Segmenting Complex Environments Using Cisco ACI

JULY | 2019

Presented by Peter Zhang
Technical Solutions Architect

World Wide Technology
www.wwt.com

Table of Contents

Abstract

Application Centric Infrastructure (ACI) is Cisco's software-defined networking (SDN) solution for data center and cloud networks. ACI is a powerful technology offering rich features for SDN to include application-centric security segmentation, automation and orchestration in the data center. Implementing application-centric design to specifically meet a segmentation strategy and a zone architecture requires a different approach and is referred to as the hybrid model. The hybrid model is necessary because of the unique challenges segmentation brings in terms of limitations with applications, how to address shared resources, performing discovery and overall security requirements.

ACI places endpoints into a logical endpoint group (EPG) and applies security enforcement for the entire group to ensure consistency. Many deployments of ACI rely upon the "network-centric" configuration model that maps legacy VLANs, EPGs and subnets in a 1-to-1-to-1 relationship. As a contrast, "application-centric" design of ACI deploys EPGs modeled on applications' architectures, rather than subnets and network structures. This paper will provide insight on the design model, which will allow easier segmentation of applications while ensuring mobility of endpoints.

Business Justification

There is a significant increase in the demand for businesses to protect high-value data along with the associated critical systems. This is evident by newly defined compliance and regulatory language mandating protection of sensitive data and applying layers of security enforced through segmentation techniques. What was once considered an IT challenge is now at the center of business-driven requirements and necessitates an enterprise level of segmentation.

From an IT security viewpoint, the core of protecting sensitive data more than likely translates into enhanced controls to and/or around the applications. While those controls can vary widely, security at the network layer that transcends into application-centric architecture is usually the first layer of protection.

An advanced networking technology, ACI can provide the enhanced security and first line of protection, if properly implemented. The reality is, traditional networks are not designed based on application architecture, and adopting ACI application-centric model in large brown-field data center environments can present multiple challenges. Addressing these challenges requires a different ACI design approach, and the hybrid model is an alternative. This paper presents the hybrid migration model intended to address the core issues when migrating to application-centric design.

The hybrid model provides key advantages by addressing the following challenges:

- **IP re-addressing** – Application and system owners often find it challenging to change the IP addresses without rebuilding those applications due to compounded complexity over years. The hybrid model helps eliminate or reduce the need for re-IP.

- **Shared/Common applications** – Some systems often provide services to multiple applications such as a shared SQL database. By deploying an ACI hybrid model, you can leave the shared services in network-centric EPGs until a plan is formed to separate those services into their own application-centric EPGs.

- **Lack of Application Dependency Mapping (ADM) Software** – Understanding the flow of applications can be challenging due to insufficient flow data. The hybrid model deploys an "application-centric first and segmentation-after" methodology to allow you to capture flows without having to deploy a full ADM solution.

- **Migrate from Network Centric to Application Centric** – The hybrid model emphasizes on the co-existence of network-centric and application-centric design. Such design increases flexibility in terms of both timeline and resources availability, which allows you to migrate at your own pace.

- **Application-centric Security** – Segmentation of applications does not have to happen overnight. Traditional networking usually enforces minimal segmentation for east/west traffic in the data center. The hybrid model utilizes multiple ACI features to ensure both the blacklist model and whitelist model can co-operate, while allowing seamless security transitions between them.

ACI Design Overview

There are two main components involved in ACI when designing a hybrid model:

- Underlying network infrastructure
- Transport and session of applications

By separating these two components, your fabric becomes more flexible, which essentially enables you to build a fabric that not only can provide segmentation for application, but also maintains the same network operational model as in traditional networking.

The following sections briefly describes three states:

- Network-centric state: similar to typical network-centric deployment.
- Transitional state: both network-centric and application-centric EPGs co-exists.
- Final state: applications are segmented with all application-centric EPGs.

