UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escuela Técnica Superior de Ingeniería Informática
Universitat Politècnica de València

REDES SEGURAS EN ENTORNOS VIRTUALIZADOS

Proyecto Final de Carrera

Ingeniería Informática

Autor: Francisco José Vañó Reig

Director: Mª Lourdes Peñalver Herrero

18-09-2016

DEDICATORIA

Als meus pares i germana, per ensenyar-me a valorar tot allò que és important a la vida.

Als meus amics Mari i Enric, per estar sempre amb mi.

Per a Toni, sense tu res d'açò hagués estat possible.

Per al meu Nakama, no sóm germans de sang, però sempre estarem ahí.

Resumen

A lo largo de la historia de la humanidad, cada avance que se ha producido ha suscitado una cierta inquietud y ha generado un abanico de normas que han intentado garantizar y mantener el buen uso de estos avances, así como la integridad de los mismos. La misma convivencia del ser humano en sociedades, se lleva a cabo en lugares regidos por una serie de normas y donde algunos se encargan de la seguridad.

Desde la aparición de la informática y más aún desde que Internet llegó gran público, la seguridad informática ha ido aumentando, haciendo-se cada vez más sofisticada y teniendo que adaptarse a un entorno enormemente cambiante.

A lo largo de este Proyecto pretendemos ahondar en la seguridad informática tratada dentro del entorno de la virtualización, punta de lanza y elemento fundamental de los centros de procesamiento de datos actuales y tecnología base del entorno Cloud.

Los objetivos a desarrollar en este proyecto son los siguientes:

- Estudiar las vulnerabilidades de una red virtual.
- Adaptar el modelo de seguridad tradicional a un entorno virtualizado.
- Buscar una solución escalable y fácil de implementar
- Comparar con la seguridad de un entorno de red físico.
- Implementar los servicios mínimos.
- Garantizar la adaptabilidad a diferentes tipos de Cloud.

Tabla de contenidos

1. Seguridad informática

En la actualidad, los entornos de TI son la base fundamental de nuestra sociedad, hacemos uso de ellos tanto consciente como inconscientemente y transmiten y almacenan enormes cantidades de información. Se almacenan tanto datos de empresas, como datos personales. Además, controlan entornos muy sofisticados y garantizan la seguridad. Cualquier eventualidad que vulnere la integridad de los mismos provoca consecuencias desastrosas.

Debido a que el uso de internet se encuentra en aumento, cada vez más compañías y entidades permiten a socios, proveedores y usuarios acceder a sus sistemas de información. Por lo tanto, es fundamental saber que recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a la compañía a través de internet.

Adicionalmente, debido a la tendencia creciente de la deslocalización de los sistemas y al ritmo de vida nómada que están asumiendo las personas hoy día una organización, permite a los empleados, alumnos o colaboradores conectarse a los sistemas de información casi desde cualquier lugar. Esto añade un escalafón más en la preocupación por la seguridad.

A su vez los sistemas están empezando a deslocalizarse y a hacer uso de un elemento importante llamado “la cloud”.

1.2. Definición

Entendemos por seguridad informática la disciplina que se encarga de proteger la integridad de los activos informáticos importantes para una entidad, así como la privacidad de la información almacenada en sus sistemas. Estos activos normalmente son software (archivos, aplicaciones, etc.) pero también pueden ser hardware o todo aquel material que contenga información. Además, se encarga de mantener la disponibilidad de dicha información.

1.3. Características

Un sistema informático es tan fuerte como su eslabón más débil. No existe un sistema 100% seguro, la seguridad es algo dinámico que implica un continuo mantenimiento. La clave reside en tener un sistema que sea seguro en todos sus puntos, y que garantice la mayor relación efectividad/coste, para ello, debe tener las siguientes cuatro características:

Integridad: Los activos o la información solo pueden ser modificados por las personas autorizadas y de forma autorizada.

Confidencialidad: La información o los activos informáticos son accedidos solo por las personas autorizadas para hacerlo.

Disponibilidad: Los activos informáticos son accedidos por las personas autorizadas en el momento requerido.

Irrefutabilidad: El uso y o modificación de la información por parte de un usuario debe ser irrefutable, es decir no puede negar dicha acción.

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en tres partes: Seguridad física, Seguridad Ambiental y Seguridad lógica.

1.4. Incidente de seguridad

Se considera un incidente de seguridad a un evento adverso en un entorno informático, que puede comprometer o compromete la confidencialidad, integridad o disponibilidad de la información. Una violación o inminente amenaza de violación de una política de seguridad de la información

La seguridad se logra mediante la implementación de un apropiado sistema de controles, que pudieran ser políticas, prácticas, estructuras organizacionales y funciones de software. Las funciones asociadas a la Seguridad informática son las siguientes:

Regulación: capacidad de establecer las normas, preceptos reglamentos y otro tipo de medidas jurídicas que garanticen las bases para lograr un nivel de seguridad adecuado.

Prevención: las acciones que se realizan con el fin de minimizar los riesgos contra los activos informáticos.

Detección: Conocimiento de la materialización de una amenaza contra los activos informáticos.

Enfrentamiento: Acciones de respuesta a un hecho detectado contra los activos informáticos.

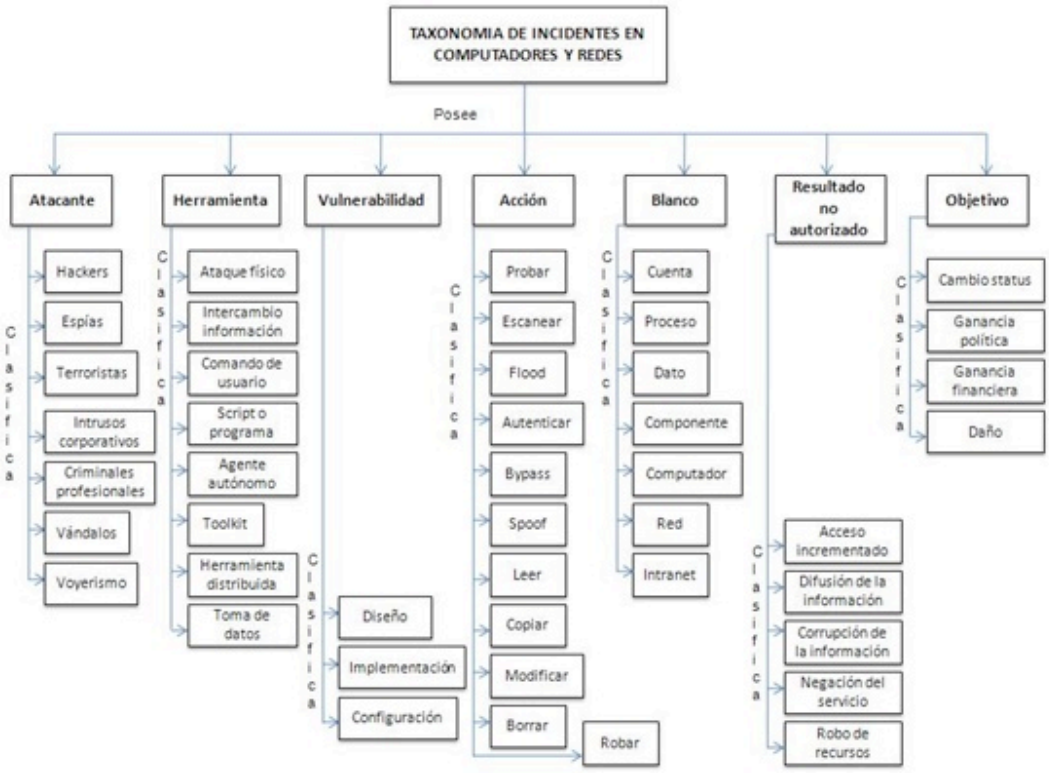


Figura 1. Taxonomía de incidentes de redes y computadores.

