Simulación de un entorno real con Firewall virtualizado basado en PfSense

Joan Menéndez Alaminos

Resumen– Con la aparición cada vez mayor de nuevas tecnologías y nuevos softwares, las empresas necesitan poder tratar estos nuevos servicios en un entorno que les proporcione la seguridad de saber que, si algo falla, el entorno de producción de la empresa no se verá afectado. Para ello, en este trabajo se plantea la idea de crear un entorno (llamado comúnmente Preproducción) lo más parecido a un entorno real. Dependiendo del tamaño de la infraestructura de una empresa, crear un entorno idéntico al real puede suponer un coste muy elevado. Por esta razón en este proyecto se ha trabajado con varias herramientas Open Source, para comprobar si a través de ellas, se puede crear un entorno competente que simule la realidad. La herramienta principal en la que se ha basado este proyecto es PfSense, un firewall virtual con una gran capacidad para proteger la infraestructura. La finalidad de este proyecto consiste en poder analizar el desempeño de un entorno virtualizado o , por el contrario, si es necesario duplicar un entorno a nivel físico, con el coste que conlleva.

Palabras clave– Firewall, PfSense, Nagios, Vmware Workstation, VPN, DCHP, Active Directory, DMZ, Preproducción, Crontab, Squid Proxy, NAT.

Abstract– With the growing emergence of new technologies and new software, companies need to be able to handle these new services in an environment that gives them the security of knowing that, if something goes wrong, the production environment of the company will not be affected. For this, in this project the idea is to create an environment (commonly called Preproduction) the closest thing to a real environment. Depending on the size of the infrastructure of a company, creating an environment identical to the real one can be very expensive. For this reason, in this project we have worked with several Open Source tools, to see if through them, you can create a competent environment that simulates reality. The main tool on which this project has been based is PfSense, a virtual firewall with a great capacity to protect the infrastructure. The purpose of this project is to analyze the performance of a virtualized environment or, conversely, if it is necessary to duplicate an environment at a physical level, with the cost involved.

Keywords– Firewall, PfSense, Nagios, Vmware Workstation, VPN, DCHP, Active Directory, DMZ, Pre-production, Crontab, Squid Proxy, NAT.

1 Introducción

Hoy en día, es habitual que cada poco tiempo salgan al mercado nuevos softwares, actualizaciones tanto de sistemas operativos como de aplicaciones, nuevos servicios, etc. Cuando una empresa se plantea implementar estas nuevas herramientas, existe el temor que el entorno deje de funcionar correctamente, ya que dentro de la infraestructura existen muchas dependencias entre softwares (Firewall, backup, bases de datos...).

Es por ello por lo que las empresas acostumbran a disponer de varios entornos de infraestructura:

- Desarrollo: Entorno que se utiliza para realizar modificaciones en alguna aplicación, añadir nuevas características o corregir algunos errores.
- Preproducción: Entorno que se utiliza para probar y testear las nuevas aplicaciones, modificaciones, servicios, etc. Se trata de la fase previa antes de llevar a producción los nuevos cambios.
- Producción: Entorno principal de cualquier empresa. Se trata del entorno crítico donde se encuentran todos los servicios finales, usuarios y aplicaciones. Sin el

• Correo de contacto: joanmanuel.menendez@e-campus.uab.cat
• Mención realizada: Tecnologías de la Información
• Trabajo tutoritzado por: Ángel Elbaz (Ingeniería de la información y comunicaciones)
• Curso 2019/2020

correcto funcionamiento de este entorno, difícilmente una empresa puede ofrecer el servicio correspondiente.

Fig. 1: Flujo de cambios entre los entornos.

Este proyecto esta basado sobre el entorno de Preproducción. Se trata de un entorno indispensable en cualquier empresa, sobretodo en las que ofrecen servicios. Este entorno debe ser configurado y desarrollado para obtener una réplica exacta (o lo más parecida) al entorno de Producción. Una vez desarrollado, permite realizar pruebas como testear nuevas aplicaciones, nuevas funcionalidades desarrolladas, verificar nuevas configuraciones de cualquiera de los servicios, etc. Si los resultados son satisfactorios, dan la garantía que en el entorno de Producción los nuevos cambios tendrían que funcionar adecuadamente.

En cualquier empresa de mediano/gran tamaño, la inversión en la infraestructura acostumbra a ser de gran valor, ya que existen una gran variedad de elementos como cabinas de almacenamiento, switches, Firewall, servidores físicos... Este hecho conlleva a que, desarrollar un entorno de Preproducción de manera física implique un coste muy elevado, ya que supone duplicar la compra de todos los elementos. Por ello, en este proyecto se plantea la idea de elaborar este entorno virtualizando todas las máquinas y servicios para poder crear un entorno igual al de producción, pero con menos coste. Debido a que se trata de una simulación y no una réplica de un entorno real, se ha realizado con herramientas Open Source.

La principal y más importante herramienta es el Firewall PfSense, uno de los firewalls gratuitos más utilizados en el mundo [1]. Se trata de un software Open Source con base Debian (Linux) que el fabricante pone a disposición de cualquier usuario. Se trata de un firewall muy reconocido a nivel mundial ya que es efectivo, está bien documentado y se le está dando seguimiento por parte de los desarrolladores con el fin de estar a la altura de las demandas de seguridad de hoy en día.

Además, se irán añadiendo nuevos servicios y funcionalidades que permitirán ir conformando el entorno que se quiere crear, como la Alta Disponibilidad, que permite crear un clúster de nodos PfSense o el servicio NDMP usado para compartir información con las herramientas de monitorización.

