Cisco Tech Update – Security X-mas 2012

Rasmus Kamper Mathiasen
Security Systems Engineer
Cisco Denmark

Agenda

- ASA-CX Gennemgang
- ASA-CX Demo
- ASA 9.0 (SGA / Cisco Cloud Web Sec)
- ASA 9.0 med CCWS Demo
- Pause
- Unified Access Gennemgang
- Unified Access Demo – BYOD/SGA/ PRIME
- Cisco Security ELA (Enterprise License Agreement)
- Diverse Nyheder

Agenda

- ASA-CX Gennemgang
- ASA-CX Demo
- ASA 9.0 (SGA / Cisco Cloud Web Sec)
- ASA 9.0 med CCWS Demo
- Pause
- Unified Access Gennemgang
- Unified Access Demo – BYOD/SGA/ PRIME
- Cisco Security ELA (Enterprise License Agreement)
- Diverse Nyheder

Complete Context

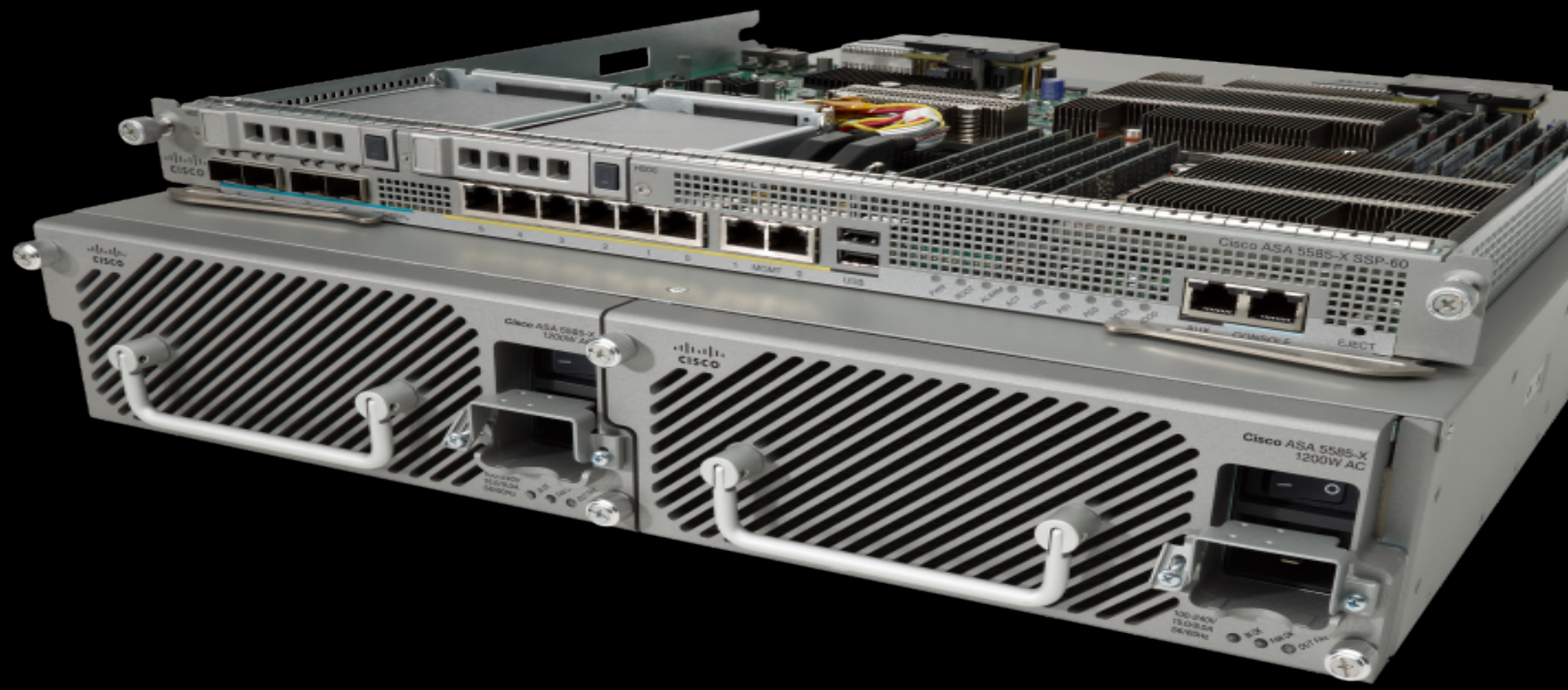
Visibility **with** Control

Productivity **with** Security

Next-Generation **with** Stateful Firewall

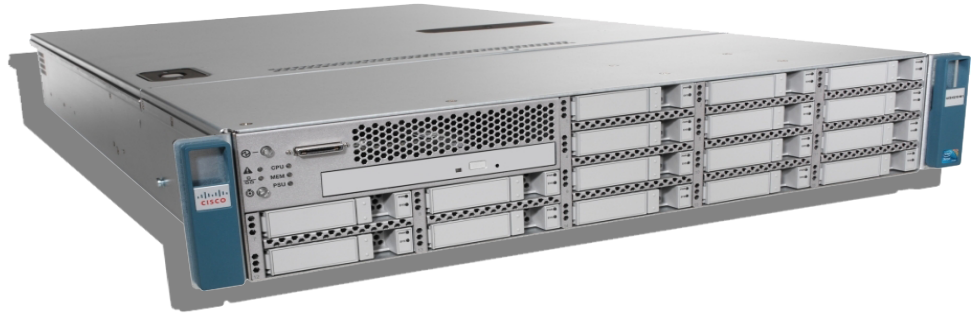
ASA CX

- Context-Aware Firewall
- Active/Passive Authentication
- Application Visibility and Control
