TOMORROW starts here.
Agenda

Introduction to NGFW

Software Architecture

Licensing

Deployment

How to configure policies

Management and Eventing ("logging")
The Challenges Come from Every Direction

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

Defenders
The Problem with Legacy Next-Generation Firewalls

Focus on the Apps

But miss the threat...

Legacy NGFWs can reduce attack surface area but advanced malware often evades security controls.
Integrated Threat Defence Across the Attack Continuum

**Before**
- Control
- Enforce
- Harden

**During**
- Detect
- Block
- Defend

**After**
- Scope
- Contain
- Remediate

**Visibility and Automation**
- Firewall/VPN
- NGIPS
- Advanced Malware Protection
- Granular App Control
- Security Intelligence
- Retrospective Security
- Modern Threat Control
- Web Security
- IoCs/Incident Response

**Modern Threat Control**
- BEFORE
- Enforce
- Harden

**Defend**
- Detect
- Block
- Defend

**Remediate**
- Scope
- Contain
- Remediate
Superior Integrated and Multilayered Protection

- Cisco ASA is world’s most widely deployed, enterprise-class stateful firewall
- Granular Cisco® Application Visibility and Control (AVC)
- Industry-leading FirePOWER next-generation IPS (NGIPS)
- Reputation- and category-based URL filtering
- Advanced malware protection
Cisco ASA with FirePOWER Services

Base Hardware and Software
New ASA 5585-X Bundle SKUs with FirePOWER Services Module
New ASA 5500-X SKUs running FirePOWER Services Software
FirePOWER Services Spare Module/Blade for ASA 5585-X Series
FirePOWER Services Software
Hardware includes Application Visibility and Control (AVC)

Security Subscription Services
• IPS, URL, Advanced Malware Protection (AMP) Subscription Services
• One- and Three-Year Term Options

Management
FireSIGHT Management Centre (HW Appliance or Virtual)
Cisco Security Manager (CSM) or ASDM

Support
SmartNET
Software Application Support plus Upgrades
What Platforms Support FirePOWER Services as a Software Module?

Maximum AVC and IPS throughput

<table>
<thead>
<tr>
<th>Platform</th>
<th>Throughput (Mbps)</th>
<th>Connections (K)</th>
<th>CPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5512-X</td>
<td>300</td>
<td>100</td>
<td>10,000</td>
</tr>
<tr>
<td>ASA 5515-X</td>
<td>250</td>
<td>250</td>
<td>15,000</td>
</tr>
<tr>
<td>ASA 5525-X</td>
<td>650</td>
<td>500</td>
<td>20,000</td>
</tr>
<tr>
<td>ASA 5545-X</td>
<td>1</td>
<td>750</td>
<td>30,000</td>
</tr>
<tr>
<td>ASA 5555-X</td>
<td>1.25</td>
<td>1,000</td>
<td>50,000</td>
</tr>
</tbody>
</table>

Branch Locations

Small/Medium Internet Edge
What Platforms Support FirePOWER Hardware Module

- 5585-X + FirePOWER module in top slot – Hardware Module

**FirePOWER SSP**
- Two Hard Drives Raid 1 (Event Data)
- 8 GB eUSB (System)
- 10GE and GE ports
- Two GE Management Ports
- ASA SSP
What Platforms Support FP Hardware Module?