Para realizar este proyecto se ha usado como virtualizador una computadora propia que corre Windows 10, con 16 Gb de RAM y procesador Intel Core i5 7600k de 3,8 GHz.

2 Motivación

La motivación principal de este proyecto consiste en crear y valorar el funcionamiento de un entorno de preproducción a través de herramientas Open Source, ya que habitualmente la confianza reside en los grandes softwares de pago. En cualquier infraestructura de una empresa con un mínimo de recursos, se puede encontrar como mínimo un firewall, servidores físicos que proporcionan servicios (SQL, Exchange, etc), software de backup, switches que administran las conexiones internas, etc. Si uno se pone a hacer cálculos, entre la parte física de cada elemento y las licencias, el coste puede llegar a ser muy elevado. En este proyecto, además de crear de forma virtual un entorno de preproducción, se trabajará con el firewall PfSense.

Otro aspecto a destacar es la demanda de seguridad de hoy en día. Cada vez son más comunes las infecciones a sistemas a través de Pishing, Ransomware, Botnets, etc. En este proyecto se tratará de configurar el firewall de la manera más ajustada posible a la infraestructura con el fin de garantizar unos mínimos de seguridad. En un entorno de preproducción más completo, son muchos los factores que intervienen en la seguridad general de la empresa como los antivirus, herramientas de monitorización, agentes instalados en las computadoras, Firewall, configuración de los switches, etc. En este caso, al no disponer de suficientes recursos para dividir lógicamente las subredes a través de switches, todo el tráfico será controlado por el Firewall y gracias a ello podremos crear reglas y configuraciones específicas.

Por último, este proyecto permitirá crecer a nivel personal con el conocimiento y implementación de herramientas importantes usadas a nivel mundial como Active Directory, Nagios, VPN...

3 Objetivos

En esta sección, se detallan los objetivos principales a desarrollar en este proyecto. A lo largo de la explicación técnica, se comentarán las dificultades encontradas para llegar al objetivo y si ha sido posible alcanzarlo o no.

Se han esocgido estos objetivos ya que son la base de creación de cualquier entorno. Como se puede observar, los pilares básicos de este proyecto son la seguridad de la infraestructura, la gestión de los usuarios y la monitorización. A partir de ahí, las herramientas elegidas pueden variar dependiendo de las preferencias de la persona que implemente un laboratorio. Los objetivos que se pretenden son:

- Dar a entender la importancia de tener un entorno de Preproducción correctamente configurado para realizar pruebas.

- Desplegar el firewall PfSense con las correctas configuraciones de seguridad.
- Administración de certificados.
- Gestión de usuarios a través de Active Directory.
- Desplegaruna herramienta de monitorización de la infraestructura.
- Gestionar sistema de backup del firewall.
- Objetivos extra.

3.1. La importancia de tener un entorno Preproducción

Tal y como se ha comentado en la introducción, es importante configurar un correcto entorno de preproducción para desarrollar test y pruebas de nuevos servicios antes de trasladar estos cambios al entorno de producción. A lo largo de este proyecto se mostrará la base a desplegar de la infraestructura.

3.2. Desplegar el firewall PfSense con las correctas configuraciones de seguridad

La base principal de este proyecto consiste en el despliegue de este Firewall virtualizado. El firewall es la capa que separa la infraestructura interna de Internet, por lo que es muy importante establecer unas reglas básicas para el control de tráfico de red. Además, es importante desarrollar una correcta configuración para la comunicación entre las subredes dentro de la infraestructura, ya que así se evitarán comunicaciones innecesarias. Por ejemplo, en caso de ser víctima de una intrusión y que un atacante obtenga el control de la computadora de un usuario final, se evitará el pivotamiento entre servidores.

3.3. Administración de certificados

Cuando se exponen servicios Web a Internet o a la propia corporación, es recomendable obtener un certificado para poder realiza conexiones seguras (HTTPS) y garantizar la privacidad entre los usuarios y los servicios.

3.4. Gestión de usuarios a través de Active Directory

En cualquier empresa en la que existan distintos roles (Administración, Sector IT, Marketing...) es recomendable gestionar los permisos acorde con sus responsabilidades. Cada tipo de usuario, dependiendo de su rol, debe tener acceso a ciertos servicios, servidores o softwares y por el contrario, tener el acceso denegado a otros. En este proyecto se definirá un dominio a través de Active Directory [2] para poder gestionar los usuarios. Se ha decidido utilizar esta herramienta debido a que en la mayoría de las empresas, gran parte de los usuarios finales utilizan computadoras con Windows. Es una herramienta muy potente de gestión que permite realizar configuraciones muy explícitas.

3.5. Desplegar una herramienta de monitorización de la infraestructura

Es importante dispner de una herramienta que monitorice a tiempo real los elementos que se consideren oportunos, en general servidores que ofrecen algún tipo de servicio o el firewall, ya que, sin un correcto funcionamiento de éstos, el desempeño global puede verse seriamente afectado. Para este proyecto, la herramienta utilizada es Nagios [3].

3.6. Gestionar sistema de backup del firewall

Implementar un sistema de backup implica que en caso de desastre (como puede ser la sustitución de un firewall por mal funcionamiento, la corrupción de una base de datos o la entrada de un Ransomware), se disponga de una copia de los datos que existían para poder restablecerlos cuanto antes. En un entorno bien construido, es necesario tener backup de toda la información crítica. En este proyecto, debido a la limitación de recursos, se configurará el sistema de backup de manera que realice una cópia del fichero de configuración del firewall.

