White Paper

Cisco Application Centric Infrastructure Services Vision

What You Will Learn

A high-performance, low-latency switching infrastructure is just one element of a successful data center. A full solution requires integration of the network with a large ecosystem of devices, including Layer 4 through 7 stateful services appliances such as firewalls, application delivery controllers (ADCs), intrusion protection systems (IPS), deep-packet inspection (DPI) devices, and WAN optimization devices (WODs).

These devices traditionally are physical, but the move to virtual devices, for flexibility, agility, and per-tenant management isolation, is gathering momentum, especially in data centers in which computing and storage resources already are virtualized. This change introduces new challenges and requirements for managing service insertion in the virtualized environment.

Cisco Application Centric Infrastructure Services Vision

Today, the traditional model of services insertion is highly manual, involving complicated VLAN (Layer 2) or Virtual Routing and Forwarding (VRF) instance (Layer 3) stitching between network elements and services appliances, or sometimes services are inserted with protocols and policies such as Web Cache Communication Protocol (WCCP) redirection and policy-based routing (PBR). This traditional model adds complexity to the network. The services are less flexible, and operating errors are more likely. Troubleshooting is also more difficult because of this complexity. In addition, the existing designs can often lead to suboptimal solutions: for example, all traffic from an end device may need to be forwarded through a service appliance configured as a default gateway, regardless of whether the device adds any service value to the traffic.

To provide a solution to these challenges, Cisco® Application Centric Infrastructure (ACI) asks - and answers - these crucial questions:

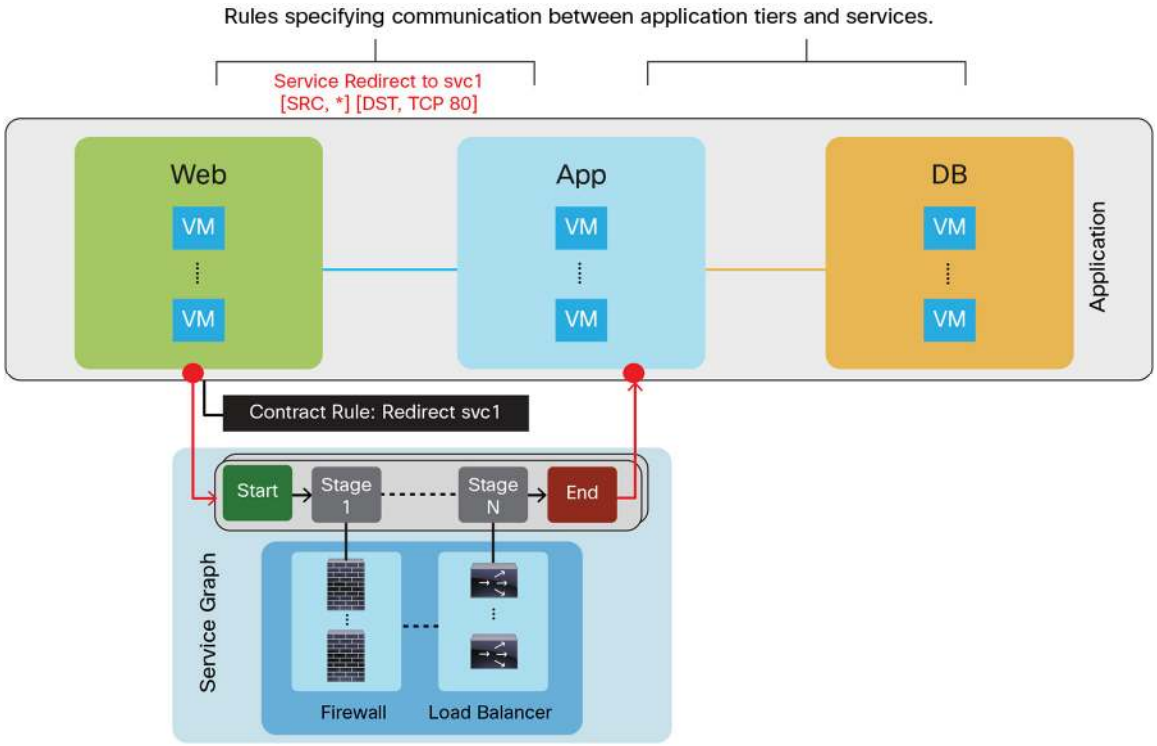
- **What if** service insertion is made easy and automated based on policy?
- **What if** service policies on the appliances could be defined in terms of application components instead of VLANs, IP subnets, and Layer 4 ports?
- **What if** services configuration could be managed along with the network from a central point of automation and control?

