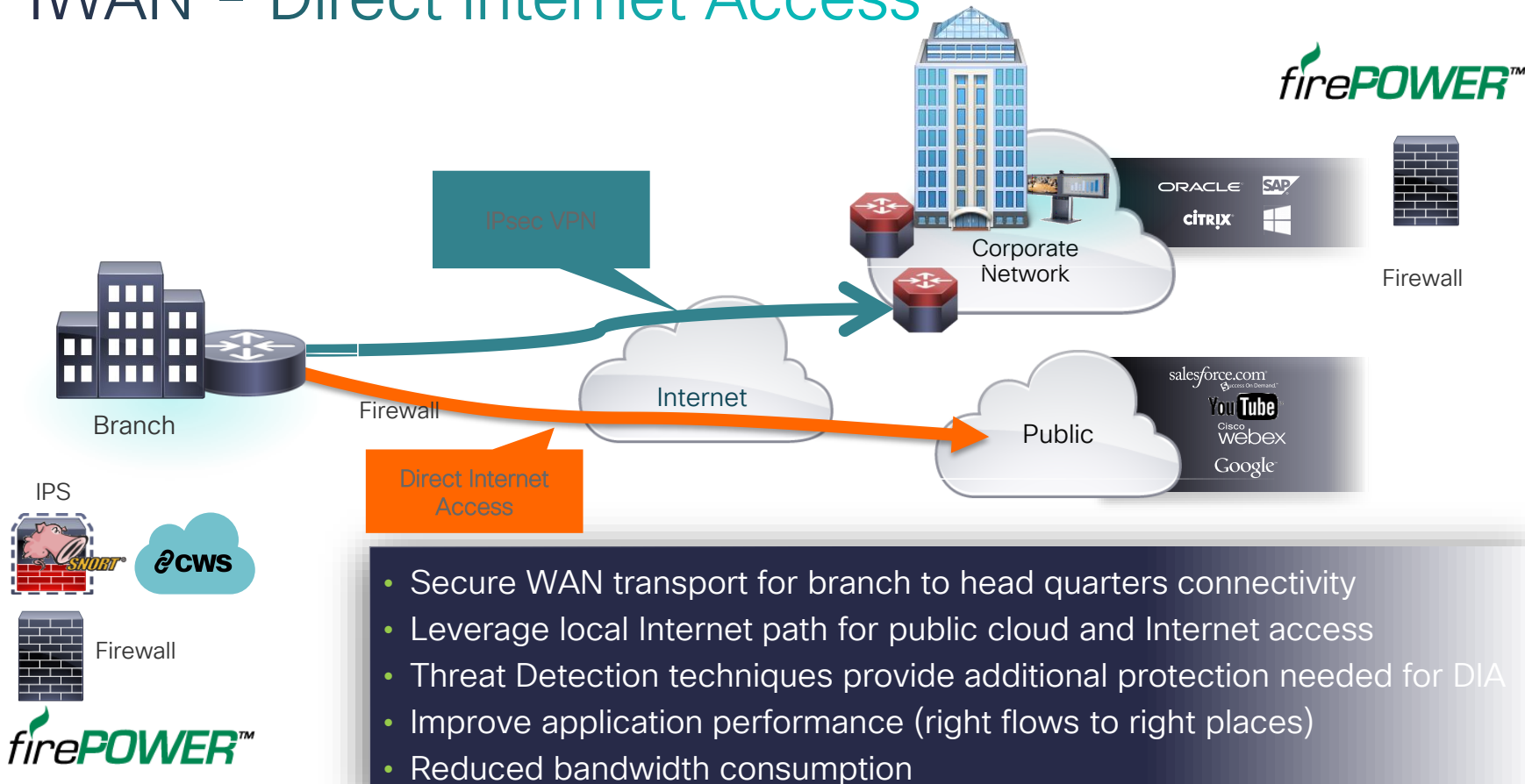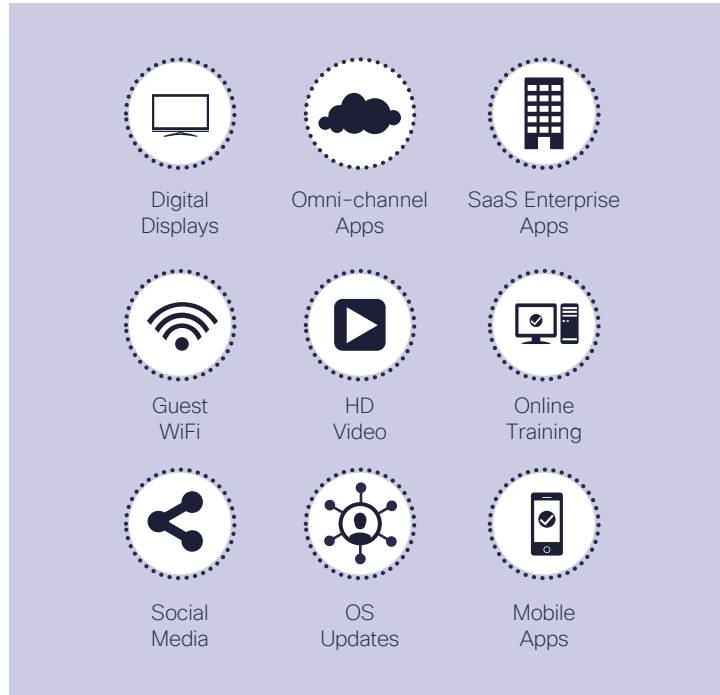# Agenda

