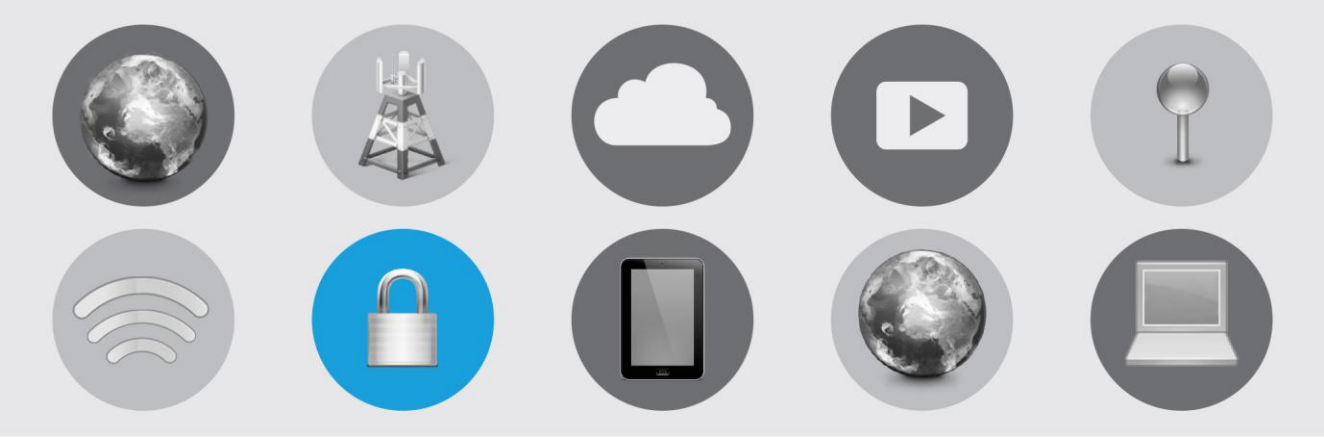
F5 BIG-IP Local Traffic Manager Service Insertion with Cisco Application Centric Infrastructure

Design Guide

July 2015



Contents

Introduction

Preface

This document discusses how to deploy the F5 BIG-IP Local Traffic Manager (LTM) with the Cisco® Application Policy Infrastructure Controller (APIC) in the data center using a device package (an XML definition of BIG-IP LTM functions). It focuses on the most commonly deployed use cases for Layer 4 through 7 services in today's data center, integrated with the APIC. The solution uses the Cisco Application Centric Infrastructure (Cisco ACI™).

The topologies used in this document can be altered to reflect the setup and design that meets customer's specific needs and environment.

Audience

This document is intended for network architects and engineers to aid in the development of solutions for Cisco ACI and F5 Layer 4 through 7 service insertion and automation.

Scope

This document defines the design recommendations for BIG-IP LTM placement in Cisco ACI architecture to provide network services. Limited background information is included about other related components whose understanding is required to implement the solution.

- For more information about Cisco ACI design, see the Cisco Application Centric Infrastructure Design Guide.
- For more information about Cisco ACI service insertion, see the Cisco Application Centric Infrastructure white paper.
- For more information about F5 BIG-IP LTM, see the BIG-IP Local Traffic Management documentation.

Cisco APIC Overview

Cisco Application Centric Infrastructure is a holistic architecture with centralized automation and policy-based application profiles. It delivers software flexibility with scalable hardware performance and facilitates rapid systems integration and customization for network services, monitoring, management, and orchestration with visibility of both physical and virtual networks. It is built on a fabric foundation that delivers best-in-class infrastructure by combining hardware, software, and application-specific integrated circuit (ASIC) innovations into an integrated system.

The architecture provides a common management framework for network, application, security, and virtualization teams, making IT more agile while reducing application deployment time. It is optimized to run today's physical and virtual applications and is also ready for tomorrow's emerging architectures that will need to support an "application anywhere" model with complete freedom of application movement and placement. The architecture is designed for multitenancy, helping ensure proper isolation and detailed telemetry to meet service-level agreements (SLAs) for different consumers of the infrastructure while also providing consistent security policy across both physical and virtual applications.

Cisco ACI empowers IT teams to directly offer cloud-based services to their customers that meet the SLAs and performance requirements for the most demanding business applications. It's an open programmable architecture with a comprehensive set of APIs that are exposed to the open-source community, enabling a broad choice of data center management and infrastructure.

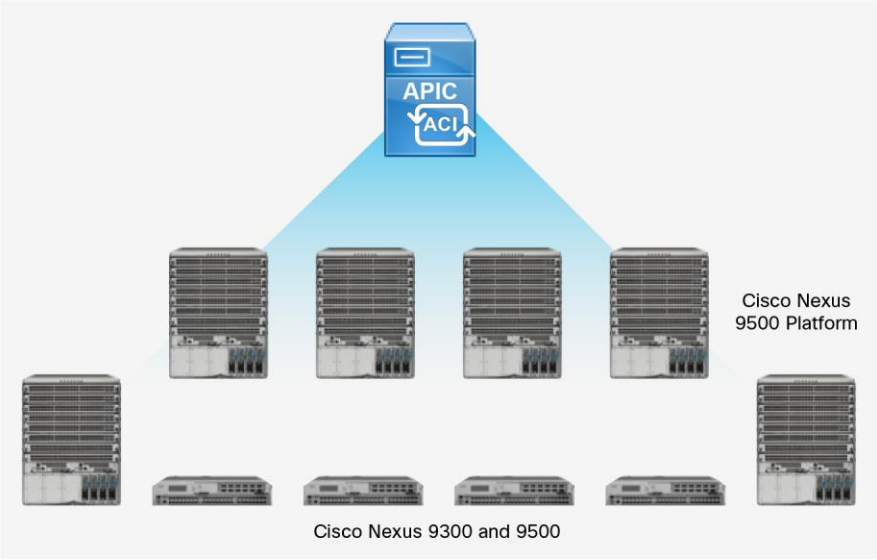
The main features of Cisco ACI include:

- Simplified automation using an application-based policy model
- Centralized management, automation, and orchestration
- Mixed workload and migration optimization
- Secure and scalable multitenant environment
- Extensibility and openness, with open source, open APIs, and open software flexibility for development and operations (DevOps) teams and ecosystem partner integration
- Investment protection (for both people and infrastructure)

The Cisco ACI fabric consists of discrete components that operate as routers and switches, but the fabric is provisioned and monitored as a single entity. The fabric is designed for consistent low-latency forwarding across high-bandwidth links (40 Gbps, with 100-Gbps future capability). Traffic with the source and destination on the same leaf is handled locally, and all other traffic travels from the ingress leaf to the egress leaf through a single spine switch. Although this is a two-hop architecture from a physical perspective, it is a single Layer 3 hop because the fabric itself operates as a single Layer 3 switch. The single entity that manages the control and management plane in Cisco ACI fabric is the Cisco Application Centric Infrastructure Controller, or APIC (Figure 1).

The APIC uses the Cisco ACI fabric to automate the deployment of the infrastructure, improve availability, and provide service insertion and application-level monitoring. Although the APIC acts as the centralized policy and network management engine for the fabric, it is completely removed from the data path, including the forwarding topology. Therefore, the fabric can still forward traffic even when communication with the APIC is lost.

Figure 1: Cisco APIC



The APIC acts as a central point of configuration management and automation for Layer 4 through 7 services. It tightly coordinates service delivery, serving as the controller for network automation. A service appliance (device) performs a service function defined in a service graph. One or more service appliances may be required to render the services required by a service graph. A single service device can perform one or more service functions.

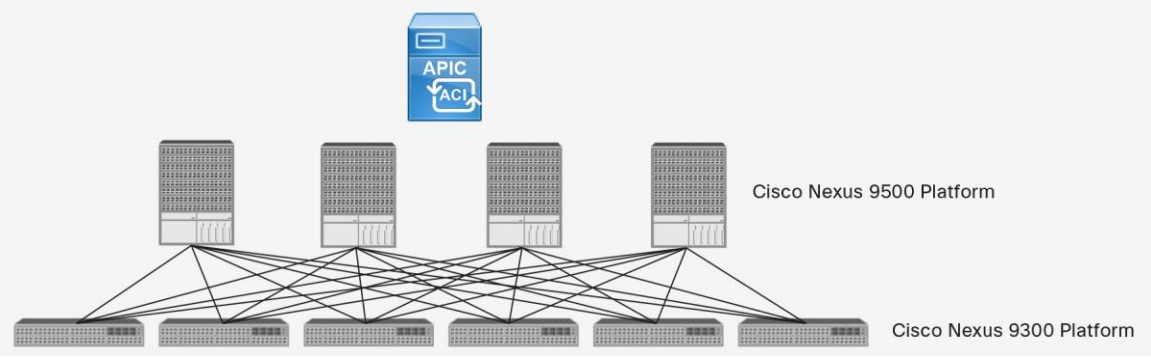
The APIC enables the user to define a service graph or chain of service functions in a graph: for example, the web application firewall (WAF) function, load-balancing function, and network firewall function. The graph defines these functions based on a user-defined policy. One or more service appliances may be needed to render the services required by the service graph. These service appliances are integrated in the APIC using southbound APIs presented in a device package that contains the XML schema of the F5 device model. This schema defines the software version, functions provided by F5 BIG-IP LTM (SSL termination, Layer 4 server load balancer [SLB], etc.), parameters required to configure each function, and network connectivity details. It also includes a Python script that maps APIC events to function calls to F5 BIG-IP LTM.