4 Estado del arte

Actualmente existe una gran variedad de software que permiten virtualizar máquinas y crear redes virtuales entre ellas, como por ejemplo VMware [4] y VirtualBox [5]. VirtualBox es una herramienta Open Source, disponible para cualquier usuario. Los pros de este software es que es de libre uso, pero, por contra, tiene un límite de creación de cuatro subredes internas. Para proyectos básicos fácilmente se alcanzará este límite. Por el contrario, VMWare es un software de pago que dispone de varias herramientas de virtualización (VMWare Workstation, VMWare ESX). Se trata de herramientas muy potentes utilizadas a nivel mundial.

Inicialmente se decidió utilizar VirtualBox para este proyecto, pero debido a la limitación comentada anteriormente y otros aspectos explicados en la sección técnica, se tuvo que cambiar a VMWare Workstation a los inicios de proyecto.

Por otro lado, en cuanto a los Firewalls Open Source, la comunidad informática coincide en que PfSense se trata del firewall más completo, con mayor documentación por parte del fabricante y varios servicios gratuitos que se pueden instalar [6]. La principal competencia de PfSense es el Firewall IPFire. Se trata también de un software Open Source. Son dos firewalls muy parecidos a nivel funcional, pero con algunas diferencias que pueden decantar a los usuarios a decidirse por uno u otro. IPFire, es un software más básico y sólido. Tiene las funcionalidades algo limitadas a cambio de ser más fácil de configurar y evitar errores. Por el contrario, PfSense es un software más avanzado que empieza desde un nivel muy básico, pero admite la instalación de nuevos servicios de manera muy rápida que permiten aumentar el nivel de complejidad hasta donde se desee. Se trata de un software más enfocado a usuarios que dispongan de experiencia y tengan el conocimiento suficiente para desplegar servicios y aplicar configuraciones que no sean incorrectas.

Debido a estos detalles se ha preferido trabajar con PfSense. En este proyecto, no se aprovechará ni mucho menos el potencial entero de esta herramienta, ya que se dispone de

un tiempo limitado para ejecutar las tareas basadas en el Firewall y se trata de un entorno sencillo que, al no disponer de mucho tráfico interno no se pueden hacer informes reales de la eficacia de los servicios. Por cambio, se obtiene la certeza que, en caso de desplegar este software en un entorno mayor, se podrían aplicar configuraciones de seguridad más complejas que con IPFire.

Cabe destacar que a día de hoy los entornos cloud han crecido de tal manera que grandes empresas como Amazon, disponen de una cantidad muy grande de servidores de virtualización, donde a cambio de divisas se pueden utilizar sus recursos para desplegar máquinas virtuales y cloud privadas.

Puede resultar una alternativa muy útil, ya que alquilar este servicio significa no invertir en una infraestructura de virtualización propia, sino que solo es necesario encargarse de la configuración y el mantenimiento.

Sería necesario realizar un presupuesto del valor anual que supondría virtualizar de manera local el entorno de producción o virtualizarlo a través de servicios que ofrecen grandes empresas.

5 Implementación de cambios a Producción

Tal y como se lleva comentando a lo largo del proyecto, el entorno creado es utilizado para realizar pruebas antes de llevar un cambio a producción. En esta sección, se explicará brevemente el diagrama de flujo que se obtiene desde que se decide realizar un cambio hasta que se implanta en el entorno de producción. Para poder explicar este proceso, se ejemplificará con el despliegue de un servidor Domain Controller para obtener una redundancia con el principal.

En primer lugar, el encargado del entorno de producción haría una petición al entorno de preproducción para analizar la viabilidad de su propuesta. Una vez aceptada, el personal encargado del entorno de preproducción se debería encargar de realizar un análisis de impacto de este nuevo servidor (Aumento de uso y memoria del servidor de virtualización) y en caso de ser viable, empezar con el desarrollo y configuración. Se virtualizaría un Windows server y se configuraría para que el servidor DC principal replicase toda la información contra el nuevo servidor. Una vez obtenida esta redundancia, se haría una prueba de desastre, donde la prueba debe consistir en apagar el servidor principal para comprobar que el servidor secundario sigue ofreciendo servicio a la red y que los usuarios y servicios no tienen pérdida de servicio. Todo este proceso es necesario documentarlo para poder realizar la misma configuración en el entorno de producción y tenerlo para posibles copias en un futuro.

Una vez terminado y aprobado el trabajo en el entorno de preproducción, en este caso, se podría exportar la máquina virtual creada con el Windows Server y desplegarlo en los hosts de virtualización de producción.

Al asegurar el correcto funcionamiento, habría terminado todo el proceso de aplicar un cambio en el entorno de producción.

6 Metodología y herramientas

6.1. Metodología

En esta sección se explicará la metodología seguida para realizar el proyecto.

Cada objetivo explicado anteriormente, se ha desarrollado siguiendo las siguientes etapas.

En primer lugar, una fase de análisis, donde se estudia la ubicación del nuevo servicio o servidor, el funcionamiento, las posibles consecuencias o cambios que puede provocar y, por último, las especificaciones técnicas (IP, reglas nuevas en firewall, etc.).

Seguidamente, una fase de desarrollo donde se implementa el nuevo objetivo para que tenga una funcionalidad total.

Por último, una fase de pruebas donde se verifica el correcto funcionamiento, para dar por concluido el objetivo.

