Despliegue de FWaaS en un cloud privado

Javier Sánchez Capellán
Grado de Ingeniería Informática

Manuel Jesus Mendoza Flores

11/2018

Licencias alternativas (elegir alguna de las siguientes y sustituir la de la página anterior)

A) Creative Commons:

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento 3.0 España de Creative Commons

B) GNU Free Documentation License (GNU FDL)

Copyright © AÑO TU-NOMBRE.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	Despliegue de FWaaS en un cloud privado
Nombre del autor:	**Javier Sánchez Capellán**
Nombre del consultor:	**Manuel Jesus Mendoza Flores**
Fecha de entrega (mm/aaaa):	11/2018
Área del Trabajo Final:	**Administración de redes y sistemas operativos**
Titulación:	*Grado de Ingeniería Informática*

Resumen del Trabajo (máximo 250 palabras):

En este proyecto nos centraremos en la evolución de los cortafuegos al nuevo paradigma de las tecnologías de la información; "la nube", que tal y como la define Microsoft es "la entrega de servicios informáticos (servidores, almacenamiento, bases de datos, redes, software, análisis, inteligencia, etc.) a través de Internet, y cuyo objetivo es ofrecer una innovación más rápida, recursos flexibles y economías de escala. Lo habitual es pagar solo por los servicios en la nube utilizados, de tal forma que se ayude a reducir los costos operativos, a ejecutar la infraestructura con más eficacia y a escalar a medida que cambian las necesidades de su negocio"[1].

Esta evolución se conoce por sus iniciales en ingles "FWaaS" (Firewall as a Service); es decir, cortafuegos como servicio. "FWaaS" ofrece un servicio de seguridad lógico que está disponible en cualquier lugar, se adapta perfectamente a cualquier carga de tráfico, aplica una política unificada y se mantiene a sí mismo ubicándose en "la nube". En lugar de existir como un dispositivo, el cortafuegos existe como una barrera virtual.

El alcance del presente proyecto se centra en el aprovechamiento de la implantación de una "nube privada" utilizando Openstack, para el despliegue de "FWaaS" para dar cobertura a la seguridad de diferentes sedes remotas.

Abstract (in English, 250 words or less):

In this project we will focus on the evolution of firewalls to the new paradigm of information technologies; "The cloud", as defined by Microsoft is "the delivery of computer services (servers, storage, databases, networks, software, analysis, intelligence, etc.) through the Internet, and whose objective is to offer a faster innovation, flexible resources and economies of scale. The usual thing is to pay only for the services in the cloud used, in such a way that it helps reduce operating costs, to run the infrastructure more effectively and to scale as the needs of your business change "[1].

This evolution is known by its initials in English "FWaaS" (Firewall as a Service); that is, firewalls as a service. "FWaaS" offers a logical security service that is available anywhere, adapts perfectly to any traffic load, applies a unified policy and keeps itself located in "the cloud". Instead of existing as a device, the firewall exists as a virtual barrier.

The scope of this project focuses on the use of the implementation of a "private cloud" using Openstack, for the deployment of "FWaaS" to cover the security of different remote sites.

Palabras clave (entre 4 y 8):

Cloud
Openstack
Security
FWaaS

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

Las recientes tendencias en redes empresariales han creado un desafío para los ingenieros de seguridad de redes. Las soluciones de movilidad y la informatización de las organizaciones implican un aumento de las posibles amenazas a los activos de las mismas.

Dentro de este proyecto, se realizará un análisis de las diferentes soluciones de seguridad disponibles para implantar en una organización con una gran cantidad de sedes, con diferentes tipologias y una elevada dispersión geográfica. Este análisis nos permitirá ampliar nuestros conocimientos sobre la tecnología existente para la puesta en marcha de una “nube” privada y los servicios “FwaaS”.

La puesta en marcha de servicios “FwaaS” sobre una “nube” privada no es un proyecto que se pueda desplegar en cualquier ámbito.

En primer lugar, porque es necesario contar con una infraestructura propia centralizada, que sea suficiente para albergar todos los recursos necesarios.

En segundo lugar, porque la solución de “nube” privada solo es necesaria en el caso de que por motivos legales o de imagen corporativa no se quieran utilizar servicios en la “nube” pública. Ya que estos últimos implican una menor inversión inicial y además aseguran un coste estable una vez que el servicio se ha implantado.

En tercer lugar, la organización que adopte esta solución debe contar con una red lo suficientemente grande y con sedes muy dispersas que justifiquen la evolución del servicio de cortafuegos.

Por último, de cara a reducir los plazos de implantación y puesta en marcha de los servicios “FwaaS” sobre una “nube” privada, existen soluciones comerciales con menor complejidad. La utilización de una solución abierta que debe ser construida desde cero, estaría fundamentada en motivos específicos de contratación o limitación presupuestaria.

En el caso de este TFG la Organización objetivo del mismo es un organismo público y por tanto la misma esta sujeta a las leyes de contratación del Estado; ello implica la necesidad de asegurar el acceso en igualdad de condiciones a todos los proveedores en caso de realizar cualquier tipo de licitación relacionada con este proyecto. Y además obliga al cumplimiento expreso de la legislación existente en cuanto a materia de seguridad.

La implementación de servicios “FWaaS” permite que cada recurso organizativo (CPDs, sedes centrales, sedes remotas) se conecten a un

servicio global y aprovechen todas sus capacidades de seguridad. Adicionalmente permite reducir los gastos operativos y de capital relacionados con el mantenimiento software y hardware de los dispositivos físicos repartidos a lo largo de la organización, así como la superficie de ataque resultante de parches retrasados y vulnerabilidades no mitigadas.

A continuación ampliaremos el detalle de las mejoras obtenidas con servicios “FwaaS”:

Ventaja	Descripción
Eliminación del hardware en las sedes remotas	La utilización de “FwaaS” permite que los servicios de cortafuegos estén disponibles en todas las sedes sin la necesidad de instalar hardware en todas las sedes de una Organización. En las organizaciones se suelen encontrar entornos de cortafuegos heterogéneos, ampliando la exposición creciente a piratas informáticos y amenazas de Internet.
Reducción de los costes de mantenimiento	El ciclo de vida del mantenimiento del equipamiento de seguridad, requiere un esfuerzo inmenso y agrega posibles puntos de fallo a la red. Al tener centralizado el servicio estos riesgos desaparecen.
Mejora en la respuesta a las necesidades del negocio	Uno de los mayores problemas con la seguridad basada en dispositivos se centra en que los dispositivos físicos están limitados por la capacidad. Cuando el dispositivo físico debe afrontar una mayor carga debido a un mayor volumen de tráfico, el dispositivo a menudo tiene que actualizarse para cumplir con los requisitos. Debido a las restricciones presupuestarias, las limitaciones de los dispositivos físicos a menudo obligan a elegir entre la seguridad y la evolución de los servicios. Como resultado, la seguridad de las sedes remotas suele ser dejada de lado.
Aplicación uniforme de políticas de seguridad	Con “FWaaS” se puede aplicar uniformemente una política de seguridad en todo el tráfico, para todas las ubicaciones y para todos los usuarios, incluidos los usuarios móviles, remotos y fijos. Si bien los fabricantes crearon consolas de administración centralizadas para facilitar la administración de los despliegues distribuidos de cortafuegos, es necesario considerar las instancias de cortafuegos individuales por ubicación y, a menudo, personalizar las políticas a los atributos únicos de dichas ubicaciones
Automatización de tareas	El mantenimiento y la gestión continua de la configuración de los cortafuegos es un asunto que requiere mucho tiempo y recursos. En contraste, una de las principales ventajas de “FWaaS” es su arquitectura. Es más rápido de implementar y más fácil de mantener, y ofrece una mejor opción de seguridad de red para los equipos de TI sobrecargados. Estas mejoras se deben a su definición mediante software y la posibilidad de automatizar tareas mediante APIs.

1.2 Objetivos del Proyecto

Los principales objetivos de este proyecto son:

- Reducción de costes operativos.
- Mejora en la gestión de la seguridad.
- Mejora en la gestión de la infraestructura.
- Gestión unificada de todos los recursos de computación, aplicaciones y seguridad de las sedes de manera descentralizada. Cada responsable provincial debe poder gestionar sus propios recursos de IT.
- Mejora en la seguridad de un red con múltiples ubicaciones.

Los objetivos parciales para lograrlo son los siguientes:

- Despliegue de la infraestructura necesaria para una “nube” privada.
- Despliegue de un software de automatización.

1.3 Enfoque y método seguido

En primer lugar se ha desarrollado la planificación del proyecto. Dicha planificación se ha realizado en base a estimaciones temporales de las tareas identificadas y ajustándose a la duración definida desde la dirección del TFG.

Para el despliegue de la solución de seguridad en la Organización objetivo de este proyecto, se realizaran estudios de las tipologías y soluciones de seguridad actuales en el mercado. En función de los mismos se elaboraran conclusiones en función del cumplimiento de los requisitos definidos por la Organización.

Para poder comprobar que todas las decisiones han sido las correctas optaremos por desarrollar el presente proyecto con un modelo de prototipos. Desplegaremos un piloto para comprobar el procedimiento de implantación y que el resultado obtenido es el deseado.

