Estudio de redes definidas por software y su implantación en redes privadas

Autor: Tafalla Pemán, Alfonso

Director/es: Fernández García, Norberto y Suárez Lorenzo, Fernando

Contacto: alfonsotafalla@yahoo.es

Resumen: SDN son las siglas de Redes Definidas por Software. La definición más sencilla y directa de esta arquitectura es la separación física del plano de control del plano de datos o reenvío y donde el plano de control gestiona distintos dispositivos de red. Con ello, se favorece la implementación de servicios de red de forma ágil, dinámica y escalable, estando la lógica de control en un dispositivo común denominado controlador.

El paradigma SDN mejora la seguridad de la red, ya que se proporciona una total visibilidad de la misma, realizando análisis continuos y dando respuesta de una forma proactiva, propagando políticas de seguridad desde el controlador de forma ágil y dinámica, a todos los dispositivos de la red.

SDN y en concreto la SD-WAN (Redes de Área Amplia Definidas por Software), está evolucionando a otra solución denominada SASE (Acceso Seguro de Servicios de Borde) en el que incluye la propia SD-WAN, pero se añaden servicios en la nube en relación a control de accesos, funciones de seguridad y cortafuegos.

En este trabajo se estudian las redes definidas por software y su implementación en redes privadas, con diferentes soluciones propietarias de diversos fabricantes posicionados en el cuadrante mágico de Gartner, como líderes en infraestructuras frontera en redes de área amplia. A modo de práctica se realiza una simulación de la solución Cisco ACI, con su controlador Cisco APIC, observando la facilidad y sencillez en la implementación, monitoreo y gestión de una arquitectura spine-leaf en centros de datos.

Palabras clave: SDN, Openflow, NFV, Overlay y Underlay

---

1. Introducción

1.1. Introducción a las redes definidas por software

SDN son las siglas de Software Defined Networking o redes definidas por software, la definición más sencilla y directa de esta arquitectura nos la da la Open Networking Foundation (ONF) [1],

organización impulsada por los usuarios cuyo fin es promover la estandarización y comercialización de SDN a través del desarrollo de estándares abiertos. Esta organización define SDN como:

"La separación física del plano de control del plano de datos o reenvío y donde el plano de control gestiona distintos dispositivos de red" [1]

Básicamente esto significa que vamos a reducir la carga del plano de control en los equipos de red y se le otorgará a un elemento de la red (plataforma de gestión) que, de manera centralizada, no solamente gestionaría un equipo, sino que lo hará con un conjunto completo de varios equipos de forma dinámica y efectiva. Es por ello que una red definida por software es una arquitectura ideal para los entornos de red en los que en el día a día se debe responder de manera oportuna a la creciente demanda de servicios por parte de sus clientes.

Entre las características más destacables, al integrar una red con SDN le proporcionamos la capacidad de ser directamente programable. Ahora podemos aprovechar las fortalezas del software para hacer que nuestra red sea fácil de gestionar, configurar y operar. Otra de sus características es que, dado su dinamismo, es una arquitectura ágil donde podemos programar software o aplicaciones que realicen distintas tareas de acuerdo con ciertos parámetros o comportamientos de la red.

SDN utiliza controladores centralizados para la gestión de los dispositivos de la red, haciéndola bastante flexible y escalable y permitiendo configurar, gestionar y optimizar los recursos de red de manera dinámica. El controlador centralizado se encargará de tomar las decisiones y gestionar el comportamiento de los equipos de red, siendo su arquitectura compuesta de tres capas, tal y como se ve en la figura 1-1.

Lo primero que se puede lograr con este paradigma es tener un control centralizado y más efectivo de la red, pudiendo mejorar significativamente la gestión y la detección de eventos no deseados en la red, lo que luego permitirá tomar las mejores decisiones y tener un mayor rendimiento. Se pueden desplegar conmutadores/enrutadores virtualizados en cortos periodos de tiempo y, por último, se puede automatizar el comportamiento de la red mediante la creación de políticas.

