Cisco live!
July 10-14, 2016 • Las Vegas, NV

Your Time Is Now
Security Best Practices for ACI

Navaid Shamsee
BRKACI-2303
Agenda

• Introduction
• Security Architecture
• ACI Overview
• ACI Fabric Security
• Role Based Access Control
• Segmentation for Security

• Visibility
• Implementing Advanced Security
• Design Practices
• Conclusion
Introduction
Cyber attacks are increasing in number and complexity

- Millions of email accounts compromised in massive data breach that includes Google and Yahoo
- Hackers pilfer $10 million from Ukraine Bank
- Data breach authority Verizon Enterprise breached; 1.5 million customers impacted
- Massive Acer security breach exposes highly sensitive data of 34,500 online shoppers
- University of Calgary paid $20K in ransomware attack
- UAE InvestBank hacked, nearly 100k recycled data records leaked?
- Indonesia, South Korea central bank websites hit by cyber attacks; no losses
- Over 25,000 IoT CCTV cameras used in DDoS attack
- 32 million Twitter logins put up for sale
The Challenges Come from Every Direction

- Sophisticated Attackers
- Dynamic Threats
- Complex Geopolitics
- Complicit Users
- Boardroom Engagement
- Misaligned Policies

Defenders
Use a Threat-Centric and Operational Security Model

Before
- Discover
- Enforce
- Harden

During
- Detect
- Block
- Defend

After
- Scope
- Contain
- Remediate

Visibility and Context
- Firewall
- Patch Mgmt
- IPS
- IDS
- AMD
- App Control
- Vuln Mgmt
- Anti-Virus
- FPC
- Log Mgmt
- VPN
- IAM/NAC
- Email/Web
- Forensics
- SIEM
Cisco: Covering the Entire Continuum

Attack Continuum

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

ASA
NGFW
Secure Access + Identity Services

VPN
Meraki

NGIPS
ESA/WSA
CWS

Advanced Malware Protection
Cognitive
ThreatGRID

FireSIGHT & PXGrid

Services
How to Defend…

- **Breach**: Understand scope, contain & remediate
- **Threat**: Focus on the threat – security is about detecting, understanding, and stopping threats
- **Control**: Set policy to reduce surface area of attack
- **Visibility**: Broad awareness for context

APIs  Workflow (automation) Engine
Security Architecture
TRENDS IMPACTING DATACENTER SECURITY

EVOLVING THREATS

NEW APPLICATIONS (PHYSICAL, VIRTUAL AND CLOUD)

NEW TRAFFIC TRENDS

Source: Cisco Global Cloud Index, 2012
Right SECURITY architecture for NEXTGEN data center?

PERIMETER CENTRIC
- Manual and Complex
- Static Topology
- Error-Prone
- Limited Places

VIRTUALIZATION CENTRIC
- No Physical Support
- Management Complexity
- Limited Visibility

APPLICATION CENTRIC
- Any workload and any place
- Automated
- Full Visibility
Cisco SAFE recommends a phased methodology of building Security Solution

1. Requirement Phase / Security Capabilities
   - Identify security capabilities based on business goals, risks, policies, and threats.

2. Architecture phase
   - Create logical architecture based on the required capabilities in previous phase

3. Design phase
   - Create a design using the architecture
   - Identify products, configuration, services and cost.
Requirements Phase

COMPLIANCE
How do I maintain compliance in the cloud and mobile era?

RISK MITIGATION
How do I pro-actively detect and mitigate new attacks?

AUTOMATION
How can I simplify management across my IT?
Architecture Phase
Design Phase

Tenant

VRF-1

Bridge Domain-1

Zone-1 VRF

WEB1 uEPG

APP1 uEPG

DB1 uEPG

VRF-2

Bridge Domain-2

Zone-2 VRF

WEB2 EPG

APP2 EPG

Bridge Domain-3

VRF-3

Bridge Domain-4

Zone-3 VRF

WEB3 EPG

APP3 EPG

Bridge Domain-5

10.1.1.1/24

10.1.2.1/24

10.1.3.1/24

10.1.4.1/24

10.1.5.1/24

10.254.1.1/29

10.254.2.1/29

10.254.3.1/29

10.254.4.1/29

Firepower 9300
For more information on security architecture

Cisco SAFE Blueprint

Cisco Security Control Framework
ACI Overview
What is ACI?

Cisco’s Software Defined Networking (SDN) Solution to enhance business agility, reduce TCO, accelerate data center application deployments by automating IT tasks.
What is ACI?

Configuration → Policy Model

Controllers + APIC

Switches + Nexus 9000
The ACI Fabric - Topology

Spine Switches

Leaf Switches

APIC

APIC

APIC
The ACI Fabric – IS-IS

L3 Fabric
Routed links
(IP unnumbered)
IS-IS Level 1

VXLAN

Default Gateway
Server-1
Server-2

Default Gateway
Server-n
The ACI Fabric - Inside & Outside

**Inside**
Forwarding policy for ‘inside’ EPG’s defined by associated bridge domain network policies

MP-BGP is used to distribute external routes within the fabric.