Una vez finalizado el despliegue se elaboraran un conjunto de conclusiones relacionadas con la ejecución del proyecto.

De forma incremental se elaborará la memoria de este TFG con 3 entregas parciales para comprobar el progreso alcanzado en el mismo antes de su entrega definitiva.

1.4 Planificación del Trabajo

1.4.1 Desglose de tareas del proyecto

Tarea 1: Análisis y estudio tecnológico.

Descripción de la tarea: En esta primera tarea se realizará un análisis de las soluciones de seguridad existentes, en función del cumplimiento de los objetivos y requisitos del proyecto.

Objetivos de la tarea:
Decidir la solución a implantar.

Tarea 2: Análisis y diseño de los requisitos de infraestructura necesaria para la “nube privada”

Descripción de la tarea: Una vez elegida la distribución de Openstack, incluyendo la estrategia de alta disponibilidad de los diferentes componentes, se realizará un análisis de los recursos hardware mínimos para la puesta en marcha de un piloto y para la puesta en marcha de una infraestructura de producción. Esta infraestructura deberá recoger las herramientas de automatización para el despliegue.

Objetivos de la tarea: Obtener un diagrama con el número de componentes de la infraestructura y los requisitos hardware detallados de cada uno de ellos.

Tarea 3: Análisis y diseño de las automatizaciones necesarias para el despliegue de la “nube privada”

Descripción de la tarea: Debido a la complejidad del despliegue de “la nube” con Openstack será necesario realizar diferentes automatizaciones. Estas automatizaciones las implementaremos con ansible, herramienta open source soportada por la compañía Red Hat. Serán necesarios varios roles y un playbook que faciliten la instalación de la solución.

Objetivos de la tarea: Obtener las especificaciones necesarias para el desarrollo de las automatizaciones.

Tarea 4: Tareas de documentación para configuración de las propiedades del despliegue.

Descripción de la tarea: Una vez identificadas la arquitectura de despliegue se realizarán las configuraciones a utilizar en las automatizaciones de despliegue de cada componente de “la nube”.

Objetivos de la tarea: Obtener los ficheros de propiedades utilizados por las automatizaciones

Tarea 5 Implementación de las automatizaciones.

Descripción de la tarea: En esta paso se desarrollaran o reutilizarán roles existentes para la distribución de Openstack elegida, siempre de acuerdo a las especificaciones obtenidas. Estos roles se integraran en un único playbook de despliegue.

Objetivos de la tarea: Obtener un playbook que despliegue toda la infraestructura desde ansible.

Tarea 6: Análisis y diseño de la arquitectura de comunicaciones necesaria para la conexión de las sedes remotas a la “nube privada”

Descripción de la tarea: Para el despliegue de un “FwaaS” es necesario realizar un diseño de interconexión a nivel de capa 2 para las sedes remotas. Existen varias opciones para este diseño, como puede ser la conexión mediante tecnologías de extensión de VLANs o la realización de tuneles VPN y modificación del routing de las sedes. En esta tarea escogeremos la estrategia para el despliegue de comunicaciones.

Objetivos de la tarea: Obtener un diseño de capa 2 y 3 de la arquitectura de comunicaciones del proyecto.

Tarea 7: Puesta en marcha del piloto de “nube” privada

Descripción de la tarea: Utilizando las automatizaciones obtenidas en tareas previas en esta tarea desplegaremos “la nube”. Obtendremos acceso a la interfaz de administración de la misma y comprobaremos que todos los componentes se encuentran operativos.

Objetivos de la tarea: Obtener acceso a la consola Horizon de Openstack del piloto.

Tarea 8: Despliegue del servicio de “FWaaS” en el piloto

Descripción de la tarea: Una vez que “la nube” esta correctamente desplegada en el piloto, procederemos a configurar un servicio “FwaaS” mediante el componente Neutron de Openstack.

Objetivos de la tarea: Configurar un servicio “FwaaS” en Neutron

Tarea 9: Pruebas del servicio de “FwaaS” en el piloto y corrección de errores

Descripción de la tarea: En este punto procederemos a inyectar tráfico entrante y saliente utilizando el servicio como puerta de enlace y se configuraran varios filtros para comprobar su efectividad. En caso de detecta algún error, se procederá a su corrección.

Objetivos de la tarea: Obtener pruebas de que el servicio funciona correctamente

Tarea 10: Despliegue de la “nube privada”

Descripción de la tarea: Una vez que todo ha sido verificado, utilizaremos de nuevo la automatización para desplegar los componentes de Openstack con la arquitectura definitiva.

Objetivos de la tarea: Obtener acceso a la consola Horizon de Openstack del piloto.

Tarea 11: Despliegue del servicio de “FwaaS”

Descripción de la tarea: Una vez que “la nube” esta correctamente desplegada de forma definitiva, procederemos a configurar un servicio “FwaaS” mediante el componente Neutron de Openstack.

Objetivos de la tarea: Configurar un servicio “FwaaS” en Neutron

Tarea 12: Pruebas del servicio de “FwaaS”

Descripción de la tarea: En este punto procederemos a inyectar tráfico entrante y saliente utilizando el servicio como puerta de enlace y se

configuraran varios filtros para comprobar su efectividad con el despliegue definitivo de los componentes.

Objetivos de la tarea: Obtener pruebas de que el servicio funciona correctamente

1.4.2 Cronograma

	Semana		Actividad	Memoria
1	17/09/18	23/09/18	Investigación y documentación tecnológica	
2	24/09/18	30/09/18	Descomposición inicial de tareas	Índice
3	01/10/18	07/10/18	Entrega PEC1: Plan de Trabajo	
4	08/10/18	14/10/18	Ejecución de las tareas de Diseño	
5	15/10/18	21/10/18	Ejecución de las tareas de Implementación	
6	22/10/18	28/10/18	Instalación del piloto	
7	29/10/18	04/11/18	Corrección de errores	
8	05/11/18	11/11/18	Entrega PEC2: Pruebas piloto	Background+ Propuesta
9	12/11/18	18/11/18	Configuraciones de comunicaciones	
10	19/11/18	25/11/18	Instalación de “la nube”	
11	26/11/18	02/12/18	Despliegue del “FWaaS”	
12	03/12/18	09/12/18	Pruebas del servicio	
13	10/12/18	16/12/18	Entrega PEC3: Resultados	Resultados
14	17/12/18	23/12/18	Elaboración de la documentación	
15	24/12/18	30/12/18	Elaboración del vídeo de presentación	
16	31/12/18	06/01/19	Entrega TFC y Presentación	

1.4.3 Diagrama de Gantt

WBS	Nombre	Trabajo	Fin
1	Tarea 1: Análisis y estudio tecnológico.	15d	oct 5
2	Entrega PEC1	N/D	oct 5
3	Tarea 2: Análisis y diseño de los requisitos de infraestructura necesaria para la “nube privada”	5d	oct 12
4	Tarea 3: Análisis y diseño de las automatizaciones necesarias para el despliegue de la “nube privada”	5d	oct 12
5	Tarea 4: Tareas de documentación para configuración de las propiedades del despliegue	5d	oct 19
6	Tarea 5: Implementación de las automatizaciones.	5d	oct 26
7	Tarea 6: Análisis y diseño de la arquitectura de comunicaciones necesaria para la conexión de las sedes remotas a la “nube privada”	10d	oct 26
8	Tarea 7: Puesta en marcha del piloto de “nube privada”	5d	nov 2
9	Tarea 8: Despliegue del servicio de “FwaaS” en el piloto	2d	nov 6
10	Tarea 9: Pruebas del servicio de “FwaaS” en el piloto y corrección de errores	4d	nov 12
11	Entrega PEC2	N/D	nov 12
12	Tarea 10: Despliegue de la “nube privada”	10d	nov 26
13	Tarea 11: Despliegue del servicio de “FwaaS”	5d	dic 3
14	Tarea 12: Pruebas del servicio de “FwaaS”	5d	dic 10
15	Entrega PEC3	N/D	dic 10
16	Elaboracion de la documentacion y video de presentacion	20d	dic 31
17	Entrega final	N/D	dic 31

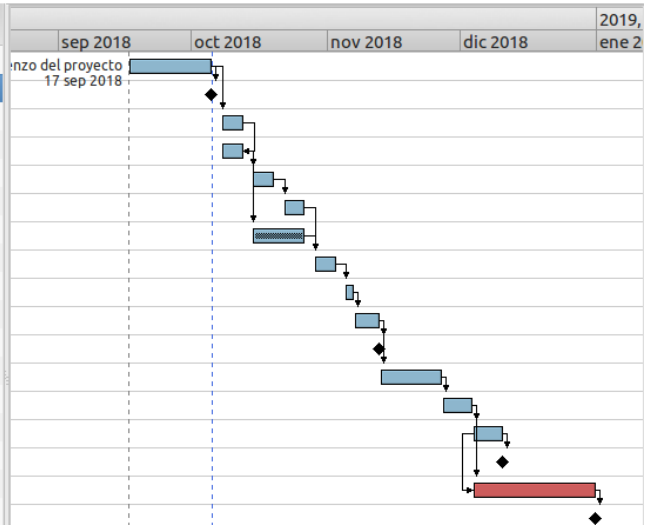

Ilustración 1: Cronograma

1.4.4 Gestión de riesgos

De cara al cumplimiento de los objetivos de este proyecto es necesario definir un plan de riesgos donde se identifiquen los mismos y se les proponga un plan de contingencia:

Riesgo	Causa	Efecto	Tipo	Probabilidad	Estrategia	Plan de contingencia
Resistencia al cambio.	Falta de cultura del cambio. Reacción negativa a la automatización.	Proceso de cambio ineficiente	Estratégico	ALTA	Mitigación	Elaboración de un plan de comunicación durante el proyecto de transición que ayude a la Organización a aceptar el cambio.
Perdida de información.	Errores técnicos en la gestión del proyecto	Imposibilidad de acceso a la información.	Operativo	BAJA	Mitigación	Establecer una política de copias de seguridad de la documentación del proyecto
Piloto incompleto	Desconocimiento de la plataforma tecnológica	Imposibilidad de ejecución de las pruebas	Tecnológico	MEDIA	Mitigación	Estudio de la documentación publica de la solución escogida

1.5 Breve sumario de productos obtenidos

Los productos obtenidos en el presente proyecto son:

- Scripts de ansible para el despliegue de openstack
- Documentación de configuración del servicio “FwaaS”.

