We’re ready. Are you?
Cisco IT - Identity Services Engine (ISE) Deployment and Best Practices

Simon Finn, Security Solutions Architect
Agenda

- Introduction
- Why ISE? Justifying the program
- Resolving Priorities
- ISE Cluster Deployment
- Network Foundations
- Key Capability Deployment
- Future Vision
- Conclusion
- Q&A
Cisco Enterprise and What We Must Protect

- 300 partners using 550 IT extranet connections into Cisco
- 141k Workforce
- 98 Countries
- ~3M IPv4 Addresses
- 215,000 Infra Devices
- 275,000 Total Hosts
- 2500+ IT Applications
- 26k Remote Office Connections via Cisco Virtual Office
- 425 Devices Deployed for Preventing/Detecting Security Incidents
- ~3TB Network Data Collected p/day
- 16 major Internet connections
- ~32 TB bandwidth used daily
- 500 cloud/ASP providers (officially)
- 1350 Labs
- 160+ Acquisitions
IT and Security Trend Challenges
Why Deploy ISE?
Justifying Your Deployment
What is Identity Services Engine (ISE)?

A centralised security solution that automates context-aware access to network resources and shares contextual data.

<table>
<thead>
<tr>
<th>Network Door</th>
<th>Access Policy</th>
<th>Network Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical or VM</td>
<td>Who</td>
<td>Guest Access</td>
</tr>
<tr>
<td></td>
<td>What</td>
<td>BYOD Access</td>
</tr>
<tr>
<td></td>
<td>When</td>
<td>Role-Based Access</td>
</tr>
<tr>
<td></td>
<td>Where</td>
<td>Threat Containment</td>
</tr>
<tr>
<td></td>
<td>How</td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>Compliant</td>
<td>ISE pxGrid Controller</td>
</tr>
</tbody>
</table>

Network Resources

- Traditional
- Cisco TrustSec®

Identity Profiling and Posture

- Identity Profiling
- Posture

Context

- Physical or VM

ISE pxGrid Controller

COCSEC-2002 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

7
“Cisco TrustSec and Cisco ISE are consistent with our view of identity-centric end-to-end security that is both needed and lacking in the enterprise today.”

Forrester 2011
Questions From a Customer CIO / CSO

Is there anything Cisco can do to help me…..

• Understand what devices are plugged into the network and who these devices belong to? I don’t know today.

• Consistently control access to my network regardless of whether a user or device connects via wired, wireless or VPN?

• Limit access from computers, tablets and mobiles that do not comply with IT and Security requirements or during a security incident?

• Deploy IOT devices in a consistent, scalable, secure and rapid fashion?

• Extend these capabilities to cloud services that an IT department consumes even when not connected to the network?

Represents direct linkage to 6 of the SANS Top 20 Security controls and can assist with an addition 6.
## Cisco IT Network Security Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Major Technical Outcome</th>
<th>Major Business Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Guest Network ION (Internet Only Network)</td>
<td>Simplified single secure platform (reduce server footprint from 28 to 8)</td>
<td>• High availability&lt;br&gt;• Secure, scalable, and flexible offering for guests, partners, and employees</td>
</tr>
<tr>
<td>802.1x Auth: WLAN, CVO*, LAN, and VPN</td>
<td>Complete visibility and control of users and devices connecting to the network</td>
<td>• One scalable policy enforcement environment&lt;br&gt;• Network segmentation</td>
</tr>
<tr>
<td>Consistent Assured Network Access</td>
<td>Scalable enterprise secure network</td>
<td>• Enhanced Risk Management&lt;br&gt;• Consistent User Experience&lt;br&gt;• Improved Operations</td>
</tr>
</tbody>
</table>

*CVO is Cisco Virtual Office, for small office/home office*
ROI and Value Case - Sample

**Specific Value Case:**
- Avoided Device Mgmt. and Support Costs
- Cost Avoidance post ION Enhancements
- Cost Avoidance Guest
- Cost Avoidance Help Desk
- Reduced Costs due to Security Improvements

**Overall at Cisco IT:**
- Payback on ROI in ~2.75 years
  - Year 1 is 2014
- ~75% reduction in guest account creation
- ~90% reduction in sponsor account creation post enhancement
- ~60% reduction in help desk costs
- ~75% avoidance cost in personnel costs due to breach
What We Left Out Of Claimed Savings…

