Global vision.
Local knowledge.

Cisco Connect Dubrovnik
Croatia
The Case for SDN
Applications All Around Us

...are the driving force of business that are being...
  
  Rapidly developed and
  
  Deployed at scale

...while requiring...
  
  Frequent updates and
  
  Highest Availability (SLAs)
Challenge for Infrastructure

...to keep up with the pace of change imposed on the:

- Network
- Security

...functions, while maintaining application:

- Capacity
- Resiliency
- Agility
Software-Defined Networking ...Comes to the Rescue

“...is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.”

Source: www.opennetworking.org
What are the critical Security Functions in the DataCenter?
Defining SDN use case for DC security

- Micro-Segmentation
- Embedding security policy within Application
- Programmability
- Automatic Remediation
- Ease of Service Insertion
ACI Devices Role

- APIC Controller
- Leaf Nodes
- Service Producers
- Spine Nodes

Service Consumers

- “App”
- “DB”
ACI Whitelist Policy supports “Zero Trust” Model

Whitelist policy = Explicitly configured ACI contract between EPG 1 and EPG 2 allowing traffic between their members.

TRUST BASED ON LOCATION
(Traditional DC Switch)

Servers 2 and 3 can communicate unless blacklisted.

ZERO TRUST ARCHITECTURE
(Nexus 9K with ACI)

No communication allowed between Servers 2 and 3 unless there is a whitelist policy.
The Heart of ACI

ACI uses a **policy based approach** that focuses on the **application**.
ACI Communication Abstraction

Security Policy
“App” → “DB”

All TCP/UDP:
- Accept
- Redirect to FW and IPS
All Other:
- Drop
First, we need a way to identify and group together end points.
In the ACI model, we do this using the **End Point Group (EPG)**.
Devices within an Endpoint group can communicate, provided that they have IP reachability (provided by the Bridge Domain/VRF).

Communication between Endpoint groups is, by default, not permitted.
Once we have our EPGs defined, we need to create policies to determine how they communicate with each other.
A contract typically refers to one or more ‘filters’ to define specific protocols & ports allowed between EPGs.
Create a Contract

Stateful filters – limited to checking if the ACK bit is set in the packets from provider to consumer without any TCP flow state tracking
Access Control From Outside

Perimeter Stateless Access Control
Segmentation Using Contracts

L3out


Stateless Access Control (Contract)
A collection of EPGs and the associated contracts that define how they communicate form an Application Profile.
A Tenant is a *container* for all network, security, troubleshooting and L4 – 7 service policies.

Tenant resources are *isolated* from each other, allowing management by different administrators.

Tenants can provide traffic and *RBAC isolation*...
VRF (also called contexts) are defined within a tenant to allow isolated and potentially overlapping IP address space.
Bridge Domain: Not a VLAN but almost...

Within a private network, one or more bridge domains must be defined.

A bridge domain is a L2 forwarding construct within the fabric, used to constrain broadcast and multicast traffic.
But what if I want all EPGs to be able to send syslog, query DNS, communicate with the AD, etc...?
vzAny applies rules to all EPGs in a VRF

Any EPG can consume syslog that EPG A provides

EPG A can consume Syslog from any EPG in the VRF

Any EPG in the VRF can consume or provide syslog

But what if I want some EPGs to communicate freely between themselves?
Contract Preferred Groups

Allow traffic between a group of EPGs

- EPG A
- EPG B
- EPG C
- EPG D

Contract Preferred Group
Alphabet

No contract required within the group

Contract required

ACI Micro Segmentation
The ACI Micro Segmentation Toolbox

EPGs & Contracts
ACI Policy Model
The ACI Micro Segmentation Toolbox

- Functional equivalent to Isolated Private VLAN: **ALL endpoints in EPG are isolated from each other**
  - Supported since ACI 1.2(2)
  - Can be combined with Micro-segmented EPG

Intra-EPG isolation
The ACI Micro Segmentation Toolbox

EPGs & Contracts
ACI Policy Model

Intra-EPG isolation

Intra-EPG Contracts

From 4.0 with Service
Graph attached
The ACI Micro Segmentation Toolbox

Use of attributes to classify endpoints in a specific kind of EPG called µEPG

**Network-based attributes:**
- IP/MAC

**VM-based attributes:**
- Guest OS, VM name, ID, vnic, DVS, Datacenter

Does not create a Port Group on VMM (no vnic reassign)

Supported since ACI 1.1(1)