1.6 Breve descripción de los otros capítulos de la memoria

En el capitulo de premisas del diseño de la solución, presentaremos cual es la situación a la que debemos dar solución con el presente proyecto y cuales son en detalle los requisitos a cumplir una vez finalizado el mismo. El éxito del proyecto podremos definirlo en función del cumplimiento de dichos requisitos.

En los siguientes capítulos se realizaran estudios sobre las diferentes soluciones de seguridad que son aplicables al ámbito del proyecto. Finalmente se presentara el diseño e implementación de una “nube” privada, el despliegue de un servicio “FwaaS” y se mostrará cual es la distribución de Openstack escogida para nuestro proyecto y el porque de dicha decisión. Además se realizará una descripción de los elementos que la componen, como serán desplegados y que resultados obtendremos.

En el capitulo de administración de los datos, se detallara cual será el tratamiento de los datos en este proyecto.

En el capitulo de valoración productiva y presupuestaria, analizaremos cuales son los resultados obtenidos en el proyecto y cuales son los costes de su implementación.

2. Premisas del diseño de la solución

2.1 Situación actual

El presente proyecto toma como punto de partida un despliegue geográfico disperso con diferentes tipos de sedes y un CPD central de alta capacidad.

Actualmente solo las sedes grandes cuentan con cortafuegos dedicados, dichos cortafuegos son de tipo hardware y con firewalls software desplegados en los equipos de los usuarios. Las sedes medias y pequeñas solo cuentan con estos últimos.

La conexión entre las sedes se realiza mediante fibra y una red MPLS contratada con un proveedor de telecomunicaciones.

Las sedes del Organismo objeto del presente proyecto se pueden clasificar en 3 tipos:

Tipología	Número de usuarios	Servicios	Velocidad del Acceso
Pequeñas	1-5	• Directorio Activo • WSUS • Navegación	20 MB
Medias	5-15	• Directorio Activo • WSUS • Impresión • Navegación	10 MB
Grandes	15-50	• Directorio Activo • WSUS • Impresión • Escaneo de documentación • Navegación	100 MB

El número de sedes del Organismo según su tipologia es el siguiente:

Tipología	Número de sedes
Pequeñas	250
Medias	50
Grandes	15

2.2 Requerimientos solicitados

Los requerimientos para el presente proyecto son tanto técnicos como económicos y legales.

En el ámbito de los requerimientos técnicos:

- Necesidad de contar con una solución de tipo empresarial y que incluya soporte por parte de fabricante. A
- Diseño de la solución en el que se prime la disponibilidad, la continuidad y a la sencillez durante el despliegue.

En el ámbito de los requerimientos económicos:

- Necesidad de diseñar una solución que implique un baja inversión inicial con respecto a la compra de licencias
- Reutilización de hardware ya existente para reducir la necesidad de nuevas compras.

En el ámbito de los requerimientos legales:

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos que estableció el Esquema Nacional de Seguridad y que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos. En 2015 se publicó la modificación del Esquema Nacional de Seguridad a través del Real Decreto 951/2015, de 23 de octubre, en respuesta a la evolución del entorno regulatorio, en especial de la Unión Europea, de las tecnologías de la información y de la experiencia de la implantación del Esquema.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

3. Estudio de soluciones

3.1 Introducción

En este apartado estudiaremos las diferentes soluciones tecnológicas existentes para implementar las medidas necesarias para proteger las sedes identificadas en este proyecto, cumpliendo los requisitos marcados y de cara a la consecución de los objetivos definidos.

3.2 Firewalls software

Es el tipo más común de firewall, ya que no sólo es el más económico, sino por su simplicidad de instalación. Sin embargo presenta inconvenientes que son inherentes a su condición; por ejemplo, consume recursos del equipo de usuario, en ocasiones no se ejecuta correctamente y pueden ocasionar errores de compatibilidad con otros tipos de software que se encuentren instalados en el equipo.

Actualmente, la mayoria de software antivirus o de vpn incluye también el servicio de firewall software en los equipos de usuario. Esto nos permite gestionar de forma centralizada las reglas aplicadas en los mismos.

3.3 Firewalls hardware

El firewall hardware es utilizado más en empresas y grandes organizaciones. Normalmente son dispositivos que se colocan entre los servicios desplegados y la conexión externa de los mismos. Adicionalmente se puede contar con varios niveles para mejorar la seguridad. Al ser dispositivos dedicados, se encuentran optimizados para realizar la función de firewall, y además no consumen los recursos de los equipos de usuario.
Su mayor inconveniente es el mantenimiento, ya que son difíciles de actualizar y de configurar correctamente.

3.4 Firewalls lógicos

Los firewalls lógicos son un método para dividir un firewall hardware en dos o más unidades lógicas para que estas funcionen como múltiples unidades independientes. Los firewalls lógicos pueden proporcionar políticas de firewall por separado y configuraciones completamente separadas para enrutamiento y servicios VPN para cada red u organización conectada. La gran ventaja de los firewalls lógicos es el ahorro de coste al solo tener que mantener y licenciar los firewalls hardware donde se hayan configurado.

3.5 Firewalls virtuales

Un firewall virtual es un servicio o dispositivo de red que se ejecuta completamente dentro de un entorno virtualizado. Los firewalls virtuales

pueden ser desplegados como maquinas virtuales normales en la mayoría de hipervisores del mercado así como en cloud privadas y cloud publicas.

3.6 Firewalls en cloud públicas

Los firewalls ofrecidos como servicios en la nube publica eliminan los obstáculos operacionales planteados por los enfoques tradicionales de infraestructura de seguridad distribuida y ofrece las capacidades preventivas de las plataformas de seguridad de fabricantes de primer nivel, los cuales brindan a los clientes las protecciones necesarias necesarias para evitar ataques cibernéticos en entornos de red y nube distribuidos globalmente.

Los clientes pueden agregar o eliminar ubicaciones y usuarios remotos rápida y fácilmente, y establecer y ajustar las políticas de seguridad según sea necesario. Este nuevo servicio de seguridad, flexible, siempre disponible y actualizado puede ayudar a los clientes a escalar fácilmente para satisfacer las demandas de crecimiento y lograr una seguridad constante en los entornos informáticos de sus organizaciones, sin importar dónde residan los dispositivos o los usuarios, a un coste predecible.

3.7 Firewalls en cloud privadas

Los firewalls ofrecidos como servicios en la nube privada tambien eliminan los obstáculos operacionales planteados por los enfoques tradicionales de infraestructura de seguridad distribuida. Adicionalmente permiten una gestión de políticas de seguridad incluidas en la gestión del resto de infraestructura desplegada en el cloud privado.

3.8 Conclusiones

En primer lugar debemos decir que parte de las soluciones presentadas en este punto no son incompatibles y de hecho tal y como se indica en el apartado anterior, los firewall software ya se encuentran desplegados en los equipos de los usuarios de la Organización. Sin embargo aunque se cuenta con una consola centralizada de gestión, en la misma no se pueden gestionar servicios de infraestructuras o aplicaciones ajenas a las mismas, por tanto no cumple uno de los objetivos marcados para el proyecto.

En el caso de los firewalls hardware debemos descartarlos como solución para este proyecto debido a que un despliegue de los mismos en todas las sedes supondría un coste que la Organización no puede asumir puesto que esta buscando una reducción en sus costes operativos.

En el caso de los firewalls lógicos y virtuales debemos descartarlos como solución para este proyecto puesto que aunque cumplen la

reducción de costes operativos y la mejora de la seguridad al poder generar un firewall lógico por sede no permiten una gestión unificada de los recursos de IT.

Aunque los firewalls en la nube publica parecen cumplir los requisitos del proyectos en cuanto a disponibilidad, continuidad y a los objetivos de reducción de coste y mejora de la seguridad siguen impidiendo una gestión unificada de los recursos de IT de forma descentralizada. Además seria necesario confirmar que el proveedor del servicio de cloud publica cumple los requisitos legales en cuanto al Esquema Nacional de seguridad.

Por tanto la única solución de firewalls de las estudiadas que cumple a priori con todos los requisitos y puede alcanzar todos los objetivos marcados para este proyecto es el despliegue de cortafuegos integrados en una nube privada.

