Un informe de Lippis Consulting sobre la industria

Cisco prepara ACI para su lanzamiento general Expectativas

Por Nicholas John Lippis III
Presidente de Lippis Consulting

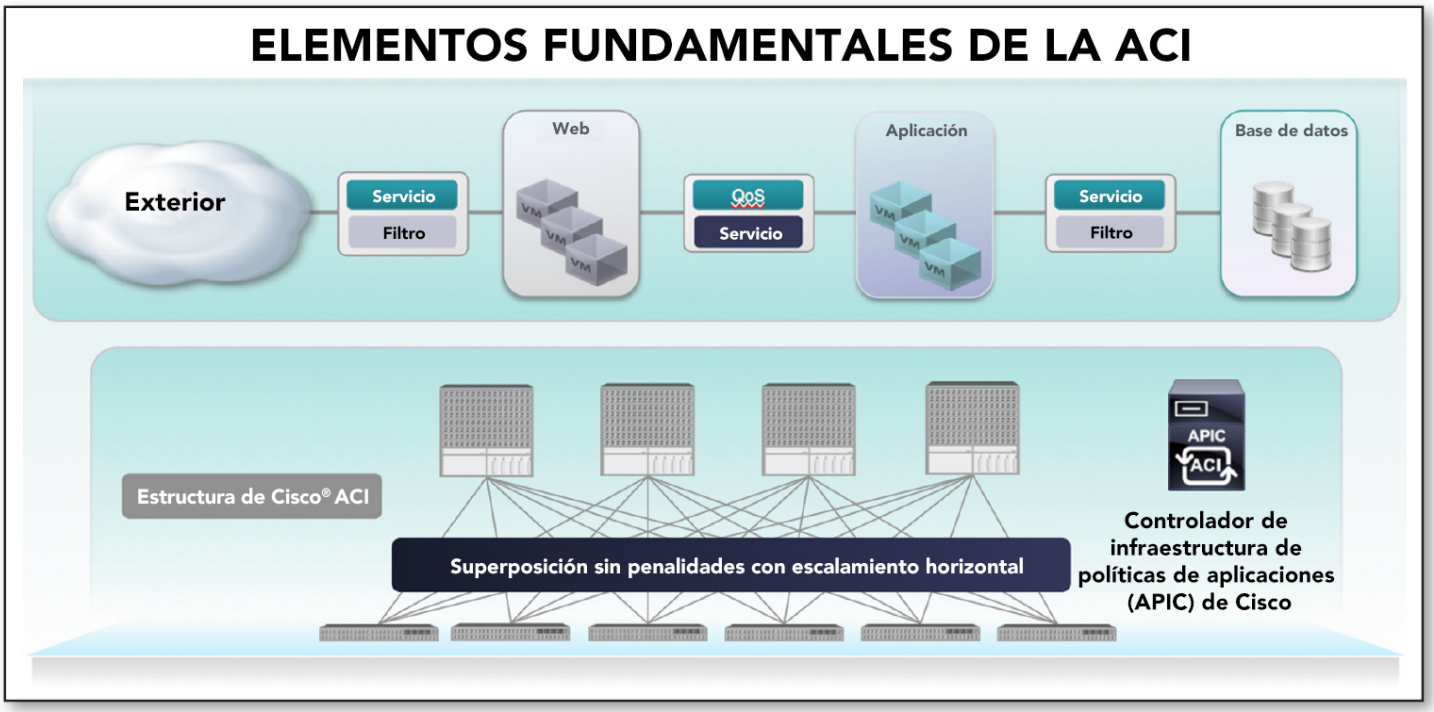
Agosto de 2014

Uno de eventos de redes más importantes de este mes de agosto es el lanzamiento general de la Infraestructura centrada en aplicaciones (ACI) de Cisco. Cisco ha enviado su serie de switches Nexus 9000 en lo que se ha llamado “modo autónomo”, un switch Ethernet para centro de datos ultrarápido, desde el mes de noviembre de 2013. Los pedidos de Nexus 9000 se triplicaron: pasaron de 180 en el tercer trimestre a 580 al finalizar el cuarto trimestre fiscal de Cisco. Como parte del lanzamiento de la serie Nexus 9000, Cisco prometió que estos switches se podrían implementar en lo que se llama “modo de estructura ACI”. Este modo de estructura ACI promete reducir el costo operativo, aumentar el dinamismo y vincular aplicaciones a la infraestructura de red como nunca antes se hizo. La manifestación del modo de estructura es ACI y ahora está ingresando a la etapa de lanzamiento general. En esta nota de investigación del informe Lippis, analizamos ACI desde la perspectiva de lo que puede hacer hoy por los arquitectos de centros de datos.

La solución ACI está compuesta por tres elementos fundamentales: 1) un modelo de políticas que actúa como principio de organización para determinar cómo se deben agrupar los dispositivos en constructos similares a contenedores y para describir cómo se conectan, 2) el APIC, o Controlador de infraestructura de políticas de la aplicación, que proporciona un único punto de administración y repositorio para las políticas descriptas y 3) la estructura ACI, que es una abstracción de todos los dispositivos de red físicos y virtuales que conforman la estructura ACI. Aquí le ofrecemos un breve resumen de los tres componentes de la ACI como recordatorio.

de base de datos back-end; es posible que esta aplicación requiera actividad desde el mundo exterior. La política para describir las necesidades de conectividad correspondientes a esta aplicación se pueden definir directamente utilizando las políticas basadas en grupos que se encuentran dentro de la ACI, pero el modelo también podría ser muy genérico. La política podría usarse para definir políticas orientadas a la seguridad en las que un grupo externo (sitio remoto y tráfico de Internet) se conecta al grupo de la zona perimetral (DMZ), el que luego se conecta al grupo interno, por ejemplo. Como alternativa, una GBP incluso podría modelar la manera en la que se describe la mayoría de las redes actualmente, en términos de redes VLAN y/o subredes, lo que se asignaría en diversos grupos. En última instancia, Cisco desearía presentar a las diferentes partes interesadas este concepto de políticas basadas en grupos para no sea necesario contar con personal con certificación CCIE **(Cisco Certified Internetwork Expert)** ni con un genio en redes para generar conectividad. Un administrador simplemente expresaría que este “grupo de cosas” se conecta a otro “grupo de cosas”. Cisco denomina a estos “grupos de cosas” arbitrarios con la la terminología EPG (grupo de terminales) y representa un grupo de terminales físicos o virtuales. Es decir, un EPG podrían ser servicios físicos, servidores de hardware puro, máquinas virtuales en varios hipervisores diferentes, etc. Lo importante es que Cisco puede ubicar “cosas” dentro de grupos con relativa flexibilidad, independientemente de dónde se encuentren en toda la estructura de la ACI.