• Reduced operational costs.
  • No extra VLANs
  • Manual configuration of public area/special use ports

• Faster time to service
  • E.g. acquisitions

• Risk Reduction
  • Reduced complexity, reduced downtime per incident
Resolving Priorities
Resolving Priorities

Understand your network
- What can you deliver
- What are your planned upgrades and projects

Understand your business problems
- Mobile devices
- Dynamic user policy
- Compliance

Understand the Dependencies
**Infrastructure Access Control**
- Wireless access
- Wired access
- Remote Access
- Virtual Machine

**User Policy**
- Guests
- Extranet/Vendors/Contractors/Interns
- Acquisitions/Diverse Business/ICZ
- Employees and role based access

**Device Policy**
- Incident Containment (Quarantine)
- Profiling and Posture Policy
- IOT Policy
- IT services

**Trusted Service Enablement**
- Attribution/Assessment
- Enforcement
- Cloud Access Control
- Service policy enablement
IT Requirements ⇔ ISE Capabilities

Guest Access
Restrict unauthorised devices & users to Internet access only

Profiling
Ability to identify users and devices on our network

Access Control
Authentication on wired & wireless networks as well as VPN

Endpoint Protection
Protect the network from infected devices

Device Control
Secure network while allowing mobile device access*

IOT/BYOE
Support Trusted Device Standard and enable BYOE

Contextual Data
Cross-platform contextual data sharing across the entire IT infrastructure

* Cisco IT uses a 3 different Device Management Products
The Four Stages of a Secure Network

1. Profiling
   - Identity of a device on the network
   - Quantify the risk

2. Authentication
   - User and end device attribution
   - Identification of end points on Wireless connections
   - Device security posture identification
   - Allows for better policy & security decisions

3. Posture
   - Ability to enforce policy decisions based on context
   - Untrusted devices have restricted access

4. Enforcement

ISE 1.2
Profiling and monitor mode
ISE 1.2
802.1X Auth WLAN, CVO
ISE 1.3/1.4
802.1X Auth CVO, Wired, VPN, MDM
ISE 2.1
802.1X Wired Auth Mode MDM
Our First Deployment
ION – Internet Only Network

- BYOD ready
  - Enables and empowers GIS BYOD strategy
- Differentiated policy based network access
- Reduced architectural complexity
  - More scalable, less operational overhead, highly redundant
- Enables IPv6 Internet & guest networking
- Multi-language support
- Same visibility and control as other areas of the network

“ION will be the basic access for users and devices at Cisco, and offers a basic level of service such as remediation services, mobile mail, VPN and internet
Successful pass of authentication and policy checks will be required for more access”
Proposed Business Outcomes - Sample

**Short Term 0 -1 yr**

**Enhanced Risk Management**
- Block Minimal OS or device type via Quarantine.
- Posture Assessment of Mac, Android, iOS. Limited assessment of Windows.
- ISE authenticated network

**User Experience**
- Dynamic User Policy — Acquisitions + Information Control Zones

**Improved Operations**
- Quarantine / Remediation (EPS)
- Dynamic Device Policy -- IOE/IOT (IT or Workplace Resources managed)
- Intelligent business decisions based on ISE data

**Medium Term 1 -2 yrs**

**Enhanced Risk Management**
- Posture assessment of all supported OS’s including Windows (ISE 2.1).
- Basic Posture Enforcement.

**User Experience**
- Dynamic User Policy – Wide scale deployment

**Improved Operations**
- Leverage TrustSec capabilities for Acquisitions, Labs & Diversified Business Units.

**Advanced 2 year+**

- Graceful Posture Enforcement with workflow management.
- Trusted Service
- Extranet Enablement
Evolution of the Workplace

Identity
• You must authenticate to gain network access
• Access based upon identity

Device
• IOE, IOT – dynamic device policy
• Posture based controls

Culture Changes
• Access is an entitlement
• Physical access does not mean full access
Cisco IT Deployment Strategy

• Avoid the “Big Bang”
  • Too many new capabilities to enable in a single deployment.