Maximum AVC and IPS throughput

ASA 5585-SSP10
- 2 Gbps NGFW
- 500K Connections
- 40,000 CPS

ASA 5585-SSP20
- 3.5 Gbps NGFW
- 1 M Connections
- 75,000 CPS

ASA 5585-SSP40
- 6 Gbps NGFW
- 1.8 M Connections
- 120,000 CPS

ASA 5585-SSP60
- 10 Gbps NGFW
- 4 M Connections
- 160,000 CPS

Campus / Data Centre

Enterprise Internet Edge
# Cisco FireSIGHT Management Centre Appliance

<table>
<thead>
<tr>
<th>Maximum devices managed*</th>
<th>750</th>
<th>1500 *</th>
<th>2000</th>
<th>3500</th>
<th>4000</th>
<th>Virtual *</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>35</td>
<td>70</td>
<td>150</td>
<td>300</td>
<td></td>
<td>Virtual FireSIGHT® Management Centre</td>
</tr>
<tr>
<td>Event storage</td>
<td>100 GB</td>
<td>125 GB</td>
<td>1.8 TB</td>
<td>400 GB</td>
<td>4.8/6.3 TB</td>
<td>ASA or FirePOWER appliances</td>
</tr>
<tr>
<td>Maximum network map (hosts/users)</td>
<td>2000/2000</td>
<td>50,000/50,000</td>
<td>150,000/150,000</td>
<td>300,000/300,000</td>
<td>600,000/600,000</td>
<td>Virtual FireSIGHT® Management for 2 or 10 ASA devices only! Not upgradeable FS-VMW-2-SW-K9 FS-VMW-10-SW-K9</td>
</tr>
<tr>
<td>Events per second (EPS)</td>
<td>2000</td>
<td>6000</td>
<td>12,000</td>
<td>10,000</td>
<td>20,000</td>
<td></td>
</tr>
</tbody>
</table>

Max number of devices is dependent upon sensor type and event rate

* = Recommended!
Management-interface Considerations on ASA5500-X
ASA FirePOWER Management Options

Two layers of management access: Initial Configuration and Policy Management

- **Initial Configuration** must be done via the CLI (command line interface):
  - Session to the module over the ASA backplane on both ASA5500-X and ASA5585-X
- ASA FirePOWER policy configuration is done using FireSIGHT Management Centre.
- Traffic redirection to FirePOWER services is done from the ASA configuration.
- FirePOWER module IP address can be changed through CLI or ASDM Setup Wizard
ASA5500-X FirePOWER Management Interface

- One shared Management interface for ASA and FirePOWER module on ASA5500-X platform
- The FirePOWER module uses Management Interface for
  - all updates (base OS, OS upgrade packages)
  - all feature updates (rules, reputation data)
  - all Management Centre interaction (Mgmt, event-data)
- FireSIGHT policy management is performed through the management interface
ASA5500-X FirePOWER Management Interface Considerations (Cont.)

- Best practice is to separate ASA and FirePOWER management interfaces
- ASA managed in-band (from the “inside” interface)
- FirePOWER module managed via the Management Interface
- No nameif assigned to the ASA M0/0 Interface
- ASA Inside Interface and FirePOWER Management can share the same Layer 2 domain and IP subnet
- Access from the “inside” to the FirePOWER module through switch/router, without ASA involvement

```
FirePOWER# show module SFR detail
Mgmt IP addr: 192.0.2.2
Mgmt Network Mask: 255.255.255.0
Mgmt Gateway: 192.0.2.254
```

```
Best Practice

interface Management0/0
no nameif
security-level 0
management-only
no shutdown
```

```
Interface GigabitEthernet0/0
nameif inside
security-level 0
ip address 192.0.2.254
```
Agenda

Introduction to NGFW
Software Architecture
Licensing
Deployment
How to configure policies
Management and Eventing
Detailed ASA SFR Packet Flow

FirePOWER does not drop flows, it marks them for drop by the ASA.
Snort Technology

• The Snort Engine’s Basic Architecture
  • The sniffer
  • Preprocessors
  • The detection engine
  • The output and alerting module
Snort Technology

Preprocessors

Handle the task of presenting packets and packet data in a contextually relevant way to the detection engine.

For example: HTTP header seen on non-standard port

Packet fragment reassembly
Maintaining TCP state
TCP Stream reassemble
Protocol normalisation
Snort Technology

Detection Engine:

Accepts the parsed, normalised and stream-reassembled network traffic for inspection against the rule base.