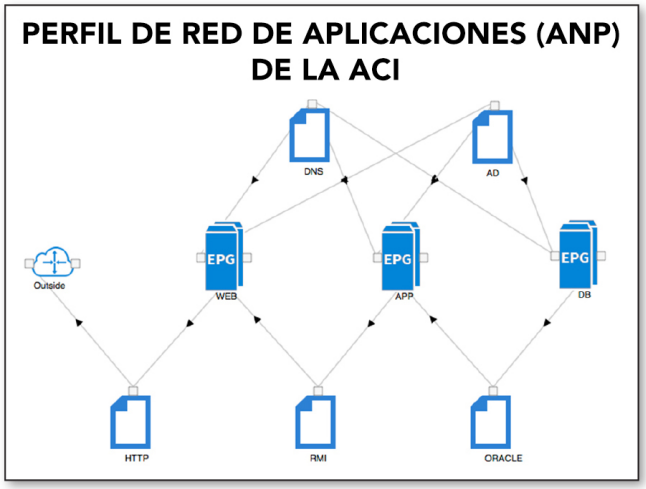
Otro de los conceptos centrales del modelo de políticas de la ACI es la capacidad para definir la relación entre diversos EPG.



Modelo de políticas: el modelo de políticas de la ACI crea una nueva manera de describir la conectividad por medio de lo que Cisco llama el concepto de política basada en grupos (GBP). El modelo de políticas de Cisco proporciona una manera genérica de describir cómo se conectan los componentes. Como ejemplo, considere una aplicación típica de tres niveles implementada en un centro de datos que puede estar compuesto por un nivel front-end web, un nivel de aplicaciones de middleware y un nivel

Esta relación se llama “contrato” y describe lo que puede circular o los métodos de conectividad que se permiten entre diferentes EPG. Un contrato puede estar conformado por un protocolo (o un conjunto de protocolos) específico que tendría permitido circular entre los grupos, o que también podría usarse para incorporar un gráfico de servicios de capa 4 a 7 para aplicar servicios de red como un firewall, un equilibrador de cargas, etc., a la conectividad entre grupos.

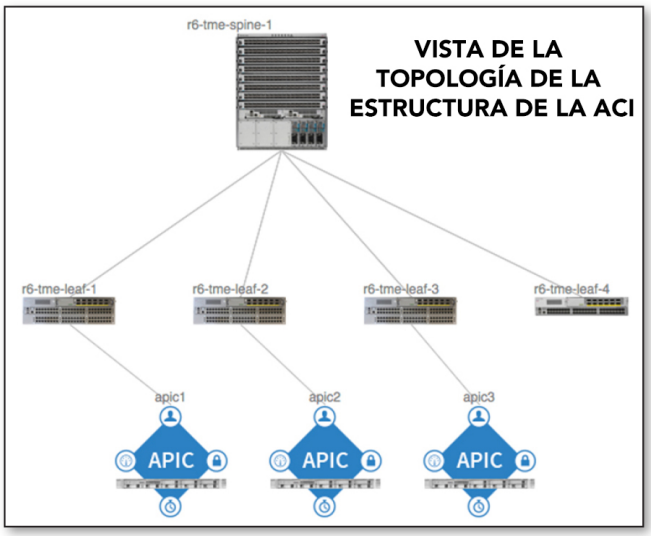
Desde la perspectiva de operaciones de seguridad (SecOps), el modelo de políticas de la ACI implementa esencialmente un modelo de lista blanca para la seguridad, lo que difiere ampliamente de la implementación actual de las ACL. En el modo de red actual, operaciones de red (NetOps) asume cualquier elemento puede comunicarse, pero solo que no puedan deberían bloquearse con listas de control de acceso (ACL); estosigue un modelo de lista negra para la seguridad. En esencia, toda la estructura de la ACI puede considerarse idéntica desde lo operativo a un gran firewall distribuido basado en el contexto, que hace cumplir políticas en forma integral en todo el centro de datos.



Cisco incluye estas definiciones de EPG, contratos y redes externas en lo que denomina perfil de red de aplicaciones (ANP). Estos ANP están completamente abstraídos/desacoplados de cualquier infraestructura física/virtual subyacente y, por lo tanto, se pueden copiar en una estructura de la ACI completamente diferente y crear una nueva instancia. Esto facilita enormemente la tarea de definir la conectividad de las aplicaciones globalmente en diferentes pods o sitios sin que el administrador de las aplicaciones precise comprender los detalles de la arquitectura de una estructura determinada.

APIC: las políticas de la ACI se describen en el Controlador de infraestructura de políticas de la aplicación, o APIC. El APIC es un clúster de servidores en rack x86 UCS de la serie C de 1 unidad de rack (1RU) y ofrece un único punto de administración y repositorio para todas las políticas descritas, además de cualquier otra política, para aprovisionar, administrar, monitorear y resolver problemas en la estructura; según Cisco, ¡ahora todo es una política! Tenga presente que el APIC no se utiliza para reenvíos ni búsquedas. De hecho, una vez que las políticas se describen dentro del APIC, se lo puede eliminar por completo y todo lo demás seguirá funcionando; pero decimos esto para enfatizar que el APIC no es necesario durante operaciones de reenvío.

