Testing New Applications In The DMZ Using VMware ESX

Ivan Dell'Era

Software Engineer

IBM

VMWORLD 2006

Agenda

- Problem definition
- Traditional solution
- The solution with VMware VI
- Remote control through the firewall

Problem Definition

- A new product or service being actively developed and tested needs to be accessible from the Internet
- It requires the installation of one or more servers in the DMZ (in this presentation we assume several, however the problem is similar if you only need one server)
- Your administrator is already familiar with VMware and you'd like to leverage this technology
- Your company security standards allow only for restricted access from the DMZ to your intranet and vice versa
- Your testing needs do not necessarly allign with the DMZ administrator timeline for installing the servers

Wikipedia definition of DMZ:

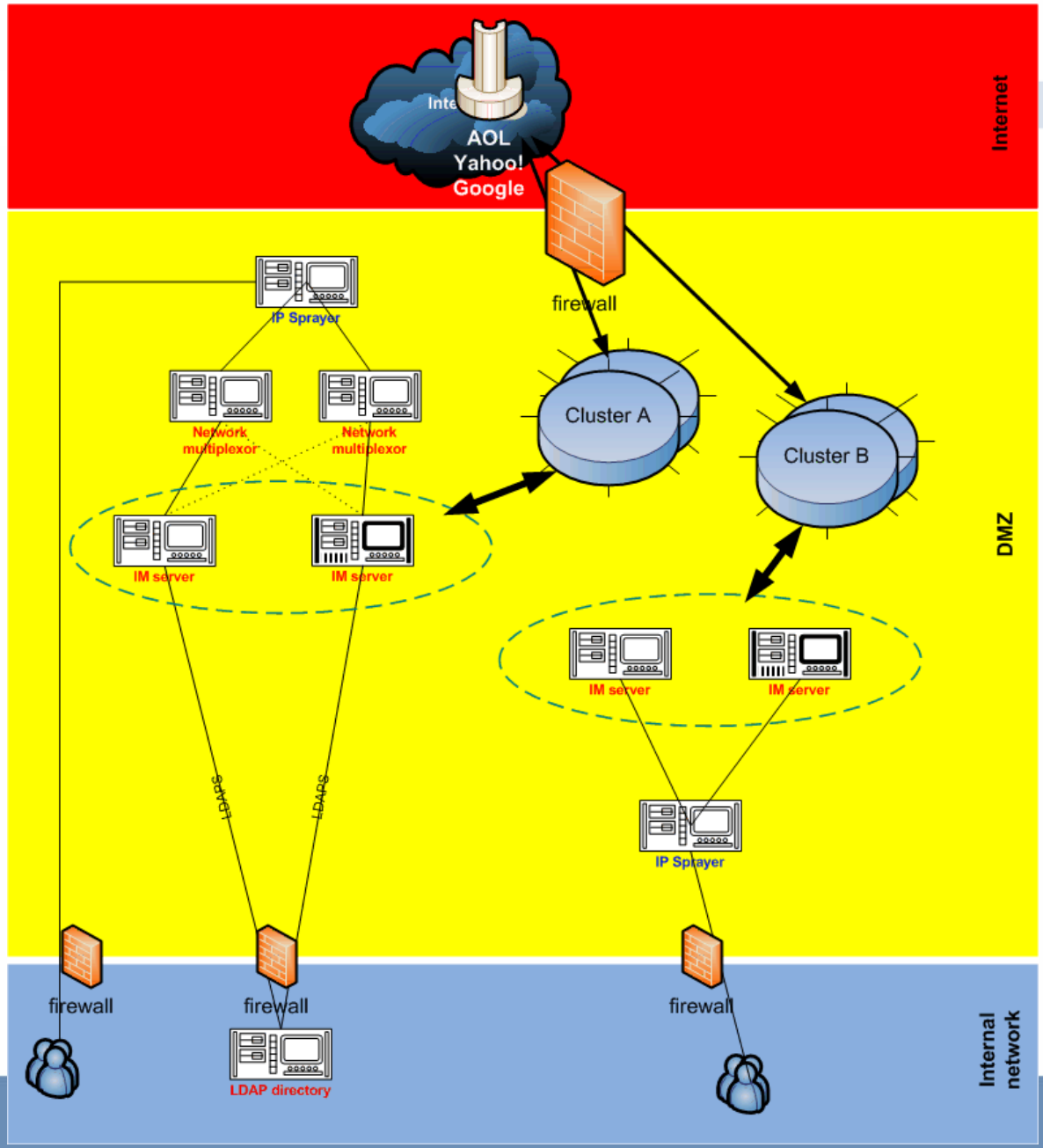
> *DMZ is a network area that sits between an organization's internal network and an external network, usually the Internet.*

