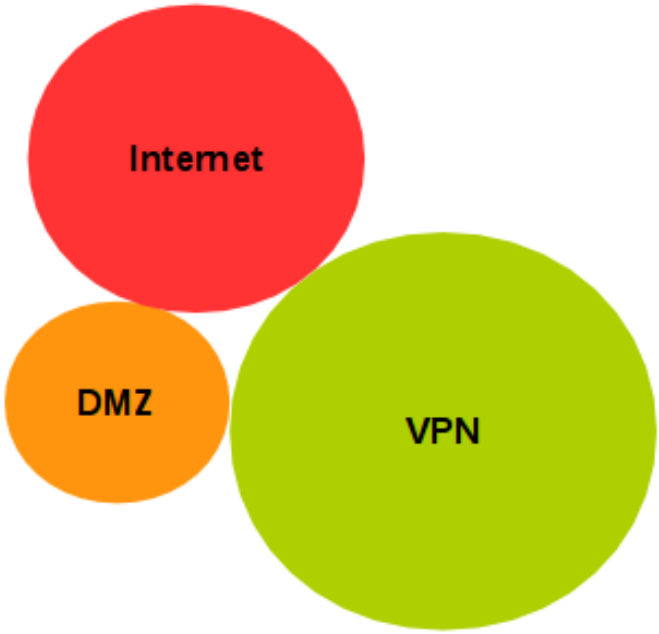
http://www.tecnica24.es
INFORMACION TECNICA
Julio 2014

técnica24.es

Infraestructura de Seguridad para organizaciones con información crítica

(asegure la información crítica que gestiona su organización)



TECNICA24 desarrolla aplicaciones web usando tecnología Oracle con el objetivo de proporcionar un entorno de ejecución estable y seguro que además reduce sus costes de licencia.

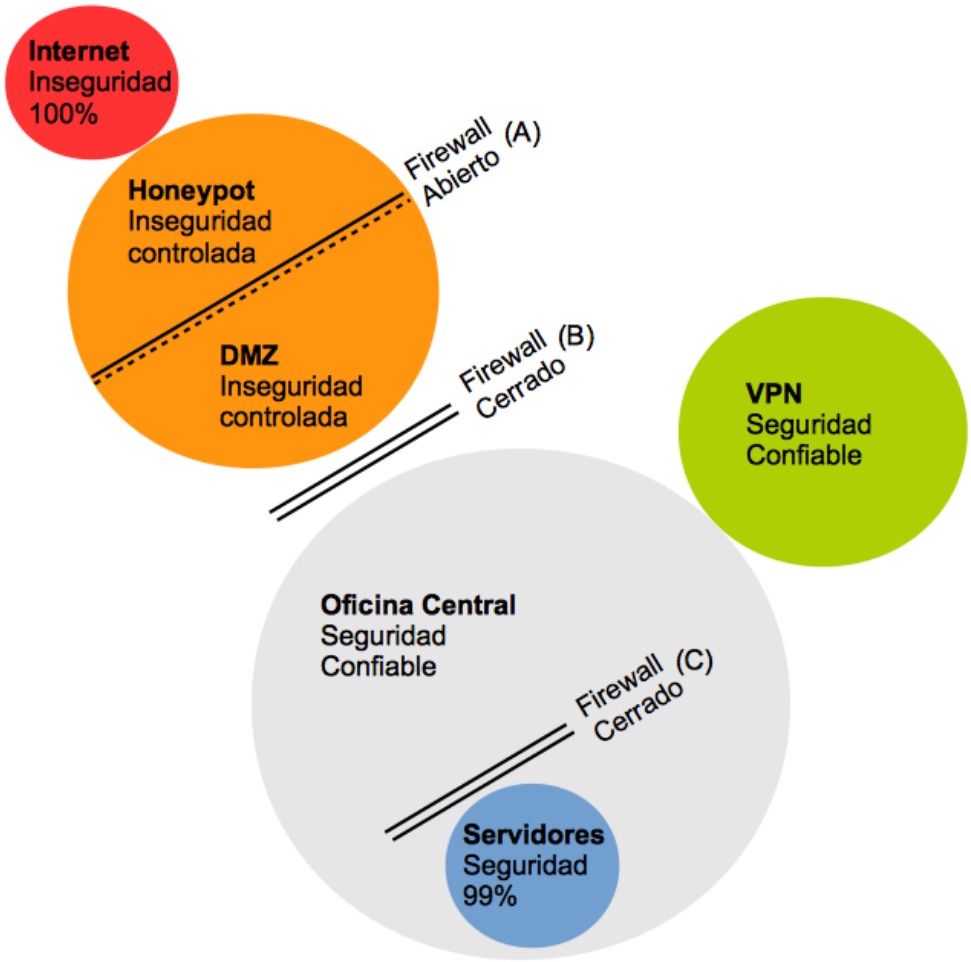
Queremos que su información esté segura, accesible, y controlada. Para ello creamos una infraestructura de seguridad en 3 capas integrando una falsa infraestructura en un "honeypot" que servirá como engaño a posibles atacantes desde el exterior.