• “ISE Deployment Bundle” model
  • Capabilities have been grouped into bundles to enable targeted & manageable deployments

• Multiple clusters consolidated
  • Pros and cons of single vs. distributed: ISE Limits, Scalability, # EP, Auth, Latency, AD…
  • “Start with one cluster and add more if necessary”

• Global Infrastructure Foundation
  • Use different Virtual IPs by service (e.g., WLAN, LAN, CVO, VPN) for better manageability and ease/speed of control
  • Build a parallel production infra for testing, readiness to scale, and easier upgrade

• Build a cross-functional team from the start
  • Everybody is an equal partner; extend to the BU
Cross Functional Ownership for Execution

Security BU
- Product Development
- Engineering Development
- Engineering Test

SVP Operations
- CIO
- SVP IT

SVP Security & Trust
- VP InfoSec
- VP Infra Services
- Sr. Dir Arch/Design
- Sr. Dir Data Centres
- Dir Strategy & Security
- VP Ops/Impl
- Sr. Dir Network Services
- Mobility Any Device

VP IT

Owns Mobile Devices, Responsible for Posture Enforcement

SVP Infra Services

Owns and Manages the Deployment of NW Services

SVP Security & Trust

Owns and Operates the NW Infrastructure

VP InfoSec

Team, owns the infra for Network and Application security services

Sr. Dir Arch/Design

Security Services

Provides DC and Virtual Infrastructure

High Level Architecture and Design

Directory Services

Owns Active Directory Infra and Services

Security s and Policy Requirement

Team, owns the infra for Network and Application security services
ISE Cluster Deployment
ISE Deployment Ecosystem: Building Blocks

- **Logical Layer**
  - ISE Appliance OR VM (Fabric, Compute, Storage)

- **Physical Layer**
  - Network: DNS, NTP, SFTP, UDP, TCP, (& Load Balancers)

- **Endpoints**
  - Devices, Users & Supplicants

- **ISE** (Logical Layer)
  - 1 PAN

- **Network Access Devices**
  - 10’s K

- **Endpoints**
  - Devices 100’s K

- **User Provisioning**
- **Mobile Device Management**
- **Call Manager**
- **Network Device Provisioning**
- **ISE Policy Management**

- **Enterprise Monitoring**
  - HTTP(S), RADIUS, PEAP, EAP-FAST, EAP-TLS

- **Active Directory**
- **Data Analysis (Syslog)**

- **Quality MAP**
- **Monitor**
- **Prevent**
- **Act**

- **Call Manager**
  - 100’s K
  - 10’s K
  - 1 PAN

- **Network Device Provisioning**
  - PAN

- **Data Analysis**
  - Syslog
In The Beginning: ISE 1.0 Clusters

Proposed locations – subject to change
Single Global ISE 1.3 Deployment (WLAN, CVO, LAN, VPN)

Global Deployment: 24 ISE Nodes
20 PSNs; 8 DC (Node Groups)
Cisco IT ISE Global Deployment (WLAN, LAN)
Users/Endpoints by Node Group

- AER: 32,856 Users, 18,362 Endpoints/MAC
- ALLN: 23,969 Users, 9,961 Endpoints/MAC
- BGL: 40,995 Users, 23,969 Endpoints/MAC
- HKG: 37,481 Users, 26,070 Endpoints/MAC
- MTV: 58,846 Users, 32,651 Endpoints/MAC
- RTP: 51,878 Users, 28,124 Endpoints/MAC
- SNG: 21,384 Users, 12,870 Endpoints/MAC
- TYO: 9,445 Users, 5,317 Endpoints/MAC
### Cisco IT ISE Hardware Specifications

<table>
<thead>
<tr>
<th>Hardware</th>
<th>CPUs</th>
<th>Memory</th>
<th>Storage Type</th>
<th>Disk Space (PAN)</th>
<th>Disk Space (MnT)</th>
<th>Disk Space (PSN)</th>
<th>NIC Speed/Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended Min</td>
<td>4 x 2.4 GHz</td>
<td>16 GB</td>
<td>Dedicated SAN</td>
<td>200 GB</td>
<td>200 GB</td>
<td>100 GB</td>
<td>4 x Integrated Gigabit NICs</td>
</tr>
<tr>
<td>Cisco IT PROD</td>
<td>8 x 2.032 GHz (Gold Reservation)</td>
<td>32 GB</td>
<td>Dedicated SAN (except HKG/TYO)</td>
<td>600 GB</td>
<td>600 GB (1 TB for tftp)</td>
<td>200 GB</td>
<td>1 x 1 GB NIC</td>
</tr>
</tbody>
</table>

