-add.net> ha scritto nel messaggio
news:9924jdFnnlU1@mid.individual.net...
[...]

Ti ringrazio per la risposta. Devo scusarmi perchè nell'inviare il post ho
omesso alcune informazioni fondamentali.

La configurazione è la seguente:

[Router Alice 192.168.1.1] ------ [eth1
192.168.1.115]--[squid]--[danguardian]--[eth0 192.168.0.2]----------[LAN]

Esiste già una configurazione iptables che avevo impostato tempo addietro:

iptables -t nat -A OUTPUT -p tcp -m owner ! --uid-owner proxy --dport 80 -j
REDIRECT --to-port 8080
sysctl -w net.ipv4.ip_forward=1
iptables -t nat -I POSTROUTING -j MASQUERADE
iptables -F FORWARD
iptables -P FORWARD ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -j REJECT
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j
REDIRECT --to-port 8080

Grazie di nuovo per l'aiuto.

Mik

Subject: Re: Aiuto per configurazione iptables
Posted by Alessandro Selli on Sun, 24 Jul 2011 13:04:24 GMT
View Forum Message <> Reply to Message

Michele Barbato ha scritto:

> Grazie di nuovo per l'aiuto.

Inserisci la regola di PREROUTING.

Ciao,

--
Alessandro Selli http://alessandro.route-add.net
AVVERTENZA: i messaggi inviati a "trappola" non mi arriveranno.
WARNING: messages sent to "trappola" will never reach me.

Subject: Re: Aiuto per configurazione iptables
Posted by Michele Barbato on Sun, 24 Jul 2011 13:51:32 GMT
View Forum Message <> Reply to Message

"Alessandro Selli" <trappola@route-add.net> ha scritto nel messaggio
news:992jioF9b8U1@mid.individual.net...
> Michele Barbato ha scritto:
>
>> Grazie di nuovo per l'aiuto.
>
> Inserisci la regola di PREROUTING.
>

Ho sostituito eth0 con eth1:

sudo iptables -t nat -I PREROUTING -p tcp -i eth0 --dport 9001 -j
NAT --to-destination 192.168.0.7

ma non ho risultati apprezzabili, nel senso che quando da fuori entro in
http://pincopallo.dyndns.org:9001 non avviene nessun forward verso la porta
9001 di 192.168.0.7.
Una domanda, la dicitura --dport 9001 indica sia la porta FROM che la porta
TO ?

Ciao.
Mik

Subject: Re: Aiuto per configurazione iptables
Posted by Alessandro Selli on Sun, 24 Jul 2011 13:55:06 GMT
View Forum Message <> Reply to Message

Michele Barbato ha scritto:
> "Alessandro Selli" <trappola@route-add.net> ha scritto nel messaggio

> news:992jioF9b8U1@mid.individual.net...
>> Michele Barbato ha scritto:
>>
>>> Grazie di nuovo per l'aiuto.
>>
>> Inserisci la regola di PREROUTING.
>>
>
> Ho sostituito eth0 con eth1:
>
> sudo iptables -t nat -I PREROUTING -p tcp -i eth0 --dport 9001 -j
> NAT --to-destination 192.168.0.7
>
>
> ma non ho risultati apprezzabili, nel senso che quando da fuori entro in
> http://pincopallo.dyndns.org:9001 non avviene nessun forward verso la porta
> 9001 di 192.168.0.7.

  Sicuro? Il contatore della regola rimane a zero?

> Una domanda, la dicitura --dport 9001 indica sia la porta FROM che la porta
> TO ?

Da man iptables(8):

 [!] --destination-port,--dport port[:port]
  Destination port or port range specification. The
  flag --dport is a convenient alias for this option.

  Ciao,

--
Alessandro Selli http://alessandro.route-add.net
AVVERTENZA: i messaggi inviati a "trappola" non mi arriveranno.
WARNING: messages sent to "trappola" will never reach me.

