

Re: [fw-wiz] ipsec communications with windows server

Re: [fw-wiz] ipsec communications with windows server

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2008-02/msg00020.html>

- *From:* Jeremy C Russell <JeremyRussell@xxxxxxxx>
 - *Date:* Tue, 19 Feb 2008 12:43:32 -0600
-

Are you sure that the router quits sending messages, or is the windows machine just not logging them...

I would believe its a stack issue on the windows box and when you run a *networked* app, it resets a buffer or something to that affect..

I would make sure it is the router and not the windows box.

Jeremy Russell
Senior Unix Systems Administrator
Pre-Paid Legal Services, INC.
580.272.2834

"shadow floating"
<nadengine@googlemail.com> To
Sent by: "Firewall Wizards Security Mailing
firewall-wizards- List"
bounces@listserv.icsalabs.com <firewall-wizards@xxxxxxxxxxxxxxxxxxxx
icsalabs.com .com>
cc

02/19/2008 11:31 Subject
AM Re: [fw-wiz] ipsec communications
with windows server

Please respond to
Firewall Wizards
Security Mailing
List
<firewall-wizards@listserv.icsalabs.com>

Re: [fw-wiz] ipsec communications with windows server

Re: [fw-wiz] ipsec communications with windows server

hi guys

i managed to get it up between the windows server and the cisco router with a little problem, first the configuration of the devices:

config of router:

```
ip:10.0.0.1
IKE:HMACHMAC-SHA1,DH2,preshared
IPSec:transparent ESP-3DES-SHA1
DPD: 10 sec
acl of interesting traffic:
access-list 100 permit ip 10.0.0.1 10.0.0.2
access-list 100 permit ip 10.0.0.2 10.0.0.2
other functions of router: NAT, stateful Inspection firewall
```

config of windows

```
ip:10.0.0.2
IKE:HMACHMAC-SHA1,DH2,preshared
IPSec:transparent ESP-3DES-SHA1
acl: any ip from 10.0.0.2 to 10.0.0.1 (mirrored)
services on windows: syslog server installed
```

10.0.0.1 is also the gateway for the management machine so all traffic from the windows machine to the internet must pass first through that router

it all worked fine except for one thing...after variable amount of time the router seems not to be sending logs to the syslog server on the windows machine until it first receives packets from from the windowshost...these packets could be a dns request routed by router to external dns....

in other words i keep receiving logs from the router to the syslog server for say 8 hours...then i receive nothing....if i started windows update for example on the windows machine , the routers start again sending syslog messages as "inspection rule allowed outbound dns from 10.0.0.2"..and keep receiving syslog messages for a about 10 hours..and then stop receiving any syslog messages...and same thing happens again and again...the time is not fixed but never got more than 1 day of continuous syslog messages receiving

does anyone have any suggestions?

thanks alot

regards,

Nad

On Feb 10, 2008 7:25 PM, Brett Cunningham <cssniper22@xxxxxxxxxx> wrote:

What's the config on the router? Do you have xauth and config-mode

Re: [fw-wiz] ipsec communications with windows server

Re: [fw-wiz] ipsec communications with windows server

disabled?

On 2/10/08, shadow floating <nadengine@xxxxxxxxxxxxxxxx> wrote:

Hi list,
i've been trying to get an IPSec communication channel to work between a cisco 2811 router IOS 12.4 and a windows server that have ipsec capabilities, have anyone tried this before and worked?
i want to have a secure communication between the windows management host and the router via ipsec vpn
the ike phase one seems to be ok as but the quick mode always fails though the same parameters are configured on both sides for a transparent mode vpn
any hints?

thanks alot
regards

Nad

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>

Confidentiality Note:

This email and any attachment to it is confidential and protected by law and intended for the use of the individual(s) or entity named on the email. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination or distribution of this communication is prohibited. If you have received this communication in error, please notify the sender via return email and delete it completely from your email

Re: [fw-wiz] ipsec communications with windows server

Re: [fw-wiz] ipsec communications with windows server

system. If you have printed a copy of the email, please destroy it immediately.

Thank you

firewall-wizards mailing list

firewall-wizards@xxxxxxxxxxxxxxxxxxxxxx

<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>