### Cisco IT ISE Software Specifications

<table>
<thead>
<tr>
<th>Service</th>
<th>Installations</th>
<th>License File</th>
<th>License Expires</th>
<th>Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Package</td>
<td></td>
<td></td>
<td></td>
<td>6839/100000</td>
</tr>
<tr>
<td>Base Package(1)</td>
<td></td>
<td>Base_POSITRONFEAT201306041941307980.lic</td>
<td>permanent</td>
<td></td>
</tr>
<tr>
<td>Advanced Package</td>
<td></td>
<td></td>
<td></td>
<td>5862/100000</td>
</tr>
<tr>
<td>Advanced Package(1)</td>
<td></td>
<td>Adv_POSITRONFEAT201306041943436540.lic</td>
<td>3-jun-2018</td>
<td></td>
</tr>
</tbody>
</table>
Cisco IT Early Deployment Challenges

• Scaling ISE for large scale distributed deployments
• Don’t let replication or misconfiguration become an issue for authentication:
  • Tuning the “deployment” (ISE, NADs, and Endpoints)
    • RADIUS Accounting
    • Profiling
    • Authentication(s)
    • Latency & Distributed Replication
    • Failover & Redundancy
  • Tuning the “environment”
    • Load Balancers
    • Active Directory
Replication Challenges

Iceberg (īsʼbûrg’)
(Former state)

ISE Burj
(Current state)

Replication Issues

Latency
Misconfiguration
Error notification
NAD misbehaviour
Profiling
SNMP errors
Radius
accounting
Endpoint misbehaviour
Load Balancer misbehaviour

Cisco live!
Tune the Deployment and the Environment

Configuration Changes:
NAD and ACE (LB)

Accounting Suppression Fix:
CSCur42723

Removing IP as Significant Attribute Fix:
CSCur44879
Large Deployments – Bandwidth and Latency

- Bandwidth most critical between:
  - PSNs and Primary PAN (DB Replication)
  - PSNs and MnT (Audit Logging)

- Latency most critical between PSNs and Primary PAN.

200ms
Max round-trip (RT) latency between any two nodes in ISE 1.2/1.3

- RADIUS generally requires much less bandwidth and is more tolerant of higher latencies – Actual requirements based on many factors including # endpoints, auth rate and protocols.
Scaling and Load Balancers

- Reasons to use a load balancer
  - Moving clusters without touching NAD infra
    - Testing
    - Limited deployment
    - Upgrades
  - WLC 17 server limit
  - Resiliency

CoA requires UDP/1700
Don’t NAT other traffic
SNAT only CoA
Single Point of Failure

All services will be affected, and likely to also impact the secondary node.
Guestnet (ION) Redesigned Deployment
Geo Proximity Based NAD & GSS Configuration

- **Secondary AER**
  - PPAN Alias
  - VMS Tool

- **Primary MTV**
  - Lobby Ambassadors
  - Guest Account Creation Integration With Reception

**MTV**
- ion-mtv-guest
- ion-mtv-sponsor
- ION LB VIPs
- Wireless access
- Wired access

**AER**
- ion-aer-guest
- ion-aer-sponsor
- ION LB VIPs

**Guest Portal Auth**
- Primary
- Secondary

**Sponsor Portal GSS**
- internet.cisco.com
- Guest Account Creation

**NADs AMER**
- Wireless access
- Wired access

**NADs EMEA/APJC**
- Wireless access
- Wired access
Network Foundations
Cisco IT ISE Production Deployment Metrics

- Production Infrastructure
  - Network Access  
    - ISE 1.4, P6  24 VM servers in one global deployment
  - Guest Services  
    - ISE 1.2, P13  8 VM servers in one dedicated deployment

- Services In Production
  - Guest services (ION)  
    - Internet Only Network access requires pre-registration via ISE guest portal for all users; CWA (central web auth)
  - 802.1X Wireless Auth Mode  
    - 400+ wlan sites, 90K+ users, ~150K endpoints
  - 802.1X Auth CVO (wireless/wired)  
    - 27K Network Devices for home access; ~60K endpoints
  - 802.1X Wired Monitor Mode*  
    - 3.5K LAN Switches and Gateways, ~200K endpoints
  - 802.1X VPN Access (AnyConnect)  
    - 70 ASAs; ~110K users; 150K+ endpoints
  - 802.1X Wireless Partners/Xtranet  
    - 3 sites; ~1K Users/Endpoints
  - SGT/TrustSec (wireless/wired)  
    - 3 sites; ~6K Users/Endpoints