Hardware and Software Support

Cisco ACI

The joint solution uses the Cisco Nexus® 9000 Series Switches (Figure 2).

Figure 2: Cisco Nexus Family Switches and Cisco ACI



The solution described in this document requires the following components:

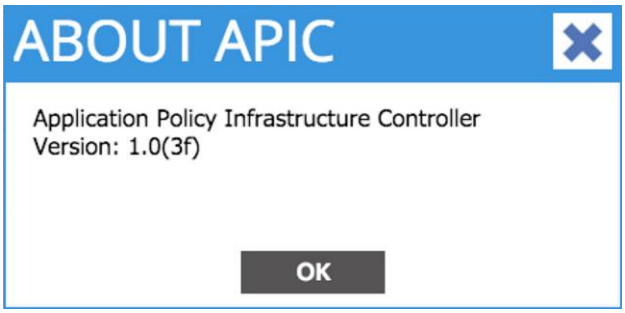
- Spine switches: The spine provides the mapping database function and connectivity among the leaf switches. At the time of this writing, these switches can be either the Cisco Nexus 9508 Switch equipped with the Cisco N9K-X9736PQ line card or fixed-form-factor switches such as the Cisco Nexus 9336PQ ACI Spine Switch. Spine switches provide high-density 40 Gigabit Ethernet connectivity between leaf switches. The Cisco Nexus 9336PQ form factor is well suited for smaller deployments because it provides 36 ports of 40 Gigabit Ethernet. The Cisco Nexus 9508 provides 288 40 Gigabit Ethernet ports.

- Leaf switches: The leaf switches provide physical and server connectivity and policy enforcement. At the time of this writing, the leaf switches can be fixed-form-factor switches such as the Cisco Nexus 9396PX, 9396TX, and 93128TX Switches. The choice of leaf switches provides the option to use 10GBASE-T or Enhanced Small Form-Factor Pluggable (SFP+) connectivity to the servers. Leaf switches can be used in two modes: as standalone Cisco NX-OS Software devices, or as devices that are part of the Cisco ACI fabric (with a Cisco ACI version of NX-OS).

- APIC: The controller is the point of configuration for policies and the place at which statistics are archived and processed to provide visibility, telemetry, application health information, and overall management for the fabric. The APIC is a physical server appliance such as a Cisco UCS® C220 M3 Rack Server with two 10 Gigabit Ethernet interfaces that are meant to be connected to the leaf switches and with Gigabit Ethernet interfaces for out-of-band management.

  The version on which the designs in this document have been validated is APIC Version 1.0(3f) and Version 1.0(4h) of the fabric switch.

Figure 3: Cisco APIC Version Used in This Document



- 40 Gigabit Ethernet cabling: Leaf and spine switches can connect at 40 Gbps with multimode fiber by using the new Cisco 40-Gbps short-reach (SR) bidirectional Quad SFP (QSFP) optics modules, which do not require new cabling. With these optics modules, you can connect equipment at distances up to 100 meters on OM3 cabling and up to 125 meters or more on OM4 cabling. Other QSFP options are also available for 40-Gbps links. For more information about 40 Gbps cabling options, see:
  - http://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-729384.pdf
  - http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_24900.html

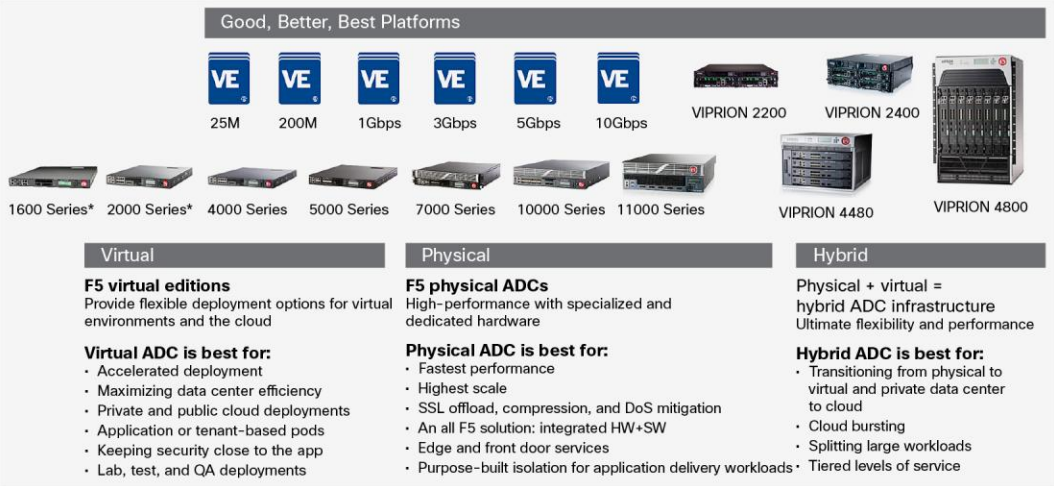
- Classic 10 Gigabit Ethernet cabling: Cabling to the server with 10 Gigabit Ethernet can be implemented with SFP+ fiber or copper or with 10GBASE-T technology.

For more information about Cisco ACI hardware, please refer to Cisco Application Centric Infrastructure.

F5 BIG-IP

F5 VIPRION, BIG-IP, and Virtual Edition (VE) running Version 11.4.1 and later software can be integrated with Cisco ACI (Figure 4).

Figure 4: BIG-IP Platforms Integrate with Cisco ACI

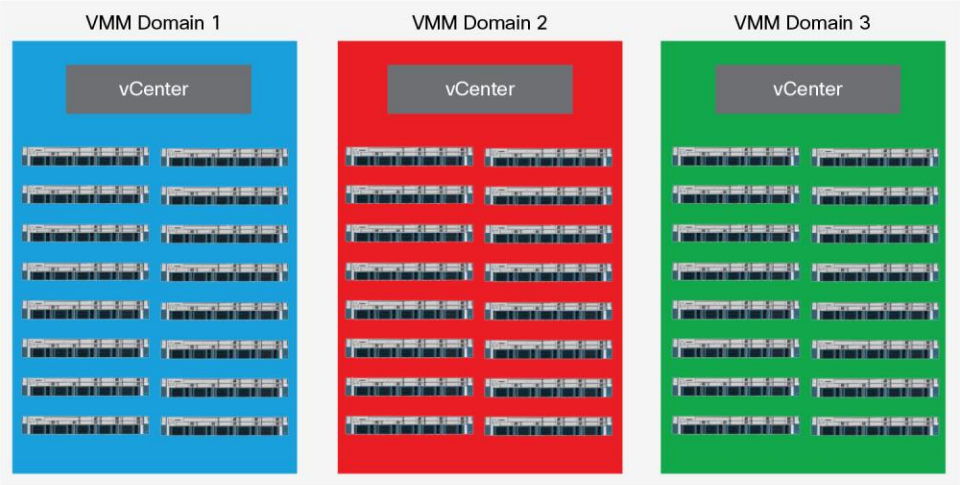


If you use Virtual Edition, before using it you must integrate VMware vSphere with APIC.

Cisco ACI can closely integrate with the server virtualization layer. In practice, this means that when you instantiate application policies through Cisco ACI, the equivalent constructs at the virtualization layer (that is, port groups) will be created automatically and mapped to the Cisco ACI policy.

Integration with the server virtualization layer is defined through the creation of a policy construct known as a virtual machine manager (VMM) domain (Figure 5). A VMM domain is a container for one or more virtual machine management systems (for example, VMware vCenter) with similar network policy requirements. Each VMM domain represents a live migration domain; in other words, virtual machines can be migrated live within the VMM domain, but not beyond it.

