

Re: AD & NAT

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-09/msg00739

- *From:* "Anthony" <anthony.spam@xxxxxxxxxxxxxxxx>
 - *Date:* Mon, 17 Sep 2007 09:19:16 +0100
-

It sounds as though the 3 data centres are trying to put your servers outside their infrastructure, on a different interface of their firewall, and then trying to get you back onto their WAN interface. They really don't need to NAT you. They can just use firewall rules. The best solutions would be to:

- ask them to create a VPN connecting your 3 10. infrastructures and your 3 offices
- create your own VPN, and route it over the internet.

Its more of a political problem than a technical one.

Anthony,

<http://www.airdesk.co.uk>

"LCS AP-Certificate" <LCSAPCertificate@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:A01ECA46-97D1-44F6-9BE2-3B4274C08759@xxxxxxxxxxxxxxxxxxxxxxxx

Hi Ryan,

I thought i explained the scenario we are facing in detail but i would attempt to explain again in detail

The client is a demerged company of the parent. The parent has a 3.x.x.x environment comprising of servers and end user desktops. The demerged company

or the client is being asked by the parent to use a 10.x.x.x IP addressing schema for its server infrastructure while the end user desktops for the demerged company or the client are still on a 3.x.x.x environment. The demerged company or the client doesnt foresee its end user client desktops moving from the current 3.x.x.x environment for atleast a year or more.

The demerged company or client wants to set up its own AD server infrastructure. The AD infrastructure would be distributed across 3 datacentres worldwide and additional 20 locations / branches / offices worldwide. The AD server infrastructure at the 3 datacentres would be configured to use the 10.x.x.x IP addressing range and these would be

Re: AD & NAT

natted
with a 3.x.x.x IP addressing range on the firewall or NAT device located
at
each of the datacentre. The natting would be done by a NAT device and not
the
AD server.

The AD server infrastructure at 20 locations would use the 3.x.x.x IP
addressing schema

The end user desktop environment worldwide would use the 3.x.x.x IP
addressing schema

The proposed AD architecture for the demerged company or client consists
of
a parent-child AD domain architecture where the parent is an empty root
domain or placeholder and all the demerged company or client resources
such
as users, computers, file servers would be part of the child domain.

The root domain controller of the parent domain and the first domain
controller of the child domain would be in one of the datacentres for
understanding purpose we would call it as primary datacentre while
additional
domain controllers for the child domain would be installed at the
remaining
two datacentres and 20 locations / branches / offices worldwide.

We have made an additional DNS server besides the AD DNS on the DC's at
the
primary datacentre which consists of a secondary DNS zone of 3.x.x.x but
inspite of it we are facing AD replication issues or problems when running
dcpromo at locations or when performing name resolution from the DC's or
end
user desktops at locations to the DC's at primary datacentre, it returns
10.x.x.x IP which is the real ip of the DC's

In this context, We want to know options or approach we can consider.

Regards,

Manish

"Ryan Hanisco" wrote:

Hi Manish,

First off, remember that your IP structure is on OSI Layer 3 whereas
Windows

Re: AD & NAT

and Active directory are on Layer 7 as it is an application. Granted, an NOS works across a number of layers, but in this case, the issue really only arises if you are having Windows Server handle the NATing itself — this is something I would not recommend at all.

Normally in an environment like yours, you will have routers or security devices connecting your WAN links or VPN links and handling the NAT translations for each connection (tunnel, PVC, MPLS site, or whatever.) This means that you will have some logical IP scheme that you will use to route traffic, while there is a different IP scheme that the Routing needs to be aware of to move the traffic — fortunately, your DCs should be behind the translation, so they needn't be aware of it.

Usually you'll see an organization use a 10.x.x.x scheme logically so that the second octet represents the site so that each /16 network is a different site. This may well actually translate to different 3.x.x.x networks for the routing of the traffic, but the inside devices needn't be aware of this structure. From there, You'll just need your sites set up on the 10.x.x.x/16 subnets and you're gold.

There are some more complicated scenarios that could be going on here, but you really haven't given enough information to infer anything else. The scenario outlined above is most common though and should be able to be adapted to suit your needs.

I hope this helps.

—

Ryan Hanisco
MCSE, MCTS: SQL 2005, Project+
Chicago, IL

Remember: Marking helpful answers helps everyone find the info they need quickly.

"LCS AP-Certificate" wrote:

Hi Mathieu,

Re: AD & NAT

Thanks for your reply.