1.5. Principios básicos de la seguridad informática

Existen algunos mecanismos y estrategias a seguir para mantener una adecuada seguridad informática y es a lo que llamamos Principios básicos de Seguridad Informática:

- **Mínimo privilegio**

Se deben otorgar los permisos estrictamente necesarios para efectuar las acciones que se requieran, ni más ni menos que lo solicitado.

- **Eslabón más débil**

La seguridad de un sistema es tan fuerte como su parte más débil. Un atacante primero analiza cual es el punto más débil del sistema y concentra sus esfuerzos en ese lugar.

- **Proporcionalidad**

Las medidas de seguridad deben estar en correspondencia con lo que se protege y con el nivel de riesgo existente. No sería lógico proteger con múltiples recursos un activo informático

que no posee valor o que la probabilidad de ocurrencia de un ataque sobre el mismo es muy baja.

- **Dinamismo**

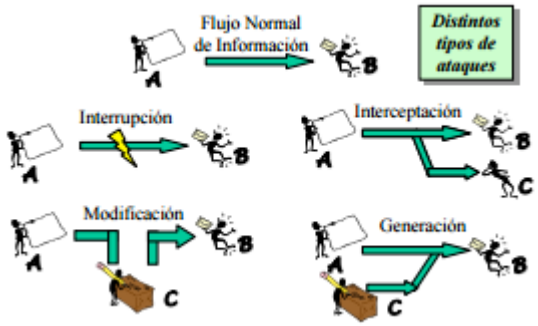
La seguridad informática no es un producto, es un proceso. No se termina con la implementación de los medios tecnológicos, se requiere permanentemente monitoreo y mantenimiento.

- **Participación universal**

La gestión de la seguridad informática necesita de la participación de todo el personal de una institución. La seguridad que puede ser alcanzada mediante medios técnicos es limitada y debiera ser apoyada por una gestión y procedimientos adecuados, que involucren a todos los individuos.

1.6. Tipos de ataques informáticos en una red

A la hora de estudiar los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o acceder a la información guardada o transmitida por el sistema.



1.6.1. Actividades de reconocimiento de sistemas

Estas actividades directamente relacionadas con los ataques informáticos, si bien no se consideran ataques como tales ya que no provocan ningún daño, persiguen obtener información previa sobre las organizaciones y sus redes y sistemas informáticos, realizando para ello un escaneo de puertos para determinar qué servicios se encuentran activos o bien un reconocimiento de versiones de sistemas operativos y aplicaciones, por citar dos de las técnicas más conocidas.

1.6.2. Detección de vulnerabilidades en los sistemas

Este tipo de ataques tratan de detectar y documentar las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas fácilmente (herramientas conocidas popularmente como “exploits”).

1.6.3. Robo de información mediante la interceptación de mensajes

Ataques que tratan de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores como Internet, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.

1.6.4. Modificación del contenido y secuencia de los mensajes

En estos ataques los intrusos tratan de reenviar mensajes y documentos que ya habían sido previamente transmitidos en el sistema informático, tras haberlos modificado de forma maliciosa (por ejemplo, para generar una nueva transferencia bancaria contra la cuenta de la víctima del ataque). También se conocen como "ataques de repetición" ("replay attacks").

1.6.5. Análisis del tráfico

Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los "sniffers". Así, se conoce como "eavesdropping" a la interceptación del tráfico que circula por una red de forma pasiva, sin modificar su contenido.

1.6.6. Ataques de suplantación de identidad

Intentan duplicar un elemento de la red conocido, para hacerse pasar por él y obtener sus privilegios e información. Suelen suplantar la IP de una máquina o su nombre.

1.6.7. Modificaciones del tráfico y de las tablas de enrutamiento

Los ataques de modificación del tráfico y de las tablas de enrutamiento persiguen desviar los paquetes de datos de su ruta original a través de Internet, para conseguir, por ejemplo, que atraviesen otras redes o equipos intermedios antes de llegar a su destino legítimo, para facilitar de este modo las actividades de interceptación de datos.

1.6.8. Ataques de Denegación de Servicio Distribuidos (DDoS)

Los Ataques de Denegación de Servicio Distribuidos (DDoS) se llevan a cabo mediante equipos "zombis". Los equipos "zombis" son equipos infectados por virus o troyanos, sin que sus propietarios lo hayan advertido, que abren puertas traseras y facilitan su control remoto por parte de usuarios remotos. Estos usuarios maliciosos suelen organizar ataques coordinados en los que pueden intervenir centenares o incluso miles de estos equipos, sin que sus propietarios y

usuarios legítimos lleguen a ser conscientes del problema, para tratar de colapsar las redes y los servidores objeto del ataque.

2. Virtualización y Cloud Computing

Hoy en día la mayoría de los appliances están conectados a una entidad misteriosa llamada "Cloud". Nuestros teléfonos, ordenadores coches y hasta electrodomésticos están conectados a la Cloud. La computación en la nube o "Cloud Computing" se ha convertido en una palabra de moda, cada gadget nuevo está conectado a la nube o tiene algún tipo de interacción con ella. Detrás de este fenómeno llamado Cloud Computing, hay una tecnología llamada virtualización. La virtualización permite a todos, desde entornos de un solo usuario a grandes empresas la posibilidad de crear máquinas virtuales (VM) dentro de una máquina física, abriendo un abanico de posibilidades. Es posible tener diferentes tipos de sistema operativo (OSs) o el mismo con diferentes configuraciones ejecutándose en la misma máquina. Cuando usamos una Cloud pública podemos alquilar tanto una máquina virtual para alojar una simple página web, a 10.000 máquinas virtuales para alojar una compañía de video por streaming. A continuación, vamos a desarrollar los tipos de entorno virtualizados que podemos encontrar.

2.2. Tipos de entornos virtualizados

Cuando se crea un servicio en la Cloud, es necesario decidir entre usar una Cloud pública, privada o hibrida. La computación en Cloud es normalmente un sinónimo de entorno Cloud Pública, pero existen dos soluciones adicionales.

En un entorno de **Cloud Pública,** un proveedor se encarga de proveer el hardware, APIs y herramientas a los clientes para desarrollar sus sistemas. Proveen además de una solución bajo demanda que puede crecer y decrecer a voluntad. Es de coste escalable y usualmente más barato que construir un entorno Cloud privado u On-site. Es más fácil de desplegar y más rápido, además de tener normalmente herramientas de monitorización.