6.2. Herramientas

A continuación, se detallan todas las herramientas utilizadas para este proyecto.

- VMWare Workstation: software de virtualización, encargado de desplegar todo el entorno utilizado.
- Nagios: software Open Source encargado de la monitorización del sistema.
- PfSense: firewall Open Source encargado de la seguridad y administración de tráfico interno y externo.
- Active Directory: Servicio propio de Microsoft Windows, encargado de la gestión de usuarios y dominios.
- OpenVPN: software Open Source encargado de poder establecer conexiones VPN hacia la infraestructura interna [7].
- SquidProxy: servicio integrado en PfSense que permite reducir el número de peticiones web gracias a un sistema de caché [8].
- Pages: software propio de MacOS utilizado para realizar toda la documentación [9].

7 Planificación

En esta sección se comenta la distribución de tareas para realizar este proyecto.

Se han creado 8 fases correspondientes a los distintos objetivos:

- Fase 0: Desarrollo del escenario principal. Consiste en el despliegue de las máquinas principales, la creación de las distintas subredes y el firewall con las pertenecientes reglas base.
- Fase 1: Implementación de Nagios. Se instala en un servidor Ubuntu dedicado y se configura para que empiece a monitorizar las principales infraestructuras críticas. Se añadirán más hosts a medida que avance el proyecto.

- Fase 2: Sistema de Backup. Se crea un script lanzado por el mismo servidor donde se encuentra Nagios. Realiza una copia de seguridad del fichero de configuración del firewall para poder restaurar en caso de desastre.
- Fase 3: Implementación Active Directory. Se despliega un Windows Server con el servicio de Active Directory. Se crea un dominio local para poder configurar grupos de usuarios.
- Fase 4: Implementación VPN. Se instala y configura este servicio integrado en PfSense para poder realizar conexiones desde Internet.
- Fase 5: Implementación de certificados. Se utiliza Let's Encrypt para obtener certificados válidos para el servidor web.
- Fase 6: Pruebas de seguridad. Se realizan pruebas básicas de seguridad para asegurar el correcto desempeño de la infraestructura.
- Fase 7: Tareas opcionales.

8 Desarrollo del proyecto

En esta sección, se explicarán más a fondo las diferentes partes del proyecto y las problemáticas, si las ha habido, a la hora de poder cumplir el objetivo.

8.1. Escenario principal

En esta primera fase del proyecto, se diseña y desarrolla el esquema de infraestructura que definirá el proyecto y se despliega el Firewall. Para ello, se crean 3 subredes principales: una red Productiva, una red de Monitorización y una red DMZ.

A continuación, se muestra el diagrama de red creado:

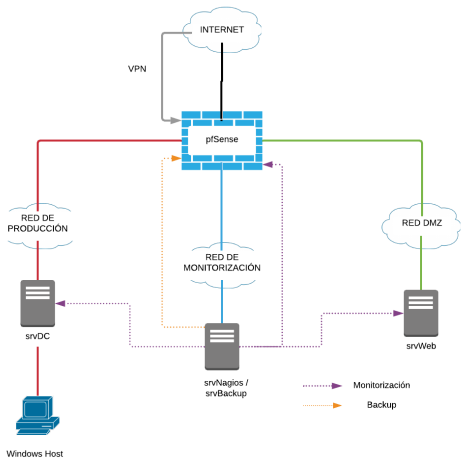

Fig. 2: Diagrama de red infraestructura

La red Productiva contiene los hosts que utilizan usuarios finales y un servidor Domain Controller que administra el dominio. En la red de Monitorización se encuentran todos los hosts encargados de ofrecer algún servicio de monitorización o backup. En un entorno real, es recomendable tener servidores dedicados a cada una de las tareas. En este caso, por falta de recursos, un servidor Linux engloba los servicios de Nagios y Backup. Por último, se encuentra la red DMZ (Demilitarized Zone). La principal característica de esta red es que no puede acceder a la red interna de la infraestructura. Esta configuración se realiza por razones de seguridad, para evitar que los hosts que tienen publicado un servicio a Internet (DNS, Servidor Web...) en caso de infección, los atacantes encuentren bloqueos para acceder a otras redes.

En el Firewall, se han creado un conjunto de reglas básicas para obtener una cierta seguridad. Para la red WAN (conexiones que provienen de Internet) se ha establecido que las conexiones al servidor web alojado a la DMZ solo pueda realizarse por el protocolo HTTPS. También una regla que se crea automáticamente con la creación del túnel VPN. Todo el demás tráfico está bloqueado.

Para la red productiva, se ha establecido que posea conexiones hacia la red DMZ, ya que como se ha comentado anteriormente, se encuentran los DNS, servidores Web, etc. También se ha configurado acceso a Internet y a la subred de Monitorización.

Para la red DMZ, se ha establecido que no disponga de ninguna conexión con la infraestructura interna. Si por algún motivo fuera conveniente una conexión, como por ejemplo una conexión desde el servidor web a un servidor que aloja un base de datos, sería necesario crear una regla muy específica.

Por último, en la red de Monitorización se ha permitido el acceso a la DMZ, al Firewall, a la red Productiva y a Internet. Esto es debido a que en esta subred se encuentra Nagios y el sistema de backup, por lo que necesitan acceder a los hosts de las distintas redes.