En este momento deberemos comenzar con el análisis de las soluciones existentes para el despliegue de una nube privada en la Organización.

4. Estudio de soluciones de cloud privada propietarias

4.1 Introducción

Para el despliegue de una nube privada donde desplegar servicios “FwaaS” existen diferentes aproximaciones en función de los requisitos y recursos de la Organización donde se vaya a desplegar. Es por ello que se ha decidido realizar en primer lugar un estudio de la oferta existente y una valoración de las soluciones propietarias. Se ha decidido comenzar con este tipo de soluciones porque a priori son las que tienen mas posibilidades de cumplir los requisitos y objetivos del proyecto.

4.2 vCloud Suite de VMware

VMware Inc., es una filial de Dell que proporciona software de virtualización, cloud y servicios de cloud pública e hibirda.

La solución de Vmware para cloud privado es vCloud Suite. Esta suite es la que más tiempo lleva en el mercado y por tanto se encuentra más probada.

A continuación se presenta un esquema básico de la solución:

Ilustración 2: Esquema vCloud Suite de VMware

Como ventaja a resaltar cuenta con poder desplegarse sobre cualquier hardware, como desventaja fundamental cuenta con un coste de licenciamiento muy alto. El mismo se presenta en tres ediciones diferentes, con diferentes funcionalidades cada una:

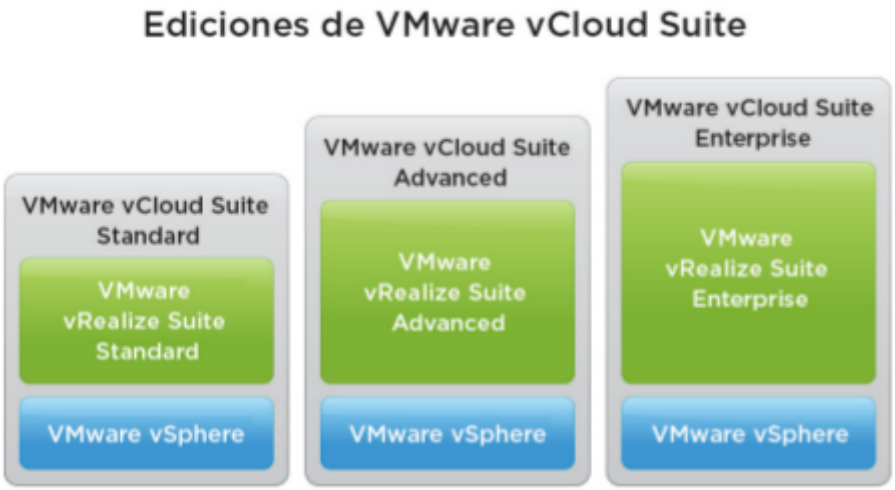

Ilustración 3: Ediciones de VMware vCloud Suite

4.3 FusionCloud de Huawei

Huawei Technologies Co., Ltd. es una empresa privada multinacional china de alta tecnología especializada en investigación y desarrollo, producción electrónica y marketing de equipamiento de comunicaciones. Además, provee soluciones de redes personalizadas para operadores de la industria de telecomunicaciones.

El producto para cloud privada de Huawei es FusionCloud y se basa en Openstack. Esta suite es reciente en el mercado pero cuenta con grandes despliegues como es el caso del de Deutsche Telekom. Como ventaja a resaltar no cuenta con coste de licenciamiento, como desventaja principal su despliegue debe ser realizado en hardware propietario de Huawei.

A continuación se presenta un esquema de la solución de Huawei:

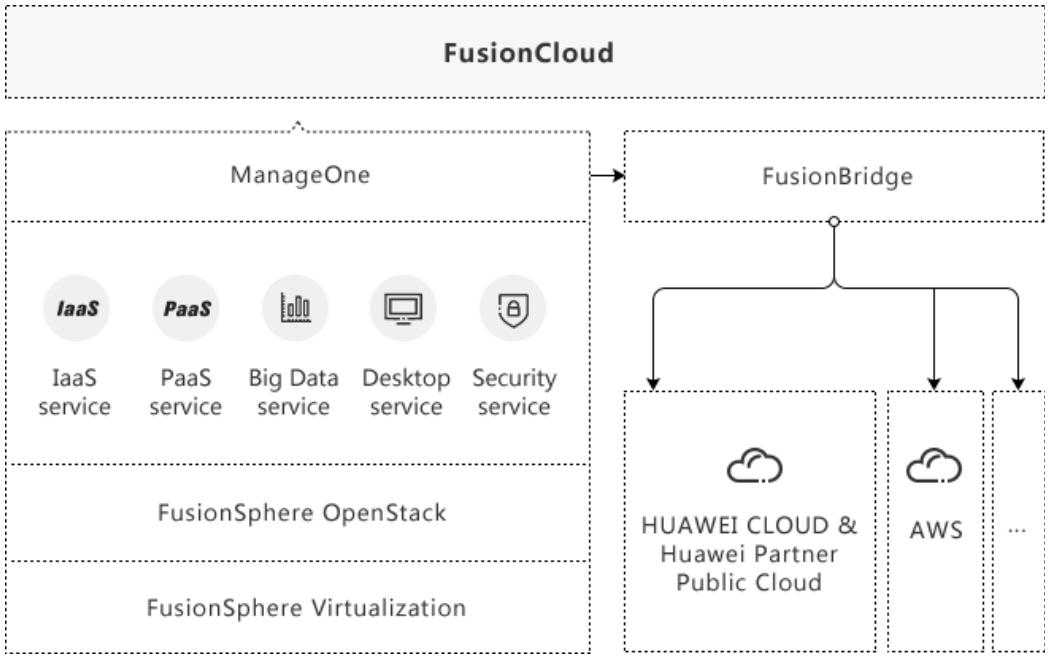

Ilustración 4: Esquema de FusionCloud de Huawei

4.4 Nutanix Enterprise Cloud de Nutanix

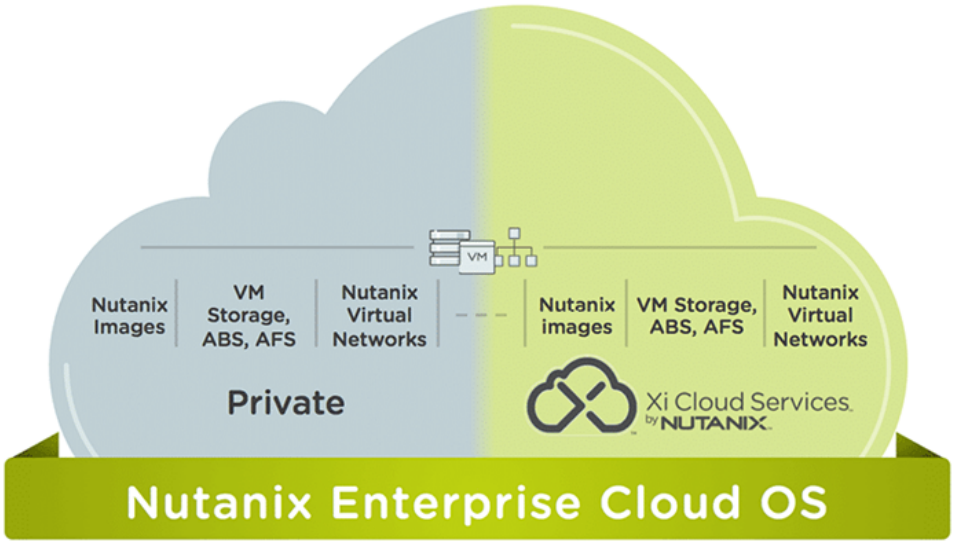

Ilustración 5: Esquema del Nutanix Enterprise Cloud OS

Nutanix es una compañía de software de computación en la nube que vende lo que llama dispositivos de infraestructura hiperconvergente y almacenamiento definido por software. Nutanix fue fundada en 2009 por Dheeraj Pandey, Mohit Aron y Ajeet Singh

La solución para nube privada de Nutanix es Nutanix Enterprise Cloud. Esta suite también es reciente en el mercado pero si cuenta con la ventaja competitiva de ser la mejor solución con respecto a la tecnología de hiperconvergencia, permitiendo el ahorro de costes en el almacenamiento necesario en el despliegue de la “nube”. Como ventaja

a resaltar cuenta con un coste bajo de licenciamiento, como desventaja principal su despliegue debe ser realizado sobre un chasis de la propia marca aunque los nodos que componen el cloud si pueden ser multivendor.

4.5 Conclusiones

Debido a los inconvenientes indicados anteriormente y que con las soluciones propietarias no cumpliríamos los requisitos legales, referentes a la contratación marcados para el proyecto, debemos seguir con la siguiente opción para la implementación de la nube privada.