- To-date: 1M+ Profiled Endpoints; Max of 75K+ Concurrent Endpoints
Cisco IT ISE Global Deployment (All Network Access Devices)
Top 4 cities by number of guest authentication over a 7-day period:

- 6,379
- 3,583
- 2,107
- 2,232
Change of Authorisation

Policy must also be understood by the NAD
Understanding What Is Connecting To The Network
ISE Global Deployment Profiling Setting
PSN Configuration

27K CVO Network Devices configured under 29 subnets in ISE. SNMP polling is disabled using the new option “zero” as the devices were not always connected, resulting in timeout errors (600K), affecting replication.

Explicitly choose the polling PSN

CSCur95329 Simple fix; Great value!
# ‘Misbehaving’ Supplicants

<table>
<thead>
<tr>
<th>EndPoint Profile</th>
<th>Auths Per Day</th>
<th>Count of EndPoints</th>
<th>% of Total EndPoints</th>
<th>Avg Auths Per Endpoint</th>
<th>Observation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows7-Workstation</td>
<td>98,394</td>
<td>25,918</td>
<td>20.99</td>
<td>3.8</td>
<td>Normal level of authentication</td>
</tr>
<tr>
<td>Apple-iPhone</td>
<td>745,807</td>
<td>17,820</td>
<td>14.43</td>
<td>41.85</td>
<td>Very, very “chatty” device</td>
</tr>
<tr>
<td>Microsoft-Workstation</td>
<td>69,216</td>
<td>16,469</td>
<td>13.34</td>
<td>4.2</td>
<td></td>
</tr>
<tr>
<td>Apple-Device</td>
<td>67,167</td>
<td>8,720</td>
<td>7.06</td>
<td>7.7</td>
<td></td>
</tr>
<tr>
<td>Workstation</td>
<td>49,834</td>
<td>8,408</td>
<td>6.81</td>
<td>5.93</td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td>115,839</td>
<td>5,160</td>
<td>4.18</td>
<td>22.45</td>
<td>Very “chatty” device</td>
</tr>
<tr>
<td>OS_X_Mavericks-Workstation</td>
<td>17,529</td>
<td>4,644</td>
<td>3.76</td>
<td>3.77</td>
<td></td>
</tr>
<tr>
<td>OS_X_Yosemite-Workstation</td>
<td>17,718</td>
<td>4,276</td>
<td>3.46</td>
<td>4.14</td>
<td></td>
</tr>
<tr>
<td>Apple-iDevice</td>
<td>97,862</td>
<td>3,813</td>
<td>3.09</td>
<td>25.67</td>
<td>Very “chatty” device</td>
</tr>
<tr>
<td>Android-Samsung-Galaxy-Phone</td>
<td>78,539</td>
<td>3,146</td>
<td>2.55</td>
<td>24.96</td>
<td></td>
</tr>
<tr>
<td>Android-Samsung</td>
<td>39,250</td>
<td>3,132</td>
<td>2.54</td>
<td>12.53</td>
<td></td>
</tr>
<tr>
<td>Apple-MacBook</td>
<td>14,014</td>
<td>2,883</td>
<td>2.34</td>
<td>4.86</td>
<td></td>
</tr>
<tr>
<td>Android-Motorola</td>
<td>70,695</td>
<td>2,226</td>
<td>1.8</td>
<td>31.76</td>
<td></td>
</tr>
<tr>
<td>Android-Google</td>
<td>44,835</td>
<td>1,761</td>
<td>1.43</td>
<td>25.46</td>
<td></td>
</tr>
</tbody>
</table>

Cisco live! Wireless auth over 24 hours.
## Platform Compatibility*

<table>
<thead>
<tr>
<th>Platform</th>
<th>Min. Acceptable Code</th>
<th>Preferred Code (if appropriate)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>C3750E</td>
<td>15.0(2)SE5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3750X</td>
<td>15.2(1)E</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3850</td>
<td>3.3.1 (15.0(1)EZ1)</td>
<td>3.6.3E</td>
<td></td>
</tr>
<tr>
<td>C4510R+E/Sup7E</td>
<td>3.6.1E</td>
<td>3.6.3E</td>
<td></td>
</tr>
<tr>
<td>C4510R+E/Sup8E</td>
<td>3.6.1E</td>
<td>3.6.3E</td>
<td></td>
</tr>
<tr>
<td>C6k/Sup32</td>
<td>12.2(33)SXJ6</td>
<td></td>
<td>SXP support only</td>
</tr>
<tr>
<td>WLCs</td>
<td>8.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C881W (CVO)</td>
<td>15.4(1)T</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISE 4451</td>
<td>IOS-XE 3.15.01S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASR1K</td>
<td>IOS-XE 3.11S</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*based upon Cisco IT Routing & Switching roadmap

