

Re: Static IP

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-12/5974.html>

From: James B (*no_spam_at_please.com*)

Date: 12/23/04

Date: Thu, 23 Dec 2004 13:49:25 -0500

Actually Linksys says it does Stateful Packet Inspection so it is more than a NAT device **HOWEVER!!!!** Linksys devices have trouble with GRE so I question their packet inspection quality.

It is also a wireless router so I suspect he has wireless clients so he has to run DHCP on it most likely because I don't think that model will support DHCP forwarding so he needs to setup DHCP on SBS to exclude a range or include a range not being used by the router and I hope he has setup some wireless security or otherwise he may as well just hook the modem into his server.

"Lanwench [MVP - Exchange]"

<lanwench@heybuddy.donotsendme.unsolicitedmail.atyahoo.com> wrote in message news:edcdZy75EHA.1396@tk2msftngp13.phx.gbl...

> *Clay Gerrard wrote:*

> > *no need for inline just a few quick things.*

> >

> > *I am using a Firewall, its built into the router. Linksys WRT55AG.*

> >

> > *This device doesn't appear to be a true "stateful inspection firewall" -*

> > *just a NAT device that "acts" as a firewall. I don't think it's good enough.*

> > *Also, if you're using wireless on your LAN you need extra extra security or*

> > *you might as well invite the whole world in -*

> >

> > *Can anyone else second the idea that I should be using SBS for DHCP?*

> > *Using the router for DHCP has worked so well for us so far. I only*

> > *have one NIC in the server.*

> > *internet -> cable model -> router -> switch -> clients & SBS*

> >

> > *root hints: (for anyone else following this post)*

> >

> >

> > <http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/res>

> >

> > *google => - and your right I'm not using root hints.*

> >
> > *I'm acctually not sure if GoDaddy's system requires I request the
> > deliverary or if it automatically attempts deliverary on some
> > interval. I'll call their tech support. Anyone else using Godaddy?*
> >
> > <http://www.rfc-ignorant.org/> – *there's a lot to this RFC, I'll do my
> > best.*
> >
> > *Lanwench, thanks again for all your time.*
>
> *You're welcome!*
> >
> > –clay
> >
> > *"Lanwench [MVP – Exchange]"*
> > <lanwench@heybuddy.donotsendme.unsolicitedmail.atyahoo.com> wrote in
> > message news:eWnj1M45EHA.3648@TK2MSFTNGP11.phx.gbl...
> >> *Clay Gerrard wrote:*
> >>> *thanks for the detailed response! Please see below I have some more
> >>> questions and want to make sure I understand you.*
> >>>
> >>> *Also inline –*
> >>>>
> >>>> –clay
> >>>>
> >>>> *"Lanwench [MVP – Exchange]"*
> >>>> <lanwench@heybuddy.donotsendme.unsolicitedmail.atyahoo.com> wrote in
> >>>> message news:OFOWcT35EHA.924@TK2MSFTNGP14.phx.gbl...
> >>>> *Clay Gerrard wrote:*
> >>>>> *We're migrateing to a static IP so that we can have a registiered
> >>>>> domain name for our email address (i.e. username@companyname.com).*
> >>>>>>
> >>>>>> *This is a first for me, and I'm a little confused. I'm just
> >>>>>> getting one ip. The router has my SBS server as the primary DNS
> >>>>>> (and my ISP's as secondaries).*
> >>>>>>
> >>>>>> *What do you mean? Your router config should not specify anything in
> >>>>>> your LAN*
> >>>>>> *IP range. What kind of router are you using – is this your Internet
> >>>>>> modem? Are you using ISA?*
> >>>>>>>
> >>>>>>>
> >>>>>>> *Not using ISA – is this a security risk?*
> >>>>>>>>
> >>>>>>>> *If you don't have a firewall (if your Linksys is just a NAT device)
> >>>>>>>> then yes, you have a potential security problem. You need something
> >>>>>>>> – I personally don't generally use ISA; I use Sonicwalls or similar
> >>>>>>>> between Internet modem/router and LAN.*
> >>>>>>>>>
> >>>>>>>>> *My Router is also my DHCP
> >>>>>>>>> server (would you recommened using SBS instead?)*

> >>
> >> *Absolutely– SBS should be your DHCP server.*
> >>
> >>> *. It's a Linksys*
> >>> *router – The Cable modem is seperate. It's always been configured*
> >>> *to use the server for internal name resolution. I'm not sure I*
> >>> *understand how I could ping computername.companyname.local if it was*
> >>> *not. Please elaborate.*
> >>
> >> *The router doesn't need to access your internal DNS for any reason.*
> >> *Because*
> >> *you run your own DNS in SBS, and all clients point only at it (or*
> >> *should), they can all use that for internal name resolution. You*
> >> *should not be able to resolve your internal names from the Internet*
> >> *side (and can't if you are*
> >> *using .local anyway)*
> >>>
> >>>> *Internally, make sure that all servers and workstations specify*
> >>>> **only* the internal AD–integrated DNS server's IP address in their*
> >>>> *network settings. The AD–integrated DNS server itself on SBS should*
> >>>> *be set up with forwarders*
> >>>> *to your ISP's DNS servers for external resolution and/or use root*
> >>>> *hints*
> >>>>
> >>>>
> >>>> *I have all the clients set to obtain DNS automatically.*
> >>
> >> *Right, but your router is providing this. Change it.*
> >>
> >> *, When you run*
> >>> *an ipconfig /all the client machines only show the internal DNS*
> >>> *server.*
> >>
> >> *That's good – and the server is set up with the same, statically?*
> >>
> >>> *And SBS does forward all unresolved names to my ISP's DNS.*
> >>
> >>
> >> *Good.*
> >>> *However when we're talking about a client machines trying to hit*
> >>> *google or whatever it never touches the server*
> >>
> >> *Yes it does – they look at your SBS server for DNS, and your SBS*
> >> *server gets*
> >> *the info from the forwarders or root hints.*
> >>
> >>> *because the router*
> >>> *knows to use the ISP's DNS – again unless I'm misunderstanding*
> >>> *something. I'm not firmiliar with "root hints"*
> >>
> >> *I don't have a good definition link handy & am in a rush, but google*