- Reputation Filtering
- URL Filtering
- Secure Mobility
- SSL Decryption
- Available as a sw/hw module on selected existing ASA hardware



PRMS – Prime Security Manager

- Two deployment Options
  - Virtual Machine (VM) CCO
    - UCS Bundle
- Virtual Machine
  - Delivered as single file with .ova extension
  - Open Virtual Appliance (OVA) format
  - VMware vSphere Hypervisor 4.1 (Update 2)
- UCS Bundle
  - UCS C220 M3 Server + ESXi 4.1 U2 + VM



Applications: Visibility With Control

WHAT

Broad…

… classification
of all traffic

1,000+ apps

MicroApp Engine

Deep classification
of targeted traffic

75,000+ MicroApps

App Behavior

Control user interaction with the application

Business Class URL Filtering

Industry-leading coverage and efficacy

60 languages

200 countries

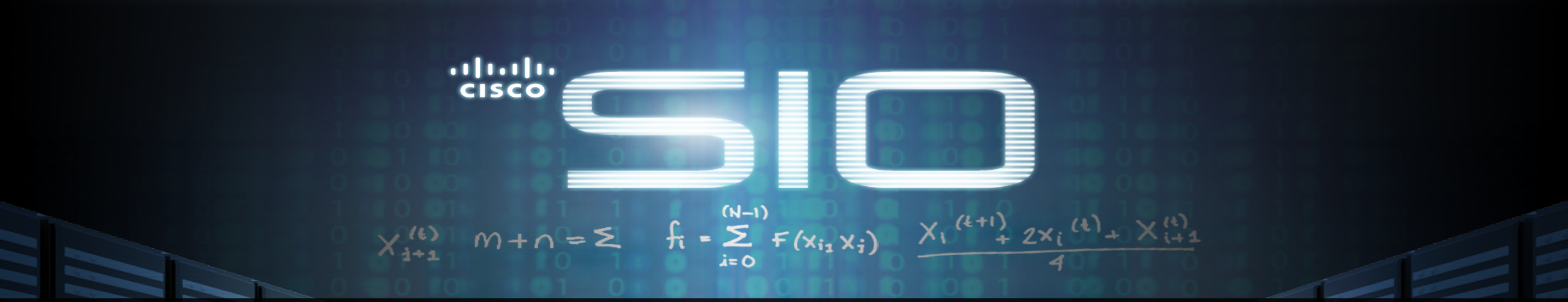
20 mn URLs

98% coverage

Complete Context. **Plus** Threat Awareness.

