

Re: What does a firewall do?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-01/1177.html>

From: IPGrunt (*me_at_privacy.net*)

Date: 01/20/05

Date: 20 Jan 2005 08:04:12 GMT

Nick Roberts <nick.roberts@acm.org> confessed in
news:gemini.ial5ue00fcw1501u4.nick.roberts@acm.org:

> IPGrunt <me@privacy.net> wrote:

>

>> Hard to get a straight answer here, isn't it? I have no problem with
your

>> question and will answer briefly.

>

> Hehe. I think I'm partly to blame, in the way I asked it.

>

>> Basically, a firewall does what a good protocol stack *should* do:

>> controls when ports are opened and closed, according to a rule set.

>

> I understand the opening and closing of ports, but I don't entirely

> understand the rule set.

>

> My idea of the incoming packet functions for the IP router for host

> (address) H is:

>

> 1. Forward packets not for H, if forwarding is activated. I would expect
> that forwarding would usually be deactivated altogether in AdaOS (because
it

> uses a non-IP protocol to communicate within a cluster). If activated, I

> think there should be an automatic adaptive filtering system, based on

> reject packets coming back the other way: if H forwards a packet from
node X

> to node Y (from port P to port Q?) and a reject comes back to H, drop all

> further packets from node X to node Y (from port P to port Q) for the
next

> 15 minutes.

>

> 2. Direct packets that are for H to port P, provided port P is open for

> receipt of packets. If the port is not open for receipt, send a reject

> packet back. A port will be opened for receipt either by the TCP
component

> or by some other UDP-based server program. Again, I think there should be
an

comp.security.firewalls: Re: What does a firewall do?

> *automatic filtering system: if more than 5 packets are sent to closed port P*
> *within a 30 second window, drop all further packets to that port for the next 15 minutes (unless the port is opened for receipt within that time).*
>
> *In other words, if I want packets sent to port 111 to be rejected (and, if they keep coming, dropped), I just don't open a service on port 111.*
Right?
>
>> *As an adjunct, firewalls these days are also part router, in that they provide a port proxy service by implementing network address translation, and part filter, in that they can provide arbitrary port blocking (never accept connections on port 111, for instance).*
>
> *Am I right that NAT tends to create problem for a variety of internet applications (that were programmed to assume that if a packet's send address is A, the computer that sent it was computer A)? I intend AdaOS to support IPv6 (as well as IPv4 and IPSec). Roll on IPv6.*
>
>> *But one of the most important features that firewalls provide is so-called "statewise" or "stateful" port access control, in that the firewall software maintains an open connection table that records the source of an open port, and acts accordingly, allowing packets from only that source to enter that particular port, blocking packets from any other address.*
>
> *Isn't that something that the TCP component could and should do (very easily)? Or is it more complicated than that?*
>
>> *Firewalls also provide very good logging capabilities these days, so add that to your list.*
>
> *Yes, but I think (and I have read in the literature) that it is generally better for applications to their own auditing, because they can do it at a higher level (more intelligent filtering, more useful data).*
>
>> *Finally, firewalls are now managing private channels through public transports, like VPN, using both standard and proprietary protocols.*
Some
>> *of these involve data packet encryption/decryption using symmetric and asymmetric key mechanisms, for example, IPSec.*
>
> *Is that a good argument for hardware firewalls? I'm thinking about the speed of packet encryption.*

Re: What does a firewall do?

comp.security.firewalls: Re: What does a firewall do?

>
>> *As we move toward universal use of IP6, some of these functions will*
>> *migrate naturally to the network stack, however, I say it's high time to*
>> *move firewalling, or at [least] perhaps the hooks and stubs for*
>> *firewalling appliances inside the network stack.*
>
> *That is what I feel.*
>
>> *In this century, networking without security is a fool's undertaking.*
>
> *I couldn't agree more.*
>
> *Thank you hugely for your helpful answer!*
>

Thanks for your reply, Nick.

Hardware firewalls are the only way to go, for a variety of reasons, but speed and reliability are the two most important. First, your point is correct—encryption using dedicated chips is one immediate advantage, and the firewall appliance inherently more efficient as its CPU is dedicated to the job at hand, examining packets, evaluating state, logging, etc. Secondly, a network 'appliance' is less susceptible to buffer overflow system failures, general crashes of the host computer, root capturing, etc.

There are of course, exceptions, but generally, a hw firewall is the only way to go.

As far as applications doing their own auditing, I don't disagree. Let a software intrusion detection system analyze the data. I'm not promoting that to be a function of the firewall, though simple alerts are popular features of most devices. The trigger is usually a parameter-based trip value, like so many messages per hour, or a certain type or source of attack. But I like simple tools. I'm not sure if the firewall should know how to dial your pager.

(I'm reading your comments bottom to top). Your comment about having the protocol stack manage ports is exactly the point I was getting at when I said that some firewall functionality should reside in the protocol stack. It just makes sense—the stack manages the connection table. Why should an external firewall have to duplicate that effort to the same end? Doesn't seem efficient or most effective to me. Let this function be a piece of the TCP protocol stack (which it is designed for in the IP6 specification, if I'm not mistaken).

A word of advice...although you'll have to support IP4, base your networking stack on IP6 and be backward compatible. Get familiar with this specification.

Good luck. Sounds like a fascinating project—I hope that it's well funded.

Re: What does a firewall do?

comp.security.firewalls: Re: What does a firewall do?

-- ipgrunt

PS--Is Grady Booch still around?