Classic pre-VMware solution and dilemma

- Dedicated servers needed to be installed and configured in the DMZ
- It would require you to burn CDs in order to copy files and install new applications on the servers in the DMZ
- It was difficult to simulate applications without installing them in the DMZ
- After installing applications in the DMZ, it was difficult to apply changes (i.e if one of the application needs more resources than planned originally)

A practical example

- Clustered servers that connect and accept ecnrypted connections from the internet
- These servers need access to other resources inside your internal network (i.e. Directories of users and groups)
- In a dynamic development environment, requirements can evolve from what was planned vs what is feasible
  - Often limited control is available on what 3rd parties can provide


Internet
AOL
Yahoo!
Google
firewall
IP Sprayer
Network multiplexor
Network multiplexor
Cluster A
Cluster B
DMZ
IM server
IM server
IM server
IM server
LDAPS
LDAPS
IP Sprayer
firewall
firewall
firewall
LDAP directory
Internal network

Planning

VMWORLD 2006

The 3P rule

- **P**lanning in advance will prevent problems later
  - Schedule time to move servers, install, patch as usual, but keep in mind what may be specific to your company security requirements for servers in the DMZ
- **P**ort requirements: clearly state what services need to be accessible from the internet and intranet
  - Specify which servers should be accessible on the internal network
  - Also specify which internal servers should have access to the server(s) in the DMZ Prepare a network diagram with ports you need and seek approval of your network administrators **and** DMZ security team
- A **P**icture is worth 1,000 words, make sure to also specify ports used along with hostnames
  - Summarize all requirements in tables with details from:
    - Internet to DMZ and DMZ to internet
    - DMZ to intranet and intranet to DMZ

VMware specifics

- Don’t forget VI ESX specifics ports!
  - Port 22 for ssh and scp to your ESX server
  - Port 902 for Virtual Center access and for Virtual Machines console
- nfs, ftp and Windows share should not be used as they are potentially insecure
  - Most likely your company DMZ security requirements do not allow for these services anyway (even if they don’t, you’re better off keeping them disabled anyway)

Document everything

- Keep a reference manual of every port, connection and rule set on the firewall
- Very important when troubleshooting access issues
  - Is it a bug in my application or is the firewall blocking the connection?
- It can be used as documentation by new people involved in the project to become familiar with the infrastructure

The $10K question

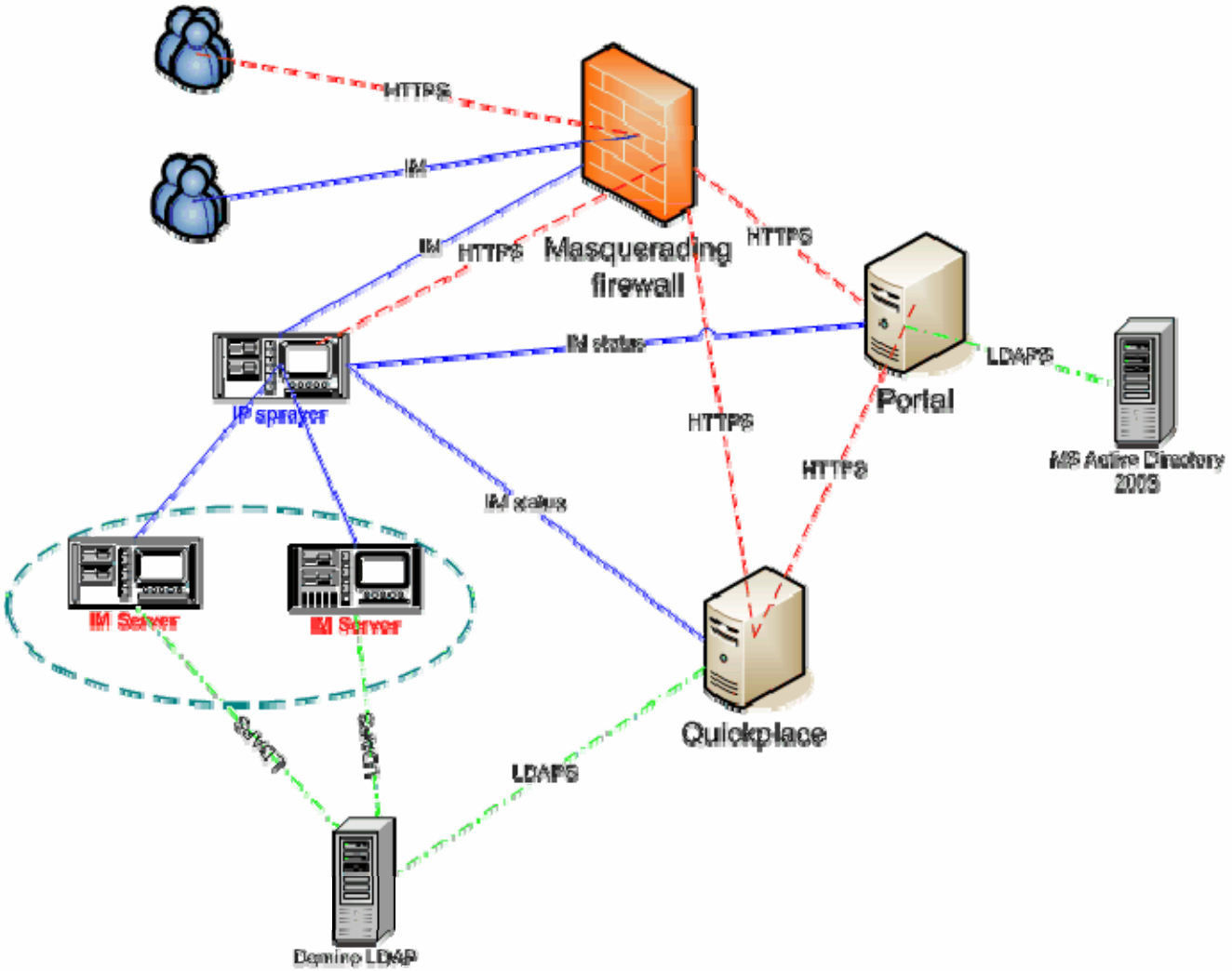
- My company DMZ is hosted in the same lab where I have other VMware ESX servers. What if I connect the service console to my intranet and the other NIC(s) to the DMZ network?