- Overview and Use Cases

- How to use tools such as ZBFW, Snort IPS, CWS, FirePower & TrustSec

- How to deploy and manage security policies and events using Cisco Prime and FireSight

- Use of third party tools such as LiveAction and Splunk

IWAN - Direct Internet Access

*fire***POWER**™

IPsec VPN

Corporate
Network

ORACLE SAP
CITRIX Windows

Firewall

Branch

Firewall

Direct Internet
Access

Internet

Public

salesforce.com
YouTube
Cisco
webex
Google

IPS

SNORT CWS

Firewall

*fire***POWER**™

- Secure WAN transport for branch to head quarters connectivity
- Leverage local Internet path for public cloud and Internet access
- Threat Detection techniques provide additional protection needed for DIA
- Improve application performance (right flows to right places)
- Reduced bandwidth consumption

Enterprise Challenges

Digital
Displays

Omni-channel
Apps

SaaS Enterprise
Apps

Guest
WiFi

HD
Video

Online
Training

Social
Media

OS
Updates

Mobile
Apps

BRANCH

MORE USERS

80%
Of employee and customers are served in branch offices*

MORE DEVICES

73%
Growth in in mobile devices from 2014 - 2018**

MORE APPS

20-50%
Increase in Enterprise bandwidth per year through 2018**

MORE THREATS

30%
Of advanced threats will target branch offices by 2016 (up from 5%) **

*Tech Target, Branch Office Growth Demands New Devices., 2013
**Gartner, Forecast Analysis: Worldwide Enterprise Network Services, Q2 2014 Update
*** Gartner: "Bring Branch Office Network Security Up to the Enterprise Standard, Jeremy D'Hoinne, 26 April. 2013.

Positioning IPS/IDS Solution for the WAN

Regulatory/ PCI Compliance

Internet guest access

MSSP

Direct Internet access to partner sites or public cloud (i.e. Office365, Salesforce.com)

