Designing a Data Center Security Architecture...

One Capability at a Time
Where is the security?

How are the business flows secured?
Cisco SAFE Design Method
Security capability flow

E-commerce transaction and payment
Client AV/AM
Identity
Firewall
Intrusion Prevention
Flow Analytics
Threat Intelligence
Server segmentation

OpenCart & Payment Applications

Data Center Security Architecture

Three focus areas:

Visibility/Analytics
“See everything”

Segmentation
“Reduce the attack surface”

Orchestration

Intent-based
Analytics

Threat Protection
“Stop the breach”

Automation
Threat intelligence - Talos

© 2018 Cisco and/or its affiliates. All rights reserved.
animate this slide with traffic bubbles flowing constantly on the racetrack between 3 tenants

Jamey Heary, 8/7/2017
Cisco Datacenter Security Solutions – Focus Areas

Segmentation
Firewall & Access Control
- NGFW, ACI and Tetration
- Policy Orchestration
- Firepower Management Center and CloudCenter
- APIC and Identity Services Engine

Visibility/Analytics
Network & Application Analytics
- Stealthwatch / SW Cloud
- Tetration + Stealthwatch

Threat Prevention
Threat Protection
- NGFW/NGIPS
- Advanced Malware Protection (AMP)

Integrated
Security capabilities in the Hybrid Cloud

- **Visibility**
  - Stealthwatch Cloud
  - AMP Threat Response

- **Segmentation**
  - ACI TrustSec
  - ASAv NGFWv

- **Threat Protection**
  - Umbrella
  - AMP Tetration

- **Client**
  - Anti-Virus
  - Anti-Malware

- **Server Workload**
Secure DC dCloud Update
dCloud Demo versus dCloud Lab

- Demo is intended to highlight available integrations, with the integrations ALREADY CONFIGURED.
- Lab is intended to train engineers on how to enable the integrations.
dCloud – Secure DC DEMO

“Cisco Secure Data Center in Action v1”

Walks through Multiple Secure DC Integration Demos, with a minimal amount of setup. Total demo takes approximately 1 hour.

Setup takes approximately 15 minutes.

1. Using Tetration and Firewall API, export a Tetration policy to both ASA and Firepower Threat Defense. Also, import a policy from ASA and FTD to Tetration.

2. Explore APIC.

3. See how ISE enables SGT and EPG to be shared between Campus and DC. Use them in a firewall policy.
4. Rapid Threat Containment demonstration, where a zero-day malware file is created, and detected with Firepower. The new file is submitted to ThreatGrid for analysis and the infected host is quarantined in both Tetration and APIC at the same time. View file analysis in Firepower Management Center.

5. Identify a Data Exfiltration incident in Stealthwatch Enterprise, and in the process of investigating the incident, pivot into Tetration for deeper analysis of the affected hosts.
Secure DC Workshops
Secure DC Workshops

A series of 2-hour sessions are going to run in the US, Canada, and LATAM. Each location will have a 2-hour internal training session, followed by a 2-hour customer-facing session.

Workshops will kickoff in November, and run through April or so.

- Chicago
- Ft. Lauderdale
- Atlanta
- Fulton MD
- Houston
- Phoenix
- Boston
- Irvine
- Sao Paulo, Brazil
- NYC
- Toronto
- Mexico City
- Dallas