- Run this by your security team first.
  - Most likely they'll say no.
  - Even if they don't say no, consider the risk of a PC bridging the internet to your internal network: do you really want this?
  - All you need to use your ESX server remotely is port 22 and 902, both are SSH encrypted.
    - Make sure you have a strong authorization policy and audit in place

Before you install your server in the DMZ

- Leverage your investment, use VMware ESX Server to simulate a DMZ environment before you move your infrastructure to the DMZ
- Try to simulate the DMZ environment in your lab
- This allows to find application dependencies and allows to identify what is required in the DMZ
  - How many VMs are needed?
  - What services are accessible in the internal network?
  - And what is forbidden?

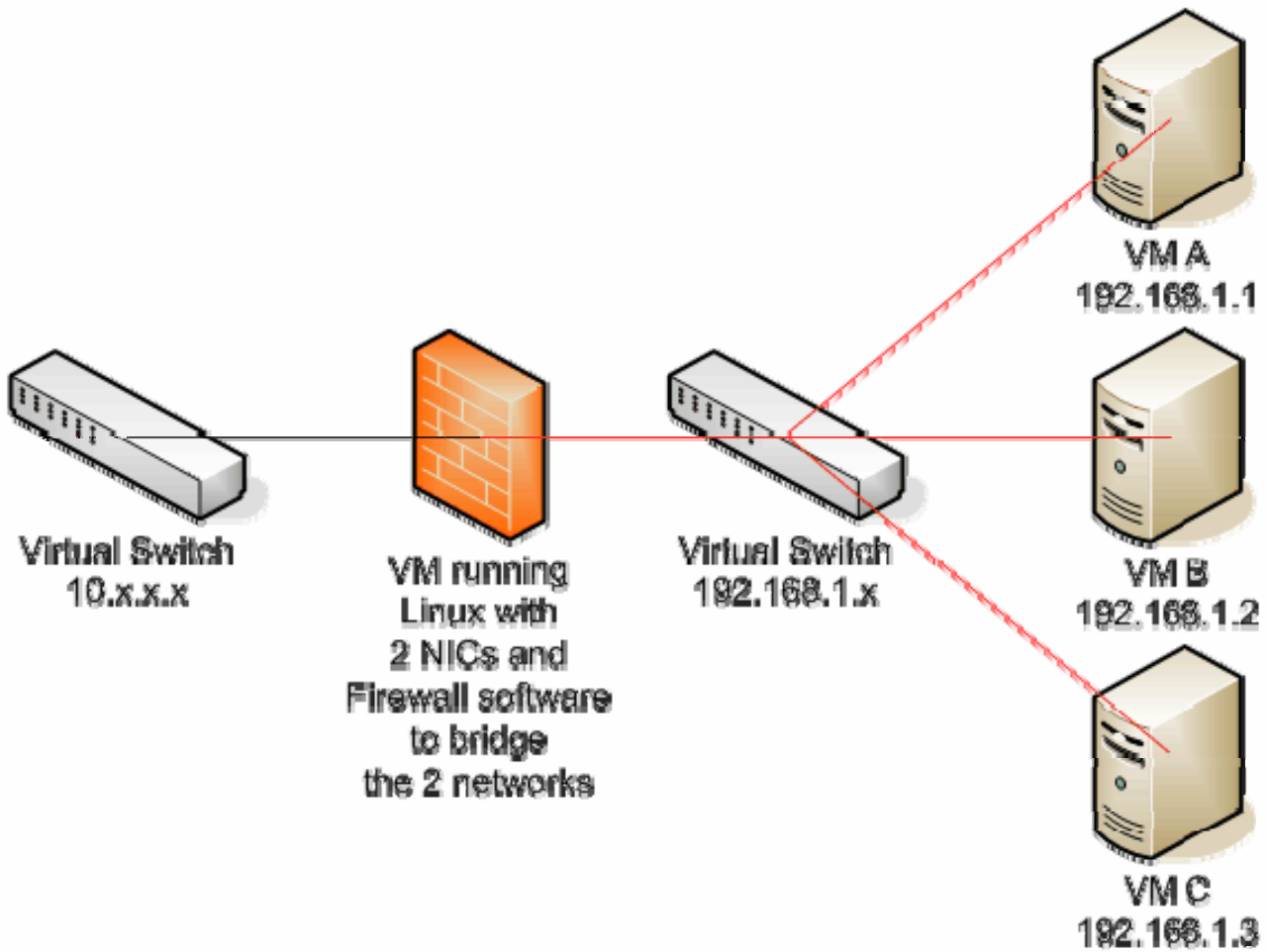
Sample infrastructure diagram



How it looks from a VMware point of view

- You'd create 2 Virtual Network switches
- Connect only one virtual switch to your network (i.e. Assign a physical NIC only to this one)
- Assign 2 NICs to a Linux VM that runs a firewall
  - The firewall will need to be configured to bridge the connections, allowing only the ports you need to be open
- The Linux VM connects to both Virtual Switches
- The other VMs only connect to the internal Virtual Switch (the one without any physical NIC assigned to it)

How it looks from a VMware point of view



Tips

- Make sure you use the same IP settings you'd use in your DMZ, this way you don't need to change the configuration after deploying in the production environment
  - Use the OS host file in your VMs for temporary IP address mapping to override DNS entries