Figure 5: VMM Domains

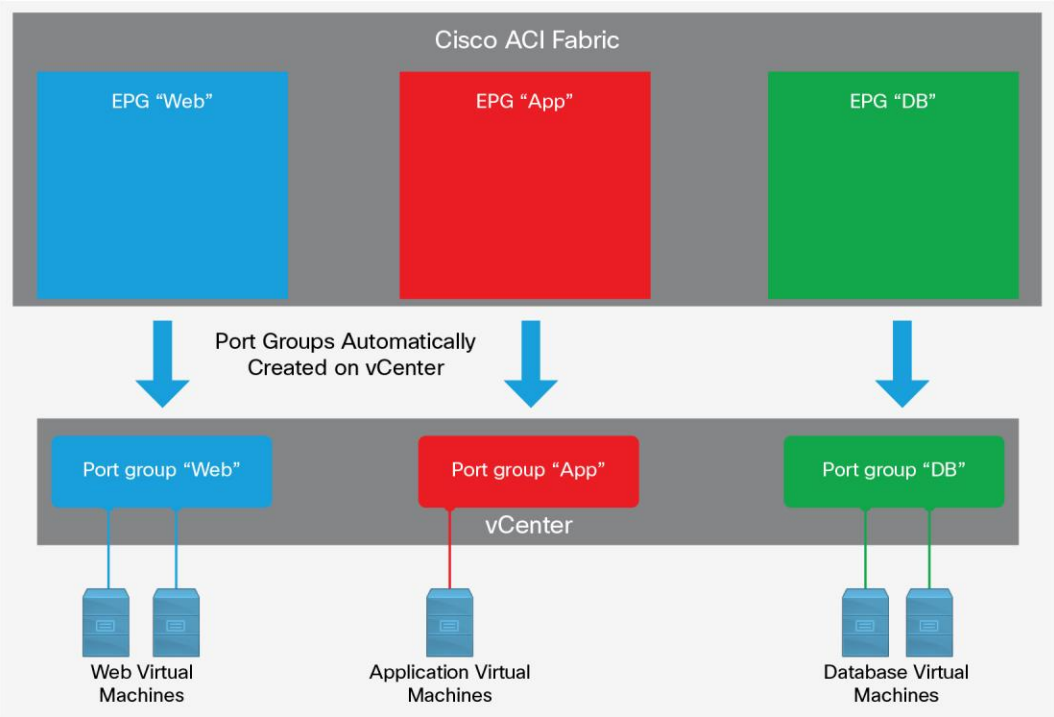


Each VMM domain is associated with a name space. The name space defines a range of identifiers (normally VLANs or VXLANs) that are used to identify traffic within the domain and map that traffic to endpoint groups (EPGs). If VLANs are used to identify the traffic, then each VMM domain can support up to 4000 EPGs.

Note: Multiple VMM domains can have the same name space (that is, overlapping VLANs) as long as they are separated physically: that is, if they exist on separate leaf switches.

After the integration with vCenter is complete, the fabric or tenant administrator creates EPGs, contracts, and application profiles as usual. When an EPG is created, a corresponding port group is created at the virtualization level. The server administrator then connects virtual machines to these port groups (Figure 6).

Figure 6: EPGs, Port Groups, and Virtual Machines



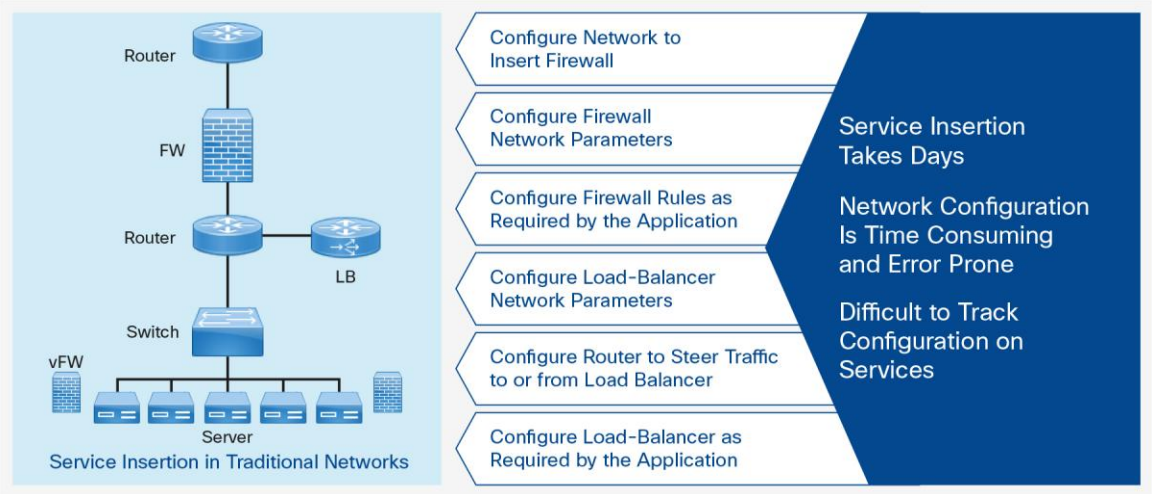
Cisco ACI Layer 4 through 7 Service Insertion

Service Insertion Challenges

Applications have become critical to the survival of businesses, and network delivery problems that affect the security, reliability, or performance of applications can negatively affect businesses in a variety of ways: from lost productivity to customer dissatisfaction and marred reputations. Applications should not only work, but they need to respond to business objectives in near-real time to meet business goals. But significant shifts in technology are making these challenges increasingly complicated and costly to address.

Traditionally, when you insert services into a network, you must perform a highly manual and complicated VLAN (Layer 2) or Virtual Routing and Forwarding (VRF) instance (Layer 3) stitching between network elements and service appliances. This traditional model requires days or weeks to deploy new services for an application. The services lack flexibility, operating errors are common, and troubleshooting can be difficult. When an application is retired, removing a service device configuration, such as firewall rules, can be difficult. In addition, services cannot be scaled out or scaled down based on load (Figure 7).

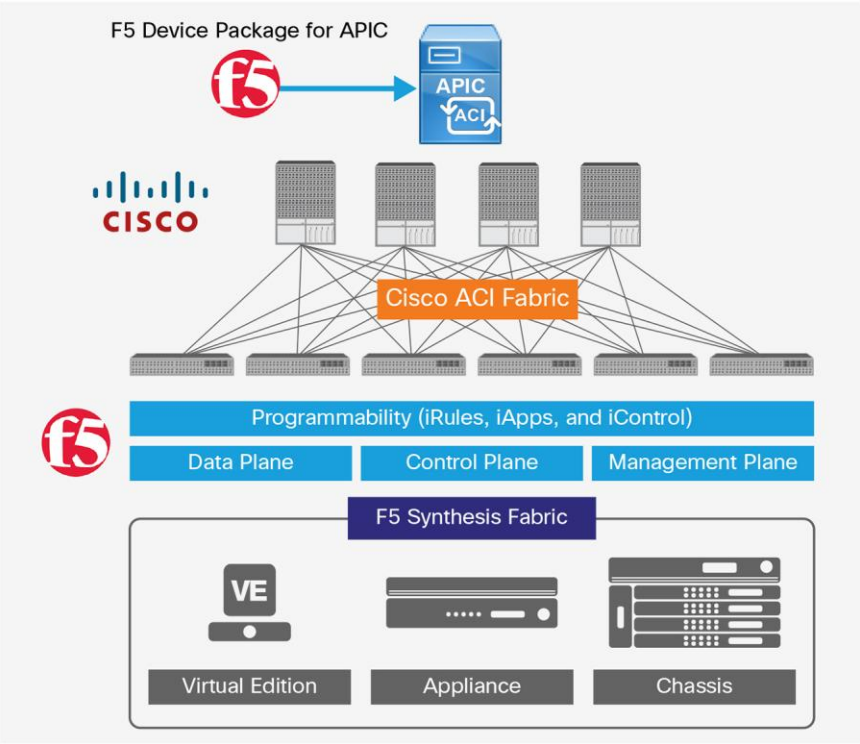
Figure 7: Service Insertion: Traditional Model



Benefits of F5 and Cisco ACI Joint Solution

Although traditional service insertion models support VLAN and VRF stitching, the APIC can automate service insertion while acting as a central point of policy control. APIC policies manage both the network fabric and service appliances. The APIC can configure the network automatically so that traffic flows through the services. It can also automatically configure the service according to the application's requirements, which allows organizations to automate service insertion and eliminate the challenge of managing the complex techniques of traditional service insertion (Figure 8).

