Consultancy Report for a secure Virtual Infrastructure

Authors:
Berry Hoekstra - berry.hoekstra@os3.nl
Niels Monen - niels.monen@os3.nl

Research Project 1:
Virtual Infrastructure Security

Version 1.0
02-05-2010

BELNET
Universiteit van Amsterdam - SNE/OS3

Abstract

BELNET (the Belgian National research and education network) is a Belgium ISP that mainly focuses on research institutions. They are currently working on the migration of their physical servers to a virtual environment.

BELNET wants to know what type of security issues they can expect from such a migration. This report discusses the relevant aspects that can potentially lower the security level of BELNET's infrastructure while migrating to a Virtual Infrastructure.

Topics like the security of hosts, guests and Virtual Center come by. The report also discusses monitoring and auditing of the security state, iSCSI security, updating and firewalling.

Table of Contents

Introduction

BELNET (the Belgian National research and education network) is a Belgium ISP that mainly focuses on research institutions. Beginning in 1989, BELNET provides web services to higher education, federal departments, federal ministries, and international organisations. [1]

BELNET is currently working on the migration of their physical servers to a virtual environment. A setup is already in place. This setup exists of physical blade servers running VMware ESX 3.5. They consider this as their Virtual Infrastructure. BELNET wants to know what security related issues to take into account when migrating to the Virtual Infrastructure. [2]

In this report, we won't go into detail on how the VMware virtualization technology works, as BELNET already has the in-house knowledge for this. We will mainly focus on the scope of the project, which consists of researching security related issues on a virtualized platform, based on virtualization technology by VMware.

Problem definition

Migrating an existing physical environment to a virtual one is already done before. Taking the step to virtualize the physical servers might be considered easy, but one has to take several things into account to successfully migrate from a physical to a virtual environment. For instance, security is an important aspect of a virtual infrastructure.

BELNET's goal is to successfully implement a secure virtual infrastructure. A virtual infrastructure that serves hosts in different logical network segments poses a security and maintenance challenge. The goal of this project is to write a report that contains recommendations for the setup of such an infrastructure. The report will mainly focus on the security aspects of setting up such a virtual infrastructure. To do this, we defined some key research questions.

Research questions

For a successful implementation of security policies in BELNET's virtual infrastructure, we defined one main research question and multiple key sub-questions to help answer the main question.

Main question

What is the best way to successfully implement a virtual infrastructure while dealing with all possible security (related) issues?

Sub-questions

We defined sub-questions to help answer the main research question above.

- What level of firewalling should be implemented? (What level of strictness, etc.)
- Does the use of different passwords for each virtual host heighten the security level?
- Does the use of Virtual Datacenters and Clusters have any impact on security?
- What is the risk if a compromised virtual machine is able to gain access to the virtual infrastructure itself at the ESX or Virtual Center level?
- How can the security state be audited and monitored?

To answer the questions above. We're discussing the research done in the following chapter.

Research

In this chapter, we're going to look into the setup of a virtual environment and the security implications such an environment comes with.

Existing setup

BELNET already has multiple virtual servers setup. They consider the main servers as their Virtual Infrastructure.

Virtual Infrastructure

The Virtual Infrastructure consists of multiple physical blade servers installed and configured with VMware ESX 3.5. Generally, an environment running on VMware ESX 3.5 (and other products) is called VMware Virtual Infrastructure 3.

The Virtual Infrastructure is managed with VMware Virtual Center. This is actually a VM running on one of the ESX servers.

BELNET currently has 10 blade servers running under VMware ESX 3.5. These serve as the virtual production environment. For testing purposes, they have 2 blade servers running on VMware vSphere.

Besides the main ones, there are also a few servers running VMware ESXi and VMware Server. These servers are used to host test machines.

As the virtual servers contain virtual machines (VMs) that each has specific requirements for networking access, there's research to be done.

BELNET needs the virtual infrastructure to be able to provide access to all the various VLANs. But it is not needed that each individual ESX server actually has access to all VLANs. Some of them only host servers running in the DMZ, while others host internal servers. [2]

Used solutions
VMware has developed several solutions for setting up and managing a virtual infrastructure. The solutions that BELNET has already implemented are the following products:

Products in the main production environment:

- VMware Infrastructure 3.5
- VMware ESX 3.5
- VMware Virtual Center

Products used for hosting test machines:

- VMware ESXi
- VMware Server

Products used for testing VMware vSphere:

- VMware vSphere
- VMware vCenter

Current setup
BELNET currently has the following setup: [13]

- Main Datacenter
  - External Cluster
    - esxblade5.fw.belnet.be
    - esxblade6.fw.belnet.be
    - esxblade9.fw.belnet.be
  - External Test Cluster
    - esxblade7.fw.belnet.be
  - Internal Cluster
    - esxblade1.fw.belnet.be
    - esxblade2.fw.belnet.be
    - esxblade3.fw.belnet.be
    - esxblade4.fw.belnet.be
- Test Datacenter
  - Scarlet Cluster
    - esxblade10.fw.belnet.be
    - esxblade8.fw.belnet.be

As stated before, they have 2 additional blades for testing vSphere.

