TOMORROW starts here.
F5 Demystifying Network Service Orchestration and Insertion in Application Centric and Programmable Network Architectures

Jeffrey Wong - Solution Architect
F5 Networks

February, 2015
Agenda

• F5 Synthesis Overview
• ACI L4 –L7 Service Insertion Overview
• F5 Device Package Release 1.1.0 Details
• F5 BIG-IP LTM Integration with Cisco ACI
• Workload Migration from Traditional Networks to Cisco ACI
• F5 BIG-IQ Integration with Cisco ACI
F5 Synthesis Overview
Impact on Data Center Architecture: Applications

**MICRO-ARCHITECTURES**

Each service is isolated and requires its own:
- Load balancing
- Authentication / authorization
- Security
- Layer 7 Services
- May be API-based, expanding services required

More applications needing services

**API DOMINANCE**

Proxies are used in emerging API-centric architectures for:
- API versioning
- Client-based steering
- API Load balancing
- Metering & billing
- API key management

More intelligence needed in services
F5 and Cisco ACI Joint Solution Benefits

- Automated L4-L7 application service insertion
- Accelerated application deployments with scalable L4-L7 services
- Application agility & significant reduction in operating costs
- Preserves richness of F5 Synthesis offering. Ease of integration due to rich programmability
- Existing F5 Physical and Virtual appliances, topologies integrate seamlessly with Cisco ACI
- Maintains operational best practices & offers faster provisioning of workflows
F5 and Cisco ACI Integration – Latest Addition
Announcing APIC and BIG-IQ Integration Early Availability

APIC to BIG-IP Integration Model Phase 1
(Shipping)

APIC to BIG-IQ Integration Model Phase 2
(Early Availability Jan’15, FCS Q2 CY15)

Customers have choice to leverage Cisco APIC to BIG-IP or through BIG-IQ Integration Models
## Choosing F5 BIG-IP for Cisco ACI

**Supports 11.4.1 and above, Platform Independent**

<table>
<thead>
<tr>
<th>Good, Better, Best Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>F5 physical ADCs</strong></td>
</tr>
<tr>
<td>High-performance with specialized and dedicated hardware</td>
</tr>
<tr>
<td><strong>Physical ADC is best for:</strong></td>
</tr>
<tr>
<td>• Fastest performance</td>
</tr>
<tr>
<td>• Highest scale</td>
</tr>
<tr>
<td>• SSL offload, compression, and DoS mitigation</td>
</tr>
<tr>
<td>• An all F5 solution: integrated HW+SW</td>
</tr>
<tr>
<td>• Edge and front door services</td>
</tr>
<tr>
<td>• Purpose-built isolation for application delivery workloads</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Physical</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>F5 virtual editions</strong></td>
</tr>
<tr>
<td>Provide flexible deployment options for virtual environments and the cloud</td>
</tr>
<tr>
<td><strong>Virtual ADC is best for:</strong></td>
</tr>
<tr>
<td>• Accelerated deployment</td>
</tr>
<tr>
<td>• Maximizing data center efficiency</td>
</tr>
<tr>
<td>• Private and public cloud deployments</td>
</tr>
<tr>
<td>• Application or tenant-based pods</td>
</tr>
<tr>
<td>• Keeping security close to the app</td>
</tr>
<tr>
<td>• Lab, test, and QA deployments</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Hybrid</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical + virtual = hybrid ADC infrastructure</strong></td>
</tr>
<tr>
<td>Ultimate flexibility and performance</td>
</tr>
<tr>
<td><strong>Hybrid ADC is best for:</strong></td>
</tr>
<tr>
<td>• Transitioning from physical to virtual and private data center to cloud</td>
</tr>
<tr>
<td>• Cloud bursting</td>
</tr>
<tr>
<td>• Splitting large workloads</td>
</tr>
<tr>
<td>• Tiered levels of service</td>
</tr>
</tbody>
</table>

### F5 physical ADCs

- **VIPRION 2200**: 1Gbps, 3Gbps, 5Gbps, 10Gbps
- **VIPRION 2400**: 10Gbps
- **VIPRION 4480**: 1600 series*, 2000 series*, 4000 series, 5000 Series, 7000 Series, 10000 Series, 11000 Series, VIPRION 2200, VIPRION 2400, VIPRION 4480, VIPRION 4800

### F5 virtual editions

- **VIPRION 2200**: 1Gbps, 3Gbps, 5Gbps, 10Gbps
- **VIPRION 2400**: 10Gbps
- **VIPRION 4480**: 1600 series*, 2000 series*, 4000 series, 5000 Series, 7000 Series, 10000 Series, 11000 Series, VIPRION 2200, VIPRION 2400, VIPRION 4480, VIPRION 4800
ACI L4 – L7 Service Insertion Overview
Service Insertion In traditional Networks