November  | December  | January
<table>
<thead>
<tr>
<th>Date</th>
<th>City</th>
<th>Contact Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 13</td>
<td>Chicago</td>
<td>Andrew Netburn for US,</td>
</tr>
<tr>
<td>November 29</td>
<td>Fulton, MD</td>
<td>Mexico, and Canada</td>
</tr>
<tr>
<td>December 11</td>
<td>Boston, MA</td>
<td></td>
</tr>
<tr>
<td>January 10</td>
<td>New York City</td>
<td>Chris Reay for EMEAR and</td>
</tr>
<tr>
<td>January 15</td>
<td>Atlanta, GA</td>
<td>APAC</td>
</tr>
<tr>
<td>January 17</td>
<td>Ft. Lauderdale, FL</td>
<td></td>
</tr>
<tr>
<td>February 5</td>
<td>Houston, TX</td>
<td></td>
</tr>
<tr>
<td>February 12</td>
<td>Irvine, CA</td>
<td></td>
</tr>
<tr>
<td>March 5</td>
<td>Toronto, Canada</td>
<td></td>
</tr>
<tr>
<td>March 12</td>
<td>Phoenix, AZ</td>
<td></td>
</tr>
<tr>
<td>March 19</td>
<td>Sao Paulo, Brazil</td>
<td></td>
</tr>
<tr>
<td>April 9</td>
<td>Mexico City</td>
<td></td>
</tr>
<tr>
<td>April 16</td>
<td>Dallas, TX</td>
<td></td>
</tr>
</tbody>
</table>
DUO
DUO helps us do these things..

**Establish Trust**
- Verify user
- Multi-factor authentication
- Verify device
- Agentless compliance checks

**Adaptive Access**
- Intent-based networking
- On or off premises
- Trust-based policy
- Single sign-on

*Any User, Any Device, Any Application, Any Location*
Cloud-based in-depth and broad device visibility

In-Depth Visibility

- Endpoint detection and response
- Off-VPN internet security
- Endpoint posture and context

180M+ managed devices

Broad Visibility

- Agentless inspection with real-time enforcement
- Unified compliance check
- Cloud-based onboarding and management

- mobile and non-mobile devices
- managed and unmanaged devices
Fortifying Cisco’s zero-trust leadership

Before

Internal

Trusted Network

External

Insecure
off the VPN

Cisco today

Internal

Zero-Trust
for the network

External

Protected
on or off the VPN

Cisco + Duo

Internal

Zero-Trust
for the network and apps

External

Perimeter Extended
to the Point of Access

Duo brings together zero-trust with consistent policies for the network and apps.
Integrations
Tetration and ASA / Firepower

Demonstrated in dCloud scenario 1 (demo and lab)

Scripts are posted on Github:
https://github.com/oxsannikova/fmc_asa_tetration_policy_import_export

- asa_to_tetration.py
- fmc_to_tetration.py
- tetration_to_asa.py
- tetration_to_fmc.py
Tetration and ASA / Firepower

What’s next?

Tetration Streaming Policy Push
Combines Tetration policy with a firewall policy (ASA in this example), so as policy is edited in Tetration, it is streamed automatically to ASA.

https://github.com/tetration-exchange/pol-client-go
Rapid Threat Containment
Tetration Remediation Module for FMC

Demonstrated in dCloud scenario 4 (demo) and scenario 3 (lab)
Remediation Module is posted on CCO

Adds annotation to host in Tetration that is used to apply a quarantine policy.
APIC Remediation Module for FMC

Demonstrated in dCloud scenario 4 (demo) and scenario 3 (lab)
Remediation Module is posted on CCO

Places host in a quarantine μSeg EPG
Identity Services Engine can be used for Control Plane exchange of SGT from Campus with EPG from Data Center, and allow firewalls policies to enforce.
SGT to Cloud Tags

Coming in DNA-C

Enables automatic mapping of SGT for hosts in AWS or other cloud provider, based on tag or other attribute.
Stealthwatch Enterprise to Tetration External Lookup

Demonstrated in dCloud scenario 5 (demo) and scenario 4 (lab)
Script is not yet posted

Allows easy pivot from Stealthwatch Enterprise to Tetration.

"I see a Data Exfiltration alert in Stealthwatch. What does Tetration have to show about the affected host?"
Stealthwatch Enterprise to Tetration External Lookup

Pivot from Stealthwatch to Tetration interface during an investigation
Stealthwatch Enterprise to Tetration
External Lookup

What’s next?

Exciting new capabilities targeted, but NOT COMMITTED, around April...
IMPORT: Tetration Groups as SW Host Groups

Map

Threat to Target information in Real-time
Questions?