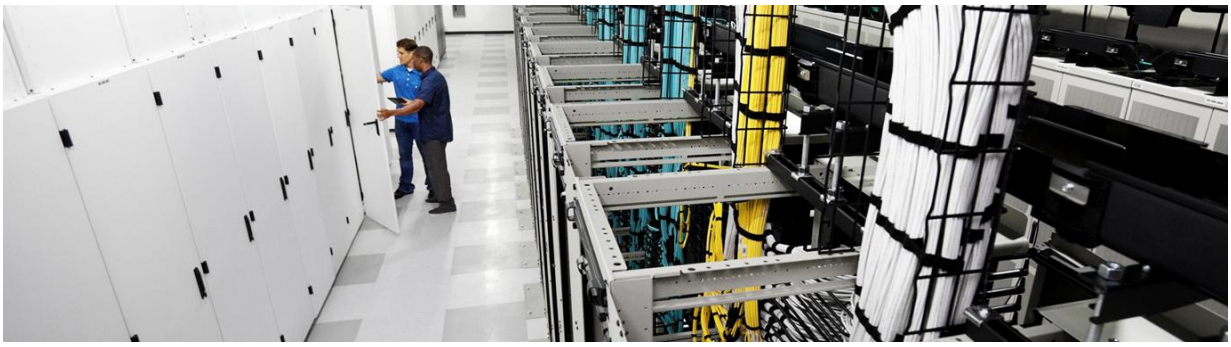
Informe técnico

Principios de la infraestructura centrada en aplicaciones



Descripción general

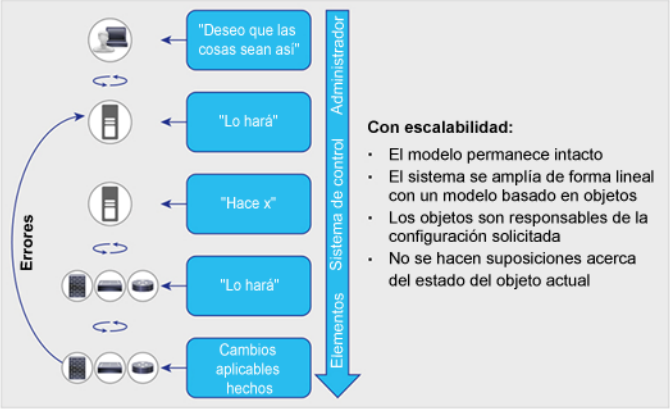
Una de las principales innovaciones de la infraestructura centrada en aplicaciones (ACI, por sus siglas en inglés) es la introducción de una interfaz muy abstraída para indicar la conectividad de los componentes de las aplicaciones junto con las políticas de alto nivel que rigen dicha conectividad. El modelo se ha diseñado con el fin de que a los desarrolladores de las aplicaciones les resulte sencillo de usar al mismo tiempo que mejora la automatización y la seguridad.

Teoría de la política de ACI

El modelo de la política de ACI es un modelo orientado a los objetos que se basa en la teoría de la promesa. La teoría de la promesa se basa en el control escalable de los objetos inteligentes en lugar de los modelos imperativos más tradicionales, que puede considerarse como un sistema de gestión de tipo "top-down" (es decir, de la TI al negocio). En este sistema, el administrador central debe ser consciente de los comandos de configuración de los objetos subyacentes y del estado actual de dichos objetos.

La teoría de la promesa, por el contrario, se basa en los objetos subyacentes para controlar los cambios de los estados de la configuración que inicia el sistema de control en sí como “cambios de estado deseados”. Así, los objetos son los responsables de transmitir las excepciones o los fallos de vuelta al sistema de control. Este planteamiento reduce la carga y la complejidad del sistema de control y permite una mayor escalabilidad. Este sistema es más escalable al permitir que los métodos de objetos subyacentes soliciten cambios de estado entre ellos y de objetos de niveles inferiores (figura 1).

Figura 1. Enfoque de la teoría de la promesa para un control del sistema a gran escala



En el marco de este modelo teórico, ACI crea un modelo de objetos para la implementación de aplicaciones, con estas como foco central. Tradicionalmente, las aplicaciones se han visto limitadas por las capacidades de la red y por los requisitos para evitar el mal uso de las construcciones para implementar la política. Se han unido conceptos como direccionamiento, VLAN y seguridad, lo que limita las capacidades de escalabilidad y movilidad de las aplicaciones. A medida que las aplicaciones se están volviendo a diseñar para favorecer la movilidad y su uso a través de la Web, este enfoque tradicional dificulta una implementación rápida y uniforme.