5. Estudio de soluciones de cloud privada open source

5.1 Introducción

Una vez descartadas las soluciones propietarias para la implantación de una cloud privada, nos centraremos en las soluciones open source. Para decidir cuales se estudiaran se ha decidido utilizar el informe de Forrester “The I&O Pro’s Guide To Enterprise Open Source Cloud Adoption, Q1 2018”

5.2 OpenNebula

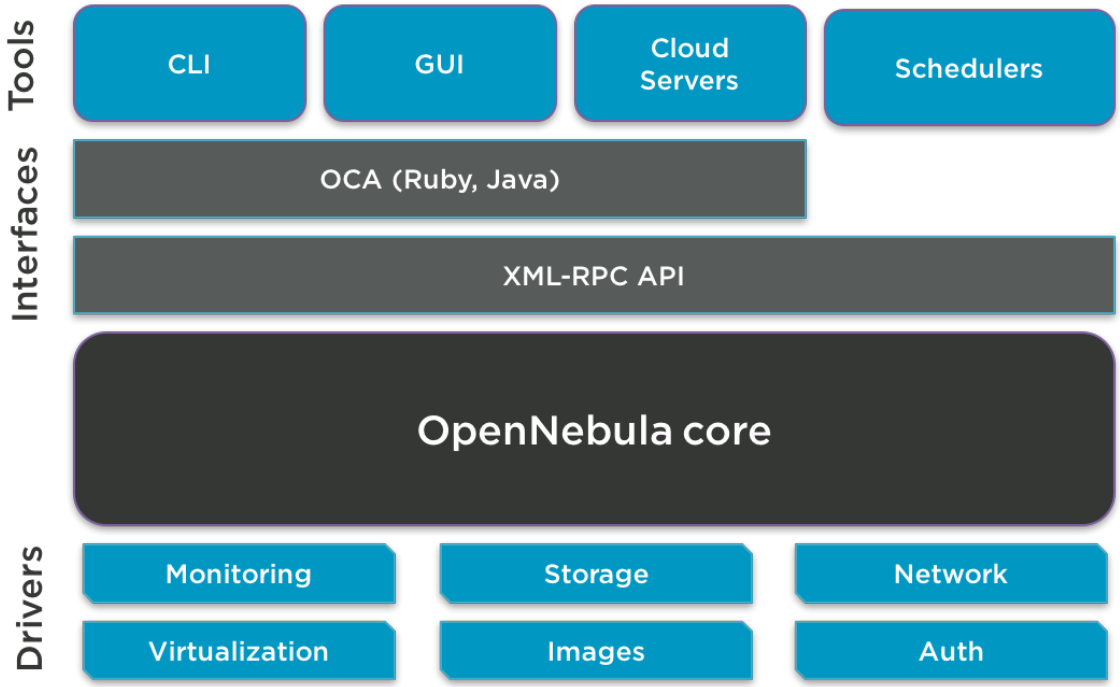

Ilustración 6: Esquema de componentes de OpenNebula

Esta suite es simple pero con bastante aceptación, sin embargo solo esta soportado por OpenNebula Systems. Como ventaja a resaltar no cuenta con coste de licenciamiento y es muy simple de desplegar, como desventaja principal su soporte es más limitado que el de Openstack.

5.3 Openstack

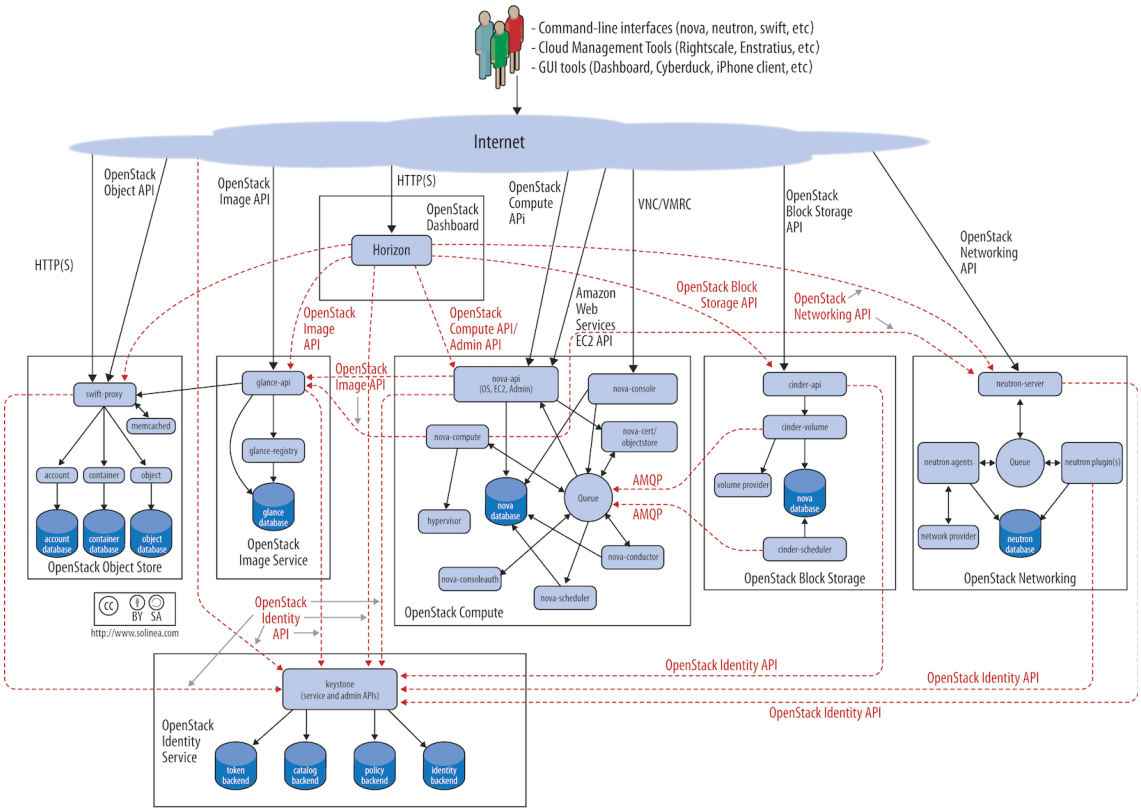

Ilustración 7: Esquema de componentes de Openstack

Es una plataforma que permite utilizar diferentes tipos de hipervisores, dispositivos y servicios de red y almacenamiento, utilizando una única API que crea un tejido de centro de datos unificado. Su API cuenta con integraciones con la mayoría de fabricantes y además grandes compañías le prestan soporte. Es utilizada por compañías como Red Hat para las implementaciones de sus “nubes” públicas. Como ventaja a resaltar cuenta con poder ser desplegada sobre cualquier hardware y sin coste de licenciamiento, como desventaja fundamental su instalación es muy compleja.

5.4 Conclusiones

La estrategia escogida ha sido la de optar por realizar un despliegue con Openstack, que permite:

- Gestionar de manera unificada todos los recursos desplegados en el cloud
- La reutilización del hardware ya existente en la Organización, al no estar atada a un fabricante y por tanto un ahorro de costes en el despliegue. Además se cumplirán los requisitos legales.
- La integración mediante su API con el resto de elementos existentes en cualquier CPD tradicional, como cabinas o gestores DNS, permitiendo de nuevo un ahorro de costes.
- Compra de soporte una vez el servicio este en producción. Reduciendo de nuevo los costes.

De esta forma cumpliremos los objetivos definidos para el proyecto.

Una vez escogida la suite procederemos a la elección de la distribución especifica de Openstack ha utilizar, en función de sus características técnicas y económicas.

6. Estudio de soluciones Openstack

6.1 Introducción

El proyecto OpenStack se define a sí mismo como una plataforma de Cloud Computing hecha con software libe para desplegar nubes públicas y privadas, desarrollado con la idea de ser sencillo de implementar, escalable y con muchas prestaciones.

El proyecto OpenStack se inició en 2010 por la empresa Rackspace Cloud y por la agencia norteamericana, NASA. Actualmente más de 150 empresas se han unido al proyecto, entre las que se encuentran empresas tan importantes como AMD, Intel, Canonical, Red Hat, IBM, Dell, HP, Cisco, etc. OpenStack ha optado por utilizar la licencia de Apache 2.0, una licencia de software libre permisiva y no copyleft. En el caso de OpenStack se ha decidido además por un desarrollo completamente abierto, en que se pueden aceptar opiniones y contribuciones de cualquiera, debiendo hacer uso del lenguaje de programación Python en lo que a la generación del código se refiere.

Una vez clara la opción de Openstack, se presenta la necesidad de seleccionar una distribución que cumpla los requerimientos solicitados. Para cumplir el requerimiento técnico relativo al soporte proporcionado por fabricante y de nivel empresarial solo se analizarán 3 distribuciones que cuenta con una compañía de primer nivel detrás:

- Red Hat Openstack
- Oracle Openstack
- Suse Openstack

6.2 Red Hat Openstack de Red Hat

Red Hat, Inc. es una multinacional estadounidense de software que provee software de código abierto principalmente a empresas. Fundada en 1993, Red Hat tiene su sede corporativa en Raleigh, North Carolina, con oficinas satélite en todo el mundo. La distribución de Openstack de Red Hat y que distribuye como Red Hat Openstack 12 se encuentra basada en la release de Openstack Queens (5.0).

A continuación se presenta un esquema de los componentes de la misma:

Ilustración 8: Esquema de componentes de Red Hat Openstack

6.3 Suse Openstack

Fundada en 1992, SUSE es el primer proveedor mundial de una distribución Enterprise Linux. Su distribución se encuentra basada en la release de Openstack Pike (4.0).

