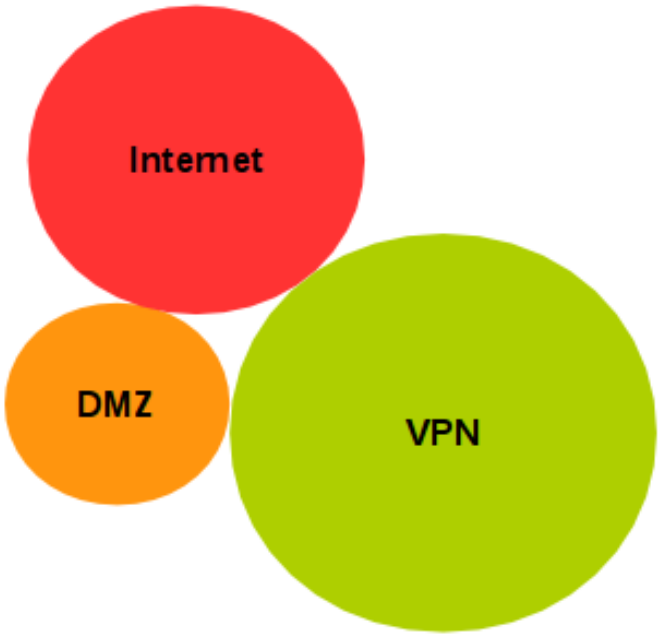
http://www.tecnica24.es
TECHNICAL INFORMATION
July 2014

técnica24.es

Security Infraestructure for organizations with critical information

(secure critical information that manage your organization)



TECNICA24 develops web apps using Oracle Technology with focus on to get an execution environment as secure and stable as posible, also maintaining your licensing costs at lower level.

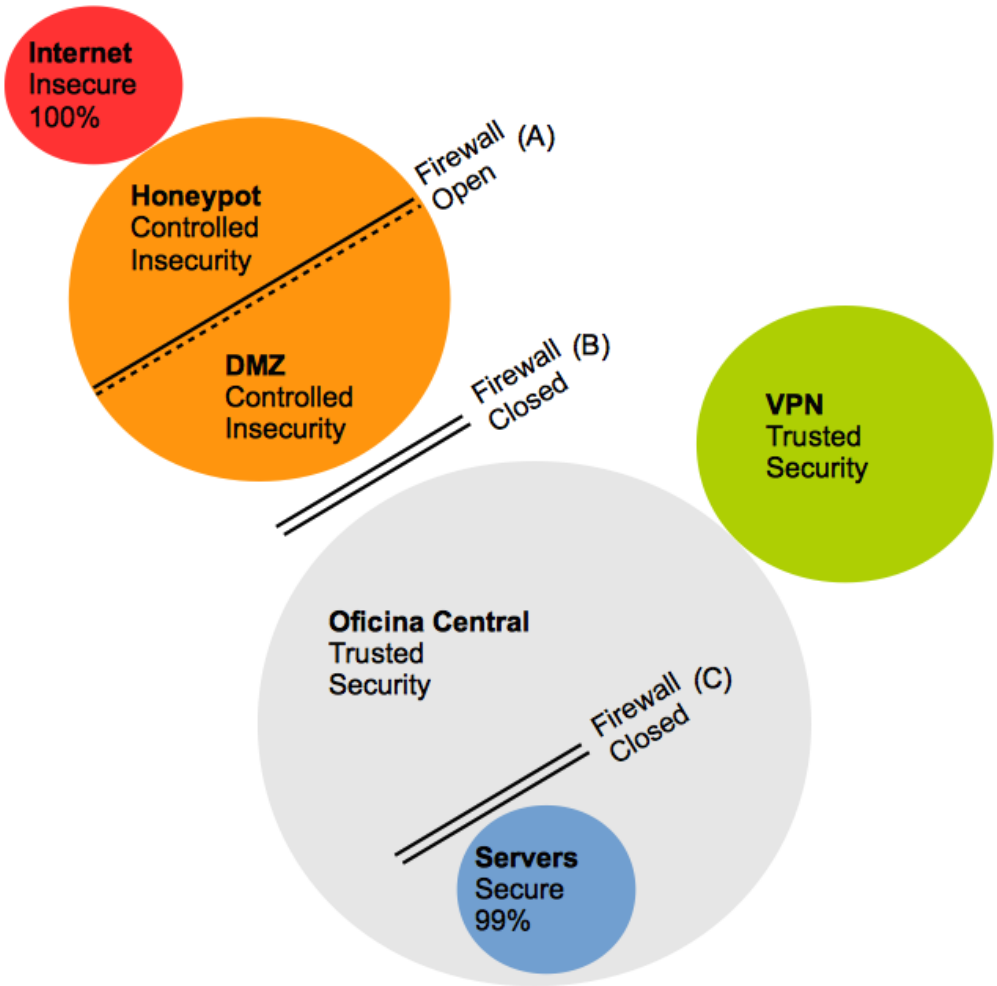
We want that your data would be in a secure, accesible, controlled manner. Focused on that goal we create a security infraestructure in 3 layers that integrate a honeypot serving as "false infraestructure" to maintain attackers out of business critical information.