- Make sure you set the same port filtering on the firewall VM as you'd have with the internal facing DMZ firewall
  - This will simplify the configuration when you move the VMs in the DMZ
- Also important: define how many concurrent connections you expect to all your VMs and verify your firewall can support them

Remote Access

VMWORLD 2006

How to securely control Virtual Machines

- It all depends on how strict the rules are on the internal facing DMZ firewall
- In general you have at least ssh that is allowed from the intranet to the firewall and from the firewall to the Virtual Machines
- Most likely Remote Desktop Protocol (RDP, port 3389) is disbled
- Also VNC (port 5900+) may be disabled as only some VNC implementation are secure and encrypted
- If you have port 902 open on the intranet facing firewall (you didn't forget to ask for it to be open, did you?) you can use it to control the Virtual Machines in the DMZ, but what if only a restricted subnet can access the DMZ network?
- VMware remote console can work if port 902 is open, however other methods can offer better performance

VPN without VPN to your Virtual Machines

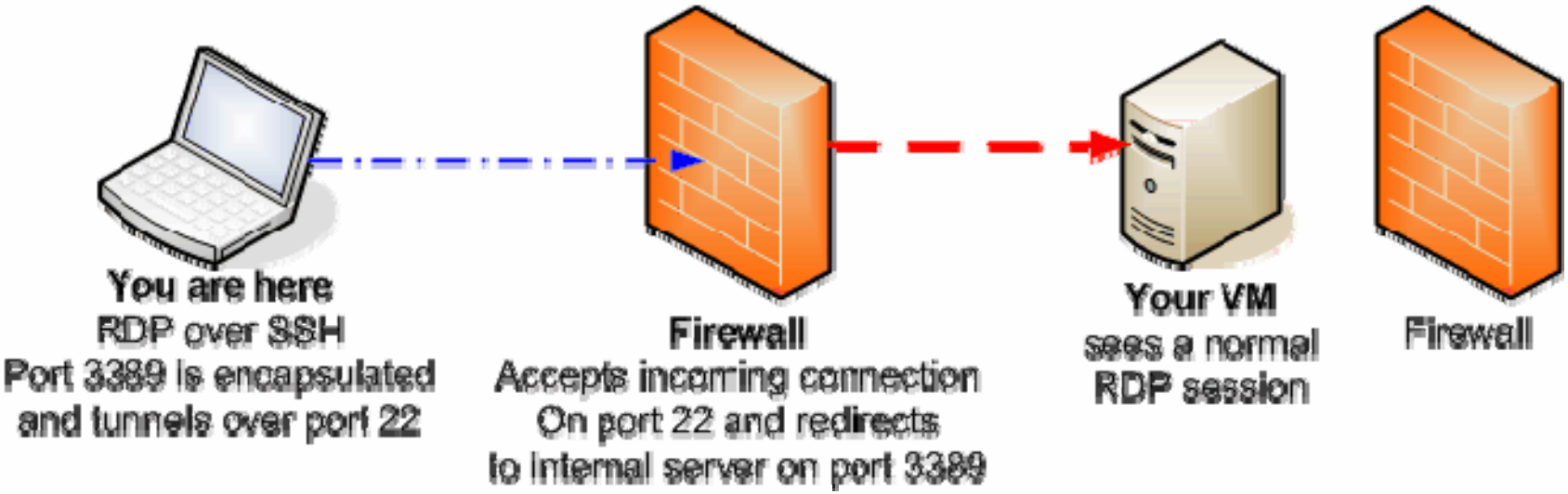
- If you can SSH to your firewall (or a server that is trusted by the firewall to access the whole DMZ) you can do anything
  - You can tunnel almost anything over SSH
  - SSH is encrypted
  - By tunneling, you have an encrypted communication channel to your environment
  - Very useful if you want to use Remote Desktop Protocol (RDP, aka Terminal Services, Remote Desktop Connection) or VNC
- Why should you care?
  - If you can't have yet another port open on your firewall to access your virtual (or physical) machines.