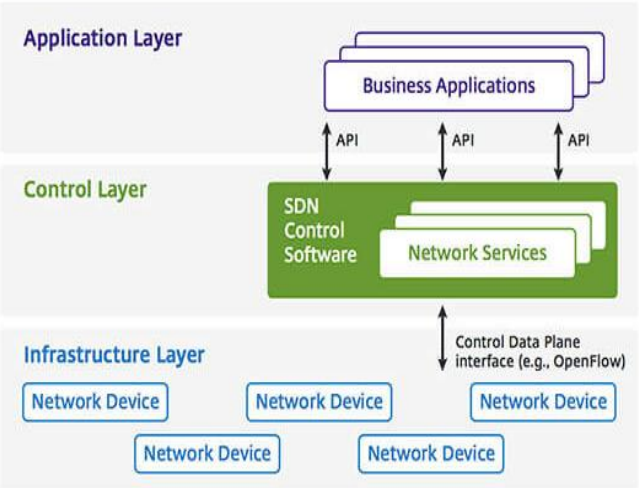

Figura 1-1: Arquitectura SDN (Fuente [1])

2. Desarrollo

2.1 Soluciones comerciales SDN

Una vez introducido el paradigma SDN, se van a exponer diversas soluciones SDN actuales, basándose en el cuadrante mágico de Gartner, en relación a las infraestructuras de borde en redes WAN, íntimamente ligadas a la tecnología SD-WAN. En la figura 2-1 se observa dicho cuadrante [2].

Figura 2-1 Cuadrante de Gartner WAN Edge Infrastructure

(septiembre 2021) (Fuente [2])

Las mejores soluciones SDN del mercado (zona de líderes en el cuadrante), en este caso más concretamente SD-WAN, las aportan las siguientes empresas:

- Fortinet
- VMware
- Versa Networks
- Palo Alto Networks
- Cisco
- HPE (Aruba y Silver Peak)

2.2 Fortinet

La solución SD-WAN de Fortinet está implementada en el hardware de los equipos que comercializan, en el sistema operativo de los cortafuegos de nueva generación denominados Fortigate, permitiendo simplificar las operaciones de red y seleccionar los mejores caminos hacia un destino, con la capacidad de tener múltiples conexiones a distintas sucursales de una organización y seleccionar

automáticamente cuál es la mejor alternativa para conectarnos de extremo a extremo, visualizando qué aplicaciones están corriendo por la red y dando prioridad a las más críticas.

Todos los equipos Fortigate tienen unos circuitos integrados con tecnología patentada por Fortinet (ASIC) que realizan el procesamiento de tráfico y el procesamiento de seguridad independientemente al procesamiento principal, es decir, los equipos tienen una CPU como cualquier equipo informático, pero además tienen un procesador dedicado para el tráfico de red y un procesador dedicado para el tráfico de seguridad, siendo esto una innovación de Fortinet, consiguiendo con ello alcanzar muy altas velocidades de procesamiento.

2.3 VMware

La solución de la empresa VMware de SD-WAN se denomina VMware SD-WAN de Velocloud, su lanzamiento se produjo en 2019 conectando más de 200 oficinas remotas de MD Anderson, una extensión de la Universidad de Texas, localizada en Houston, dedicada al campo de la medicina. VMware SD-WAN introdujo la automatización y la visibilidad en las oficinas remotas, lo que permitió una implementación rápida y eficiente. Con el aprovisionamiento de cero toques (ZTP), los trabajadores de oficinas remotas pueden instalar VMware SD-WAN Edge ellos mismos. El dispositivo se conecta automáticamente a la herramienta de administración central basada en la nube, denominada Orquestador VMware SD-WAN. Esto conecta inmediatamente al trabajador a la red corporativa y los administradores de red pueden ver los bordes individuales de VMware SD-WAN activados, pudiendo solucionar problemas desde la sede central.

2.4 Versa Networks

La solución de SD-WAN forma parte de la solución SASE de Versa Networks. Característica de la solución es la superposición (overlay) cifrada o no cifrada vía MPLS, GRE (Generic Routing Encapsulation), VXLAN, etc.

La tecnología de Secure SD-WAN de Versa Networks se diferencia de otros fabricantes o proveedores de SD-WAN porque implementa capacidades que permiten una arquitectura de SASE, incluyendo visibilidad del tráfico que recorre la red entre los usuarios, las aplicaciones y los dispositivos independientemente de su ubicación.