Partial DIA

Full DIA

firePOWER™

firePOWER™

CWS

CWS

ISR 4451 - 2Gbps
ISR 4431 – 1 Gbps

ISR 4351
200-400 Mbps

ISR 4331
100-300 Mbps

ISR 4321
50-100 Mbps

Cisco FirePOWER Threat Defense for ISR

FirePOWER Threat Defense

Attack Continuum

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Network Visibility

Granular App Control

Modern Threat Control

NGIPS

Security Intelligence

URL Filtering

Advanced Malware Protection

Retrospective Security

IoCs/Incident Response

Visibility and Automation
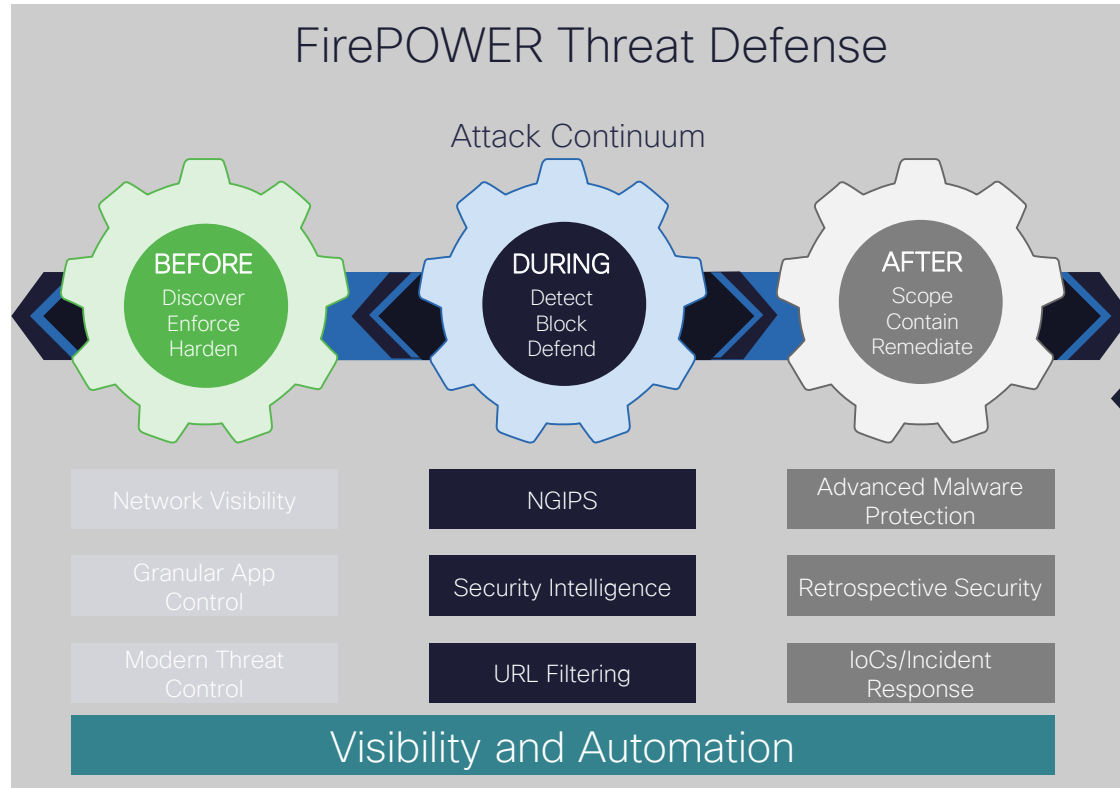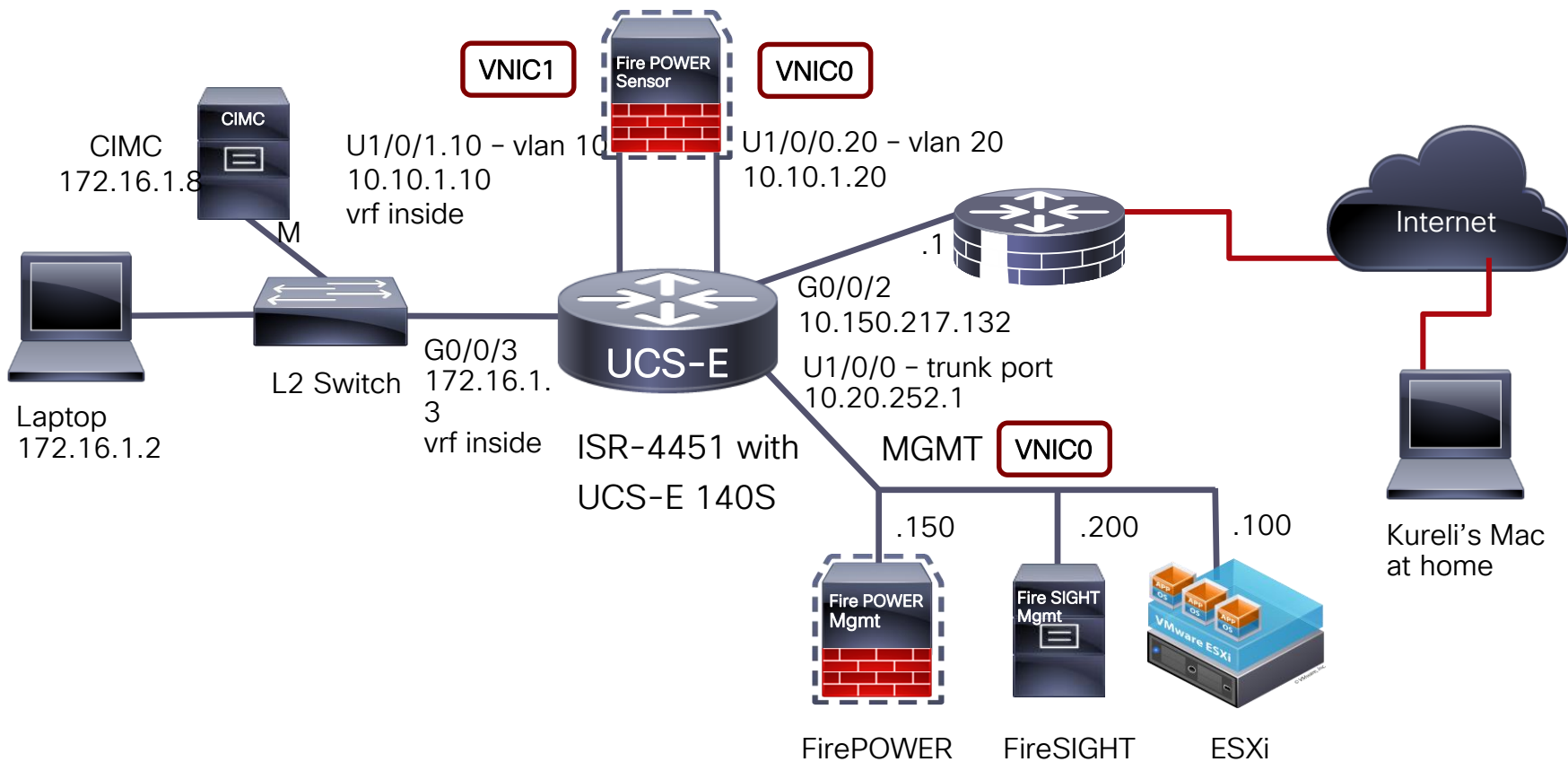
- Capitalize on DIA Without Compromising Security
- Industry-Leading Threat Protection for Branch and Remote Offices
- Consolidated Footprint Frees Revenue-Generating Square Footage
- Centralized Management with Clearly Divided Roles and Responsibilities
- Lower Total Cost of Ownership