8.2. Active Directory

Se ha desplegado un servidor Windows 2012 R2 en la subred de Producción que ofrece el servicio de Active Directory a la red interna. En este caso, se ha creado un dominio, TFG.local. En un entorno real, se podría considerar si crear un solo árbol de dominio o un bosque, dependiendo de las características y necesidades de la empresa. Una vez puesto en marcha el servidor, se ha configurado para que actúe como DHCP y DNS de la red productiva. Se ha configurado para que herede el DNS del firewall, es decir, actualiza su tabla de DNS a partir de los valores de la tabla del DNS del Firewall. Para el servicio DHCP, se ha creado un rango de IP iniciado en 10.10.1.16 hasta 10.10.1.100. El grupo de IP's iniciado en 10.10.1.1 hasta 10.10.1.15 se ha reservado para hosts que proporcionan servicios como el Firewall, Servidor DC o nuevos servicios que se podrían implementar en un futuro.

Se han creado grupos de usuarios de prueba para comprobar el correcto funcionamiento. Existe el usuario Administrador que posee todos los privilegios para acceder a cualquier host dentro del dominio y realizar cualquier acción. Se trata de un usuario al que únicamente debe tener acceso el administrador de sistemas principal. Por otro lado, se pueden crear tantos grupos de usuarios como se desee, fragmentando así los accesos según el departamento al que correspondan, para poder facilitar la administración de privilegios. Por ejemplo, los usuarios de cualquier grupo que no

sean de IT no deben tener acceso al servidor Domain Controller.

Una vez desplegado el servidor, creado el dominio y los grupos de usuarios correspondientes, solo falta añadir al dominio todos los hosts que se consideren oportunos. En este caso, se dispone de un host Windows 10, al que, una vez añadido al dominio, se puede entrar con las credenciales de los usuarios permitidos.

8.3. Nagios

En este caso, se ha desplegado un nuevo servidor Ubuntu en la subred de monitorización. Se ha desplegado el software Nagios siguiendo la documentación que proporciona el fabricante. Para este proyecto se ha decidido monitorizar el servidor Domain Controller, ya que sin el funcionamiento correcto de este los usuarios no podrían "loggearse" en su computadora, el Firewall, ya que en caso de caída no existiría comunicación entre las subredes ni salida a Internet y el servidor Web, ya que en caso de caída o saturación es importante saberlo a tiempo real para poner solución de inmediato.

Para poder añadir los hosts a la monitorización de Nagios, existe una estructura de ficheros de configuración, dónde en uno de ellos, "hosts.cfg.[en] este caso, se añaden los nuevos hosts con nombre, IP y grupo que pertenecen.

Para los hosts Windows, para poder realizar una monitorización más a fondo, es necesario instalar un agente en la computadora llamada NSSClient++. Este agente permite obtener datos que serían imposibles de recolectar externamente, como uso de CPU, porcentaje de ocupación del disco, etc. Para los hosts Linux, el equivalente es el NRPE (Nagios Remote Plugin Executor).

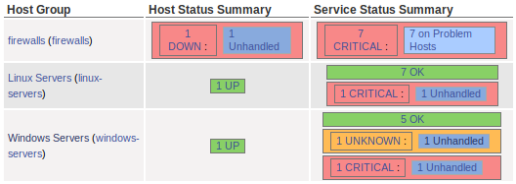

Fig. 3: Interfaz de Nagios.

8.4. Gestión de certificados

Para esta fase, como se ha comentado se ha decidido utilizar Let's Encrypt [10]. Se trata de una entidad certificadora que permite crear conexiones seguras (HTTPS) con el servicio web publicado a Internet. En este proyecto, debido a la escasez de tiempo para poder realizar todas las tareas, se optó por utilizar una máquina virtual vulnerable, OWASP [11], que ofrece una interfaz básica a través del puerto 80 (HTTP).

No ha sido posible crear un certificado para esta máquina virtual debido a que el uso de la terminal se encuentra muy restringido y son varios los comandos que se necesitan ejecutar para realizar una solicitud de certificado. En un entorno real, se dispondría de un servidor Apache que ofrece un servicio web que sería más fácil de administrar. En este caso, no ha sido posible ejecutar esta solución por dos motivos, el primero la falta de recursos de cómputo para desplegar un nuevo servidor de Apache y el segundo, porqué conllevaría crear un mínimo de código para mostrar una interfaz web.

8.5. Sistema de backup

En algunos softwares de virtualización más avanzados, como VMWare ESX [12], se configura un servidor físico con amplios recursos y dentro de él corren las máquinas virtuales. Existen software privados y Open Source que se conectan al servidor y ejecutan copias de las máquinas virtuales para luego almacenarlas donde se indique. En este caso, al no disponer de este tipo de software, se ha descartado realizar un sistema automático de backup general. En cambio, se ha podido realizar una automatización de backup del fichero de configuración del firewall. Este fichero es crítico debido a que contiene toda la información del Firewall, como reglas, interfaces, IP's, VPN, etc. En caso de no disponer de este fichero, en caso de corrupción del Firewall sería necesario implementar toda la configuración a mano otra vez.

Para poder realizar el backup, se ha implementado un Script proporcionado por el fabricante [13] que abre una sesión remota contra el Firewall y hace una copia del fichero de configuración. Este Script es lanzado desde el mismo servidor que se encuentra Nagios a través de Crontab, una herramienta propia de Linux que permite establecer la asiduidad con la que lanzar el script que se indique.

