
Subject: Firewall?

Posted by [Ronin](#) on Sat, 02 Apr 2011 17:16:09 GMT

[View Forum Message](#) <> [Reply to Message](#)

Salve, dovendo proteggere da accessi esterni i miei computer domestici (quelli selvatici non mi piacciono), e avendo ragione di credere che ci sia almeno un hacker (all'estero) intenzionato a violarli (non sto qui a spiegare i perchÃ© e i percome di questa convinzione), cercavo un firewall che fosse abbastanza semplice da usare ed al contempo sufficientemente efficace, tipo ZoneAlarm.

Vorrei bloccare tutte le porte salvo quelle delle applicazioni che uso (email, browser, p2p ecc.) e che ad ogni nuovo tentativo di accesso in entrata o in uscita mi venga richiesto se lo autorizzo o meno.

Se ho capito bene, esistono dei sistemi che filtrano gli indirizzi IP, ma, se Ã¨ cosÃ¬, non vanno bene dato che attraverso gli anonymizer sono facilmente aggirabili (ci riesco perfino io che non sono un accher...)

Qualcuno ha qualche suggerimento da darmi?

Ripeto, semplice, magari draconiano, ma che quando blocca... BLOCCA :)

Grazie a tutti :)

C.

PS: chi volesse, puÃ² scrivermi in pvt

Subject: Re: Firewall?

Posted by [Zarathustra](#) on Sat, 02 Apr 2011 17:32:48 GMT

[View Forum Message](#) <> [Reply to Message](#)

On Sat, 02 Apr 2011 10:16:09 -0700, Ronin wrote:

> Salve, dovendo proteggere da accessi esterni i miei computer domestici
> (quelli selvatici non mi piacciono), e avendo ragione di credere che ci
> sia almeno un hacker (all'estero) intenzionato a violarli (non sto qui a
> spiegare i perchÃ© e i percome di questa convinzione), cercavo un
> firewall che fosse abbastanza semplice da usare ed al contempo
> sufficientemente efficace, tipo ZoneAlarm.

Ma hai dei pc con IP pubblico? Altrimenti Ã¨ piuttosto difficile (ma non impossibile) che l'attaccante possa violare un pc dietro un NAT.

Se poi hai ip pubblici, guardati come funziona shorewall, Ã¨ semplice, ma molto diverso da ZoneAlarm.

Subject: Re: Firewall?

Posted by [Manuel](#) on Sat, 02 Apr 2011 17:47:50 GMT

[View Forum Message](#) <> [Reply to Message](#)

On Apr 2, 7:16Â pm, Ronin <igoo...@dominomodels.com> wrote:

> Salve, dovendo proteggere da accessi esterni i miei computer domestici
> (quelli selvatici non mi piacciono), e avendo ragione di credere che
> ci sia almeno un hacker (all'estero) intenzionato a violarli (non sto
> qui a spiegare i perchÃ© e i percome di questa convinzione), cercavo un
> firewall che fosse abbastanza semplice da usare ed al contempo
> sufficientemente efficace, tipo ZoneAlarm.

Non ho capito una cosa: vuoi proteggere la tua rete domestica con un firewall perimetrale (cioÃ¨ una macchina che faccia solo il firewall o poco piÃ¹), oppure intendi proteggere ciascuna macchina con un personal firewall?

Si possono fare entrambe le cose, ma siccome per connettere piÃ¹ computer ad internet ti serve comunque un router, tanto vale fargli fare anche da firewall e non se ne parla piÃ¹. E' sicuramente piÃ¹ semplice ed efficiente che gestire N personal firewall ed un router "aperto". Se poi sei paranoico puoi fare entrambe le cose :-).

> Vorrei bloccare tutte le porte salvo quelle delle applicazioni che uso
> (email, browser, p2p ecc.) e che ad ogni nuovo tentativo di accesso in
> entrata o in uscita mi venga richiesto se lo autorizzo o meno.

E fin qui niente di strano.

> Se ho capito bene, esistono dei sistemi che filtrano gli indirizzi IP,
> ma, se Ã¨ cosÃ¬, non vanno bene dato che attraverso gli anonymizer sono
> facilmente aggirabili (ci riesco perfino io che non sono un accher...)

E ok...

> Qualcuno ha qualche suggerimento da darmi?

Bloccare completamente un indirizzo IP di solito Ã¨ inutile; ci sono sistemi per creare e gestire automaticamente delle blacklist a tempo (ad esempio istruendo il firewall a bloccare un dato IP per tot tempo se da esso arrivano troppi tentativi di connessione da un determinato IP)

> Ripeto, semplice, magari draconiano, ma che quando blocca... BLOCCA :)

Mah, bloccare bloccano tutti, dipende da come vengono configurati.

Personalmente, se hai dell'hardware anche vecchio a disposizione ti raccomando di crearti un firewall dedicato con una delle tante

distribuzioni dedicate; personalmente amo pfsense (anche se non Ã linux, ma bsd), ma come quella ce ne sono tante: ipcop, zeroshell, ... Cerca di avere le idee piÃ¹ chiare possibili su cosa vuoi lasciare aperto al mondo (ammesso e non concesso che tu abbia veramente necessitÃ di esporre _qualcosa_).

