

Re: Router's Firewall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/5797.html>

From: luis (not@vaila.ble)

Date: 07/28/02

From: "luis" <not@vaila.ble>
Date: Sun, 28 Jul 2002 03:12:42 GMT

Hello Tony, thanks again for the extended reply. It definitely answers a lot of my questions and it allows me to move forward with this project. It's great that I have found this pleasant and informative newsgroup this one this time.

Regards,
Luis

"Tony Whitmore" <tony_whitmore@nospamhotmail.com> wrote in message news:zBz09.1490SS03.200466@stones...

- > *Hi again Luis,*
- >
- > *Sorry this reply is so long!*
- >
- > *AFAIK most firewall fitted routers do not allow incoming connections by*
- > *default. This means that traffic is only allowed through the firewall and*
- > *into the network if it is in response to an outgoing request. For example,*
- > *if you request a web page from a remote web server using your web browser*
- > *then the webpage should load. However, if someone on the remote server*
- > *tried*
- > *to connect to a port your public IP address the router would reject the*
- > *traffic, as it is not in response to a request from your network.*
- >
- > *You can check whether there are any ports open on your firewall using*
- > *web-based port scanning services such as the one at*
- > *<http://www.pcflank.com/scanner1.htm>. If this reveals open ports on your*
- > *router you may be vulnerable. If not, then you are pretty safe from*
- > *external*
- > *attacks. Of course, trojans and viruses can still compromise the security*
- > *of*
- > *your network, so remember to keep virus definitions up-to-date and using*
- > *Adware detection software.*
- >
- > *If there ***are*** ports open on your firewall, close them! This is best done*
- > *using the configuration software supplied with your router – check the*
- > *manual! You only need to have open ports on your router if you want to*
- > *offer*
- > *the world a service over the internet (a different topic!)*

comp.security.firewalls: Re: Router's Firewall

>

> *An open port on the router could be connected to a service running on the
> router itself or a computer on your local network. If it is connected to a
> service on the router (most likely telnet or the small web-server used in
> configuring some routers) then this is dangerous. Users on the internet
will
> be able to connect to your router. They may be able to exploit a
vulnerable
> service, or try to crack your password to get into your router. Having
said
> that, I don't know of any routers that are supplied this way
out-of-the-box.*

>

> *If the open port is "forwarded" to an open port on a computer on your
local
> network then any user trying to connect to the open port on your public IP
> address will actually connect to the open port on your local computer.
This
> is called "port forwarding" and is very useful when running separate
> computers offering internet services through one public IP address. Again
> routers aren't supplied with port forwarding configured out-of-the-box,
but
> check the settings on your router to be sure.*

>

> *I don't think that ZoneAlarm is redundant on a firewalled network.*

Although

> *I have a basic firewall built into my router/ADSL modem and I also use a
> linux based firewall for additional functionality, I still use ZoneAlarm
on
> my desktop machine. Incoming connections to the router are denied, so why
> still use ZoneAlarm? Well, it would protect your computer from
accidentally
> misconfigured port forwarding settings, for example. I also use it to
> control which applications are able to access the internet. It also shows
if
> any applications have changed, which could be due to malicious activity,
or
> if new applications (possibly a trojan?) are trying to access the
internet.*

>

> *To allow just your local network to access all the resources of your
> computer, you can designate the range of local IP addresses as "trusted"
in
> ZoneAlarm. Make sure that you don't include your internet gateway in the
> trusted IP range! Any one attempting to connect to your services from
> outside this range of IP addresses would be denied. It is then up to you
> whether you use user-based or password-based authentication for File and
> Printer Sharing. This should be based on what operating system is running,
> how trustworthy the users are, and who else could physically access the
> machines.*

>

Re: Router's Firewall

comp.security.firewalls: Re: Router's Firewall

> *Quick summary: the only way someone could connect to your File and Printer*
> *Sharing port 139 on a local computer is if:*
> *1) You open a port on the public side of your router*
> *2) You forward this port to the File and Printer Sharing port 139 on your*
> *local machine*
> *3) You set your firewall to allow connections to this port from any IP*
> *address, rather than a small range of private IP addresses.*
> *4) You have vulnerable services running on your machine. (Keep up-to-date*
> *with patches and software releases!)*
> *5) You use low level sharing authentication/weak passwords.*
> *Not doing one of these would stop a malicious user connecting. Not doing*
> **any* of them is best, though!*
>
> *Hope this helps,*
>
> *Cheers,*
>
> *Tony Whitmore*
>
>
> *"luis" <not@vaila.ble> wrote in message*
> *news:iow09.664559\$352.138111@sccrnsc02...*
> > *Hi Tony,*
> > *thanks for the answer... very enlightening. I've got the CompUsa*
router
> > *(Gigafast)... economical and it works well... The only concern is*
> > *security since I am using "sharing" within the network . While I learn*
> *the*
> > *details on setting up the security I am also setting up passwords to the*
> > *shared resources but that's a pain. I also have ZApr0 in the client*
> > *computers hoping that it would stop any breach although I am afraid that*
> > *it's redundant... Any suggestion will be appreciated.*
> > *Thanks again.*
> > *Luis*
>
>
>

-
- ***Next message:*** : ["Re: RUNDLL32.EXE"](#)
 - ***Previous message:*** [Techie: "Re: How to stop a port with za pro?"](#)
 - ***In reply to:*** : ["Re: Router's Firewall"](#)
 - ***Next in thread:*** [Duane Arnold: "Re: Router's Firewall"](#)
 - ***Messages sorted by:*** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)