

## Re: Help with initial small org AD setup convention when using DMZ network

**Source:**

[http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active\\_directory/2005-01/0384.html](http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2005-01/0384.html)

---

**From:** Cary Shultz [A.D. MVP] ([cwshultz\\_at\\_mvps.org](mailto:cwshultz_at_mvps.org))

**Date:** 01/09/05

Date: Sat, 8 Jan 2005 20:11:11 -0500

Mike,

This post is way too long.....

Short story – hook up with an ISP. They will handle the networking side of things ( Public DNS, IP Address, etc. ). Okay, maybe 'handle' is not the correct term here.

If you have multiple physical locations ( San Francisco, Los Angeles, New York, etc. ) then use one domain ( yourdomain.com ) and use Active Directory Sites and Services to create each Site in AD. You would want to use a different range for each ( say, 192.168.1.x for San Francisco, 192.168.2.x for Los Angeles, 192.168.3.x for NYC, etc. etc. etc. ) and make sure that if you do not have dedicated private links ( say, a T1 ) connecting things that you make use of a Site-to-Site VPN between the locations. I know that the PIX will do this. I have used the SonicWall Firewalls for this and they work very nicely! Mucho Mucho Importante! Unless there are specific reasons for having multiple Domains or having child domains ( usually political – or Password Policy related ) do not bother! With WIN2000 Active Directory you do not need to do this anymore ( it was much more needed in WIN NT 4.0 ). Key word – 'need'. You can if you like but that adds a lot of costs and administration.

Consider using Dynamic DNS internally ( aka Active Directory Integrated DNS ) and make sure that each Site has at least one Global Catalog Server in it ( a GC must be on a Domain Controller ). Depending on the size of things most people in here will suggest to you that you have at least two DCs per Site. If you are going to use BIND internally then you need to make sure that it supports the all important SRV records. I think that it is version 8.2.1 and up that does??????? Or was that version 8.1.2??????

If you need a DMZ then I would not really put anything in it other than your public web server ( but then someone like register.com or godaddy.com can do that! ). You definitely do not want to put a Domain Controller in the DMZ!!!! Might sound silly to say but there have been a lot of people who

have done this!!!

If you want, you can use yourdomain.com for the public domain name as well as for the internal domain name. You would have to add a 'www' host record in your internal DNS so that your internal users can get to your public web site. I think that most people would suggest that you use something that is not public ( such as yourdomain.local – but IIRC there is a problem with the .local if you have Macs in your environment, so maybe something like yourdomain.lan would work ). I have almost always used yourdomain.com for both public and private naming....no problems to date!

With Active Directory there are two types of Replication: intrasite and intersite. This would be something to take into account.

You might also want to take a look at the Delegation Wizard so that you can better control who can do what. What does this mean? Maybe you are in LAX but you want a select few in SFO and NYC to be able to do things within Active Directory ( say, create user account objects or reset passwords or whatever ). The Delegation Wizard would be your friend.

Does this get you going?

I can not speak too much to the Linux/Unix involvement as I have never worked in a mixed environment. There is a tool that will allow you to 'synch' things up between the two.

HTH,

Cary

<mjcsfmail-google@yahoo.com> wrote in message  
news:1104807737.845962.202760@z14g2000cwz.googlegroups.com...  
> *I'm just getting ready to create my first AD domain structure for a  
> small company, which for the sake of argument owns the domain acme.com.  
> I'm used to setting things up with BIND as follows. I typically  
> purchase an 8 or 16 static IP block and use a Cisco border router (ADSL  
> or T1) which routes this public IP block to a dmz network containing  
> bastion hosts running web and other public services, and a Cisco PIX  
> firewall which then connects the public IP dmz network to a private IP  
> back-end or office network with NAT and static translations to provide  
> access from dmz to back-end systems. Usually I add the third-level  
> domain name for such subnets based on the nearest airport code, for  
> example, in San Francisco, I would use sfo, or in New York, nyc. I  
> usually create a DNS server on the back-end network to handle  
> intra-office needs, and a second DNS server on the dmz to serve the  
> public IP address space for internal and sometimes external users if I  
> want to manage it that way; alternately I'll use network solutions or  
> Yahoo to manage my externally-visible DNS names on the acme.com domain.  
>  
>  
> Questions at the bottom – here's a list of domains with their*

