Subject: iptables
Posted by Francesco.d on Wed, 03 Aug 2011 20:30:19 GMT
View Forum Message <> Reply to Message

Voglio costruirmi un firewall che permetta a certi mac di accedere su
alcune porte (in particolare ssh) mentre il resto venga droppato. PerÃ²
non mi funziona nemmeno nella lan. Mi sapete dare qualche dritta ?
Magari un link a un tutorial semplice su iptables

```
#!/bin/bash

PORTE_TCP=8080,21,22,3690,5901

MACALLOW=/usr/share/iptables/conf/mac.allow.txt


iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT


while read indirizzo
do
 iptables -A INPUT -p tcp -m mac --mac-source $indirizzo --match
multiport --dports  $PORTE_TCP -m state --state NEW -j ACCEPT
   iptables -A INPUT -p tcp -m mac --mac-source $indirizzo --match
multiport --dports  $PORTE_TCP        -j ACCEPT

done < "$MACALLOW"


########################  Accetto tutto dal lopback
#####################################
iptables -A INPUT  -s 127.0.0.1  -j ACCEPT


############################### Il resto viene tutto bloccato
############################
iptables -A INPUT  -j DROP

############################### OUTPUT e FORWARD vengon accettati
############################
iptables -A OUTPUT -j ACCEPT
iptables -A FORWARD -j ACCEPT
```

Subject: Re: iptables
Posted by Alessandro Selli on Wed, 03 Aug 2011 21:48:19 GMT

Francesco.d ha scritto:
> Voglio costruirmi un firewall che permetta a certi mac di accedere su
> alcune porte (in particolare ssh) mentre il resto venga droppato. PerÃ²
> non mi funziona nemmeno nella lan. Mi sapete dare qualche dritta ?
> Magari un link a un tutorial semplice su iptables

Ãˆ frustrante analizzare una sfilza di regole di firewall se non si sa com'Ã¨ organizzata topologicamente la rete e chi deve essere bloccato dove sta e dove non deve andare. Insomma, il tuo firewall che cosa sta proteggendo? Se stesso? Tutta la rete? Sta facendo da router? Che cosa vuol dire che non funziona, non blocca chi dovrebbe bloccare o blocca chi non dovrebbe bloccare o altro?

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: iptables
Posted by daniele on Thu, 04 Aug 2011 18:03:21 GMT

"Francesco.d" <a.pagliari.1974@gmail.com> writes:

> Magari un link a un tutorial semplice su iptables

su oltrelinux.org hanno appena pubblicato un corposo tutorial sull'argomento.
--
Gli insulti hanno effetto solo dove e' presente l'emozione.
-- Spock, "Who Mourns for Adonais?" (TOS), data astrale 3468.1