HTH,
Manuel

Subject: Re: Firewall?
Posted by [NicoKid](#) on Sat, 02 Apr 2011 21:49:03 GMT
[View Forum Message](#) <> [Reply to Message](#)

Ronin wrote:

> Vorrei bloccare tutte le porte salvo quelle delle applicazioni che uso
> (email, browser, p2p ecc.) e che ad ogni nuovo tentativo di accesso in
> entrata o in uscita mi venga richiesto se lo autorizzo o meno.
> Se ho capito bene, esistono dei sistemi che filtrano gli indirizzi IP,
> ma, se Ã cosÃ¬, non vanno bene dato che attraverso gli anonymizer sono
> facilmente aggirabili (ci riesco perfino io che non sono un accher...)
>
> Qualcuno ha qualche suggerimento da darmi?
> Ripeto, semplice, magari draconiano, ma che quando blocca... BLOCCA :)

Non sono un esperto di firewall, a parte un minimo uso di iptables. Ma dubito che ci sia in firewall per linux adatto ad un newbie. GiÃ se sai qualcosa lasci sempre qualche buco in giro, se poi non sai nulla ti tocca imparare per forza. Tutto IMHO naturalmente.

Nicola.

--

chi va pian va san e va lontan

Subject: Re: Firewall?
Posted by [Carlo MILIANO](#) on Sun, 03 Apr 2011 11:09:52 GMT
[View Forum Message](#) <> [Reply to Message](#)

On 2 Apr, 19:32, Lorenzo Mainardi <lorma...@gmail.com> wrote:

....
> Ma hai dei pc con IP pubblico? Altrimenti Ã piuttosto difficile (ma non
> impossibile) che l'attaccante possa violare un pc dietro un NAT.

Non credo, la mia Ã una rete domestica dietro un router dietro un

modem attaccato a una rete che presumo sia NATtata (ma non so bene cosa significhi quindi non ci metterei la mano sul tagliere...)

> Se poi hai ip pubblici, guardati come funziona shorewall, Ã" semplice, ma
> molto diverso da ZoneAlarm.

Grazie, lo guardo subito :)

Subject: Re: Firewall?

Posted by [Carlo MILIANO](#) on Sun, 03 Apr 2011 11:23:24 GMT

[View Forum Message](#) <> [Reply to Message](#)

On 2 Apr, 19:47, Manuel <manuel.rava...@gmail.com> wrote:

> Non ho capito una cosa: vuoi proteggere la tua rete domestica con un
> firewall perimetrale (cioÃ" una macchina che faccia solo il firewall o
> poco piÃ¹), oppure intendi proteggere ciascuna macchina con un personal
> firewall?

Ho un vecchio carcassone, che si presterebbe egregiamente, ma non ho voglia di avere un terzo computer costantemente acceso oltre allo sbattimento di installare, imparare e configurare una nuova distro, ho giÃ i miei grattacapi a tenere allineate (e domare quando si imbizzarriscono) due PC con Mint 10.

Per qualche strana ragione, nonostante io abbia un diploma in informatica, conseguito nel lontano '83, quando metto le mani su un PC e comincio a usarlo, quello dopo poco immancabilmente si incasina. A scuola i miei compagni prima di presentare un lavoro al prof, chiamavano me come "beta tester": se non riuscivo a incasinare io il programma (usandolo), vuol dire che erano in una botte di ferro. Quindi no distro dedicate altrimenti passo tutto il tempo a riconfigurare :)

> Si possono fare entrambe le cose, ma siccome per connettere piÃ¹
> computer ad internet ti serve comunque un router, tanto vale fargli
> fare anche da firewall e non se ne parla piÃ¹. E' sicuramente piÃ¹
> semplice ed efficiente che gestire N personal firewall ed un router
> "aperto". Se poi sei paranoico puoi fare entrambe le cose :-)

Sono paranoico ma non fino a quel punto :)

Ho un router CISCO che ha anche una funzionalitÃ firewall, il problema Ã che il router va configurato "ex-ante", cioÃ gli devo dire tutto in anticipo, invece programmi come ZoneAlarm funzionano anche "ex-post", cioÃ io lanciao un programma che accede a internet e il FW mi chiede cosa intendo fare: consentire l'accesso SI, NO ecc.

> > Ripeto, semplice, magari draconiano, ma che quando blocca... BLOCCA :)
>

- > Mah, bloccare bloccano tutti, dipende da come vengono configurati.
- >
- > Personalmente, se hai dell'hardware anche vecchio a disposizione ti
- > raccomando di crearti un firewall dedicato con una delle tante
- > distribuzioni dedicate; personalmente amo pfsense (anche se non Ã
- > linux, ma bsd), ma come quella ce ne sono tante: ipcop, zeroshell, ...

Vedi sopra... comunque approfondirÃ² l'argomento, male non puÃ² sicuramente farmi :)

- > Cerca di avere le idee piÃ¹ chiare possibili su cosa vuoi lasciare
- > aperto al mondo (ammesso e non concesso che tu abbia veramente
- > necessitÃ di esporre _qualcosa_).