Rules Builder

Inspection against the built rules
URL Filtering
URL Filtering

- Block non-business-related sites by category or reputation
- Based on user and user group
URL Filtering

Editing Rule - Web Block List

Name: Web Block List
Enabled: 
Action: Block
Move:

Categories and URLs
- Search by name or value
- Abortion
- Abused Drugs
- Adult and Pornography
- Alcohol and Tobacco
- Auctions
- Bot Nets
- Business and Economy
- CDNs
- Computer and Internet Info
- Computer and Internet Security

Reputations
- Any
- 5 - Well known
- 4 - Benign sites
- 3 - Benign sites with security risks
- 2 - Suspicious sites
- 1 - High risk

Selected URLs
- Adult and Pornography (Any Reputation)
- Bot Nets (Any Reputation)
- Confirmed SPAM Sources (Any Reputation)
- Gambling (Any Reputation)
- Keyloggers and Monitoring (Any Reputation)
- Malware Sites (Any Reputation)
- Marijuana (Any Reputation)
- Nudity (Any Reputation)
- Open HTTP Proxies (Any Reputation)
- Parked Domains (Any Reputation)
- Pay to Surf (Any Reputation)

Enter URL: 

Save | Cancel
AMP: File Based Malware Prevention

- ASA with FirePOWER Services
- Dedicated FirePOWER Appliance
- Web & Email Security Appliances
- Cloud Based Web Security & Hosted Email
- Private Cloud

Fire reputation and file sandboxing
Continuous & Zero-Day Detection
Advanced Analytics And Correlation
Advanced Malware Protection

All detection is less than 100%

One-to-One Signature
Fuzzy Finger-Printing
Machine Learning
Advanced Analytics
Dynamic Analysis

Reputation Filtering and File Sandboxing
AMP Provides Continuous Retrospective Security

Breadth of Control Points

- Email
- Endpoints
- Web
- Network
- IPS
- Devices

Telemetry Stream

File Fingerprint and Metadata
File and Network I/O
Process Information

Continuous Feed

Inspection verdicts

Continuous Analysis
Retrospective Analysis: File Trajectory

Quickly Understand the Scope of Malware Problem

Looks **ACROSS** the organisation and answers:

- What systems were infected?
- Who was infected first ("patient 0") and when did it happen?
- What was the entry point?
- When did it happen?
- What else did it bring in?
Agenda

Introduction to NGFW Deployment
Software Architecture
Licensing
How to configure policies
Management and Eventing
Functional Distribution of Features

URL Category/Reputation
NGIPS
Application Visibility and Control
Advanced Malware Protection

TCP Normalisation
TCP Intercept
IP Option Inspection
IP Fragmentation
Botnet Traffic Filter

FirePOWER Services
File Type filtering
File capture

ASA
NAT
Routing
ACL
VPN Termination
Failover & Clustering
Licensing

- Five (5) feature license packages are available
- AVC is part of the default offering
- One (1) and three (3) year terms are available
- SMARTnet is ordered separately with the appliance
How to Add FirePOWER Services to an ASA-5500-X

• Purchase ASA5500X-SSD120=
  – Adds Solid State Disc drive to ASA platform
  – Two drives required for ASA-5545 / 5555 (mirror redundancy)

• Purchase $0 ASA55xx-CTRL-LIC=
  – Adds perpetual “Protect and Control” license

• Purchase FS-VMW-x-SW-K9
  – FireSIGHT Management Centre Virtual Appliance
  – 2 and 10 device SKU’s can NOT be upgraded later

• Purchase additional licenses as needed (not required)
  – URL / IPS / AMP offered as 1 or 3 year subscriptions
Agenda

Introduction to NGFW
Software Architecture
Licensing

Deployment
How to configure policies
Management and Eventing
FirePOWER Services Support All Current ASA Deployment Models

Clustering for linear scalability

- Up to 16x ASA in cluster
- Eliminates Asymmetrical traffic issues
- Each FirePOWER Services module inspects traffic independently

*State sharing does not occur between FirePOWER Services Modules

Multi-context mode for policy flexibility

- Each ASA Interface appears as a separate interface to FirePOWER Services module
- Allows for granular policy enforcement on both ASA and FirePOWER services

Clustering for linear scalability

- Up to 16x ASA in cluster
- Eliminates Asymmetrical traffic issues
- Each FirePOWER Services module inspects traffic independently

Multi-context mode for policy flexibility

- Each ASA Interface appears as a separate interface to FirePOWER Services module
- Allows for granular policy enforcement on both ASA and FirePOWER services