En el Script se ha integrado la creación de carpetas con fecha para poder identificar correctamente las copias de seguridad. Se ha configurado para que se ejecute cada viernes a las 18:00h.

```
#!/bin/bash

cd /home/monitor/Desktop/Backup
mkdir "$(date +"%d-%m-%Y")"
cd "$(date +"%d-%m-%Y")"

curl -L -k --cookie-jar cookies.txt \
     https://10.40.1.2/ \
     | grep "name='__csrf_magic'" \
     | sed 's/.*value="\(.*\)".*/\1/' > csrf.txt

curl -L -k --cookie cookies.txt --cookie-jar cookies.txt \
     --data-urlencode "login=Login" \
     --data-urlencode "usernamefld=admin" \
     --data-urlencode "passwordfld=pfsense" \
     --data-urlencode "__csrf_magic=$(cat csrf.txt)" \
     https://10.40.1.2/ > /dev/null

curl -L -k --cookie cookies.txt --cookie-jar cookies.txt \
     https://10.40.1.2/diag_backup.php  \
     | grep "name='__csrf_magic'"   \
     | sed 's/.*value="\(.*\)".*/\1/' > csrf.txt

curl -L -k --cookie cookies.txt --cookie-jar cookies.txt \
     --data-urlencode "download=download" \
     --data-urlencode "donotbackuprrd=yes" \
     --data-urlencode "__csrf_magic=$(head -n 1 csrf.txt)" \
     https://10.40.1.2/diag_backup.php > config-router-`date +%Y%m%d%H%M%S`.xml
```

Fig. 4: Script que ejecuta el backup del firewall.

8.6. Squid Proxy

Corresponde a tareas opcionales. Se trata de una herramienta que viene integrada con PfSense. La finalidad de este servicio es reducir el consumo de ancho de banda a través de un caching de las páginas web más visitadas. En una infraestructura con un número considerable de usuarios, es importante disponer de servicios que reduzcan el consumo de ancho de banda para así evitar una saturación de red. A través de un mecanismo que guarda las peticiones web más concurrentes, permite ofrecer esa página web sin que el Firewall tenga que realizar una consulta.

8.7. VPN

Se trata de un servicio que viene integrado con PfSense. A través del firewall, instalando el paquete correspondiente, permite la creación de un túnel VPN donde se pueden configurar todos los parámetros, como subred interna a la que se obtendrá conexión, usuarios que pueden conectarse a través de la VPN, etc. Una vez especificados todos los campos, esta funcionalidad permite descargar un ejecutable OpenVPN que puede trasladarse al host que se le desea dar acceso remoto a la infraestructura.

8.8. High Availability

Corresponde a tareas opcionales. En cualquier infraestructura, es necesario tener redundado cualquier servicio para que, en caso de fallada, la pérdida de servicio sea mínima. Para este proyecto, inicialmente se planteó el hecho de crear un clúster de Firewalls en modo Activo-Pasivo, es decir, los dos nodos del firewall constantemente se comunican para compartir el fichero de configuración, pero solo uno trabaja, el Máster, el otro nodo se encuentra en reposo". Cuando el nodo Slave detecta una pérdida de comunicación con el Máster, entiende que este ha caído y automáticamente toma el relevo. Al existir una IP virtual, a través del protocolo CARP, al que se conectan los hosts de la infraestructura, automáticamente el nodo Slave es el receptor de todo el tráfico. Una vez detecta que el nodo Máster se encuentra operativo otra vez, le delega la responsabilidad y vuelve al estado de reposo".

Las buenas prácticas del fabricante indican que es necesario crear una red dedicada para la comunicación entre los nodos del Firewall. Esto es debido a aspectos de seguridad y rendimieimgnto, ya que no es conveniente que el tráfico generado por los firewalls para compartir información sobre la configuración circule por otras redes en las que existan usuarios.

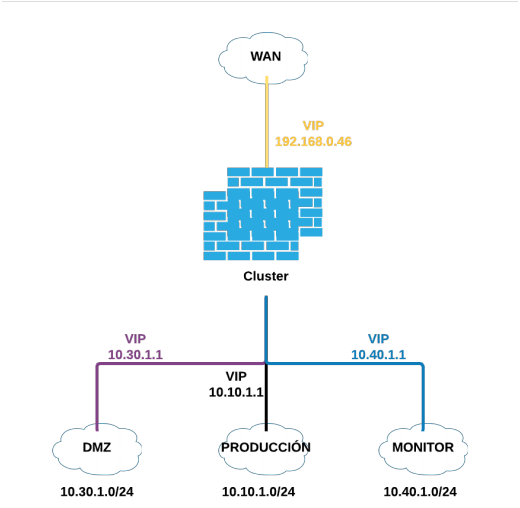

Fig. 5: Diagrama lógico del funcionamiento de un clúster.

9 Conclusiones

A continuación, una vez finalizado el desarrollo del proyecto, se extraen conclusiones a partir de los resultados obtenidos.

Como se ha podido observar a lo largo del proyecto, ya sea en los informes de progreso o en este artículo final, cada herramienta o servicio que se ha instalado ha tenido alguna que otra dificultad a la hora de implantarlo.

En cuanto a virtualización, Virtual Box es un software Open Source muy conocido, pero vistos los resultados del proyecto, no es una herramienta que permita crear un entorno completo. Una de las mayores deficiencias que tiene es la limitación para crear subredes. Esta limitación impide crear las subredes que se consideren oportunas. En un entorno real, probablemente existirán más de 10 subredes dedicadas (Servidores, administración, TI, backup...). A parte, a lo largo del proyecto se han observado comportamientos irregulares en las máquinas virtuales y fallos en las conexiones de red. Por ello, se decidió cambiar de software de virtualización y utilizar VMWare Workstation.