Figure 8: Service Insertion Using F5 and Cisco ACI Solution



The F5 and Cisco joint solution enables virtual workload mobility while retaining consistent Layer 4 through 7 services and without requiring co-location of services with the application. As workloads migrate, so do the network and the Layer 4 through 7 services they need to meet the reliability, security, and performance requirements demanded by customers and business stakeholders.

- End-to-end policy-based configuration of physical and virtual networking, including Layer 4 through 7 services: The solution provides the agility needed to significantly reduce operating costs. Workflow provisioning is efficient and fast, with operation best practices maintained across multiple IT teams.
- Single point of provisioning, management, monitoring, and visibility with APIC: By centralizing network and application service policy management and topology control, the solution helps ensure the best user experience without compromising the performance, security, or scalability of applications. Thus, what traditionally were single application deployments are transformed into dynamic and scalable application fabric solutions.
- Automated Layer 4 through 7 application service insertion, policy updates, and optimization in Cisco ACI fabric with F5 BIG-IP: The solution preserves the robustness of the F5 Synthesis offering through policy abstraction. Together, Cisco ACI and F5 Software-Defined Application Services (SDAS) offer a comprehensive, application-centric set of network and Layer 4 through 7 services, enabling both traditional and next-generation data centers to deploy and deliver applications with the speed, reliability, and security necessary to meet the challenges of an increasingly interconnected and highly demanding application environment.
- Accelerated application deployments with reliability, security, and consistent scalable network and Layer 4 through 7 services: Existing F5 hardware and software and topologies integrate transparently with Cisco ACI.
- Improved deployment speed for services: Both Cisco ACI and F5 Synthesis are highly extensible through programmatic extensions, enabling consistent automation and orchestration of critical services to support business and application requirements for performance, security, and reliability.
- Protection of existing investments: Cisco ACI supports the existing F5 application delivery model as well as the F5 Synthesis fabric-based model, preserving existing investments in both infrastructure and policy creation. Doing so enables IT to transition to new data center models at its own pace, without requiring disruptive change to applications.

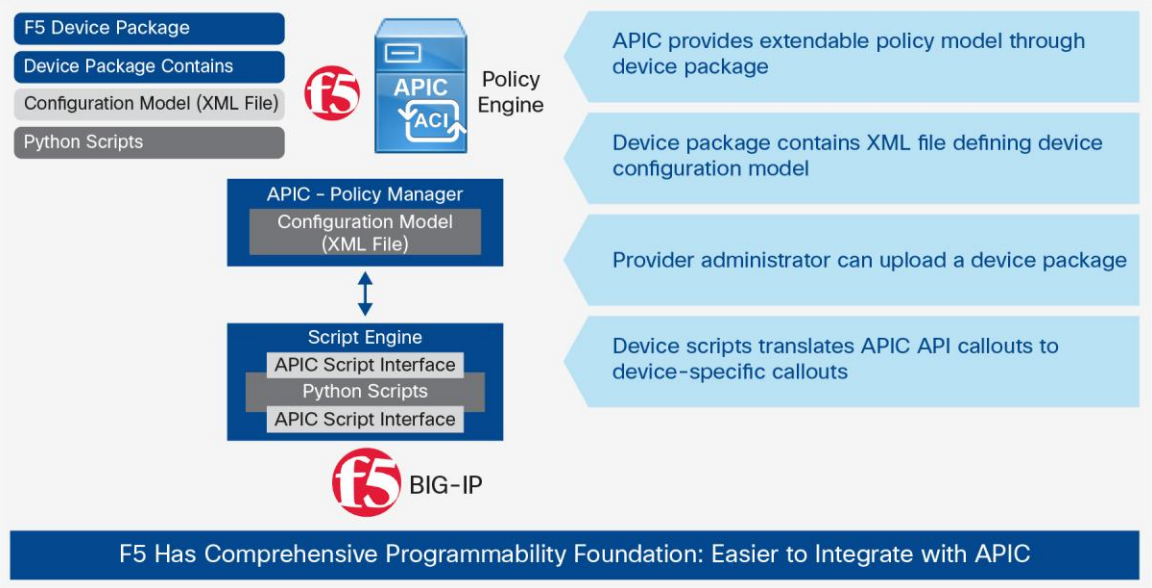
Service Automation through Device Package

The 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 APIC interfaces with a service device using Python scripts and calls device-specific Python script functions on various events. 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 APIC. The device script handler interfaces with the device using its Representational State Transfer (REST) or Simple Object Access Protocol (SOAP) interface (preferred) or its command-line interface (CLI), depending on the device configuration mode.

When a device package is uploaded to APIC, the APIC creates a hierarchy of managed objects representing the device and validates the device script. Figure 9 shows the relationship between a device package and the APIC.

The APIC manages BIG-IP LTM and its supported functions through device packages, which are used to define, configure, and monitor service devices. A device package allows a network service to be added, modified, removed, and monitored on the APIC without interruption. To add a new device type to the APIC, you upload a device package. The device package is a zip file containing all the information needed for the APIC to integrate with any type of service device.

Figure 9: Device Packages



Main Service Insertion Concepts

This section describes the main concepts used in service insertion.

Device Package

A device package is a zip file that contains the components listed in Table 1.

Table 1: Device Package Components

Component	Description
Device specification	An XML file that defines the following properties: • Device properties: – Model: Model of the device. – Vendor: Vendor of the device. – Version: Software version of the device. • Functions provided by a device, such as load balancing, content switching, and SSL termination • Interfaces and network connectivity information for each function • Device configuration parameters • Configuration parameters for each function

Component	Description
Device script	A Python script that performs the integration between the APIC and a device; the APIC events are mapped to function calls that are defined in the device script
Function profile	A profile of parameters with default values that are specified by the vendor; you can configure a function to use these default values
Device-level Configuration parameters	A configuration file that specifies parameters that are required by a device at the device level; the configuration can be shared by one or more of the graphs that are using the device

Logical Device Cluster

A logical device cluster is one or more concrete devices that act as a single device. A device cluster has logical interfaces, which describe the interface information for the device cluster. During the rendering of the service graph template, function node connectors are associated with logical interfaces. The APIC allocates the network resources (VLAN or Virtual Extensible LAN [VXLAN]) for a function node connector during service graph template instantiation and rendering and programs the network resources onto the logical interfaces.

The service graph template uses a specific device cluster that is based on a device cluster selection policy (called a logical device context) that an administrator defines.

An administrator can set up a maximum of two concrete device clusters in active-standby mode.

Concrete Device

A concrete device has concrete interfaces. When a concrete device is added to a logical device cluster, concrete interfaces are mapped to the logical interfaces. During service graph template instantiation, VLANs and VXLANs are programmed on concrete interfaces based on their association with logical interfaces.

Service Graph

Cisco ACI treats services as an integral part of an application. Any services that are required are treated as a service graph that is instantiated on the Cisco ACI fabric from the APIC. Users define the service for the application, and service graphs identify the set of network or service functions that the application needs. Each function is represented as a node.

Private Network and Bridge Domain

A context (private network) is a unique Layer 3 forwarding and application policy domain (a private network or VRF instance) that provides IP address space isolation for tenants.

A bridge domain represents a Layer 2 forwarding construct within the fabric.

A bridge domain must be linked to a context and have at least one subnet that is associated with it. The bridge domain defines the unique Layer 2 MAC address space and a Layer 2 flood domain should such flooding be enabled. A context defines a unique IP address space, and that address space can consist of multiple subnets. These subnets are defined in one or more bridge domains that reference the corresponding context.

F5 Device Package

F5 Device Package Supported Features (Release 1.1.0)

The F5 Release 1.1.0 device package supports the features listed here.