Grazie dei suggerimenti.

Alcuni programmi agiscono come server (es P2P) e altri devono comunque accettare traffico in ingresso (ricezione di email, streaming video ecc.), vorrei che le uniche porte aperte fossero quelle necessarie ai programmi che utilizzo, ma che sia il FW ad attivarsi e chiedermi di volta in volta come voglio regolarmi

C.

Subject: Re: Firewall?

Posted by [Carlo MILIANO](#) on Sun, 03 Apr 2011 11:26:26 GMT

[View Forum Message](#) <> [Reply to Message](#)

On 2 Apr, 23:49, NicoKid <nic...@false.com> wrote:

- > Non sono un esperto di firewall, a parte un minimo uso di iptables. Ma
- > dubito che ci sia in firewall per linux adatto ad un newbie. GiÃ se sai
- > qualcosa lasci sempre qualche buco in giro, se poi non sai nulla ti tocca
- > imparare per forza. Tutto IMHO naturalmente.

Imparare va bene, dedicarci tutto il tempo a disposizione non va bene. Oltretutto ho notato che non sempre imparare Ã utile. Avevo imparato tutto su come fare certe cose con Ubuntu fino alla 8, poi con la 9 hanno cambiato tutto e sono dovuto ripartire da capo, e quello che avevo imparato prima era diventato inutile (filosofeggio). Quindi vorrei mantenermi al "minimo sindacale" :)

C.

Subject: Re: Firewall?

Posted by [Zarathustra](#) on Sun, 03 Apr 2011 12:23:48 GMT

[View Forum Message](#) <> [Reply to Message](#)

On Sun, 03 Apr 2011 04:09:52 -0700, Carlo MILIANO wrote:

> Non credo, la mia Ã una rete domestica dietro un router dietro un modem
> attaccato a una rete che presumo sia NATtata

Da come lo dici presumo anche io.
Che indirizzo ha il tuo pc?

> (ma non so bene cosa
> significhi quindi non ci metterei la mano sul tagliere...)

Se non hai le basi di networking, lascia perdere la configurazione del
firewall

Subject: Re: Firewall?

Posted by [Crononauta](#) on Sun, 03 Apr 2011 18:17:17 GMT

[View Forum Message](#) <> [Reply to Message](#)

On 03/04/11 13:09, Carlo MILIANO wrote:

> Non credo, la mia Ã una rete domestica dietro un router dietro un
> modem attaccato a una rete che presumo sia NATtata (ma non so bene
> cosa significhi quindi non ci metterei la mano sul tagliere...)

Quindi scusa, ma se non hai la minima base del networking, come fai a
stabilire di aver bisogno di un firewall, e soprattutto di un certo tipo
di firewall?

CiÃ che odio di quelle sciocchezze tipo ZoneAlarm, Ã che hanno diffuso
un'ignoranza paurosa nel campo del networking. I "personal firewall"
sono giocattoli inutili quando va bene, dannosi quando va male. Si
adattano ottimamente alla filosofia Windows, tutto chiuso da dentro a
fuori, tutto aperto da fuori a dentro; quel che Ã peggio, inducono un
falso senso di sicurezza, ma Ã giÃ dimostrato che virus, trojan et sim.
come prima cosa aggirano questi giocattoli.

L'inutilitÃ Ã concettuale, se la macchina Ã in frontiera deve potersi
difendere da sÃ, non esisterÃ un programma che la renderÃ sicura se Ã
intrinsecamente insicura. Un firewall non serve a difendere *la macchina
stessa*, serve a discriminare l'accesso ai servizi di rete.

Sulla macchina stessa, specie se Ã usata soltanto come workstation (e
quindi solo client) non ha molto senso, perchÃ se una porta Ã aperta Ã
perchÃ c'Ã un programma che la usa, e allora deve stare aperta.
Viceversa non esisterÃ, e quindi non ha senso "firewallare" una porta
che non c'Ã.

La questione a questo punto si sposta sul chi sta tenendo aperte certe
porte, e se non sai cosa sta girando sul tuo sistema, la prima cosa che

devi fare Ã" guardare *cosa sta girando*. Un semplice netstat -natp ti puÃ² dire giÃ" molte cose.

In sostanza prima di domandarti "come posso configurare il firewall" dovresti domandarti: "ho bisogno di un firewall?".

--

Massimo Bacilieri AKA Crononauta
Skype: crononauta <massimo.bacilieri@gmail.com>
Facebook: Massimo Bacilieri

Subject: Re: Firewall?

Posted by [Ronin](#) on Sun, 03 Apr 2011 19:04:56 GMT

[View Forum Message](#) <> [Reply to Message](#)

On 3 Apr, 20:17, Crononauta <massimo.bacili...@gmail.com> wrote:

> On 03/04/11 13:09, Carlo MILIANO wrote:

>

> > Non credo, la mia Ã" una rete domestica dietro un router dietro un
> > modem attaccato a una rete che presumo sia NATtata (ma non so bene
> > cosa significhi quindi non ci metterei la mano sul tagliere...)