(c) 2014, Jesús Moreno Díaz
http://www.tecnica24.es
TECHNICAL INFORMATION
July 2014

Security Model using 3 layers

Introduction
Actually there is no doubt that being connected to internet is high risk and frecuently hackers try to steal our information using malware that are propagated inside usb devices, using known security holes in commercial products or even doing attacks against our internet router.

Every organization must protect their information taking place not “if attacks would produce or not” but “when they will succed, from where, and what information will be compromised”.



“TECNICA24’s proposal is to create a security infraestructure in 3 layers for a) to protect internet access, b) to protect access to servers, c) to get a false infraestructure with no critical information to be accessed without interest by hackers”.

“We analyze your network before starting our project to achieve that no malware is running without your knowledge”.

Model built on virtualization

Today use of virtualization technology is a must not an option. We believe that your organization will own its infraestructure built using products as VMWare or Oracle VM. We will integrate our security infraestructure using virtual machines that will run in your vm platform.

Model that use “open source” software

TECNICA24 uses open source software when possible with goal in mind to reduce your licensing costs. Products we integrate in our solutions also are directly supported by our support contract monthly cost. Also if your organization demands more guaranties it can opt to a direct support from vendor of open source software.

Network analysis

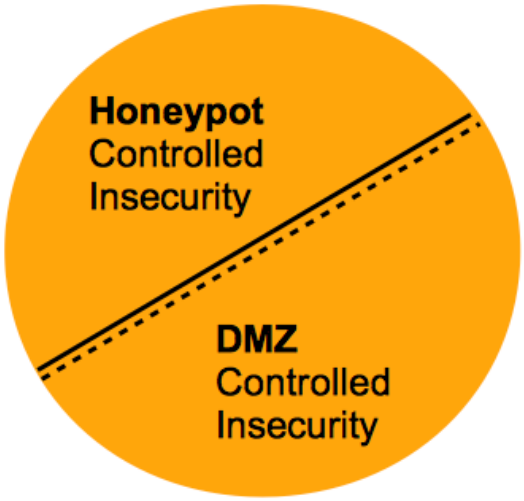
TECNICA24 makes a network analysis prior to start project of create your new security infraestructure. We use WireShark to analyze tcp/ip traffic paquets that source in your organization and destiny of them. We can determine if malware software is accessing to information of your organization, origin of attackers and destiny of information.

(c) 2014, Jesús Moreno Díaz
http://www.tecnica24.es
TECHNICAL INFORMATION
July 2014

Security Model using 3 layers

Layer #1: False infraestructure using honeypot to trick external attackers

"Controlled Insecurity: we know that anyone can attack our system to steal information, we allow it, we control they do".



We create a false infraestructure protected by a firewall connected to internet router wich will act as first protection barrier. It will contain not critical information that could be queried without interest by an attacker. He will believe that entered inside low level organization and will end interest in more investigation.

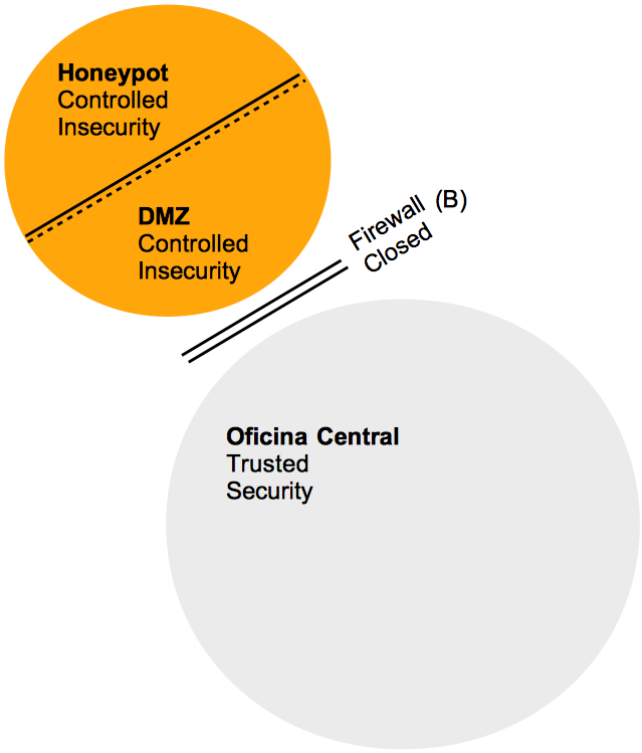
We use Oracle Linux 6.5 configured as external firewall leaving ports/services open:
a) 21, FTP service, containing not critical documentation of your organization but protected access by user and password.
b) 80, web with "in construction" banner o simulating services from TECNICA24.
c) 8080, web app without critical mission for your organization as "incidents management".