Traditional Network Service Insertion

Challenges

Service insertion takes days

Network configuration is time consuming and error prone

Difficult to track configuration on services

Configure Network to insert Firewall

Configure firewall network parameters

Configure firewall rules as required by the application

Configure Load Balancer Network Parameters

Configure Router to steer traffic to/from Load Balancer

Configure Load Balancer as required by the application
APIC L4 – L7 Service Integration

- TENANT (HR)
- APPLICATION PROFILE (3 TIER APP)
  - EPGs are defined here
- NETWORKING POLICY
  - Connectivity for the tenant L2-L3
- SECURITY POLICY
  - (Policy decision is done here)
  - Filters, QoS, Traffic Steering
- TROUBLESHOOTING POLICY
  - SPAN, ERSPAN etc
- MONITORING POLICY
  - Events, SNMP
- L4-L7 SERVICES POLICY
  - Define L4-L7 service policy

**endpoint Group (EPG)** – collection of bare metal servers, VMs, vNIC
Ex: WEB EPG - all web servers (bare metal or VMs) are grouped into this EPG
Ex: APP EPG - all APP servers (bare metal or VMs) are grouped into this EPG

**Contract** – services between the WEB and APP EPG (web graph, HTTP graph)
Ex: APP is a provider and WEB is the consumer
Define services within a contract: FW, ADC in this example ADC defined
F5 Device Package: Definition

APIC requires a **Device Package** to communicate with service devices.

A **Device Package** is a zip file containing two parts:

**Device Specification (xml):** The configuration of the APIC is represented as an object model consisting of a large number of Managed Objects (MOs). A Device type is defined by a tree of MOs with a Meta Device (MDev) at the root.

**DeviceScript (py):** The integration between the APIC and a Device is performed by a DeviceScript, which maps APIC events function calls defined in Device Script.
Service Graph: Definition
Abstract graph concept mapping to Service Graph

- Service graph is an ordered set of functions between a set of terminals e.g.; Firewall Function, Load balancer Function
- A function has one or more connectors
- Network connectivity like VLAN/VNID tag is assigned to these connectors

- A function within a graph may require one or more parameters
- Parameters can be scoped by an EPG or an application profile or tenant context
- Parameter values can be locked from further changes

Service Graph: “web-application”

- Functions rendered on the same device

Consumes

- EPG - EXT

Terminals

Firewall params
Permit ip tcp * dest-ip <vip> dest-port 80
Deny ip udp *

Connectors

SSL params
Ipaddress <vip> port 80

Terminals

Provides

- EPG - WEB

- WEB

Load-Balancing params
virtual-ip <vip> port 80
Lb-algorithm: round-robin

- EXT
Web Farm provide services to External Users; Policy Contract defines relationship between Web Farm and Users

Users assign to EPG EXT
Web Farm assign to EPG WEB
Users accessing the Web Servers

Service Graph Insertion at the Policy Contract Subject level

Service Graph contains Function Nodes, Virtual Server is a Function Node

F5 BIG-IPs are Concrete Devices belong to a Logical Device Cluster that enables ADC as a Function Node within a Service Graph
Goals of APIC Service Insertion and Automation

- Configure and Manage VLAN allocation for service insertion
- Configure the network to redirect traffic through service device
- Configure network and service function parameters on service device
F5 and Cisco ACI Integration Models

APIC to BIG-IP Integration Model

APIC to BIG-IQ Integration Model
F5 ACI Device Package 1.1.0 is now Released!
Supports ACI FCS+3 version 1.0(2m)

- vCMP support (New with 1.1.0)
- Dynamic endpoint attach and detach (New with 1.1.0)
- Supports any BIG-IP LTM physical and virtual form factor running version 11.4.1 and above
- Device package can be downloaded from downloads.f5.com at no cost
- Does not require any new module installation on the BIG-IP
- Can leverage BIG-IQ as device management
- iRules (custom defined) that reside in common partition can be called by APIC
- BIG-IP is licensed and OOB management configured prior to APIC integration
- Supports Active / Standby High Availability model per APIC logical device cluster
F5 Device Package 1.1.0 Supported Functions

Functions

- Virtual Server
  - Layer 4 Server Load balancing
  - Layer 4 SLB with SSL offload
  - Layer 7 Server Load balancing
  - Layer 7 SLB with SSL offload
- Microsoft SharePoint

Parameters under Virtual Server

- Configuring Global and Tenant Self IP addresses
- Configuring Global and Tenant static routes
- Device Counters
- Server Pools
- TCP Optimizations (WAN/LAN/Mobile)
- HTTP optimization
- HTTP Security (Application protocol security)
- TCP connection multiplexing (One Connect)
- Validators and Creation of tenant OneConnect profiles
- iRules
- Validators and Creation of tenant acceleration profiles
- SNAT Pool management

More than 80% of F5 customers use the L4 SLB / L7 SLB / MSFT SharePoint / SSL offload hence 1st release targets these use cases
F5 Device Package 1.1.0: vCMP Guests Support

vCMP (Virtual Clustered Multiprocessing) is F5 purposed built hypervisor, allow multiple virtual ADC instances, called vCMP guests, reside on the same vCMP host.