De hecho, Cisco no recomienda eliminar por completo todo el clúster del APIC porque los administradores no podrían modificar políticas hasta que se vuelva a conectar al menos un APIC. El clúster del APIC es completamente redundante y presenta equilibrio de cargas al mismo tiempo, con un estado estable recomendado tres dispositivos APIC que conformen el clúster. El sistema ACI modela todo como un objeto y despliega estos objetos en lo que Cisco llama “árbol de información sobre administración distribuida” o dMIT (por su sigla en inglés), de



modo que los objetos individuales heredan propiedades (privilegios de seguridad, atributos, etc.) de sus objetos en un nivel superior inmediato de jerarquía. Estos objetos, a su vez, quedan expuestos en un nivel de jerarquía superior al resto del mundo por medio del APIC a través de diversos medios, entre ellos API de REST (XML/JSON), una interfaz gráfica de usuario (GUI) o una shell de línea de comandos que se asemeja a un entorno BASH de Linux. Como alternativa, Cisco también ofrece kits de desarrollo de software (SDK) adicionales para quienes deseen desarrollar aplicaciones con el objetivo de interactuar directamente con el modelo de políticas de la ACI. En el lanzamiento general (GA), Cisco envía y ofrece soporte para un SDK de Python, pero nos dice que se está trabajando en una variante Ruby e, incluso, en una variante C#.

Estructura de la ACI: esencialmente, la estructura de la ACI es un grupo de dispositivos físicos y virtuales que conforman la estructura de la red y que procesa todas las funciones del plano de datos, como búsquedas, reenvíos, cumplimiento de políticas, etc. Estos dispositivos pueden proporcionar servicios de reenvío (switches y routers) y/o servicios de red de capa 4 a 7 (firewalls, equilibradores de cargas, etc.).

En el centro de la estructura de la ACI nos encontramos con los nuevos switches insignis de Cisco para centros de datos, Cisco Nexus 9000, que están configurados en una topología de nodo principal/nodo secundario que proporciona conectividad, rendimiento, recuperabilidad y flexibilidad con escalamiento horizontal. Al momento de la GA, Cisco ofrece dos variantes de switches de nodo secundario:

- Nexus 9396PX: 48 puertos de 1/10G de factor de forma pequeño enchufable mejorado (SFP+) con un adicional de 12 puertos de uplinks 40G de factor de forma pequeño enchufable cuádruple (QSFP)
- Nexus 93128TX: 96 puertos de 1/10G Base-T+ con un adicional de 8 puertos uplinks 40G QSFP

Cisco también ofrece las siguientes dos variantes de switches de nodo principal:

- Nexus 9336PQ: 36 puertos de enlaces 40G QSFP a los switches de nodo secundario
- Nexus 9508: hasta 288 puertos de enlaces 40G QSFP a los switches de nodo secundario

Cisco también ha asumido el compromiso de ofrecer soporte para otros factores de forma de switches de nodo principal y secundario, incluidos switches de nodo secundario de 1RU, además de switches de nodo principal más pequeños (Nexus 9504 de 4 ranuras) y más grandes (Nexus 9516 de 16 ranuras) en el futuro cercano.

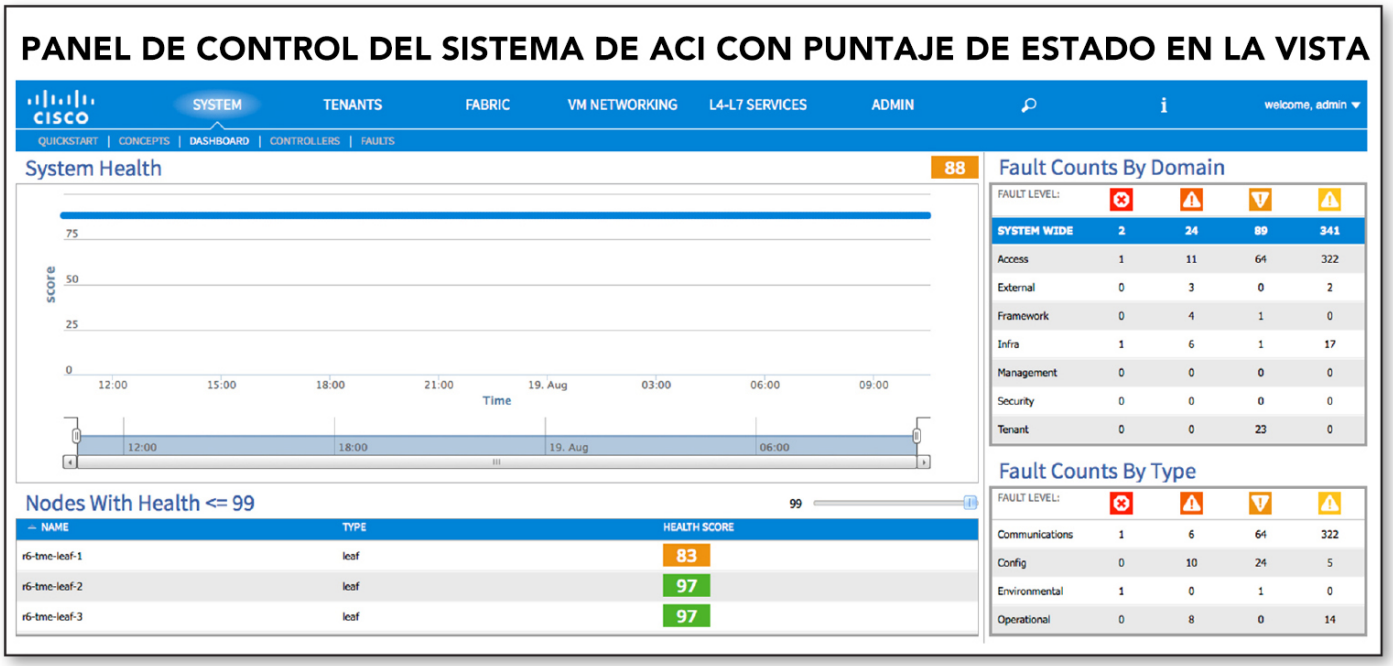
Desde la perspectiva del diseño de red, todos los dispositivos se conectan a los switches de nodo secundario. Los únicos dispositivos que se conectan a los switches de nodo principal son otros switches de nodo secundario. En el interior, Cisco ejecuta routing IPv4 en toda la estructura como su protocolo "subyacente" y utiliza encapsulación "de superposición" de LAN extensible virtual (VXLAN) de hardware para proporcionar puentes y roputing de capas 2 y 3 de cualquier elemento a cualquier elemento en toda la estructura de la ACI.