2.5 Palo Alto Networks

Palo Alto Networks tiene varias soluciones SD-WAN entre las cuales las más extendidas son CloudGenix SD-WAN y Prisma Access.

CloudGenix SD-WAN es una solución en la nube que opera a nivel de sesión y flujo de aplicaciones, a diferencia de los conmutadores y enrutadores de las SD-WAN tradicionales, que lo hacían en capa 2 y 3.

Prisma Access es otra solución, que consigue una mayor seguridad y protección donde sea necesario, tanto en sedes, como para cualquier trabajador de la organización en movilidad, ya que se trata de una evolución de SD-WAN a un servicio de acceso seguro de borde (SASE), que proporciona seguridad a todos sus usuarios y aplicaciones.

2.6 Cisco

Cisco tiene la solución SD-WAN de empresa, anteriormente denominada Viptela. En ella están implementados todos los componentes principales de la solución Cisco SD-WAN consistiendo en el sistema de administración de red vManage (plano de administración), el controlador vSmart (plano de control), el orquestador vBond (plano de orquestación) y el enrutador WAN Edge (plano de datos).

Todos los componentes se basan en software salvo el enrutador WAN Edge que está disponible como dispositivo de hardware o enrutador basado en software y se ubica en un sitio físico o en la nube, proporcionado conectividad segura en el plano de datos entre los sitios a través de uno o más transportes WAN.

2.7 HPE (Aruba y Silver Peak)

La arquitectura de SD-WAN de Silver Peak se denomina Aruba EdgeConnect SD-WAN, donde hay un orquestador centralizado que controla, monitoriza y gestiona los equipos EdgeConnect, que son dispositivos de infraestructura de borde, los cuales se pueden implementar en tres modalidades (físicos, virtuales o en la nube), dependiendo de los requerimientos de la organización o empresa.

El orquestador se puede ejecutar de forma local “on premise”, en la nube o como un servicio, todo dependerá de las necesidades de la empresa. De manera opcional, se puede implementar un dispositivo denominado Boost WAN Optimization, para acelerar los procesos y optimizarlos. Si un usuario ejecuta una aplicación, la misma se almacena en la memoria caché del EdgeConnect, de tal forma que cuando otro usuario quiera disponer de ella, lo haga con menos latencia.

3. Prueba y validación

3.1 Arquitectura spine-leaf

Durante años, los centros de datos se han construido en una arquitectura de tres niveles (capa de núcleo, capa de agregación/distribución y capa de acceso). Pero con los centros de datos integrados, la virtualización y el surgimiento de sistemas hiperconvergentes, una nueva arquitectura de red, spine-leaf [3], se ha convertido en la implementación actual de la red de los centros de datos, superando algunas limitaciones de la arquitectura tradicional de tres niveles. Con esta arquitectura se consigue una latencia mejorada, los cuellos de botella reducidos y el ancho de banda ampliado.

La arquitectura de red spine-leaf se está imponiendo hoy en día en grandes centros de datos o redes en la nube debido a su escalabilidad, fiabilidad y un mejor rendimiento. El diseño de spine-leaf solo tiene dos capas, la capa spine y la capa leaf. La capa spine está formada por conmutadores para el proceso de enrutamiento, siendo la columna vertebral de la red. Por otro lado, la capa leaf consta de conmutadores a los que se conectan dispositivos finales, de almacenamiento, servidores, etc. Cada conmutador leaf está conectado con todos los conmutadores spine (entre ellos no conectados), por lo tanto, para que un dispositivo final se comunique con otro dispositivo conectado en otro conmutador leaf, sólo habrá una ruta posible a través del conmutador spine que conecta dos conmutadores leaf.

El simulador Cisco ACI proporciona un software del controlador Cisco APIC con funciones completas, junto con una infraestructura de estructura simulada de conmutadores spine y leaf en un servidor físico. Se puede usar para comprender las funciones, ejercitar las API e iniciar la integración con sistemas y aplicaciones de orquestación de terceros.

El simulador de Cisco ACI incluye conmutadores simulados, por lo que no puede validar una ruta de datos. Además, el simulador Cisco APIC permite la simulación de fallos y alertas para facilitar las pruebas y demostrar funciones.