En aspectos de firewall y de seguridad, PfSense ha cumplido con la mayor parte de expectativas. Se trata de un software intuitivo, muy bien documentado por parte del fabricante, que permite instalar nuevas funcionalidades (Como la Alta Disponibilidad, Squid Proxy...) y sólido en cuanto a la aplicación de nuevas configuraciones. Por contra, no tiene aún desarrolladas herramientas de seguridad como las que actualmente se encuentran en otros Firewalls de pago, como por ejemplo el servicio DNS Watch del fabricante Watchguard, que se trata de un servicio cloud que inspecciona las consultas DNS para comprobar que no se intenta acceder a una página marcada como maliciosa. Otro contra, seguramente el más importante, es que, en los Firewall de pago, viene incluido un servicio de soporte que proporciona respaldo y información respecto la herramienta. El software de PfSense es gratuito, pero es necesario contratar el soporte para obtener este respaldo. El balance de PfSense es positivo y podría ser útil para recrear un entorno de Preproducción. Es una herramienta muy completa, que dispone de una gran cantidad de servicios que permiten crear configuraciones complejas.

En este proyecto en particular, los servicios adicionales usados (VPN, alta disponibilidad y Squid Proxy) han resultado un éxito. Se trata de servicios muy útiles en cualquier infraestructura que PfSense ofrece y permite configurarlos de manera rápida.

Se ha conseguido instaurar completamente el Active Directory tal y como se planeó inicialmente. Un servidor Domain Controller que proporciona un dominio a la red donde se encuentra y permite que las computadoras Windows que se encuentran en ella puedan entrar en dominio. A la vez, este servidor disminuye el uso de recursos del Firewall ya que actúa como DNS y DCHP. Si bien es cierto que en un escenario real este servidor debe ser redundado, ya que en caso de fallada los usuarios no podrían autenticarse en ninguna computadora.

Por último, en cuanto a la monitorización y backup, como se ha observado anteriormente, también ha cumplido con las expectativas iniciales. Nagios, se ha mostrado como una herramienta muy sólida y eficaz. Realizando test de desastre, muestra una media de 10 segundos desde que cae un host hasta que Nagios notifica la caída. Un tiempo corto como para poder intervenir rápidamente. Por contra, el despliegue y configuración de Nagios resulta muy tedioso. La configuración, al principio, no resulta nada intuitiva, ya que

cuesta encontrar los ficheros base del software y encontrar que ficheros está utilizando para obtener los hosts y grupos a analizar. Una vez se descubre la jerarquía de los ficheros, resulta más fácil de configurar ya que existen plantillas para cada tipo de dispositivo a monitorizar.

En el aspecto de backup, el script utilizado desarrollado por el fabricante resulta muy útil. Se ha comprobado con éxito varias veces la restauración del firewall a través de los ficheros de configuración de backup y ha sido un éxito.

En general, cabe destacar la importáncia de tener un entorno de estas características en cualquier empresa que ofrece un servicio, ya sea a Internet o a la propia empresa o empresas dedicadas a la creación de software. Se trata de empresas que en algún momento, necesitan realizar cambios, ya sean actualizaciones de SO, nuevas funcionalidades de la App, etc. Sin un entorno que les permita realizar estas pruebas y verificar su funcionamiento, siempre existirá el miedo al implementar directamente cambios en el entorno de producción que un servicio no arranque y pueda afectar al correcto desempeño de la infraestructura.

10 Trabajo futuro

En este proyecto, se ha trabajado en la creación de un escenario base de un entorno de preproducción. Se ha construido un entorno simplificado, con las funcionalidades más básicas sobre las que poder seguir construyendo un escenario cada vez más complejo. La limitación principal para poder desarrollar un escenario complejo, ha sido la limitación de recursos por parte de la computadora usada para virtualizar las máquinas. En un entorno donde la base de virtualización fuera más potente, permitiría crear un entorno más complejo, con más redundáncias y nuevos servicios. Por ejemplo:

- En un entorno de producción, un servidor Domain Controller es un servicio crítico. Si falla, los usuarios no pueden entrar en sus computadoras. Para ello, sería conveniente tener redundado este servicio desplegando otro servidor DC.

- Se podría desplegar un servidor que contenga las bases de datos que lee el servicio web. Una vez desplegado, crear las reglas de Firewall correspondientes para que el servidor Web solo pueda hacer conexiones internas a las bases de datos. Las demás conexiones, como se ha comentado anteriormente, restringidas.

- Se podría desplegar servidores LDAP y RADIUS para controlar las autenticaciones dentro de la infraestructura. Aumentaría el nivel de seguridad dentro de la empresa.

- Se podría desplegar un servidor que actúe como DNS y situarlo en la DMZ, ya que se trata de un servicio publicado a Internet.

- Como se ha visto, en este proyecto, todo el tráfico interno entre las distintas subredes circula a través del Firewall. En un entorno más complejo, se podría llegar a saturar. Por ello, sería conveniente utilizar Switches virtuales que realicen las comunicaciones internas, así se reduciría la carga del Firewall.

- Al disponer de una infraestructura con más servicios, se podrían proponer mejoras respecto a la monitorización a través de Nagios, con nuevos hosts, más servicios a monitorizar. También nuevas medidas de seguridad por parte del Firewall.

