

# Re: Web Proxy Client – Direct Access to internal web servers of remote subnets not working

---

*Source:* <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa.clients/2006-08/msg00037.html>

---

- *From:* "Nik" <[nik\\_meeus@xxxxxxxxxxx](mailto:nik_meeus@xxxxxxxxxxx)>
  - *Date:* Thu, 31 Aug 2006 10:28:46 +0200
- 

Ray, thx for the update . In the mean time it's solved via another forum [www.isaserver.org](http://www.isaserver.org). For who is interested...

#####

Hi Nik007,

if the direct access is correctly configured than the ISA server is no longer part of the communication path. In other words, your internal routing infrastructure should take care of the correct routing. For more info about the network within a network scenario, check out the following articles :

- <http://isaserver.org/articles/2004netinnet.html>
- <http://isaserver.org/articles/2004isafirewallnetworks.html>

HTH,  
Stefaan

#####

I believe that the direct access is correctly configured but that it is not working correctly. When SP2 was installed I had also to apply the hotfix 920715 because when you add IP address (direct access), direct access for domains didn't work anymore. I've read the documentation you provided and I believe that the internal routing is correct. Forgot to tell, on the ISA server I configured route's to the remote subnets.

Futher test:

1. Webproxy client (wpad via dhcp) on lan with default gateway = NOT the ISA server. It loads the wpad file and I'm able to connect to an internal server directly AND I'm able to connect to a server on the remote subnet. It seems that the webproxy and direct access is working when the DG is not the ISA. I see in the monitoring Service=proxy;Filter=webproxy filter; GET <http://bekiisa1/wpad.dat>

2. Webproxy client on lan with default gateway = ISA server (wpdad via dhcp). It loads the wpad file and I'm able to connect to an internal server directly but I'm NOT able to connect to a server on the remote subnet (route's are configured on ISA). It seems that the ISA server sees the client as secure NAT, I see in the monitoring Service =proxy;Filtler: The ISA Server denied the specified Uniform Resource Locator. On the client I get the following error 403 the isa server denied the specified url. So it seems that direct access is not working and that the client is treat as SecureNAT.

Re: Web Proxy Client – Direct Access to internal web servers of remote subnets not working

Regarding the documentation when a client is Webproxy and Secure NAT it will first treat the client as Webproxy. But I can see on the client that the wpad file is downloaded correctly.

#####

Hi Nik007,  
that's normal and expected behavior. Please reread the articles I posted the link of.

The critical point is that you should never loopback through the ISA server. In other words, each host on the same subnet as the ISA internal interface must also know the routes to the remote subnets, just like the ISA server.

Therefore, I always use a network design as shown in my article [http://www.isaserver.org/articles/How to Implement VPN OffSubnet IP Addresses.html](http://www.isaserver.org/articles/How_to_Implement_VPN_OffSubnet_IP_Addresses.html), section '2. Network Design'. In that way, each host needs only one route, the default gateway.

HTH,  
Stefaan

#####

Stefaan, thanks a lot for the info. As you explained and I now understand, even if the client is webproxy the client need to know how to reach the remote subnet. Because the client doesn't know the network it sends again the traffic to DG=ISA. The ISA now treat the client as SNAT and blocks the traffic. Our current firewall is an (old) SonicWall and here we only had one client version = SNAT (if you use the ISA terms) and the Sonicwall acted as router (routes configured) and didn't check this traffic => different with ISA.

Because I'm not able (not allowed and becomes rather complex)in our network setup to install an additional router (layer3 device) as mentioned in your article "stub network" I've configured our DHCP server to distribute the static routes (option 249) to our remote subnet (instead of doing it via a login script) and it works now.

#####

"Ray" <no@xxxxxxxxxxxxxxxxxxxx> wrote in message [news:exr2UMqyGHA.3428@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:exr2UMqyGHA.3428@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

How do you route traffic between those subnets? Are you using ISA as the router?

\*\*\* Web browser tab  
– checked bypass proxy for web servers in this network  
– directly access computers specified in the domain tab, following domain/servers"

If you manually specify the proxy settings in IE (address and port), you force the traffic to go to ISA. That's why you want to use auto-detect and/of a configuration script ONLY.

Re: Web Proxy Client – Direct Access to internal web servers of remote subnets not working

wpad via DHCP only works if the end user is a local administrator. Are they?

Ray

"Nik" <nik\_meeus@xxxxxxxxxxxx> wrote in message  
[news:u%23v%23qeEyGHA.4372@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:u%23v%23qeEyGHA.4372@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Setup: ISA Server2004 Edge firewall SP2  
External: Static IP provider WAN  
\*\* Internal addresses configured on ISA  
– 192.168.0.0–192.168.0.255 => LAN  
– 10.1.0.0–10.2.255.255 => remote subnet  
\*\* Web browser tab  
– checked bypass proxy for web servers in this network  
– directly access computers specified in the domain tab, following domain/servers  
\*.abc.com/\*

We use Web Proxy clients via wpad.dat provided by DHCP (in our setup not possible via DNS). Remark: DG on client is ISA. I can see that the wpad.dat file is downloaded correctly to the clients.

Applied hotfix KB 920715 "Web Proxy clients do not directly access a Web site that you enter in the "Directly access these servers or domains" list in ISA Server 2004 SP2"

Problem description

E.g.

www.abc.com = 192.168.0.60 (server on lan)

sametime.abc.com = 10.2.1.7 (server on remote subnet)

Because of technical reasons we want to access our internal (web)servers directly and not via the ISA server. When we access a server directly on our LAN it goes directly to the (web)server (e.g. www.abc.com) => OK. I checked this via monitoring, it first download the wpad file and then I'm able to access the server without going over the ISA. When we access a server (e.g. sametime.abc.com), which is located on a remote subnet, it goes via the ISA server and blocks the connection. Adding IP addresses (e.g. 10.2.1.7) to the "directly access computers ..." doesn't work. Also very strange is that \*.abc.com/\* is in this list and contains the servers.

The following are no solutions for us:

1. When I add a route on the PC to the gateway for the remote subnet via login script, it works but I can not do this because of technical issues (e.g gives problem when laptop user goes to remote office).
2. I can also add a firewall rule to allow this traffic but I can not do this because this traffic may not go over the ISA server

Re: Web Proxy Client – Direct Access to internal web servers of remote subnets not working

Thanks