From Wikipedia

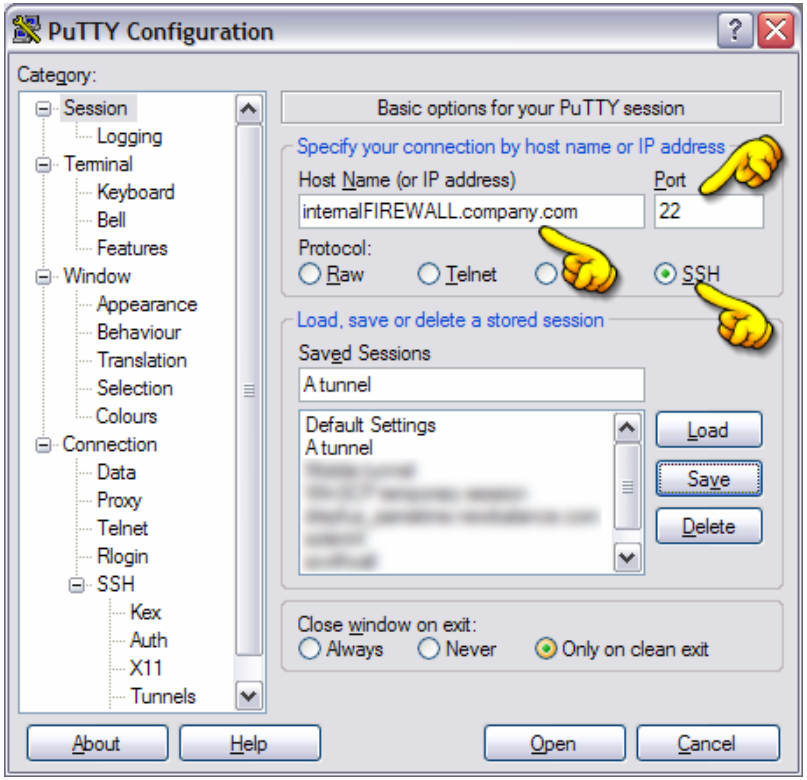
- Tunneling protocol: transmitting one computer network protocol that is encapsulated inside another network protocol
- SSH: Secure Shell is a set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer

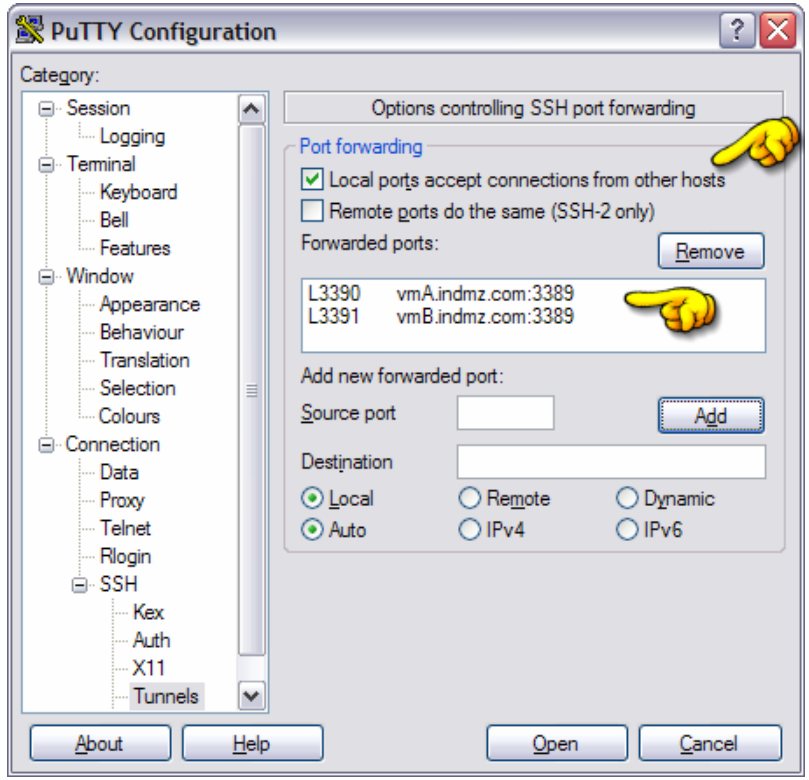
Tunneling over SSH using putty

- Putty is a free SSH client for W32 available from: http://www.chiark.greenend.org.uk/%7Esgtatham/putty/
- Tunneling instructions for RDP: http://www.engr.wisc.edu/computing/best/rdesktop-putty.html
- Tunneling instructions for VNC: http://www.maths.utas.edu.au/People/Hill/vnc/vnc.html