**Outside**
‘Outside’ EPG associated with external network policies (OSPF, BGP, … peering)

MP-BGP is used to distribute external routes within the fabric.
The APIC – Northbound Interface

API

GUI

CLI

REST API
The APIC – Southbound Interface

OpFlex

ACI-enabled Fabric devices

Device Package

L4-7 Scripting APIs

ACI-enabled Fabric devices
- Open vSwitch
- Cisco
- Microsoft Hyper-V

L4-7 Scripting APIs
- f5
- Citrix
The Policy Model

- **Logical Model**: Contains policy defined by administrator
- **Resolution Model**: Intermediary format between APIC and network node
- **Concrete Model**: Device specific implementation of logical model
ACI Terminologies

Tenant-A

Private Network-1
- Bridge Domain-1
  - Subnet-1
  - EPG-A
  - EPG-B
  - EPG-C
- Bridge Domain-2
  - Subnet-2
  - EPG-D

Private Network-2
- Bridge Domain-3
  - Subnet-3
  - EPG-E
- Bridge Domain-4
  - Subnet-4
  - Subnet-5
  - EPG-F

Tenant-B

Private Network-3
- Bridge Domain-5
  - Subnet-6
  - Subnet-7
  - EPG-A
  - EPG-B
  - EPG-C
  - EPG-D
  - EPG-E
  - EPG-F

Customer / Group / BU
- Routing Table
- VRF
- L2 Boundary
- IP Space(s)
- Groups of end points
Management Information Model

- Solid lines indicate objects below contained
- Dashed lines indicate a relationship
- 1:n indicates one to many
- n:n indicates many to many
For more information on ACI

ACI

Related sessions:
BRKACI-2008 - A Technical Introduction into ACI
BRKACI-2004 - How to setup an ACI fabric from scratch
BRKACI-2102 - ACI Troubleshooting
ACI Fabric Security
ACI Fabric Security

- Whitelist Security Model
- APIC Hardening
- APIC Northbound Protocols
- APIC Northbound Authentication
- Two Factor Authentication

- APIC to Switch Authentication and Encryption
- NXOS Image Signing and Verification
- COOP Authentication
- Audit Logs for all Changes
- Security Certifications
Whitelist Security Model

Outside → Web
  - Allow TCP 80
  - Allow TCP 443

Web → App
  - Allow TCP 443

App → DB
  - Allow TCP 1434

ACI Fabric

APIC
APIC Hardening

• Hardened OS CentOS 6.5 (Future CentOS 7.2)
• Only open TCP ports are 22, 80, 443
• Port 80 is redirected to 443
• API Throttling (transactions/sec)
APIC Northbound Protocols

• HTTP/HTTPS for GUI or REST API
  - Webtoken login (username & password)
  - X.509 certificate login (username & X.509 certificate)

• CLI over SSH
  - Standard SSH login (username & password)
  - Password-free login (username & public key)
APIC Northbound Authentication

- APIC Local authentication
- External RADIUS
- External TACACS+
- External LDAP and Active Directory
Two Factor Authentication

- ACI and Symantec Integrated 2-factor Authentication

APIC to Switch Authentication and Encryption

APIC-to-APIC, and APIC-to-Switch Authentication

1. Establish SSL connection and exchange public key certificates
2. For additional security, shared secret or device serial number can be optionally exchanged
3. After successful validation, connection is ready
4. Messages are authenticated with HMAC digest
**NXOS Image Signing and Verification**

- **Generate Hash (SHA512)**
  - Using ACI RSA 2048 Private Key

- **Create Signature (RSA-2048 bit)**

- **Signed Image Verification on Switch Sup & LCs**
  - Extract signature from image
  - Compare Hash with Image SHA512 Hash

- **FIPS-140-2 compliant build system**
  - Development Key
  - Release Key
  - Revocation Key

- **Image Download**
  - Switch Image
  - TPM Chip
  - Secure Key Store

- **Leaf/Spine Switch**
  - ACT2 HSM
COOP Authentication

Council of Oracle Protocol (COOP) is used to communicate the mapping information (location and identity) to the spine proxy.

Two ZMQ authentication modes:

**Strict mode:** MD5 authenticated ZMQ connections only.

**Compatible mode:** MD5 authenticated and non-authenticated ZMQ connections

```
apic1# configure
apic1(config)# coop-fabric
apic1(config-coop-fabric)# authentication type ?
compatible  Compatible type
strict      Strict type
apic101-apic1(config-coop-fabric)# authentication type strict
```
Audit Logs for all Changes

Audit-logs are native to the ACI object model. Audit-logs contain:

- The object that was affected by a change
- What changed, Time stamp, user who made the change, the trigger, etc.
Port Security

- Limits the number of mac-addresses learnt on a bridge-domain port of ACI leaf switch.
- Supported on newer leaf switches (-E)
- MAC addresses on port are exceeding Maximum Endpoints setting:
  - Learning is disabled
  - New mac-address not added to CAM
  - Traffic is dropped for new MAC
  - Generate 1 syslog entry for violation action
## Security Certifications