  Como se puede observar, un entorno de preproducción puede crecer de hosts y servicios hasta dónde los recursos permitan. Los anteriores ítems son ejemplos de nuevas funcionalidades que se podrían implantar en este proyecto. Los entornos de preproducción deben ser una réplica del entorno de producción, esto implica que cada infraestructura será un caso distinto. En este proyecto se ha trabajado en la base que contiene cualquier infraestructura.

Agradecimientos

Gracias a los consejos proporcionados por mi tutor Ángel Elbaz para poder desarrollar un trabajo bien estructurado y consistente. También a mis compañeros de trabajo por nutrirme de conocimientos sobre tecnologías.

Referencias

[1] Con miles de empresas que utilizan el software PfSense, se está convirtiendo rápidamente en la solución de seguridad de red de código abierto más confiable del mundo. https://www.pfsense.org/, 28/02/2019.

[2] Active Directory almacena información sobre objetos en la red y facilita esta información para que los administradores y usuarios la puedan encontrar y usar. Active Directory utiliza un almacén de datos estructurado como base para una organización lógica y jerárquica de información de directorio. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview, 30/02/2019.

[3] Nagios XI proporciona monitorización de todos los componentes críticos de infraestructura, incluyendo aplicaciones, servicios, sistemas operativos, protocolos de red, métricas de sistemas e infraestructura de red. https://www.nagios.org/, 03/03/2019.

[4] La virtualización es el proceso de crear una representación virtual o virtual de algo, como aplicaciones virtuales, servidores, almacenamiento y redes. Es la forma más efectiva de reducir los gastos de TI mientras aumenta la eficiencia y la agilidad para empresas de todos los tamaños. https://www.vmware.com/solutions/virtualization.html, 06/03/2019.

[5] VirtualBox es un potente producto de virtualización x86 y AMD64 / Intel64 para empresas y para uso doméstico. VirtualBox no solo es un producto extremadamente rico en funciones y alto rendimiento para clientes empresariales. También es la única solución profesional de código abierto. https://www.virtualbox.org/, 06/03/2019

[6] Una solución de seguridad de código abierto con un kernel personalizado basado en el sistema operativo FreeBSD. pfSense es uno de los cortafuegos de red líderes con un nivel comercial de funciones. https://geekflare.com/best-open-source-firewall/, 28/02/2019.

[7] OpenVPN ofrece soluciones de VPN flexibles para proteger sus comunicaciones de datos, ya sea para la privacidad de Internet, el acceso remoto para los empleados, la seguridad de IoT o para la red de centros de datos en la nube. https://openvpn.net/, 10/03/2019.

[8] Configuring the Squid Package as a Transparent HTTP Proxy. https://docs.netgate.com/pfsense/en/latest/cache-proxy/setup-squid-as-a-transparent-proxy.html, 05/04/2019.

[9] Pages es un procesador de texto superversátil con todo lo necesario para crear documentos que se leen sin pestañear. https://www.apple.com/es/pages/, 15/02/2019.

[10] Let's Encrypt is a free, automated, and open Certificate Authority. https://letsencrypt.org, 20/03/2019.

[11] El proyecto de seguridad de aplicaciones web abiertas (OWASP) es una organización benéfica sin fines de lucro en todo el mundo centrada en mejorar la seguridad del software. https://www.owasp.org/index.php/, 20/02/2019.

[12] VMware vSphere ESXi, establece el estándar de la industria en cuanto a confiabilidad, rendimiento y soporte. https://www.vmware.com/products/vsphere-hypervisor.html/, 15/06/2019.

[13] Realizar una copia de seguridad remota de una configuración pfSense. https://docs.netgate.com/pfsense/en/latest/backup/remote-config-backup.html, 07/05/2019.

APÈNDICE

A.1. Terminos utilizados

Ransomware: El ransomware es un código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado. El ransomware se propaga a través de archivos adjuntos de correo electrónico, programas infectados y sitios web comprometidos. Un programa de malware ransomware también puede ser llamado criptovirus, criptotroyano o criptogusano. Fuente: https://www.ccn-cert.cni.es

DMZ: Abreviatura de "demilitarized zone" (zona desmilitarizada). Subred física o lógica que proporciona una capa de seguridad adicional a la red privada interna de una organización. La DMZ agrega una capa de seguridad de red adicional entre Internet y la red interna de una organización, de modo que las partes externas sólo tengan conexiones directas a los dispositivos de la DMZ y no a toda la red interna. Fuente: https://www.ccn-cert.cni.es

DHCP: Abreviatura de "Protocolo de Configuración Dinámica de Host". Se trata de un protocolo de red estandarizado que se utiliza en las redes de Protocolo de Internet (IP) para distribuir dinámicamente los parámetros de configuración de la red, como direcciones IP. Cuando una computadora entra en una red, solicita la dirección IP y los parámetros de red de forma automática a un servidor DCHP. Fuente: https://myhourdoc.zendesk.com/hc/en-us/articles/210288513-DCHP-with-networks

CARP: Abreviatura de "Protocolo de Redundancia de Direcciones Comunes". Es un protocolo automático de conmutación por error y redundancia introducido por OpenBSD en octubre de 2003. CARP está diseñado para compartir una dirección IP común entre varios hosts en el mismo segmento de red para proporcionar redundancia de conmutación por error a múltiples servidores o hosts. Es una alternativa al Protocolo de redundancia de enrutador virtual (VRRP) del Grupo de trabajo de ingeniería de Internet (IETF) y al Protocolo de redundancia de reserva en caliente (HSRP) de Cisco. Fuente: https://www.techopedia.com/definition/25696/common-address-redundancy-protocol-carp