A continuación se presenta un esquema de los componentes de la misma:

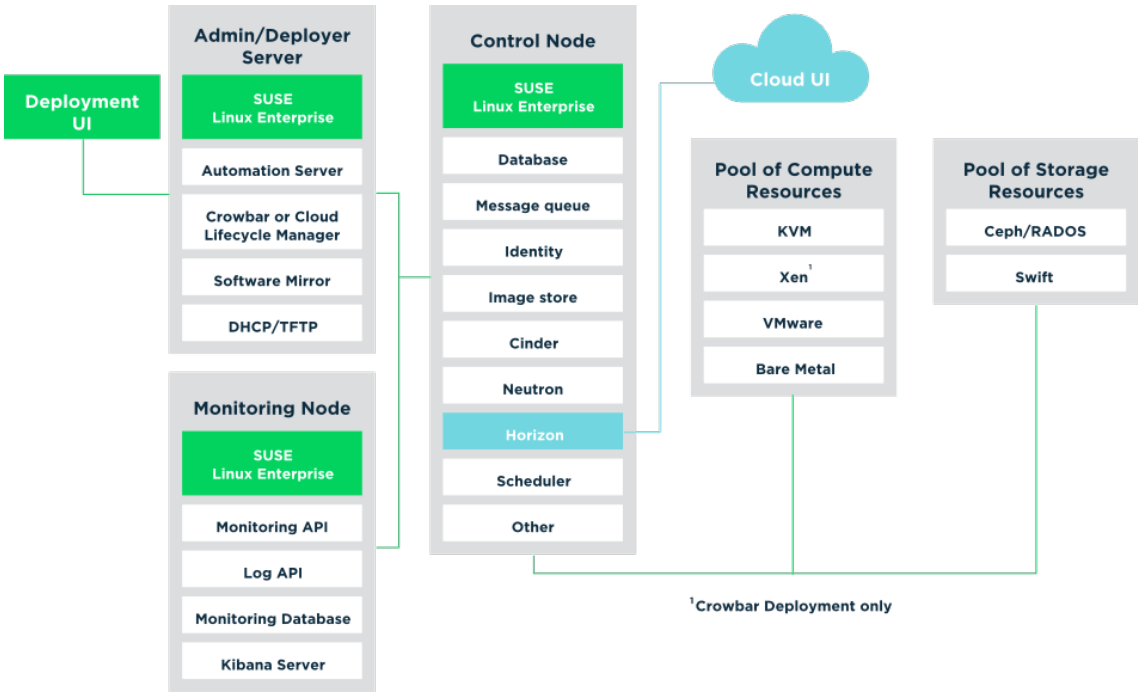

Ilustración 9: Esquema de componentes de Suse Openstack

6.4 Oracle Openstack

Oracle Corporation es una compañía especializada en el desarrollo de soluciones de nube y locales. Oracle tiene su sede en la localidad californiana de Redwood City, Estados Unidos. Su distribución se encuentra basada en la release de Queens (5.0).

6.5 Conclusiones

En primer lugar se ha descartado la distribución de Suse. Este descarte se basa en que la versión de esta compañía es una versión inferior al del resto de las analizadas. El riesgo que supondría desplegar una versión con bugs o con menores capacidades de integración impide que se siga con su análisis.

Puesto que las otras dos distribuciones utilizan la última versión disponible en este momento procederemos a seguir con el estudio.

En el caso de la distribución de Red Hat nos encontramos con un problema en el coste de licenciamiento. Para poder acceder a los repositorios necesarios para el despliegue del software de esta distribución, se deben haber comprado las licencias correspondientes, por lo cual el despliegue del piloto ya implicaría un coste. Esto último redunda en el incumplimiento del requerimiento de aplicar el menor coste posible. Además la solución para la instalación de los diferentes componentes de Openstack en esta distribución añade una restricción en cuanto a la posibilidad de escalado, al estar basado en el proyecto open source Triple-O. Esto también incumpliría parcialmente los requerimientos de disponibilidad.

Por último la distribución de Oracle satisface todos los requerimientos solicitados. En primer lugar el acceso a todos los repositorios de la distribución son libres. Solo es necesario pagar el soporte para aquellos nodos que se quiera y además el modo de instalación se basa en el despliegue de contenedores Docker. La opción de despliegue mediante contenedores permite que las actualizaciones de versiones o las marcha atrás sean muchos mas fáciles que en distribuciones gestionadas con paquetería.

6. Despliegue de un servicio FwaaS sobre Openstack

6.1 Introducción

En el presente apartado se presenta la arquitectura de la solución de Oracle Openstack.

6.3 Arquitectura de la solución

OpenStack está diseñado como un conjunto de servicios distribuidos. Estos servicios se comunican entre sí y son responsables de las diversas funciones necesarias para poder prestar los servicios de la "nube". A continuación se presentarán los servicios claves de nuestro despliegue de OpenStack:

- **Keystone:** Es el servicio responsable de la gestión de identidades, de la autenticación y la autorización de usuarios y servicios. Keystone es capaz de integrarse con servicios de directorio de terceros, como LDAP. Keystone también proporciona el catálogo de servicios de OpenStack y los endpoints asociados.

- **Nova**: Es el servicio responsable de crear instancias de máquinas virtuales y administrar su ciclo de vida, así como de administrar el hipervisor que se elija para el despliegue. Los hipervisores se conectan a Nova, independientemente del que se haya escogido, la API de Nova nunca cambia.

- **Ironic**: Es el servicio responsable del aprovisionamiento de máquinas físicas, es el servicio homologo a Nova en el plano físico. Ironic se apoya en los protocolos PXE e IPMI para aprovisionar y administrar hardware, y admite plugins de proveedores de hardware.

- **Neutron**: Es el servicio responsable de la gestión de la red en Openstack, se encarga de crear conectividad y servicios. Es capaz de conectarse con el hardware de red existente a través de plugins. Neutron viene con un conjunto de servicios predeterminados e implementados por herramientas comunes. Este es el componente responsable de la creación y gestión de los servicios "FwaaS".

- **Designate**: Es el el servicio responsable de proveer DNS, es decir de desplegar DNS-as-a-Service (DNSaas). Proporciona una API-REST con autenticación del componente Keystone integrada. Designate puede configurarse para generar automáticamente registros basados en acciones de Nova y Neutron.

- **Cinder**: Es el servicio responsable del almacenamiento en bloque, se encarga de crear y administrar el almacenamiento externo. Es capaz de conectarse al hardware de almacenamiento de un proveedor a través de plugins. En el caso de que no se cuente con un almacenamiento hardware soportado por Cinder, esta versión de Oracle Openstack soporta el uso de un cluster Ceph como backend del mismo.

- **Swift**: Es el servicio responsable del almacenamiento y administración de objetos grandes y binarios (BLOB).

- **Barbican**: Es el servicio responsable de la administración de claves para las que proporciona almacenamiento seguro, aprovisionamiento y administración de datos secretos. Esto incluye claves simétricas, claves asimétricas, certificados y datos binarios sin procesar.

- **Glance**: Es el servicio responsable de la administración de las imágenes cargadas por los usuarios. Glance no es un servicio de almacenamiento, sino que es el responsable de guardar los atributos de la imagen, haciendo un catálogo virtual de las imágenes.

- **Heat**: Es el servicio responsable de la orquestación, administrando el ciclo de vida de la infraestructura de OpenStack (como servidores, direcciones IP flotantes, volúmenes, grupos de seguridad, etc.) y aplicaciones.

- **Horizon**: Es el servicio responsable de crear una GUI para que los usuarios controlen OpenStack. Este es un marco extensible al cual los proveedores pueden agregar características. Horizon usa las mismas API que están expuestas a los usuarios.

- **Murano**: Es el servicio responsable del catálogo de aplicaciones, en él es posible publicar aplicaciones listas para la “nube” desde un catálogo. Un agente se instala en el sistema operativo de una instancia, lo que permite el despliegue de las aplicaciones directamente en él. Murano también incluye un complemento para Horizon.

- **Ceilometer**: Es el servicio responsable de la telemetría. Recopila, normaliza y transforma los datos producidos por los diferentes servicios de OpenStack. Con este servicio es posible realizar la facturación a los clientes o la gestión de la capacidad de los recursos.

- **Alarma de telemetría (aodh)**: Es el servicio responsable de gestionar las alarmas y notificaciones basadas en las métricas recopiladas por Ceilometer.

Como hemos visto en el servicio Cinder, en el caso de no contar con un almacenamiento hardware que se encuentre en la matriz de compatibilidad de Oracle Openstack deberemos desplegar un componente adicional en la infraestructura. Este es el caso del presente proyecto, puesto que en los requerimientos económicos del mismo se indica que se debe reducir al máximo la inversión en hardware. Por tanto será necesario desplegar un cluster Ceph que sirva de proveedor de almacenamiento para Openstack con el soporte existente en la infraestructura de almacenamiento por iSCSI.

Ceph es un sistema de ficheros distribuido open source. Su diseño se pensó fundamentalmente para el uso con gran cantidad de datos y muy enfocado para el uso con Big Data. Ceph tiene como objetivo ser POSIX-compatible y es por ello que es completamente distribuido y no cuenta con ningún punto de fallo. Esto es fundamental para cumplir con los requerimientos técnicos de continuidad y disponibilidad del proyecto. Ceph permite que los datos tengan una replicación libre de errores convirtiéndolo así en un sistema de ficheros tolerante a fallos.