---

*Cisco live!*
Windows Laptop Builds

1. Basic IP/BOOTP

2. Download WinPE

3. WinPE Build, AD registration, new logon
Wired Default Networking

Failed Auth ACL
Default access including:
• Laptop builds
• AD
• Support pages

Redirect ACL
Deny tcp/80+443:
• Laptop builds
• Support pages
• ISE Servers

Guest Access – Guest VLAN
Employee Credentials – Data
There Will Be Device Exceptions

How will you manage them?
Voice VLAN Limitations

- Global voice VLAN since early 2000’s
- Allowed one device in voice domain per port (global limitation)
- Problem evident with old CTS devices with phones attached. Solve via static port configuration.
<table>
<thead>
<tr>
<th>Device</th>
<th>802.1x support</th>
<th>Certificate</th>
<th>Authentication methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>7960^</td>
<td>Yes</td>
<td>LSC</td>
<td>LSC, MAB</td>
</tr>
<tr>
<td>79XX</td>
<td>Yes</td>
<td>MIC, LSC</td>
<td>LSC, MIC, MAB</td>
</tr>
<tr>
<td>88XX</td>
<td>Yes</td>
<td>MIC, LSC</td>
<td>EAP-TLS, EAP-FAST, MAB</td>
</tr>
<tr>
<td>99XX</td>
<td>Yes</td>
<td>MIC, LSC</td>
<td>MIC, LSC</td>
</tr>
<tr>
<td>DX650</td>
<td>Yes</td>
<td>MIC, LSC</td>
<td>LSC, MIC, MAB</td>
</tr>
<tr>
<td>EX-Series*</td>
<td>Yes, not centrally managed</td>
<td>CA-Signed</td>
<td>EAP-TLS, PEAP, MAB</td>
</tr>
<tr>
<td>S-Series*</td>
<td>Yes, not centrally managed</td>
<td>CA-Signed</td>
<td>EAP-TLS, PEAP, MAB</td>
</tr>
<tr>
<td>C-Series*</td>
<td>Yes, not centrally managed</td>
<td>CA-Signed</td>
<td>EAP-TLS, PEAP, MAB</td>
</tr>
<tr>
<td>MXP*</td>
<td>Yes, not centrally managed</td>
<td>CA-Signed</td>
<td>EAP-TLS, PEAP, MAB</td>
</tr>
<tr>
<td>CTS</td>
<td>No</td>
<td>No</td>
<td>MAB</td>
</tr>
<tr>
<td>TX</td>
<td>No</td>
<td>No</td>
<td>MAB</td>
</tr>
<tr>
<td>VG224</td>
<td>No</td>
<td>No</td>
<td>MAB</td>
</tr>
</tbody>
</table>
IBNS 2.0

Survivability

Flexible Authentication

Service Templates

Intelligent Aging
Operations
Deployment Readiness

- Design Engineer Personal Lab
- Solution Verification Lab
- Stage & Pilot
- Deploy!
Resources for Operations

2 Sr. Engineers + 2 Support Engineers (multi-zone)

• Performance monitoring and tuning, scalability for growth
• HW/SW issues
• Troubleshooting, field issues
• Provisioning of Network Devices, and Users support
• Monitoring and Reporting (ISE reports and Splunk)
• Patch/Upgrade
• Infra/VM issues, Change Request support
• Policy Management

+ Resources for Deployment

2 Sr. Engineers, 1 Analyst, 1 PM

• Learning and Testing new capabilities
• Solution Verification Lab testing and certification support
• Automation of new operational activities
• Limited Availability validation of new features
• Product and platform bug identification and validation
• Data analysis and scalability for new capabilities
• Acquiring knowledge of new capabilities & cross functional environment support
• Documentation
Consolidated Dashboards

ISE Enterprise Summary

Select Environment
from Jan 18 through Jan 20, 20...