- vSphere Test Datacenter
  - Test Cluster
    - esxblade11.fw.belnet.be
    - esxblade12.fw.belnet.be

The servers in the Test Datacenter aren't part of the Virtual Infrastructure, because their main purpose is to test vSphere. They are completely separate from the other Datacenters.

The vSphere test environment is managed using vCenter, which is actually a VM running on the host, just like the Virtual Center server.

The picture below visualizes the BELNET Virtual Infrastructure.

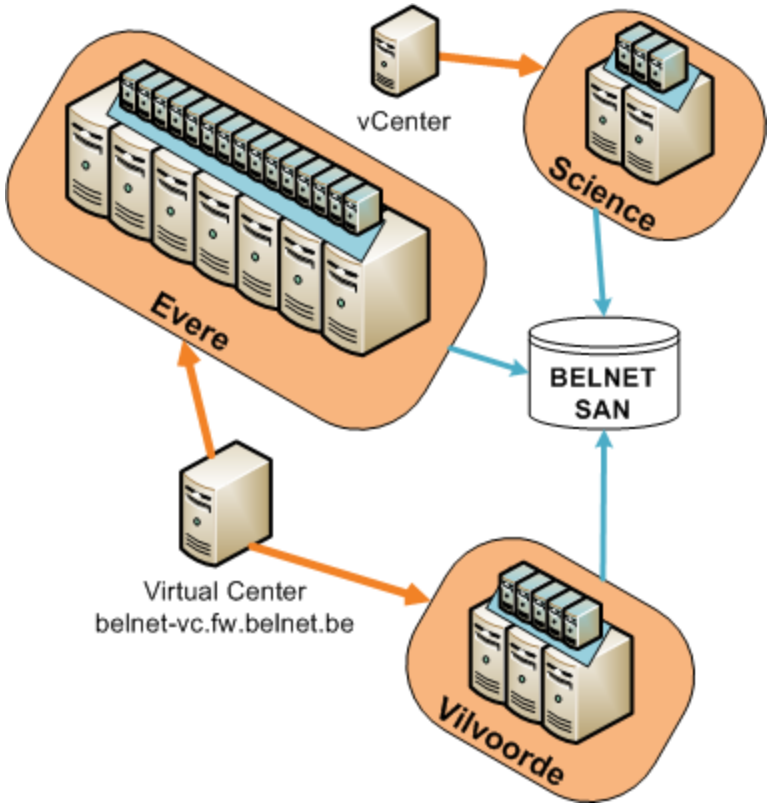

Figure 1 - BELNET Virtual Infrastructure sites [2]

The Evere and Vilvoorde "locations" are the Virtual Infrastructure, while the Test Datacenter is located at the Science "location". All locations are connected to the BELNET central SAN storage system.

VMware

Replacing physical servers with virtual ones that perform the same tasks and are configured in the same way, enables server consolidation greatly. Server resource utilization will be at a much higher level which results in, for example, much lower hardware and electricity costs.

If replacing most of your physical servers with virtual ones, like described above, you can keep relying on your existing network configurations like with a physical infrastructure. The OS configurations will also remain intact.

However, according to VMware, if you recreate a physical infrastructure as a virtual one, and do not run VMs of different trust zones together on one host server, the degree of consolidation you can achieve can remain low. [8] Also, some people believe that the virtualization of an infrastructure with different trust zones (DMZs), can cause security problems. [8,9]

So, to keep server consolidation at a high level, servers of different trust zones must be running across the available ESX servers. The best solution is to list all available (and active) VMs. Sort the VMs according to the trust zone's they're running in, or will be running in. If all VMs are categorized based on the DMZs, spread them across the ESX servers while keeping as much VMs of different trust zones on the same ESX server. This way, a high server consolidation is created, while maintaining DMZ consistency.

Hosts

In a virtual environment, the physical servers hosting the VMs are called "hosts".

VLANs
Like the name suggests, you can create multiple Virtual LANs on a network. If VLANs are implemented on a network, policies (ACLs) can be easily applied to each VLAN to create security policies on each virtual network.

VLANs are implemented on the routers and switches. VLAN tagging can be done on port level. So packets have to be tagged (by appending the 802.1Q headers [7]) on the ports the ESX blade severs are connected on. If this is properly configured on the side of the routers and switches, the host can make use of each VLAN for the VMs.

To configure VLANs on a VMware host server, you have to configure them in Virtual Infrastructure Client or in the vSphere Client. It might be possible to configure one machine and consolidate others with the configurations of the "template" machine, but that falls outside of the scope of this report.

Firewalling
The following table shows the firewall rules applicable to the hosts running VMware. To maintain strict network policies, all ports should be blocked, except for the ones in the table. Additional strictness can be applied by providing source IP addresses or ranges that may connect.