>

> Quindi scusa, ma se non hai la minima base del networking, come fai a
> stabilire di aver bisogno di un firewall, e soprattutto di un certo tipo
> di firewall?

Non credo di non avere la minima idea del networking (se vuoi posso argomentare meglio), ma sicuramente sono fermo all'ABC e non ho la possibilitÃ di approfondire oltre un certo punto.

> CiÃ² che odio di quelle sciocchezze tipo ZoneAlarm, Ã" che hanno diffuso
> un'ignoranza paurosa nel campo del networking. I "personal firewall"
> sono giocattoli inutili quando va bene, dannosi quando va male. Si

Mah, io, quando ancora usavo Windows, dopo che ho installato ZA ho rilevato un numero imprecisato di accessi non richiesti che il buon ZA ha bloccato. Erano veramente *TANTI*, anche quando non avevo alcun programma che girava. Quindi magari non blocca i cattivissimi, ma i cattivelli li tiene a bada.

> adattano ottimamente alla filosofia Windows, tutto chiuso da dentro a
> fuori, tutto aperto da fuori a dentro; quel che Ã" peggio, inducono un
> falso senso di sicurezza, ma Ã" giÃ" dimostrato che virus, trojan et sim.
> come prima cosa aggirano questi giocattoli.

Non sono del tutto a digiuno dei fondamenti teorici, quindi so bene che, se uno proprio vuole e ha le risorse, puÃ² battere qualsiasi

firewall (Ã" scritto anche in una guida all'uso di ssh).

Per come la vedo io, il firewall Ã" un po' come la porta blindata di casa o l'antifurto della macchina: scoraggia i piÃ¹, ma se uno proprio vuole, entra lo stesso, a meno che non ci si attrezzi tipo Fort Knox. A me basta scoraggiare i piÃ¹, non ho la pretesa di rendere il mio sistema invulnerabile.

- > L'inutilitÃ Ã" concettuale, se la macchina Ã" in frontiera deve potersi
- > difendere da sÃ©, non esisterÃ un programma che la renderÃ sicura se Ã"
- > intrinsecamente insicura. Un firewall non serve a difendere *la macchina
- > stessa*, serve a discriminare l'accesso ai servizi di rete.
- > Sulla macchina stessa, specie se Ã" usata soltanto come workstation (e
- > quindi solo client) non ha molto senso, perchÃ© se una porta Ã" aperta Ã"
- > perchÃ© c'Ã" un programma che la usa, e allora deve stare aperta.
- > Viceversa non esisterÃ , e quindi non ha senso "firewallare" una porta
- > che non c'Ã".

Salvo errori (correggimi), un S.O. tiene comunque delle porte aperte per servizi di rete che magari non vengono mai usati. Dovrei quindi disabilitare questi servizi, ma richiede un livello di conoscenza del sistema che non ho e che, per formarmi, richiederebbe tempo che purtroppo - o per fortuna - voglio e devo dedicare ad altre cose. Quindi mi accontenterei di qualcosa intermedio, non credo di pretendere la luna....

- > La questione a questo punto si sposta sul chi sta tenendo aperte certe
- > porte, e se non sai cosa sta girando sul tuo sistema, la prima cosa che
- > devi fare Ã" guardare *cosa sta girando*. Un semplice netstat -natp ti
- > puÃ² dire giÃ molte cose.

Ho provato Firestarter (apt-get), e fornisce giÃ parecchie informazioni

- > In sostanza prima di domandarti "come posso configurare il firewall"
- > dovresti domandarti: "ho bisogno di un firewall?".

Andiamo ancora piÃ¹ a monte, allora, e rigiro a te la seguente questione, se sarai cosÃ¬ gentile da rispondermi :)

Ho un PC Linux che uso per molte attivitÃ , fra cui email (Thunderbird con diversi plugin), Skype (nativo, non wine), browsing (Chrome), P2P, macchine virtuali (mi serve *proprio* MS Office, ahimÃ", oltre ad usare il successore di mulve che non gira in wine e un programma di bulk downloading di immagini...), on-line banking, editing di documenti (OpenOffice), streaming (Rythmbox, youtube), mediaplayer (xbmc), editing di immagini (gimp, xsane, gthumb) e forse ancora qualcosina che al momento mi sfugge.

La domanda Ã": posso assicurarmi che, nei limiti del ragionevole (cioÃ" p.es. senza allestire un PC firewall dedicato e sistemi allodola), non

sia violato dall'esterno? E se sÃ¬, come?

Abbi pazienza, non tutti sono sysadmin/Valentino Rossi ma ciÃ² nonostante possono essere utenti/motociclisti e ogni tanto dover mettere le mani sul mezzo senza pretese di fare un fine-tuning... :)

C.

Subject: Re: Firewall?

Posted by [Enrico 'Henryx' Bianc](#) on Sun, 03 Apr 2011 20:59:15 GMT

[View Forum Message](#) <> [Reply to Message](#)

Ronin wrote:

> il buon ZA
> ha bloccato

Posto che "buono" e "Zone Alarm" nella stessa frase suona di controsenso, il problema e` che i personal firewall di windows sono piu` di semplici firewall

Enrico

Subject: Re: Firewall?