- **What if** services were defined in terms of service graphs based on application requirements, not VLANs or subnets, decoupling service insertion from network forwarding?
- **What if** service appliances were grouped into resource pools to scale up or scale down based on demand and could be divided into logical functions?
- **What if** service appliances could redirect to a services resource pool based on the location of the application?
- **What if** service troubleshooting could be made simple and intuitive?

Automated Service Insertion and Policy Management

Although VLAN and VRF stitching are supported for compatibility with traditional service insertion models, Cisco ACI provides revolutionary new features, including implicit automation of service insertion, by using the Cisco Application Policy Infrastructure Controller (APIC) as a central point of automation and policy control. The Cisco APIC can manage both the network fabric and services appliances using policy. This approach is a critical part of the Cisco ACI integrated services architecture, allowing organizations to automate service insertion and eliminate the challenge of managing all the complex traffic-steering techniques of traditional service insertion. It also provides a means for automating the insertion of physical and virtual devices with a consistent look and feel. In addition, it enables automation of services policy using a Representational State Transfer (REST) API with JavaScript Object Notation (JSON) and XML data formats from a central point (Figure 1).

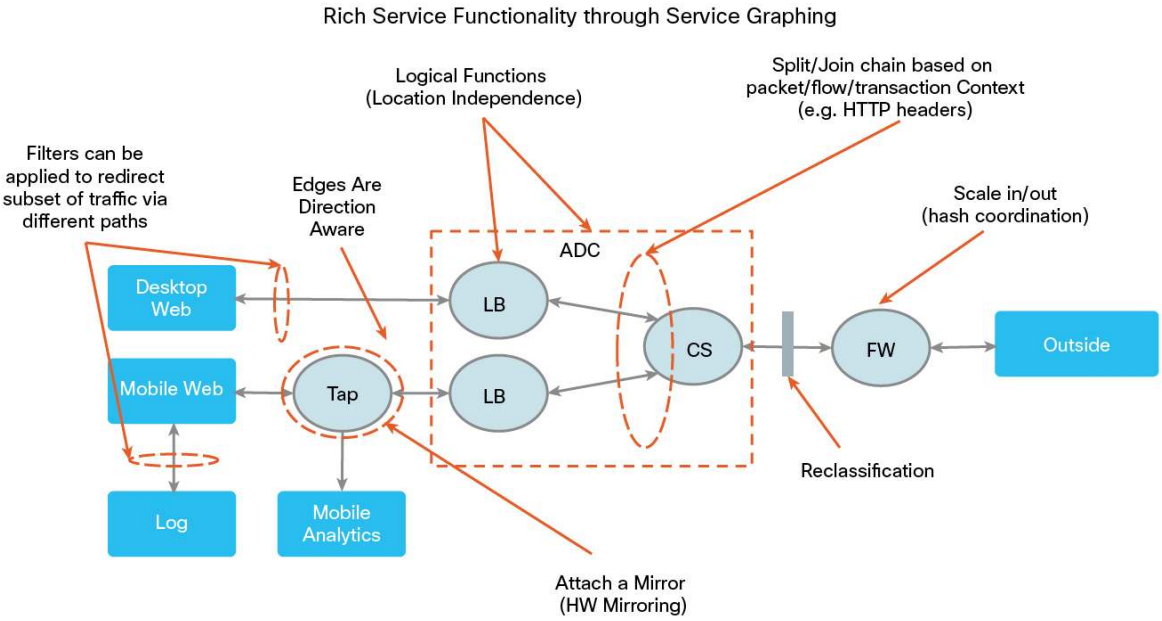
Figure 1. Rules Specifying Communication Between Application Tiers and Services



Cisco ACI Services Architecture: Service Graphs

Cisco ACI treats services as an integral part of an application, and any services required are treated as a service graph that is instantiated on the Cisco ACI fabric from the Cisco APIC. The service graph enables the Cisco APIC to capture the service application intent from the administrator. The service graph abstracts the networking details from the desired service application behavior. The service graph is expressed in the form of logical functions. This approach allows the Cisco APIC to model comprehensive service capabilities and service topologies ranging from very simple to very complicated designs. It is represented as two or more tiers of an application with the appropriate service function inserted between, as shown in Figure 2. In the figure, the blue boxes are endpoint groups (EPGs), and the gray ovals are logical service functions.