INITIAL STATE – NETWORK-CENTRIC MODEL

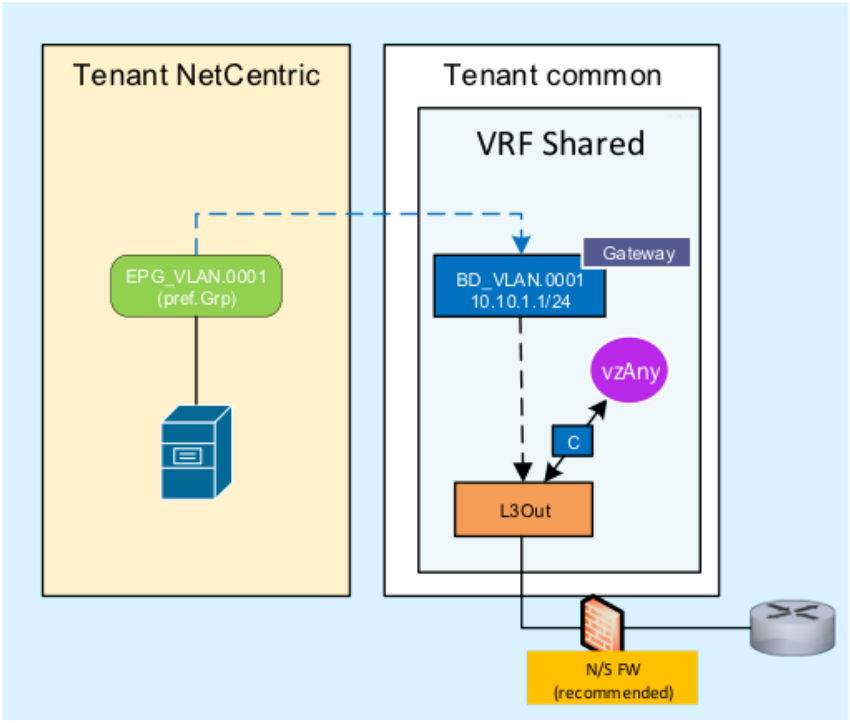

Figure 1: ACI Network Centric

For brownfield ACI, network-centric design are first built with workloads and gateways migrated into ACI. The fabric will form layer 3 adjacency with an external firewall or router in order to exchange routes. In the above figure, note the following:

- Typical network-centric EPGs models where 1 VLAN = 1 BD = 1 EPG.
- Network structure is built in tenant common, rather than in the same tenant as the network-centric EPGs.
- A N/S firewall is highly recommended because it enhances perimeter security for ACI while reducing the amount of hardware resources need on border leafs.
- All EPGs are created with preferred group membership with network-centric naming convention.
- L2 extensions are not mentioned in the diagram. However, they should be built with bridge domain extension instead of EPG extension for the following reasons:

    1. Provides extra flexibility when multiple EPGs need to leverage the same L2out extension.
    2. L2 segmentation control if needed between external EPGs and internal EPGs.
    3. Internal EPGs can use different encapsulation as the external L2 Extended EPG. This also helps reduce BPDU flooding from L2 environment into ACI. (BPDUs are flooded within encapsulation, rather than bridge domain).

TRANSITIONAL STATE – APPLICATION-CENTRIC + NETWORK-CENTRIC

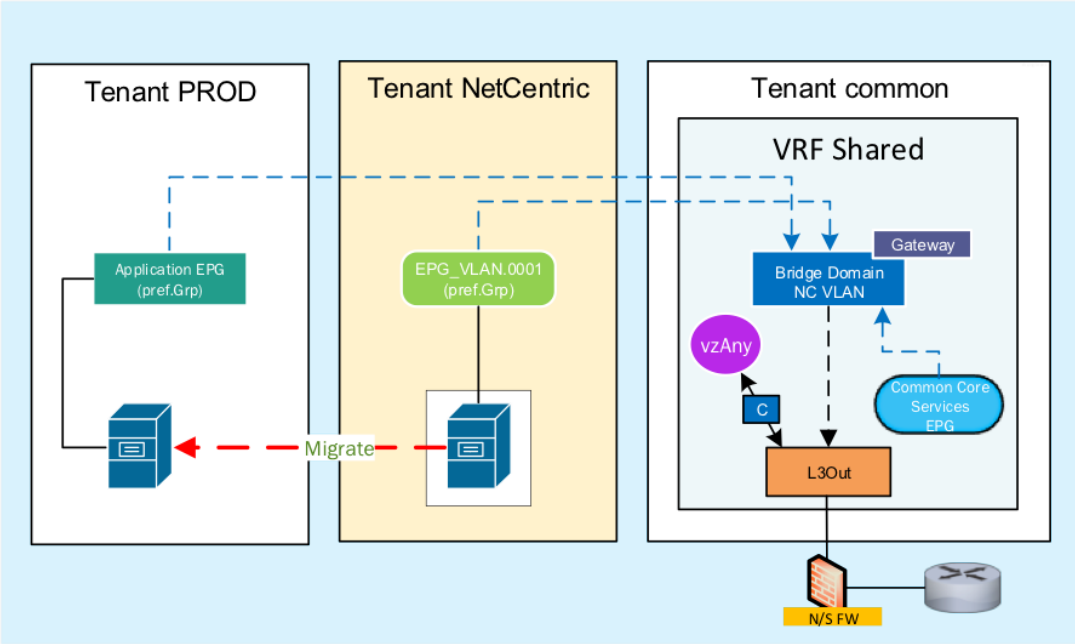

Figure 2: ACI Transitional State

In a transitional state, you can create new application-centric EPGs in a new application-centric tenant and migrate workloads into them from network-centric EPGs. Note the following key design concepts:

- Network-centric EPGs and application-centric EPGs share the same underlying network infrastructure.
- Application EPGs and network-centric EPGs communications are governed by ACI contracts.
- Core services EPGs resides in tenant common to enable sharing across tenants when needed.