Posted by [Enrico 'Henryx' Bianc](#) on Sun, 03 Apr 2011 21:04:57 GMT

[View Forum Message](#) <> [Reply to Message](#)

Ronin wrote:

> La domanda Ã¨: posso assicurarmi che, nei limiti del ragionevole (cioÃ¨
> p.es. senza allestire un PC firewall dedicato e sistemi allodola), non
> sia violato dall'esterno?

Si

> E se sÃ¬, come?

Tenendo aggiornate le applicazioni, evitando di cliccare su qualsiasi link ti capiti sotto mano, controllando quali servizi siano in esecuzione che abbiano una porta TCP/UDP aperta verso l'esterno e capendo il perche` lo siano (e.g. usi KDE? Allora e` possibile che vi sia la porta 3306/TCP - MySQL - in ascolto verso tutti i pc che possano raggiungere la tua macchina)

Enrico

Subject: Re: Firewall?

Posted by [Crononauta](#) on Sun, 03 Apr 2011 23:30:08 GMT

[View Forum Message](#) <> [Reply to Message](#)

On 03/04/11 21:04, Ronin wrote:

> Mah, io, quando ancora usavo Windows, dopo che ho installato ZA ho
> rilevato un numero imprecisato di accessi non richiesti che il buon ZA
> ha bloccato. Erano veramente *TANTI*, anche quando non avevo alcun
> programma che girava. Quindi magari non blocca i cattivissimi, ma i
> cattivelli li tiene a bada.

"Accessi non richiesti" a *cosa* esattamente?

Se una macchina non ha alcun servizio in ascolto p.e. sulla porta 65000,
tu puoi tentare di accedere per mille anni ma non otterrai niente.

Certo, se davanti ci metti il "personal firewall" che ogni volta che
rileva uno scan si mette a bippare, l'unica cosa che ottieni Ã un
spreco enorme di cicli macchina per dare dei warning completamente inutili.

Viceversa, se su quella porta c'Ã un servizio, la domanda Ã:

- Ã aperta perchÃ offri un servizio? Se sÃ-, allora inutile bippare, deve
stare aperta, e sai anche perchÃ lo Ã; se no, allora perchÃ Ã aperta?
Chi la tiene aperta? Chiudere una porta che *non deve* esistere Ã come
nascondere la polvere sotto il tappeto.

> Per come la vedo io, il firewall Ã un po' come la porta blindata di
> casa o l'antifurto della macchina: scoraggia i piÃ¹, ma se uno proprio
> vuole, entra lo stesso, a meno che non ci si attrezzino tipo Fort Knox.

No, non Ã cosÃ-. Il firewall non Ã la serratura di casa.

Il firewall Ã il buttafuori che decide chi far passare (per dove) e chi
no. Tu metteresti una serratura dove non c'Ã una porta? No, perchÃ Ã
inutile.

> Salvo errori (correggimi), un S.O. tiene comunque delle porte aperte
> per servizi di rete che magari non vengono mai usati. Dovrei quindi
> disabilitare questi servizi, ma richiede un livello di conoscenza del
> sistema che non ho e che, per formarmi, richiederebbe tempo che
> purtroppo - o per fortuna - voglio e devo dedicare ad altre cose.

Allora Ã inutile parlare di mettere su un firewall che abbia un senso,
visto che se non sai cosa gira sulla macchina, su quali porte siano
aperte, e sul *perchÃ* sono aperte, ovviamente non puoi pensare di
proteggere tali porte in modo ragionevole.

E chiudere roba a capocchia aprendo porte a casaccio mano a mano che le
applicazioni vogliono uscire su internet, significa solo:

- a) perdere piÃ¹ tempo di quello che sarebbe occorso per studiare le cose
a modo;
- b) trovarsi le applicazioni che funzionano a intermittenza senza un

apparente perché;

c) non risolvere il problema sicurezza in modo esaustivo, visto che le porte aperte nuovamente non puoi sapere se sono vulnerabili o no.

> Quindi mi accontenterei di qualcosa intermedio, non credo di
> pretendere la luna....

Ti posso dire una cosa: se hai un router ADSL, spendi 10 minuti per capire come configurarlo in NAT anziché in bridge (solitamente devi solo cambiare un'opzione nei menu web di configurazione) e poi vivi sereno, perché tanto il tuo PC non sarà esposto sulla tratta pubblica, e tutta la bega se la sbrogia il router.

> Ho un PC Linux che uso per molte attività, fra cui email (Thunderbird
> con diversi plugin), Skype (nativo, non wine), browsing (Chrome), P2P,
> macchine virtuali (mi serve proprio MS Office, ahimè, oltre ad usare
> il successore di mulve che non gira in wine e un programma di bulk
> downloading di immagini...), on-line banking, editing di documenti
> (OpenOffice), streaming (Rythmbox, youtube), mediaplayer (xbmc),
> editing di immagini (gimp, xsane, gthumb) e forse ancora qualcosina
> che al momento mi sfugge.
> La domanda è: posso assicurarmi che, nei limiti del ragionevole (cioè
> p.es. senza allestire un PC firewall dedicato e sistemi allodola), non
> sia violato dall'esterno? E se sì, come?