HA for increased redundancy

- Redundancy and state sharing (A/S & A/A pair)
- L2 and L3 designs
Installing FirePOWER Services
Installation Steps

1. Ensure requirements are met
2. Uninstall any existing Cisco IPS or CX module (if applicable)
3. Download ASA FirePOWER Boot Image and System Software packages from Cisco
4. Copy the ASA FirePOWER boot image to the ASA Flash
5. Start the recovery procedure to install the boot image
6. Host the FirePOWER system software package on an HTTP(S) or FTP server
7. Use the initial setup dialogue and system install command to install the system software package
8. Once installed, open a console session to complete the system configuration wizard.
9. Add the FirePOWER sw-module into FireSIGHT Management Centre.
10. Configure ASA to redirect traffic to the module
Requirements

- FirePOWER services is **pre-installed** on ASA5500-X **FirePOWER bundles**
  - I.e. ASA5525-FPWR-BUN SKU
- Installation for FirePOWER services on a ASA5500-X platform requires an **SSD drive**
  - ASA5500-X-SSD12= SKU

Order ASA with SSD

ciscoasa# show inventory
Name: "Chassis", DESCR: "ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC"
PID: ASA5515 , VID: V01 , SN: FGL1620413M

Name: "Storage Device 1", DESCR: "Unigen 128 GB SSD MLC, Model Number: UGB88RRA128HM3-EMY-DID"
PID: N/A , VID: N/A , SN: 11000046630
Uninstall Classic IPS or CX Software Module (5500)

- Backup IPS configuration via CLI/IDM/IME/CSM or CX configuration via Prime Security Manager
- Shut-down IPS/CX software module:
  ```
  sw-module module ips/cxsc shutdown
  ```
- Remove IPS/CX commands from Policy-Map configuration
- Uninstall the IPS software module:
  ```
  sw-module module ips/cxsc uninstall
  ```
- Reboot ASA:
  ```
  reload
  ```
- Install the FirePOWER software module
Uninstall Classic IPS or CX Software Module (5585)

- Backup IPS configuration via CLI/IDM/IME/CSM or CX configuration via Prime Security Manager
- Shut-down IPS/CX hardware module:
  ```
  hw-module module 1 shutdown
  ```
- Remove IPS/CX commands from Policy-Map configuration
- Shut-down and power off the ASA:
  ```
  shutdown
  ```
- Remove the IPS/CX module and replace it with the FirePOWER module
- Power On the ASA
- Complete the setup of the FirePOWER module
Installing the Boot Image

- Verify the boot image is present on ASA Flash

```
ciscoasa# show disk0
Directory of disk0:/
113 -rwx 37416960 13:03:22 Jun 10 2014 asa920-104-smp-k8.bin
114 -rwx 17790720 13:04:16 Jun 10 2014 asdm-711-52.bin
118 -rwx 69318656 13:09:10 Jun 10 2014 asasfr-5500x-boot-5.3.1-152.img
```

- Verify the SSD is present

```
ciscoasa# show inventory
Name: "Chassis", DESCR: "ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC“ PID: ASA5515, VID: V01, SN: FGL1620413M

Name: "Storage Device 1", DESCR: "Unigen 128 GB SSD MLC, Model Number: UGB88RRA128HM3-EMY-DID"
PID: N/A, VID: N/A, SN: 11000046630
```

- Start the “recovery” procedure to install the boot image

```
ciscoasa# sw-module module sfr recover configure image disk0:/asasfr-5500x-boot-5.3.1-152.img
```
```
ciscoasa# sw-module module sfr recover boot
```
Verify FirePOWER Services Booted (15 min)

ciscoasa# show module sfr details

Card Type: FirePOWER Services Software Module
Model: ASA5545

[OUTPUT OMITTED]
App. version: 5.3.1-152
Data Plane Status: Not Applicable

Console session: Ready
Status: Recover

- Session into the SFR Boot image and log in

ciscoasa# session sfr console

Opening console session with module sfr.
Connected to module sfr. Escape character sequence is ‘CTRL-^X’.

