

Re: Outgoing VPN Error 619

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa.vpn/2008-04/msg00039.html>

- *From:* "Damon" <enlighten@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 22 Apr 2008 23:59:44 +1200
-

Just a follow up on what I have tried with getting inbound VPN's working.

1. DHCP assigned (not working, comes up as spoofs)
2. Static assigned on a different subnet I.E. 10.1.255.255 (not working)
3. Static assigned on the same subnet I.E. 10.2.3.255 with the LAT table edited to only cover 10.2.2.255 (not working, throws misconfiguration alerts in ISA management)

I've checked in local network rules and I do have a rule called VPN clients to Internal Network which is a Route of Quarantined and VPN clients to the Internal network.

Any ideas on this, plus my outgoing PPTP VPN problem I'm getting desperate?

Cheers

Damon

"Damon" <enlighten@xxxxxxxxxxxxxxxxxxxx> wrote in message news:ON6Rh%23BpIHA.3804@xxxxxxxxxxxxxxxxxxxxxxxx

With the outgoing PPTP VPN's I have that allow all rule but they are still not working, any ideas on this?

With the incoming VPN's yes I do have the user address be allocated from the same DHCP that serves the internal network.

If I'm doing a static assignment will these need to be IP addresses which are within the range allocated via the LAT table or will they need to be outside of that.

Currently the internal network is 10.2.255.255

Cheers

Damon

Re: Outgoing VPN Error 619

"Jim Harrison (ISA SE)" <jmharr@xxxxxxxxxxxxxxxxxxxxxx> wrote in message news:%23e0uvLApIHA.3556@xxxxxxxxxxxxxxxxxxxxxxxxxx

You can do outbound PPTP, but as Phil stated, this is only possible if the PPTP clients are configured to use ISA as a hop to the Internet (SecureNET clients). Neither a web (CERN) proxy client nor a Firewall client host can send the GRE traffic that is critical to PPTP functionality through ISA.

Since the VPN client is also a SecureNET client, the rule allowing outbound PPTP must be anonymous because SecureNET traffic is by nature, anonymous. Your first "allow everything for all users" is sufficient for this task, but it's dangerously wide. Limit this to "PPTP" and you'll have the necessary rule. Make sure you don't also include "all authenticated users" in the same rule – this will force authentication and cause the PPTP request to fail.

Regarding the incoming VPN users, the "IP spoofing" error is most often related to assigning VPN users addresses from the same DHCP server that serves the internal network. You cannot satisfy the ISA requirement for separate subnets on each network by doing this. Try using static assignments instead.

—
Jim Harrison (ISA SE)

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

"Damon" <enlighten@xxxxxxxxxxxxxxxxxxxxxx> wrote in message [news:eG5USd\\$oIHA.2188@xxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:eG5USd$oIHA.2188@xxxxxxxxxxxxxxxxxxxxxxxxxx)

Hi Guys,

I have a development team which I need some members to be able to connect customers sites to do development. If we are were not to do outbound PPTP VPN's for them what other option would be better?

You mention that the clients need to be SecureNat. I have the gateways on all of the machines on the network set to use the ISA server internal NIC.
Isn't that what makes them a SecureNat client?

Re: Outgoing VPN Error 619

If by anonymous you mean 'All Users' then use my first rule allows everything outbound and the rule applies to the user set 'All Users'.

Any ideas how I can get this working?

On a side note I've now discovered that my inbound VPN's now do not work.

If

I connect external in to ISA my VPN will connect but I cannot ping any resources. If I have a look in the ISA logs I see IP Spoofing alerts.

Cheers

Damon

"Phillip Windell" <philwindell@xxxxxxxxxxx> wrote in message
news:eqpHmJ%23oIHA.3556@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

"Jim Harrison (ISA SE)"

<jmharr@xxxxxxxxxxxxxxxxxxxx> wrote in message

news:FF998E9E-3AB4-4CA5-B61D-5A706B1D2E13@xxxxxxxxxxxxxxxxxxxx

"Phillip Windell"

<philwindell@xxxxxxxxxxx> wrote in
message

news:%23xC3H17oIHA.4912@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

1. Outbound VPN is not "supposed" to ever
be allowed.

Jim – This is a business case decision. Some
folks do and some don't.