Subject: Re: Aiuto per configurazione iptables
Posted by Michele Barbato on Sun, 24 Jul 2011 14:17:37 GMT
View Forum Message <> Reply to Message

>> ma non ho risultati apprezzabili, nel senso che quando da fuori entro in
>> http://pincopallo.dyndns.org:9001 non avviene nessun forward verso la
>> porta
>> 9001 di 192.168.0.7.
>

> Sicuro? Il contatore della regola rimane a zero?
>

Ecco, questa sarebbe una verifica utile. Come si fa a vedere il contatore
della regola ?

Grazie.
Mik

Subject: Re: Aiuto per configurazione iptables
Posted by Alessandro Selli on Sun, 24 Jul 2011 14:35:45 GMT
View Forum Message <> Reply to Message

Michele Barbato ha scritto:
>>> ma non ho risultati apprezzabili, nel senso che quando da fuori entro in
>>> http://pincopallo.dyndns.org:9001 non avviene nessun forward verso la
>>> porta
>>> 9001 di 192.168.0.7.
>>
>> Sicuro? Il contatore della regola rimane a zero?
>>
>
> Ecco, questa sarebbe una verifica utile. Come si fa a vedere il contatore
> della regola ?

Da man iptables(8):

-v, --verbose
Verbose output. This option makes the list command
show the interface name, the rule options (if any),
and the TOS masks. The packet and byte counters are
also listed, with the suffix 'K', 'M' or 'G' for
1000, 1,000,000 and 1,000,000,000 multipliers
respectively (but see the -x flag to change this).

Ciao,

--
Alessandro Selli http://alessandro.route-add.net
AVVERTENZA: i messaggi inviati a "trappola" non mi arriveranno.
WARNING: messages sent to "trappola" will never reach me.

Subject: Re: Aiuto per configurazione iptables

Posted by Michele Barbato on Sun, 24 Jul 2011 15:27:14 GMT
View Forum Message <> Reply to Message

Non sono sicuro di aver capito che comando devo dare, comunque questo è
l'output di un iptables per visualizzare la configurazione:

```
 mauro@stefano-desktop:/home/stefano/public_html/lust/main/ch art2$ sudo
iptables -L -v -n
Chain INPUT (policy ACCEPT 213M packets, 289G bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain FORWARD (policy ACCEPT 20620 packets, 2454K bytes)
 pkts bytes target     prot opt in     out     source
destination
57343   23M ACCEPT     all  --  *      *       0.0.0.0/0
0.0.0.0/0           state RELATED,ESTABLISHED
    7   336 REJECT     all  --  eth1   eth0    0.0.0.0/0
0.0.0.0/0           reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT 2498K packets, 1605M bytes)
 pkts bytes target     prot opt in     out     source
destination
```

Subject: Re: Aiuto per configurazione iptables
Posted by Alessandro Selli on Sun, 24 Jul 2011 17:54:36 GMT
View Forum Message <> Reply to Message

Michele Barbato ha scritto:
> Non sono sicuro di aver capito che comando devo dare, comunque questo Ã¨
> l'output di un iptables per visualizzare la configurazione:
>
> mauro@stefano-desktop:/home/stefano/public_html/lust/main/ch art2$ sudo
> iptables -L -v -n

La regola si deve aggiungere nella catena PREROUTING, quindi nella
tabella nat. Tu stai guardando nella tabella di default, che Ã¨ la
filter, non la nat.

Ciao,

--
Alessandro Selli http://alessandro.route-add.net
AVVERTENZA: i messaggi inviati a "trappola" non mi arriveranno.
WARNING: messages sent to "trappola" will never reach me.