- > *characteristics:*
- >
- > *SCENARIO:*
- >
- > *(Thanks in advance for your patience – I think this is a rather common*
- > *setup, but want to fully document how I intend to set things up for*
- > *comment and advice.)*
- >
- > *acme.com*
- > – *Public IP address block provided by ISP*
- > – *DNS managed by external ISP and/or on bastion host on DMZ.*
- > – *SUBSET of IPs defined for dmz.acme.com which should be visible*
- > *to public, i.e. www.acme.com = www.dmz.acme.com*
- > – *NOT a real network, in that no switch contains servers or*
- > *workstations which directly use this domain – this is only used*
- > *for external DNS names for public services.*
- >
- > *dmz.acme.com (primary office dmz network)*
- > – *Same public IP address block as acme.com*
- > – *SUPERSET of IPs which resolve for external clients, i.e. inside*
- > *border router interface.*
- > – *A real network in that a switch exists which connects routers*
- > *and servers that use this domain, i.e. ns1.dmz.acme.com*
- > – *Border router on this network is default gateway and connects to*
- > *Internet*
- > – *Outside (insecure) interface of PIX firewall is on this*
- > *network*
- > – *One or more bastion hosts are on this network providing public*
- > *services such as web, ftp, public mail server, etc.*
- > – *I don't want to run a Windows-based server on the DMZ for*
- > *security reasons, and all dynamic services proxy through to*
- > *a back-end server for execution.*
- > – *I run a DNS server on a bastion host to resolve dmz.acme.com*
- > *and acme.com for internal users. I usually use the ISP's DNS*
- > *servers to serve acme.com names for external users. I sometimes*
- > *make this a master server for these domains, sometimes make*
- > *it a slave to the master DNS server on the sfo.acme.com net if*
- > *security requirements allow it.*
- >
- > *sfo.acme.com (primary office internal subnet)*
- > – *First scenario is to have one office located in San Francisco*
- > *with this domain name, connected to the dmz network also in*
- > *San Francisco via the PIX firewall*
- > – *Private address space, usually 192.168/16 range reserved for*
- > *all offices with one 192.168.(0/16/32/...)/20 (set of 16*
- > *class-C subnets for each office with the lowest being that*
- > *office's standard or primary LAN, i.e. 192.168.0/24 for first*
- > *office, 192.168.16/24 for second, etc.)*
- > – *Inside (secure) interface of PIX firewall is on this*
- > *network, PIX performs NAT*
- > – *May have multiple additional subnets with internal routing*