Cisco FirePOWER Threat Defense for ISR - IPS

VNIC1

Fire POWER Sensor

VNIC0

CIMC

CIMC
172.16.1.8

U1/0/1.10 – vlan 10
10.10.1.10
vrf inside

U1/0/0.20 – vlan 20
10.10.1.20

M

.1

Internet

G0/0/2
10.150.217.132

UCS-E

G0/0/3
172.16.1.
3
vrf inside

L2 Switch

Laptop
172.16.1.2

U1/0/0 – trunk port
10.20.252.1

ISR-4451 with
UCS-E 140S

MGMT   VNIC0

.150   .200   .100

Fire POWER Mgmt

Fire SIGHT Mgmt

VMware ESXi

FirePOWER   FireSIGHT   ESXi

Kureli's Mac
at home

Check out some additional information on Thread Defense
on the Cisco Support Community or Cisco.com

FireSIGHT, Firepower (Sourcefire) License Matrix

https://supportforums.cisco.com/document/12455001/firesight-firepower-sourcefire-license-matrix

Cisco Threat Awareness Service - Quick Start Guide

https://supportforums.cisco.com/document/12868431/cisco-threat-awareness-service-quick-start-guide

If you are not yet a registered user on the community, Click here to register and become an active participant on the community.

Hope you enjoyed this little peek into the webcast.

Remember it was just a peek. March 22, you get a chance to see the whole thing.

Register Now: http://bit.ly/mar22-16-ENwebcast

At the webcast you will be able to learn so much more and get a chance to submit questions for the expert to answer during the broadcast.
We'll see you there!