Micro-segmented EPGs with attributes
About Micro-segmented EPGs

• µSeg EPGs are **not linked to a “Base” EPG** (though virtual endpoints are still “attached” to their corresponding Port Groups):
  • They have their **own Bridge Domain** → Endpoints addressing must be taken into consideration in the design
  • They have their **own set of Contracts** → There is no contract inheritance from the “Base” EPG.
• Attributes are **matched using an “OR” operator** with a precedence order in case of conflict
  • Any VM in the VMM Domain & Tenant **matching an attribute** will be put in the µSeg EPG → Choose wisely the attribute(s) you want to match
  • In the last 2 case studies, **Custom Attributes** would be a natural choice
Use Cases

Securing infrastructure

Quarantining compromised endpoints

Securing an application life cycle
Security Services
Cisco ACI Supports Flexible East-West Security Models

L4 Stateless Security

Servers (Physical or Virtual)

Firewall at Each Leaf Switch

► L4 Distributed Stateless Firewall

L4 Stateless Firewall Attached to Every Server Port
Line Rate Policy Enforcement
Policy Follows Workloads

L4-7 Visibility and Control

L4-7 Security Services (physical or virtual, location independent)

L4-7 Security via Cisco ACI™ Service Graph

Advanced Protection with NGFW, IPS/IDS, DDoS Services Insertion
Sizing at Scale: Can add ASA Cluster
L4-7 Security Policy Applied Consistently for Any Workload
Why Inserting Security Services?

- **Stateless Segmentation** not sufficient for compliance
- More granular Access Control (i.e. user based)
- Dynamic protocol requiring **better inspection**
- **Better protection** and detection mechanisms
Cisco Security Portfolio Overview

Firewall/IPS/AMP
- Firepower NGFW/NGIPS/AMP
- ASA, FMC, NGFWv on Hypervisor
- Cisco ASA

Analytics
- StealthWatch
- StealthWatch Cloud

Cloud
- ASAv, FMCv, NGFWv
- AWS, Azure
- Umbrella & CloudLock
Where to Connect Security Services in the Fabric?

WE DON’T REALLY CARE !!!!!
How to Insert Security Services

• Network Stitching ACI L2 Fabric
• Service graph insertion
  • Unmanaged
  • Managed with Device package
  • Managed Hybrid

Match the requirements and operation model of the DC and Security Team
Flexible Options for Services Insertion

**ACI L2 Fabric**
- APIC defines Tenants
- EPG is VLAN/Subnet

**Service Graph No Package**
- Fabric GW/Routing
- No Device Package:
  - Network Policy Mode
  - SecOps Control Service

**Service Graph Managed**
- Orchestrate with Vendor:
  - Service Policy or
  - Service Manager

Device Packages

---

**Unmanaged Service Graphs**
- WEP
- EPG Geb
- EPG App
- EPG DB
- EPG Web
- EPG App
- EPG DB

**Managed Service Graphs**
- EPG Web
- EPG App
- EPG DB
Service Graph technology was designed to **automate** and **accelerate** the deployment of L4-L7 services in the network.
Why Use Service Graph?

- Security is fully inserted to the Application as the service graph is an extension of the contract in the Application Profile
- Granular way to send traffic to the Security Service using the contract
- Configuration Templates
- Automation of the Network configuration both for Fabric and Security appliance (with Device Package)
- Statistics and health score automatically collected for the services
- Dynamic update of the ACLs based on End Point discovery in the EPG
- Insert several services seamlessly with Service Chaining
ACI Zero Trust Model

ACI Fabric

APIC

CONTRACT

“DB”

“App”
Build a Policy with Service Graph

Security Policy
“App” → “DB”

ACI Fabric

APIC

Security Services

“DB”

“App”

All TCP/UDP:
- Accept
- Redirect to FW and IPS
All Other:
- Drop
Add a Service graph to a Contract
Service Automation Through Device Package

- Service automation requires a vendor device package. It is a zip file containing
  - Device specification (XML file)
  - Device scripts (Python)
- Cisco® APIC interfaces with the device using device Python scripts
- Cisco APIC uses the device configuration model provided in the package to pass appropriate configurations to the device scripts
- Device script handlers interface with the device using its REST or CLI interface
ASA Device Package Opt 1: Policy Orchestration

Managed – Service Policy

- FirePOWER Services
- Threat Defence Policies
- Threat Policy on FMC

ACLs, Inspections, HA, S2S
- VPN, Special Features

Interfaces, VLANs, IPs, Static or Dynamic Routes
- APIC Configures on ASA via ASA Device Package

ASA Policy Orchestration (PO) DP

Nexus9k Leafs/Spines – Shadow EPG VLANs, L3outs
- APIC Configures Service Graph in the ACI Fabric
ASA PO & FI Device Package
ASA DP Built-In Profiles

Template for Routed ASA
Requires Entry of IP Addresses
HA needs Standby IP Entry

Template for Transparent ASA
Requires Entry of BVI IP Address
HA needs Standby IP Entry
Why Use Managed Service Graph?