Una **Cloud privada** permite tener un mayor control sobre el hardware y el software que se va a utilizar, acceder directamente al entorno virtualizado, mantener y monitorizar el sistema. Una Cloud privada tiene un punto de seguridad extra (siempre que se ponga suficiente hincapié en ello), ya que puedes controlar exactamente la interacción entre las máquinas que se ejecutan en el entorno.

La última opción, es combinar ambas en un **Cloud híbrida,** donde parte de la Cloud se mantiene On-site y otra parte en un proveedor de terceros, con esto se mantienen en parte los beneficios de los dos entornos.

Tipos de nubes en Cloud Computing

2.3. Tipos de Hipervisores

El hipervisor es el encargado de permitir que la virtualización funcione. El hipervisor es un software, hardware o firmware que tiene la capacidad de controlar crear y hacer funcionar máquinas virtuales. También es llamado Host de virtualización, mientras que las máquinas virtuales se les llama máquinas clientes (o Guests). Además de la creación y funcionamiento de las máquinas virtuales, el hipervisor también se encarga de proveer de ciertos servicios al entorno de virtualización como puede ser gestión de la carga, conectividad de red, etc. Hay dos tipos de hipervisores, los llamados **bare-metal** hipervisor, donde el hipervisor esta embedido en el kernel del SO y los "**top OS"** donde el hipervisor corre por encima del sistema operativo como si se tratara de una aplicación más.

2.4. Seguridad en redes virtuales

Las nuevas tecnologías aportan grandes beneficios a las infraestructuras en su operativa diaria, no obstante, no hay que dejar de lado la seguridad de los datos y su acceso a través de la red.

Especialmente la virtualización aporta sustanciales mejoras tanto en la facilidad de gestión, automatización, flexibilidad y consolidación de los recursos en las empresas, no

obstante, estos entornos se enfrentan a retos de seguridad únicos en la red, que pueden afectar directamente a la empresa en su conjunto.

Por suerte es fácil el despliegue de dispositivos virtuales que nos permitan proteger este entorno frente a estos {problemas}, además de adoptar ciertas medidas de seguridad y políticas de "defensa en profundidad".

2.4.1. Entendiendo los problemas de la seguridad en la red virtual

Hasta ahora se había considerado que la seguridad adoptada en la red y los métodos de auditoría de los entornos físicos podían ser suficientes, estas reglas se deben reformular en un entorno virtualizado, ya que estas medidas no permiten abordar todos los "problemas". Algunas de las nuevas consideraciones a tener en cuenta son:

Visibilidad dentro del entorno virtualizado: El tráfico dentro de una red virtual puede ser inspeccionado y debe ser auditado.

Cumplimiento de las regulaciones: Existen ciertos estándares que deben mantenerse y hay que tener en cuenta su aplicación dentro del entorno virtualizado.

Problemas de seguridad en los servidores virtualizados: Ya que los servidores se trasladan a otros entornos, estos pueden comprometer la seguridad del nuevo entorno.

Control de acceso a los datos: Al igual que en las redes físicas, se debe garantizar que los recursos son solamente accedidos por los dispositivos e individuos autorizados.

Detección y prevención de intrusiones: Hay que monitorizar de forma constante los entornos para prevenir intrusiones y abordarlas cuando estas se detectan.

Mala configuración del entorno virtualizado: Mientras que en redes físicas el diseño puede ser chequeado siguiendo la conexión entre los diferentes dispositivos, los entornos virtuales se enfrentan a posibles problemas de mala configuración que pueden ser difíciles de detectar.

2.4.2. Evaluación de las soluciones de seguridad en entornos virtuales

Es de vital importancia que una solución de seguridad virtualizada proporcione alta disponibilidad, una velocidad adecuada y no consumir excesivos recursos de las máquinas en las que se encuentra, evitando así causar problemas al resto de máquinas que proporcionan funcionalidad crítica y coexisten con ella.

Para ser práctica, la solución debe poder ser adquirida, desplegada y gestionada de forma que no repercuta en un coste excesivo. Los criterios a tener en cuenta son:

- Sencillez del despliegue, configuración y administración de la solución.

- Integración y facilidad de extensión de funcionalidades.

- Costes de adquisición, mantenimiento y actualización asequibles.

2.4.3. Securizando redes virtuales: Necesidades

Un paso crítico para establecer la seguridad del entorno virtualizado es establecer el contexto de la solución. Para ello deberemos tener en cuenta las siguientes consideraciones:

Características del entorno virtual:

- Plataforma a usar.
- Capacidad de proceso y memoria necesaria.
- Infraestructura virtual (vSwitches, Switchs físicos o VLANS).

Características de los recursos protegidos:

- Tipo de servidores, sistemas operativos y aplicaciones que requieren protección.
- Características de los datos protegidos (Cantidad, formato, sensibilidad, valor, etc.)
- Políticas de auditoría/repporting a aplicar
- Requerimientos de disponibilidad y recuperación ante desastres de los recursos críticos.

Factores de riesgo especiales:

- Consecuencias de una brecha de seguridad en el entorno.
- Regulaciones a tener en cuenta con las que haya que cumplir.

Topología de red física:

- Lugar de despliegue del entorno virtualizado con respecto a la red local.
- Puntos clave respecto a la topología y rendimiento de la red física.

Vectores de ataque posibles:

- Posibles vías de acercamiento al entorno virtualizado.
- Posibles atacantes del entorno virtualizado.

Requerimientos de acceso:

- Personal que deba acceder al entorno virtualizado y con qué propósitos.
- Tipo de autorización, autenticación y acceso proporcionado.
- Nivel de confianza y competencias que deben ser asociadas a los usuarios del entorno virtualizado.

Existencia de medidas de seguridad en la red previamente establecidas:

- Soluciones de seguridad ya desplegadas (Firewalls, IP'S, etc.)
- Capacidades que ofrecen estas soluciones al entorno virtual.
- Posibles problemas de compatibilidad.

Restricciones operativas y administrativas:

- Necesidad de disponibilidad de los recursos operativos, operacionales y contables.
- Integración de la solución de seguridad virtualizada con las políticas ya existentes, tecnologías y sistemas de reporte administrativo.

2.4.4. Buenas prácticas de seguridad para entornos virtualizados

A medida que los entornos virtuales crecen, se debe llegar a medidas efectivas y eficientes que peritan corregir los riesgos de forma adecuada. Esto normalmente conlleva un mix de soluciones de seguridad tanto físicas como virtuales. Utilizando plataformas de seguridad de confianza, se puede adoptar una política de "seguridad en profundidad" y unas buenas prácticas de seguridad en entornos virtualizados que permitan reducir el coste frente a complejas soluciones físicas.

Adicionalmente tendremos en cuenta las siguientes pautas:

- Seguir las "best practices" en virtualización.