- Virtualized Clustered Multiprocessing (vCMP): vCMP is a feature of the BIG-IP system that allows you to run multiple instances of the BIG-IP software on a single hardware platform.
- Dynamic endpoint attach and detach: Endpoints can be either prespecified in corresponding EPGs (specified statically at any time) or added dynamically as they are attached to Cisco ACI. Endpoints are tracked by a special endpoint registry mechanism of the policy repository. This tracking gives the APIC visibility into the attached endpoints. APIC passes this information to BIG-IP. From BIG-IP's point of view, this attached endpoint is a member of a pool, and hence BIG-IP converts the APIC call that the device package receives into an addition of a member to a particular pool.
- BIG-IP LTM configurable parameters: LTM supports a number of configurable parameters.
  - Self-IP addresses: A self-IP address is an IP address on the BIG-IP system that you associate with a VLAN to access hosts in that VLAN. Because of its net mask, a self-IP address represents an address space - that is, a range of IP addresses spanning the hosts in the VLAN - rather than a single host address. You can associate self-IP addresses not only with VLANs, but also with VLAN groups.
  - Static routes: Part of routing management on a BIG-IP system is the addition of static routes for destinations that are not located on the directly connected network.
  - Listener: A virtual server is an IP address and port specification on the BIG-IP system. The BIG-IP system listens for traffic destined for that virtual server, and then directs that traffic either to a specific host for load balancing or to an entire network.
  - Server pools: A load-balancing pool is a set of devices, such as web servers, that you group together to receive and process traffic. Instead of sending client traffic to the destination IP address specified in the client request, the LTM system sends the request to any of the servers that are members of that pool.
  - Monitor: The BIG-IP LTM system can monitor the health and performance of pool members and nodes.
  - iRules: An iRule is a powerful and flexible feature in the BIG-IP LTM system that you can use to manage your network traffic. Using syntax based on the industry-standard Tool Command Language (Tcl), the iRules feature allows you to select pools based on header data. It also allows you to direct traffic by searching on any type of content data that you define. Thus, the iRules feature significantly enhances your ability to customize your content switching to suit your exact needs.
  - Secure Network Address Translation (SNAT) pool management: SNAT translates the source IP address within a connection to a BIG-IP system IP address that you define. The destination node then uses that new source address as its destination address when responding to the request.
  - HTTP redirect: This parameter redirects an HTTP request to a specified URL.
  - Client SSL offload: Client-side traffic refers to connections between a client system and the BIG-IP system. When you enable the BIG-IP system to manage client-side SSL traffic, the BIG-IP system terminates incoming SSL connections by decrypting the client request. The BIG-IP system then sends the request, in clear text, to a target server. Next, the BIG-IP system retrieves a clear-text response (such as a webpage) and encrypts the request before sending the webpage back to the client.

- Active-standby high availability model per APIC logical device cluster.
- Configuration of BIG-IP license and out-of-band (OOB) management prior to APIC integration.

F5 Device Package Supported Functions

The F5 device package supports the functions listed here.

- Service function: virtual server
  - Layer 4 server load balancing (SLB)
    - Act upon data found in network and transport layer protocols (IP, TCP, FTP, and UDP).
    - Perform Layer 4 SLB with SSL offload.
  - Layer 7 SLB
    - Distribute requests based on data found in application-layer protocols such as HTTP.
    - Perform Layer 7 SLB with SSL offload.
- Service function: Microsoft SharePoint

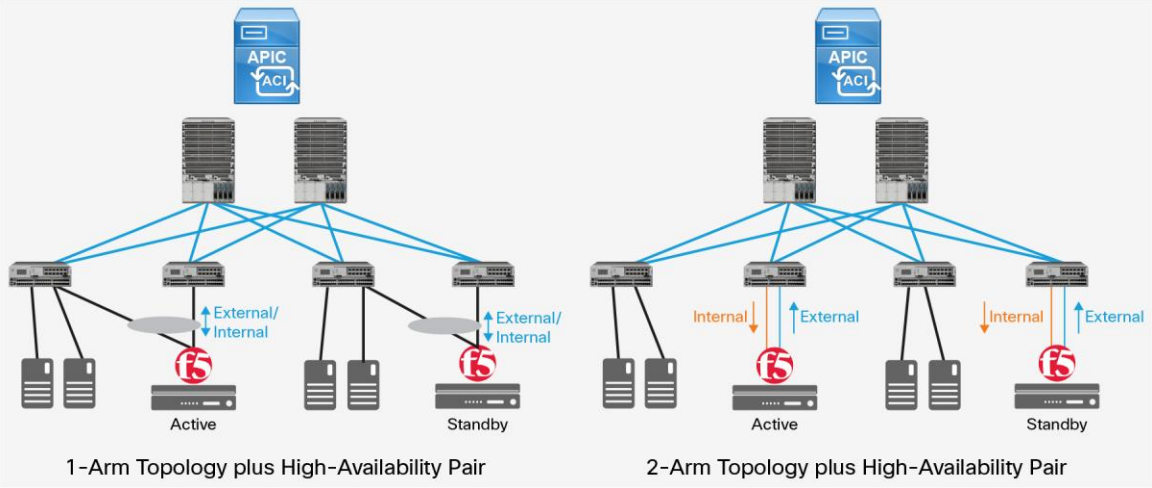
F5 and Cisco ACI Design Model

This section discusses the design model of the F5 and Cisco ACI solution.

Topology

Figure 10 shows the topology of the F5 and Cisco ACI solution.

Figure 10: Topology



One-Arm Topology

Physically, a one-arm topology as depicted in Figure 10 refers to a single interface connected to the leaf node. This one interface handles both internal (intranet) and external (Internet) traffic.

Logically, the number of arms can be considered to equal the number of VLAN's that are created and active: in the example in Figure 10, one VLAN is created and active.

One-arm mode is the most common type of deployment. In this type of deployment, just one VLAN needs to be created on the load balancer, both the physical servers need to be load balanced, and the clients that are trying to reach the servers must use the same VLAN.

This approach causes little impact on the existing LAN and WAN design. But note that for this approach to work, you need to enable SNAT settings on the load balancer.

So you can deploy a physical one-arm topology as a logical one-arm topology (one VLAN) or logical two-arm topology (two VLANs).

Two-Arm Topology

Physically, a two-arm topology as depicted in Figure 10 refers to two interfaces connected to the leaf. One interface handles internal (intranet) traffic, and one interface handles external (Internet) traffic.

Logically, the number of arms can be considered to be the number of VLANs that are created and active: in this case, two VLANs.

So you can deploy a physical two-arm topology as a logical one-arm topology (one VLAN) or logical two-arm topology (two VLANs).

Uplink Considerations

Cisco ACI supports three types of fabric connectivity:

- Port: A port maps to a BIG-IP interface (1_1, 1_2, etc.).
- PortChannel: A PortChannel maps to a BIG-IP trunk.
- Virtual PortChannel (vPC): A vPC maps to a BIG-IP trunk.

F5 and Cisco ACI Service Insertion

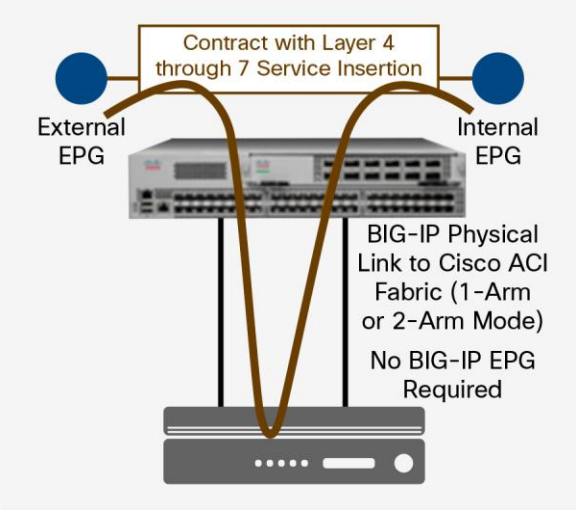
Cisco ACI provides customers with an automated service insertion and policy management model that represents the next generation of data center architecture compared to the traditional model of services insertion. The Cisco ACI controller (the APIC) can automate service insertion while acting as a central point of policy control. The controller also can automatically configure the service according to the application's requirements, which allows organizations to automate service insertion and eliminate the challenge of having to manage the complex techniques of traditional service insertion.

BIG-IP LTM integrates with the APIC through well-established and open southbound APIs. This integration automates network and service provisioning across the F5 services fabric, providing end-to-end telemetry and visibility of applications and tenants. The APIC acts as a central point of configuration management and automation for Layer 4 through 7 services and tightly coordinates service delivery, serving as the controller for network automation. The APIC automates the insertion and provisioning of network services through the BIG-IP platform

In this deployment model, F5 is inserted as a Layer 4 through 7 service in the APIC. This approach is the recommended best practice for deploying service insertion with the APIC. To explore other deployment options, refer to Appendix A.

BIG-IP is connected to one of the leaf nodes in the network in one-arm or two-arm mode. All configuration on BIG-IP is performed in band. With the F5 and Cisco ACI solution, the APIC controls all configuration on BIG-IP. It also controls the network and the flow of traffic to and from BIG-IP. This control is achieved using the concept of service insertion. Service insertion uses contracts to bind the EPGs and enable communication (Figure 11).

