

Re: Computer Migration and SecureNAT

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-04/4078.html>

From: Tony Su (*anonymous_at_discussions.microsoft.com*)

Date: 04/13/04

Date: Mon, 12 Apr 2004 21:49:00 -0700

IMO you're thinking too hard, the SBS install is supposed to take care of much of this and you can figure out what happened later (assuming all works well).

But,

At the cost of probably confusing you, I'll say that when your FW Proxy client is working, you sort of have a "little DNS" on your client machine which knows how to resolve many names without having to make a call to ISA or your SBS server's DNS service. The other clients do not have this capability. If that was confusing, just forget it because it's something valuable to know only when troubleshooting, when name resolution is working you don't usually need to know where and how it's happening.

As for your other comments, yes it's good that you are noticing these things, but at least for the Packet Filtering issue if you run the CEICW again, you should be configured properly.

But I also suggest that you go through everything again after running the CEICW. And yes, you will find all sorts of things not configured at all or configured in a way not generally recommended.

– You will find IDS turned off. You'll have to enable all the IDS features manually.

– I don't remember how IP routing is configured by default, but this is a thumbnail to doublecheck whether you are configured properly or not...

IP routing won't disable ISA, but it addresses what ISA does not support... non TCP or UDP protocols like GRE.

In Win2K, SBS2K only there was only one IP Routing setting... and if you enabled IP routing to support VPNs (WWAN <> LAN) you also were forced to permit IP routing

across the SBServer box (LAN <> WAN).

The ISA IP routing configuration is like a master switch which configures the RRAS IP Routing setting(s), and in SBS2K3/Win2K3 you now have two IP routing settings where there was only one in SBS2K/Win2K.

So, now in SBS2K3

- Your WWAN IP routing setting should be enabled only if you're supporting VPNs.
- Your LAN/WAN IP routing should be enable in either of two situations... support for protocols like PING (ICMP is neither TCP nor UDP) or enhancing SNAT performance.

Since ISA2K was released prior to Win2K3, you should not assume that the ISA IP routing switch configures things properly, you should also inspect the RRAS settings.

If you are interested in considering additional things which diverge from a default SBS2K3 installation, you may want to take a look at my Web Publishing Companyweb paper...

www.su-networking.com/faq/
(click on first link)

Tony Su

>-----Original Message-----
>> - SNAT client. Disable or no FW client installed. Since no
>> Windows logon required, all activity is "anonymous" and
>> can be tracked only by IP address. Does not support as
>> much as FW client. Required whenever an application or
>> device cannot logon to the Domain.
>>
>>I infer that nothing is done by way of the "Migrating
Computers" task in
>>ADMT. That's a relief to know.
>
>Now, with regards setting the dns service on the client
to point to the
>server box, I don't find any recognizable dns .msc
console—and infer that
>the only means to do this by setting the TCP/IP
properties in the client's
>NIC. The proxy settings are set in the Internet Options'
LAN settings.
>
>I just found KB article 297922, which tells hou to enable

IP routing to the

>*client computers. If that bypasses the firewall features of ISA server,*

>*that doesn't sound like a good idea. I also notice that Packet Filtering is*

>*disabled in out-of-the-box ISA server, as well as Intrusion Detection. It*

>*would seem that a significant part of the advantages of ISA server are*

>*disabled there.*

>

>*Hollis Paul*

>

>*"Tony Su" <anonymous@discussions.microsoft.com> wrote in message*

>*news:1b68f01c420b3\$0c3dd470\$a501280a@phx.gbl...*

>> *Abbreviated intro to ISA clients...*

>>

>> *- WebProxy. No software installed, just configure any*

>> *webproxy-aware application using a web protocol (ie. web*

>> *browser) to point to ISA, port 8080 by default.*

>>

>> *- FW client. FW client app must be installed. Extends*

>> *SOCKS support to the client machine, so practically all*

>> *TCP or UDP protocols are supported. Requires Windows*

User

>> *authentication.*

>>

>> *- SNAT client. Disable or no FW client installed. Since*

no

>> *Windows logon required, all activity is "anonymous" and*

>> *can be tracked only by IP address. Does not support as*

>> *much as FW client. Required whenever an application or*

>> *device cannot logon to the Domain.*

>>

>> *Note that VPN connectivity shouldn't have anything to do*

>> *with whether you're configured as a FW or SNAT client.*

>>

>> *Tony Su*

>>

>>

>>

>>

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

>> >*my understanding is that it allows outgoing vpn from*

>> *client machines that*

>> *are behind a ISA firewall.*

>> >*that said i've had nothing but trouble with it..*

>> >*probably more to do with me than isa :)*

>> >

>> >*"Hollis Paul [MVP - Outlook]"*