- Determinar los objetivos de la seguridad

-Implementar una solución de seguridad integral

-Tomar un enfoque por capas a la seguridad

- Adaptar la plataforma de virtualización para permitir la seguridad.

3. Entorno de laboratorio

Para poder mostrar en un caso real y práctico, además de poder comparar la solución de seguridad con la de un entorno tradicional sin virtualización, se han utilizado los siguientes elementos:

3.1. Servidores

3.1.1. Servidor de Virtualización

Se trata de un Sistema operativo optimizado para la ejecución de máquinas virtuales. Sobre él desplegaremos las diferentes máquinas que componen el entorno y se definirán las diferentes redes de nivel 2.

VMWARE ESXI 6.0 UPDATE2

CPU	Intel Core i7 4770 3,6 GHZ Quad Core
CPUS	1
RAM	8 GB DDR3 1600
HD	40GB SSD

3.1.2. Servidor de gestión del entorno de Virtualización

Servidor Vmware vCenter. Esta máquina se utiliza para la gestión centralizada del entorno virtual. Es de vital importancia cuando se tiene un entorno con varios Hipervisores. En nuestro caso, por simplicidad utilizaremos solamente un hipervisor, pero la inclusión de nuevos hipervisores es trivial.

VMWARE VCENTER SERVER

VCPUS	*1*
RAM	*2 GB DDR3 1600*
HD	*20GB SSD*

3.1.3. Servidor de DNS

Servidor basado en Debian para la resolución de nombres.

3.1.4. Servidor DHCP

Servidor basado en Debian para la asignación dinámica de IP'S para las diferentes subredes que lo requieran.

3.1.5. Servidor WEB

Servidor basado en Debian que dispondrá de un servicio web accesible desde la WAN.

SERVIDORES DEBIAN

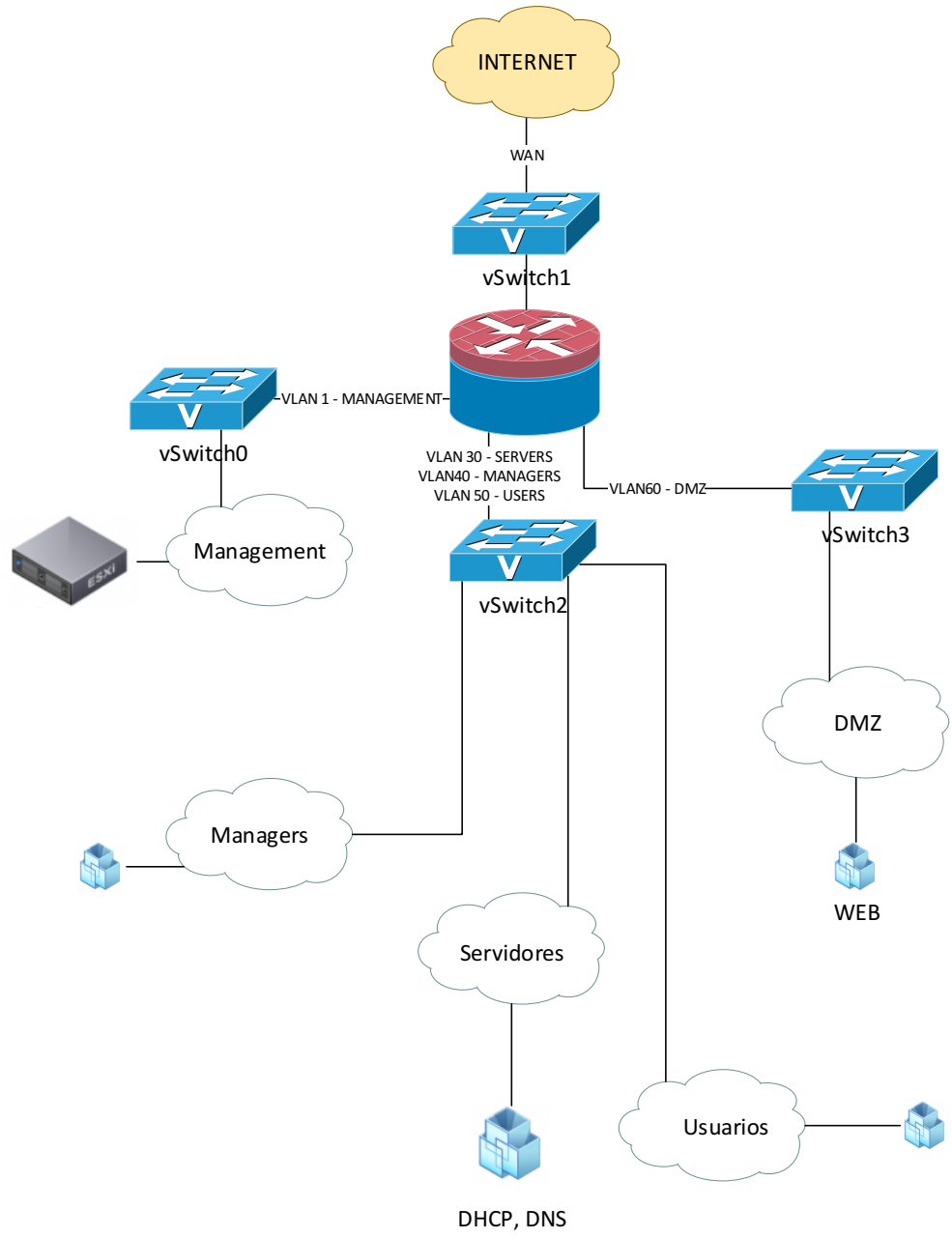
VCPUS	*1*
RAM	*1 GB DDR3 1600*
HD	*5 GB SSD*

3.2. Red de prueba

Para confeccionar la red de prueba hemos optado por un Firewall FreeBSD que incorporará tanto la función de Firewall como la de routing. Este nos permitirá dar conectividad a toda la red, enrutar el tráfico y securizar.

Hemos segmentado mediante vlans los distintos tipos de tráfico para gestionarlos de forma más eficiente y poder gestionar el acceso desde el firewall a los distintos dispositivos.

3.2.1. Modelo de Red



- **Usuarios (LAN)**

Red en la cual estarán los equipos de usuario. Esta red tendrá acceso a los servicios internos necesarios para el correcto funcionamiento de la organización, así como acceso a internet.

- **Managers (LAN)**

Red en la que se alojarán los equipos del personal de TI encargados del mantenimiento de la plataforma descrita. Esta red tendrá habilitado el acceso al resto de subredes para el correcto desempeño de las funciones del personal indicado.

- **Servers (LAN)**

Red sobre la que se desplegarán los diferentes servicios internos que serán accesibles desde la red interna por el personal que requiera de su uso para el desempeño de su trabajo.

- **Management (LAN)**

Sobre esta red residirán los interfaces de gestión de los diferentes elementos. Esta red es de vital importancia sobre entornos virtualizados, ya que, en caso de compromiso, se podría tener acceso a todas las máquinas virtuales que componen el entorno.

