Subject: iptables AIUTOOO!!!!
Posted by Michele Barbato on Tue, 24 May 2011 16:29:27 GMT
View Forum Message <> Reply to Message

Ubuntu 10.10, doppia scheda di rete.

eth1 192.168.1.115 Ã¨ collegato il router adsl.

eth0 192.168.0.1 Ã¨ collegato un pc con indirizzo 192.168.0.12.

Devo fare in modo che il PC veda la rete esterna, in sostanza un forward
da eth0 a eth1 e viceversa. Volevo cominciare non con la porta 80 ma con
la 119, quella del news server.

Come configuro iptables ? SarÃ una banalitÃ ma Ã¨ tutto il giorno che ci
smadonno senza venirne a capo.

Grazie.
Mik

Subject: Re: iptables AIUTOOO!!!!
Posted by Alessandro Selli on Tue, 24 May 2011 19:43:57 GMT
View Forum Message <> Reply to Message

Michele Barbato ha scritto:
> Ubuntu 10.10, doppia scheda di rete.
>
> eth1 192.168.1.115 Ã¨ collegato il router adsl.
>
> eth0 192.168.0.1 Ã¨ collegato un pc con indirizzo 192.168.0.12.
>
> Devo fare in modo che il PC veda la rete esterna, in sostanza un forward
> da eth0 a eth1 e viceversa. Volevo cominciare non con la porta 80 ma con
> la 119, quella del news server.
>
> Come configuro iptables ? SarÃ una banalitÃ ma Ã¨ tutto il giorno che ci
> smadonno senza venirne a capo.

SNAT per tutti, per tutte le porte e protocolli:

iptables -t nat -A POSTROUTING --out-interface eth1 -j SNAT
--to-source 192.168.1.115

SNAT per il solo host 192.168.0.12, per tutte le porte e protocolli:

iptables -t nat -A POSTROUTING --source 192.168.0.12 -j SNAT
--to-source 192.168.1.115

E, ovviamente:

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

E, ovviamente, il PC deve avere il tuo router come suo default gateway.

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 AIUTOOO!!!!
Posted by THe_ZiPMaN on Tue, 24 May 2011 20:27:38 GMT
View Forum Message <> Reply to Message

On 05/24/2011 06:29 PM, Michele Barbato wrote:
> Ubuntu 10.10, doppia scheda di rete.
>
> eth1 192.168.1.115 Ã¨ collegato il router adsl.
>
> eth0 192.168.0.1 Ã¨ collegato un pc con indirizzo 192.168.0.12.
>
> Devo fare in modo che il PC veda la rete esterna, in sostanza un forward
> da eth0 a eth1 e viceversa.

Ma anche no. Non penso sia tua intenzione aprire comunicazioni
bidirezionali, almeno nel senso inteso oggigiorno con firewall stateful.
Potrebbe esserti utile a tal proposito leggere wikipedia.
http://en.wikipedia.org/wiki/Stateful_firewall
E se non capisci qualcosa a ritroso fino alle basi del networking.

> Volevo cominciare non con la porta 80 ma con
> la 119, quella del news server.

Una o l'altra Ã¨ indifferente.

> Come configuro iptables ? SarÃ una banalitÃ ma Ã¨ tutto il giorno che ci
> smadonno senza venirne a capo.

Non sarebbe stato male se avessi descritto i tuoi smadonnamenti; in tal
modo tutti avrebbero potuto capire cosa hai provato per darti
indicazioni mirate.

Al 99.99% hai scordato il nat o l'ip_forwarding.

La cosa piÃ¹ semplice per far quel che chiedi Ã¨:

sysctl -w net.ipv4.ip_forward=1
iptables -t nat -I POSTROUTING -j MASQUERADE
iptables -F FORWARD
iptables -P FORWARD DROP
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 119 -j ACCEPT

In ogni caso ti consiglio vivissimamente di installare shorewall e imparti quello. Scrivere le regole di iptables a mano senza sapere esattamente come funziona il firewall di Linux Ã¨ uno dei modi piÃ¹ rapidi per rendere insicura una rete.

--
Flavio Visentin

Scientists have finally discovered what's wrong with the female brain:
On the left side, there is nothing right, and on the right side, there
is nothing left.

Subject: Re: iptables AIUTOOO!!!!
Posted by Michele Barbato on Tue, 24 May 2011 21:31:04 GMT
View Forum Message <> Reply to Message

> La cosa piÃ¹ semplice per far quel che chiedi Ã¨:
>
> # sysctl -w net.ipv4.ip_forward=1
> # iptables -t nat -I POSTROUTING -j MASQUERADE
> # iptables -F FORWARD
> # iptables -P FORWARD DROP
> # iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
> # iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 119 -j ACCEPT
>

Niente da fare, non va.

