What You Make Possible
End to End Security in a Hosted Collaboration Environment
BRKSPG-2605
Agenda

- Hosted Collaboration Solution
- What Does Security Mean for HCS
- Customer Network Isolation
- Storage Isolation
- Securing Inter-Cluster Communication
- Securing UC Applications
Hosted Collaboration Solution
Unified Communications in the Cloud
HCS Architecture Elements

Unified Communication & Collaboration Applications
• Deliver a unparalleled user experience

HCS Management System
• Zero-touch automation & proactive system assurance

Optimized Virtualization Platform
• Provides hardware efficiency, customization, & scaling

Scalable System Architecture
• Aggregation, Security, Network Integration & CBSA
## Cisco HCS Applications

<table>
<thead>
<tr>
<th>Services</th>
<th>Product</th>
<th>Same as Premises Deployed App</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice &amp; Video</td>
<td>Unified Communications Manager, Unified IP Phones, Jabber</td>
<td>Yes</td>
</tr>
<tr>
<td>Voice Mail &amp; Integrated Messaging</td>
<td>Unity Connection</td>
<td>Yes</td>
</tr>
<tr>
<td>Presence &amp; Instant Messaging</td>
<td>Unified Presence, Jabber</td>
<td>Yes</td>
</tr>
<tr>
<td>Mobility Services</td>
<td>Unified Mobility, Mobile Clients</td>
<td>Yes</td>
</tr>
<tr>
<td>Web Collaboration</td>
<td>WebEx Meeting Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Attendant Console</td>
<td>Cisco Unified Enterprise Attendant Console</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Cisco UC End Point Portfolio

- **Basic**
- **Business**
- **Advanced Business**
- **Advanced Professional**
- **Advanced Collaborative**
- **Mobile Collaborative**

- **Voice Communications**
- **Media Communications**
HCS Telephony Architecture
What does security mean?
Within the context of HCS

- Everybody is using the same shared DC resources
- Customers require isolation
- External traffic is untrusted
Generic Security Best Practices

Always Applicable

- HTTPS
- AAA and TACACS+ for device access and authentication
- Disable telnet on all devices, use only SSH
- Physical Security: Lock and key
  - What are the implications of virtual machines?
- Passwords such as 12345 are common on people’s luggage
Agenda

- Hosted Collaboration Solution
- What Does Security Mean for HCS
- Customer Network Isolation
- Storage Isolation
- Securing Inter-Cluster Communication
- Securing UC Applications
Customer Network Isolation
Customer Network Isolation
HCS Security Layers

- Application and Signaling
- Storage Area Network
- Virtual Access
- Data Center
- SP Core
- Customer Access
- TLS, Authentication
- Zoning
- VLAN, VSG
- VRF-Lite, VLAN
- VRF
- VLAN
Customer Access

Customer Premises and Service Provider Access

- VLAN for Network Isolation
- Firewall at the customer edge
- Private VLANs on SP Access
- UNI and NNI ports on SP Access
Service Provider Core

IP/MPLS Core

- L3VPN per Customer
  - Provider Edge implements VRF and MP-BGP
  - MPLS transport across core
Data Center
Core and Aggregation Network

- Per Customer VRF-Lite continues on the Nexus Core
- Nexus Aggregation deposits traffic back onto VLANs
Data Center

Virtual Device Context (VDC)

- Virtualization of the control, data, and management planes
- Each VDC is a logically separate device
  – Can have unique access, data, and management policies.

Different network islands virtualized onto common data center networking infrastructure
Data Center
Adaptive Security Appliance (ASA)

- Firewall
- VPN Concentrator
- Intrusion Prevention System (IPS)
Data Center

ASA

Routed Mode
- All "flavors" of NAT available
- Data traffic is routed
- Does not pass Multicast traffic
- Interfaces can be shared between contexts

Transparent Mode
- Two interfaces per context
- NAT support for transparent mode
- Data traffic is bridged
- Passes Multicast traffic
- No shared interfaces
Data Center

ASA Placement Options

Customer Premises
- Protect the CPE

DC Aggregation/UCS Access
- Protect UCS and UC Applications

DC Aggregation/Extranet
- NAT
- Any external traffic
- Extranet Management
Data Center

ASA Traffic Flow
Virtual Access
Nexus 1000v

- Virtual Switch
- VLANs for Customer Separation
- ACL for Server to Server Filtering
Virtual Access on the Nexus 1000
Virtual Security Gateway (VSG)

- Customer Separation within a VLAN
- Block Application to Application traffic
- Grant subset of resources to one branch
Storage Isolation
Storage Area Network
How a Virtual Machine keeps its data separate

- VSANs associate to a host but not to a VM
- All VMs on a host belong to the same VSAN
- The VSAN is mapped to an FC Zone
- Zones provide isolation on per-host basis
Storage Area Network
Fiber Channel Zones

- **Hard Zoning**
  - Physical switch ports are associated with a zone

- **Soft zoning**
  - HBA WWN is associated with a zone

- **LUN Masking**

- **Classes of attacks against SANs:**
  - Snooping: Mallory reads data Alice sent to Bob in private—Allows access to data.
  - Spoofing: Mallroy fools Alice thinking that he is Bob—Allows access to or destruction of data.
  - DoS: Mallroy crashes or floods Bob or Alice—Reduces availability.
Storage Area Network
Other SAN Security Measures