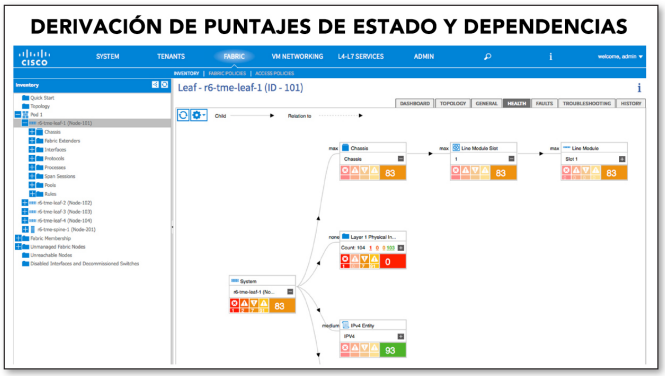
Algo que debe destacarse es que la estructura de la ACI también puede controlar cualquier switch virtual (vSwitch) que resida en diferentes hipervisores con los que se integre (ya sea VMware por medio de vCenter, Microsoft por medio de SCVMM [System Center Virtual Machine Manager] con Windows Server 2012 R2 u OVS por medio de OpenStack [admite las variantes Ubuntu y RedHat]). Además, la estructura de la ACI puede controlar servicios de red a través de plugins a los que Cisco llama "paquetes de dispositivos" y permite que el APIC facilite la coordinación, la automatización y el encadenamiento de servicios de capas 4 a 7; las políticas se extienden verticalmente a estos servicios de red para que los administradores no tengan que gestionar (O "manejar") estos dispositivos por separado. En consecuencia, la estructura de la ACI se extiende más allá de las plataformas Nexus 9000 de Cisco y también abarca a todos los otros servicios con los que se integra.

Poner en marcha la ACI: Health Scores

Lo que resulta fundamental para el enfoque de Cisco con respecto a la ACI es que, con este lanzamiento general, se está ofreciendo un conjunto de herramientas que ayudarán a que los administradores de centros de datos pongan en marcha una implementación de la ACI de Cisco. Una de estas herramientas se llama Health Scores (puntajes de estado). Además de proporcionar un modo optimizado para aprovisionar la estructura de la ACI, Cisco quiso añadir mucho valor a las operaciones del día dos; es decir, la administración y las operaciones diarias. Una vez configurada y preparada la ACI, los administradores tienen que monitorear y determinar lo bien que la estructura está respondiendo a las expectativas, o si la estructura se está comportando bien o no. Bienvenido a los "puntajes de estado", los cuales ofrecen a los administradores una forma elegante de llegar a mediciones muy discretas de problemas puntuales. Como ya se mencionó, dado que todos los dispositivos que pertenecen a la estructura de la ACI son, esencialmente, objetos, la ACI puede medir y asignar un puntaje a la mayoría de ellos porque están dispuestos en un árbol de objetos. Estos puntajes también se pueden "hacer ascender" por el árbol, de modo que se pueda reportar y reunir un puntaje por abonado acumulado o un puntaje para toda la estructura. Es un modelo fractal que proporciona un puntuaje de alto nivel y permite que los administradores lleguen a dispositivos y componentes o funciones en dispositivos como ser un puerto o, incluso, a nivel de protocolos.

Por ejemplo: es posible que toda la estructura de la ACI tenga un puntaje del 99% (lo que es muy bueno) pero luego cambia porque uno de sus componentes se degrada. Podría ser un error en un puerto, un puerto que se desactivó, o una máquina virtual en un host ESX con una medición de consumo de ciclos de CPU muy elevada. Cuando ocurre una falla, esta comienza a activar eventos y estos eventos llevan a una degradación en los puntajes de objetos por separado y eso genera un indicio visual para los administradores. Estos puntajes ascienden por el árbol y, finalmente, el puntaje de toda la estructura comenzará a disminuir a medida que también lo hagan los puntajes de los objetos subyacentes. Las personas que prestan servicios de soporte y ponen en funcionamiento las redes en centros de datos saben que es muy difícil detectar el origen de un problema sin tener un buen contexto. Los puntajes de estado ofrecen contexto y un sistema de calificación en el cual el mejor puntaje es 100.





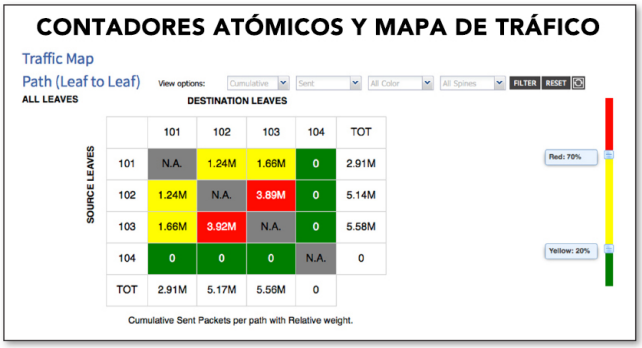
Parte del personal de NetOps podría pensar que tienen la capacidad de crear un sistema similar al de puntaje de estado ejecutando secuencias de comandos para automatizar la recopilación y el procesamiento de estadísticas de red regulares, pero es una tarea muy difícil. Es cierto: se puede ocultar gran parte de la complejidad del sistema de red existente a través de secuencias de comandos, pero imaginemos el trabajo que sería desarrollar secuencias de comandos en cada uno de los aspectos operativos individuales de la red. No solo es difícil porque requiere profundas habilidades de operaciones de desarrollo (DevOps); además, no es escalable en un entorno amplio. Lo que hizo Cisco con la ACI es lo siguiente: incluso antes de crear el hardware y el software en el sistema, desarrolló el modelo de datos orientados a objetos para que la ACI admitiera estas funciones. Este modelo no solo admite el aprovisionamiento y la eliminación cuando los administradores crean y eliminan objetos, sino que además ofrece información de manera continua sobre los atributos de objetos individuales, lo que permite que los administradores monitoreen el estado de los objetos. Es más escalable y debería añadir un valor importantísimo, especialmente en cuanto a la reducción de los gastos operativos, además de acelerar el tiempo de resolución cuando ocurre un problema.