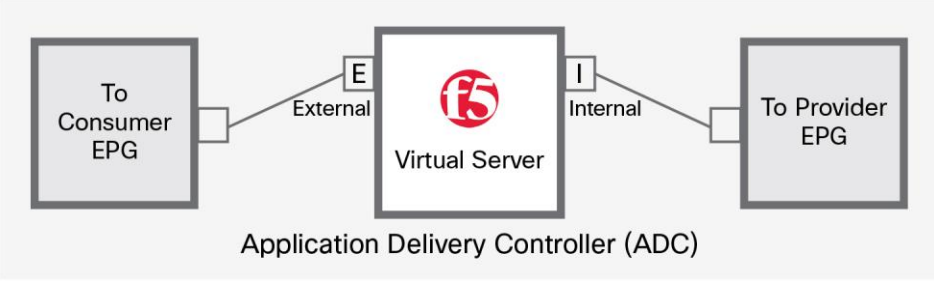
Figure 11: Service Insertion



Differences between One-Arm and Two-Arm Configuration with Layer 4 through 7 Service Insertion

Figure 12 shows the function node.

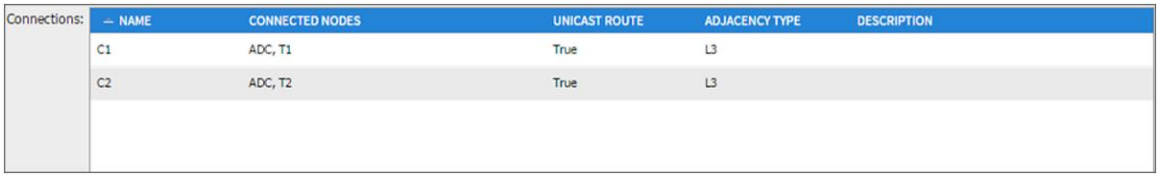
Figure 12: Function Node



Cisco APIC Logical One-Arm Service Insertion

In Cisco ACI terminology, when a service is inserted in one-arm mode, the connection between the two abstract connections is a Layer 3 connection (Figure 13).

Figure 13: Logical One-Arm Service Insertion



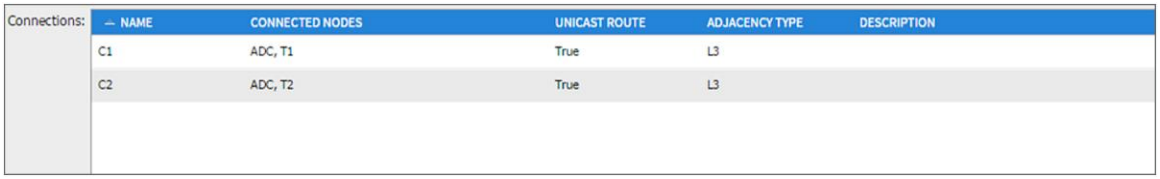
When a graph is applied with service insertion in one-arm mode, a bridge domain for F5 needs to be selected as well. The bridge domain associated with an F5 Layer 4 through 7 device must be enabled for unicast routing (Figure 14).

Figure 14: Bridge Domain Associated with Layer 4 through 7 Device Must Be Enabled for Unicast

Cisco APIC Logical Two-Arm Service Insertion

When a service is inserted in two-arm mode, the connection between the two abstract connections is a Layer 3 connection (Figure 15).

Figure 15: Logical Two-Arm Service Insertion



When a graph is applied with service insertion in two-arm mode, a bridge domain for F5 is not required (Figure 16).

Figure 16: Bridge Domain Is Not Required

F5 and Cisco ACI Service Insertion Design Considerations

This section discusses some points to keep in mind when deploying F5 and Cisco ACI service insertion.

High Availability

F5 supports high availability in active-standby mode with APIC. Here, high availability refers to the capability of a BIG-IP system to process network traffic successfully.

Redundant System Configuration

When you are running the BIG-IP system as a unit of a redundant system configuration, high availability means that core system services are up and running on one of the two BIG-IP systems in the configuration. A redundant system is a type of BIG-IP system configuration that allows traffic processing to continue in the event that a BIG-IP system becomes unavailable. A BIG-IP redundant system consists of two identically configured BIG-IP units. When an event occurs that prevents one of the BIG-IP units from processing network traffic, the peer unit in the redundant system immediately begins processing that traffic, and users experience no interruption in service.

With active-standby mode, only one of the two units is in an active state, processing traffic, at any given time. The inactive unit serves strictly as a standby unit, becoming active only if the active unit becomes unavailable. When a standby unit becomes active, it normally remains active until an event occurs that requires the other unit to become active again, or until you specifically force it into a standby state. Active-standby mode is the recommended mode for redundant system configuration.

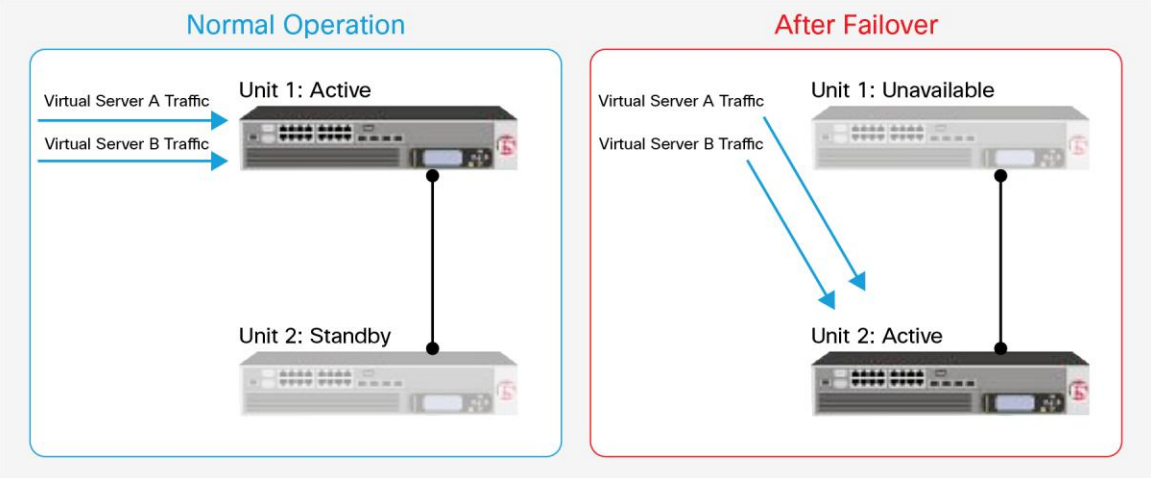
To enable a unit to fail over to its peer unit, you must first specify the type of failover that you want the redundant system to use. The two possible failover types are hard-wired failover and network-based failover.

- Hard-wired failover: When you configure hard-wired failover, you enable failover by using a failover cable to physically connect the two redundant units. This is the default setting.
- Network failover: When you configure network failover, you enable failover by configuring the redundant system to use the out-of-band management network to determine the status of the active unit. The administrator can use network failover in addition to, or instead of, hard-wired failover.

When a redundant system is in active-standby mode, one unit is active (that is, accepting and processing connections on behalf of the redundant system), and the other unit is idle (that is, in a standby state). When failover occurs, the standby unit becomes active, and it normally stays active until failover occurs again, or until the user forces it into a standby state. Forcing the unit into a standby state automatically causes the other system to become active again, if possible.

For example, you can configure unit 1 to process traffic for virtual servers A and B. The standby unit monitors the active unit, and if communications fail, the standby unit initiates a failover and becomes the active unit. The newly active unit then begins processing traffic for both virtual servers. Figure 17 shows an active-standby configuration, first as it behaves normally and then after failover has occurred.

Figure 17: Active-Standby Configuration Before and after Failover



When the failed unit becomes available again, the user can force a unit to change its state from active to standby or from standby to active, thereby initiating failback. Failback on an active-standby system causes a unit to relinquish any processing that it is doing on behalf of its peer and return to a standby state. A redundant system in active-standby mode is the most common type of redundant system.

Only active-standby mode is supported in APIC Version 1.0(3f) and 1.0(4h) with device package Version 1.1.0.

Connection mirroring is enabled by default. BIG-IP system redundancy includes the capability for a device to mirror connection and persistence information to another device, to prevent interruption in service during failover. The BIG-IP system mirrors connection and persistence data over TCP port 1028 with every packet- or flow-state update.

For physical BIG-IP, a best practice recommendation is to hard-wire two BIG-IP high-availability interfaces. The high-availability self-IP address and VLAN are local to BIG-IP. The APIC configures the high-availability VLAN; however, the BIG-IP high-availability VLAN allocation does not belong to the VLAN pool that the APIC manages.