Cisco ASA SFR Boot Image 5.3.1

asasfr login: admin
Password: Admin123
Software Package Installation

- Run the initial SFR-boot setup wizard to configure basic settings such as IP address.

```
Cisco ASA SFR Boot 5.3.1 (152)

asasfr-boot>setup
Welcome to SFR Setup
Enter a hostname [asasfr]: asasfr
Enter an IPv4 address [192.168.8.8]:
```

- Download and install the System Software image using the `system install` command.

```
asasfr-boot>system install ftp://10.89.145.63/asasfr-sys-5.3.1-152.pkg
Verifying

Package Detail
  Description:                   Cisco ASA-SFR 5.3.1-152 System Install
  Requires reboot:                Yes

Do you want to continue with upgrade? [y]:

Upgrading
Starting upgrade process ...
Populating new system image...
```
Complete System Configuration

- After a reboot wait for installation to complete and session to the FirePOWER module
  
  \[
  \text{ciscoasa\# session sfr}
  \]

  Opening console session with module sfr.
  Connected to module sfr. Escape character sequence is ‘CTRL-^X’.

  Sourcefire ASA5525 V5.3.1
  Sourcefire3D login:

  Username: Admin
  Password: Sourcefire

- Complete the system configuration as prompted

  System initialization in progress. Please stand by.
  You must change the password for 'admin' to continue.
  Enter new password: <new password>
  Confirm new password: <repeat password>
  You must configure the network to continue.
  You must configure at least one of IPv4 or IPv6.
  Do you want to configure IPv4? (y/n) [y]: y
  [OUTPUT OMITTED]
FireSIGHT Management Centre Setup

- Identify the FireSIGHT Management Centre that will manage this device

```bash
> Configure manager add 10.89.145.102 cisco123
Manager successfully configured.
```

Last step..
Summary of Module Installation

– FirePOWER Services module installs as a software module on Cisco ASA 5500-X platforms and as a hardware module on the Cisco ASA 5585-X

– Both hardware and software modules are managed by the FireSIGHT Management Centre (also known as Defence Centre)

– Traffic is redirected to module using ASA Service Policy

– ASA features and functions are managed using ASDM or CSM including the traffic redirection. FirePOWER policy configuration and other features require FireSIGHT Management Centre
Adding FP Module to FireSIGHT

- Launch FireSIGHT Management Centre and add licenses
- Create an access policy to be used by the FirePOWER Sensor
- Perform initial configuration on module
- Import FirePOWER Sensor and apply policy
- Traffic redirection from ASA
Add License(s) to FireSIGHT

- Log into FireSIGHT Console
- System -> Licenses TAB
- License registered to FireSIGHT MAC address
- Add + Submit the license(s)
Create Access Policy for FirePOWER Module

- Navigate to Policies -> Access Control.
  - Click New Policy
- Configure Name & Description (optional)
- Default Action of Intrusion Prevention is best practice
- Available Devices will not show your new ASA FirePOWER sensor until added
Add FirePOWER Sensor into FireSIGHT

- Use the FireSIGHT Management Centre - Device Manager to add the device
- Choose Access Control Policy you configured previously (or Default)

Module IP address and registration key
Licenses applied to FireSIGHT MC
Agenda

Introduction to NGFW
Software Architecture
Licensing
Deployment
Traffic redirection from ASA
Management and Eventing
Compatibility with ASA Features

– Minimum ASA version: 9.2.2
– Guidelines for traffic sent to the ASA FirePOWER module:
  • Do not configure ASA inspection on HTTP traffic.
  • Do not configure Cloud Web Security Inspection
  • Other application inspections on the ASA are compatible with the FirePOWER module
  • Do not enable Mobile User Security (MUS) Server; it is not compatible with the FirePOWER module
– In ASA Failover/Clustering mode, configuration between different modules is not automatically synchronised (FireSIGHT will handle this)
Configure ASA to Redirect Traffic to the Module

- Traffic Redirection is done using Service Policies as a part of ASA MPF
- Traffic for inspection can be matched based on interface, source/destination, protocol ports and even user identity
- In Multi-context-mode, different FirePOWER policies can be assigned to each context
- MPF can be configured from CLI, ASDM or CSM
- **Fail-open** and **Fail-closed** options are available
- **Monitor-only mode** option for a “passive” deployment.

```
policy-map global_policy
class class-default
  sfr fail-open

service-policy global_policy global
```
Configure ASA to Redirect Traffic using ASDM

Configure -> Firewall -> Service Policy Rules -> Global Policy

Edit Service Policy Rule

Traffic Classification | ACL | Rule Actions |

The Rule Actions are applied to all the rules grouped in the Traffic Match.