- **Servicios_Externos (DMZ)**

Sobre esta red se desplegarán los diferentes servicios expuestos a internet. Es de vital importancia que está red no tenga permitido el acceso a la LAN.

- **Acceso_Remoto (VPN)**

Se trata de una red virtual que se genera cuando los diferentes clientes externos establecen un túnel VPN para el acceso a la red interna.

Tras el establecimiento del tunel VPN, esta red virutal se tratará como si de otra red interna se tratase, aplicándose las reglas de filtrado en función de los requisitos del usuario. Diferenciaremos dos perfiles, usuarios y managers. Los managers tendrán acceso a todas las redes para su correcta gestión, y los usuarios solamente a los servicios habilitados para el correcto desempeño de su trabajo.

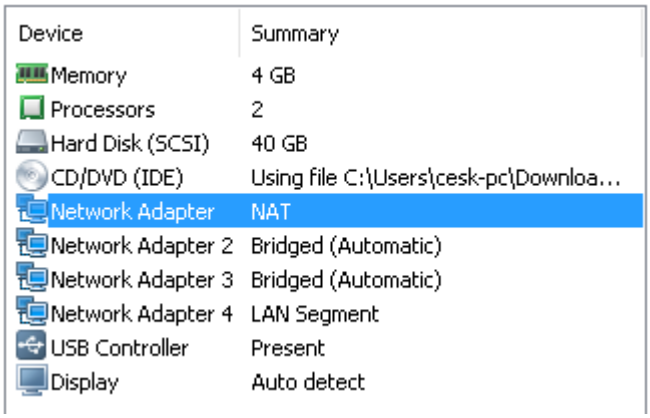
3.3. Firewall PFSense

Para hacer la función de firewall hemos elegido el dispositivo PFSense, se trata de una máquina virtual basada en FreeBSD que incorpora la funcionalidad de firewall, routing y UTM. Su función será enrutar y filtrar el tráfico entre las diferentes subredes generadas, siendo un pilar fundamental en la seguridad el entorno presentado.

Adicionalmente proporcionará servicios de VPN para la conexión segura desde el exterior a los diferentes tipos de usuarios.

4. Configuración de red Capa 2

Empezamos por la configuración a nivel 2 de la red virtualizada. El primer punto de configuración son las tarjetas de red el servidor ESXi. Indicar que son el número de tarjetas mínimo para garantizar el buen funcionamiento del entorno. Se puede ampliar cualquier grupo de tarjetas realizando una agregación de puertos para maximizar el ancho de banda.



Las dos tarjetas de red que se encuentran en modo Bridge Network adapter 2 y Network adapter 3 serán los correspondientes a la gestión, una se encontrará en modo activo y la otra en modo backup. Esto permitirá que ante un ataque que deje sin conectividad una de las dos interfaces, tendremos una de backup para poder recuperar la gestión del entorno. La Network adapter 4 correspondera al segmento de red local que dividiremos mediante vlans. Por último el primer adaptador de red corresponde con el que nos dará conectividad WAN.

IP de gestion 1: 192.168.10.2

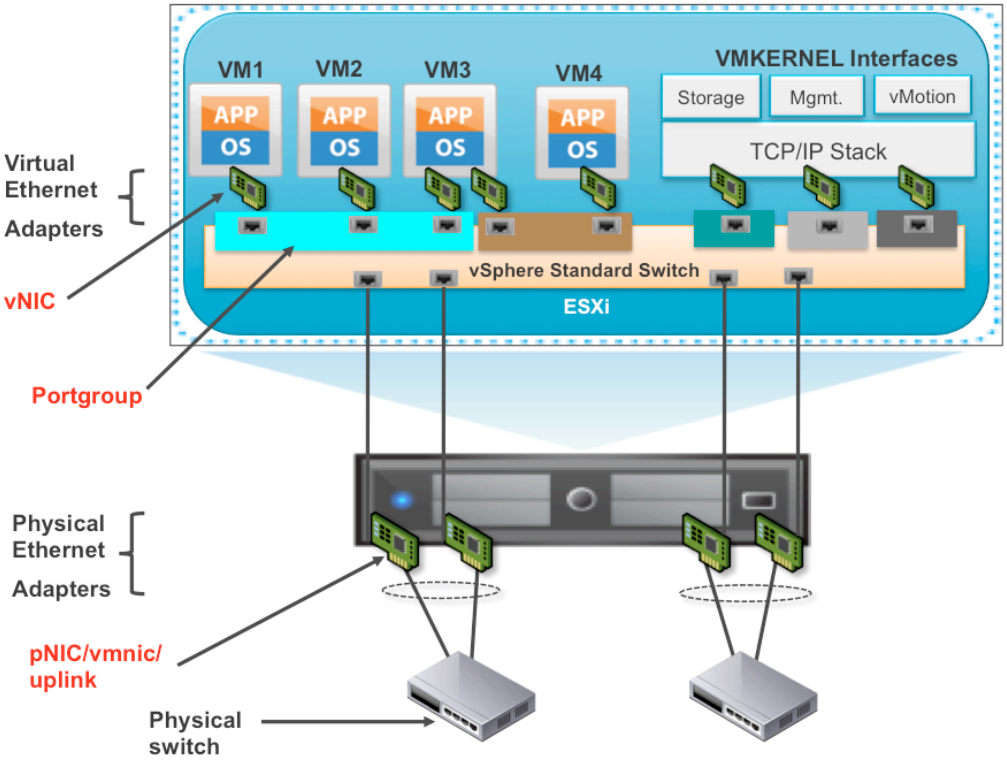
IP de gestion 2: 192.168.10.3

Puerta de enlace: 192.168.10.1

4.2. Switches virtuales

Para vmware un switch virtual hace la misma función que un switch físico de capa 2 (layer 2). Cada switch virtual puede tener asignadas múltiples tarjetas físicas (up-links), que son las que van a proveer de conectividad hacia el exterior (aunque no es estrictamente necesario). El Switch virtual posee puertos de red llamados virtual port group, estos puertos emulan la

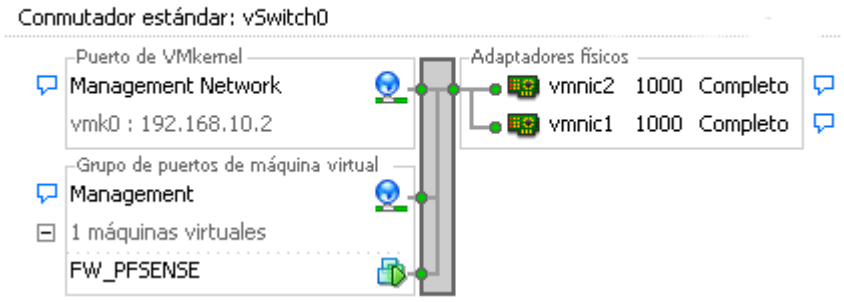
funcionalidad de los puertos de un switch físico. Las máquinas virtuales conectarán sus vNics a los puertos del switch virtual, de esta manera se podrán comunicar entre ellas y hacia el exterior.