Putty example

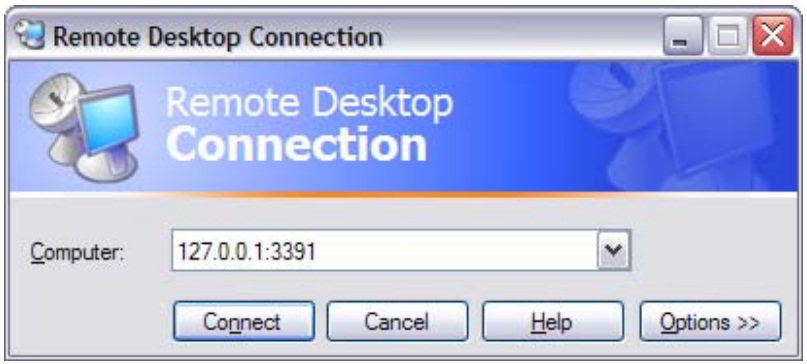




Share Putty's tunneling profile

- With Putty you can enter multiple tunneling at once
  - Each must have a different local listening port
- Once you have created a profile with all required settings for tunneling, export the settings to a registry file
- Putty.exe saves its profiles to: HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\
- Create a handy table that lists local ports and destination machines:

use this in remote desktop	**to connect to this VM**
127.0.0.1:3390	vm-a.yourdomain.com
127.0.0.1:3391	vm-b.yourdomain.com