El modelo de políticas de ACI no impone nada acerca de la estructura de la red subyacente. Sin embargo, según dicta la teoría de la promesa, se requiere un elemento periférico, llamado iLeaf, para gestionar las conexiones con distintos dispositivos.

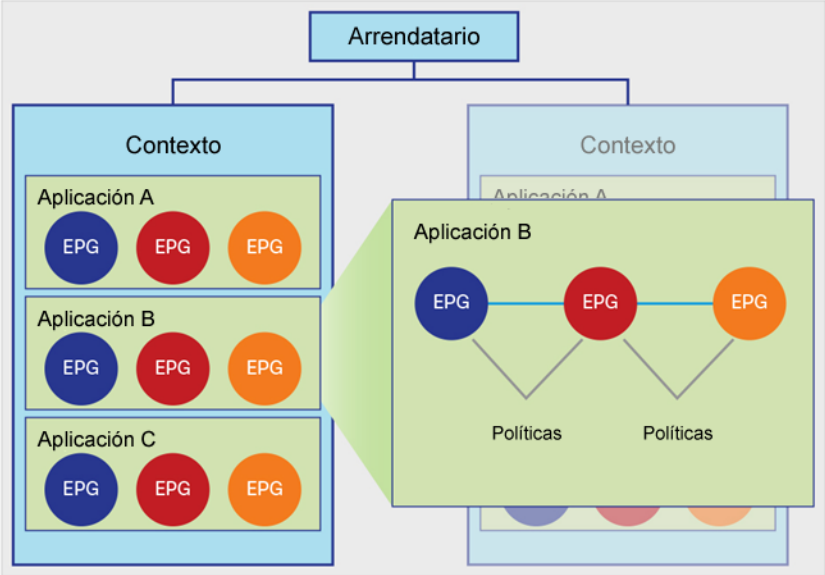
Modelo de objetos

En el nivel superior, el modelo de objetos de ACI se ha creado a partir de un grupo de uno o varios arrendatarios, lo que permite una gestión por separado de la infraestructura de red y de los flujos de datos. Los arrendatarios se pueden usar para los clientes, las unidades empresariales o grupos, en función de las necesidades de la organización. Por ejemplo, una empresa puede usar un arrendatario para toda la organización y un proveedor de nube puede tener clientes que usen uno o varios arrendatarios para representar a sus organizaciones.

Los arrendatarios se pueden dividir aún más en contextos, algo relacionado directamente con el reenvío y routing virtuales (VRF) o los espacios de IP independientes. Cada arrendatario puede tener uno o varios contextos según las necesidades de su negocio. Los contextos proporcionan una forma de separar aún más los requisitos de la organización y del reenvío para un arrendatario determinado. Debido a que los contextos usan instancias de reenvío distintas, el direccionamiento IP se puede duplicar en contextos independientes para casos de varios arrendatarios.

Dentro del contexto, el modelo proporciona una serie de objetos que definen la aplicación. Estos objetos son terminales (EP) y grupos de terminales (EPG), y las políticas que definen su relación (figura 2). Tenga en cuenta que las políticas en este caso son más que un simple conjunto de listas de control de acceso (ACL) e incluyen una recopilación de: filtros de entrada y de salida, configuración de calidad del tráfico, reglas de marcas y reglas de redirección.