Protocol Inspection | ASA FirePOWER Inspection | Connection Settings | QoS | User Statistics

- Enable ASA FirePOWER for this traffic flow
  - If ASA FirePOWER Card Fails
    - Permit traffic
    - Close traffic

Promiscuous Mode

- Enable Monitor Only
User Identification

User identification uses two distinct mechanisms

1. Network discovery
   • Understands AIM, IMAP, LDAP, Oracle, POP3 and SIP
   • Will only provide limited information when deployed at the Internet edge

2. Sourcefire User Agent (SFUA)
   • Installed on a Windows Platform
   • Windows server *does not* have to be a domain member
   • Communicates with the AD using WMI – starts on port 136 then switches to random TCP ports
   • Communicates with FMC through a persistent connection to TCP port 3306 on the FMC
   • Endpoints must be domain members
   • Well-suited for Internet edge firewalls

Note: This solution does not use the Cisco Context Directory Agent (CDA)
Agenda

- Introduction to NGFW
- Software Architecture
- Licensing
- Deployment
- How to configure policies
- Management and Eventing
FireSIGHT Management Centre

Single console for event, policy, and configuration management
Create report from any dashboard
Indications of Compromise (IoCs)

- IPS Events
  - Malware Backdoors
  - CnC Connections
  - Exploit Kits
  - Web App Attacks

- Security Intelligence Events
  - Connections to Known CnC IPs

- Malware Events
  - Malware Detections
  - Office/PDF/Java Compromises
  - Malware Executions
  - Dropper Infections

![Indications of Compromise Table](image)
Impact Assessment

Correlates all intrusion events to an impact of the attack against the target

<table>
<thead>
<tr>
<th>IMPACT FLAG</th>
<th>ADMINISTRATOR ACTION</th>
<th>WHY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Act Immediately, Vulnerable</td>
<td>Event corresponds to vulnerability mapped to host</td>
</tr>
<tr>
<td>2</td>
<td>Investigate, Potentially Vulnerable</td>
<td>Relevant port open or protocol in use, but no vuln mapped</td>
</tr>
<tr>
<td>3</td>
<td>Good to Know, Currently Not Vulnerable</td>
<td>Relevant port not open or protocol not in use</td>
</tr>
<tr>
<td>4</td>
<td>Good to Know, Unknown Target</td>
<td>Monitored network, but unknown host</td>
</tr>
<tr>
<td>0</td>
<td>Good to Know, Unknown Network</td>
<td>Unmonitored network</td>
</tr>
</tbody>
</table>
FireSIGHT™ Streamlines Operations

- Recommended Rules
Class-Leading NGFW Context and Visibility Demo
Summary: Cisco ASA with FirePOWER Services

Industry’s First Adaptive, Threat-Focused NGFW

Cisco ASA is world’s most widely deployed, enterprise-class stateful firewall

Granular Cisco® Application Visibility and Control (AVC)

Industry-leading FirePOWER next-generation IPS (NGIPS)

Reputation- and category-based URL filtering

Advanced malware protection
Useful links:

ASA with FirePOWER Services Download link:

Release Notes:

Installation guide:

User guide:
Recommended Sessions

- BRKSEC-2088 - Using Cisco FireSIGHT system to protect ICS / IoT Systems
- BRKSEC-2134 - Building a Highly Secure Internet Edge
- BRKSEC-2762 - The FirePOWER Platform and Next Generation Network Security
- BRKSEC-3126 - Configuration and Tuning of FirePOWER Services for ASA
- LABSEC-2339 - Cisco ASA with FirePOWER services
Cisco 2015 Annual Security Report

Now available:
cisco.com/go/asr2015
Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

• Directly from your mobile device on the Cisco Live Mobile App
• By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
• Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com
Thank you.