

Re: Trihomed DMZ just doesn't work

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2004-03/0323.html>

bcadieux_at_provctr.org

Date: 03/11/04

Date: 11 Mar 2004 05:06:12 -0800

Thanks for your response Andrew. You make an interesting observation about the external subnet containing the DMZ subnet. I would agree with you that my configuration should be..

*External

IP: 204.17.121.129

Mask: 255.255.255.128

*DMZ

IP: 204.17.121.1

Mask 255.255.255.128

However, I believe I've read a Jim Harrison posting that indicated the my original configuration should work. The configuration also seems to be validated by Tom Shinder's ISA Server and Beyond. There Tom' example shows...

*External

192.168.1.33/24

*DMZ

192.168.1.67/26

*DMZ Host

192.168.1.69/26

Unless I'm missing the obvious, the external subnet contains the DMZ subnet here also. In any case I've tried it both ways with no luck.

Is it possible that ISA will not route correctly using a /25 subnet?

All the examples I've seen are using at least 4 subnets.

"A Klimkin" <aklimkin at mail dot ru> wrote in message news:<OAYDf7zBEHA.3344@tk2msftngp13.phx.gbl>...

> *To be successful with tri-homed ISA configuration you should follow the next simple rules:*

> *1. You should assign your DMZ interface the IP address from the block of IPs obtained from ISP.*

microsoft.public.isa: Re: Trihomed DMZ just doesn't work

- > 2. You should not configure your DMZ interface with default gateway property.
- > 3. You should not put your DMZ interface IP in the LAT.
- > 4. Your external and DMZ interface IPs should reside in different subnets.
- > This means that if you've got only one address block from your ISP you should subnet it by yourself.
- >
- > And what we've got here with your configuration...
- > 1. For me it's not clear that you assigned public address to the DMZ interface. If the DMZ will not have the public net ID the whole internet will have no idea how to route to your DMZ.
- > 2. It's ok in your config but the internal ISA interface should never be configured with DG property too. I'm not sure if this anyway affects your DMZ connectivity from the external hosts but definitely would lead your to a problem with internal clients outbound access.
- > 3. ok
- > 4. If I properly understand your network configuration, here is the main issue. Your external subnet contains also the DMZ subnet, that is wrong. Suppose you have class C network 204.17.121.0/32. So your tri-homed ISA configuration might look as follows:
- >
- > * External interface:
- > IP: 204.17.121.129
- > Mask: 255.255.255.128
- > Default gateway: 204.17.121.254 (your ISP router's address)
- >
- > * DMZ interface:
- > IP: 204.17.121.1
- > Mask: 255.255.255.128
- > Default gateway: *none*
- >
- > * DMZ hosts:
- > IP: 204.17.121.2-126
- > Mask: 255.255.255.128
- > Default gateway: 204.17.121.1
- >
- > Regards,
- > Andrew
- >
- > <bcadieux@provctr.org> wrote in message
- > news:78a14031.0403101527.14619663@posting.google.com...
- >> I hope someone can help with this. After about 20 hours of my time
- >> and 6 hours with MS Tech Support time, I'm starting to think a
- >> trihomed ISA senario really can't work. If someone can tell me where
- >> I've gone wrong I will be deeply appreciative.
- >>
- >> We have the entire class C address xxx.xxx.121.0/24
- >>
- >> Ext = xxx.xxx.121.253
- >> NM = 255.255.255.0
- >> DG = xxx.xxx.121.254 (ISP router)

>>
>> *DMZ = xxx.xxx.xxx.13*
>> *NM = xxx.xxx.xxx.128*
>> *DG = none*
>>
>> *DMZ Host = 204.17.121.20*
>> *NM = xxx.xxx.xxx.128*
>> *DG = 204.17.121.13*
>>
>> *Int = 192.168.1.18*
>> *NM = 255.255.255.0*
>> *DG = 192.168.1.1*
>>
>> *IP Packet filtering enabled*
>> *IP routing enabled*
>> *LAT 192.168.1.0 192.168.4.255*
>>
>> *I've followed the guidelines in ISA Server and Beyond to set up my*
>> *ICMP packet filters for pings to and from the DMZ host and to and from*
>> *the external gateway. I've run Netmon on the external interface of ISA*
>> *and I can see the incoming ICMP packets, but that's as far as it*
>> *goes. ISA isn't forwarding the packets to the DMZ interface.*
>>
>> *MS Tech Support has so far offered suggestions such as "the external*
>> *client PC that is pinging the external interface of the ISA server has*
>> *to have a static route to the DMZ interface". I have two MS techs*
>> *looking at this but it seems to be a learning experience for them as*
>> *well.*
>>
>> *To be sure my production ISA isn't introducing an unforeseen*
>> *configuration issue, I've setup a test system with an ISA server, an*
>> *internal PC, a DMZ host, and an external PC setup with the internal*
>> *address of my ISP's router.*
>>
>> *I've read the postings of many others who have a much more complex*
>> *addressing scheme than I do and they seem to have this working. I*
>> *suspect the problem is with the default route table that has been*
>> *created by ISA for the three nics. I'm more than comfortable changing*
>> *the routing table and have tried several combinations. However, I*
>> *have no idea what the correct route table should look like.*
>>
>> *Any help would be sincerely appreciated, especially a complete example*
>> *of how a system like mine should be set up.*
>>
>> *Until now I have had great successes with ISA and MS Tech Support but*
>> *my faith is quickly waning.*