- VMFS lock
- Storage Media Encryption (SME) on the MDS-9000
Agenda

- Hosted Collaboration Solution
- What Does Security Mean for HCS
- Customer Network Isolation
- Storage Isolation
- Securing Inter-Cluster Communication
- Securing UC Applications
Securing Inter-Cluster Communication
Signaling
Securing the Communication and Collaboration of HCS

SIP Trunks
- TLS Signaling Authentication
- SIP Trunk TLS + Secure RTP
- SIP Trunk with Digest Authentication

IP Phones
- TLS Signaling Authentication
- TLS + SRTP media encryption
- Secure indication tones
- Digest Authentication

CUBE-SP
- CAC per CUCM adjacency
- Event forwarding and blocking (Whitelist/Blacklist)
HCS Call Flows

- Media flow for inter-Enterprise on-net call
- Signaling flow for inter-Enterprise on-net call
- Signaling flow for Off-net call
- Media flow for Off-net call

Customer 1
Customer 2

Enterprise A
Enterprise B
CUBE(SP)
PGW

Enterprise A – CUCM, UnityCx, CUP, CUPM, CUOM
Enterprise B – CUCM, UnityCx, CUP, CUPM, CUOM
SIP Security Protocol
Transport Layer Security (TLS)

- Cryptographic
- Ensures data is both consistent and correct
- Provides endpoint authentication and privacy

- Three key phase
  - Authentication
  - Security Agent Key Distribution
  - Security Agent Confirmation
SIP TCP Signaling

Not Secure

[Diagram showing the process of SIP TCP Signaling with INVITE, 100 Trying, 180 Ringing, 200 OK, ACK, BYE, Media Session Established (RTP), ACK, BYE, 200 OK]
SIP TLS Signaling

Secure
Mean Call Setup Time Comparison Chart

- Non-Secured UDP
- Non-Secured TCP
- Secured TLS-auth
- Secured TLS-encr

Call Number (for 1 to 1000 calls)
Mean CPU Utilization Comparison Chart

The chart compares the mean CPU utilization of different traffic types over time. The x-axis represents the polling interval (every 10s), and the y-axis shows the overall server CPU utilization in percentage. The chart includes lines for:

- Non-Secure UDP
- Non-Secure TCP
- Secured TLS-auth
- Secured TLS-encr

The data points are distributed across the chart, showing the variance in CPU utilization over time for each traffic type.
Mean Memory Comparison Chart

- **Non-Secure UDP**
- **Non-Secure TCP**
- **Secured TLS-auth**
- **Secured TLS-encr**

Polling Interval (every 10s)

Memory Utilization in KBytes

- 0
- 100000
- 200000
- 300000
- 400000
- 500000
- 600000
- 700000
- 800000
TLS Analysis
There have to be drawbacks

- SIP Mean Call Setup Time increased by 30-40%
- CPU Utilization increased 28-35%
- Memory Utilization increased by 35%
Agenda

- Hosted Collaboration Solution
- What Does Security Mean for HCS
- Customer Network Isolation
- Storage Isolation
- Securing Inter-Cluster Communication
- Securing UC Applications
Securing UC Applications
Security Deployments
All the Possibilities
Securing UC Applications

- SIP endpoint Digest Authentication
- SIP endpoint TLS Encryption for signaling and sRTP
- Certification exchange between CUCM and CUCxn
Securing CUCM/Phone Settings

- Restricting the Settings Access to the phone
- Keeps a phone from displaying network information
  - Call Managers IP, VLAN ID, etc.
- Usually enabled by default
CUCM/Phone TLS

- Transport Layer Security for SIP and SCCP signaling encryption
- The certificates are exchanged in a TLS handshake
- TLS Session Keys for AES-128 encryption are generated
- The phone encrypts the two session keys using the CUCM’s public RSA key and sends them to the CUCM
- The CUCM decrypts the message and now the phone and CUCM can exchange AES-encrypted packets
CUCM/Phone SRTP

- Encryption and Message Integrity for RTP traffic
  HMAC-SHA1 for message authentication
  AES-128 in Counter Mode for encryption
- Requires signaling encryption
  - The symmetric session keys are generated by the CUCM and distributed to the phones
  - Keys are exchanged in the clear in the SDP, needs TLS for signaling encryption

<table>
<thead>
<tr>
<th>V</th>
<th>P</th>
<th>X</th>
<th>CC</th>
<th>M</th>
<th>PT</th>
<th>sequence number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>timestamp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>synchronization source (SSRC) identifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>contributing sources (CCRC) identifiers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RTP payload</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Authentication tag -- 4 bytes for voice</td>
</tr>
</tbody>
</table>
Securing Applications

- Credential Policy options
  - Length
  - Complexity
  - Lockout
  - Expiration
  - History
  - etc.
- Default Policy can be modified to meet customer’s Security Policy requirements
Summary

- Hosted Collaboration Solution
- What Does Security Mean for HCS
- Customer Network Isolation
- Storage Isolation
- Securing Inter-Cluster Communication
- Securing UC Applications
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com.
Final Thoughts

- Get hands-on experience with the Walk-in Labs located in World of Solutions, booth 1042
- Come see demos of many key solutions and products in the main Cisco booth 2924
- Visit www.ciscoLive365.com after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
  - Facebook: https://www.facebook.com/ciscoliveus
  - Twitter: https://twitter.com/#!/CiscoLive
  - LinkedIn Group: http://linkd.in/CiscoLI
BUILT FOR THE HUMAN NETWORK

Cisco