Port	Protocol	From	To	Description
21	TCP	FTP Client	ESX	FTP
22	TCP	SSH Client	ESX	SSH (enable manually on ESXi)
53	UDP	ESX(i)	DNS Server	DNS
123	UDP	ESX(i)	NTP Server	NTP Client
161	UDP	ESX(i)	SNMP Server	SNMP Polling
162	UDP	ESX(i)	SNMP Server	SNMP Trap Send
427	TCP	vSphere Client /web access	ESX(i)	SLPv2 for auto services detection
443	TCP	vCenter/ vSphere Client/web access	ESX(i)	HTTPS
902	TCP	ESX(i)	vCenter/ vSphere client/web access	
902	UDP	ESX(i)	vCenter/ vSphere client/web access	xinetd/vmware authd for authentication
2050 - 2250	TCP	ESX(i)	ESX(i)	High Availablity between hosts
3260	TCP	ESX(i)	iSCSI SAN	Software iSCSI Client & Hardware iSCSI HBA
5989	TCP	vSphere Client /web access	ESX(i)	CIM transactions for
8042 - 8045	TCP	ESX(i)	ESX(i)	High Availability between hosts

Figure 2 - Firewall rule table for VMware host servers [21]

Other services like web services that are available on the network should also be implemented in the firewall rules.

Security
As extra security measurements you can set a password on some entries in the bootloader (GRUB), so people can't boot into the single user mode. In the single user mode, a user can change the root password and reboot into normal mode to access the service console. This is only needed on ESX hosts and not for ESXi hosts, this because ESXi doesn't have a service console. [3]
Another security measurement is to create custom roles for the Infrastructure/vSphere client. The security aspect of this is to minimalize the use of the root user. [3]

After a host is completely installed, configured and added to the pool, it is important to enable root lockdown mode. This mode disables remote root access to the host. Additional users with less privileges than the root user can then only manage the VI remotely. [3]

Limit the resources
It is recommended to set the resource reservations and limits on the host. ESX has to be configured so that a VM can always receive at least 10 percent of the host's CPU resources, but never more than 20 percent. This to avoid a Denial-of-Service on a virtual machine taking down the whole host. Of course, exceptions can be made for particular guests. [3]

Limit VMware log files
Each virtual machine stores troubleshooting information to a log file on the VMware VMFS volume. Those log files can be abused by users and processes by flooding these log files. Over time, this can consume all the space of a hard disk causing a Denial-of-Service so the virtual machines can't write to the datastore anymore.
To prevent this, you can limit the size and number of log files. VMware recommends limiting the log files to 100KB, and save a total of 10 log files. This should be sufficient for debugging most problems. [3]

Guests

In a virtual environment, the VMs running on a physical host are called "guests". BELNET has VMs running both Windows and Linux.

VLANs
As you could read earlier on, the VLANs are configured on the host servers, and assigned to the virtual NICs of each guest.

Linux/UNIX
On a Linux OS, you can assign multiple IP addresses to one NIC. You can do this by creating an IP alias. An interface is copied in the configuration and separated from the main interface by adding a colon (:). The interface with an IP alias can be called *eth0:1* for instance.

To implement multiple VLANs on a Linux host, a sub adapter can be configured. This can be done by adding a dot (.) to the configuration and configuring the VLAN on that port. *eth0.100* for example, has VLAN ID 100 on the eth0 NIC.

On Debian-based distributions, edit the following file: /etc/network/interfaces
On Redhat-based distributions, create a new ifcfg-eth0:xxx file in the following directory: /etc/sysconfig/network-scripts

On VMware, it is only possible to configure one VLAN per virtual NIC. This isn't a problem though, because it is possible to configure up to 4 virtual NICs for a Linux guest on VMware ESX 3.5 and up to 10 virtual NICs on VMware vSphere. [7] Each virtual NIC can then be configured on a specific VLAN.

Windows
For machines running a Windows OS, it depends on the drivers used. However, most of the drivers support multiple VLANs on one NIC. They support this by adding a virtualized NIC from the physical NIC to the network configuration, which can be configured independently.

If you want to use VLANs on a Windows OS, you can only configure one VLAN on a virtual NIC. If you want to put a Windows VM in multiple VLANs, you have to allocate the same amount of virtual NICs for that VM.

Passwords
To secure the guest machines you of course use passwords. While you could think different passwords for every machine is more secure, some sources [16] say it sometimes is counter effective. The argument for this is: "Users have trouble remembering many passwords, so they will write them down. The security is reduced to the physical security of a piece of paper." [16]
However, when every machine has a different password and one gets compromised, not all the other machines can be accessed.

So, it comes down to the following:

- One password for all: as secure as the least secure system on the network.
- Different passwords: as secure as a piece of paper.

However, you can use different passwords if you can save them easily and encrypted. There are some tools for this purpose, like *Keepass* [18].

Firewalling
We advise to treat a virtual machine just as a physical machine. So for maximum security, only allow the needed services to connect to or from the Internet. This can be done by a hardware firewall, or a software firewall on the machine itself. For Windows, the build-in firewall is sufficient. For Linux there is, for instance, iptables available.

Another recommendation is to disable all unnecessary functions like unused virtual devices (CD/DVD-ROM and floppy drive). Disabling unused services and turning off screensavers and X Window systems (if not needed) on Linux based systems is also recommended. [3] The reason for this is that every program has its flaws. Also, the less services and programs running, the less exploits can be used.

Templates
To ensure you install a secure operating system every time, you have the option to use templates. In such a template you can install a hardened base operating system image. This means there are no applications installed in this template. If you create a virtual machine with such a template, you always create one with a known baseline level of security. Because templates can be converted to virtual machines and back quickly, you can keep those templates up-to-date with patches and security measures.