- Full Tenant orchestration with L4-L7 services
- ACL changes on the firewall can be offloaded to custom tools, using Northbound API
- Device package allows for very fast deployment of security
- APIC monitors the service health and validates configuration
Why Use Unmanaged Service Graph?

- Continuity of the SecOps management workflows and tools
- No device package available from a Vendor
- Quicker migration of security appliance configs and policies into ACI fabric
- Allow use of the full spectrum of product features, not just the features supported by the device package
Service Graph Hybrid Managed

- Leverage the **network and interface configuration automation** from APIC with the Device Package
- Leverage the **External Security management solution** for the security team to create the security policy
- Use the Service graph to tie together the policy and the network insertion
ASA Device Package Opt 2: Fabric Insertion

ASA has an option that allows APIC to configure insertion into fabric while all other ASA features are configured out of band (CLI, REST-API, CSM, CDO).

Nexus9k Leafs/Spines - Shadow EPG VLANs, L3outs

APIC Configures Service Graph in the ACI Fabric

Managed – Service Policy

- FirePOWER Services
- Threat Defence Policies
- Threat Policy on FMC
- ACLs, Inspections, HA, S2S
- VPN, Special Features
- Interfaces, VLANs, IPs, Static or Dynamic Routes
- APIC Configures on ASA via ASA Device Package
- ASA Policy Orchestration (PO) DP

Managed – Service Policy

- Security team configures via FMC
- ACLs, Inspections, HA, and all other ASA features
- Security team adds more ASA cfg.
- Interfaces, VLANs, IPs, Static or Dynamic Routes
- APIC Configures on ASA via ASA Device Package
- ASA Fabric Insertion (FI) DP
ASA PO & FI Device Package
FTD Device Package Workflow

Existing Rule - Security Admin uses FMC to create an ACP Rule to be used with the new service graph. The rule includes allowed protocols, NGIPS, and AMP protections.

- Network Admin uses APIC to attach Security Zones to a given Rule, directing service graph traffic to an appropriate NGFW inspections.

New Rule – Network Admin uses APIC to create a new security Rule on FMC using the service graph. This is a Deny rule, preventing traffic flow until Security Admin gets a changes to update it.

- Security Admin uses FMC to update the new ACP Rule with an appropriate allowed protocol, NGIPS, and AMP policy. To prevent deletion of this rule on service graph detach, Security Admin can preserve configured security policy by updating ACP Rule comments.
FTD FI Device Package for ACI

Policy Creation:
Security Admin uses FMC to create an appropriate policy

Fabric Insertion:
Network Admin uses APIC to program Fabric Insertion of FTD
FTD Device Package for ACI

1.0.1
- Cluster support
- Ether-Channel
- Static Routes

1.0.2
- HA support
- FTDv VLAN trunks
- FPR2100 support
- Dynamic EPG
- Enhance validation
- Suffix changes

1.0.3
- Routed
- Transparent
- NGIPS modes
- Interfaces/Zones
- Inline Pairs
- Attach Zones to ACP Rules
FTD FI Device Package Version 1.0.3

APIC configures FMC 6.2.3, using REST-APIs to manage the following devices:

➢ Pre-registered FTD devices in either Stand-alone, HA or Cluster mode

APIC configures the following features:

• **Interfaces** in Routed, Switched, or Inline mode. Defines VLAN sub-interfaces (including Port-Channels) for Routed and Transparent firewall mode, including IRB. **Static routes** can be added under interface configuration.

• **Security Zones, Interface Names, Inline Sets**, as specified in function profile parameters. FMC names are prefixed with APIC Tenant and registered FTD device name. **EPG learning feature is supported** with FMC.