<table>
<thead>
<tr>
<th>Certification</th>
<th>NXOS N9K Standalone</th>
<th>ACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI</td>
<td>N/A</td>
<td>Done</td>
</tr>
<tr>
<td>UC APL</td>
<td>Done</td>
<td>Q4 CY16</td>
</tr>
<tr>
<td>Common Criteria</td>
<td>Target Complete Feb 16</td>
<td>Q3 CY 16</td>
</tr>
<tr>
<td>FIPS</td>
<td>Done</td>
<td>Q4 CY16</td>
</tr>
<tr>
<td>NIST</td>
<td>Done</td>
<td>Planning</td>
</tr>
</tbody>
</table>
For more information on ACI fabric security:

Cisco Application Centric Infrastructure Security: Chain of Trust White Paper
Role Based Access Control
Role Based Access Control

- Controlling user access according to their specified roles
- Control READ and WRITE for ALL Managed Objects
- Users with different roles get selective Access to MIT Managed Objects
Configuring Role Based Access Control

Roles
- admin
- fabric-admin
- tenant-admin
- vmm-admin

Privileges
- fabric-equipment
- tenant-epg
- vmm-connectivity
- nw-svc-device

AD/LDAP
- RADIUS
- TACACS+
- Local

User

What user can do
- readPriv
- writePriv

Security Domains

Which subtree the role applies
- Fabric
- Common
- Tenant A
- Tenant B
- Managed Information Tree (MIT)
Tenant A

Domain: TenantA, Roles: Admin-Write

Domain: Common, Roles: read-only

Tenant Domains

Shared Policies Domain

Fabric Infra Domain

 Tenant A-admin

Domain: TenantA, Roles: Admin-Write

Domain: Common, Roles: read-only
RBAC Rules

• Normal RBAC functionality grants access to all instances of classes of objects under the tenant subtree.

• RBAC rules allow granular control on top of existing RBAC framework

• Example: Tenant A has two firewalls with following RBAC requirements:

  **fw1-admin**: Write access on FW1
  • Domain TenantA: read-all privileges
  • Domain sd-fw1: fw1-admin WRITE privileges

  **fw2-admin**: Write access on FW2
  • Domain TenantB: read-all privileges
  • Domain sd-fw2: fw2-admin WRITE privileges
RBAC Rules

- RBAC Rules are additive and associative.
- Cannot be negative/blocking rules.
- Require knowledge of the DNs of resources.
- RBAC Rule DNs and Domains are validated only for format, not for existence.
- You can pre-create RBAC Rules prior to the creation of the DN object they refer to.
Segmentation for Security
Segmentation for Security

- Segmentation using EPGs
- Micro-Segmentation
- Intra-EPG Isolation
- Distributed Firewall (DFW)
Segmentation using EPGs

No communication between EPGs unless allowed by a contract

Contract defines how an EPG communicates with other EPGs

“Provided” by one EPG and “consumed” by another.

Subjects are used to build definition of communication between EPGs.

Subject is a combination of a **filter**, an **action**, and optional **label**

**Labels** allows greater flexibility in complex relationship definitions
Application Network Profile (ANP)

- Group of EPGs and the Contracts (policies)
- Defines which EPGs can communicate and how they communicate

**APPLICATION NETWORK PROFILE**

**One-way Contract**
- Users consume WEB services

**Two-way Contract**
- WEB & APP provide & consume services between each other

**One-way Contract**
- DB provides services to APP
Application Network Profile - Example

- **Outside**
  - NW Public
  - NW Private
    - subnet
    - subnet

- **EPG WEB**
  - web contract
  - provide
  - consume

- **EPG APP**
  - java contract
  - provide
  - consume

- **EPG DB**
  - sql contract
  - provide
  - consume

- **infra shared services**
  - consume

- **mgmt contract**
  - bd
  - provide

- **L3 context**
  - bd
  - bd
  - bd

---

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
Micro-Segmentation with ACI

2 Capabilities:
1. Micro-Segmentation
2. Intra-EPG Isolation

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address Filter</td>
<td>Network</td>
</tr>
<tr>
<td>IP Address Filter</td>
<td>Network</td>
</tr>
<tr>
<td>VNic Dn (vNIC domain name)</td>
<td>VM</td>
</tr>
<tr>
<td>VM Identifier</td>
<td>VM</td>
</tr>
<tr>
<td>VM Name</td>
<td>VM</td>
</tr>
<tr>
<td>Hypervisor Identifier</td>
<td>VM</td>
</tr>
<tr>
<td>VMM Domain</td>
<td>VM</td>
</tr>
<tr>
<td>Datacenter</td>
<td>VM</td>
</tr>
<tr>
<td>Custom Attribute (VMWare AVS/vDS only)</td>
<td>VM</td>
</tr>
<tr>
<td>Operating System</td>
<td>VM</td>
</tr>
</tbody>
</table>