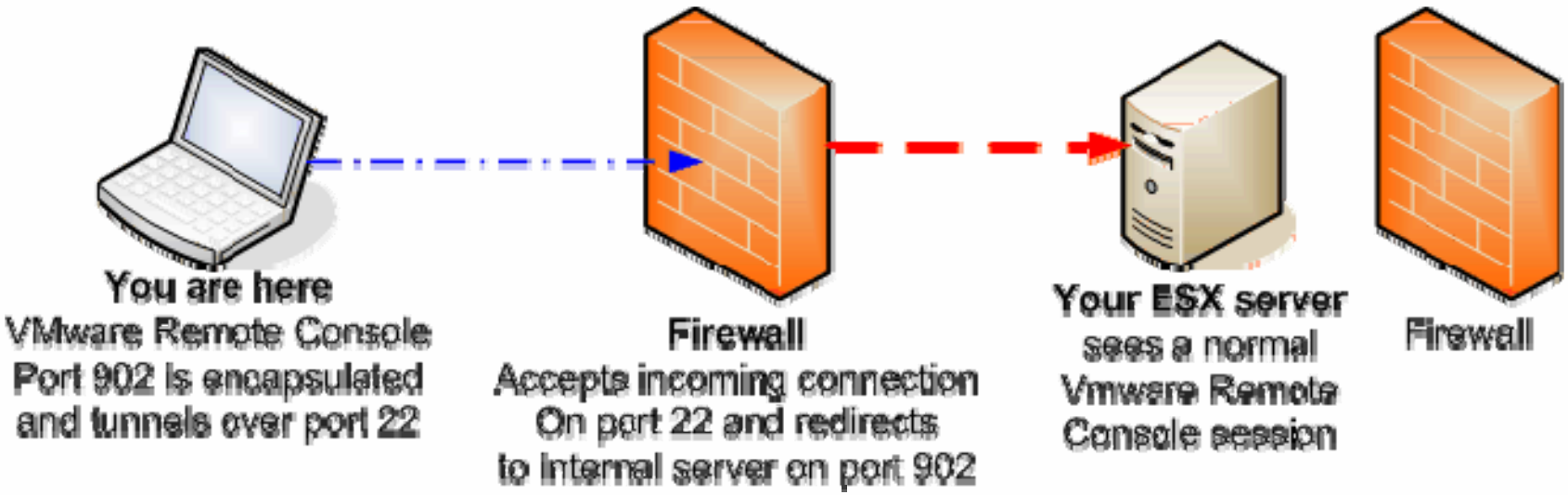


Tunnelling using the command line

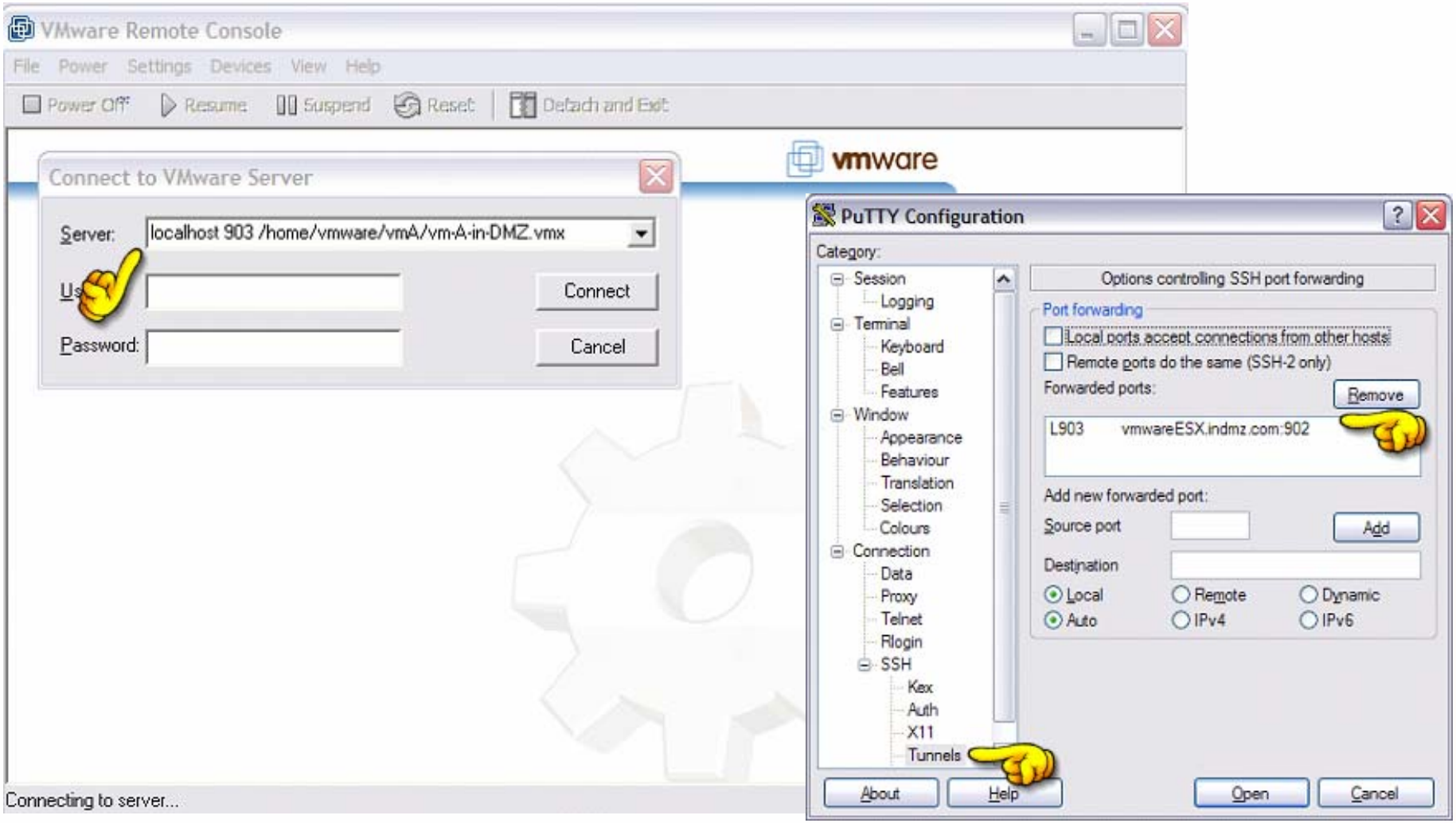
- Real Geeks never use a GUI – everything must be done using a command line
  - Install OpenSSH – availabe in your Linux distribution and from http://cygwin.com/ for W32
- From a Windows XP SP2 machine:
  - ssh -l loginname -L 3390:vmA.indmz.com:3389 internalFIREWALL.company.com cat –
- From a Windows XP SP1 machine:
  - ssh -l loginname -L 127.0.0.2:3390:vmA.indmz.com:3389 internalFIREWALL.company.com cat -

Tunneling VMware Console

- Conceptually identical to the RDP tunneling
- In VMware Remote Console change the hostname to localhost and port to match the local port selected for initiating the tunneling (i.e. 903):
  - localhost 903 /home/vmware/myremotedir/myremotevm.vmx