Figura 2. Modelo de objetos lógicos



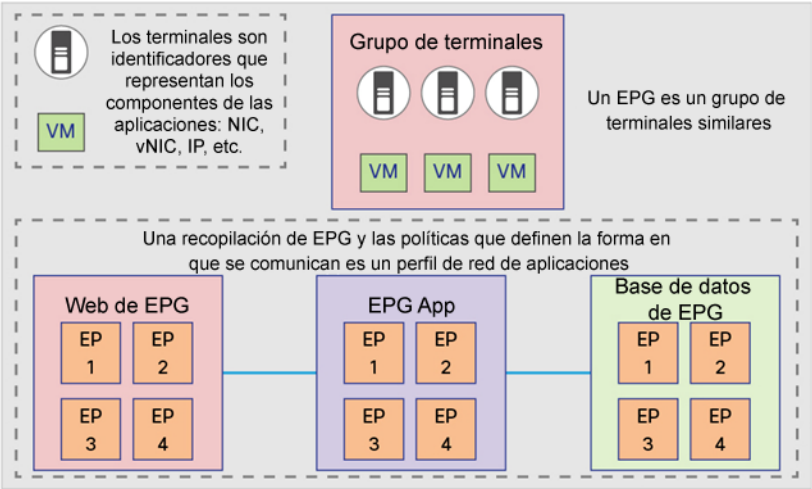
En la figura 2 se muestra un arrendatario con dos contextos y las aplicaciones que crean dichos contextos. Los EPG que se muestran son grupos de terminales que crean un nivel de la aplicación u otro grupo de aplicaciones lógico. Por ejemplo, la aplicación B que se muestra ampliada en el lado derecho de la figura, puede estar compuesta por un nivel web (azul), un nivel de aplicación (rojo) y un nivel de base de datos (naranja). La combinación de los EPG y las políticas que definen su interacción es un perfil de red de aplicación en el modelo de ACI.

Grupos de terminales

Los EPG son una recopilación de terminales similares que representan un nivel o un conjunto de servicios de una aplicación. Proporcionan una agrupación lógica de los objetos que requieren una política similar. Por ejemplo, un EPG podría ser un grupo de componentes que crean el nivel web de una aplicación. Los terminales se definen usando la tarjeta de interfaz de red (NIC), la NIC virtual (vNIC), la dirección IP o el nombre del sistema de nombres de dominio (DNS), con capacidad para admitir futuros métodos de identificación de componentes de la aplicación.

Los EPG también se usan para representar a las entidades como redes externas, servicios de red y almacenamiento de red. Los EPG son recopilaciones de uno o varios terminales que proporcionan una función similar. Son agrupaciones lógicas con diversas opciones de uso, según el modelo de implementación de la aplicación en uso (figura 3).

Figura 3. Relaciones de grupos de terminales



Los EPG se han diseñado para favorecer la flexibilidad, lo que permite que su uso se adapte a uno o varios modelos de implementación que el cliente pueda elegir. Los EPG se usan para definir los elementos a los que se aplica la política. Dentro del fabric de red, la política se aplica entre los EPG, lo que define la forma en que los EPG se comunican entre sí. Este enfoque se ha diseñado para ser ampliable en el futuro a la aplicación de políticas dentro de los EPG.

A continuación se presentan algunos ejemplos de uso de EPG:

- EPG definido por VLAN de red tradicionales: todos los terminales conectados a una VLAN determinada ubicada en un EPG
- EPG definido por una LAN virtual ampliable (VXLAN): igual que las VLAN, excepto en que usan VXLAN
- EPG asignado a un grupo de puertos de VMware
- EPG definido por la IP o subred: por ejemplo, 172.168.10.10 o 172.168.10
- EPG definido por nombre de DNS o rangos de DNS: por ejemplo, ejemplo.foo.com o *.web.foo.com

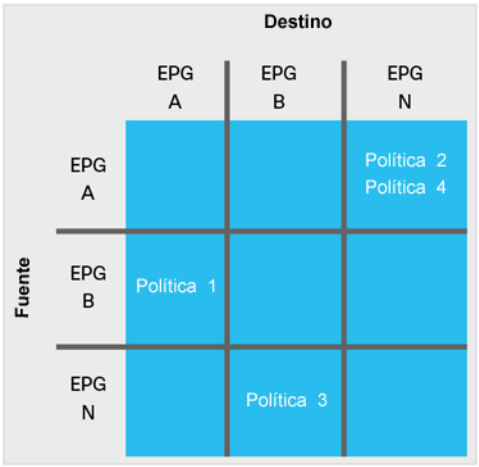
El uso de EPG es tanto flexible como ampliable. El modelo está pensado para proporcionar herramientas que permitan construir un modelo de red de aplicaciones que se asigne al modelo de implementación del entorno real. La definición de los terminales también es ampliable, lo que aporta más compatibilidad con futuras mejoras de los productos y requisitos del sector.

El modelo de EPG ofrece diversas ventajas de gestión. Ofrece un solo objeto con una política uniforme, lo que propicia una automatización de nivel superior y herramientas de orquestación. Las herramientas no deben funcionar en terminales individuales para modificar las políticas. Además, ayuda a garantizar la uniformidad entre los distintos terminales en el mismo grupo independientemente de su ubicación en la red.

