

Re: Proxy capabilities and securenat/firewall client

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isaserver/2007-07/msg00019.html>

- *From:* "steve" <steve@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 17 Jul 2007 09:12:39 GMT
-

"Phillip Windell" <philwindell@xxxxxxxxxxxx> wrote in message
<news:%234xzW7CyHHA.4264@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

"steve" <steve@xxxxxxxxxxxxxxxxxxxx> wrote in message
[news:5CImi.71324\\$0A4.51083@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:5CImi.71324$0A4.51083@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hi all,

I currently have a watchguard box as my perimeter firewall.

Same here.

I want to install an ISA box as another perimeter firewall (on another public IP) in order to utilise it's reverse web proxy functionality. I would also like to use it as a forward proxy in combination with the surfcontrol ISA product so

We've done that, but without the SurfControl

1) Can I proxy both HTTP and HTTPS traffic through ISA?

Yes.

2) Do I need the firewall client installed to achieve this?

No. But you should use it anyway.

I was intending to push out IE proxy settings via GPO.

Re: Proxy capabilities and securenat/firewall client

Forget GPO. It is too rigid, inflexible, and sometimes unpredictable.
Use the WPAD proxy autodetection method. Plenty of info on the Net and MS's site for doing that with both DNS and DHCP (use both the DNS and DHCP methods at the same time).

3) Do I need to do anything special to get the remote workers to proxy through ISA?

Yes. Their browsers need the proxy details added to the specific Dialup Connection (found in the browser internet options). The proxy settings in the LAN Settings are irrelevant to VPN dial in clients.

They are standard XP machines with an IPSEC firewall client

IPSEC firewall client? I don't think there is any such thing.

Once they VPN into the watchguard, the firewall client gets an IP address on our local subnet

Actually the WG does not do that. That is why we stopped using the WG for VPN. It uses a static pool of addresses,...it does not "get an IP from the local subnet". In addition to only using a static pool of address it does not provide for any other TCP options like DNS, WINS, etc....so those have to be added statically/manually to the user's Dialup Connectiod. The WG also won't allow you to have VPN clients with static addressing. Fortunately ISA smoothly allows all those thing to work perfectly fine if you choose to use it as the VPN server instead of the WG (which we now do). The role of our WG has been reduced to providing the Corporate Site-to-Site VPN Connection (with a WG at each site) and providing outbound access to certain servers and network devices,...it does nothing else any longer and those other jobs have all been rolled over to the ISA.

and can access the ISA box's private interface by hostname or IP address?

Hostnames require WINS in the user's Dialup Connectiod.
FQDNs require DNS in the user's Dialup Connectiod.
Without those you are stuck with IP#s

—
Phillip Windell
www.wandtv.com

Re: Proxy capabilities and securenat/firewall client

Are there any disadvantages of using the firewall client? For example, will it happily sit alongside standard firewall software (e.g. f-secure) that may be on a client machine?

I'll look into WPAD (it looks quite straightforward), however I'd like to know what the problem is with using GPO to push the HTTP/HTTPS proxy settings to IE? I thought this would be the easiest thing to do, given all my machines are on the domain.

The remote workers have the watchguard VPN client installed, which (when connected) is treated by windows as a standard NIC connection. At this point the users can ping the ISA internal interface, so if their IE proxy = ISA internal address then won't that work? How will the firewall client work in this remote scenario?

Thanks for the replies so far, I'm an ISA virgin =>

.