Dentro de las ventajas que incluye Ceph se encuentra un orquestador para la instalación y la configuración del servicio. En el ámbito de nuestro proyecto otra ventaja adicional es que los clientes Linux utilizaran directamente un módulo de kernel para montarlo y que el almacenamiento iSCSI para desplegarlo puede ser de cualquier fabricante o solución que provea dicho tipo de conexión.

Como ultimo componente es necesario el despliegue del software de automatización de Red Hat, ansible.

Además de los componentes anteriores que representan la parte software de la solución, es necesario contar con puertos suficientes en el hardware de red y contar con un cortafuegos dedicado a las tareas de encaminamiento y de seguridad perimetral, adicionalmente en este cortafuegos se configuraran los interfaces de administración del hardware donde se desplegara Openstack.

6.4 Diseño de red

Para el despliegue de un servicio “FwaaS” optaremos por adoptar diferentes estrategias para la conexión entre las diferentes sedes remotas a la “nube”, habitualmente esta interconexión se identifica con las siglas DCI (Data Center Interconnect), en función de su tipologia.

Para las sedes pequeñas optaremos por utilizar los servicios de VPN incluidos en Oracle Openstack. Esto nos permitirá reducir la complejidad en nuestra red que no estaría justificado para tan pocos usuarios y tan poco trafico.

Para las sedes medias optaremos por el encaminamiento del trafico desde las sedes remotas al CPD central. Aunque se aumentará la

latencia en el trafico al tener que entrar y salir por el cortafuegos de la sede central y que puesto que deberemos utilizar policy routing para poder detectar cuando entra o sale el trafico desde los firewalls cloud, también aumentara la complejidad de la gestión del encaminamiento en el CPD central. Sin embargo esta solución supondrá una carga menor sobre los equipos de comunicaciones de las sedes y el CPD central y el trafico existente no justifica utilizar la misma estrategia que en las sedes grandes.

Para las sedes grandes optaremos por una estrategia diferente, esta tendrá como objeto reducir el trafico entrante sobre nuestro firewall perimetral basándonos en la extensión de VLANs entre sedes. La implementación consistirá en el uso del protocolo 802.1q nativo entre las diferentes sedes. Nos hemos asegurado que los equipamientos proporcionados por el proveedor de comunicaciones de las sedes remotas soportar este tecnología y que además contamos con dicho servicio en el catalogo de servicios del mismo.

6.5 Elementos desplegados

Una vez identificados los servicios de Openstack para nuestro despliegue y el diseño de red, pasaremos a mostrar como desplegaremos dichos servicios. En primer lugar deberemos saber que en nuestra distribución de Openstack existen diferentes tipos de nodos, que no son más que servidores físicos instalados con el sistema operativo Oracle Linux y con un conjunto determinado de servicios agrupados por su funcionalidad. A continuación detallaremos dichos tipos:

- **Controller Node**: Estos nodos son aquellos donde se instalan la mayoría de los servicios de OpenStack. Un nodo controlador puede ejecutar todos los servicios que no son de cómputo o solo algunos de ellos.

- **Compute Node**: Estos nodos son aquellos donde se ejecutan los servicios para administrar instancias de máquinas virtuales.

- **Database Node**: Estos nodos son aquellos donde corren las bases de datos y los servicios necesarios para la administración de las mismas.

- **Networking Node**: Estos nodos ejecutan los servicios de red, como proporcionar una dirección IP a una maquina virtual, o gestionar reglas de cortafuegos.

- **Storage Node**: Esto nodos ejecutan los servicios necesarios para administrar el almacenamiento de imágenes e instancias. Algunos servicios de almacenamiento no son administrados directamente por los servicios de OpenStack, sino que son administrados por el dispositivo de almacenamiento. Por ejemplo

en un nodo, Cinder se comunica con la API del dispositivo de almacenamiento o en nuestro caso el cluster Ceph, y es este el que realiza la administración del almacenamiento.

Un nodo maestro ejecuta la CLI de Oracle OpenStack (kollacli), que se utiliza para implementar los servicios de OpenStack en los nodos. Un nodo maestro no es un nodo de OpenStack. Normalmente, un Controller Node se usa como un nodo maestro, pero un nodo maestro puede ser un nodo separado. Adicionalmente en nuestro proyecto utilizaremos el Controller Node como Database Node, esto lo hacemos para reducir el uso de hardware.

Tal y como indicamos anteriormente el despliegue de Oracle Openstack se realiza mediante contenedores Docker. Los servicios de los nodos están creados como un contendor y almacenados en un Registry. Un Registry no es más que un sistema de almacenamiento y entrega de contenido, que contiene imágenes de Docker. Se puede optar por un Registry local o directamente el de Oracle, en nuestro caso utilizaremos el de Oracle.

A continuación se muestra un esquema del despliegue realizado para este proyecto:

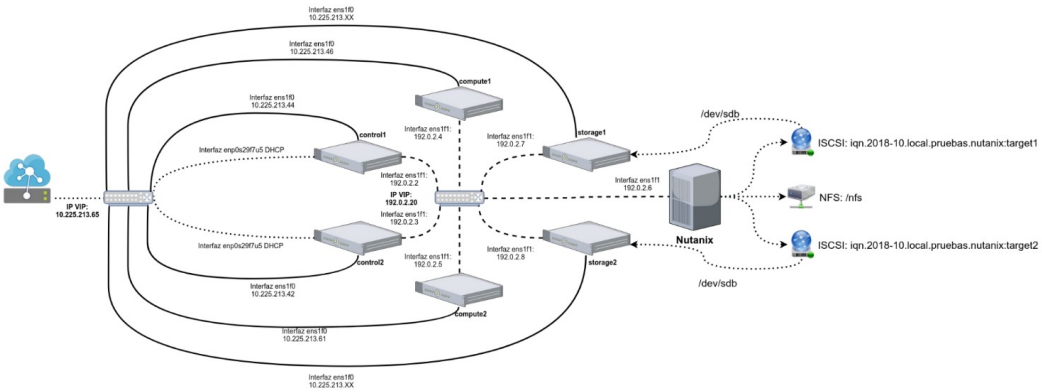

Ilustración 10: Esquema básico de los componentes de Oracle Openstack

6.6 Despliegue de la solución

Si el proceso ha sido correcto, podremos acceder al servicio Horizon:

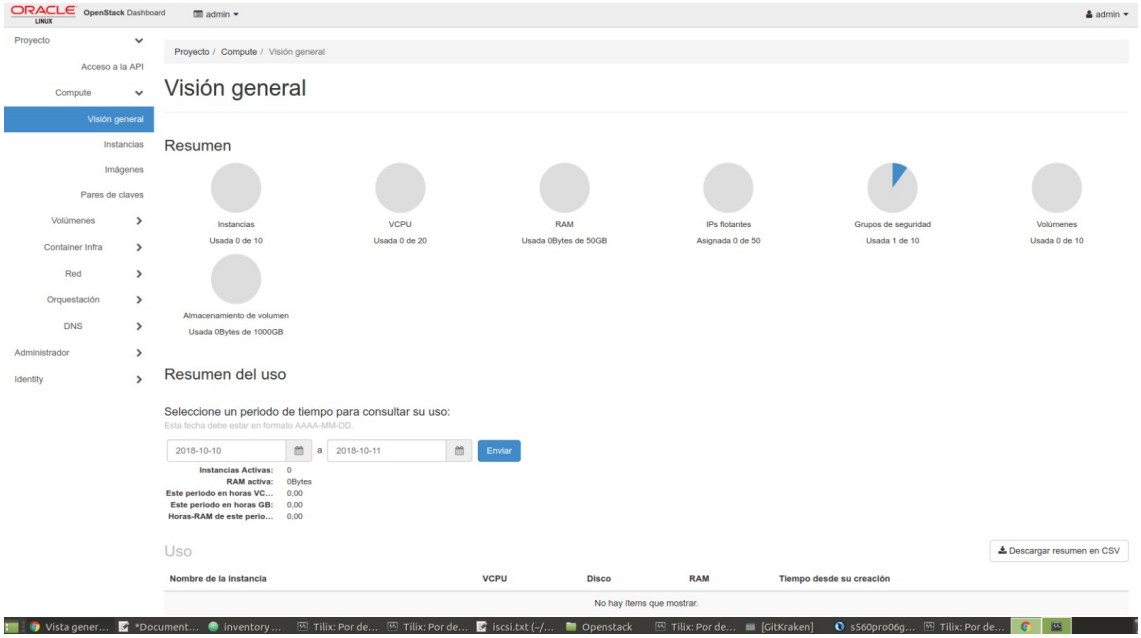

Ilustración 11: Panel de control de openstack

7. Administración de los datos

7.1 Centralización de la información

En nuestro proyecto toda la información quedará centralizada en los servicios de base de datos de Openstack.

7.2 Política de acceso y seguridad a los datos

La seguridad de los datos se asegurará mediante diferentes estrategias:

- En el caso de las redes de transporte, esta se realizará mediante el uso de redes MPLS. Esto permitirá mantener el trafico de la Organización aislado del resto de trafico del proveedor.

