

Re: Outgoing VPN Error 619

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa.vpn/2008-04/msg00051.html>

- *From:* "Jim Harrison \ (ISA SE)" <jmharr@xxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 23 Apr 2008 17:07:02 -0700
-

This won't help.
Please send me the whole capture to jim at isatools dot org.

—
Jim Harrison (ISA SE)

This posting implies no warranty and confers no rights.
<http://catb.org/~esr/faqs/smart-questions.html>

"Damon" <enlighten@xxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:eHfjqcYpIHA.2636@xxxxxxxxxxxxxxxxxxxxxxx

Hi Jim,

I believe I have grabbed the right part of the Netmon log, have a look at this and let me know what you think:

```
239 9.843750 203.97.2.34 10.2.1.10 TCP TCP: Flags=.S..A..., SrcPort=1723,
DstPort=3524, Len=0, Seq=3740007268, Ack=1485119410, Win=16384 (scale factor
not found)
240 9.843750 10.2.1.10 203.97.2.34 PPTP PPTP: Control Message , Start
Control Connection Request
241 9.859375 203.97.2.34 10.2.1.10 PPTP PPTP: Control Message , Start
Control Connection Reply
242 9.859375 10.2.1.10 203.97.2.34 PPTP PPTP: Control Message , Outgoing
Call Request
243 9.875000 10.2.1.10 10.2.0.253 TCP TCP: Flags=....A..., SrcPort=2153,
DstPort=MS WBT Server(3389), Len=0, Seq=1694684887, Ack=2251219804,
Win=64592 (scale factor not found)
244 9.890625 203.97.2.34 10.2.1.10 PPTP PPTP: Control Message , Outgoing
Call Reply
245 9.890625 10.2.1.10 203.97.2.34 PPTP PPTP: Control Message , Set Link
Info
246 9.890625 10.2.1.10 203.97.2.34 LCP LCP: Configure-Request, ID = 0,
Length = 21
247 9.906250 203.97.2.34 10.2.1.10 LCP LCP: Configure-Request, ID = 0,
Length = 57
```

Re: Outgoing VPN Error 619

248 9.906250 203.97.2.34 10.2.1.10 LCP LCP: Configure-Ack, ID = 0, Length = 21
249 9.906250 10.2.1.10 203.97.2.34 LCP LCP: Configure-Reject, ID = 0, Length = 35
250 9.921875 203.97.2.34 10.2.1.10 LCP LCP: Configure-Request, ID = 1, Length = 26
251 9.921875 10.2.1.10 203.97.2.34 LCP LCP: Configure-Ack, ID = 1, Length = 26
252 9.921875 10.2.1.10 203.97.2.34 LCP LCP: Identification, ID = 1, Length = 18
253 9.921875 10.2.1.10 203.97.2.34 LCP LCP: Identification, ID = 2, Length = 22
254 9.937500 203.97.2.34 10.2.1.10 TCP TCP: Flags=..R.A..., SrcPort=1723, DstPort=3524, Len=0, Seq=3740007457, Ack=1485119758, Win=0 (scale factor not found)
255 9.937500 203.97.2.34 10.2.1.10 CHAP CHAP: Challenge, ID = 0, Length = 25, Name = 'ISA1'

Cheers

Damon

"Damon" <enlighten@xxxxxxxxxxxxxxxxxxxx> wrote in message
news:%23dB2uaYpIHA.3568@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Just to make sure I hvae got this right, I should do the install of Netmon 3 on the ISA server and set it to capture both ISA interfaces while I try and connect to the PPTP from a workstation on the network?

Cheers

Damon

"Jim Harrison (ISA SE)" <jmharr@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:0FF8ACBE-AA6D-4ED5-B1E8-3CC40E7749CF@xxxxxxxxxxxxxxxxxxxx

1. there is no gain in duplicating DNS server in multiple NICs. Remove them from the External NIC
2. you can capture with Wireshark or (my personal fav) Netmon 3; it doesn't matter. What does matter is that you capture at both ISA interfaces *at the same time* while performing your tests.

Result Code: 0x80074e24 FWX_E_CONNECTION_KILLED is very useful. This means that the PPTP filter saw something in the PPTP protocol that it didn't like and killed the session.

Re: Outgoing VPN Error 619

A network capture will be very revealing.

--

Jim Harrison (ISA SE)

This posting implies no warranty and confers no rights.

<http://catb.org/~esr/faqs/smart-questions.html>

"Damon" <enlighten@xxxxxxxxxxxxxxxxxxxx> wrote in message
<news:uQfbgeSpIHA.5096@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Ok Inbound VPN access is now working, just the Outbound VPN problem to go now!

Thanks for your help so far.

Have a read of the Outbound questions I tried to answer below and let me know what you think. There are also a bunch of settings in my Inbound VPN that you might want to check out.

Cheers

Damon

"Damon" <enlighten@xxxxxxxxxxxxxxxxxxxx> wrote in message
<news:ezfelhPpIHA.3428@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

On Inbound VPN

Ok these are the settings for my lan.