Visibilidad y resolución de problemas: contadores atómicos

Otra característica operativa importante es lo Cisco llama "contadores atómicos": una herramienta analítica y para la resolución de problemas. Los contadores atómicos se exponen de varias maneras pero, esencialmente, Cisco ha incluido contadores atómicos como una funcionalidad específica en su hardware para evitar que se produzca una penalidad de rendimiento al activarse. Cisco también ha prometido que los contadores atómicos se extenderían al switch de software de Cisco (el switch virtual de aplicaciones, AVS) y que también podría incluirse en otros switches de software abierto. Entonces, ¿qué hacen los contadores atómicos? En esencia, su función es muy simple, pero extremadamente valiosa. Los contadores atómicos cuentan cada paquete que ingresa y sale de la estructura pero también proporcionan contextualización en el conteo de paquetes.

Tradicionalmente, siempre ha sido muy difícil poder ver el movimiento de los flujos de tráfico en el interior de una red. La estructura de la ACI procura cambiar eso con contadores atómicos que rastrean los flujos a medida que ingresan y egresan de la estructura, tanto alrededor como en el interior de los agrupamientos de políticas ya mencionados. Los paquetes que ingresan a la estructura de la ACI son etiquetados en el primer punto de ingreso a la estructura; estas etiquetas se retiran en el egreso. Estos paquetes etiquetados son el origen del rastreo y conteo de flujo de los contadores atómicos. Con los contadores atómicos, los administradores sabrán muy rápidamente si la estructura ha rechazado paquetes correspondientes a un par determinado de ramas ingreso/egreso (lo que Cisco llama "ruta"), o incluso entre un par determinado de nodos secundarios de ingreso/egreso (lo que Cisco llama "ruta"), o incluso entre un par determinado de puertos de uplink de ingreso/egreso (lo que Cisco llama "pista"). Esta información ofrece a los administradores una manera de realizar un seguimiento de la información de paquetes/flujo de extremo a extremo en el interior de la estructura y de dimensionar esos flujos entre orígenes y destinos.

Cisco ha creado un gráfico ordenado para mostrar la recopilación de datos de los contadores atómicos en la forma de un mapa de calor o tráfico para mostrar los porcentajes de utilización generales de los flujos entre diferentes rutas y trazas. Los diferentes grados de utilización están codificados con colores para proporcionar áreas con niveles de utilización alto, mediano y bajo. Esta información es útil para saber si hay caída de paquetes en la estructura y como herramienta de planificación para saber dónde ubicar más carga de trabajo en la estructura.



Uno de los desafíos más grandes al momento de diagnosticar problemas de red se da cuando NetOps tiene que correlacionar información proveniente de varios dispositivos y sistemas de administración diferentes. Es muy común que el personal de NetOps tenga que interactuar con diferentes dispositivos, para lo que ejecutará una serie de comandos de la CLI como "show ip arp," "show mac-address"…, y luego deba tratar de graficar toda esta información, usualmente en una hoja de papel para comprender la ruta de red. La capacidad de desglose de los contadores atómico permite que el personal de operaciones omita este proceso tedioso y prolongado en el tiempo y vaya directamente al origen del problema. Los contadores atómicos se pueden usar en estas situaciones para ayudar en la resolución integral de problemas en sistemas, lo que permite que los administradores filtren clientes, grupos EPG, terminales, etc. específicos en los que estén interesados y cuenten solamente los paquetes que coincidan con los criterios especificados.

Conexión de aplicaciones a servicios de red

A los administradores de infraestructuras les interesa mucho cómo conectar perfiles de red de aplicaciones (ANP) a servicios de red en los que se puedan iniciar instancias de servicios de red de capas 4 a 7 como dispositivos físicos, factores de forma virtualizados como un dispositivo físico, como factores de forma virtualizados o como una combinación de ambos. ACI ofrece varias maneras de abordar este problema de diseño y, a la vez, minimizar la cantidad de puntos de administración a uno. Para conectar un servicio de red L4-7 a un ANP, el administrador no tiene que interactuar con diferentes interfaces de dispositivos o sistemas de administración. Para conectar un servicio de red de

capas 4 a 7 se modelan como parte de la estructura de la ACI, Cisco básicamente diseñó la arquitectura de esos servicios dentro del mismo modelo de políticas basadas en grupos ya analizado. Como enorme beneficio adicional al modelo de estructura de la ACI de conectar servicios L4-7 a perfiles ANP podemos mencionar que los servicios L4-7 pueden ser independientes de la ubicación; es decir, estos servicios se pueden conectar en cualquier lugar de la estructura de modo que, cuando el administrador conecte la función de servicio al ANP, la estructura determina automáticamente dónde están ubicados y aprovisiona todas las encapsulaciones que correspondan a esos nodos de servicio para automatizar el reenvío de las rutas de datos.

Cisco modela estas funciones de servicio L4-7 como un gráfico de servicio, que puede contener una o más funciones de servicio (firewall, equilibrador de cargas, etc.). Estos gráficos de servicio se pueden incorporar a la definición del ANP para reflejar la conducta deseada del ANP.

CREACIÓN DE UN GRÁFICO DE SERVICIOS L4-7

Por ejemplo: si asocia gráficos de servicio L4-7 al ANP, el administrador o el auditor de seguridad puede comprender, en un nivel elevado, que todo el tráfico que coincide en HTTP/S destinado al EPG web en la estructura de la ACI primero debe pasar por un Gráfico de servicio de Firewall en particular. O que antes de que un flujo ingrese al EPG de base de datos back-end, debe pasar por un Gráfico de servicio de equilibrio de cargas. El enfoque de la ACI de Cisco con respecto a la conexión de perfiles ANP a servicios de red mitiga uno de los aspectos que más tiempo consumen en la cadena de prestación de servicios de TI, donde se necesitan minutos para preparar una máquina virtual pero semanas o meses para configurar la red y los servicios de red L4-7. Al momento de la redacción de este documento, la ACI de Cisco proporciona integración con firewalls Cisco ASA y ASAv, además de equilibradores de cargas para Citrix y F5. Se pueden conseguir paquetes de dispositivos para cada uno de estos nodos de servicio en los sitios de los proveedores respectivos.

