

RE: [fw-wiz] Strange setup

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-02/0247.html>

From: Sloane, David (*DSloane_at_vfa.com*)

Date: 02/27/04

To: <firewall-wizards@honor.icsalabs.com>

Date: Fri, 27 Feb 2004 13:54:20 -0500

Not having seen the configuration, it's hard to say. It's possible that the netscreen won't accept traffic from non-server IP addresses – that would help.

–David

-----Original Message-----

From: firewall-wizards-admin@honor.icsalabs.com

[mailto:firewall-wizards-admin@honor.icsalabs.com] On Behalf Of mcary@badgermeter.com

Sent: February 27, 2004 12:17 PM

To: firewall-wizards@honor.icsalabs.com

Subject: RE: [fw-wiz] Strange setup

What prevents a user from changing his default route from ISA to the FW, bypassing any authentication that ISA provided?

-----Original Message-----

From: firewall-wizards-admin@honor.icsalabs.com

[mailto:firewall-wizards-admin@honor.icsalabs.com] On Behalf Of Bill Royds

Sent: Thursday, February 26, 2004 7:02 PM

To: 'Melson, Paul'; 'franco segna'; firewall-wizards@honor.icsalabs.com

Subject: RE: [fw-wiz] Strange setup

Actually there is a good reason for the ISA to be configured this way. The ISA server acts as an HTTP cache/authenticator. So if you have the inside boxes with default route going to internal address of ISA server, it can validate the user of that workstation with Windows authentication and either, forward the request out to the Internet and cache the reply, or return the cached value. This adds to security by ensuring that all internal workstation access is by authenticated users. The straight through branch is used for server traffic like mail that is coming towards the internal network or is being forwarded by authorized MTA style servers that use the FW as default route.

ISA may not be a great firewall but it is a good proxy/authenticator for

Firewall-Wizards: RE: [fw-wiz] Strange setup

a Windows network. Its examination it does of HTTP traffic before caching it is a bonus.

-----Original Message-----

From: firewall-wizards-admin@honor.icsalabs.com
[mailto:firewall-wizards-admin@honor.icsalabs.com] On Behalf Of Melson,
Paul
Sent: February 26, 2004 2:24 PM
To: franco segna; firewall-wizards@honor.icsalabs.com
Subject: RE: [fw-wiz] Strange setup

Franco,

Without seeing the rule sets on either system, it is impossible to say.

Clearly this design misses the point of a 'DMZ' network. There's no reason that I can think of for the ISA server to be dual-homed. There's no reason that outbound proxy traffic, RAS/VPN traffic, or reverse proxy traffic can't pass through two sets of firewall rules, one between the outside and DMZ, and another between the DMZ and inside. If you're tasked with redesigning this network, that should be first on your to-do list.

That said, a possible explanation is that the ISA server is a reverse proxy for servers on the internal network, and the firewall only allows inbound traffic to the DMZ for NAT purposes. In this situation, the ISA server could provide extra access controls at the application layer in the form of authentication or restricting access to specific pages/services through destination lists. Workstation browsing and other inside->out traffic could pass directly through the firewall without going through ISA.

That's just a theory, though. Looking at the rules on both the SonicWall and the ISA Server will give you a better idea of the intended function of this design.

PaulM

PS - I can't help but notice that a disproportionately large number of European, and specifically German IP networks (including my previous employer's) have been designed using internal addressing schemes that do not conform to RFC1918. Anybody have an educated guess as to why this is? It's just a personal curiosity of mine.

> -----Original Message-----

> *Hi everybody,*

> *I'm being confronted with the following existing setup:*

>

>

> *TI -----*

> *(Internet | LAN backbone |*

RE: [fw-wiz] Strange setup

Firewall-Wizards: RE: [fw-wiz] Strange setup

> *and VPNs*) -----+---+---+--+--+---
> |||||
> /+-----+ *local x.x.x.254/24* |||||+
> || *Sonic* +-----+ ||||+
> +---+ *Wall* |||||
> | *Pro* +-----+ |||+ *SQL*
> +-----+ *dmz* |||+ *mail*
> (?)|+-----+ |+ *etc.*
> || *MS ISA* ||
> +---+ *2000* +-----+
> | *Server* | *x.x.x.251/24*
> +-----+
>
> *The public web server is hosted elsewhere. The LAN comprises*
> *30 workstations.*
> *To complicate the matter, the LAN address family x.x.x. is*
> *NOT RFC1918-compliant (and is conflicting with existing*
> *Internet hosts).*
> *The system is up and running, but I cannot understand the*
> *bypassing of the ISA server through the direct connection*
> *firewall/LAN. And the meaning of DMZ seems to be lost.*
> *Anyone can help me to understand the matter ? Thanks in advance*

firewall-wizards mailing list firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

The information contained in this message is confidential and is intended for the addressee(s) only. If you have received this message in error or there are any problems please notify the originator immediately. The unauthorized use, disclosure, copying or alteration of this message is strictly forbidden. Badger Meter, Inc. will not be liable for direct, special, indirect or consequential damages arising from alteration of the contents of this message by a third party or as a result of any virus being passed on.

firewall-wizards mailing list firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>