Yes, We cant avoid this NAT. So, We want to know how do we approach this scenario.

We need to implement DC over the enterprise. There would be three datacentres across the world and which has internet architectures and these are the three places where NAT would be employed meaning the real IP addresses of these DCs at the three datacentres would be natted.

The real IP at the three datacentre for DCs is 10.x.x.x. Natted IP for the DCs at the datacentre is 3.x.x.x while the remaining DCs at locations or branches or offices apart from the datacentre would have a 3.x.x.x IP addressing schema. The client desktops at all locations would be having 3.x.x.x IP addressing schema.

We would like to know how can we proceed in such a scenario or what are the options we can try

Regards,

Manish

"Mathieu CHATEAU" wrote:

Hello,

I guess you really can't avoid this nat ? Be prepared to the hard way..
-DC will register in DNS with bad address
-IpSec doesn't like nat, even NAT-T:
IPSec NAT-T is not recommended for Windows Server 2003 computers that are

Re: AD & NAT

behind network address translators

<http://support.microsoft.com/default.aspx?scid=kb:en-us:885348>

-You may have kerberos error:
0x26 (KRB_AP_ERR_BADADDR)
""Incorrect net address"
Session tickets include the addresses from
which they are valid. This
error
can occur if the address of the computer
sending the ticket is
different
from the valid address in the ticket. A
possible cause of this could
be an
Internet Protocol (IP) address change.
Another possible cause is when
a
ticket is passed through a proxy server or
NAT. The client is unaware
of the
address scheme used by the proxy server, so
unless the program caused
the
client to request a proxy server ticket with
the proxy server's
source
address, the ticket could be invalid.

--
Cordialement,
Mathieu CHATEAU
<http://lordoftheping.blogspot.com>

"LCS AP-Certificate"
<LCSAPCertificate@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in
message
<news:09701575-CCC3-4824-9C69-A7BDD6D733FC@xxxxxxxxxxxxxxxxxxxx>

Hi,

We are working on a case
where we need to
implement AD architecture
using
a
natted IP for the DC.

Re: AD & NAT

Scenario / Business
Requirement –

Client would use a Parent and Child AD domain architecture. Parent AD domain would be World.com while child domain would be Child.World.com. World.com is an empty root forest while Child.World.com would contain all resources, DC's worldwide. The first domain controller for root domain and child domain would be installed at America datacentre and a ADC for root domain would be at APAC datacentre for redundancy while domain controllers belonging to the child domain are spread across locations in APAC, Americas and Europe. APAC, Americas and Europe has one Datacentre. AD DC's in each of the datacentre have a real IP of 10.x.x.x while they are natted to 3.x.x.x on the NAT device. The other server infrastructure such as E-Mail, etc also use 10.x.x.x as real IP and natted with 3.x.x.x on the NAT device. The locations which are in

Re: AD & NAT

APAC or America or Europe have their DC with a 3.x.x.x IP. There is no NAT configured for locations except datacentre. There are a total of 20 such locations that would have a DC with 3.x.x.x IP addressing range and without NAT. Clients across the globe are on 3.x.x.x IP addressing range. They are not configured for NAT. There are no clients except servers in datacentre. Client would be using the natted IP scenario for atleast a year further. Client has configured a secondary DNS zone having 3.x.x.x address in the America datacentre cause of which locations in America can enroll workstations to domain

Problem Scenario / Queries
– Due to the nat scenario, the following scenarios exist

Additional domain controllers can only be added at America datacentre. These ADC's cannot be added for other locations in Americas. DNS name resolution by client at locations returns the real IP of 10.x.x.x

Re: AD & NAT

DHCP Scope would be
3.x.x.x for clients at
locations
How to configure AD site
replication between
locations in APAC,
Americas
and
Europe and between three
datacentres

Kindly advise on the
workaround that can be
employed when DC's use
NAT IP
across the enterprise and in
this scenario, how to effect
name
resolution,
ad
site replication from all
locations across the
enterprise and other
essential
configurations such as
DHCP, etc.

We need advisory assistance
on implementing the above
and how the
problem
scenario can be addressed or
the workaround that can be
employed in
effectively deploying an AD
infrastructure using a NAT
IP across
the
enterprise and also able to
perform DNS name
resolution, DHCP, AD
replication, adding machines
to the domain, installing
additional
domain
controllers, etc

Regards,

Manish

Re: AD & NAT