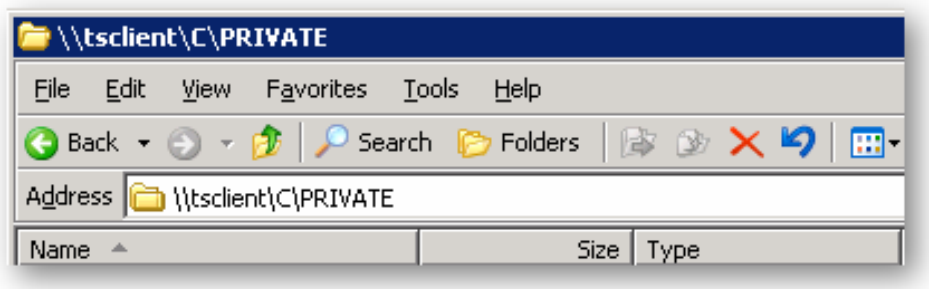


Example with VMware Remote Console



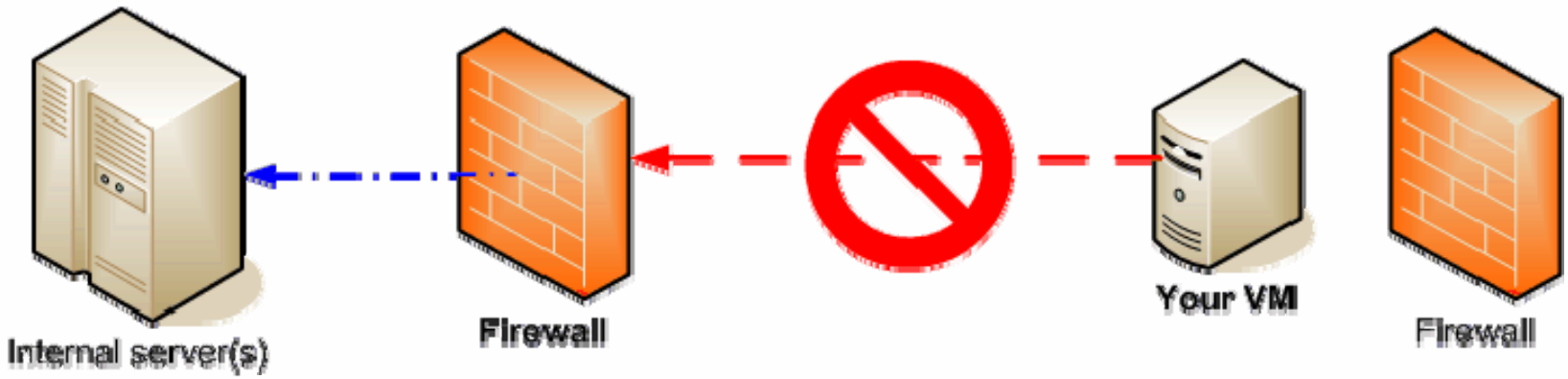
Copying files to/from your W32 Virtual Machines

- You should assume you can't – at least directly
- If you tunneled RDP, you can use what RDP offers to move files around
  - Your local drives will be available on the remote machine for the timeof the connection
  - TIP: mount any share you need to your local machine first, then you can copy files to your VMs inside the DMZ



Tunnelling from DMZ to your network is not a good idea

- Big security warning: why would you want to trust your DMZ and give it open access to your internal network?
- It's OK to allow some services from specific VMs over specific protocols to a specific host (i.e. LDAP over SSL for authentication)
  - This however requires to document the need and coordinate the request with your firewall administrator
- While it's possible, it's not a good idea to have your disk storage in your internal network



Other Considerations

What about Virtual Center?

- If you have port 902 available from VC to the DMZ, you're all set
- If you don't, you should ask to have it open from VC to your VMware servers

- For VI 3.x licensing becomes an issue to consider
- Even if VC can access the ESX servers, it doesn't mean the reverse is true
  - Often ports are open only from internal to DMZ network
  - You may have to export the license to a file, or
  - Install a separate VC server in the DMZ

Security requirements for your Virtual Machines

- Create a VM with the OS and patches you need
- Modify security settings as required by your corporate security guidelines
- At a minimum you want to have a password policy which disallows simple passwords and with expiration and lockout in case of too many unsuccesfull logon attempts, along with audit of all attempts

Deploying your Virtual Machines in the DMZ

- If you have port 902 open, at least from the Intranet connecting to the DMZ, you can use Virtual Center to clone or migrate your Virtual Machines
- Most likely you'll have to use local storage, unless you have a SAN in your DMZ
- If the DNS in the DMZ only knows about internet hosts, you need to use the hostfile to make your Virtual Machines aware of each other
  - Prepare a master list of hostnames and IPs and copy it to the Virtual Machine used as a template for cloning

Summary

- Plan in advance
- Document your needs
- Prepare to be flexible
- Tunneling is really your (only) friend – take the time to learn it
  - It realy works and it’s easier than it may seem – once it clicks, you will find more and different ways to use it

Questions?

Presentation Download

Please remember to complete your
session evaluation form
and return it to the room monitors
as you exit the session

The presentation for this session can be downloaded at
http://www.vmware.com/vmtn/vmworld/sessions/

Enter the following to download (case-sensitive):

Username: cbv_rep
Password: cbvfor9v9r

VMWORLD 2006