Subject: Re: Aiuto per configurazione iptables
Posted by Michele Barbato on Sun, 24 Jul 2011 19:58:56 GMT
View Forum Message <> Reply to Message

Ok, questo dovrebbe andare.

```
 mauro@stefano-desktop:/home/stefano/public_html/lust/main/ch art2$ sudo
iptables -L -v -t nat
Chain PREROUTING (policy ACCEPT 29883 packets, 4200K bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 DNAT       tcp  --  eth0   any     anywhere             anywhere
tcp dpt:9001 to:192.168.0.7
   15   720 DNAT       tcp  --  eth1   any     anywhere             anywhere
tcp dpt:9001 state NEW,RELATED,ESTABLISHED to:192.168.0.7
    0     0 DNAT       tcp  --  eth1   any     anywhere             anywhere
tcp dpt:9001 to:192.168.0.7:9001
    0     0 DNAT       tcp  --  eth1   any     anywhere             anywhere
tcp dpt:9001 to:192.168.0.7
  725 34800 REDIRECT   tcp  --  eth0   any     anywhere             anywhere
tcp dpt:www redir ports 8080
    0     0 DNAT       tcp  --  eth1   any     anywhere             anywhere
tcp dpt:9001 to:192.168.0.7:9001

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
 354K   29M MASQUERADE  all  --  any    any     anywhere
anywhere

Chain OUTPUT (policy ACCEPT 334K packets, 26M bytes)
 pkts bytes target     prot opt in     out     source
destination
 1312 78720 REDIRECT   tcp  --  any    any     anywhere             anywhere
! owner UID match proxy tcp dpt:www redir ports 8080
```

Da quello che capisco:
- il contatore nella seconda riga che qui è a 15, quando tento di accedere dall'esterno alla porta 9001 viene incrementato quindi la regola parrebbe funzionare tuttavia non ho risposte dalla telecamera.
- le altre regole che si vedono nella stessa tabella, relative sempre all'indirizzo 192.168.0.7, sono alcune prove che ho fatto: prima ho cambiato l'interfaccia di rete e poi ho provato ad indicare la porta dopo l'IP. Potrebbero creare confusione ?

Thanks again.
Mik

Subject: Re: Aiuto per configurazione iptables
Posted by Alessandro Selli on Mon, 25 Jul 2011 17:47:13 GMT
View Forum Message <> Reply to Message

Michele Barbato ha scritto:
> Ok, questo dovrebbe andare.
>
> mauro@stefano-desktop:/home/stefano/public_html/lust/main/ch art2$ sudo
> iptables -L -v -t nat
> Chain PREROUTING (policy ACCEPT 29883 packets, 4200K bytes)
> pkts bytes target   prot opt in   out   source
> destination
>   0   0 DNAT   tcp -- eth0   any   anywhere   anywhere
> tcp dpt:9001 to:192.168.0.7
>   15   720 DNAT   tcp -- eth1   any   anywhere   anywhere
> tcp dpt:9001 state NEW,RELATED,ESTABLISHED to:192.168.0.7
>   0   0 DNAT   tcp -- eth1   any   anywhere   anywhere
> tcp dpt:9001 to:192.168.0.7:9001
>   0   0 DNAT   tcp -- eth1   any   anywhere   anywhere
> tcp dpt:9001 to:192.168.0.7
>   725 34800 REDIRECT   tcp -- eth0   any   anywhere   anywhere
> tcp dpt:www redir ports 8080
>   0   0 DNAT   tcp -- eth1   any   anywhere   anywhere
> tcp dpt:9001 to:192.168.0.7:9001
>
> Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
> pkts bytes target   prot opt in   out   source
> destination
> 354K   29M MASQUERADE all -- any   any   anywhere
> anywhere
>
> Chain OUTPUT (policy ACCEPT 334K packets, 26M bytes)
> pkts bytes target   prot opt in   out   source
> destination
> 1312 78720 REDIRECT   tcp -- any   any   anywhere   anywhere
> ! owner UID match proxy tcp dpt:www redir ports 8080
>
>
> Da quello che capisco:
> - il contatore nella seconda riga che qui Ã¨ a 15, quando tento di accedere
> dall'esterno alla porta 9001 viene incrementato quindi la regola parrebbe
> funzionare tuttavia non ho risposte dalla telecamera.