I have it set-up as the following:

Its is 10.2.*.*

I.E. the subnet is 255.255.0.0

The gateway on all machine on the network is 10.2.0.253

I have the servers on 10.2.0.*

I have the workstations on 10.2.1.* (DHCP assigned)

The ISA server has two network cards:

One named Internal Network which is configured as follows:

IP address: 10.2.0.253

Subnet: 255.255.0.0

Re: Outgoing VPN Error 619

Default gateway: blank
Pre DNS 10.2.0.3
Alt DNS 10.2.0.4

One named External Network which is configured as follows:

IP address: 192.168.1.1
Subnet: 255.255.255.0
Default gateway:192.168.1.254
Pre DNS 10.2.0.3
Alt DNS 10.2.0.4

I have a linksys AG241 DSL router which is running on 192.168.1.254 and has all of the VPN passthroughs configured

In ISA I have the lat table confured as follows:

Start: 10.2.0.0 End: 10.2.255.255
Start: 10.255.255.255 End: 10.255.255.255

I have now changed to a static address pool with the following settings:

Start: 10.1.0.0 End: 10.1.0.255
Use the following network to obtain DHCP.. : Internal

If I connect remotely I get assigned the following:

IP: 10.1.0.1
Subnet: 255.255.255.255

If I try and ping a server on the network like 10.2.0.1 I get request timed out.

Any ideas what I have done wrong?

On Outbound VPN

Q1: Yes it is a hop onthe path to the Internet. It is configured as the

gateway I.E. 10.2.0.253

Q2: If I do the following Query:

Log Record Type – Equals – Firewall or Web Publish
Log Time – Live
Action – Not Equal – Connection Status

Re: Outgoing VPN Error 619

Protocol – Equals – PPTP

I get the following:

Destination IP: the vpn server
Destination Port: 1723
Action: Initiated Connection
Rule: Allow All
Result Code: 0x0 ERROR_SUCCESS

Destination IP: the vpn server
Destination Port: 0
Action: Initiated Connection
Rule: Allow All
Result Code: 0x0 ERROR_SUCCESS

Destination IP: the vpn server
Destination Port: 1723
Action: Closed Connection
Rule: Allow All
Result Code: 0x80074e24
FWX_E_CONNECTION_KILLED

Q3: Would I do this with Wireshark on the computer I'm
initializing the
connection from? If so what would I filter on?

Cheers

Damon

"Jim Harrison (ISA SE)"

<jmharr@xxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:2AC3EEB0-F2E5-4CEB-8AB4-A5750DEFA088@xxxxxxxxxxxxxxxxxxxx

No; ISA doesn't dynamically move anything
between the VPN network and
the
internal network address ranges.
This network address range is based on the
setting you apply when you
run
the VPN wizard.
As long as the VPN client is assigned an
address from this predefined
range,
all will be well.

The "dynamic motion" you allude to is the
movement of the VPN client

Re: Outgoing VPN Error 619

between
Quarantine and VPN networks; nothing else.

--
Jim Harrison (ISA SE)

This posting implies no warranty and
confers no rights.
<http://catb.org/~esr/faqs/smart-questions.html>

"Phillip Windell"
<philwindell@xxxxxxxxxxxx> wrote in
message
<news:%23Pr2SxJpIHA.548@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
"Jim Harrison (ISA SE)"
<jmharr@xxxxxxxxxxxxxxxxxxxx> wrote
in message
<news:8D2EF7C2-BDCE-43CF-B29F-5BE8D75945DB@xxxxxxxxxxxxxxxxxxxx>

I only beat you when you
ask me to; it's part of our
"special
relationship"... :-p

Fair enough :-)

"stealing" from the LAT for
the VPN network
without actually changing
the LAT network (includes
actually changing
that
network) creates an overlap

That's what I was thinking of and is what I
do with my VPN Clients.
I'm
not
having any trouble in the sense that it
"works." I had expected to get
the
spoofing alerts although there is none listed at
the moment related to
VPN
Clients. So yes,..I just treated the alerts as
"safe to ignore".

Re: Outgoing VPN Error 619

Ok, to make sure I understand the process...

So if I understand Tom's description of the
VPN Clients Network near
the

beginning of the article

(<http://www.isaserver.org/tutorials/Enabling-Remote-Access-VPN-Clients-Access->

correctly, ISA will dynamically move an IP#
from the Internal into the
VPN

Clients Network when a connection is
made,..but during that brief
amount

of

time, before it completes, a spoofing alert is
triggered. When the VPN

Client is done and disconnects the process is
dynamically reversed.

Coupling that with what you are saying, if an
admin makes sure that the
IP#

a VPN Client receives is already not in the
Internal Network definition

(or

any other network def) then the ISA
dynamically adds it to the VPN

Clients

Network when needed and there is no
spoofing alert generated.

--

Phillip Windell
www.wandtv.com

The views expressed, are my own and not
those of my employer, or
Microsoft,
or anyone else associated with me, including
my cats.

Re: Outgoing VPN Error 619