Queste sono solo applicazioni client da workstation, nessun servizio di rete. Perciò è perfettamente inutile applicare un firewall in quelle condizioni, visto che tutte le porte che verranno aperte saranno necessarie al funzionamento di quelle applicazioni. E dovranno restare aperte.

Purtroppo per te la risposta è proprio quella che non volevi: devi guardare che servizi hai attivi e configurare quelli.
Poi un bel netstat -natp ti dirà quali porte sono aperte e quale programma le tiene aperte.

Guardi quelle che sono in listening su 0.0.0.0 o sull'interfaccia pubblica, e valuterai eventualmente di bloccare quelle.

Così a naso avrai la 22 dell'sshd, la 25 dell'smtp, la 901 dello swat, la 137 e 139 se hai samba, la 631 se hai cups, e qualcos'altro che dipende da cosa hai attivato.

Bloccati questi "well known services" attivi, hai già fatto il massimo che si può fare. Non sarebbe male neanche guardare un attimo a come funzionano questi servizi, in modo da configurarli a dovere (es. l'smtp lo puoi certamente configurare in modo che agganci SOLO 127.0.0.1, ovvero il loopback).

- > Abbi pazienza, non tutti sono sysadmin/Valentino Rossi ma ciÃ²
- > nonostante possono essere utenti/motociclisti e ogni tanto dover
- > mettere le mani sul mezzo senza pretese di fare un fine-tuning... :)

Ma metti in NAT il router e vivi sereno, dammi retta! Facendo cosÃ¬ ho da anni pure dei Windows dietro il router che non hanno problemi, con giusto un antivirus minimale (perchÃ© Windows Ã¨ sempre Windows).

--

Massimo Bacilieri AKA Crononauta
Skype: crononauta <massimo.bacilieri@gmail.com>
Facebook: Massimo Bacilieri

Subject: Re: Firewall?
Posted by [Conraid](#) on Mon, 04 Apr 2011 08:30:19 GMT
[View Forum Message](#) <> [Reply to Message](#)

Carlo MILIANO wrote:

- > Imparare va bene, dedicarci tutto il tempo a disposizione non va bene.
- > Oltretutto ho notato che non sempre imparare Ã¨ utile. Avevo imparato
- > tutto su come fare certe cose con Ubuntu fino alla 8, poi con la 9
- > hanno cambiato tutto e sono dovuto ripartire da capo, e quello che
- > avevo imparato prima era diventato inutile (filosofeggio).

sempre filosofeggiando, questo Ã¨ successo perchÃ© avevi "imparato" la pratica, invece della teoria. I concetti rimangono, i comandi non sempre

--

:cf

Subject: Re: Firewall?
Posted by [Ronin](#) on Mon, 04 Apr 2011 08:40:22 GMT
[View Forum Message](#) <> [Reply to Message](#)

On 4 Apr, 01:30, Crononauta <massimo.bacili...@gmail.com> wrote:
> Ma metti in NAT il router e vivi sereno, dammi retta! Facendo cosÃ¬ ho da
> anni pure dei Windows dietro il router che non hanno problemi, con
> giusto un antivirus minimale (perchÃ© Windows Ã¨ sempre Windows).

Massimo, grazie dei consigli, mi varÃ² un giro su netstat che Ã¨ un comando che non conosco ma dal nome mi ispira :)
Vedendo (da un sito) come il mio PC si presenta all'esterno, ho

provato a fare un traceroute fino all'IP indicato dal sito, ma in effetti non va oltre il modem.

Il modem assegna a sÃ© stesso e al router un indirizzo 10.*.*, mentre la rete di casa Ã© su rete 192.168.0.* (e il router viene visto come 192.168.0.x), per cui desumo che sia giÃ in nat, o sbaglio?

Grazie

C.

Subject: Re: Firewall?

Posted by [Crononauta](#) on Mon, 04 Apr 2011 09:48:36 GMT

[View Forum Message](#) <> [Reply to Message](#)

On 04/04/2011 10.40, Ronin wrote:

> Il modem assegna a sÃ© stesso e al router un indirizzo 10.*.*, mentre
> la rete di casa Ã© su rete 192.168.0.* (e il router viene visto come
> 192.168.0.x), per cui desumo che sia giÃ in nat, o sbaglio?

Se Ã© cosÃ¬ giÃ in NAT (1), quindi sei giÃ a posto ed Ã© inutile che ti ponga problemi. Il tuo PC non Ã© esposto sulla tratta pubblica, quindi eventuali aggressori dall'esterno vedono solo il router, che non avendo servizi non ha porte aperte (a meno che tu non abbia configurato specificamente qualche "virtual host", ovvero "pubblicato" all'esterno qualche porta locale su cui c'Ã© qualche servizio che vuoi offrire all'esterno).