Updating
A secure operating system means updating frequently. VMware created Virtual Center/ vCenter Update Manager to update Windows and Linux guests, templates and the ESX hosts. With this manager you can schedule updates which it will automatically install on the guests. It can update online and offline virtual machines, so even machines that are turned off are secure when turned on again.
For this to work, there is an Update Agent that should be installed on the guests. Also, some additional ports should be opened from and to several servers.

The Virtual Center/vCenter Update Manager will periodically check Metadata Servers on shavlik.com and/or vmware.com for updates. If updates are available, it will get them off content servers from Independent Software Vendors, or AKAMAI, which is a large content distributor that provides the content data from locations all over the world.

The table below shows ports that need to be opened in the firewall in addition to the previous table.

Port	Protocol	From	To	Description
80	TCP	ESX(i)	Update Manager	ESX(i) connects to port 80, which the reverse proxy will forward to port 9084
80	TCP	Update Manager	www.vmware.com	Update Manager obtains the metadata for the updates
80	TCP	Update Manager	xml.shavlik.com	Update Manager obtains the metadata for the updates
443	TCP	vCenter	Update Manager	vCenter connects to port 443, which the reverse proxy will forward to port 8084
443	TCP	Update Manager	www.vmware.com	Update Manager obtains the metadata for the updates
443	TCP	Update Manager	xml.shavlik.com	Update Manager obtains the metadata for the updates
902	TCP	Update Manager	ESX(i)	The Update Manager connects to the ESX(i) Server on port 902 for pushing VM patches.

Figure 3 - Additional firewall rule table for Update Manager [21]

The following image shows the Update Manager Infrastructure:

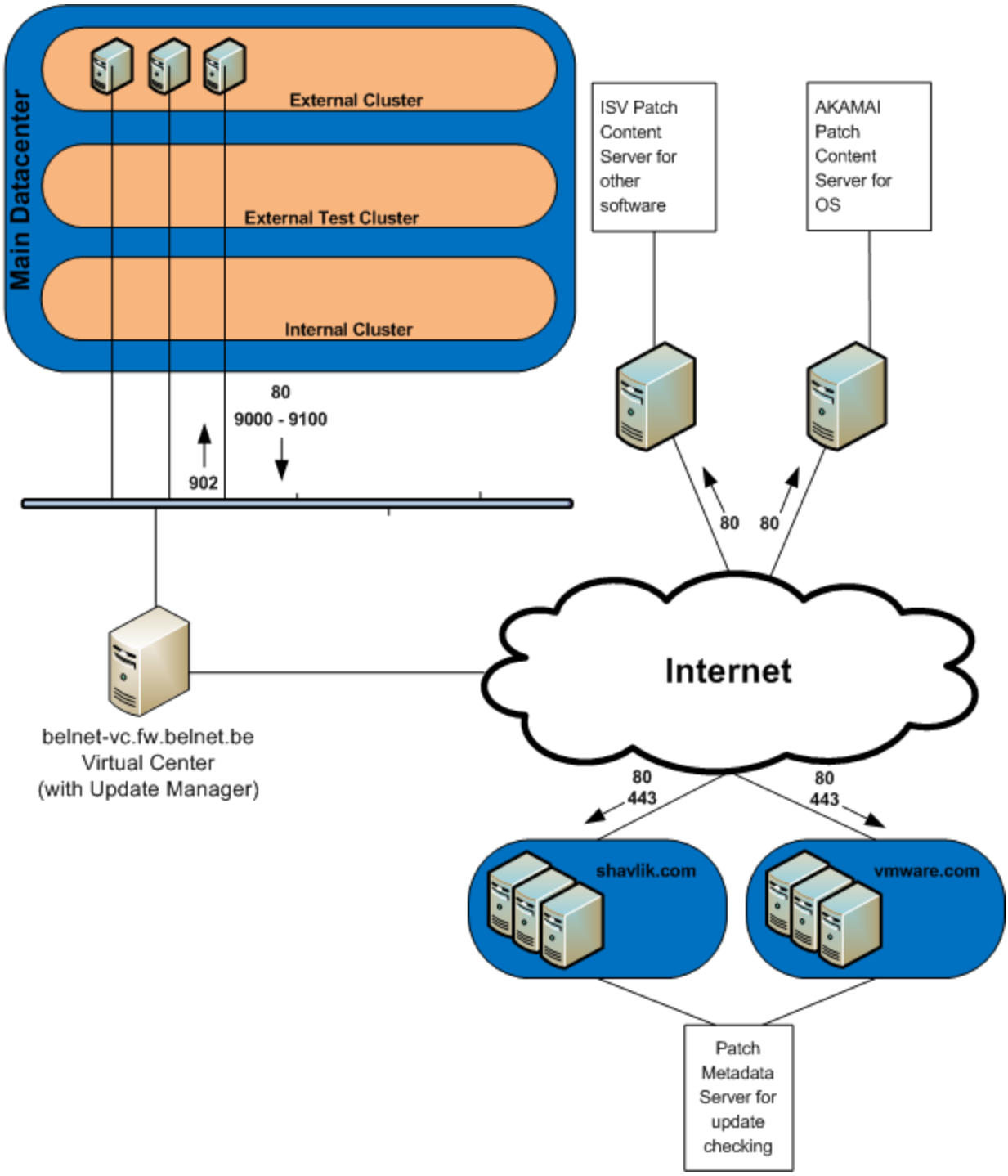

Figure 4 - Update Manager Network Port Requirements [11]

Of course there is the option to update your servers manually. This is however more time consuming, but you will have more control over the update process.