Cisco ha asumido el compromiso de trabajar con más de doce proveedores de servicios L4-7 para la entrega de paquetes de dispositivos adicionales. Para conocer la lista más reciente de partners del ecosistema para ACI, consulte la página de Cisco ACI: http://www.cisco.com/go/aci

Encadenamiento y replicación de servicios

Se pueden emplear dos enfoques básicos para integrar servicios L4-7: utilizar servicios de red físicos y dividirlos lógicamente en varios contextos para cada cliente, o dedicar servicios virtuales individuales por abonado.

ACI puede admitir ambos enfoques ya que la mayoría de las organizaciones de TI y de los proveedores de servicios en la nube los necesitan. Por ejemplo: en la mayoría de las empresas, antes de que el tráfico ingrese a la definición de aplicaciones de la empresa, debe pasar por un firewall perimetral. Habitualmente, esta función de firewall está muy bien controlada y cuenta con un alto grado de seguridad, prácticamente como un espacio de aire en naves espaciales o submarinos. Pero en los últimos años se ha determinado que no es necesario un espacio de aire físico real, aunque gran parte de las operaciones de seguridad (SecOps) quieren un dispositivo físico que actúe como punto de control de políticas. Ante este escenario, la ACI puede integrar plataformas de firewall Cisco y de otros proveedores, ya que deben ser capaces de conectarse a la estructura de la ACI. Las organizaciones que tienen controles de seguridad más estrictos prefieren este modelo de arquitectura porque no confían mucho en que los firewalls virtualizados puedan protegerlas de amenazas en la DMZ. Se sienten más cómodos utilizando sus firewalls Cisco ASA, Check Point, Juniper SRX o Palo Alto Networks existentes. APIC permite que estas organizaciones de TI utilicen su inversión existente en firewalls físicos porque los conecta directamente a la estructura de la ACI, con lo que se incorpora su funcionalidad y aprovisiona políticas a través del APIC.

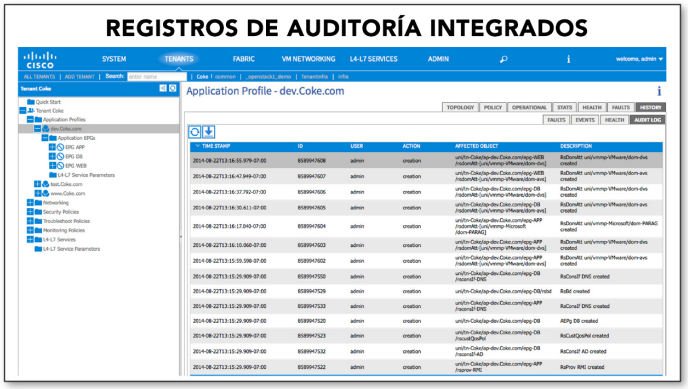
El interés por bloquear o segmentar la comunicación entre diferentes niveles de aplicaciones crece día a día; es por esto que el modelo de políticas de la ACI resulta útil desde una perspectiva de escala y de rendimiento. Como las políticas se definen a través del ANP, esas políticas se expresan en toda la infraestructura y se hacen cumplir en el primer punto de ingreso a la estructura de la ACI, lo que proporciona funcionalidad de firewall distribuida en todos los ANP.

En el interior de la ACI se admiten servicios virtuales individuales exclusivos por abonado de una forma muy similar a los dispositivos de factor de forma físico. Los proveedores de servicios en la nube pretenden seriamente configurar y dedicar una instancia de un firewall, un equilibrador de cargas virtual, etc., para cada abonado que se aloje, para poder controlar y administrar esa instancia individualmente por abonado. Muchas organizaciones de TI aplican el concepto de cliente a las unidades de negocios individuales, por ejemplo. Sin embargo, con servicios de red virtuales, se requiere un paso adicional para implementar el firewall o equilibrador de cargas virtual, que proporcionará un control apropiado de versiones e instalará las licencias correctas. Comúnmente, esto se conoce como administración del ciclo de vida de servicios virtuales. Cisco está asociado con Embrane para incorporar esta funcionalidad en su oferta de ACI.

Un enorme avance para auditores de sistemas de TI

Uno de los principales beneficios de la definición explícita de los EPG y los “contratos” es que ofrecen, tanto a administradores como a auditores de TI, la capacidad para auditar fácilmente qué política se ha probado en comparación con el objetivo inicial del propietario de la aplicación. No es ningún secreto que la documentación de políticas de sistemas es, en el mejor de los casos, escasa en la mayoría de las organizaciones y que, cuando existe, mantener la exactitud de esos documentos y actualizarlos se convierte en un enorme gasto administrativo para los administradores de TI. Adicionalmente, el propietario de las aplicaciones o de la plataforma original puede haberse desplazado a diferentes roles o alejado de la compañía por completo, lo que deja un significativo vacío de información. Quienes han tenido que rederivar el objetivo original del propietario de la aplicación/plataforma (recuperar y revisar configuraciones de switches, routers o equilibradores de cargas) saben que es un proceso costoso, abrumador y que lleva mucho tiempo.

Se trata de un área de enorme magnitud en la que la ACI desempeña un rol importante. Como las políticas de la ACI se expresan en términos abstraídos en un nivel más elevado, los auditores de TI pueden comprender rápidamente el objetivo del propietario de la aplicación con tan solo mirar el ANP. El auditor no necesita rastrear/correlacionar archivos de configuración de redes y servicios detallados para comprender las políticas de aplicaciones de mayor jerarquía. Adicionalmente, Cisco ha implementado un registro de auditoría muy detallado para objetos que se modifican. Este registro indica la fecha y la hora, el usuario, el objeto y una descripción de lo que se modificó para permitir una capacidad total de seguimiento.