Cisco live!
What is Micro-Segmentation? Example

CokeEPG = VM_name(Coke*)

1. ALL VMs can talk to each other in Base EPG
2. Admin creates CokeEPG policy for micro-segmentation
3. CokeEPG policy distributed via Opflex to HyperV/ESX
4. VM's VLAN gets changed to new CokeEPG VLAN
5. VMs in CokeEPG can’t talk to VMs in Base EPG anymore

57
Why is Intra-EPG Isolation Needed?

Problem

Intra-EPG Isolation Denies All Communication within an EPG

Solution
Micro-Segmentation and Intra-EPG Isolation

Hypervisor Agnostic Micro-segmentation
For Any Virtual Workload

Flexible Segmentation

Intra-EPG Isolation + Micro-segmentation
For Any Workload (Physical, Virtual)

Basic DC Segmentation

Network-Centric Segmentation

Service Level Segmentation

Attributes Based Micro-Segments
(DVS, AVS, Hyper-V Switch, OVS)

Virtual Switch (any)

Hypervisor

Quarantine Infected VMs With Guest OS = Linux

FW

FW

Intra-EPG Isolation + Micro-Segmentation

Quarantine Infected VMs

Intra-EPG Isolation

Local switching

Intra-EPG Isolation

Local switching

FW

FW

WEB

APP

DB

Quarantine Infected VMs With Guest OS = Linux
Distributed Firewall (DFW) on AVS

- Connection tracking support (TCP) on AVS
- DFW is only applicable to Virtual End Points.
- DFW is not applicable to system ports (vmkernel ports) and uplinks.
- Global (per AVS host) flow limit: 250,000
- Per Interface (End Point) flow limit: 10,000
- Aging Interval: Adaptive aging (5 minutes – 2 hours)
- States for a flow:-
  - STATE_SYN_RECV
  - STATE_SYN_ACK_RECV
  - STATE_ESTABLISHED
  - STATE_FIN_RECV
  - STATE_ESTABLISHED_ONE_DIR
  - STATE_2ND_FIN_RECV
  - STATE_FTP_DATA
Firewall Policies

- System creates Global *default* policies which can be changed by the user

- Global defaults can be overridden per VMM Domain:
  - Configure vSwitch policies under Attachable Entity Profile

- Firewall Policy Modes:
  - Disabled: Disables Firewall
  - Enabled: Enables Connection Tracking and Packet Drops in AVS
  - Learning: Enables Connection Tracking, but packets are not dropped on a miss
Stateful Contracts and Filters

- User can set *Stateful* bit while configuring filters for TCP traffic
- Reflexive ACL in the hardware is programmed to allow TCP packets only if ACK flag set.
Visibility
Visibility

• Endpoint Tracker
• Syslog
• SNMP version 2 & 3
• Cisco Tetration Analytics
End Point Tracker

- Endpoint tracker is located under Operations tab
- Find real time location of the endpoint: EPG, Node, Interface, Ecnap.
- Keeps history of endpoint movement with date and time stamp.
Syslog

- MOs with associated faults or stats have a scope
- Notifications for different scopes can be sent to different destinations
- Faults, Event Records and Audit Records can be dispatched using syslog, as well as callhome & SNMP traps
- Switches send syslog message directly to the destinations, APIC is not involved in forwarding switch syslog messages.
SNMP v2 & 3

- Following SNMP Features are supported on APIC:
  - SNMP Protocol v2c and v3
  - SNMP Traps (v1, v2c and v3)
- The SNMP agents run independently on Switches and APIC.
- The APIC MIBs are read-only. The SNMP Set operation is not supported.
- Each APIC must be monitored separately for SNMP MIBs.
- Each APIC provides MIB Objects local to it.
- Each switch must be queried independently to provide the monitoring information.
Cisco Tetration Analytics

Forensics: Every Packet, Every Flow, Every Speed

Application Insight

Policy Simulation and Impact Assessment

Automated Whitelist Policy Generation

Policy Compliance and Auditability
Cisco Tetration Analytics Architecture

Data Collection

- Host Sensors
  - VM
- Network Sensors
  - Cisco Nexus® 92160YC-X
  - Cisco Nexus® 93180YC-EX
- Third-Party Metadata Sources

Analytics Engine

- Tetration Telemetry
- Configuration Data

Cisco Tetration Analytics™ Platform

Visualization and Reporting

- Web GUI
- REST API
- Push Events
The Cisco Tetration Analytics Continuum
Persistent Visibility for Any Workload, 24 x 7

**Zero Trust**
- **Discover**: Centralized policy orchestration and distributed sensors
- **Enforce**: Secure multitenancy with whitelisting
- **Harden**: Per-application microsegmentation

**Visibility**
- **Detect**: Deep traffic visibility
- **Block**
- **Defend**

**Compliance**
- **Scope**: Network forensic analysis
- **Audit**: Network and security audit
- **Remediate**: Remediation of policy issues
For more information on Cisco Tetration Analytics