Manageability

VMware Infrastructure 3.5 is managed by Virtual Center, but is now superseded by VMware vSphere. It is used for maintaining and managing the virtual datacenter. [4]

BELNET is currently testing VMware vSphere. They've already setup an environment for this. The test environment contains 2 physical blade servers running VMware vSphere. With this setup they can test how the vSphere product can fit into their existing Virtual Infrastructure.

BELNET uses VMware Virtual Center to manage their Virtual Infrastructure 3.5 environment. Their testing environment is managed by vSphere.

Secure VI

To create a secure Virtual Infrastructure, you must apply rules on the network. We advise to subscribe to the security mailing lists from VMware to stay informed about the latest security issues.

Virtual Center/vCenter security
Virtual Center used to manage the Virtual Infrastructure (3.5), while vCenter is used to manage the vSphere test environment. The tools are running on a VM. It is important to limit access to these VMs.

Virtual Datacenter and Clusters
The use of Virtual Datacenter and clusters could lower the security. The reason behind this is that you can manage multiple hosts with just one password. This is because you connect to one Virtual Center/vCenter server.

Host security
The security of the host can be read in the beginning of this report.

VM security
In the past, a compromised VMware guest was able to get access to the resources of another VM, which gave an attacker the possibility to crash an entire host. A patch was released (security advisory VMSA-2009-0005 [19]) by VMware to fix this. It should not be possible to gain access to the entire virtual environment, because BELNET's corporate policies should describe the limited access to management tools like VMware Virtual Center and VMware vSphere. Also, prevention of denial of service attacks should by applied by resource allocation to VMs.

Monitoring the security

BELNET already has multiple (virtual) servers that monitor their existing infrastructure. The physical servers can be migrated to a VM and continue their monitoring tasks. The existing servers can also be used to monitor the virtual infrastructure.

The following servers that BELNET has running can be used for the monitoring of the virtual infrastructure:

- Virtual Center/vCenter (alerts)
- Nagios server (notifications by e-mail, sms or pager)
- MRGT server (trend analyzing)

Central logging
It is recommended to store all ESX logfiles on a central server. A central log server provides the storing of all ESX logs in one place. This optimizes any research that has to be done if an event occurs. We found that VMware ESX also uses gzip to archive the logfiles if they get too large in filesize, which makes it harder for administrators to check for events.

A couple of things that are/can be important to monitor: [10]

- API user login (root/other/unknown)
- Tech Support user login (root only)
- Tech Support mode invocation
- Root login via Tech Support Mode on local console
- Root login via Direct Console User Interface (DCUI) on local console

To be able to monitor the above points, central logging is necessary. A script can then provide alerts to one of the monitoring servers previously described.

Apart from logins, console sessions can also be an interesting event to monitor. An unauthorized user login may pass detection. This unauthorized user can open a console session to a VM.

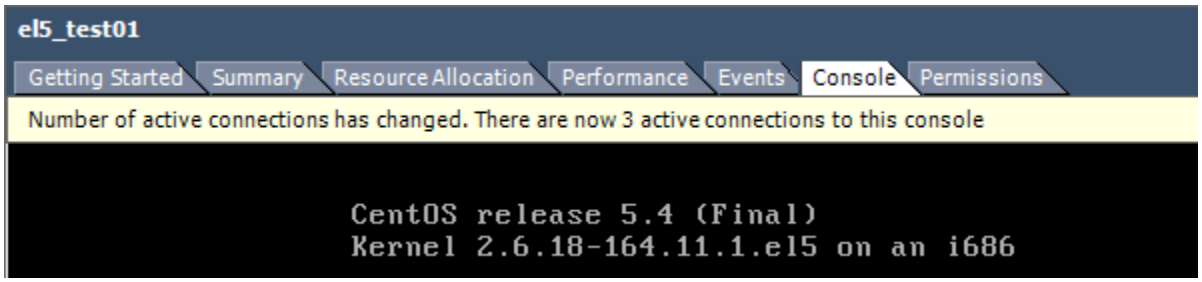

Figure 5 - Multiple Virtual Console sessions

It may be the case that an OS user with a high authorization level is still logged in at this virtual console, the unauthorized user then has access to this VM via the virtual console. This makes it important to generate an alert if the number of console sessions is elevated beyond the acceptable level.

- Virtual Console events
    - Single Virtual Console
    - Multiple Virtual Consoles

Not all the log notifications have to be logged on the central server though. It is recommended to limit the logfiles to specific notifications. On our test setup with one ESXi host, 2 Linux-based guests and one Windows guest, we generated around 2.2MB in 24 hours. If you filter the logging from ESX(i), logfile size can be substantially reduced. On our test machine running Cent OS 5.4, we setup syslog-ng, which supports filtering of the incoming logs. Port 514 (TCP) should be opened in the IPtables firewall on the central log server. That is if syslog-ng is used, which uses TCP for transport [12]. If another syslogging solution is used, it could use UDP for transport.