- En el caso de la plataforma Openstack, esta se realizará mediante el componente Keystone. En el mismo se definirán las políticas de acceso a los diferentes recursos de la Organización. De esta forma podremos asignar tareas de gestión de los cortafuegos por roles.

8. Valoración Productiva y Presupuestaria

En el caso de la estimación de coste de la infraestructura, los nodos utilizados en el despliegue han sido reutilizando servidores existentes en la infraestructura de la Organización, con lo cual el coste ha sido cero.

Con respecto al coste de licenciamiento, solo es necesario tener en cuenta el pago de la licencia de Oracle Linux, puesto que Oracle no licencia Openstack. Para ello utilizaremos la calculadora http://www.oracle.com/us/media/calculator/vm/vm-home-2132015.html.

9. Conclusiones

Una vez finalizado el proyecto podemos concluir que el mismo ha tenido un resultado satisfactorio. La situación de partida era un escenario complejo y la solución propuesta para el mismo aunque también compleja satisface los objetivos propuestos:

- Reducción de costes operativos: Gracias a la puesta en marcha de Openstack se podrá eliminar todo el hardware, tanto de seguridad como de infraestructuras, que presta los servicios en las sedes

- Mejora en la gestión de la seguridad: Gracias a contar con políticas de seguridad en todas las sedes gracias al “FwaaS” se mejora la seguridad en toda la red de la Organización.

- Mejora en la gestión de la infraestructura: Gracias a contar con una infraestructura fiable en el CPD centralizado se mejora la gestión de los servicios que anteriormente se prestaban desde las sedes.

- Gestión unificada de todos los recursos de IT: Gracias a contar con un panel donde se pueden gestionar tanto los servidores como las políticas de seguridad de las sedes se podrá realizar una gestión unificada.

Como lecciones aprendidas durante esta proyecto debemos resaltar:

- La definición de los riesgos no fue lo suficientemente detallada y cuando se presentaron los planes de contingencia, no fueron totalmente efectivos. En particular en el caso del conocimiento tecnológico de la plataforma, la ejecución del plan se realizó con retraso y esto pudo afectar a la finalización en plazo de este proyecto.

De cara a futuro se abre las siguientes lineas de trabajos:

- Desplegar un servicio de VPN corporativo dentro de Openstack.

- Crear un despliegue en alta disponibilidad de Openstack. Mediante una implantación simétrica a la realizada en este proyecto, como una nueva zona y en un CPD de respaldo.

10. Glosario

Hiperconvergencia: Infraestructura definida por software que separa las operaciones de la infraestructura del hardware del sistema y las converge a nivel de hipervisor en un bloque único. Los sistemas hiperconvergentes aprovechan la inteligencia definida por software para desglosar los silos de almacenamiento y procesamiento y permiten que se ejecuten y gestionen en la misma plataforma de servidor, lo que elimina las ineficiencias y acelera el procesamiento.

Hipervisor: Plataforma que aplica técnicas de virtualización de hardware para ejecutar diferentes sistemas operativos sobre un mismo servidor.

Multivendor: Múltiples proveedores.

11. Bibliografía

[1] https://azure.microsoft.com/es-es/overview/what-is-cloud-computing/ [2018-10-03]
[2] https://docs.oracle.com/cd/E96260_01/index.html [2018-10-10]

12. Anexos

12.1 Despliegue de Oracle Openstack

Tal y como hemos indicado en la memoria, utilizaremos una script de automatización de ansible para el despliegue. En este script indicaremos los host sobre los que se debe actuar mediante un inventario:

ansible-playbook -i inventory playbook-openstack.yml -e particion_docker="/dev/sdb" -e num_particion_docker="1"

A continuación mostramos el contenido del inventario:

```
[controllernode]
#control1 ansible_host=10.225.213.44 ansible_user=root
ansible_password=dem012345 particion_docker="/dev/sda"
num_particion_docker="4"
#control2 ansible_host=10.225.213.42 ansible_user=root
ansible_password=dem012345 particion_docker="/dev/sda"
num_particion_docker="4"
#compute1 ansible_host=10.225.213.46 ansible_user=root
ansible_password=dem012345 particion_docker="/dev/sda"
num_particion_docker="4"
#compute2 ansible_host=10.225.213.61 ansible_user=root
ansible_password=dem012345 particion_docker="/dev/sda"
num_particion_docker="4"
#network1 ansible_host=10.225.213.66 ansible_user=root
ansible_password=dem012345 particion_docker="/dev/sda"
num_particion_docker="4"
#network2 ansible_host=10.225.213.67 ansible_user=root
ansible_password=dem012345 particion_docker="/dev/sda"
num_particion_docker="4"
#storage1 ansible_host=10.225.213.68 ansible_user=root
ansible_password=dem012345 particion_docker="/dev/sda"
num_particion_docker="4"
#storage2 ansible_host=10.225.213.73 ansible_user=root
ansible_password=dem012345 particion_docker="/dev/sda"
num_particion_docker="4"

[controllermaster]
#control1 ansible_host=10.225.213.44 ansible_user=root
ansible_password=dem012345 particion_docker="/dev/sda"
num_particion_docker="4"

[controllers:children]
controllernode
controllermaster
```

En este momento deberemos acceder al nodo master como administrador y ejecutar:

```
kollacli host list
kollacli host add control1.pruebas.local
kollacli host add control2.pruebas.local
kollacli host add compute1.pruebas.local
kollacli host add compute2.pruebas.local
kollacli host add network1.pruebas.local
kollacli host add network2.pruebas.local
kollacli host add storage1.pruebas.local
kollacli host add storage2.pruebas.local
kollacli host list
```

Creamos el acceso ssh para ansible (pide password de root de cada servidor):

```
kollacli host setup control1.pruebas.local
kollacli host setup control2.pruebas.local
kollacli host setup compute1.pruebas.local
kollacli host setup compute2.pruebas.local
kollacli host setup network1.pruebas.local
kollacli host setup network2.pruebas.local
kollacli host setup storage1.pruebas.local
kollacli host setup storage2.pruebas.local
```

A continuación comprobaremos el acceso:

```
kollacli host check all
```

Obteniendo como resultado:

```
Host network2.pruebas.local: success
Host control2.pruebas.local: success
Host control1.pruebas.local: success
Host network1.pruebas.local: success
Host compute1.pruebas.local: success
Host compute2.pruebas.local: success
Host storage1.pruebas.local: success
Host storage2.pruebas.local: success
```

En este momento deberemos configurar el Registry:

```
kollacli property set docker_registry ""
kollacli property set docker_registry_email ""
kollacli property set docker_registry_username ""
kollacli property set docker_namespace "oracle"
```

Asignamos los grupos:

```
#control
kollacli group addhost control control1.pruebas.local
kollacli group addhost control control2.pruebas.local
#database
kollacli group addhost database control1.pruebas.local
kollacli group addhost database control2.pruebas.local
#network
kollacli group addhost network network1.pruebas.local
kollacli group addhost network network2.pruebas.local
#storage
kollacli group addhost storage storage1.pruebas.local
kollacli group addhost storage storage2.pruebas.local

#compute
kollacli group addhost compute compute1.pruebas.local
kollacli group addhost compute compute2.pruebas.local
```

Y comprobamos la asignación de grupos:

```
kollacli group listhosts
+----------+-----------------------------------------------+
| Group    | Hosts                                         |
+----------+-----------------------------------------------+
| compute  | [compute1.pruebas.local,compute2.pruebas.local] |
| control  | [control1.pruebas.local,control2.pruebas.local] |
| database | [control1.pruebas.local,control2.pruebas.local] |
| network  | [network1.pruebas.local,network2.pruebas.local] |
| storage  | [storage1.pruebas.local,storage2.pruebas.local] |
+----------+-----------------------------------------------+
```

En este momento activaremos los servicios para el despliegue:

```
kollacli property set enable_barbican yes
kollacli property set enable_magnum yes
kollacli property set enable_ironic no
kollacli property set enable_designate yes
kollacli property set glance_backend_ceph yes
kollacli property set glance_ha_test yes
kollacli property set enable_ceph yes
kollacli property set glance_backend_ceph yes
kollacli property set nova_backend_ceph yes
kollacli property set enable_ceph yes
kollacli property set enable_neutron_fwaas yes
kollacli property set enable_neutron_lbaas yes
```

Configuraremos la red

```
kollacli property set kolla_internal_vip_address 192.0.2.20
kollacli property set network_interface ens1f1
kollacli property set network_interface enp12s0f1 --groups storage
```

#kollacli property set property_name value --hosts host_list
kollacli property set neutron_external_interface enp0s29f7u3
kollacli property set kolla_enable_tls_external no #quita esto!!!
kollacli property set kolla_external_vip_address 10.225.215.8
kollacli property set kolla_external_vip_interface ens1f0
kollacli property list
kollacli property set glance_backend_ceph yes
kollacli property set glance_nfs_share 192.0.2.50:/nfs
kollacli property set glance_file_datadir_volume /nfs
kollacli certificate init

Volvemos a comprobar que todo está correcto antes del deployment:

kollacli host check all --predeploy

Y realizamos el deploy

kollacli deploy -vvv
kollacli deploy -vvv --debug --log-file log-out.txt
kollacli deploy --debug --log-file 11_octubre.txt
kollacli deploy –serial #para actualizar sin interrupciones