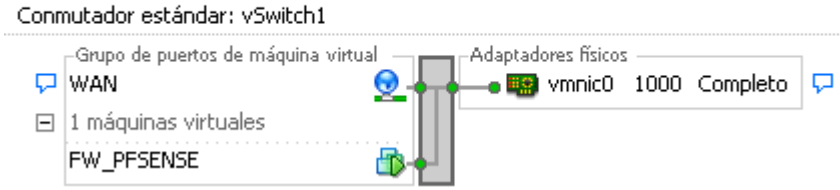
4.2.1. Configuración de los switches virtuales

El primer Switch virtual **vSwitch 0** se compone de un virtual machine port group y un vmkwenel. El vmkernel dará acceso a la gestión del Hipervisor sobre el que residen las máquinas virtuales. Por otro lado, el virtual machine port group de Management dará acceso a la gestión del firewall y aquellas máquinas que se pusieran en la vlan de gestión, tanto física como virtual.

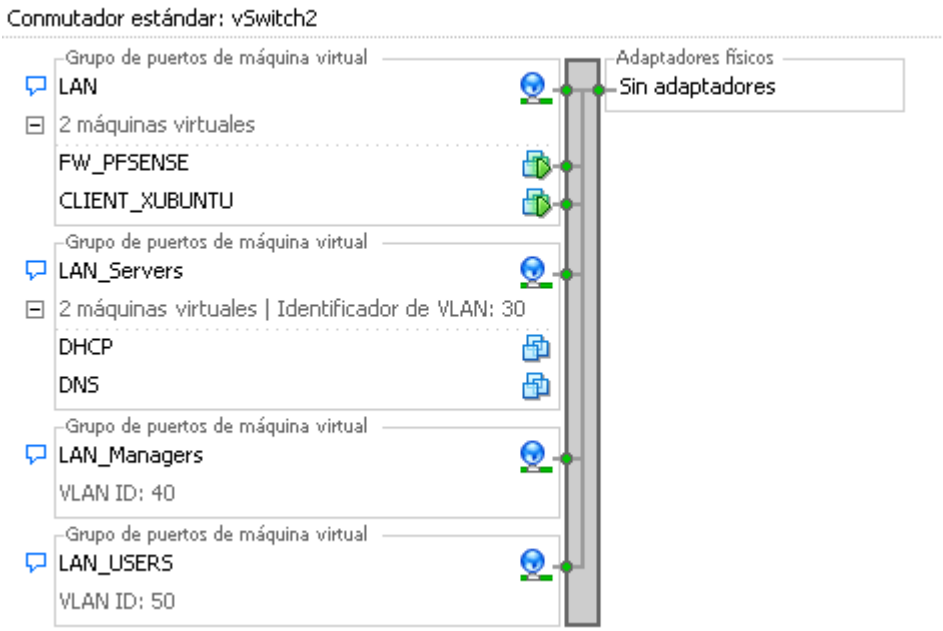
Las dos tarjetas de red están en modo activo-pasivo, de tal manera que en caso de que se comprometa la integridad de una de las dos seguiremos teniendo acceso a la gestión del mismo.



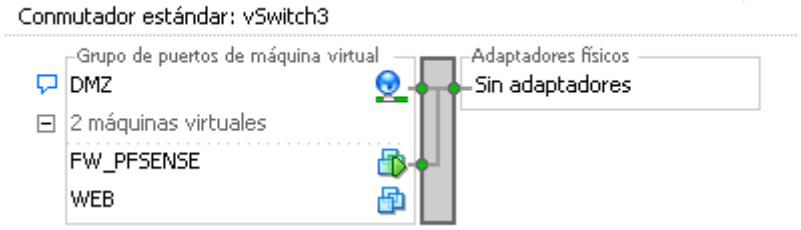
En cuanto al **vSwitch1**, es el encargado de proporcionar conexión através del uplink hacia la WAN. Únicamente tendrá conectado a través de un virtual machine port group, el firewall (PFSense).



El **vSwitch2** se ha segmentado en diferentes subredes, diferenciando el tipo de trafico empleando vlans. A pesar de compartir un mismo switch el tráfico entre vlans queda totalmente aislado para que sea el Pfsense el encargado desu enrutamiento y filtrado. Este switch virtual no dispone de uplinks, ya que será el Pfsense el encargado de proporcionar conectividad hacia el exterior.



Por último, el **vSwitch3**, será el encargado de alojar las máquinas destinadas a prestar servicio al exterior através de la WAN. Tampoco dispondrá de interfaces uplink, de esto se encargara el firewall Pfsense.



Descripción de vlans:

Las tarjetas de red de gestión las pondremos en la vlan por defecto para que ante cualquier eventualidad podamos conectarnos directamente a las mismas, sin necesitdad de tener configurada ninguna vlan (Disponibilidad).

5. Configuración de red Capa 3

Para la interconexión y enrutamiento del tráfico entre las diferentes subredes, utilizaremos el firewall PFSense. Para ello será necesario definir una itnerfaz del firewall en cada una de las diferentes subredes.

5.2. Definición de interfaces

Cada una de las interfaces definidas en el firewall dispondrá de una IP estática, la cual hará de puerta de enlace para los nodos de cada subred.

Interface	*Tipo*	*IP Asignada*	*Mapeo vNic*	*Uso*
WAN	Regular	DHCP	Vmx0	Acceso Wan
MANAGEMENT	Regular	192.168.10.1	Vmx1	Gestión
DMZ	Regular	192.168.60.1	Vmx3	Servicios externos
VLAN_SERVERS	vLan	192.168.30.1	Vmx2	Red de Servidores
VLAN_MANAGERS	vLan	192.168.40.1	Vmx2	Administradores
VLAN_USERS	vLan	192.168.50.1	Vmx2	Usuarios

5.2.1. Conectividad VPN

Dado la demanda de los usuarios de acceso desde el exterior a la red, se ha configurado una VPN tipo SSL a través de la cual se define una nueva interfaz de red, la cual no aparece como interfaz definida manualmente, permitiéndonos el enrutamiento del tráfico y el posterior filtrado del mismo.

OpenVPN Servers	
Protocol / Port	**Tunnel Network**
UDP / 1194	10.10.0.0/24

5.3. Enrutamiento

Después de definir las interfaces de red, el firewall se encarga de crear todas las rutas necesarias automáticamente. La tabla de rutas quedaría de la siguiente manera:

IPv4 Routes				
Destination	**Gateway**	**Flags**	**Mtu**	**Netif**
default	192.168.32.2	UGS	1500	vmx0
127.0.0.1	link#8	UH	16384	lo0
192.168.10.0/24	link#2	U	1500	vmx1
192.168.10.1	link#2	UHS	16384	lo0
192.168.20.0/24	link#3	U	1500	vmx2
192.168.20.1	link#3	UHS	16384	lo0
192.168.30.0/24	link#9	U	1500	vmx2_vlan30
192.168.30.1	link#9	UHS	16384	lo0
192.168.32.0/24	link#1	U	1500	vmx0
192.168.32.2	00:0c:29:cc:3a:6e	UHS	1500	vmx0
192.168.32.131	link#1	UHS	16384	lo0
192.168.40.0/24	link#10	U	1500	vmx2_vlan40
192.168.40.1	link#10	UHS	16384	lo0
192.168.50.0/24	link#11	U	1500	vmx2_vlan50
192.168.50.1	link#11	UHS	16384	lo0
192.168.60.0/24	link#4	U	1500	vmx3
192.168.60.1	link#4	UHS	16384	lo0

En la tabla de rutas no aparece ninguna ruta referente a la VPN ya que no tiene una puerta de enlace asociada y es el mismo firewall el que se encargará de redirigir el tráfico.

