

Re: Routing between subnets with a twist

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-05/msg03623.html>

- *From:* "Steve" <wonderlan1@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 27 May 2008 22:08:07 -0500
-

You should be able to do what you want. Just configure the firewall to not allow outbound internet access from the LAN for subnet 172.0.0.x. I believe you may also be able to do that in RRAS by configuring input/output filters on the external NIC if you want but personally I would do it on the hardware firewall.

Steve

"Ryan" <mindflux98@xxxxxxxx> wrote in message
news:4f936b88-1bf1-4e9d-b7bc-f8f48943a9cb@xx

On May 27, 4:28 pm, Joe <j...@xxxxxxxxxxxxxxxx> wrote:

It's not clear how you're connecting these subnets, where the Internet router is, and whether you're using the conventional SBS-as-firewall two-NIC configuration. The traditional way would be to have the Internet-using machines on the SBS 'LAN' NIC with the other NIC on a different network shared only with the router, then the isolated network connected to the LAN network via a separate router.

What I suspect you're hoping for is to use the SBS single-NIC, with LAN machines and router all on the same network, and to use the second SBS NIC as the gateway to the isolated network. I have a feeling that would work on Server 2003 but not on SBS, as placing the Internet gateway on the LAN network implies single-NIC, and the wizards are unlikely to cooperate in the use of a second one. I could be wrong there.

However you end up arranging the topology, the answer is to set static routes on the isolated machines, telling them where to find the gateway to the LAN, but not setting a default gateway for them. They won't know that there's a way out to the Internet via their static route, only a default gateway setting would tell them that. Also, unless you tell the Internet router where to find the isolated network, no replies will get back to it. Only the SBS LAN machines need to have routes configured to that network, as you describe things.

Re: Routing between subnets with a twist

I'd also make my usual suggestion of *not* subnetting the 10.0.0.0/255.0.0.0 network, especially if older network-aware software is involved. There are many other private ranges to choose from.

I want to make an ascii diagram but I know that'll never come out well.

Here's my current config, best I can give.

Internet-->Cisco ASA 5505 (10.0.0.1) -> Netgear Switch -> SBS 2003 no ISA (10.0.0.5) -> DHCP -> Workstations

I want to add (172.0.0.0) as a separate subnet off the second nic of the SBS server and have it route between them. But judging from other responses this doesn't seem the ideal way to go. The problem is these Agilent instruments come configured all hokey like they have 5 different teams working on them. Sometimes they come in as 10.10.10.0, sometimes as 192.168.168.0.. sometimes something entirely different.

Since I'm tired of these hodgepodged machines on my network I want to consolidate them to a range of addresses off my normal net. That way I dont end up with address conflicts from bootp that these things run.