> > *if you're curious. Since you're also using forwarders, you may never
> > even be using them.*
> >>>
> >>>> *My understanding will be that if I point the MX
> >>>> record for my domain (companyname.com – hosted on godaddy) to the
> >>>> ip that my ISP is assigning to my router – any thing on
> >>>> companyweb.com (e.g. smtp.company.com) will get resolved by the
> >>>> SBS DNS.*
> >>>>
> >>>> *I think you've misunderstood how this works. Your SBS DNS is
> >>>> *internal only*. That's Active Directory, and it has nothing to do
> >>>> with the outside world.*
> >>>>
> >>>> *Yes I think I am misunderstanding this. I understand now that I
> >>>> have no need to host a public DNS – and we're not. Under what
> >>>> conditions might a company want to host its own public DNS?*
> >>>>
> >>>> *A large company with an appropriate server/network infrastructure
> >>>> might want
> >>>> to for more control.*
> >>>>
> >>>>> *But I read
> >>>>> somewhere its not a good idea to host the DNS for companyname.com
> >>>>> and companyname.local on the same machine.*
> >>>>>
> >>>>> *Correct – but it doesn't sound like you'd be hosting your public
> >>>>> DNS in house anyway, which is a good thing.*
> >>>>>>
> >>>>>> *Any education on this subject would be appreciated. Windows
> >>>>>> SBS2003 Administrators Companion doesn't go into detail on this
> >>>>>> subject.*
> >>>>>>>
> >>>>>>> *General notes:*
> >>>>>>>
> >>>>>>> ** Your public DNS should be hosted by Godaddy or whomever
> >>>>>>>*
> >>>>>>>
> >>>>>>> *It is.*
> >>>>>>>
> >>>>>>> *Good.*
> >>>>>>>>
> >>>>>>>> ** Your router/firewall/ISA/whatever should be doing NAT – all
> >>>>>>>> internal machines/servers need private IP addresses*
> >>>>>>>>>
> >>>>>>>>>
> >>>>>>>>> *It is. They do.*
> >>>>>>>>>>
> >>>>>>>>>> *Good. But as I said, you must get some sort of firewall in place –
> >>>>>>>>>> not just
> >>>>>>>>>> NAT.*
> >>>>>>>>>>>

> >>>> ** Port 25 needs to be open inbound to the private IP of your SBS
> >>>> server
> >>>>
> >>>>
> >>> Just set that. What about 21 (FTP) or 443 (for OWA) any others I
> >>> should set to forward?
> >>>
> >> Do not open up FTP to your LAN or you'll be sorry. 443 for OWA is
> >> fine. Don't open 80, either.
> >>>>
> >>>> ** Your public DNS folks need to create an A record/host –
> >>>> mail.mydomain.com,
> >>>> specifying your public IP – and your primary MX record for
> >>>> mydomain.com should point to mail.mydomain.com. You should also
> >>>> have someone else act as
> >>>> backup (secondary MX) – see www.dyndns.org 's MailHop BackupMX for
> >>>> one inexpensive option. You must not try to specify an IP address
> >>>> as your MX record – this is a violation of the RFCs.
> >>>>
> >>>>
> >>> should it be mail.mydomain.com or smtp.mydomain.com or are we
> >>> talking six one way half-a-dozen the other?
> >>>
> >> Whatever you want. Could be mylittlepony.mydomain.com if you chose.
> >>>>
> >>>> GoDaddy provides a service
> >>>> similar to BackupMX so in the event my server goes down mail should
> >>>> be forwarded to their mail server until I can retrieve it.
> >>>>
> >> Not familiar with their stuff, but find someone who wont' make you
> >> come in to retrieve it – it should be store/forward for automatic
> >> redelivery for X days.
> >>>>
> >> Thanks for
> >>>> the tip on pointing the MX record directly to the IP – I wasn't
> >>>> aware of that. Any suggestions on some good material on RFCs.
> >>>>
> >> Google :)
> >>>>
> >>>> Also is
> >>>> there anyway to make changes propogate "out into the web" faster? I
> >>>> suppose I could change the TTL until I get this strightened out, in
> >>>> case I need to make any more changes – what would you suggest?
> >>>>
> >> Yes, you can change the TTL to something lower for a bit – then make
> >> the changes you need on a Friday, and watch the magic happen. Then
> >> reset the TTLs to something more sensible.
> >>>>
> >>>> ** Your recipient policy needs to specify mydomain.com as the
> >>>> default SMTP address space – and all mailboxes need to be set to
> >>>> inherit from the policy***

> >>>> *(the CEICW should do this for you)*
> >>>>
> >>>>
> >>> *CEICW = Client Email & Internet Connection Wizard?*
> >>
> >> *Yep.*
> >>>
> >>> *Thank you again for the prompt and detailed response, I hope you*
> >>> *get a change to look over the rest of these questions. This board*
> >>> *is GREAT!*
> >>>
> >>> *-clay*
> >>
> >> *You're most welcome – hope this helps. And yes, the SBS newsgroups*
> >> *are among*
> >> *the more 'awesome' in terms of MS groups.*
>
>