

Re: Best practices: Two nic's but have hardware firewall

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-02/msg05173.html>

- *From:* "SuperGumby [SBS MVP]" <not@xxxxxxxxxxxx>
 - *Date:* Tue, 28 Feb 2006 15:41:30 +1100
-

I am not aware of any application layer filtering in WatchGuard products. This may be a failing on my part. I would welcome a link to any references to such.

"Leythos" <void@xxxxxxxxxxxx> wrote in message [news:tMPMf.183090\\$PY6.96663@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:tMPMf.183090$PY6.96663@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)
In article <O79QkgBPGHA.3260@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, not@xxxxxxxxxxxx says...

I don't agree with much Tom says, and this article is more than a little 'skewed', but I find it of interest:

ISA Firewall Fairy Tales – What Hardware Firewall Vendors Don't Want You to Know (v1.02)
<http://www.isaserver.org/articles/2004tales.html>

Here is a snippet of what he seems to be saying that ISA does while Firewall Appliance don't:

=====

It is at this level that an ISA Server 2004 firewall becomes critical. In contrast to a packet filter hardware device, you need real firewall protection. Simple packet filtering is inadequate when it comes to protecting resources in the network asset ring. Not only must you be able to insure that all incoming connections are subjected to deep application layer inspection, you must also control what leaves the asset networks using strong user/group based access control.

Strong outbound user/group based access control is an absolute requirement. In contrast to your typical hardware packet filtering firewall that lets everything out, the firewalls at the Asset Network edge must be able to control outbound connections based on user/group based membership. Reasons for this include:

* You must be able to log the user name of all outbound connections so that you can make users accountable for their Internet activity

Re: Best practices: Two nic's but have hardware firewall

- * You must be able to log the application the user used to access Internet content; this allows you to determine if applications not allowed by network use policy are being used and enables you to take effective countermeasures
- * Your organization may be held responsible for material leaving your network; therefore you must be able to block inappropriate material from leaving your network
- * Sensitive corporate information may be transferred outside the network from Asset Network locations. You must be able to block this and record user names and applications the users are using to transfer proprietary information to a location outside your network

The ISA Server 2004 firewall is the ideal firewall for the Asset Network edges because it meets all of these requirements. When systems are properly configured as Firewall and Web Proxy clients, you are able to:

- * Record the user name for all TCP and UDP connections made to the Internet (or any other network that the user might connect to by going through the ISA Server 2004 firewall)
- * Record the application the user uses to make these TCP and UDP connections through the ISA Server 2004 firewall
- * Block connections to any domain name or IP address based on user name or group membership
- * Block access to any content outside their network based on user name or group membership
- * Block transfer of information from the Asset Network to any other network based on user name or group membership

All this deep application layer stateful inspection and access control requires processing power. That's why you should size your servers appropriately to meet the requirements of powerful stateful application layer processing. Fortunately, even with complex rule sets, the ISA Server 2004 firewall is able to handle well over 1.5 gigabits/second per server, and even higher traffic volumes with the appropriate hardware configuration.

=====

The WatchGuard firewall appliances do all of this and more, I know, I've got it setup doing the above. So, it seems that the Quality solutions do what ISA does and don't expose the solution to Windows flaws at the same time.

--

spam999free@xxxxxxxxxx
remove 999 in order to email me

.