Premetto che il pc Ã¨ un portatile con windows xp sul quale accedo al server news tramite outlook express, quando tento di accedere ai newsgroup compare all'istante il messaggio "Impossibile trovare il server". L'indirizzo lo prende in automatico dal dhcp che ho installato in ubuntu. Questo il dhcpd.conf

default-lease-time 600;
max-lease-time 7200;

option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option routers 192.168.0.2;
subnet 192.168.0.0 netmask 255.255.255.0 {
range 192.168.0.12 192.168.0.100;
option routers 192.168.0.2;
}

quindi il pc si ritrova con ip 192.168.0.12 e gateway 192.168.0.2 dal lato eth0. Non capisco perchÃ¨ non debba funzionare.

Metto anche il file interfaces, per scrupolo, casomai avessi scritto qualche cavolata anche qui.

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.0.2
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.255
dns-nameservers 192.168.1.1

auto eth1
iface eth1 inet static
address 192.168.1.115
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
dns-nameservers 192.168.1.1

Grazie per l'aiuto.
Mik

Subject: Re: iptables AIUTOOO!!!!
Posted by Michele Barbato on Tue, 24 May 2011 21:40:22 GMT
View Forum Message <> Reply to Message

>
> SNAT per tutti, per tutte le porte e protocolli:
>
> # iptables -t nat -A POSTROUTING --out-interface eth1 -j SNAT
> --to-source 192.168.1.115

>
> SNAT per il solo host 192.168.0.12, per tutte le porte e protocolli:
>
> # iptables -t nat -A POSTROUTING --source 192.168.0.12 -j SNAT
> --to-source 192.168.1.115
>
> E, ovviamente:
>
> # echo 1> /proc/sys/net/ipv4/ip_forward
>
> E, ovviamente, il PC deve avere il tuo router come suo default gateway.
>

Grazie per i consigli ma non riesco a farlo andare.
Come ho scritto a Flavio nell'altra risposta il pc Ã¨ un portatile con
xp. Prende l'IP in automatico dato che nel server ho installato dhcp,
come gateway ho messo l'indirizzo della scheda eth0 al quale Ã¨
collegato, cioÃ¨ 192.168.0.2 (nel post iniziale avevo scritto .1 in
realtÃ Ã¨ .2)

>
> Ciao,
>
>

Ciao.
Mik

Subject: Re: iptables AIUTOOO!!!!
Posted by THe_ZiPMaN on Tue, 24 May 2011 21:50:15 GMT
View Forum Message <> Reply to Message

On 05/24/2011 11:31 PM, Michele Barbato wrote:
>> La cosa piÃ¹ semplice per far quel che chiedi Ã¨:
>>
>> # sysctl -w net.ipv4.ip_forward=1
>> # iptables -t nat -I POSTROUTING -j MASQUERADE
>> # iptables -F FORWARD
>> # iptables -P FORWARD DROP
>> # iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
>> # iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 119 -j ACCEPT
>>
>
> Niente da fare, non va.

Quindi il tuo problema non Ã¨ iptables, perchÃ© se fosse solo quello il problema con le regole di cui sopra dovrebbe andare.

> Premetto che il pc Ã¨ un portatile con windows xp sul quale accedo al
> server news tramite outlook express, quando tento di accedere ai
> newsgroup compare all'istante il messaggio "Impossibile trovare il server".

Il che Ã¨ un chiaro segno di impossibilitÃ nel risolvere il nome.

> L'indirizzo lo prende in automatico dal dhcp che ho installato in
> ubuntu. Questo il dhcpd.conf
>
> default-lease-time 600;
> max-lease-time 7200;
> option subnet-mask 255.255.255.0;
> option broadcast-address 192.168.0.255;
> option routers 192.168.0.2;
> subnet 192.168.0.0 netmask 255.255.255.0 {
> range 192.168.0.12 192.168.0.100;
> option routers 192.168.0.2;
> }

E difatti abbiamo due option routers e nessuna opzione per i DNS.

> quindi il pc si ritrova con ip 192.168.0.12 e gateway 192.168.0.2 dal
> lato eth0. Non capisco perchÃ¨ non debba funzionare.

Se provi a fare telnet 193.43.96.1 119 vedrai che funziona.

Come immaginavo il problema Ã¨ ben differente da quello da te prospettato. Per iptables puoi fare queste semplici regole:

```
# 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
```

e vedrai che una volta aggiunti i DNS tutto funziona

--
Flavio Visentin

Scientists have finally discovered what's wrong with the female brain:
On the left side, there is nothing right, and on the right side, there
is nothing left.

Subject: Re: iptables AIUTOOO!!!!
Posted by Michele Barbato on Tue, 24 May 2011 22:14:52 GMT
View Forum Message <> Reply to Message

>
> e vedrai che una volta aggiunti i DNS tutto funziona
>

Grandioso !!! Funziona !!!
Sto scrivendo dal portatile con outlook express.

Una giornata persa ed era il DNS. Comunque ho dovuto scrivere il secondo
gruppo di regole perchè con il primo non andava, ho visto che hai
trasformato un iptables -P FORWARD DROP in iptables -P FORWARD ACCEPT, boh!
me lo studierò meglio domani mattina.