For our test environment, we used the iptables rule below:

-A INPUT -p tcp -m tcp --dport 514 -j ACCEPT

This rule accepts TCP connections on port 514.

The following is a list of events that are important to monitor.

- Login
    - VI/vSphere Client (API)
        - existing user
            - with right password
            - with wrong password
        - nonexistent user/password
    - Direct Console User Interface (DCUI)
        - existing user
            - with right password
            - with wrong password
        - nonexistent user/password
    - SSH
        - existing user
            - with right password
            - with wrong password
        - nonexistent user/password
    - Tech support mode (on console)
        - existing user
            - with right password
            - with wrong password
        - nonexistent user/password

The log lines that appears for the above login and virtual console access events can be read in Appendix A.

Auditing the security

If BELNET has successfully implemented a secure virtual infrastructure, it is very important to keep it as secure as originally intended. The intended security level should be maintained at all time.

If available, keep the existing company auditing policies and perform auditing of the virtual environments on a regular basis, like once every month.

If something is changed in the configurations for testing purposes, it should also be rolled back when the testing phase is over.

If you are going to do your own security audits, according to [20], it can be helpful to take the following points into account:

- Define the scope of your audit
- Create a threats list
- Prioritize your assets and vulnerabilities
- Implement network access controls
- Implement intrusion prevention
- Implement identity and access management
- Create backups on a regular basis
- Email protection and filtering
- Prevent physical intrusion

Infrastructure

VLAN setup

The image below shows what servers and services are configured on a specific VLAN. The servers and their services are all divided over the VLANs. [2]

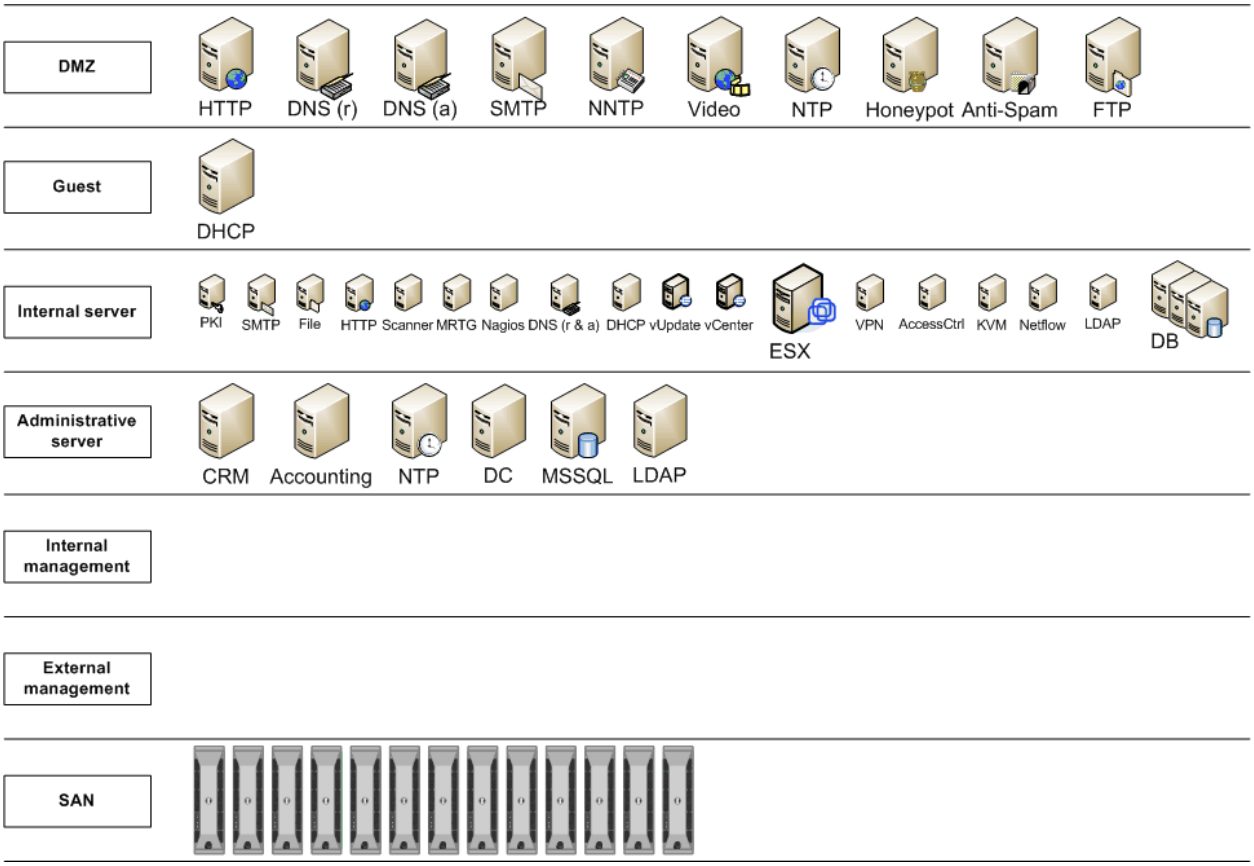

Figure 6 - Update Manager Network Port Requirements [2]

Trusted Zones (DMZs)

BELNET indicates that virtualizing their DMZs are one of the important aspects of setting up a secure Virtual Infrastructure. [2]

The most secure way to separate DMZ traffic is to use an additional physical network adapter, specifically for this purpose. This way, DMZ traffic is physically separated from the other VLANs, instead of just tagged on the same network.