Visit Cisco Tetration Analytics Page:

Related sessions:

BRKDCN-2040: Tetration Analytics - Network Analytics & Machine Learning Enhancing Data Center Security and Operations

BRKACI-2060: Cisco Tetration: Data Center Analytics Deployment and Use Cases
Implementing Advanced Security
Advanced Security

- Advanced Security Controls
- Security Automation (Service Graph)
- Trustsec Integration
Cisco ACI and Cisco Advanced Security

Cisco Advanced Security – ASA / Firepower / AMP

- APIC integration
- Threat-Centric Protection
- Deep traffic inspection
- Real-time Threat Intelligence
- Dynamic Workload Quarantine
- Forensic Analysis

Native ACI Security

- Centralized Policy Automation
- Secure Multi-Tenancy with Whitelisting
- Attribute-Based Microsegmentation
- VM-Based Segmentation
- ACI Group Policy
- Industry Compliance Standards (PCI)

Cisco ACI + Cisco Advanced Security Advantages:

- Addresses key DC challenges: threat-centric, visibility, compliance
- Only complete Before, During, and After approach to threats
- Industry’s most comprehensive threat intelligence with TALOS
- Highest rated Next Generation Intrusion Prevention System*
- Highest rated Breach Detection System – 99.2% effective**

Cisco ASA FW and Management Features

- 1G/10G/40G ports, max 1024 VLAN tagged sub-interfaces
- Failover active/standby and Clustering active/active high-availability models
- Embedded Firepower Services (AVC, NGIPS, URL-filter, AMP)
- SDN (Cisco APIC) and traditional (Cisco ASDM and Cisco Security Manager) management tools
- Dynamic routing includes Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and Border Gateway Protocol (BGP)
- IPv6 inspection support, Network Address Translation (NAT) 66, 46, and 64
- REST API for programmed configuration and monitoring
- Cisco TrustSec® Policy Enforcement Point (PEP) with security group tag (SGT)-based access control lists (ACLs), plus inline-tagging capable
- Zone-based firewall, Equal-Cost Multipath, Policy-based routing, VxLAN support (VTEP)
- Multiple Context for customer segmentation (max 250 contexts)
- LAN-to-LAN and RA VPN (AnyConnect and Native RAVPN clients)
Cisco FirePOWER NGIPS Features

- Configurable Fail Open Interfaces
- Connection / Flow Logging, Network, User, and Application Discovery
- Traffic filtering / ACLs and Fastpath
- NSS Leading IPS Engine
- Comprehensive Threat Prevention
- Security Intelligence (C&C, Botnets, SPAM etc.)
- Blocking of Files by Type, Protocol, and Direction
- Basic DLP in IPS Rules (SSN, Credit Card etc.)
- Access Control: Enforcement by Application and User AD integration
- Switch, Routing, NAT Options, and ISE PxGRID integration
- URL Filtering, Malware Blocking, Continuous File Analysis, Malware Network Trajectory
- Firepower Management Center (fka. FireSIGHT or Defense Center)
Converging code for **Threat-Centric NGFW**

1. **ASA**
   - L2-L4 Stateful Firewall
   - Scalable CGNAT, ACL, routing
   - Application inspection

2. **FirePOWER**
   - Threat-centric NGIPS
   - AVC, URL Filtering for NGFW
   - Advanced Malware Protection

3. **Firepower Threat Defense (FTD)**
   - New converged NGFW/NGIPS image
   - Full FirePOWER functionality for NGFW/NGIPS deployments
   - ASA Datapath with TCP Normalizer, NAT, ACL, dynamic routing, failover functions
Firewall (FW)

- ASA

ASA

Data Center Gear

NGIPS

- FirePOWER

ASA + FirePOWER services

FTD Inline / Passive

NGFW

- Firepower Threat Defense

ASA + FirePOWER services

Simplifying NGFW Deployments

<table>
<thead>
<tr>
<th>Two Appliances</th>
<th>One Appliance – Two Images</th>
<th>One Appliance – One Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two Management Consoles</td>
<td>Two Management Consoles</td>
<td>One Management Console</td>
</tr>
<tr>
<td>ASA FW</td>
<td>ASA FW Code</td>
<td>Firepower Threat Defense</td>
</tr>
<tr>
<td>Network Stitching or ACI Service Graph Chain</td>
<td>FirePOWER NGIPS Service SFR Code</td>
<td>Threat-focused NGFW</td>
</tr>
<tr>
<td>FirePOWER NGIPS</td>
<td>ASA + FirePOWER (SFR)</td>
<td></td>
</tr>
</tbody>
</table>
Cisco ASAv

Hyper-V
Hyper-V Manager and PowerShell deployments
Generation 1 guests
- Microsoft Windows

VMware
vSphere client, ovsftool, and
vCenter OVF Config Dialog
VMware ESXi 5.x, 6.x, Fusion
E1000
- VMware

Public Cloud
- Amazon Web Services
  - AWS marketplace
c3.large, c3.xlarge
- Microsoft Azure
  - Azure Marketplace
  - Standard D3