Grazie, grazie e grazie ancora.

Mik

Subject: Re: iptables AIUTOOO!!!!
Posted by THe_ZiPMaN on Tue, 24 May 2011 22:31:37 GMT
View Forum Message <> Reply to Message

> Grandioso !!! Funziona !!!
> Sto scrivendo dal portatile con outlook express.

Funziona e Outlook nella stessa frase sono un ossimoro.

> Una giornata persa ed era il DNS. Comunque ho dovuto scrivere il secondo
> gruppo di regole perchÃ¨ con il primo non andava,

Chiaramente. Tu avevi richiesto come configurare iptables per far
passare la porta 119 e io nella prima risposta ho risposto
pedissequamente al tuo quesito. Peccato che quello che tu avevi
richiesto non fosse quello che tu volevi.
Come minimo avresti dovuto aggiungere le porte 53 udp e tcp per il DNS e
probabilmente la 25 per l'SMTP; poi per usare il PC anche per altro
avresti dovuto aggiungere tutte le altre porte come la 21, 80, 443, 110,
995, 143, 993, ecc.ecc.

> ho visto che hai
> trasformato un iptables -P FORWARD DROP in iptables -P FORWARD ACCEPT, boh!

E' la politica di default da usare quando il pacchetto non matcha alcuna
regola. Nel primo caso droppi tutto quel che non era porta 119 tcp dalla
eth1 alla eth0 e ritorno. Nel secondo caso lasci passare tutto da tutte

le interfacce e blocchi con un REJECT (preferibile al DROP sulle reti fidate) il traffico che va dalla eth0 alla eth1 a meno che non sia traffico corrispondente a connessioni giÃ aperte in precedenza o in altre direzioni.

--
Flavio Visentin

Scientists have finally discovered what's wrong with the female brain:
On the left side, there is nothing right, and on the right side, there
is nothing left.

Subject: Re: iptables AIUTOOO!!!!
Posted by Michele Barbato on Wed, 25 May 2011 17:54:33 GMT
View Forum Message <> Reply to Message

Senti, visto che sei stato cosÃ¬ gentile ti smarrono per l'ultima volta.
Ho installato squid e dansguardian, ora vorrei aggiungere alla configurazione che mi hai mandato un redirect alla porta 8080 sia per il traffico sulla porta 80 proveniente da eth0 (LAN) che per quello proveniente dal server.
Mi rendo conto che mi mancano alcune basi del networking ma ho voluto lo stesso provarci. Alla tua configurazione:

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

ho aggiunto:

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT
--to-port 8080

ovviamente non funziona.

sigh ! Help !!!

Mik.

Subject: Re: iptables AIUTOOO!!!!
Posted by THe_ZiPMaN on Wed, 25 May 2011 19:07:11 GMT
View Forum Message <> Reply to Message

On 05/25/2011 07:54 PM, Michele Barbato wrote:
> ho aggiunto:
>
> iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT
> --to-port 8080
>
> ovviamente non funziona.

Ovviamente non funziona cosa significa? La regola di iptables Ã¨
corretta. Se la policy di default della catena INPUT Ã¨ ACCEPT (ed Ã¨ cosÃ¬
se non l'hai toccata) la redirezione dei pacchetti dovrebbe avvenire
correttamente. E' piÃ¹ probabile che non funzioni qualcosa nella
configurazione del tuo proxy.
Per esempio:
- ascolta su tutti gli IP o solo su 127.0.0.1?
- Ã¨ attivo il proxy?
- Ã¨ configurato per funzionare in modalitÃ trasparente?

Quando devi verificare qualcosa che non funziona, il "trucco" sta nel
sezionare il troubleshooting eliminando tutte le variabili possibili.
Nel tuo caso la cosa piÃ¹ intelligente Ã¨ iniziare a verificare se
iptables funziona correttamente. Per fare ciÃ² ferma i servizi di proxy
(sia squid che dansguardian), metti nc in ascolto sulla 8080 e poi prova
a fare telnet sulla porta 80 e vedi se ti risponde nc.

Quindi sul "firewall" dai un bel
nc -l 8080

e sul client un bel
telnet www.google.com 80

Scrivi qualcosa a caso, poi chiudi la comunicazione e verifichi se sul
terminale dove gira nc vedi qualcosa.

--
Flavio Visentin

Scientists have finally discovered what's wrong with the female brain:
On the left side, there is nothing right, and on the right side, there
is nothing left.

Subject: Re: iptables AIUTOOO!!!!
Posted by Michele Barbato on Wed, 25 May 2011 22:47:27 GMT
View Forum Message <> Reply to Message

>

> Ovviamente non funziona cosa significa?

Non so che dire, Ã¨ tutta stasera che ci smanetto e ora funziona. Ho messo il tutto in uno script per non sbagliare, mentre prima facevo il copia incolla delle righe ... avrÃ² sbagliato a riportare qualcosa !!!
Mi cospargo il capo di cenere ....