Tunelización e interoperabilidad con varios hipervisores

Fundamentalmente, ACI proporciona conectividad, pero el medio para conectar dispositivos está cambiando porque las aplicaciones abarcan entornos tanto físicos como virtuales. Aunque se ha registrado un aumento constante en la migración de cargas de trabajo físicas a virtuales, sigue existiendo el requisito inevitable de que las cargas de trabajo virtuales deben comunicarse con cargas de trabajo alojadas en hardware físico. Es más, en el último año, se ha notado un enorme aumento en el interés de investigar cargas de trabajo basadas en contenedores para optimizar aún más el desempeño y reducir los gastos generales de procesamiento. La red siempre ha sido un punto de normalización subyacente para activos de TI y modelos de cómputo porque todas las cargas de trabajo la utilizan con fines de conectividad. ACI procura convertirse en la nueva base en la normalización de estas diferentes cargas de trabajo, tanto en términos de conectividad como en términos de política.

Actualmente, el espacio que más necesita la normalización es en el ámbito de las redes virtualizadas, donde diferentes ofertas de hipervisores proporcionan distintos métodos para administrar redes virtuales con compatibilidad para diversas encapsulaciones en el plano de datos (VLAN, VXLAN, NVGRE, etc.). Cada día hay más cantidad de entornos en los que se desea implementar entornos con varios hipervisores y, con esta tendencia, las compañías deben buscar un modo integral de administrar estos entornos dispares y, a la vez, sus respectivas encapsulaciones subyacentes.

Cisco ACI proporciona integración directa con la versión de Icehouse para vCenter y OpenStack de VMware, ejecutando Ubuntu KVM con su versión GA de software. Cisco ha asumido el compromiso de admitir SCVMM de Microsoft, Microsoft AzurePack y Red Hat KVM con OpenStack en el futuro cercano. Como integra múltiples hipervisores con la ACI, el APIC se convierte en el punto central de administración para políticas de red tanto físicas como virtuales, y la estructura de la ACI pasa a ser un punto de normalización con encapsulación distribuida para varios tipos de encapsulación (VLAN, VXLAN, NVGRE), lo que proporciona a los administradores la flexibilidad necesaria para finalizar, interpretar y reasignar diferentes encapsulaciones en y entre sí. Estas encapsulaciones también son coordinadas por el APIC para que el administrador de la red o de las máquinas virtuales no tenga que coordinar la vinculación de etiquetas. Cuando los paquetes ingresan a la estructura de la ACI, se retiran estas etiquetas de encapsulación únicas y se las vuelve a conectar al momento del egreso o son traducidas al esquema de encapsulación del hipervisor de destino para proporcionar conectividad con múltiples hipervisores.

La integración con estos administradores de máquinas virtuales (VMM) permite que el administrador trate cargas de trabajo físicas y virtuales exactamente del mismo modo; para ello, utiliza el modelo de políticas de la ACI. Cuando los administradores crean niveles de aplicación, zonas de seguridad o cualquier elemento que se vincule con un EPG, estos grupos esencialmente son reenviados a los dispositivos físicos y virtuales subyacentes. En vCenter de VMWare, el APIC reenvía grupos EPG como grupos de puertos VMWare. En SCVMM de Microsoft, el APIC reenvía grupos EPG como redes de máquinas virtuales y, con OpenStack, el APIC reenvía grupos EPG como redes simples.

A modo de ejemplo consideraremos un hipervisor VMWare ESX en el que se está usando VXLAN: etiqueta todos los paquetes por medio de VXLAN pero necesita comunicarse con otros dos hipervisores ESX que emplean encapsulación VLAN. La estructura de la ACI ejecuta la traducción a VLAN o la conexión y el rouuting VXLAN a VLAN, para que estos paquetes puedan ir más allá de los límites de las distintas subredes. En pocas palabras, la ACI proporciona funciones completas de finalización, normalización y routing VLAN y VXLAN al nivel de desempeño del hardware.

Enfoque de host o red para la normalización de esquemas de tunelización virtuales

ACI proporciona un enfoque diferente desde la arquitectura que los sistemas de red en los que se emplean hipervisores exclusivamente. En el enfoque en el que solo se utilizan hipervisores, las funciones de red se implementan en el hipervisor. Esto comienza con los mecanismos de etiquetado y cumplimiento de políticas en el hipervisor, lo que proporciona información de total sobre la red virtual al nivel del hipervisor. En este modelo, cada host al que se tuneliza (es decir, los terminales del túnel) debe ser de la misma pila vertical, por ejemplo: VMWare, Microsoft o cualquier otro esquema de tunelización virtual que se esté usando. Los esquemas de tunelización virtual deben coordinarse con los demás hosts de hipervisores presentes en el dominio de conectividad. Esto quiere decir que, esencialmente, las cargas de trabajo deben ser virtualizadas y acopladas también con el mismo hipervisor. Entre los sistemas de administración de hipervisores que permiten una combinación y emparejamiento de encapsulaciones y políticas, el nivel de interoperabilidad es escaso o nulo. Es más, para conectarse a servidores exclusivos instalados directamente en el hardware (no virtualizados), por ejemplo, un switch físico de la red debe interpretar los mismos esquemas de tunelización virtual, además de requerir una profunda integración con los sistemas de administración del hipervisor p para que se puedan organizar/coordinar sus encapsulaciones y políticas.

Otro desafío para las implementaciones de producción es que, ahora, los administradores de centros de datos deben probar y validar no solo la estructura subyacente física (el “underlay”), sino que, luego, deben utilizar otro conjunto de herramientas para validar las redes virtuales (el “overlay” o superposición) con lo que, esencialmente, se duplica el tiempo de certificación necesario para que toda la infraestructura de la red llegue a un estado de implementación lista para la producción.