Figure 2. Comprehensive Service Capabilities Modeled Through Service Graphing



Some important pieces of information captured by a service graph are listed here:

- Traffic sent or received by an EPG can be filtered based on a policy, and a subset of the traffic can be redirected to different edges in the graph.
- Service graph edges are directional.
- Taps (hardware-based packet copy service) can be attached to different points in the service graph.
- Logical functions can be rendered on the appropriate (physical or virtual) device, based on policy.
- The service graph supports splits and joins of edges, and it does not restrict the administrator to just linear service chains.
- Traffic can be reclassified again in the network after a service appliance emits it.
- Logical service functions can be scaled up or down, or they can be deployed in a cluster mode or 1:1 active-standby high-availability mode, depending on the requirements.

Service Automation Architecture and Services Configuration Management

The Cisco APIC can optionally act as a point of configuration management and automation for service devices and tightly coordinate the service devices with the network automation. The Cisco APIC interfaces with the service device using Python scripts and calls device-specific Python script functions on various events (Figure 3).

The device scripts and a device specification that defines functions supported by the service device are bundled as a device package and installed on the Cisco APIC (Figure 4).

The device script handlers interface with the device using its REST interface (preferred) or command-line interface (CLI) based on the device configuration model.

Figure 3. Service Automation Architecture

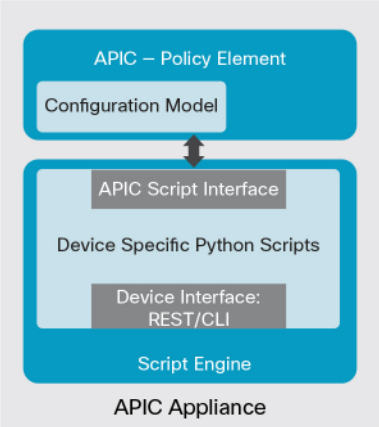
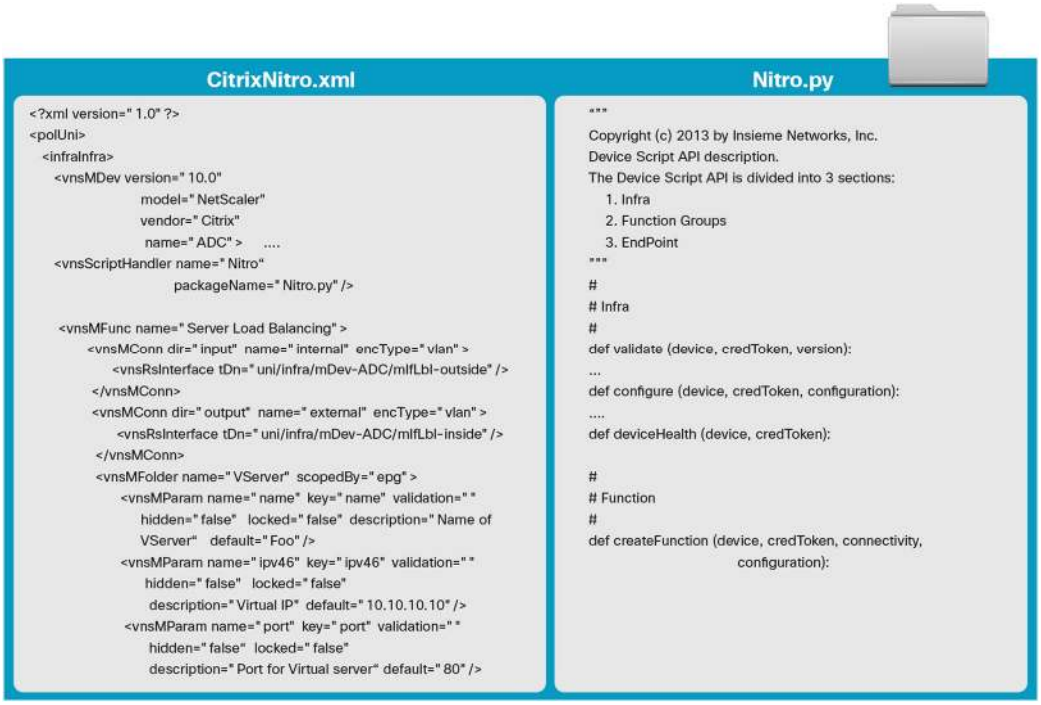