5.4. NAT de salida

Para el correcto acceso a internet, es necesario traducir las IP's internas con la IP asociada a la interfaz de salida. Para ello se definen las siguientes reglas de *nating:*

Automatic Rules:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port
✔	WAN	127.0.0.0/8 192.168.20.0/24 192.168.10.0/24 192.168.60.0/24 192.168.30.0/24 192.168.40.0/24 192.168.50.0/24 10.10.0.0/24	*	*	500	WAN address	*	✔
✔	WAN	127.0.0.0/8 192.168.20.0/24 192.168.10.0/24 192.168.60.0/24 192.168.30.0/24 192.168.40.0/24 192.168.50.0/24 10.10.0.0/24	*	*	*	WAN address	*	✂

6. Securización de la red

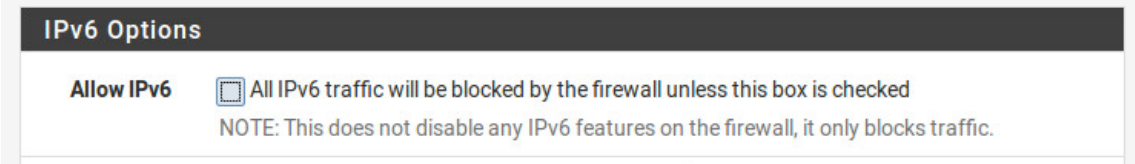
Para la securización de las redes utilizamos las políticas de filtrado del firewall. Permitimos y denegamos el acceso entre las diferentes subredes y dispositivos para garantizar la integridad según el principio de mínimo acceso.

6.2. Securización del firewall appliance

EL primer punto a considerar dentro de la securización de la red es minimizar los posibles puntos de ataque al dispositivo firewall, pues una caída del mismo supone perder la mayor parte de la seguridad de la red.

6.2.1. Protocolo IPV6

Se deshabilita el protocolo IPV6 debido a las múltiples vulnerabilidades que se pueden explotar del mismo.



6.2.2. Acceso externo al firewall

Queda bloqueado todo acceso al firewall a través de la wan, de esta manera evitamos que se pueda comprometer el dispositivo desde un punto externo a la organización.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✖	0/243 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks
✖	0/144 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks

6.2.3. Acceso Interno al firewall

Se ha garantizado únicamente el acceso a través de protocolo seguro (HTTPS) desde la red de gestión al firewall.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✔	7/3.98 MiB	IPv4 TCP	*	*	MANAGEMENT address	*	*	none		Gestión del Firewall

6.3. Securización de la LAN

Para la correcta diferenciación del tráfico en la red local se ha segmentado en 4 subredes diferentes, separando por un lado la red de Servidores, por otro la de administradores o managers, management o gestión y por último la de usuarios. Esto nos permitirá, que cada elemento de la red tenga los mínimos puntos de fallo posibles. Se han generado políticas de acceso entre zonas para los servicios que se prestan en varias subredes.

6.3.1. VLAN Servidores

Con el objetivo de maximizar la seguridad de los servidores, pieza clave de la organización, no se ha permitido la navegación a internet desde los servidores. No obstante, para el correcto desempeño de la resolución de nombres a nivel interno, ha sido necesario permitir la función de relay DNS hacia servidores externos.

	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✔	IPv4 TCP/UDP	DNS Server	53 (DNS)	*	53 (DNS)	*	none		Permitir Relay DNS al servidor Interno.

6.3.2. VLAN Manager

Debido a la necesidad por parte del equipo de Ti que da soporte a la organización, se han implementado unas reglas específicas que les garantizan el pleno acceso al resto de redes y a Internet.

	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✔	IPv4 TCP/UDP	MANAGEMENT net	*	VLAN_USERS net	*	*	none		Acceso a la red de usuarios.
✔	IPv4 TCP/UDP	MANAGEMENT net	*	MANAGEMENT net	*	*	none		Acceso a la red de gestión.
✔	IPv4 TCP/UDP	MANAGEMENT net	*	VLAN_SERVERS net	*	*	none		Acceso a la red de servidores.
✔	IPv4 TCP	VLAN_MANAGER net	*	*	*	*	none		Acceso completo a internet.

6.3.3. VLAN Users

El desempeño de la operativa de los usuarios y la necesidad de tener servicios básicos como correo, navegación y servicio de DNS, ha requerido la implementación de las siguientes reglas:

	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✔	IPv4 TCP	VLAN_USERS net	*	*	25 (SMTP)	*	none		Servicios de correo.
✔	IPv4 TCP	VLAN_USERS net	*	*	443 (HTTPS)	*	none		Navegación Usuarios.
✔	IPv4 TCP	VLAN_USERS net	*	*	80 (HTTP)	*	none		Navegación Usuarios.
✔	IPv4 TCP/UDP	VLAN_USERS net	53 (DNS)	DNS Server	53 (DNS)	*	none		Acceso a los servicios DNS del servidor interno.

Podemos distinguir 2 tipos de reglas, las de acceso a otras subredes y las de acceso a la WAN. Por una parte, se permite el tráfico de servicios básicos cómo la navegación y el correo hacia la WAN. Por otro lado, el tráfico DNS que va hacia la red de servidores desde la de usuarios.

6.3.4. VLAN Management

Hay que tener especial consideración en esta red, pues es la encargada de proveer acceso a la configuración y gestión de todos los elementos críticos del entorno. En caso de verse comprometida, todos los sistemas se verían impactados por el ataque. Debido a esto, solamente se permiten los servicios básicos de resolución DNS de forma interna y ningún usuario que no sea administrador tiene acceso a la misma.

	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✔	IPv4 TCP/UDP	MANAGEMENT net	*	DNS Server	53 (DNS)	*	none		Acceso a los servicios DNS del servidor interno.
✔	IPv4 TCP	VLAN_MANAGER net	*	VLAN_MANAGER address	443 (HTTPS)	*	none		Acceso a la gestión del Firewall.

La regla que vemos al final, corresponde a la que permite el acceso a la interfaz de gestión del firewall.