Le porte sul router vengono aperte dinamicamente mano a mano che i client interni fanno richiesta di uscire all'esterno, e viene gestito il ritorno dei pacchetti solo dall'indirizzo remoto verso cui si Ã© fatta la connessione.

Sono ovviamente sempre possibili attacchi di spoofing o "man in the middle", ma questi ti scavalcherebbero anche un normale firewall se non configurato ad hoc, per cui non Ã© che ci perdi qualcosa in termini di sicurezza.

In tutta onestÃ , quando hai un router configurato in routing (e non in bridging) sei giÃ a posto per il 100% delle esigenze domestiche. Ovviamente, il discorso cambia a livello aziendale specie se di mezzo ci sono dati da tutelare, ma non mi pare il caso.

(1) in realtÃ non Ã© propriamente in NAT, che Ã© una cosa leggermente diversa, in questo caso stai facendo banalmente routing.

--

Massimo Bacilieri AKA Crononauta

Subject: Re: Firewall?

Posted by [Ronin](#) on Mon, 04 Apr 2011 09:57:35 GMT

[View Forum Message](#) <> [Reply to Message](#)

On 4 Apr, 01:30, Crononauta <massimo.bacili...@gmail.com> wrote:
> Ma metti in NAT il router e vivi sereno, dammi retta! Facendo cos' ho da
> anni pure dei Windows dietro il router che non hanno problemi, con
> giusto un antivirus minimale (perch Windows " sempre Windows).

Massimo, grazie dei consigli, mi var' un giro su netstat che " un comando che non conosco ma dal nome mi ispira :)

Vedendo (da un sito) come il mio PC si presenta all'esterno, ho provato a fare un traceroute fino all'IP indicato dal sito, ma in effetti non va oltre il modem.

Il modem assegna a " stesso e al router un indirizzo 10.*.*, mentre la rete di casa " su rete 192.168.0.* (e il router viene visto come 192.168.0.x), per cui desumo che sia gi' in nat, o sbaglio?

Grazie

C.

Subject: Re: Firewall?

Posted by [NicoKid](#) on Mon, 04 Apr 2011 16:23:19 GMT

[View Forum Message](#) <> [Reply to Message](#)

Ronin wrote:

> On 4 Apr, 01:30, Crononauta <massimo.bacili...@gmail.com> wrote:
> Il modem assegna a " stesso e al router un indirizzo 10.*.*, mentre
> la rete di casa " su rete 192.168.0.* (e il router viene visto come
> 192.168.0.x), per cui desumo che sia gi' in nat, o sbaglio?

Premesso che non ho capito se ha un modem o un router (ma hai l'adsl o roba della tim, tre, vodafone?), l'indirizzo 10.*.* non " pubblico n' tantomeno il 192.168.0.*. Devi avere per forza un altro IP, magari assegnato dinamicamente.

Nicola.

--

chi va pian va san e va lontan

Subject: Re: Firewall?

Posted by [Crononauta](#) on Mon, 04 Apr 2011 17:29:52 GMT

[View Forum Message](#) <> [Reply to Message](#)

On Mon, 04 Apr 2011 18:23:19 +0200

NicoKid <nicola@false.com> wrote:

> Premesso che non ho capito se ha un modem o un router (ma hai l'adsl o
> roba della tim, tre, vodafone?), l'indirizzo 10.*.* non Ã¨ pubblico nÃ©
> tantomeno il 192.168.0.*. Devi avere per forza un altro IP, magari
> assegnato dinamicamente.

Ãˆ il point-to-point dell'ADSL. Per Alice Ã¨ 192.168.100.1, per esempio.
Se fai un traceroute lo vedi. Un mio traceroute:

```
1 192.168.1.1 10.462 ms 10.482 ms 10.550 ms
2 192.168.100.1 18.695 ms 21.624 ms 23.857 ms
3 88.44.230.149 24.450 ms 26.938 ms 29.129 ms
4 80.17.209.142 31.380 ms 34.160 ms 34.540 ms
[...]
```

--

Massimo Bacilieri AKA Crononauta

Skype: crononauta <massimo.bacilieri@gmail.com>

Facebook: Massimo Bacilieri

Subject: Re: Firewall?

Posted by [NicoKid](#) on Mon, 04 Apr 2011 20:23:27 GMT

[View Forum Message](#) <> [Reply to Message](#)

Crononauta wrote:

> On Mon, 04 Apr 2011 18:23:19 +0200

> NicoKid <nicola@false.com> wrote:

>

>> Premesso che non ho capito se ha un modem o un router (ma hai l'adsl o
>> roba della tim, tre, vodafone?), l'indirizzo 10.*.* non Ã¨ pubblico nÃ©
>> tantomeno il 192.168.0.*. Devi avere per forza un altro IP, magari
>> assegnato dinamicamente.

>

> Ãˆ il point-to-point dell'ADSL. Per Alice Ã¨ 192.168.100.1, per esempio.