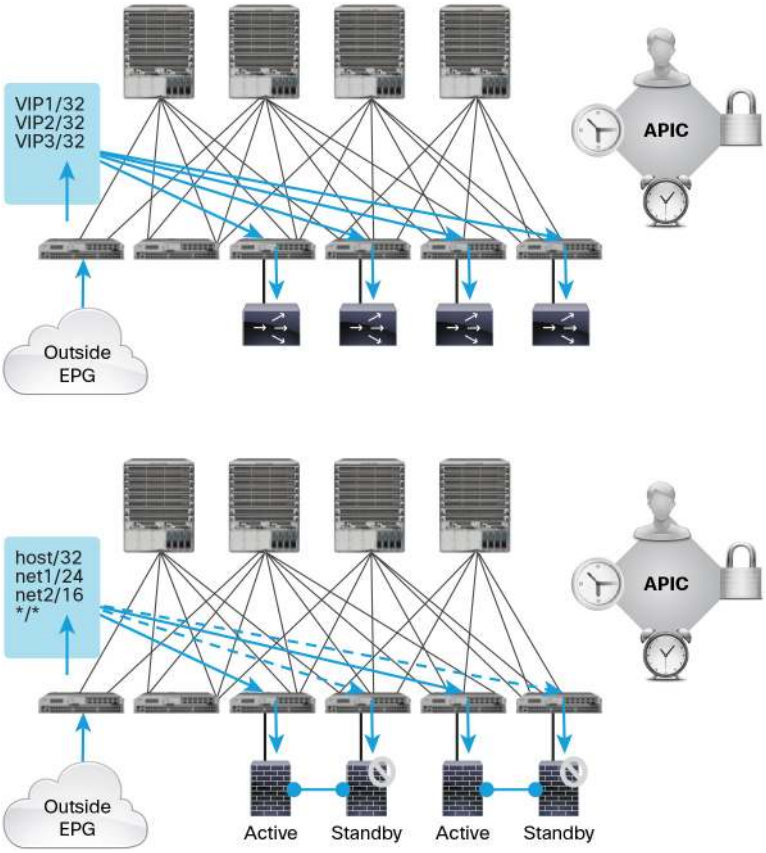
Figure 4. Example of a Device Package



Service Resource Pooling

The Cisco ACI fabric can perform nonstateful load distribution across many destinations. This capability allows organizations to group physical and virtual service devices into service resource pools, which can be further grouped by function or location. These pools can offer high availability if desired using standard high-availability mechanisms, or they can be used as simple stateful service engines, with the load redistributed to the other members in the event of a failure. Either option provides horizontal scaleout that far exceeds the current limitations of the Equal-Cost Multipath (ECMP) and PortChannel features and service appliance clustering, which requires shared state (Figure 5).

Figure 5. Resource Pooling



Cisco ACI can perform a simple version of resource pooling with any service devices if the service devices do not have to interact with the fabric, and it can perform more advanced pooling that involves coordination between the fabric and the service devices. This capability provides the flexibility needed to work with any service partners today and new partners in the future.

Conclusion

Service devices are critical components of the network and need to be treated as integrated elements, not as add-ons to the network. Cisco ACI provides a new services vision for data center networks. This vision involves centralized network and service policy management, implicit automation, and service scaleout for both physical and virtual devices. The Cisco ACI services architecture is designed to deliver all these features as part of our revolutionary fabric technology.

For More Information

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-729998-00 11/13