  Prova a sniffare i pacchetti di risposta, ossia i pacchetti in
ingresso sulla eth0 con porta di origine 9001.

> - le altre regole che si vedono nella stessa tabella, relative sempre
> all'indirizzo 192.168.0.7, sono alcune prove che ho fatto: prima ho cambiato
> l'interfaccia di rete e poi ho provato ad indicare la porta dopo l'IP.

> Potrebbero creare confusione ?

  Soltanto all'amministratore che legge le tabelle. :-)
Cancellale pure.

  Ciao,

--
Alessandro Selli http://alessandro.route-add.net
AVVERTENZA: i messaggi inviati a "trappola" non mi arriveranno.
WARNING: messages sent to "trappola" will never reach me.

Subject: Re: Aiuto per configurazione iptables
Posted by Michele Barbato on Mon, 25 Jul 2011 22:27:13 GMT
View Forum Message <> Reply to Message

>
> Prova a sniffare i pacchetti di risposta, ossia i pacchetti in
> ingresso sulla eth0 con porta di origine 9001.
>

Questo il tcpdump, ma niente.

mauro@stefano-desktop:/etc$ sudo tcpdump -i eth0 host 192.168.0.7 and port
9001 -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96
bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel

Ovviamente ho provato ad aprire la telecamera al 192.168.0.7:9001 da locale
e il tcpdump mi visualizza il finimondo di dati.

Secondo me c'è qualche errore nelle regole impostate in precedenza, che
ripeto:

iptables -t nat -A OUTPUT -p tcp -m owner ! --uid-owner proxy --dport 80 -j
REDIRECT --to-port 8080
sysctl -w net.ipv4.ip_forward=1
iptables -t nat -I POSTROUTING -j MASQUERADE
iptables -F FORWARD
iptables -P FORWARD ACCEPT

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -j REJECT
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j
REDIRECT --to-port 8080

alle quali va aggiunta quella che mi hai consigliato.

Ad esempio non capisco questa: iptables -A FORWARD -i eth1 -o eth0 -j REJECT
letta da ignorante parrebbe che tutto quello che entra in eth1 ed esce in
eth0 debba essere rejected.

Ciao.
Mik

Subject: Re: Aiuto per configurazione iptables
Posted by Michele Barbato on Tue, 26 Jul 2011 12:28:36 GMT
View Forum Message <> Reply to Message

> Secondo me c'è qualche errore nelle regole impostate in precedenza, che
> ripeto:
>
> iptables -t nat -A OUTPUT -p tcp -m owner ! --uid-owner proxy --dport
> 80 -j REDIRECT --to-port 8080
> sysctl -w net.ipv4.ip_forward=1
> iptables -t nat -I POSTROUTING -j MASQUERADE
> iptables -F FORWARD
> iptables -P FORWARD ACCEPT
> iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
> iptables -A FORWARD -i eth1 -o eth0 -j REJECT
> iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j
> REDIRECT --to-port 8080
>
> alle quali va aggiunta quella che mi hai consigliato.
>
> Ad esempio non capisco questa: iptables -A FORWARD -i eth1 -o eth0 -j
> REJECT
> letta da ignorante parrebbe che tutto quello che entra in eth1 ed esce in
> eth0 debba essere rejected.
>

Ho cancellato le regole di forward e reimpostato tutto come sopra ma SENZA
questa regola:

iptables -A FORWARD -i eth1 -o eth0 -j REJECT

Ora funziona, cioè il redirect verso la porta 9001 va ed accedo alla
telecamera dall'esterno.

Immagino però di aver rimosso un importante elemento di sicurezza che nella mia conoscenza caprina non riesco a ripristinare senza perdere la funzionalità della porta 9001.

Mik