For Virtual Edition, a best practice recommendation is to use interface 1_3 on the BIG-IP as the high-availability interface. This interface can be tied to the management network (the failover detection will take place based communication with one another about system status on this interface).

You must use the fully qualified domain name (FQDN) as the F5 BIG-IP host name when configuring the system in active-standby mode.

Dynamic and Static Pools

Load-Balancing Pool

In a typical client-server scenario, a client request goes to the destination IP address specified in the header of the request. For sites with a large amount of incoming traffic, the destination server can quickly become overloaded as it tries to service a large number of requests. To solve this problem, the BIG-IP LTM system distributes client requests to multiple servers instead of to the specified destination IP address only. You configure the LTM system to do this when you create a load-balancing pool.

A load-balancing pool is a set of devices, such as web servers, that you group together to receive and process traffic. Instead of sending client traffic to the destination IP address specified in the client request, the LTM system sends the request to any of the servers that are members of that pool.

When you create a pool, you assign servers (known as pool members) to the pool, and then associate the pool with a virtual server in the LTM system. The LTM system then directs traffic coming into the virtual server to a member of that pool. An individual server can belong to one or multiple pools, depending on how you want to manage your network traffic.

The specific pool member to which the LTM system chooses to send the request is determined by the load-balancing method that you have assigned to that pool. A load-balancing method is an algorithm that the LTM system uses to select a pool member to process a request. For example, the default load-balancing method is **Round Robin**, which causes the LTM system to send each incoming request to the next available member of the pool, thereby distributing requests evenly across the servers in the pool.

Static Pool

The device package can define a pool as either static or dynamic. If a pool is defined as static, the user is expected to supply the pool member IP address and port information.

Using the APIC, pool members can be defined statically: that is, when the service graph is deployed, in addition to specifying other LTM parameters, you can also assign the pool members. The APIC then configures these static pool members on BIG-IP.

Dynamic Pool

For dynamic pool addition to work, the attachment notification on the function connector (connecting to the server subnet) must be enabled on the APIC, **and** the pool must be defined as dynamic when the service graph is deployed. The user is not expected to supply the pool member IP address and port information.

Endpoints are added dynamically as they are attached to Cisco ACI. Endpoints are tracked by a special endpoint registry mechanism of the policy repository. This tracking gives the APIC visibility into the attached endpoints. The APIC passes this information to BIG-IP. From BIG-IP's point of view, this attached endpoint is a member of a pool. The device package converts the APIC attached endpoint notification that it receives to an iControl (SOAP or REST API supported by BIG-IP) message that BIG-IP understands. The package then adds that member to a particular pool on BIG-IP.

This feature is useful when workloads and servers to be load-balanced need to be increased or decreased based on time and load or other triggers. This feature is also useful if you need to load-balance across a large number (100 or more) servers, making manual addition of those servers to the pool especially time consuming.

Cisco APIC Logical One-Arm Deployment

Bridge Domain Considerations

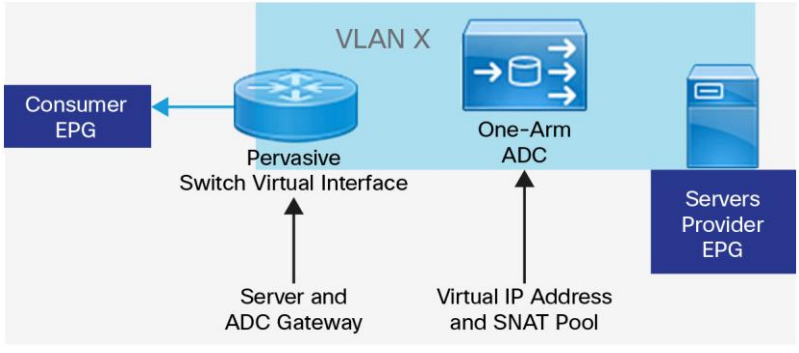
In an APIC one-arm deployment, a bridge domain must be assigned to the F5 function node. This bridge domain can be a separate bridge domain created for F5, or it can be existing bridge domain. More important, it is the subnet that belongs to the bridge domain in the design.

Note: In Cisco ACI, a subnet can belong to only a single bridge domain.

Depending on the subnet assignment, the consumer, provider, and F5 can all belong to the same bridge domain if they are all on the same subnet; or they can be assigned to separate bridge domains if they all have different subnets.

Figure 18 shows the Cisco ACI service graph with a one-arm ADC design.

Figure 18: Cisco ACI Service Graph with One-Arm ADC Design



Cisco APIC Logical Two-Arm Deployment

Bridge Domain Considerations

In an APIC two-arm deployment, no bridge domain is associated with the F5 Layer 4 through 7 device because the connections between the F5 device and the consumer and provider terminals are Layer 2. The F5 Internal self-IP address is in the same bridge domain as the server side (provider EPG); and the F5 external self-IP address is in the same bridge domain as the client side (consumer EPG). In the two-arm case, the provider and consumer cannot belong to the same bridge domain.

Table 2 shows the valid subnet assignment combinations in the APIC two-arm mode use case, where:

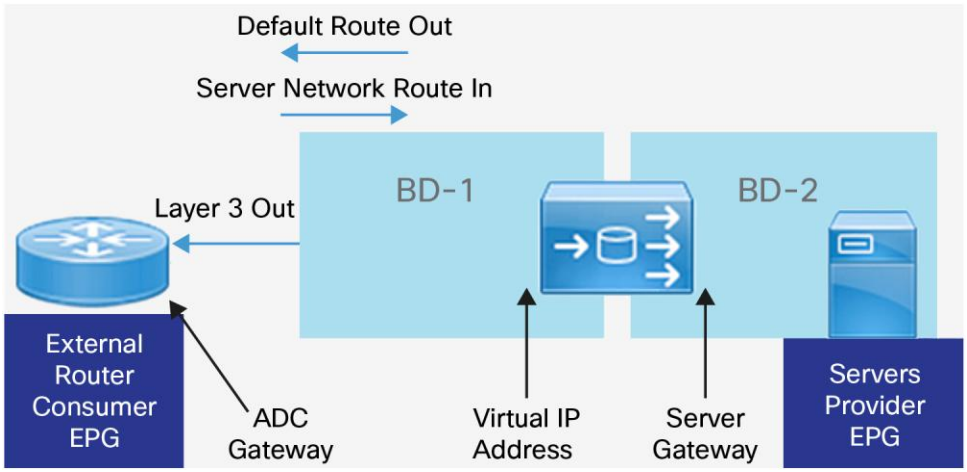
- BD-1: Subnet 10.10.10.x/24
- BD-1: Subnet 10.10.20.0/24

Table 2: Valid Subnet Assignments in APIC Two-Arm Mode

Role	Bridge Domain
Consumer	BD-1
Provider	BD-2

Figure 19 shows the Cisco ACI service graph with a two-arm ADC design.

Figure 19: Cisco ACI Service Graph with Two-Arm ADC Design



Secure Source Network Address Translation

SNAT translates the source IP address in a connection to a BIG-IP system IP address that you define. The destination node then uses that new source address as its destination address when responding to the request. The BIG-IP virtual server supports three source address translation modes:

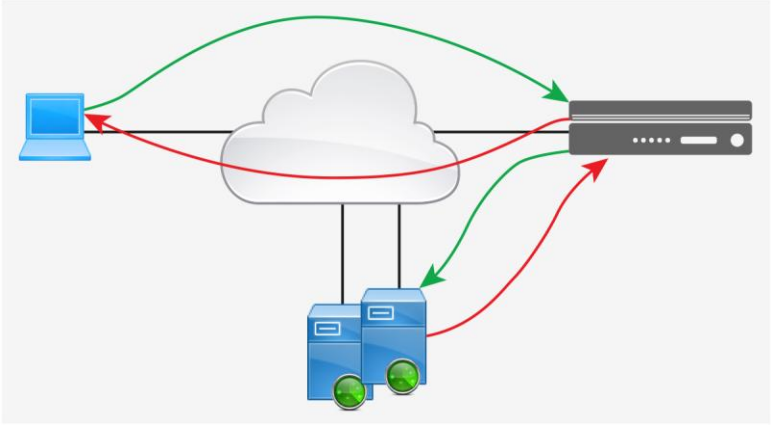
- None: SNAT is disabled. The server will see the original IP address as the source IP address.
- SNAT: Specific or all original IP addresses are mapped to a single translation or pool of translation addresses (SNAT pool).

