

## Re: Servers in two Vlans

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-10/0323.html>

---

**From:** S. Pidgorny (*slavickp\_at\_yahoo.com*)

**Date:** 10/27/05

Date: Thu, 27 Oct 2005 20:45:08 +1000

A good old Active Directory Replication Across Firewalls whitepaper (<http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/deploy/confeat/adrepfir.msp>) is a good start for the information. Refer to the "Limited RPC" section for a reasonable port list achieved with a minimal registry tweak. As an absolute minimum you can disable NetBIOS (requires Windows 2000 and up or Samba 3 clients) and not use SSL protocols or WINS, which results in the following list of protocols:

- \* RPC endpoint mapper – 135/tcp
- \* RPC static port for AD replication – <fixed-port-of your-choice>/tcp
- \* SMB over IP (Microsoft-DS) – 445/tcp
- \* LDAP – 389/tcp, 389/udp (the latter for LDAP ping)
- \* Global catalog LDAP – 3268/tcp
- \* Kerberos – 88/udp
- \* DNS 53/tcp, 53/udp

Plus, you need to be able to ping the DC from the workstation. Leaving ping open is generally not a bad idea anyway.

--

Svyatoslav Pidgorny, MS MVP - Security, MCSE

-- F1 is the key --

<chart@homesoc.com> wrote in message

news:1130338832.217307.167640@g43g2000cwa.googlegroups.com...

> Question #1

> I have a domain forest in my current WAN. I have been asked to tighten up security but implementing ACL's between VLAN's. My problem is this. I have say office A on VlanA with the main controller and office B on VlanB with a child controller. What ports am i going to have to open up between those vlans so the two servers can talk to each other and keep active directory happy.

>

> Question #2

> Would I need to open the same ports say if a workstation was on a different Vlan then the server it authenticates with. Not sure this would happen but just wanted to know in the event I run into that.

>

> I have all offices connected via Point to Point T1, switches are all Cisco 3550's and all servers are compaq DL series of one flavor or another.

>

> the goal is to open only the ports needed to have the server talk to each other and keep Active Directory working, allow clients to

microsoft.public.windows.server.security: Re: Servers in two Vlans

```
> authenticate and all that other sever functions and block everything  
> else  
>
```