Day 0 and Any Virtual Switch
vSwitch or dvSwitch
Cisco® AVS
Cisco Nexus® 1000V (no vPath), Open vSwitch
Cisco® ACI Integration

KVM
Cisco ASAv qcow2 image
KVM 1.0 Virtio driver

Cisco Virtual Firewall ASAv - multiple-hypervisor support with traditional network interaction.
Cisco Virtual FirePOWER and Mgmt Console

VMware
vSphere client, ovftool, and vCenter OVF Config Dialog
VMware tools on sensor/FMC
VMware ESXi 5.x, Fusion E1000

Cisco Virtual FirePOWER NGIPS Sensor and Multi-device Firepower Management Console
Cisco Virtual FTD with Mgmt Console

VMware
- vSphere client, ovftool, and vCenter OVF Config Dialog
- VMware ESXi 5.1, 5.5, Fusion
- No VMware tools yet on FTDv E1000

AWS
- c3.xlarge, BYOL

Cisco Virtual **NGFW** and Multi-device Firepower Management Console
Virtual vs. Physical Appliance Features

Cisco Virtual ASA and FirePOWER

Cisco ASAv
- 10 vNIC interfaces, VTEP, and VLAN tagging
- Virtualization displaces multiple context and clustering
- Failover active/standby high-availability model
- New SMART Licensing model (One license per model)
- Parity with all other Cisco® ASA platform features

Cisco FirePOWERv
- Virtual Sensor for the Hypervisor environment
- Virtualization prevents fail-to-wire and fastpath
- Inline L2 or tap traffic deployment
- The same licensing model: Control, URL Filtering, and AMP licenses

Cisco FirePOWERv 6.0

Removed Fail-Open, Fastpath, Routing, and NAT

Cisco ASAv

Removed clustering and multiple-context mode

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
Service Graph Definition
Abstract graph concept mapping to Service Graph

- Service graph is an ordered set of functions between a set of terminals (consumer and provider) 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
Purpose of the Service Graph

• By using the Service graph you can
  • install a service, like the ASA firewall once and
  • deploy it multiple times in different logical topologies

• Each time the graph is deployed ACI takes care of changing the configuration on the firewall to enable the forwarding in the new logical topology.

• ACI takes care of dynamically provisioning VLANs, IP addresses while re-using the same graph template

• The benefits of the service graph are:
  • a configuration template that can be reused multiple times
  • a more logical / application-related view of services
  • provisioning a device that is shared across multiple departments
Configurations with Service Graph

• All configurations performed in a single operation:

• Fabric configuration: Bridge Domains, VLANs, Routing, EPGs

• Firewall configuration: VLANs, Interfaces

• ACLs
Service Configuration before the Service Graph

1. Add client 172.18.20.13, call Security Admin to enable access.

2. Add ASA rules for client 172.18.20.13:
   - access-list OUT permit tcp host 192.168.1.1 host 10.1.1.1 eq 80
   - access-list OUT permit tcp host 192.179.1.1 host 10.1.1.1 eq 443
   - access-list OUT permit icmp host 192.168.1.100 host 192.168.100.1

3. Remove client 192.168.1.1, “no other action necessary”

4. Original ASA rules never change:
   - access-list OUT permit tcp host 172.18.20.13 host 10.1.1.1 eq 80
   - access-list OUT permit tcp host 172.18.20.13 host 10.1.1.1 eq 443
   - access-list OUT permit icmp host 172.18.20.13 host 192.168.100.1
Automatic endpoint addition/removal with ACI

Network Admin

Remove client 192.168.1.1

Add client 172.18.20.13, use existing ASA instance

Clients

192.168.1.1

192.168.1.100

192.168.1.1

172.18.20.13

Security Admin

Insert ASA instance in the service graph with desired policies

ASA1

Same 5 service rules and actions

access-list OUT permit tcp any any eq 80
access-list OUT permit tcp any any eq 443
access-list OUT permit tcp any any eq 135
access-list OUT permit tcp any any eq 22
access-list OUT permit icmp any any

Servers

10.1.1.1

HTTPS (TCP/443)

HTTP (TCP/80)

DCERPC (TCP/135)

SSH (TCP/22)

ICMP

172.16.1.1

192.168.100.1

Port Rules

<table>
<thead>
<tr>
<th>Source</th>
<th>EPG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leaf 1, port 1</td>
<td>Users</td>
</tr>
<tr>
<td>Leaf 1, port 10</td>
<td>Users</td>
</tr>
<tr>
<td>Leaf 2, port 12</td>
<td>Users</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination</th>
<th>EPG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leaf 3, port 2</td>
<td>Servers</td>
</tr>
<tr>
<td>Leaf 4, port 8</td>
<td>Servers</td>
</tr>
<tr>
<td>Leaf 5, port 12</td>
<td>Servers</td>
</tr>
</tbody>
</table>

BRKACI-2303 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
For more information on Service Graph