• **Assignment** of the **Security Zones to** pre-configured ACP Rule(s).
Matching FTD/ACI Deployment Modes

- Firewall Modes
  - Routed
  - Transparent

- NGIPS/IDS Modes
  - Inline (managed)
  - or Inline TAP (unmanaged)
  - Passive (unmanaged)
Security Service insertion using PBR
Policy Based Redirect is your Best Friend

APIC relies on Routing to forward traffic from Server in EPG WEB to Server in EPB APP based on contract.
Policy Based Redirect is your Best Friend
With PBR Service Graph

APIC relies on **PBR** to redirect the traffic defined in the contract to the Security Service

- **BD: App**
  - 192.168.11.1/24
  - GW: 192.168.11.254
- **BD: DB**
  - 192.168.12.1/24
  - GW: 192.168.12.254
- **BD: DB**
  - 192.168.13.1/24
  - GW: 192.168.13.254
- **BD: ASA-external L3 Enabled**
  - 192.168.100.0/30
  - 192.168.100.4/30

APIC relies on **PBR** to redirect the traffic defined in the contract to the Security Service.
PBR for micro-Segmentation
Based only on Contract

Because this is a communication between two End-Points in different EPG, the forwarding decision is made in the leaf switch.
PBR for micro-Segmentation

Leveraging PBR

Because the traffic goes to Leaf Switch where PBR rules are enforced, traffic will be sent to the security service defined in the Service Graph.
The Firewall must be in **ONE ARM** as source and destination are in the same Subnet. It must **allow traffic in and out via the same interface.**
New features related to PBR
ACI Version 3.2

• Multi-node PBR
• vzAny with PBR
• Resilient Hash PBR
Multi-node PBR

• Prior to ACI 3.2: Concatenating PBR nodes was not supported.
  • For example, both 1st and 2nd node can't be PBR nodes. Either one of them can be.

• ACI 3.2: Support more than 1 node PBR in a Service Graph. (up to 3 nodes)
  • We can mix PBR node and non-PBR node in same Service Graph
PBR with vzAny

• In ACI 3.2, PBW with vzAny (provider) is also supported.
• Use case: Insert Firewall everywhere.
Resilient Hash PBR

• Symmetric PBR is supported today, but if one of the PBR nodes is down, traffic will be rehashed. So existing connection having been going through available PBR nodes could be affected.

Thanks to Symmetric PBR, incoming and return traffic go to same PBR node.

Some traffic could be load-balanced to different PBR nodes that don’t have existing connection info.
Resilient Hash PBR

- With Resilient Hash PBR, only the traffics that went through a failed node will start using different PBR node.
Policy Based Redirect Requirements

• APIC must be v 2.0.1 or Higher

• The Service switch must be at least ‘-EX’ or more recent

• If not all the fabric is ‘-EX’, the Service switch must be dedicated to Services (i.e. no workload connected with the L4-7 services)
What about IDS ?
IDS Insertion in ACI

• Traditional Span mechanism based on EPG source/Destination

• NEW Copy Service:
  • Specific Service graph
  • As based attached to contract, leverage Subject for a more granular selection of traffic than SPAN

• Require −EX leaf switch
• Support only one device per copy cluster
Service Copy Configuration Steps

- Identify the source and destination endpoint groups.
- Configure the contract that specifies what to copy according to the subject and what is allowed in the contract filter.
- Configure Layer 4 to Layer 7 copy devices that identify the target devices and specify the ports where they attach.
- Use the copy service as part of a Layer 4 to Layer 7 service graph template.
- Configure a device selection policy that specifies which device will receive the traffic from the service graph. When you configure the device selection policy, you specify the contract, service graph, copy cluster, and cluster logical interface that is in copy device.
Copy Service : Service Graph Template

Create L4-L7 Service Graph Template

Drag device clusters to create graph nodes.

Device Clusters

- svcType: COPY
  - fgandola/my-IDS
- svcType: FW
  - fgandola/ASA-berlin (Managed)
  - fgandola/Berlin-unamanged_ASA
- svcType: IDSIPS
  - fgandola/VNGIPS-54 (Managed)

Graph Name: Berlin-Copy-Service
Graph Type: Create A New One

Consumer

EPG

Provider

my-IDS

Please drag a device from devices table and drop it here to create a service node.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/L4-L7_Services_Deployment/guide/b_L4L7_Deploy_ver211/b_L4L7_Deploy_ver211_chapter_01101.html#id_28562
Threat Protection with IPS
Cisco Firepower Threat Defense Features