In release 1.1.0; in vCMP HA configuration, both vCMP guests must reside on the same vCMP host.

Using vCMP guests as L4-L7 Devices when creating Logical Device Cluster:

vCMP guest 1 and 2 mgmt. IP
vCMP host mgmt. IP
F5 Device Package 1.1.0: vCMP Guests Support

vCMP and HA configuration under Concrete Devices specific configurable parameters

### vCMP guest 1 and 2 host name

- **vCMP guest 1**
- **vCMP guest 2**

### vCMP guests HA parameters

- **Host Name**
- **NTP Server**
- **Syslog Server IP Address**
- **Primary DNS IP Address**

### vCMP host mgmt. IP under device config as well

- **Device Interface**
- **Device Route**
- **vCMP host**

---

**CREATE L4-L7 DEVICES**

**STEP 2 > DEVICE CONFIGURATION**

<table>
<thead>
<tr>
<th>Features</th>
<th>BASIC PARAMETERS</th>
<th>ALL PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>HostName</td>
<td>vcmp1.bd.f5.local</td>
</tr>
<tr>
<td>NTP Server</td>
<td>NTPServer</td>
<td>192.108.75.100</td>
</tr>
<tr>
<td>Syslog Server</td>
<td>SyslogServerIPAddress</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PrimaryDNSIPAddress</td>
<td></td>
</tr>
<tr>
<td>Device Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Route</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCMP host</td>
<td>VcmpHost</td>
<td>172.31.21.55</td>
</tr>
<tr>
<td>VCMP Configuration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
F5 Device Package 1.1.0: Dynamic endpoint attach/detach

Pool members, which consider endpoint in ACI fabric, once “attached to” OR “detached from” an EPG; APIC will send notification to BIG-IP to add or remove this pool member.

- Internal Connector, which is tied to the provider EPG, assigns to the WEB servers = pool members in F5 LTM Pool.
- Enable Attachment Notification.
- Under Graph Template, function node ADC has two logical interfaces: external and internal.
F5 Device Package 1.1.0: Dynamic endpoint attach/detach

**BIG-IP Pool has no pool members**

No need to define pool members when adding configurable parameters to the service graph template.
F5 Device Package 1.1.0: Dynamic endpoint attach/detach

After receiving attach notification from APIC, BIG-IP add members to pool
Same for endpoint detach

Assign provider EPG (Web) to the servers
F5 BIG-IP LTM Integration with Cisco ACI
Using Device Package 1.1.0 and ACI 1.0(2m)
Terminology: APIC Tenant Single Context / BIG-IP Partition

A function node identifies a set of network service functions that are required by an application.

BIG-IP Virtual Server is equivalent to service graph function node.

Tenant is a container for policies (filters, contracts, bridge domains and application profiles).

BIG-IP partition is equivalent to a single context ACI tenant.
Terminology: APIC Service Graph Config pushed to BIG-IP

APIC Service Graph Function Node Config Parameters, for example, webPool, will be pushed from APIC to BIG-IP.

In this example, BIG-IP populates Pool configuration from APIC.
Device Package Feature: Referencing iRules

APIC can reference iRules that resides in BIG-IP Common partition

BIG-IP is responsible for iRules management, including creation / modification / validation
F5 supports **TRUE** Multiple Graph Multiple Tenancy

- Multiple Virtual Servers for different applications in the different BIG-IP partitions/APIC Tenants, sharing the same device
- Partition created by APIC inside BIG-IP is prefixed by the apic,”_” tenant-id to represent the partition in F5 (for ex: apic_5437)
- F5 demonstrate true multi-tenancy using different partitions for each tenant in APIC
- Each partition has been assigned individual route domain for L3 separation
- Virtual Servers created by APIC inside BIG-IP is prefixed by the apic,”_” tenant_id”_”graph (for ex: apic_5437_3456)
Mixed Mode Support

APIC Partition
Configuration pushed and populated by APIC. User does not modify this partition. APIC will perform L4-L7 service insertion on this partition.