FINAL STATE – APPLICATION-CENTRIC EPG WITH SEGMENTATION

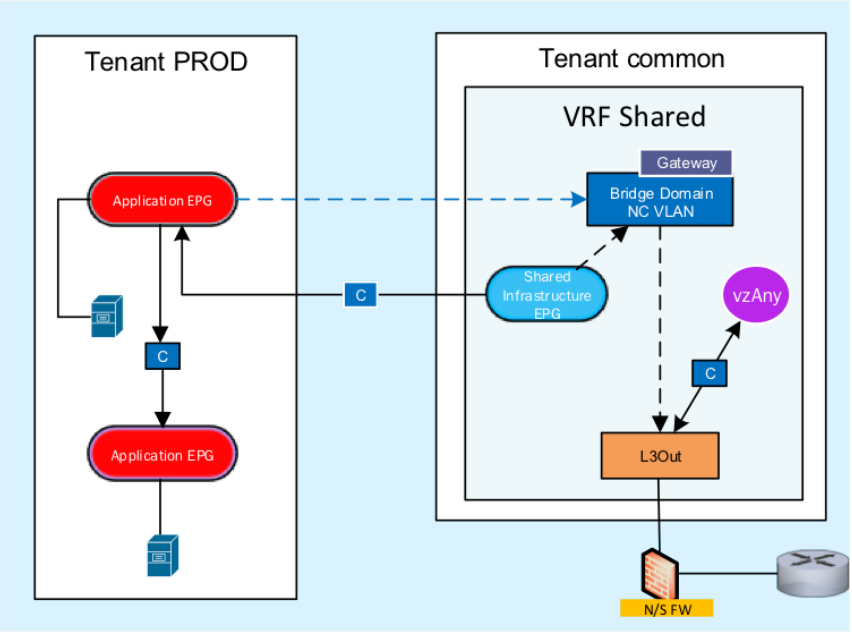

Figure 3: ACI Application-Centric Model

The above diagram illustrates a final state where only application-centric EPGs remain. The network structure is still the same as day one when the fabric was initially built. EPG to EPG communications are all controlled via ACI contracts where no "preferred group" EPGs exist anymore.

APPLICATION DEPENDENCY MAPPING (ADM) OVERVIEW

ADM is a critical process for any network segmentation effort, more importantly, ADM is deployed in data center operation to reduce response time to threats with real-time monitoring of events, as well as integrating ADM systems with automation and orchestration. There are generally two levels/processes for ADM efforts: application discovery and flow discovery.

APPLICATION DISCOVERY AND ACI LOGICAL STRUCTURE

Application discovery is the process of building application profiles based on tiers involved for any given application. The application discovery process usually encompasses the following:

- Review/collect CMDB information.
- Review application architecture.
- Interview application owners and stakeholders.

The output of this process will help creating ACI ANPs and EPGs, as well as for building logical structures for within ADM software such as Illumio and Tetrations.

For "tenants," it is recommended to be created based on business units and administrative management requirements of the tenants. Here are some examples of tenancy:

- Service providers where customers = tenants.
- Separate internal business units, such as HR, IT, finance = tenants.
- Separate infrastructure environments, such as Dev, Prod, QA = tenants.
- Company acquisitions and mergers, such as CSCO, ANET, PANW = tenants.
- Separate IAAS, such as Openstack, Redshift = tenants.
- Separate DMZ from other infrastructure, such as DMZ = tenants.
- Separate security compliance tenant, such as HIPAA, PCI = tenants.
- ACI net-centric to future app-centric deployment and common tenant is leveraged.

APPLICATION FLOW DISCOVERY

Flow Discovery is the process to monitor and collect raw traffic flows on the wires via ADM software or via "ACI Telemetry (EX+)." The minimum flow data attributes needed are "source," "destination," "protocol" and "port." The flow data will also need to be classified into application profiles built during application discovery phase. For example, the following flow maybe discovered:

Source IP	Destination IP	Protocol	Port
10.10.10.1	10.10.20.99	TCP	443

Table 1: Application Flow Example

Based on application discovery process, the following was created:

Application	Tier	IP addresses
ScienceLogic	Probe	10.10.10.1
wwt.com	Web	10.10.20.99

Table 2: Application Discovery Example

You can now map the flow discovered to the application discovered in the following format:

Application	Tier	IP addresses	Provide	Consume
ScienceLogic	Probe	10.10.10.1		HTTPS (443)
wwt.com	Web	10.10.20.99	HTTPS (443)	

Table 3: Map Data between Application and Flow

The application discovery data will then be mapped to EPGs and the flow data will be translated into filters in ACI or firewalls, for building ACLs.

It is important that the raw data be refined:

- Flows should be de-duplicated.
- All data should be at least 30 days+ old to cover monthly jobs/activities.
- Security team should review the data and confirm that they are valid prior to implementation.

Conclusion

The hybrid model allows smooth transition to ACI application-centric and segmentation by addressing some of the major challenges. This includes greenfield deployment such as re-IP, shared services or lack of flow data.

The hybrid model also offers a path to separate systems running multiple services that require different security posture, which is often the case on systems that have always operated in a flat network with no internal firewalls. By using the hybrid model, you can stand up the same services on separate physical servers without affecting current applications.

For large segmentation efforts, it is best to breakdown a complex project into smaller and manageable phases, instead of performing large amount of work up front, which is challenging in a dynamic environment.

Do not let the complexity of ACI application centric stop you from taking full advantage of this SDN technology. After all, the investments made are for building a robust and dynamic network for the application and the business; let's not stop at only network centric.