3.2 Instalación del simulador Cisco ACI

Para el desarrollo de la práctica es preciso la instalación del simulador Cisco ACI. Para ello es necesario descargar el archivo de extensión ova de su máquina virtual, de la página web de Cisco [4]. Una vez dentro de la web de descarga, se elige la versión del simulador ACI más actualizada. Dicha versión se compone de seis archivos, que posteriormente se unirán para recomponer el archivo ova de la máquina virtual del simulador.

Para ejecutar el archivo ova de la máquina virtual del simulador hay que disponer del software hipervisor de VMware Workstation, ya que la citada máquina virtual no es compatible con el hipervisor VirtualBox. Dependiendo de la versión de sistema operativo Windows 10 (Pro o Enterprise) que se tenga instalado, será necesaria una versión de VMware Workstation compatible.

3.3 Práctica del simulador de Cisco ACI

Una vez que se ha cargado la web del simulador Cisco ACI, con el usuario/contraseña que definimos en la instalación del mismo, lo abrimos, implementamos los dispositivos spine-leaf y configuramos los parámetros básicos que nos solicita para su funcionamiento (figura 3-1) :

- Fabric Membership. Se configuran y registran los dispositivos que el propio simulador detecta que están conectados a la red (por diseño e instalación del simulador sólo se dispondrá de un conmutador spine y dos conmutadores leaf).
- BGP. Configuración de los conmutadores spine que van actuar con el protocolo BGP, para comunicar entre sí a los conmutadores leaf que consideremos oportuno para el buen funcionamiento de la solución (por diseño e instalación del simulador sólo se dispondrá de un conmutador spine).
- NTP. Configuración de servidores NTP (Network Time Protocol) para el uso del controlador Cisco APIC (sólo uno en esta implementación) y los conmutadores spine-leaf.
- DNS. Configuración de servidores DNS para el uso del controlador Cisco APIC y los conmutadores spine-leaf.
- Proxy. Configuración de servidores Proxy para el uso del controlador Cisco APIC.
- Out of Band Management. Configuración de la interfaz de gestión para nodos vía IP que se conecten a la red de gestión OOB (Out of Band).
- Global Configurations. Configuraciones generales recomendadas.