Service Graph Design with Cisco Application Centric Infrastructure White Paper:

Related sessions:

BRKACI-2121: Making the best of Services Automation with ACI Service Graph and Python
Dynamic Security with Trustsec on ASA in ACI

1. Corporate users on traditional Nexus 7000 in Corp EPG get assigned SGT values by ISE

2. ASA learns SGT mappings OOB through SXP

3. Coarse filtering: ACI Policy Contract allows all traffic from corporate network to database, redirects to ASA

4. Fine filtering: ASA permits only Engineering to access database from corporate based on SGT

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>[SGT 333]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
</tbody>
</table>
ISE and ACI Policy Models

ISE Policy Model

ISE Controller

Src-SGT (identity)  
SGACL  
Dest-SGT (identity)  
Policy Mapping

ACI Policy Model

APIC Controller

Src-EPG (identity)  
Contract  
Dest-EPG (identity)
ACI + Trustsec Policy Plane Architecture

ISE Policy Domain

1. Exchange SG/EPG Names
2. Exchange IP->SG/EPG Bindings

User IP->SGT Bindings

Server IP-> EPG bindings

APIC Policy Domain

Server classification

User classification

Propagation

SGT not propagated in data plane

Enterprise Core

Network Layer

Controller Layer
Policy Federation ISE to APIC Flow:
TrustSec SGT Policy used to Program ACI EPG Policy

ISE Retrieves:
EPG Name: App EPG,
EPG Binding = 10.1.100.52

App EPG Endpoint = 10.1.100.52
External EPG Name = BYOD
EPG binding = 10.1.102.20

ISE Exchanges:
SGT Name: BYOD
SGT Binding = 10.1.102.20

SGT Federated to ACI Policies
Policy Federation APIC to ISE: ACI EPG Policy used to Program Trustsec Policy

ISE Retrieves:
- EPG Name: App EPG
- EPG Binding = 10.1.100.52

Propagated with SXP
- SGT Name = BYOD
- EPG Binding = 10.1.100.52

BYOD 10.1.10.220

SGT Policy Enforcement

Plain Ethernet (no SGT)

Brocade ACI

Network Layer

Controller Layer

Cloud

Enterprise Backbone

Network Layer

Controller Layer

Network Layer
Campus Identity Scale Up Automatically Propagated into ACI Data Center

ISE Controller

APIC dynamically learns Scale Up User Bindings in Campus

ACI Data Center

User 1

User 1000

SGT Binding Scale Up
ACI App Scale Up Automatically Propagated into Campus ISE Controller

ISE Controller

ISE dynamically learns Scale Up VM Bindings in DC

ACI Data Center

Trustsec Domain

App Dynamic Scale Up in DC
APIC Settings in ISE Controller

APIC Settings:
- Credentials
- Tenant name
- L3out
ISE TrustSec SGT Policy Federated to APIC as External EPGs + Bindings
Design Practices
Design Practices

• Manual EPG Stitching
• Partial Automation
• Full Automation
• Design Example
**Manual EPG Stitching**
- APIC defines Tenants
- EPG is VLAN/Subnet

**Partial Automation**
- Fabric GW/Routing
- No Device Package
- ‘Happier’ SecOps

**Full Automation**
- Orchestrate it ALL!
- Vendor Device Package

---

ACI L2 Fabric

Unmanaged Service Graphs

Managed Service Graphs

EPG Web  EPG App  EPG DB  EPG Web  EPG App  EPG DB  EPG Web  EPG App  EPG DB
Manual EPG Stitching

- Firewalls managed separately from APIC by security team.
- Service attaches to EPG / VLANs / PGs and serves as a host gateway to steer traffic.
- Creation of EPG segments still done on APIC, EPs are virtual machines or physical servers.
- Firewalls control traffic flows between EPGs.
- Firewalls are GWs and peer with external routers
- Northbound API to script full Tenant network creation

Allow flexibility to enable ACI fabric for EPG management, and attach security directly into EPGs.
Partial Automation

- Firewalls managed separately from APIC by security team.
- Virtual appliance data plane vNICs get attached to proper PGs via APIC.
- Physical appliance attaches to the given fabric ports and must match VLANs.
- Creation of EPG segments still done on APIC, EPs are virtual machines or physical servers.
- Contract is between EPGs and adds unmanaged Service Graphs

Customers enable full ACI fabric benefits with out forcing a device package.
Full Automation

- Firewalls managed within APIC GUI. Security team can now program L4-L7 Function Profiles.
- Physical appliance attached to fabric and APIC configures DP with matching VLANs.
- Virtual appliance data plane vNICs get attached to proper PGs via APIC.
- Creation of EPG segments done on APIC, EPs are virtual machines or physical servers.