(c) 2014, Jesús Moreno Díaz
http://www.tecnica24.es
INFORMACION TECNICA
Julio 2014

Modelo de Seguridad en 3 capas

Introducción
Actualmente no existe duda que estar conectado a internet supone un alto riesgo y que constantemente atacantes o "hackers" intentan robar información usando "malware" que se propaga en dispositivos de almacenamiento USB, por ataques aprovechando agujeros de seguridad en productos comerciales, o realizando ataques contra nuestro "router" de conexión a internet.

Toda organización debe proteger su información teniendo en cuenta no "si se producirán o no los ataques" sino "cuándo se producirán, desde dónde y qué información estará comprometida".

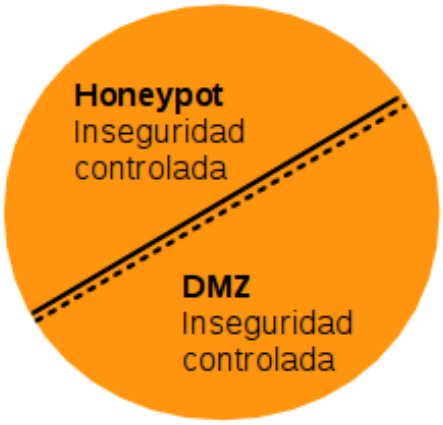


"TECNICA24 propone crear una infraestructura de seguridad en 3 capas para a) proteger el acceso a internet, b) proteger el acceso a los servidores, c) disponer de una falsa infraestructura con información no crítica para ser accedida sin interés de continuar los ataques".

"Analizamos su red antes de comenzar para asegurarnos que no existe software malintencionado funcionando sin su conocimiento."

Modelo construído usando virtualización
Actualmente usar tecnología de virtualización es una necesidad más que una opción técnica. Creemos que su organización tendrá su infraestructura construída en un entorno virtualizado como VMWare u Oracle VM. En tal caso integramos nuestra infraestructura de seguridad a modo de máquinas virtuales que se integran en su sistema.

Modelo que usa tecnología "open source"



TECNICA24 promueve el uso de tecnología "open source" con el objetivo de reducir sus costes de licencia. Los productos que integramos en nuestras soluciones son soportados directamente por TECNICA24 en nuestra cuota de servicio de mantenimiento. Además si su organización demanda mayores garantías puede optar a soporte directo del fabricante porque usamos productos "open source" con opción de soporte.

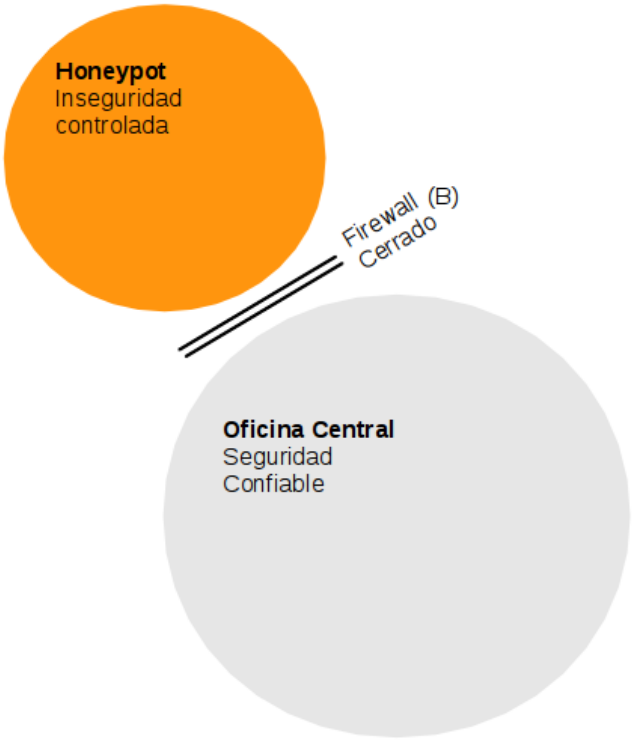
Análisis de red
TECNICA24 realiza un análisis de red en su organización antes de acometer el proyecto de crear su nueva infraestructura de Seguridad. Usamos WireShark para analizar los paquetes de red que se originan en su organización y el destino de los mismos. Determinamos si software malintencionado está accediendo a información de su organización, el origen de los atacantes y el destino de la información.

(c) 2014, Jesús Moreno Díaz
http://www.tecnica24.es
INFORMACION TECNICA
Julio 2014

Modelo de Seguridad en 3 capas

Capa 1: Falsa infraestructura a modo de "honeypot" para engañar a atacantes externos

"Inseguridad controlada: sabemos que nos pueden atacar para robar información, permitimos que lo hagan, controlamos que lo hacen".