Aplicación de políticas

La relación entre los EPG y las políticas se puede considerar una matriz con un eje que representa el EPG de origen (sEPG) y el otro que representa el EPG de destino (dEPG). Una o varias políticas se ubicarán en la intersección de los sEPG y dEPG adecuados. La matriz se rellenará de forma dispersa en la mayoría de los casos porque muchos EPG no tienen necesidad de comunicarse entre sí (figura 4).

Figura 4. Matriz de aplicación de políticas



Las políticas se dividen mediante filtros para la calidad del servicio (QoS), el control de acceso, la inserción de servicios, etc. Los filtros son reglas específicas para la política entre dos EPG. Los filtros se componen de reglas de entrada y de salida: permiso, denegación, redirección, registro, copia y marcas. Las políticas permiten funciones comodín en las definiciones (figura 5). La aplicación de políticas normalmente usa un planteamiento en el que se prima la coincidencia más específica.

Figura 5. Reglas de aplicación de comodines

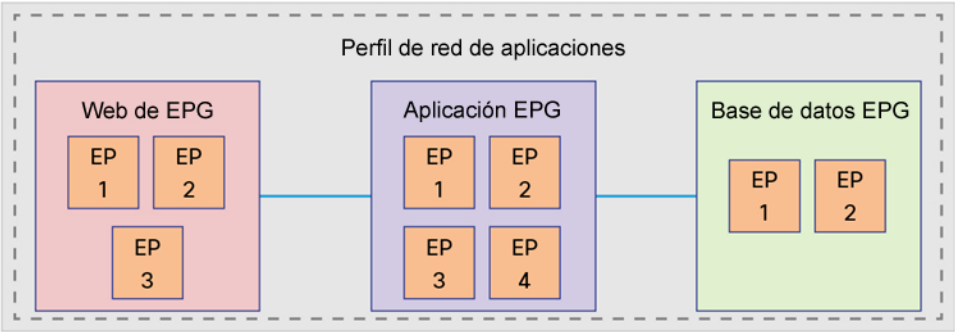
sEPG	dEPG	Aplicación	Comentarios
Completo	Completo	Completo	Reglas completas (S, D, A)
Completo	Completo	*	Reglas (S, D, *)
Completo	*	Completo	Reglas (S, *, A)
*	Completo	Completo	Reglas (*, D, A)
Completo	*	*	Reglas (S, *, *)
*	Completo	*	Reglas (*, D, *)
*	*	Completo	Reglas (*, *, A)
*	*	*	Predeterminado (por ejemplo, denegación implícita)

Perfiles de redes de aplicaciones

Un perfil de red de aplicaciones es una recopilación de EPG, sus conexiones y las políticas que definen dichas conexiones. Los perfiles de redes de aplicaciones son la representación lógica de una aplicación y sus interdependencias en el fabric de la red.

Los perfiles de redes de aplicaciones están diseñados para adaptarlos de un modo lógico que coincida con la manera en que se han diseñado e implementado dichas aplicaciones. En lugar de un administrador, es el sistema el que administra la configuración y la aplicación de políticas, así como la conectividad. En la figura 6 se muestra un ejemplo de un perfil de acceso.

Figura 6. Perfiles de redes de aplicaciones



Para crear un perfil de red de aplicación, se deben seguir estos pasos generales:

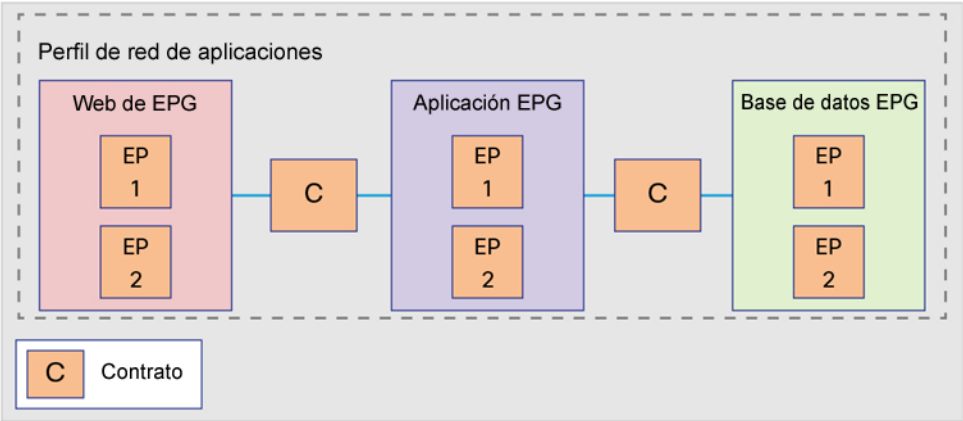
1. Crear los EPG (como se ha descrito anteriormente).
2. Crear políticas que definan la conectividad con las siguientes reglas:
   - Permitir
   - Denegar
   - Registrar
   - Marcar
   - Redirigir
   - Copiar
3. Crear puntos de conexión entre los EPG mediante construcciones de políticas conocidas como contratos.