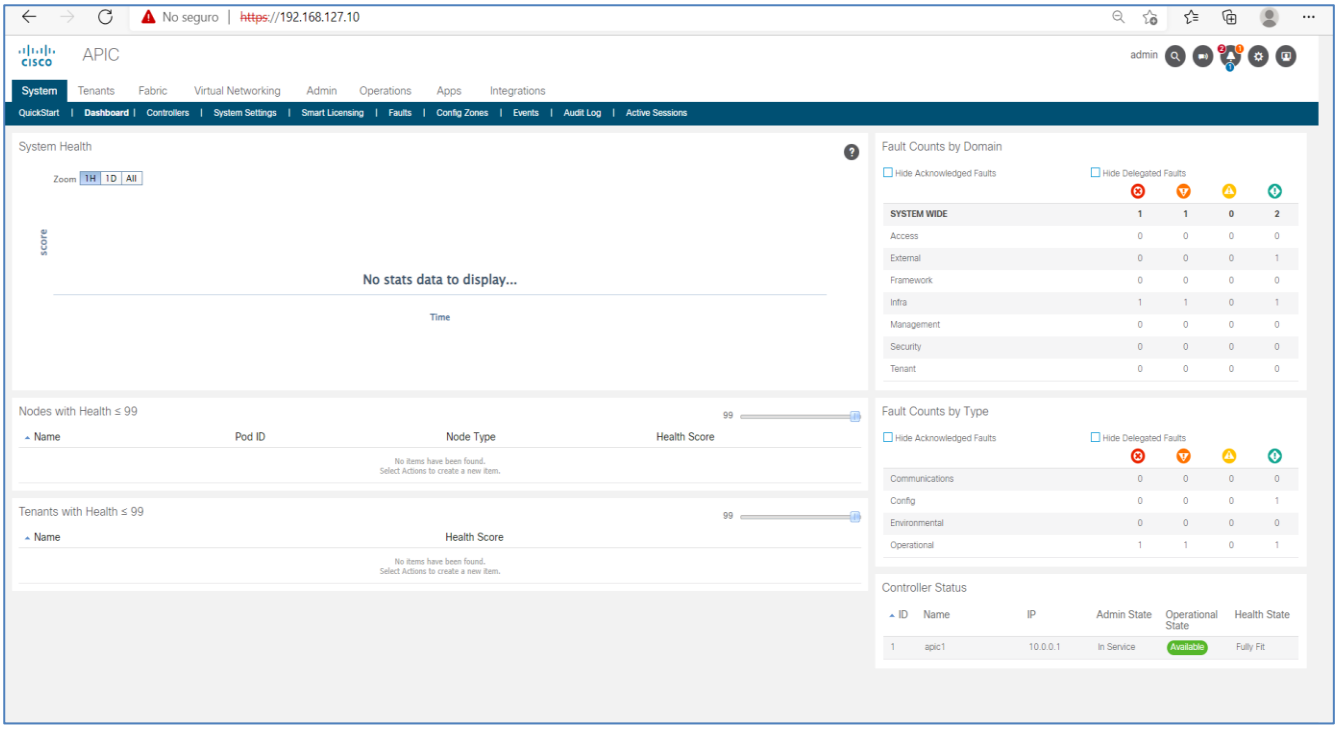

Figura 3-1 Simulador APIC (Fuente propia)

Una vez en funcionamiento la solución Cisco ACI se pueden recorrer los innumerables menús de la misma, configurando y personalizando nuestros requerimientos. Se pueden hacer diversas configuraciones, mostrar la topología, crear nuevos tenant o grupos de usuarios con sus perfiles (por defecto el simulador crea tres), configurar las actualizaciones de firmware (con un solo clic de ratón), visualizar todos los puertos de los conmutadores o la configuración de roles de acceso y su autenticación entre otros.

4. Conclusiones

Como hemos visto en el trabajo, SDN son las siglas de Software Defined Networking o redes definidas por software. La característica principal de este paradigma es la separación física del plano de control del plano de datos o reenvío y donde el plano de control gestiona distintos dispositivos de red.

Este paradigma favorece la implementación de servicios de red de forma ágil, dinámica y escalable, estando la lógica de control en un dispositivo común a toda la red denominado controlador, desde el cual se gestionan todos los componentes de la red de forma centralizada, descargando de este trabajo al propio hardware de los dispositivos.

Con la característica del control centralizado y de programabilidad de la red en SDN, se puede implementar de forma más sencilla y dinámica la seguridad de los dispositivos de red, pero por otro lado, el controlador se convierte en un potencial objetivo debido a su papel fundamental en una red definida por software.

Se han mostrado en el desarrollo de este trabajo multitud de soluciones y tipos de SDN, de fabricantes que en estos momentos lideran este campo, según lo indicado en el cuadrante mágico de Gartner, con las cuales cualquier organización puede actualizar sus redes para el cumplimiento de los requisitos que sean necesarios en la misma.

En beneficio de la seguridad, SDN está evolucionando a otro paradigma denominado SASE (Acceso Seguro de Servicios de Borde) en el que incluye SD-WAN, pero complementándolo con servicios en la nube en relación a control de accesos, funciones de seguridad y cortafuegos.

Como conclusión final, resulta beneficiosa la implementación del paradigma SDN, además de para mejorar la seguridad, para hacer más dinámicos otros procesos de red, ya que tiene muchas ventajas sobre las redes tradicionales y en la mayoría de las soluciones se puede realizar la transición al nuevo modelo de forma progresiva, coexistiendo las dos, de forma conjunta.

Referencias

1. Web de Open Networking Foundation (ONF), [en línea]. Disponible: https://opennetworking.org/ [Último acceso enero 2022].
2. Web de Bafing, [en línea] Disponible: https://www.bafing.com/infraestructura-wan-edge-de-fortinet-lider-en-gartner-2021/ [Último acceso enero 2022].
3. Web de FS community [en línea] Disponible: https://community.fs.com/es/blog/leaf-spine-with-fs-com-switches.html [Último acceso enero 2022].
4. Web de Cisco sobre simulador Cisco ACI, [en línea] Disponible: https://www.cisco.com /c/en/us/products/cloud-systems-management/application-centric-infrastructure-simulator [Último acceso enero 2022].