- > *structure at some future point in time, but initially, this*
- > *network contains all servers and workstations in the local*
- > *office. If added, additional networks will be of the form*
- > *xyz.sfo.acme.com, and would use the next subnet in the block*
- > *of 16 allocated to that location, i.e. 192.168.1/24 for second*
- > *network of first office.*
- > *– I've typically run a couple of Linux-based BIND DNS servers*
- > *on this network, one slave and the other the master for*
- > *sfo.acme.com, dmz.acme.com and acme.com (for internal users).*
- >
- > *nyc.acme.com; lax.acme.com (secondary office internal subnets)*
- > *– Second scenario is to handle the later addition of additional*
- > *offices.*
- > *– These will generally be connected to the Internet in a similar*
- > *way, and may or may not have dmz networks of their own with*
- > *public address space.*
- > *– A PIX or similar (i.e. Watchguard) firewall capable of creating*
- > *IPSec site-to-site tunnel-mode connections would be in each*
- > *secondary office, and Cisco or IPSec standards-based tunnels*
- > *would be created between each office in a point-to-point*
- > *configuration to tie the offices together. It is very unlikely*
- > *we would use Windows servers as the endpoints for the site-to-*
- > *site tunnels.*
- > *– These offices would each have a block of 16 private class C*
- > *subnets as noted above, with the first of those being the*
- > *subnet used for normal workstations and servers.*
- >
- > *Additional notes:*
- > *– Additional domains within each office will generally be project*
- > *or client based for security reasons, and generally temporary.*
- > *They will generally only contain the servers for a large web*
- > *site under development, and will be accessed by Windows clients*
- > *connected to the primary office subnet. We will want to give*
- > *them DNS extensions and a different subnet on the other side of*
- > *a router which protects that subnet from all other subnets, but*
- > *will usually NOT want to create a child domain from Window's*
- > *viewpoint if that requires another primary and secondary domain*
- > *controller, as that would be overkill – these subnets will be*
- > *small and primarily for security segmentation.*
- > *– I can either use a Cisco 3005 VPN Concentrator or a Windows 2003*
- > *server on the office network (i.e. sfo.acme.com) or the PIX*
- > *firewall itself to handle occasional remote user L2TP/IPSec VPN*
- > *connections. We may want to have each office have the ability*
- > *to have remote users connect directly to that office.*
- >
- > *ASSUMPTIONS:*
- > *– I want to create a single forest with a single tree with each*
- > *office being a domain, but could create each office as a tree.*
- > *Not sure of the tradeoffs.*
- > *– This will be a new installation with no legacy Windows 2000*
- > *servers, and primarily Windows XP clients with a few Windows*

- > 2000 clients and some Solaris and Linux servers.
- > – The total number of servers in each office will be between
- > 1 and 20.
- > – The total number of workstations in each office will be between
- > 5 and 100.
- > – I'd rather not pay for Windows servers that perform almost no
- > work, and only exist to serve as some sort of root-level domain
- > controller. Cost is definitely a major factor.
- > – We may need to create additional DNS levels without creating
- > additional Active Directory client domains. These sub-domains
- > will frequently not be running any Microsoft OSes. When they
- > are, we may be setting up a new forest/tree/domain structure
- > which is self-contained, and then creating trust relationships
- > with the main office AD configuration to support inter-
- > operability during development which can be severed once the
- > system is complete and is moved to a production facility.
- >
- > GUESSES:
- > – Eventually, each office should have either a top-level domain of
- > the form sfo.acme.com, dmz.acme.com, nyc.acme.com or a child
- > domain of acme.com of similar form.
- > – Additional domains within each office will either be created
- > within DNS without AD being aware of them, or as child domains
- > which match the 4-level DNS domain structure,
- > i.e. client1.sfo.acme.com, if they're big and long-lasting
- > enough to justify it.
- >
- > QUESTIONS:
- > – Do I create acme.com or sfo.acme.com as the first domain?
- > – If I create acme.com, I assume I would create sfo.acme.com as a
- > subdomain to match the DNS naming convention, but does this
- > mean I must run two separate Windows 2003 servers, one as the
- > primary domain controller of each domain, or can I have one
- > Windows 2003 server act as the PDC of both?
- > – We may not want to create additional Active Directory domains
- > for additional locations immediately. Is it possible to create
- > a nyc.acme.com domain from a DNS perspective without creating
- > a matching AD domain structure, but add the child domain at a
- > later point? Can one AD domain cover multiple DNS subdomains,
- > as long as they have a matching parent domain in common?
- > – If I do not want to pay for a Windows 2003 server that will
- > only run acme.com and can not really do anything else, it seems
- > like I might need to create a new tree for each secondary office
- > with sfo.acme.com being the first tree/domain. Correct?
- > – I'm just trying to find out what the best practice is for such
- > small company configurations. We need a DMZ for a secure web
- > presence, and will quickly connect two more offices. But
- > initially, due to a recent merger, cost is a factor which means
- > we must initially do this as cheaply as possible. We don't want
- > to create an AD configuration due to initial limits that can't
- > handle long-term needs however!

microsoft.public.win2000.active\_directory: Re: Help with initial small org AD setup convention when using DMZ network

>  
> *Please post all advice to this forum, and cc me if possible. Thanks in*  
> *advance!*  
>  
> *Mike*  
>