Authentications

10m ago

Denied

Passed

Failed

Datacenter

aer
allne
bgl
hkg
mtv
rtp
sng
tyo

Profiler

10m ago

Success
Failure
Warning

Datacenter

aer
allne
bgl
hkg
mtv
rtp
sng
tyo

Hardware Performance

10m ago

Performance Score

Normal
Warning
Critical

Datacenter

aer
allne
allw
bgl
hkg
mtv
rch
rtp
sng
tyo

System Load Distribution

10m ago

Node Group

aer
allne
bgl
hkg
mtv
rtp
sng
tyo

System Management

10m ago

Normal
Warning
Critical

Node Group

aer
bgl
hkg
mtv
rch
rtp

Alarms

10m ago

Count

aer
allne
bgl
mtv
rch
rtp

Profile Queue Size Limit Reached
Profile Queue Size Limit Reached
Profile Queue Size Limit Reached
Profile Queue Size Limit Reached
Profile Queue Size Limit Reached
Profile Queue Size Limit Reached

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
Load Distribution Deep Dive

Traced Back to Load Balancer Configuration (Stickiness by Source IP)
ISE Authentication Storm/Meltdown From a “Simple” Change

IP Phones accidentally enabled for 802.1x auth

Call Manager

Endpoints: Devices, Users & Supplicants

Network Access Devices

ISE (Logical Layer)

Data Analysis (Syslog)

1,600 IP Phones started MAB/dot1x auth frenzy: 2,600 attempts per day, per phone = ~4M

Detection & troubleshooting

Luckily only ~4M auth requests per day due to limited deployment of a dozen switches.

Target scope is 100K IP Phones = 250M Auth
Key Capability Deployments
Planned Enhancements for Guest Networking

There are currently three planned enhancements for improved user experience in ION (Internet Only Network).

1. Integration with new LATS (Lobby Ambassador Ticketing System) Visitor Badge system
   - 1a: Additional features to be added such as guest pre-registration and bulk upload sync between LATS and ION

2. Guest self-registration with approval

3. Improved Guest Experience via new services on ION
   - Additional services added to Guest experience, to include but not limited to:
     - Print Services – allow guests to locate and print to closest Cisco printer
     - Demo Services – allow sales and training demos to attach and pre-register NADs and other equipment for sales and/or training demonstrations
     - Connected Mobile Experience (CMX): Allow for registration by guests to push billboards, targeted messaging, etc...
     - Location based solutions (LBS) can provide additional value for user tracking, showcasing and marketing.
### Business Driver

**Initiative**
To *divest* Assets including employees and properties to Technicolour

**Objective**
To create *logical separation* on network infrastructure and provide secure resource access in shared workspace

**Solution**
To utilise TrustSec Security Group Tagging solution based on *user ID* for authentication and authorisation

**Benefits**
Reduced complexity, increased business agility
Reduced costs physical controls and circuits

### Dynamic User Policy (DUP)

![Dynamic User Policy Diagram]

LWR01-06 / SHN7

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
## SHN7/LWR01-06 DUP Solution Summary

<table>
<thead>
<tr>
<th></th>
<th>Desktop Switch</th>
<th>Desktop Gateway</th>
<th>BB/SBB Gateway</th>
<th>WAN Gateway</th>
<th>WLC</th>
<th>WLC Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SHN7 12th Floor</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HW Model</td>
<td>C4510-SUP8E</td>
<td>C6K-SUP2T</td>
<td>C4500X</td>
<td>N/A</td>
<td>WiSM2</td>
<td>C6K-SUP2T</td>
</tr>
</tbody>
</table>
| CTS / DUP      | • 802.1X Authenticator  
|                | • Wired SGT Classifier  
|                | • SXP Speaker  
|                | • PreAuth/Permit-Any ACL  | • Wired SGT Enforcer  
|                | • SXP Listener  
|                | • Downloadable SGACL   | • 802.1X Authenticator  
|                |                |                |                |             |     |             |
| **LWR01-06**   |                |                 |                |             |     |             |
| HW Model       | C6K-SUP32      | C6K-SUP2T       | C4500X         | N/A         | WiSM2 | C6K-SUP2T   |
| CTS / DUP      | • 802.1X Authenticator  
|                | • Wired SGT Classifier  
|                | • SXP Speaker  
|                | • PreAuth/Permit-Any ACL  | • Wired SGT Enforcer  
|                | • SXP Listener  
|                | • Downloadable SGACL   | • 802.1X Authenticator  
|                |                |                |                |             |     |             |