En lugar de dirigir la coordinación al nivel del host, ACI utiliza la red para coordinar esquemas de tunelización virtual, con lo que se proporciona normalización en cada nodo secundario. Como los nodos de la red son el punto de normalización en la ACI, se proporciona conectividad total y políticas para todos los dispositivos, ya sean físicos, virtuales o contenedores que se conectan a la red. Para llevar la estructura de lal ACI a un estado de implementación lista para la producción, lo único que tiene que hacer el administrador del centro de datos es probar y validar la estructura de la ACI, porque combina tanto el underlay como el overlay en el mismo plano. Con esto se ahorra mucho tiempo en la certificación integral de la solución.

En consecuencia, las opciones que se presentan hoy antes los arquitectos son: 1) utilizar la red como punto de normalización para conectividad y políticas, y certificar la red física y la virtual en conjunto, 2) virtualizar todo y dictaminar que cada host ejecute exactamente el mismo hipervisor en todo el centro de datos y duplicar el tiempo de certificación y/o 3) ejecutar varias redes de superposicióque no interoperen entre hipervisores y/o servidores de hardware, para añadir los ciclos de certificación que correspondan.

En el modelo ACI, las aplicaciones pueden ser Microsoft Hyper-V, VMWare ESX y Ubuntu/RedHat KVM, además de servidores físicos. En este modelo, parte de la aplicación web se puede alojar en una VXLAN en la que se esté ejecutando ESX, la aplicación se puede alojar en Hyper-V con sus bases de datos en KVM y servidores físicos con conectividad y políticas aplicadas a todo el conjunto a través de un único punto de administración. Si se desea tener alternativas y flexibilidad reales en la infraestructura del centro de datos, ACI es una excelente oferta.

Conclusión

Cisco notó los problemas que sufrían los ejecutivos de TI con el manejo de la infraestructura de los centros de datos modernos y desarrolló un enfoque con el que se pretender reducir el costo operativo, agilizar la prestación de servicios de TI, abarcar activos de TI tanto físicos como virtuales y, además, proporcionar compatibilidad e interoperabilidad con múltiples hipervisores. Cisco mantuvo el principio de diseño por excelencia de los sistemas de red: admitir todas las aplicaciones y cargas de trabajo y estar preparada para ser una infraestructura de uso general que se pueda personalizar en torno a la conectividad por medio de una política, de la automatización y de la programabilidad. Este nuevo enfoque es la Infraestructura centrada en aplicaciones (ACI) y, con ella, Cisco ha desarrollado algunas de las ideas nuevas más profundas que se han visto en la industria de redes en casi 25 años. Aunque pueda llevar cierto tiempo para que la industria adopte la ACI por completo, gran parte de nosotros cree que Cisco está ofreciendo un nuevo modelo de sistemas de red que plantea valiosas innovaciones tecnológicas y es mucho más fácil de controlar y administrar que las redes orientadas a dispositivos de la actualidad. El resultado debería ser una reducción en los gastos operativos a corto plazo y, a largo plazo, una arquitectura para infraestructuras de centros de datos de próxima generación que será la base que impulsará el avance de las economías mundiales durante otros 25 años.

Acerca de Nick Lippis

Nicholas J. Lippis III es una autoridad reconocida mundialmente en redes IP avanzadas, comunicaciones y sus beneficios para los objetivos empresariales. Él publica *el Informe Lippis*, un recurso para los responsables de la toma de decisiones comerciales sobre redes y TI al que están suscriptos más de 35 000 líderes empresariales de TI. El podcast del Informe Lippis se ha descargado más de 200 000 veces; iTunes informa que el público también descargó Money Matters del *Wall Street Journal*, Climbing the Ladder de *Business Week*, IdeaCast de *The Economist* y *The Harvard Business Review*. También es co-fundador y conferencista principal de Open Networking User Group, que patrocina una reunión semestral de más de 200 líderes empresariales de TI de empresas importantes. El Sr. Lippis actualmente trabaja con clientes para diseñar sus arquitecturas de red de computación en la nube privada y pública de centros de datos virtualizados con tecnologías de red abierta, con el fin de obtener valor y resultados máximos empresariales.

Ha asesorado a muchas empresas de Global 2000 sobre arquitectura de red, diseño, implementación, selección y asignación de presupuestos de proveedores y entre sus clientes se incluyen: Barclays Bank, Eastman Kodak Company, Federal Deposit Insurance Corporation (FDIC), Hughes Aerospace, Liberty Mutual, Schering-Plough, Camp Dresser McKee, el estado de Alaska, Microsoft, Kaiser Permanente, Sprint, Worldcom, Cigitel, Cisco Systems, Hewlett Packet, IBM, Avaya y muchos otros. Trabaja de manera exclusiva con directores de informática y sus subalternos directos. El Sr. Lippis posee una perspectiva única de las fuerzas y las tendencias de mercado que ocurren dentro de la industria de redes de computación que deriva de su experiencia con clientes proveedores y consumidores.

El Sr. Lippis recibió el prestigioso premio de Ex-alumnos de la Facultad de Ingeniería de la Universidad de Boston por sus logros en la profesión. Fue nombrado una de las 40 personas más poderosas e influyentes en la industria de redes por *Network World. Tech Target,* una publicación en línea de la industria, lo nombró gurú del diseño de redes y la *revista Network Computing* lo llamó gurú estrella de TI.

El Sr. Lippis fundó Strategic Networks Consulting, Inc., una empresa de consultoría de redes de computadoras muy respetada e influyente que compró Softbank/Ziff-Davis en 1996. Es ponente principal frecuente en eventos de la industria y mencionado ampliamente por la prensa empresarial y de la industria. Trabaja como Decano de la Junta de asesores de la Facultad de Ingeniería de la Universidad de Boston así como en muchas juntas asesoras de firmas que se están iniciando. Pronunció el discurso de iniciación para los graduados de la Facultad de Ingeniería de la Universidad de Boston en 2007. El Sr. Lippis recibió su Licenciatura en Ingeniería Eléctrica y Maestría en Ingeniería en Sistemas de la Universidad de Boston. La tesis para su maestría incluyó cursos técnicos seleccionados y asesores del Instituto de Tecnología de Massachusetts sobre comunicaciones y computación óptica.