Cisco Firepower Threat Defense Full Feature-Set - NGFW

- L2-L7 Firewall with L3 (Routed), L2 (Transparent IRB or Inline-NGIPS) Modes
- Scalable CGNAT, ACL, Dynamic Routing, Fail-to-Wire I/O modules
- Application Inspection, PKI for Site-to-Site VPN, Onbox Manager
- Inter-chassis cluster, FlexConfig, REST-APIs, Packet Tracer/Capture
- NSS Leading Next-Gen IPS - SourceFIRE
- Comprehensive Threat Prevention, L7 Application Visibility and Control
- Security Intelligence (C&C, Botnets, IP, DNS, etc.), Threat / Risk Reports
- Blocking of Files by Type, Protocol, and Direction, Protocol Rate Limiting
- 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, User-based IOCs, URL lookup
- AMP public & private cloud with ThreatGrid, FMC-ThreatGrid APIs
- Firepower Management Center (fka. FireSIGHT or Defense Center)
Automation
Dynamic Update to EPG Object-Group

1: Enable “Attachment Notification” on function connector internal.

2: APIC create object-group for the EPG.

3: APIC add new endpoints to object-group (192.168.10.101, 192.168.10.102)

APIC dynamically detects new endpoint, ASA subscribes to attach/detach event, and ASA device package automatically adds EPs to object-group.
FMC to APIC Rapid Threat Containment

Step 1: Infected End Point launches an attack that NGFW(v), FirePOWER Services in ASA, or FirePOWER(v) appliance blocks inline.

Step 2: Intrusion event is generated and sent to FMC revealing information about the infected host.

Step 3: Attack event is configured to trigger remediation module for APIC that uses NB API to contain the infected host in ACI fabric.

Step 4: APIC quickly contains/quarantines the infected App1 workload into an isolated uSeg EPG.
TrustSec
Traditional Security Policy

TrustSec Security Policy

Security Control Automation
Simplified Access Management
Improved Security Efficacy

Software Defined Segmentation

Network Fabric
Switch Router Wireless DC FW DC Switch

Flexible and Scalable Policy Enforcement
Enabling Group-Based Policies across the Enterprise

- Cohesive security policy
- Simplified security management
- End-to-End segmentation
TrustSec Security Groups Provisioned in ACI

ISE Dynamically provisions TrustSec Security Groups in ACI Fabric

Max: 200 Security Groups
Up to 4000/32 mappings (gen1)
Up to 10K/32 mappings (gen2) (-EX)

TrustSec Groups represented as External EPGs
TrustSec Groups Shared with ACI

### Security Groups

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>SGT (Dec / Hex)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>Auditors</td>
<td>9/0009</td>
<td>Auditor Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>BYOD</td>
<td>15/000F</td>
<td>BYOD Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Contractors</td>
<td>5/0005</td>
<td>Contractor Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Developers</td>
<td>8/0008</td>
<td>Developer Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Development_Servers</td>
<td>12/000C</td>
<td>Development Servers Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Employees</td>
<td>4/0004</td>
<td>Employee Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Guests</td>
<td>6/0006</td>
<td>Guest Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Network_Services</td>
<td>3/0003</td>
<td>Network Services Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>PCI_Servers</td>
<td>14/000E</td>
<td>PCI Servers Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Point_of_Sale_Systems</td>
<td>10/000A</td>
<td>Point of Sale Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Production_Servers</td>
<td>11/0008</td>
<td>Production Servers Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Production_Users</td>
<td>7/0007</td>
<td>Production User Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Quarantined_Systems</td>
<td>255/00FF</td>
<td>Quarantine Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Test_Servers</td>
<td>13/0000</td>
<td>Test Servers Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>TrustSec_Devices</td>
<td>2/0002</td>
<td>TrustSec Devices Security Group</td>
</tr>
<tr>
<td>☐</td>
<td>Unknown</td>
<td>0/0000</td>
<td>Unknown Security Group</td>
</tr>
</tbody>
</table>

**Security Groups List > BYOD**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑</td>
<td>Propagate to ACI</td>
</tr>
</tbody>
</table>

Security Group Tag (Dec / Hex): 15/000F
Generation Id: 1
## TrustSec Groups Shared with ACI

<table>
<thead>
<tr>
<th>Name</th>
<th>Alias</th>
<th>QoS Class</th>
<th>Description</th>
<th>Target DSCP</th>
<th>Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYOD_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractors_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td>0.0.0.0/0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Developers_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development_Servers_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employees_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td>10.1.100.100/32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guests_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network_Services_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCI_Servers_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Point_of_Sale_Systems_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Production_Servers_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Production_Users_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quarantined_Systems_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test_Servers_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TrustSec_Devices_SGT</td>
<td>Unspecified</td>
<td>Unspecified</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Sharing Application Context to TrustSec Policies

TrustSec dynamically learns internal EPGs and VM Bindings from ACI fabric.

