

Re: Some Questions about my Routers Setup

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-08/1248.html>

From: Duane Arnold (*notme_at_notme.com*)

Date: 08/29/05

Date: Sun, 28 Aug 2005 23:58:14 GMT

"Nicky" <hackeras@gmail.com> wrote in
news:1125258600.402257.130300@f14g2000cwb.googlegroups.com:

>
> *Duane Arnold wrote:*
>
>> > *a) So my first question is that if there is another way of seeing*
>> > *this log file.*
>> > *Maybe some software installed on 10.0.0.1 that will be the first*
>> > *app*
>> > *that will grab the data immediately after my router forwards them to*
>> > *10.0.0.1 and then give them to the requesetd app? Does such an app*
>> > *exists(if what i say is possbile to be done)?*
>>
>> *The only way would be to find some 3 rd party firmware that provided*
>> *it and I doubt it.*
>
> *Why my suggestion wouldnt work?!?*

Because the firmware (software) that is installed in the router must have the *syslog* functionality, you cannot make the firmware do the logging if it doesn't have the functionality incorporated it. At best, you could find some 3rd party firmware that does syslogging for the SpeedTouch and flash, install it, the router and use that firmware. But the fact that it's a router/modem and a SpeedTouch (not a popular brand), I doubt that you're going to find any 3rd party firmware that will work with your SpeedTouch.

Yes, you would broadcast the router's syslog to a machine that had something like Wallwatcher installed so you can view the logs in real time, but the router's firmware must have the syslog functionality and the logwiwer must be able to work with the syslog from the device.

<http://www.sonic.net/wallwatcher/#Routers>

There is Kiwi Syslog Daemon too but the (free) version doesn't have log viewing abilities like the paid for version that can dump the logs to a database like MS Access, SQL Server or others and review the logs with a

comp.security.firewalls: Re: Some Questions about my Routers Setup

report viewer like Crystal Reports.

<http://www.notepage.net/kiwi-syslog/kiwi-syslog.htm>

>
>> >
>> > *b) Second question what about the hardware firewall of my router?*
>> > *Why dont see an option for that nowhere? Does Speedtouch 530 sucks?*
>> > *Can sol;ution a) aplly here as well?*
>>
>> *It's a good NAT router/modem unit I would suspect for home usage.*
>
> *Whats so good about it if i cant see an option to configure the*
> *hardware firewall if it has any?*

It's good for the average home user with average usage of the device that is not doing high risk things like "port forwarding*" and in that case, the NAT router on that port is not inspecting anything particularly if it is not using SPI, which I don't think your SeedTouch router/modem even has SPI. Does it have SPI in the firmware?

>
>> *If it were me and I was trying to protect a WEB server, then I would*
>> *get separate units a standalone adsl modem and a standalone packet*
>> *filtering FW router that does logging so I could see the inbound and*
>> *outbound traffic to/from the router, along with the ability to stop*
>> *inbound and outbound traffic by setting packet filtering rules by IP,*
>> *port or protocol.*
>
> *What router would you pick if it were you?*

I am not going to advise you on that one but you can look at Netgear, Linksys, maybe Dlink (the high-end) models or low-end FW appliances like Watchguard, Sonicwall etc. And you can get devices that are refurbished/used where you don't have to pay an arm and a leg. There are other models out there besides what I have mentioned that are good too. But I don't know the names off and but have seen others mention them -- the routers.

> *And also why would you seperate the modem form the router?*

The ones I have seen are a PITA to configure when taking them out of their default setup, especially on the router part. And the ones I have seen don't have the security fuctionality that you would get in a standalone device that I have seen, like content or Web blocking etc.

> *Whats wrong having them in 1 device as i have it now?*

There is nothing wrong with it for average home usage.

> *Does the packet filtering FW router only inspects the heders of a*

Re: Some Questions about my Routers Setup

comp.security.firewalls: Re: Some Questions about my Routers Setup

> *packet or data as well?*

The best I am going to do for you is provide two links *read* them. :)

<http://www.vicomsoft.com/knowledge/reference/firewalls1.html>

<http://www.more.net/technical/netserv/tcpip/firewalls/>

>

>> *What kind of Web server do you have and has the O/S, registry, file system, user accounts, Web sever such as IIS etc, etc been configured for security for a machine that is being exposed to the public Internet? Otherwise, you have another Web server out there on the Internet that's *hack* bait.*

>

> *I am runnign Apache/v2.0.54 on XP SP2.*

There are certain things one must do to secure the Windows O/S that has a Web server exposed to the public Internet even if it running Apache. The information is out there on Google or dogpile.com on the how(s) for Windows XP pro if you search for it. There may be some documantation on how to secure Appache running on the Windows platform

The link is a single example of what should do for a single XP pro machine that has a direct connection to the Internet not behind a router let alone it having a Web server running that is being exposed to the Internet.

<http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm>

The link above talks about IPsec.

<http://www.analogx.com/contents/articles/ipsec.htm>

<http://support.microsoft.com/?id=813878>

http://www.petri.co.il/block_ping_traffic_with_ipsec.htm

Services need to be shutdown and O/S configuration must take place properly to expose any MS Windows NT based O/S to the Internet running any kind of Web server and if you have not done it, it's just *hack* bait. And there a more than a few things that must be done to the O/S and you should find it.

> *and i also have Kasperksey*

> *Anti-Hacker running on my localhost to monitor outbout connections*

> *since NAT cant handle those and i dotn see any hardware firewall*

> *present.*

It's sanke oil.

I don't think you have done your homework on a machine that's running the NT based O/S that's being exposed to the Internet and it's just *hack* bait or a jumping off point to attack other machines on the Internet. And most home user don't know how and just throw it up and put it out there.

comp.security.firewalls: Re: Some Questions about my Routers Setup

Duane :)