Creamos una falsa infraestructura protegida por un firewall que conectamos a su router de conexión a internet y que servirá como primera barrera de protección. Contendrá información no crítica de su organización que puede ser consultada sin más interés por un atacante. Este creerá que se trata de una organización "pequeña" y cesará su interés.

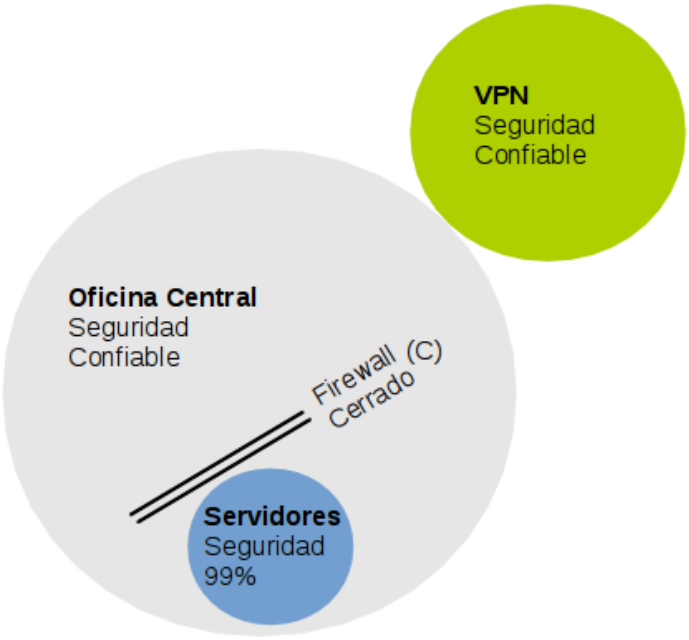
Usamos Oracle Linux 6.5 que configuramos como firewall externo abriendo los servicios:
a) 21, servicio FTP alojando documentación no crítica de su organización, pero protegido por usuario y contraseña.
b) 80, web en modo "en construcción" o simulando servicios de TECNICA24.
c) 8080, aplicación web no crítica para su organización como "gestión de incidencias".

(c) 2014, Jesús Moreno Díaz
http://www.tecnica24.es
INFORMACION TECNICA
Julio 2014

Modelo de Seguridad en 3 capas

Capa 2: Protección de acceso a internet opcionalmente filtrando contenidos

"Seguridad confiable: protegemos el acceso a internet, confiamos que ningún



software malintencionado se esté ejecutando en la red interna".

Creamos un firewall configurado en modo cerrado dejando sólo disponible la salida en el puerto web (80) y en los usados por el correo electrónico (110,587,25)

Usamos Zentyal 3 que configuramos como firewall cerrado y como proxy de filtrado web, obteniendo:
a) el acceso exclusivo a aquellas web de interés para su organización.
b) evitando que software malintencionado instalado en sus ordenadores pueda conectarse a internet para enviar/recibir información.
c) protegiendo el acceso a la red interna en caso de estar comprometida la seguridad de la primera capa.

http://www.tecnica24.es
INFORMACION TECNICA
Julio 2014

Modelo de Seguridad en 3 capas

Capa 3: Protección de acceso a sus servidores

"Seguridad 99%: protegemos nuestros servidores porque sabemos que nuestra red interna podría estar comprometida".

Creamos un firewall configurado en modo cerrado dejando sólo disponible el acceso exclusivo a los servicios publicados en sus servidores necesarios para la actividad de su organización:

a) aplicaciones web (80, 8080).
b) aplicaciones cliente/servidor, (oracle 1521, microsoft sql server 1433)

Usamos SmoothWall 3 que configuramos como firewall cerrado para:

a) proteger en conjunto todos los servidores alojados en su infraestructura, contando algunos con una protección básica basada en firewall software (productos Microsoft).

b) evitar que puedan aprovecharse agujeros de seguridad conocidos en productos comerciales para comprometer el acceso a sus servidores.

c) controlar que software malintencionado instalado sin conocimiento en los ordenadores pueda realizar ataques contra sus servidores.

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

Información Técnica

Términos

- honeypot, http://es.wikipedia.org/wiki/Honeypot: Infraestructura que se crea con la intención de atraer atacantes, controlarlos, y conseguir que pierdan el interés por nuestra organización.
- SmoothWall 3, http://www.smoothwall.org: Firewall open source que da soporte a producto comercial, http://www.smoothwall.com.
- Zentyal 3, http://www.zentyal.com: Software de infraestructura open source que puede actuar como filtro de contenidos, firewall, servidor de correo, etc.
- VMWare, http://www.vmware.com: Software de infraestructura de virtualización que ofrece una versión libre de costes de licencia, vSphere Hypervisor (ESXi),http://www.vmware.com/es/products/vsphere-hypervisor/
- Oracle VM, http://www.oracle.com/us/technologies/virtualization/oraclevm/overview/index.html: Software de infraestructura de virtualización que ofrece soporte técnico y licencia libre de costes, por Oracle, http://www.oracle.com.
- WireShark, http://www.wireshark.org/: Sofware open source de análisis de tráfico de red.