- Automap: The system automatically selects one of the self-IP addresses (typically a floating self-IP address of the egress VLAN) and maps it to the original IP address or addresses specified during SNAT creation. In this case, a translation address does not need to be specified explicitly.

Traffic Flow (with SNAT)

With SNAT, the traffic flow is normalized, and the connection starts working again. Thus, this scenario is one of the most commonly deployed (Figure 20).

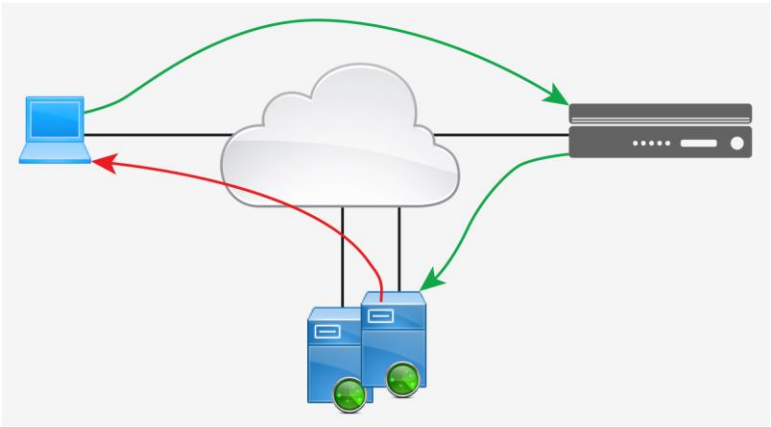
Figure 20: Traffic Flow with SNAT



Traffic Flow (without SNAT)

Without SNAT, the traffic flow will be asymmetric. and the F5 device will block the next packet and so the design shown in Figure 21 will not work.

Figure 21: Traffic Flow without SNAT



In APIC and F5 integration, if Source Address Translation is configured as None, you must configure the server default gateway back to BIG-IP.

Appendix A: Using EPGs to Attach F5 Devices

F5 Device Attached as an EPG

Cisco ACI EPGs provide a new model for mapping applications to the network. Rather than using forwarding constructs such as addresses or VLANs to apply connectivity and policy, EPGs use a group of application endpoints. EPGs act as containers for collections of applications or application components and tiers that can be used to apply forwarding and policy logic. They allow separation of network policy, security, and forwarding from addressing and instead apply these to logical application boundaries.

The use of the EPG as a subnet is one of the methods for mapping applications to the Cisco ACI fabric. Rather than redesigning the application layout for a given application, existing subnets can be configured as EPGs. All devices in the assigned IP address range will become members of the EPG and receive consistent policy.

This model is consistent with the ADC service appliance deployment model, which uses the IP subnet to identify and apply policy to traffic. Policy will be applied based on the EPG which is equal to the original subnet. Additionally, this model supports quick and straightforward migration to Cisco ACI fabric

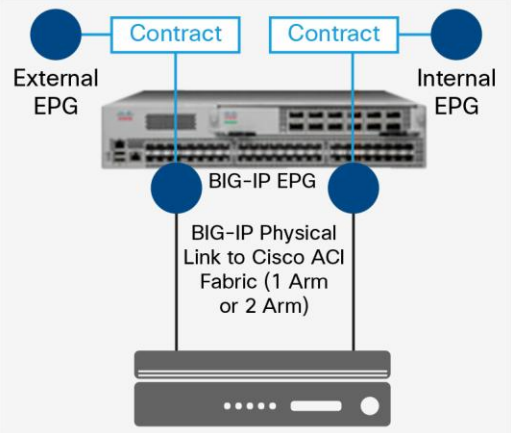
In this deployment model, the F5 device is not inserted as a Layer 4 through 7 service; rather. it is inserted into the network as an endpoint. Any BIG-IP equipment can be used (physical device or Virtual Edition), and any BIG-IP topology (one arm or two arm) can be deployed. BIG-IP is configured (according to best practices) and managed out of band (traffic passes through the Cisco ACI fabric, but the APIC does not control provisioning and management).

EPG Attachment Methods

Layer 2 within the Fabric

BIG-IP is connected to one of the leaf nodes in the network in one-arm mode or two-arm mode. All configuration on BIG-IP is performed out of band. The APIC does not control any configuration on the BIG-IP. The APIC in this case controls the network and the flow of traffic to and from BIG-IG. This control is achieved using the concept of EPGs and contracts between those EPGs that enable communication (Figure 22).

Figure 22: Contracts between EPGs



Outside Layer 2 and 3 Networks

The Cisco ACI solution allows users to use Layer 3 technology (standard IP) to connect to outside networks. You can use Cisco ACI to:

- Connect to an existing switch network infrastructure and provide a Layer 3 connection between workloads in the Cisco ACI fabric and workloads outside the Cisco ACI fabric
- Connect to WAN routers in the data center so that a WAN router provides Layer 3 data center interconnect (DCI) or Internet access for tenants; in some scenarios, a WAN router provides VPN connection to a tenant's on-premises network

The Cisco ACI solution also provides options to allow users to use Layer 2 technology to connect the Cisco ACI fabric to an existing Layer 2 network.

Layer 2 connection between a Cisco ACI fabric and an outside network is required in the following scenarios:

- In the existing data centers, connect the existing switching network to a Cisco ACI leaf, and stretch the same VLAN and subnet across Cisco ACI and the existing network. This approach allows workloads to be distributed across the existing switching infrastructure and Cisco ACI fabric. Customers also can choose to migrate the workloads from the existing networks to the Cisco ACI fabric.
- Extend the Layer 2 domain from Cisco ACI to a DCI platform so that the Layer 2 domain of Cisco ACI can be extended to a remote data center.

BIG-IP can be connected to the fabric using any of these methods. The deployment option used depends on the customer's network needs and environment.

For more information, refer to the white paper Connecting Application Centric Infrastructure (ACI) to Outside Layer 2 and Layer 3 Networks.

High-Availability Trigger Mechanisms

A redundant BIG-IP system is a configuration that allows traffic processing to continue if a BIG-IP system becomes unavailable. A BIG-IP redundant system consists of two identically configured BIG-IP units. When an event occurs that prevents one of the BIG-IP units from processing network traffic, the peer unit in the redundant system immediately begins processing that traffic, and users experience no interruption in service.

You can configure the units of a redundant system to run in either of two redundancy modes:

- Active-standby mode: With active-standby mode, only one of the two units is in an active state, processing traffic, at any given time. The inactive unit serves strictly as a standby unit, becoming active only if the active unit becomes unavailable. When a standby unit becomes active, it normally remains active until an event occurs that requires the other unit to become active again, or until you specifically force it into a standby state. Active-standby mode is the recommended mode for redundant system configuration.
- Active-active mode: With active-active mode, both units are in an active state simultaneously, each processing traffic for different virtual servers or SNATs. If an event prevents one of the units from processing traffic, the other unit begins processing that unit's traffic in addition to its own.

To enable a unit to fail over to its peer unit, you must first specify the type of failover that you want the redundant system to use. The two possible failover types are hard-wired failover and network-based failover.

- Hard-wired failover: When you configure hard-wired failover, you enable failover by using a failover cable to physically connect the two redundant units. This is the default setting.
- Network failover: When you configure network failover, you enable failover by configuring your redundant system to use the network to determine the status of the active unit. You can use network failover in addition to, or instead of, hard-wired failover.

When network failover is used for high availability with BIG-IP and Cisco ACI integration, the interfaces used to trigger the failover can carry in-band or out-of-band traffic (of the Cisco ACI fabric), or both. Multiple interfaces can be used to determine whether the network failover should occur (some of the interfaces can be passing traffic in band, and some of the interfaces can be passing traffic out of band; the management interface can also be used to determine network failover).

Consider using MAC masquerade addresses to:

- Reduce Address Resolution Protocol (ARP) communication or dropped packets during traffic group failover events
- Improve reliability and failover speed in lossy networks
- Improve interoperability with switches that are slow to respond to gratuitous ARP requests

For more information and configuration details, refer to SOL13502: Configuring MAC masquerade (11.x).

F5 (NASDAQ: FFIV) provides solutions for an application world. F5 helps organizations seamlessly scale cloud, data center, and software defined networking (SDN) deployments to successfully deliver applications to anyone, anywhere, at any time. F5 solutions broaden the reach of IT through an open, extensible framework and a rich partner ecosystem of leading technology and data center orchestration vendors. This approach lets customers pursue the infrastructure model that best fits their needs over time. The world's largest businesses, service providers, government entities, and consumer brands rely on F5 to stay ahead of cloud, security, and mobility trends. For more information, go to f5.com.

C11-735490-00 07/15