This

is not an "always" or "never" decision.

I may over emphasize sometimes,..but Tom makes almost as
strong a
statements
about the same thing in some of the stuff he wrote. Yes, I
know it is a
business decision, but are you saying that the development
team never
encourages or discourages certain usages by how they design
the
product?.
Considering the difficulty of balancing out the usage of
this with
SecureNAT Clients while still trying to have Web and
Firewall Client
functionality at the same time,...maybe it should be listed as
one of

Re: Outgoing VPN Error 619

the
many "unsupported configurations" (if it isn't already). The
"ISA on a
DC" didn't get added to the list till later, this could be the
same way.
Although I suppose with TMG, the ISA2006 is probably
already a fading
priority.

2. The Web Proxy and Winsock Proxying
services only "proxy" TCP or UDP
based
traffic. They will not, and will never do,
GRE/PPTP

Jim – there is no such thing as a "winsock
proxy" or "web proxy"
services
in
ISA 2006. There is one service; the firewall
service. There were
firewall
and web proxy services in ISA 2000, but
there has not been a "winsock
proxy"
service since Proxy 2. That said, the firewall
logs and possibly a
network
capture will help determine the problems
that may be occurring with
outbound
PPTP.

Now Jim, when I was out there after ISA2000 came out there
was
discussion
about how the Winsock Proxy Service of Proxy2 was
"renamed" for
marketing
reasons because they felt they weren't able to market Proxy2
successfully
as a "firewall". But under the new name it was still the same
old
Winsock
based proxying service with maybe some internal
improvements. Even the
Firewall Client Software was, to a certain extent, compatible
between
the

Re: Outgoing VPN Error 619

different versions. Now I'm certainly not as close to the product as you are (no one is) but no one has ever told me that the "Firewall Service" of ISA2006 has been that drastically reworked to be operating by a completely different technology and standard than the earlier versions.

Personally, I think renaming it to "firewall service" was not a good idea and caused more confusion than anything else. I see the entire product as a firewall product, not just one component of it. I agree with Tom when he often refers to it in his material as the "ISA Firewall", implying that the whole product is a firewall product.

3. Only the SecureNAT Service and do GRE/PPTP.
 - a. So the Clients have to be SecureNAT Clients.
 - b. The Access Rules for them must be "anonymous"
 - c. In some cases the Private IP# Range of the remote network being contacted may have to be added to the Internal Network Definition

Jim – 2/3 correct. item (c) is not true. Only those subnets which are actually reachable in the network structure associated with that network should be listed there. Also, you have to ensure that any anonymous rules are listed before any authenticating rules, or they cannot be processed as you expect.

http://www.microsoft.com/technet/isa/2006/BP_Firewall_Policy/default.mspx refers.

Re: Outgoing VPN Error 619

Yes, sorry, I got ahead of my self. That would only be true if the VPN

Device was some other device separate from ISA. But I did say "in some cases",..whowever, you're right, I should have stopped with a & b.

--

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.

Understanding the ISA 2004 Access Rule Processing
http://www.isaserver.org/articles/ISA2004_AccessRules.html

Troubleshooting Client Authentication on Access Rules in ISA Server 2004
<http://download.microsoft.com/download/9/1/8/918ed2d3-71d0-40ed-8e6d-fd6eeb6cfa07/ts>

Microsoft Internet Security & Acceleration Server: Partners
<http://www.microsoft.com/isaserver/partners/default.msp>

Microsoft ISA Server Partners: Partner Hardware Solutions
<http://www.microsoft.com/forefront/edgesecurity/partners/hardwarepartners.msp>