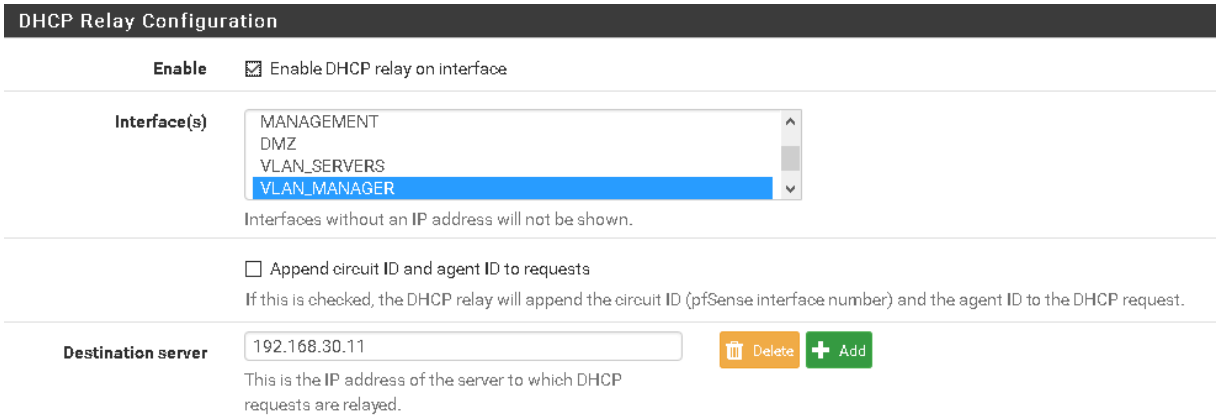
6.4. DMZ

Es necesario separar los servicios que se van a acceder desde el exterior en una VLAN diferencia. Se han creado un Port Forwarding que permitirá el acceso al portal web desde el exterior.

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports
✔	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.60.10	80 (HTTP)
✖	MANAGEMENT	TCP	*	*	LAN address	443 (HTTPS)	192.168.20.1	443 (HTTPS)

6.5. DHCP Relay

Para el correcto aprovisionamiento de IP's a las máquinas clientes. Se ha optado por implementar un DHCP relay en el PFSense. Esto nos permitirá garantizar la integridad del Servidor DHCP ante posibles ataques sin necesidad de generar políticas específicas de protección.



7. Conclusiones

Después de las pruebas realizadas sobre el entorno de test, hemos podido constatar de forma empírica las implicaciones y peculiaridades que tiene securizar un entorno de red dentro de una cloud. Además, hemos podido comparar la solución con un entorno de red físico para extraer las ventajas y desventajas que supone optar por la virtualización.

Se ha demostrado que un entorno de red virtualizado es capaz de cumplir los principios básicos de la seguridad informática. Supone una solución basada en un modelo escalable y fácilmente gestionable que permite crecer de forma controlada y mantenerlo adecuadamente. Es económicamente viable y fácil de implementar debido a la deslocalización de los sistemas.

Respecto de un entorno tradicional, hay que tener en cuenta los mismos principios básicos de seguridad y adicionalmente controlar mediante medidas específicas las peculiaridades que aparecen en un entorno de red virtualizado.

8. Anexos

Dhcp

```
##Configuración servicio DHCP
#LAN_Managers -  VLAN40
subnet 192.168.40.0 netmask 255.255.255.0 {
  range 192.168.40.10 192.168.40.200;
  option routers 192.168.40.1;
  option domain-name-servers 192.168.30.10; #VM DNS
}

#LAN_Users -  VLAN50
subnet 192.168.50.0 netmask 255.255.255.0 {
  range 192.168.50.10 192.168.50.200;
  option routers 192.168.50.1;
  option domain-name-servers 192.168.30.10; #VM DNS
}

default-lease-time 600;
max-lease-time 7200;
```

DNS

```
options {
  directory "/var/named";
```

```
  version "get lost";

  allow-transfer {"none";};

      allow-recursion
      {192.168.30.0/24;192.168.40.0/24;192.168.50.0/24;192.168.6
      0.0/24;};

  forwarders {

                8.8.8.8;

                8.8.4.4;

  };

};



zone "." {

  type hint;

  file "root.servers";

};
```


Interfaces

```
##Network DNS:
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.30.10
netmask 255.255.255.0
gateway 192.168.30.1

##Network DHCP:
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.30.11
netmask 255.255.255.0
gateway 192.168.30.1

##Network WEB:
auto lo
iface lo inet loopback
```

```
auto eth0

iface eth0 inet static

address 192.168.60.10

netmask 255.255.255.0

gateway 192.168.60.1


##VMManagers

auto lo

iface lo inet loopback


auto eth0

iface eth0 inet dhcp


##VMUsers

auto lo

iface lo inet loopback


auto eth0

iface eth0 inet dhcp
```


9. Bibliografía

[1] Lars Nielsen. The Little Book of cloud computing. 2014.

[2] Expand-Your-Virtual –Infrstructure- With-Confidence-And-Control, 2014. http://

www.vmware.com/files/pdf/smb/Expand-Your-Virtual-Infrastructure-With-Confidence-And-Control.pdf.

[3] Introducción a la seguridad informática. URL: http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica

[4]Gómez Alvaro, 2014. Tipos de ataques y de intrusos en las redes informáticas.

[5]Vasquez, Luis, 2012. Las Nubes Hibridas. URL: http:// http://ingenierosoym.blogspot.com.es/

[6] Introducción a la seguridad informática, Julio 2016. URL: http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica

[7] Mena, E. (6 de Julio de 2013). Sugerencias para la memoria de PFCs, TFMs, y Tesis Doctorales. URL: http://eolo.cps.unizar.es/docencia/PFC/Sugerencias-Documentacion.pdf

[8] Pol. (19 de Febrero de 2009). Kaos Klub. Obtenido de Kaos Klub:

http://www.kaosklub.com/recursos-y-consejos-para-hacer-el-pfc-proyecto-final-de

carrera/

[9] Fahmida Y. Rashid, Marzo 2016. The dirty dozen: 12 cloud security threats. URL: http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html

[10] Cloud computing security, Agosto 2016. URL: https://en.wikipedia.org/wiki/Cloud_computing_security

[11]Marshal, David. Best practices for securing virtual networks part one of three. URL: http://vmblog.com/archive/2008/03/26/best-practices-for-securing-virtual-networks-part-one-of-three.aspx#.V95qfSiLSUl

[12] Marshal, David. Best practices for securing virtual networks part two of three. URL: http://vmblog.com/archive/2008/03/27/best-practices-for-securing-virtual-networks-part-two-of-three.aspx#.V95q7yiLSUl

[13] Marshal, David. Best practices for securing virtual networks part three of three. URL: http://vmblog.com/archive/2008/03/28/best-practices-for-securing-virtual-networks-part-three-of-three.aspx#.V95q-iiLSUl

[14]: García Rambla, Juan Luis. Ataques en redes de datos IPv4 e IPv6. 2015. Ed: 0xWord.

[15]: González Pérez, Pablo. Ethical Hacking, Teoría y Práctica para la realización de un pentesting. 2014. Ed: 0xWord.

[16]The Fortinet Company. The Fortigate Cookbook, FortiOS 5. 2015. ED: Fortinet Publishing.

[17] Keith, Barker. Penetration Testing with Linux Tools. URL: https://www.cbtnuggets.com/it-training/penetration-testing-backtrack-kali-linux.