Wired
Know your platform enforcement support (SGT-to-subnet)

Wireless
WLC enforcement at gateway
Connected Real Estate

• Badge readers
• IP Cameras
• Thermostats
• UPS
• Parking sensors
• Lighting
• BMS

Collaboration and Devices

• Apple TV
• Smart TV’s
• Digital signage
• Kiosks
• Robots

User Devices

• Wearable Devices
• Arduino
• Raspberry Pi
• …. The next big thing

Dynamic Device Policy
Planned Enhancements for Guest Networking

There are currently three planned enhancements for improved user experience in ION (Internet Only Network).

1. Integration with new LATS (Lobby Ambassador Ticketing System) Visitor Badge system
   • 1a: Additional features to be added such as guest pre-registration and bulk upload sync between LATS and ION

2. Guest self-registration with approval

3. Improved Guest Experience via new services on ION
   • Additional services added to Guest experience, to include but not limited to:
     • Print Services – allow guests to locate and print to closest Cisco printer
     • Demo Services – allow sales and training demos to attach and pre-register NADs and other equipment for sales and/or training demonstrations
     • Connected Mobile Experience (CMX): Allow for registration by guests to push billboards, targeted messaging, etc…
     • Location based solutions (LBS) can provide additional value for user tracking, showcasing and marketing.
To lower exposure, we need tools to contain rogue endpoints, whilst minimising business impact.
Other Services Integration
“Most NAC vendors provide good support for the **BYOD** use case. Now, the market is evolving to address another use case, where NAC policy servers act as "**warehouses of context**" and share contextual data with firewalls and other security components to enable **fine-grained policy enforcement**.”

“Magic Quadrant for Network Access Control”, Gartner, Dec 2014
ISE And The Cisco Security Solutions

**Before**
- CWS
- WSA
- ESA
- FirePOWER™ Services

**During**
- NetFlow
- NGIPS
- Lancope StealthWatch

**After**
- AMP
- AMP Threat Grid
- FireSIGHT™ Console
Sharing Contextual Data via PxGrid …
Cisco WSA
User policy based upon tags, users in logs

Lancope
User and device information in console
Rapid Threat Containment

- Improve threat visibility and detection effectiveness so that IT security can detect new and stealthy malware throughout the network
- Speed time to containment so that infected endpoints are quickly and automatically removed as threats
- Lower operational overhead and malware-related costs while supporting the use of already-deployed Cisco networking devices for enforcement
Future
Service Oriented Orchestration

- ACI
- TrustSec
- IOS

Service Grouping
- IPv4
- IPv6

Access Control
- IPv4
- IPv6

EPG

Contract

SGACL

ACL

Change ipv4/6 hosts once

Change service port information once
Trusted Service – Next Gen Application Security

- Consistent Security between clouds
- Extend on Premises Security to the Cloud
- Goal of parity between A-E
How to Become a Trusted Service?

Some services may require both trusted device and app controls.
Conclusion
Lessons Learned

- Acquire ISE expertise upfront; invest in architecture and design
- Focus on business outcomes, align IT verticals
- Fine tune deployment and environment, they must work in tandem
- Build the foundation and grow with the product and its ecosystem
- Follow BU guidelines; will cover 80% of the known challenges
- Listen to the data, and the alerts/alarms
- Do not take the network for granted
- Plan for the unexpected!
References

• Cisco.com/go/ise; Cisco.com/go/anyconnect; Cisco.com/go/trustsec
• Annual Security Report 2016
• ISE Design Guides
• Bringing Context-aware Security to Applications
• Securing the Internet of Everything with ISE
• Securing Cloud Applications
• Ping and ID Over IP Leveraging PxGrid
• Forrester: “The Total Economic Impact™ Of Cisco TrustSec” [March 2015]
The Cisco on Cisco Booth

Come visit us in the World of Solutions!

Demos of the Cisco Workplace…
• Collaboration
• Working inside and outside of the office

Live Demo of the Cisco Live network NOC!
• Cisco location technologies
• Cisco Prime Infrastructure
Q & A
Complete Your Online Session Evaluation

Give us your feedback and receive a **Cisco 2016 T-Shirt** by completing the Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected Friday 11 March at Registration

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations.
[www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)
Thank you