Leverage the full benefits of ACI fabric with ability to program L4-L7 using device package.
Service Insertion Decision Flowchart

1. Service Insertion
   - FW Admin to Configure Device
     - yes: Appear in Object Model
     - no: Health & Statistics
   - Health & Statistics
     - yes: Use Managed Service Graph
     - no: Visibility in ACI
   - Visibility in ACI
     - yes: Use Orchestration
     - no: APIC managing Via 3rd party Controller (FMC/BigIQ)
   - APIC managing Via 3rd party Controller (FMC/BigIQ)
     - yes: Use Future version of Service Graph (with FMC/BigIQ)
     - no: Use Unmanaged Service Graph
   - Use Unmanaged Service Graph

2. Use EPG Stitching
   - No Service Graph
Example: Tenant Design

- **Tenant Common**
  - VRF Zone-1
  - VRF Zone-2
  - VRF Zone-3
  - VRF Zone-4

- **Tenant Prod**
  - VRF Zone-1
  - VRF Zone-2
  - VRF Zone-3
  - VRF Zone-4

- **Tenant PreProd**
  - VRF Zone-1
  - VRF Zone-2
  - VRF Zone-3
  - VRF Zone-4

- **Tenant DevTest**
  - VRF Zone-1
  - VRF Zone-2
  - VRF Zone-3
  - VRF Zone-4

- **Tenant Management**
  - VRF Zone-1
  - VRF Zone-2
  - VRF Zone-3
  - VRF Zone-4
Example: Tenant Firewall Insertion
Example: Tenant Design
Conclusion
Conclusion

• **Security Architecture**: A phased approach to build security solution

• **Secure Fabric**: ACI Embedded Security

• **Role Based Access Control**: The Principle of Least Privilege

• **Segmentation for Security**: Reduce Attack Surface, Limit Exposure

• **Visibility**: If you can not see, you can not defend

• **Implementing Advance Security**: Layard Security with Advanced Controls

• **Design Practices**: Complexity is Enemy of Security
We Securely Connect Everything to Make Anything Possible
Complete Your Online Session Evaluation

• Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.

• Complete your session surveys through the Cisco Live mobile app or from the Session Catalog on CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Lunch & Learn
• Meet the Engineer 1:1 meetings
Thank you
## Security Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCIE Security</td>
<td>Expert Level certification in Security, for comprehensive understanding of security architectures, technologies, controls, systems, and risks.</td>
<td>CCIE® Security</td>
</tr>
<tr>
<td>Implementing Cisco Threat Control Solutions (SITCS)</td>
<td>Deploy Cisco’s Next Generation Firewall (NGFW) as well as Web Security, Email Security and Cloud Web Security</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Secure Access Solutions (SISAS)</td>
<td>Deploy Cisco’s Identity Services Engine and 802.1X secure network access</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Secure Mobility Solutions (SIMOS)</td>
<td>Protect data traversing a public or shared infrastructure such as the Internet by implementing and maintaining Cisco VPN solutions</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Network Security (IINS 3.0)</td>
<td>Focuses on the design, implementation, and monitoring of a comprehensive security policy, using Cisco IOS security features</td>
<td>CCNA® Security</td>
</tr>
<tr>
<td>Securing Cisco Networks with Threat Detection and Analysis (SCYBER)</td>
<td>Designed for security analysts who work in a Security Operations Center, the course covers essential areas of security operations competency, including event monitoring, security event/alarm/traffic analysis (detection), and incident response</td>
<td>Cisco Cybersecurity Specialist</td>
</tr>
</tbody>
</table>

For more details, please visit: [www.cisco.com/go/securitytraining](http://www.cisco.com/go/securitytraining) or [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact [ask-edu-pm-dcv@cisco.com](mailto:ask-edu-pm-dcv@cisco.com)
# Data Center / Virtualization Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introducing Cisco Data Center Networking (DCICN);</td>
<td>Learn basic data center technologies and skills to build a data center infrastructure.</td>
<td>CCNA® Data Center</td>
</tr>
<tr>
<td>Introducing Cisco Data Center Technologies (DCICT)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Data Center Unified Fabric (DCUFI);</td>
<td>Obtain professional level skills to design, configure, implement, troubleshoot data center network infrastructure.</td>
<td>CCNP® Data Center</td>
</tr>
<tr>
<td>Implementing Cisco Data Center Unified Computing (DCUCI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designing Cisco Data Center Unified Computing (DCUDC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designing Cisco Data Center Unified Fabric (DCUFD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Cisco Data Center Unified Computing (DCUCT)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Cisco Data Center Unified Fabric (DCUFT)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product Training Portfolio: DCNMM, DCAC9K, DCINX9K, DCMDS, DCUCS, DCNX1K, DCNX5K, DCNX7K</td>
<td>Gain hands-on skills using Cisco solutions to configure, deploy, manage and troubleshoot unified computing, policy-driven and virtualized data center network infrastructure.</td>
<td></td>
</tr>
<tr>
<td>Designing the FlexPod® Solution (FPDESIGN);</td>
<td>Learn how to design, implement and administer FlexPod solutions</td>
<td>Cisco and NetApp Certified FlexPod® Specialist</td>
</tr>
<tr>
<td>Implementing and Administering the FlexPod® Solution (FPIMPADM)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com