

ESX 3.5 Behind a Firewall ...



[ejking](#) 16 posts since

Jan 5, 2009

Requirement

ESX server is on DMZ to be on HP hardware and VC(2.5) on the internal LAN. Server based licensing to be used and the Flex lic server is on the same server as VC

Ability to deploy software on ESX by use of ILO by Admins (both Console & Virtual media access)

Ability for the app support to remote to VM's in DMZ to manage VM's only and deploy software. Preferably if app support can load the app themselves and if not possible admin does it for them. mstsc/landesk/sms/dameware,etc is not allowed.

Ability to deploy software from Altiris RDP server which is inside the internal LAN

DNS name resolution to be allowed.

Company operates a strict policy and ports need to be kept to a bare minimum

Current Ports to be opened and solution that i can think off

ESX to Flex lic server (27000 & 27010), ESX to Vcenter/Web (443 and 903/UDP), VI to ESX(902&903), ILO to ESX(23 & 17988), DNS(53 TCP/UDP)

Other than adding IP helper ipaddresses on Switches is there any ports required for altiris RDP server VM deployment? Is the risk of using RDP more than the benefit?

App support team to be given access via "Generating Remote Console URL" for VM's on VC. And admin teams put the software for them on VM's. Is there a better solution to this?

If we used host based licensing, would 27000 and 27010 still needs to be open on the firewall

Suggest any ports that can be added or removed, or anything else usefull. Thanking you



[AndreTheGiant](#) 5,916 posts since

Aug 28, 2008 1. **Re: ESX 3.5 Behind a Firewall** Jun 14, 2009 8:08 AM

I suggest you to use a VPN system.

I more secure and you have (usually) open a single port.

Andre

**if you found this or any other answer useful please consider allocating points for helpful or correct answers



[wila](#) 3,266 posts since

Jun 27, 2006 2. **Re: ESX 3.5 Behind a Firewall** Jun 14, 2009 8:20 AM

Hi,

You should really not open any of those ports to the internet.

ESX 3.5 Behind a Firewall ...

Use VPN as Andre suggest or SSH to forward your ports to the host instead using an external firewall.

If you cannot add an external firewall for whatever reason, then you could set up a firewall VM, have it autostart with the host and route your traffic through there.

--

Wil

Visit the VMware developers wiki at <http://www.vi-toolkit.com>



[ejking](#) 16 posts since

Jan 5, 2009 3. Re: **ESX 3.5 Behind a Firewall** Jun 17, 2009 12:39 AM

👤 in response to: [AndreTheGiant](#) Thanks your opinion that i will now be considering. Much appreciated



[AndreTheGiant](#) 5,916 posts since

Aug 28, 2008 4. Re: **ESX 3.5 Behind a Firewall** Jun 17, 2009 8:57 AM

👤 in response to: [ejking](#) You're welcome.

Andre



[Texiwill](#) 10,205 posts since

Jan 13, 2004 5. Re: **ESX 3.5 Behind a Firewall** Jun 27, 2009 7:12 AM

👤 in response to: [AndreTheGiant](#) Hello

Moved to Security Forum.

Ideally you want something like this:

Home <-> Internet <-> FW <-> DMZ <-> FW <-> Production <-> FW <-> Management Network (VC + SC + VIC workstation)

Yes you want that many firewalls. The idea is that you use a VPN to cross the boundaries as necessary. You NEVER want to place your SC/VC/VIC within your DMZ or out on the internet. You could do something like the following to gain the access you need.

Home <-> VPN <-> Management Network

Check out http://www.vmware.com/files/pdf/dmz_virtualization_vmware_infra_wp.pdf

Best regards,

Edward L. Haletky VMware Communities User Moderator, VMware vExpert 2009, [Virtualization Practice Analyst](#)

Now Available: '[VMware vSphere\(TM\) and Virtual Infrastructure Security: Securing the Virtual Environment](#)'

Also available '[VMWare ESX Server in the Enterprise](#)'

[SearchVMware Proj](#)| [Blue Gears](#)| [Top Virtualization Security Links](#)| [Virtualization Security Round Table Podcast](#)