BIG-IP created Partition:
User can continue to use partition created by BIG-IP, they appeared as separate EPG to APIC. Network functionality will be managed by APIC through the Fabric, where L4-L7 will be managed by BIG-IP. User can continue to use custom iApp and iRules in this scenario.

Common Partition
User can define custom iRules under Common partition and they can be called by APIC,

BIG-IP Physical or Virtual
F5 BIG-IP + Cisco ACI Integration Options

Cisco ACI + F5 BIG-IP without service insertion (using EPG)
Cisco ACI + F5 BIG-IP Integration using L4 – L7 service insertion using service graph
Mixed Mode: same BIG-IP connects to ACI fabric with and without L4-L7 service insertion

All the above Integration Options support 1-Arm / Inline; Physical / Virtual in HA deployment
Workload Migration from Traditional Networks to Cisco ACI
Migration: Physical Topology

Traditional Network

BIG-IP Platform

CISCO ACE

VIP Traditional

BIG-IP Platform

F5 DEVICE PACKAGE FOR APIC

ACI Fabric

VIP ACI

BIG-IP Platform

CISCO ACE

WEB
### Migration: Approach

**Clients access Traditional Network VIP**

**Expanding workload to ACI fabric**

**Moving workload from traditional network to ACI**

**Completing workload migration to ACI**

**Clients now access ACI VIP**

**Step 1:**
- Bring up BIG-IP in ACI fabric
- Create Application Server
- ACI L4-L7 service insertion with BIG-IP

**Step 2:**
- Add ACI VIP to Traditional Pool

**Step 3:**
- Move Servers

**Step 4:**
- Update DNS or GTM
- Remove ACI VIP From Traditional Pool
Migration: Logical Diagram

Wiki.mycorp.com = Traditional VIP

Wiki.mycorp.com = ACI VIP

F5 & Cisco Joint Whitepaper:
F5 BIG-IQ Integration with Cisco ACI
F5 and Cisco ACI Integration Models

APIC to BIG-IP Integration Model

APIC to BIG-IQ Integration Model
F5 is Industry Leader in Application Delivery

How can we provide full set of F5 functionality to ACI environment that is “application” focused?

F5 has an extensive library of iApps for deploying applications.
An iApps is an application-centric configuration template:

- User answers a few questions about deploying an application
- iApps translates answers into a set of configuration options
- iApps can touch almost all BIG-IP functionality
  - iRules, profiles, monitors, security policies, and much more ...
- There are many F5-provided iApps:
  - HTTP, Sharepoint, Exchange, VMware View, ...
- Users can build their own iApps
Using BIG-IQ to bring iApps to APIC

BIG-IP integration with APIC
1. Download device package from F5
2. Admin import device package to APIC
3. APIC sends config to BIG-IP directly

BIG-IQ integration with Cisco ACI
1. BIG-IQ expose iApps to BIG-IQ
2. BIG-IQ create custom device package
3. Admin import BIG-IQ device package to APIC
4a. APIC sends iApp config to BIG-IQ -> BIG-IP
4b. APIC sends Device config to BIG-IP
Reference Material

• F5 and Cisco ACI Solution Overview

• F5 SDAS and Cisco ACI Solution Brief

• Cisco Application Policy Infrastructure Controller (APIC)

• F5 BIG-IP LTM and Cisco ACI Integration white paper

• Cisco Validated Design (CVD) on F5 BIG-IP LTM and Nexus 9000 (Standalone)

• F5 BIG-IP: Workload Migration from Traditional Networks to Cisco Application Centric Infrastructure

• Follow us on Twitter @f5Networks ➔ Official F5 Networks Channel
DevCentral F5 User Community
Over 105,000 Members in 191 Countries and Growing!

References
- Wikis
- API/SDK Documentation

Resources
- Sample Code
- Tech Tips
- Forums
- Podcasts
- Blogs

Tools and Frameworks
- iRule Editor
- iControl SDK
  - .NET, Java, Python, Powershell, ...
- VMware vSphere Management Plug-in
- Microsoft SCOM Monitoring Pack
Key Takeaways

• F5 Software Defined Application Services (SDAS) vision perfectly aligns with Cisco’s Application Centric Infrastructure
• How Cisco ACI solves network services insertion challenges
• How F5 BIG-IP LTM integrates into Cisco ACI architecture
• Key benefits of BIG-IP / ACI model:
  ➢ Multi-Tenancy, Multi-Graph Support
  ➢ Use Case Focus
  ➢ Automation Ready
  ➢ Application level visibility and monitoring
• F5 iApps Integration with Cisco ACI using BIG-IQ bringing application requirements to ACI policy

If I can be of further assistance please contact me:

Jeffrey Wong (j.wong@f5.com)
Solutions for an application world.