> Se fai un traceroute lo vedi. Un mio traceroute:

>

```
> 1 192.168.1.1 10.462 ms 10.482 ms 10.550 ms
> 2 192.168.100.1 18.695 ms 21.624 ms 23.857 ms
> 3 88.44.230.149 24.450 ms 26.938 ms 29.129 ms
> 4 80.17.209.142 31.380 ms 34.160 ms 34.540 ms
```

Ah, d'accordo, ma ci avrÃ pure un IP pubblico, per lo meno dinamico. Io ho un IP fisso e non conosco bene come funziona Alice ma credo che l'IP pubblico lo devi avere sul router adsl non a casa della Telecom, o no? Oppure la Telecom ha tutti gli IP dinamici sui propri server e fa il mascheramento di tutto quello che passa fino al router Alice? Non so se ho detto una cosa sensata :)

Nicola.

--

chi va pian va san e va lontan

Subject: Re: Firewall?

Posted by [Crononauta](#) on Tue, 05 Apr 2011 07:18:46 GMT

[View Forum Message](#) <> [Reply to Message](#)

On 04/04/2011 22.23, NicoKid wrote:

```
>> 1 192.168.1.1 10.462 ms 10.482 ms 10.550 ms
>> 2 192.168.100.1 18.695 ms 21.624 ms 23.857 ms
>> 3 88.44.230.149 24.450 ms 26.938 ms 29.129 ms
>> 4 80.17.209.142 31.380 ms 34.160 ms 34.540 ms
```

>

> Ah, d'accordo, ma ci avrÃ pure un IP pubblico, per lo meno dinamico. Io ho
> un IP fisso e non conosco bene come funziona Alice ma credo che l'IP
> pubblico lo devi avere sul router adsl non a casa della Telecom, o no?

Non ho mai indagato la cosa, onestamente, ma una spiegazione che mi do Ã che alla fine il point-to-point Ã un router a sua volta in bridge: quindi ha una "faccia interna" che Ã quella che vedi tu "da dentro" (192.168.100.1 nel mio caso) e una "faccia esterna" che Ã l'IP pubblico che ti viene assegnato.

Quando fai un traceroute verso l'esterno vedi l'IP interno; se invece fanno il traceroute da fuori verso di te, vedono il tuo IP pubblico.

Non so se sia vero, ma mi pare verosimile.

--

Massimo Bacilieri AKA Crononauta

Subject: Re: Firewall?

Posted by [NicoKid](#) on Wed, 06 Apr 2011 08:13:49 GMT

[View Forum Message](#) <> [Reply to Message](#)

Crononauta wrote:

> On 04/04/2011 22.23, NicoKid wrote:

```
>>> 1 192.168.1.1 10.462 ms 10.482 ms 10.550 ms
>>> 2 192.168.100.1 18.695 ms 21.624 ms 23.857 ms
>>> 3 88.44.230.149 24.450 ms 26.938 ms 29.129 ms
>>> 4 80.17.209.142 31.380 ms 34.160 ms 34.540 ms
>>
```

>> Ah, d'accordo, ma ci avrÃ pure un IP pubblico, per lo meno dinamico. Io
>> ho un IP fisso e non conosco bene come funziona Alice ma credo che l'IP
>> pubblico lo devi avere sul router adsl non a casa della Telecom, o no?

>
> Non ho mai indagato la cosa, onestamente, ma una spiegazione che mi do Ã"
> che alla fine il point-to-point Ã" un router a sua volta in bridge:
> quindi ha una "faccia interna" che Ã" quella che vedi tu "da dentro"
> (192.168.100.1 nel mio caso) e una "faccia esterna" che Ã" l'IP pubblico
> che ti viene assegnato.

Il mio discorso era che questo IP pubblico lo dovresti avere nel tuo router
adsl, quello che hai in casa tua. Questo poi Ã" in bridge o in nat rispetto
alla rete "da dentro" 192.168.100.1, ma la configurazione si trova nel tuo
router adsl. Tuttavia credo che se come dici tu il router in casa della
Telecom fa da bridge e su questo c'e' l'IP pubblico alla fine non ci
dovrebbero essere differenze rispetto al fatto (come nel mio caso) che l'IP
pubblico si trovi nel router adsl locale.

Comunque ho l'impressione che ronin non abbia chiarito bene come Ã" messa la
sua rete facendo confusione tra modem Ã" router (quale dei due?).

Nicola.

--

chi va pian va san e va lontan

Subject: Re: Firewall?

Posted by [xx Dominus xx](#) on Wed, 06 Apr 2011 10:38:17 GMT

[View Forum Message](#) <> [Reply to Message](#)

Ciao ronin... Allora...

da ciÃ² che hai scritto chiaramente sei in NAT.

Per poter parlare di sicurezza va visto tutto il contesto e non la
soluzione di un firewall come ZA.

Nelle macchine installati firestarter.... E' molto semplice e puoi
dirgli di chiudere tutte le porte ed aprire solo quelle che usi di
solito (beowser, emule.. ecc).

Se perÃ² stai dentro un modem/router.... GiÃ li c'Ã¨ un firewall,
almeno chÃ¨ tu non abbia aperto e dato accessi senza un minimo di
ritegno.
Salvatore