Contratos

Los contratos definen los permisos de entrada y de salida, las denegaciones, y las reglas y políticas de QoS como la redirección. Los contratos permiten definiciones simples y complejas de la forma en que un EPG se comunica con otros, en función de los requisitos del entorno. Aunque los contratos se aplican entre los EPG, se conectan a los EPG mediante relaciones proveedor-consumidor. Básicamente, un EPG proporciona un contrato y otros EPG consumen dicho contrato.

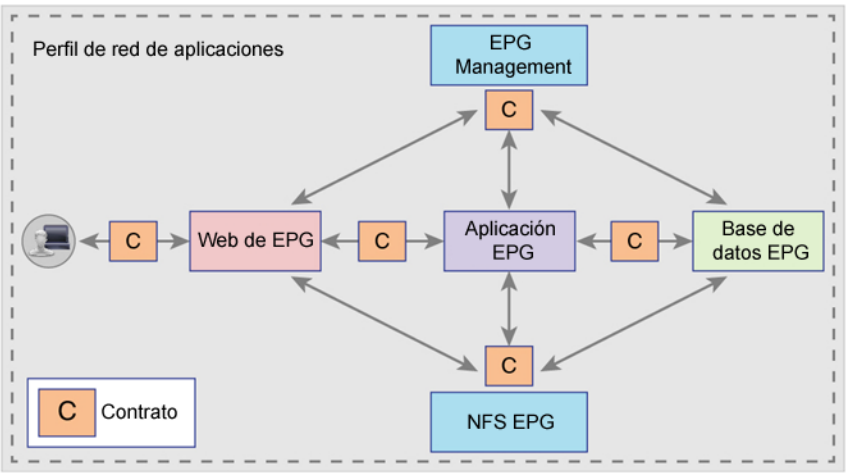
El modelo de proveedor-consumidor es útil para diversos fines. Ofrece una forma natural de añadir una "protección" o "membrana" a un nivel de aplicación que imponga la forma en que dicho nivel interactúe con otras partes de una aplicación. Por ejemplo, un servidor web puede ofrecer HTTP y HTTPS, por lo que el servidor web se puede incluir en un contrato que solo permita estos servicios. Además, el modelo de proveedor-consumidor de contrato fomenta la seguridad al permitir actualizaciones de políticas sencillas y uniformes en un solo objeto de política en lugar de en diversos enlaces que pueda representar un contrato. Los contratos también ofrecen sencillez al permitir que las políticas se definan una vez y se reutilicen muchas veces (figura 7).

Figura 7. Contratos



En la figura 8 se muestra la relación entre los tres niveles de una aplicación web que define la conectividad de EPG y los contratos que definen su comunicación. La suma de esas partes constituye un perfil de red de aplicación. Los contratos también proporcionan capacidad de reutilización y uniformidad de las políticas para los servicios que normalmente se comunican con varios EPG.

Figura 8. Perfil de red de aplicación completo



Conclusión

En este documento se ofrece una introducción al modelo de la política de ACI: se habla de qué es ACI y de cómo se puede usar su modelo de políticas. Este modelo incluye otras construcciones y objetos que, por simplificar, no se han abordado en esta ocasión.

Para obtener más información

Consulte http://www.cisco.com/go/aci.

Sede central en América
Cisco Systems, Inc.
San José. CA

Sede Central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa
Cisco Systems International BV Amsterdam.
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y de fax están disponibles en el sitio web de Cisco: www.cisco.com/go/offices.

Impreso en EE. UU. C11-729906-00 11/13