ISE dynamically learns internal EPGs and VM Bindings from ACI fabric.

TrustSec Domain

TrustSec Policies Controlling Access to ACI Data Centers

ACI Fabric

VM1

VM100
Sharing ACI Endpoint Groups to TrustSec

- EPG suffix added to Security Group name
- IP-SGT bindings from ACI can be propagated over SXP TrustSec devices and to pxGrid peers
Effective security depends on total visibility

- **KNOW** every host
- **SEE** every conversation
- Understand what is **NORMAL**
- Be alerted to **CHANGE**
- Respond to **THREATS** quickly

- **Branch**
- **Roaming Users**
- **Network**
- **Users**
- **Data Center**
- **Admin**

© 2018 Cisco and/or its affiliates. All rights reserved.
Cisco CTD Solution: Providing Scalable Visibility

Drilling into a single flow yields a plethora of information
Flow-based Anomaly Detection

1. Collect & Analyze Flows
   - # Concurrent flows
   - Packets per second
   - Bits per second
   - New flows created
   - Number of SYNs sent
   - Time of day
   - Number of SYNs received
   - Rate of connection resets
   - Duration of the flow
   - Over 80+ other attributes

2. Establish Baseline of Behaviors

3. Alarm on Anomalies & Changes in Behavior
   - Critical Servers
   - Exchange Server
   - Web Servers
   - Marketing

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public
### Behavior-Based Attack Detection

High Concern Index indicates a significant number of suspicious events that deviate from established baselines.

<table>
<thead>
<tr>
<th>Host Groups</th>
<th>Host</th>
<th>CI</th>
<th>CI%</th>
<th>Alarms</th>
<th>Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlanta, Desktops</td>
<td>10.10.101.110</td>
<td>865,645,669</td>
<td>8.656%</td>
<td>High Concern Index</td>
<td>Ping, Ping_Scan, TCP_Scan</td>
</tr>
<tr>
<td>Atlanta, Desktops</td>
<td>10.10.101.27</td>
<td>315,014,634</td>
<td>3.150%</td>
<td>High Concern Index, High Total Traffic</td>
<td>Ping, Ping_Scan</td>
</tr>
<tr>
<td>Desktops, New York</td>
<td>10.50.100.30</td>
<td>100,149,559</td>
<td>1.304%</td>
<td>High File Sharing Index, High Total Traffic</td>
<td>Ping, Ping_Scan, ReLeas, TCP_Scan</td>
</tr>
<tr>
<td>Desktops</td>
<td>10.10.101.118</td>
<td>865,645,669</td>
<td>8.656%</td>
<td>High Concern Index</td>
<td>Ping, Ping_Scan, TCP_Scan</td>
</tr>
<tr>
<td>Catch All</td>
<td>10.40.102.54</td>
<td>12,063,078</td>
<td>121%</td>
<td></td>
<td>TCP_Scan</td>
</tr>
</tbody>
</table>
It Can:

- **Detect Sophisticated and Persistent Threats.** Malware that makes it past perimeter security can remain in the enterprise waiting to strike as lurking threats. These may be zero day threats that do not yet have an antivirus signature or be hard to detect for other reasons.

- **Identify BotNet Command & Control Activity.** BotNets are implanted in the enterprise to execute commands from their Bot herders to send SPAM, Denial of Service attacks, or other malicious acts.

- **Uncover Network Reconnaissance.** Some attacks will probe the network looking for attack vectors to be utilized by custom-crafted cyber threats.

- **Find Internally Spread Malware.** Network interior malware proliferation can occur across hosts for the purpose gathering security reconnaissance data, data exfiltration or network backdoors.

- **Reveal Data Loss.** Code can be hidden in the enterprise to export of sensitive information back to the attacker. This Data Leakage may occur rapidly or over time.
StealthWatch Solution Components
How do I send Traffic to my FlowSensor?
How Send Traffic to my FlowSensor?

• Traditional Span mechanism based on EPG Source/Destination
• NEW Copy Service:
  • Specific Service graph
  • As based attached to contract, leverage Subject for a more granular selection of traffic than SPAN
• Require –EX leaf switch
• Support only one device per copy cluster
In Conclusion

• ACI helps tackling DC Security Challenges by :
  • Integrating security in the Application
  • Accelerating security deployment
  • Automating security insertion

• Cisco Security helps better protect your DC by :
  • Providing leading edge technologies
  • Integrating smoothly in ACI architecture
  • Providing a full security framework