Like stated in the beginning of this report, some people believe that the virtualization of an infrastructure with different trust zones (DMZs), can cause security problems. [8,9] It is best to keep servers of the same DMZ on the same physical ESX server. This way, a high server consolidation is created, while maintaining DMZ consistency.

However, according to [9], most security issues arise because of misconfiguration by administrative staff. To avoid this issue, we advise that multiple people will look at the configurations separately.

Routers and Switches

There won't be any need for additional changes in the configurations of the routers and switches in the BELNET infrastructure. If VLANs are implemented the right way on the Virtual Hosts, routing will be done correctly. It basically comes down to the same configurations as you would treat physical hosts.

Firewalling

Firewalling can be done on several levels:

- Use Access Control Lists (ACL's)
- Heavy firewall machine before the hosts
- Firewalling on guest level (Windows Firewall or iptables)

Current BELNET configurations can remain intact in the virtual environment.

SAN

In a Virtual Infrastructure, the most common way to store data is by using a central storage solution. If a central storage solution is used, different servers can make use of the same storage space. Besides easy to manage central storage, another advantage is that you only need to backup one large storage array, and not multiple (distributed) storage systems.

For BELNET's Virtual Infrastructure, a SAN solution is used. A SAN is a Storage Area Network, which is an architecture that can be used to attach remote computer storage devices to servers in such a way that an OS thinks the devices is connected locally. [5]

The SAN solution used for BELNET's Virtual Infrastructure is based on 13 Dell EqualLogic

PS4000E SANs.

Figure 7 - EqualLogic PS4000E SAN (copyrighted Dell EqualLogic) [6]

To SANs provide the Virtual Infrastructure with iSCSI storage. The iSCSI protocol is used to attach the remote SAN storage to the physical host machines. By doing this, the hosts can use the central storage space to store the VM data.

Apart from attaching remote storage to the hosts, iSCSI can also be used to attach storage to a VM guest. A database VM running MSSQL or MySQL, can be kept very small by storing it's actual data on an iSCSI share.

If iSCSI is used, the operating system thinks the storage is based on the local machine, but it actually is on separate hardware located on the network. [6]

iSCSI network security
If important data is going over the (local) network, security will be of a high importance. To get it secure, you can protect the SANs with a username and password. This is done by using CHAP (Challenge-Handshake Authentication Protocol). Both the VMware infrastructure and the SANs support this authentication for iSCSI, It could be more secure by securing the network layer with IPsec, but as far as we can find, the SANs don't support this.
The next step you can take to secure the SAN infrastructure is to isolate it's network. This can be done by VLANs or physically isolating them. BELNET stated they have a separate SAN VLAN, so this can be used.
Finally, authorization can be used if necessary. This can be configured on the SANs, so not all the hosts can access all the storage resources. [14,15]

Conclusion/Recommendations

Our research shows that there are many configuration aspects in a virtual infrastructure that determine the security state.

To answer the main research question we stated in the beginning of this report, the sub-questions will be answered first.

- What level of firewalling should be implemented? (What level of strictness, etc.)
    - To make it as secure as possible, the firewall solution used by BELNET should have a fully closed policy, except for the ports we described in the report.
- Does the use of different passwords for each virtual host heighten the security level?
    - The use of different passwords does heighten the security level, but all the different passwords should be saved easily and encrypted. If a solution like the one we suggested (KeePass), isn't used, remembering complex passwords isn't easy enough. Users will write the passwords down on papers, lowering the security level to a piece of paper. This way, a visitor (burglar/attacker) can easily obtain a password.
- Does the use of Virtual Datacenters and Clusters have any impact on security?
    - The use of Datacenters and Clusters can lower the security level, because multiple hosts can be managed by a single password.
- What is the risk if a compromised virtual machine is able to gain access to the virtual infrastructure itself at the ESX or Virtual Center level?
    - As we explained in the report, this shouldn't be possible any more. There was a vulnerability in the past, but VMware patched it. Apart from that, you should limit the connectivity to the Virtual Center VM.
- How can the security state be audited and monitored?
    - Monitoring
        - A way to generate alerts if suspicious log events occur is to filter for one log line only.
    - Auditing
        - Perform audits on a regular basis, just like with a physical environment
        - Roll back changes after test phase

For safe access configurations, it is best to treat the virtual environment as if it were a physical one. The main reason security issues arise while virtualizing a DMZ is because of misconfiguration and human error. To maintain a high security level, it is best to let multiple people look at the configurations separately.

To answer the main question "*What is the best way to successfully implement a virtual infrastructure while dealing with all possible security (related) issues?*", are the suggestions we propose in this report.

Used literature/Bibliography

We used the following literature during our research.