(c) 2014, Jesús Moreno Díaz
http://www.tecnica24.es
TECHNICAL INFORMATION
July 2014

Security Model using 3 layers

Layer #2: Protection of internet access optionally filtering web contents

"Trusted Security: internet access protected, trusting any malware is running in internal network".



We create a firewall configured in closed mode leaving open only web port (80) and those used in mail service (110, 587, 25)
We use Zentyal 3 configured as closed firewall and as web content filtering o proxy, obtaining:

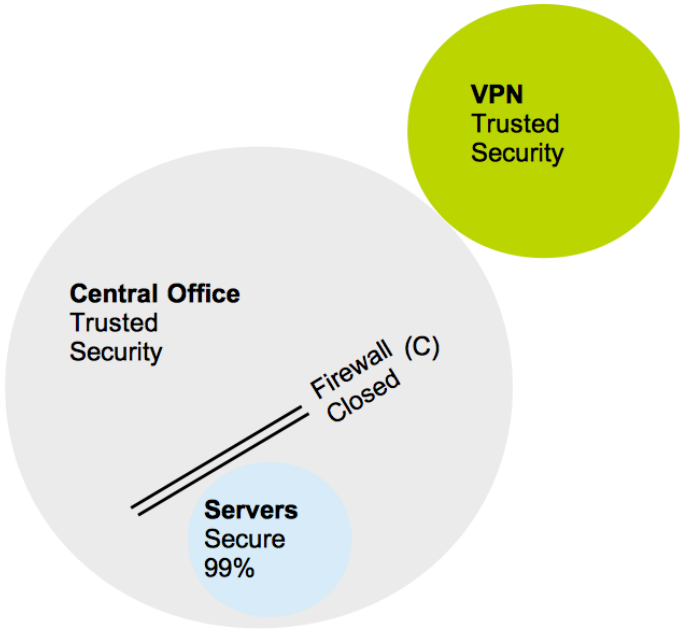
a) exclusive access to those webs of interest for your organization.
b) avoiding that malware installed in your computers could get internet access to send/ receive information.
c) protecting access to internal network in case to be compromised first layer security.

(c) 2014, Jesús Moreno Díaz
http://www.tecnica24.es
TECHNICAL INFORMATION
July 2014

Security Model using 3 layers

Layer #3: Protection of access to your servers

"Secured 99%: we protect our servers because we know that internal network could be compromised".



We create a firewall configured in closed mode leaving open only access to public services in your servers that are essential to your business activity:

a) web apps (80, 8080).
b) client/server apps, (oracle 1521, microsoft sql server 1433).

We use SmoothWall 3 configured as closed firewall to obtain:

a) protection of all set of servers hosted in your infraestructure allthough some of them would use basic protection from its firewall by software (Microsoft products).
b) to avoid that security holes in commercial products could take in place to compromise access to your servers.
c) to control that any malware installed without knowledge could make attacks against servers from internal network.

Technical Information

Terms

- honeypot, http://es.wikipedia.org/wiki/Honeypot: Infraestructure that is built with intention to attract attackers, control them, and to get lose of interest in our organization.
- SmoothWall 3, http://www.smoothwall.org: Open source firewall that is base of commercial product with support, http://www.smoothwall.com.
- Zentyal 3, http://www.zentyal.com: Infraestructure open source software that can act as web content filter, firewall, mail server, and more.
- VMWare, http://www.vmware.com: Virtualization software that offers a cost free license,, vSphere Hypervisor (ESXi),http://www.vmware.com/es/products/vsphere-hypervisor/
- Oracle VM, http://www.oracle.com/us/technologies/virtualization/oraclevm/overview/index.html: Infraestructure software that offers technical support and cost free licensing, by Oracle, http://www.oracle.com.
- WireShark, http://www.wireshark.org/: Open source software for analysis of network traffic paquets.