1. http://en.wikipedia.org/wiki/BELNET (04/01/2010)
2. BELNET architecture description
3. http://www.vmware.com/files/pdf/vi35_security_hardening_wp.pdf
4. http://www.vmware.com/products/vi/
5. http://en.wikipedia.org/wiki/Storage_area_network (12/01/2010)
6. http://www.equallogic.com/products/default.aspx?id=8313
7. http://www.vmware.com/pdf/vsphere4/r40/vsp_40_config_max.pdf
8. http://www.vmware.com/files/pdf/network_segmentation.pdf
9. http://www.vmware.com/files/pdf/dmz_virtualization_vmware_infra_wp.pdf
10. http://vinternals.com/2010/01/esxi-4-0-security/
11. http://www.vmware.com/pdf/vi3_vum_10u2_admin_guide.pdf
12. http://en.wikipedia.org/wiki/Syslog-ng
13. BELNET Clusters.jpg
14. http://www.vmware.com/pdf/vi3_iscsi_cfg.pdf
15. http://en.wikipedia.org/wiki/ISCSI
16. http://www.p-synch.com/docs/password-management-best-practices.html
17. Gartner Research - "Server Virtualization Can Break DMZ Security"
18. http://keepass.info/
19. http://lists.vmware.com/pipermail/security-announce/2009/000054.html
20. http://www.itsecurity.com/features/it-security-audit-010407/
21. http://www.vreference.com/downloads/ConnectionsPorts-v4.pdf

Appendix A

Log lines to monitor the security state

VI/vSphere Client (API)

Existing user right password
Hostd: Accepted password for user root from 0.0.0.0
Hostd: [2010-01-21 13:54:14.607 19639B90 info 'ha-eventmgr'] Event 81 : User root@0.0.0.0 logged in

Existing user wrong password
Hostd: Rejected password for user root from 0.0.0.0

Nonexistent user/password
Hostd: pam_unix(vmware-authd:auth): check pass; user unknown
Hostd: Rejected password for user unknown_user from 0.0.0.0

Direct Console User Interface (DCUI)

Existing user right password
DCUI: authentication of user root succeeded

Existing user wrong password
DCUI: authentication of user root failed

Nonexistent user/password
DCUI: pam_unix(dcui:auth): check pass; user unknown
DCUI: authentication of user berry failed

SSH

Existing user right password
dropbear[5298594]: Child connection from 0.0.0.0:60145
dropbear[5298594]: PAM password auth succeeded for 'root' from 0.0.0.0:60145

Existing user wrong password
dropbear[5319566]: bad PAM password attempt for 'root' from 0.0.0.0:61598

Nonexistent user/password
dropbear[5319249]: login attempt for nonexistent user from 0.0.0.0:61597

Tech Support mode (on console)

Existing user right password
login[5295780]: pam_unix(login:session): session opened for user root by (uid=0)
login[5295780]: root login on 'UNKNOWN'
init: init: starting pid 5329717, tty '/dev/tty1': '/bin/sh'
root: techsupport VMware Tech Support Mode available

Existing user wrong password
getty[5295780]: VMware Tech Support Mode successfully accessed
login[5295780]: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=UNKNOWN ruser= rhost= user=root

Virtual Console events

Single Virtual Console

First console session
Hostd: [2010-01-27 14:19:52.284 48F20B90 info 'vm:/vmfs/volumes/4b41d954-5e6a9cc1-78a2-0015c5e13bfe/el5_test01/el5_test01.vmx'] Ticket issued for mks connections to user: root
authd[30632]: login from 0.0.0.0 as 52ce0b30-c96e-f930-10ea-908e648ea268
authd[30632]: Local connection for mks established.
Hostd: [2010-01-27 14:19:52.776 48C9CDC0 verbose 'vm:/vmfs/volumes/4b41d954-5e6a9cc1-78a2-0015c5e13bfe/el5_test01/el5_test01.vmx'] New MKS connection count: 1

Multiple Virtual Consoles

Second console session
Hostd: [2010-01-27 14:21:31.613 48FA2B90 info 'vm:/vmfs/volumes/4b41d954-5e6a9cc1-78a2-0015c5e13bfe/el5_test01/el5_test01.vmx'] Ticket issued for mks connections to user: root
authd[30996]: login from 0.0.0.0 as 52268a2d-afe8-a264-d4f6-83f8ffea3afe
authd[30996]: Local connection for mks established.
Hostd: [2010-01-27 14:21:31.853 16941B90 verbose 'vm:/vmfs/volumes/4b41d954-5e6a9cc1-78a2-0015c5e13bfe/el5_test01/el5_test01.vmx'] New MKS connection count: 2

Third console session
Hostd: [2010-01-27 14:21:38.566 48EDFB90 info 'vm:/vmfs/volumes/4b41d954-5e6a9cc1-78a2-0015c5e13bfe/el5_test01/el5_test01.vmx'] Ticket issued for mks connections to user: root
authd[30997]: login from 0.0.0.0 as 52791c44-8f5c-f477-18c9-42839daccd0f
authd[30997]: Local connection for mks established.
Hostd: [2010-01-27 14:21:38.799 1683DB90 verbose 'vm:/vmfs/volumes/4b41d954-5e6a9cc1-78a2-0015c5e13bfe/el5_test01/el5_test01.vmx'] New MKS connection count: 3