cisco

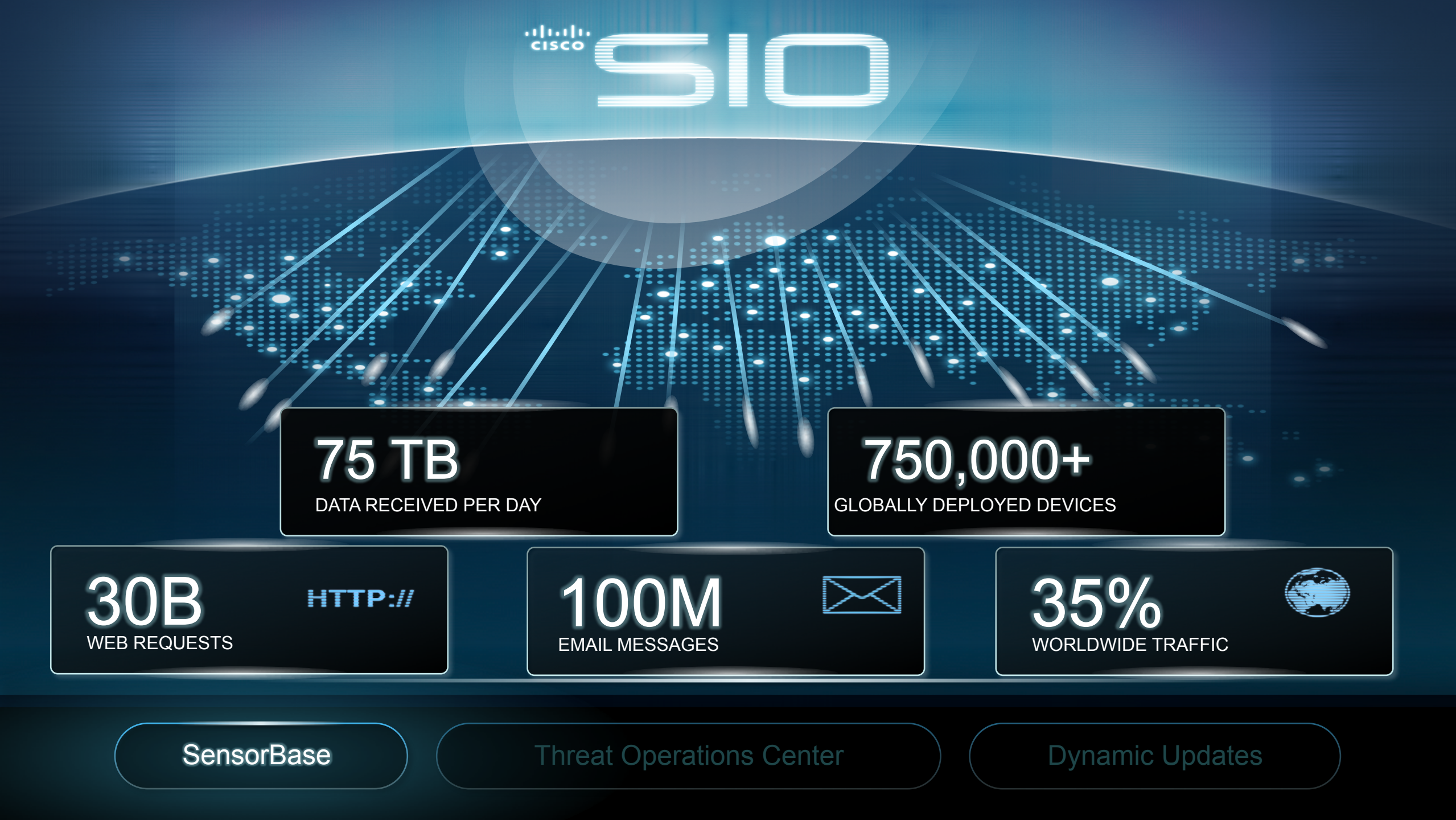
SIO



SensorBase

Threat Operations Center

Dynamic Updates


cisco
SIO
75 TB
DATA RECEIVED PER DAY
750,000+
GLOBALLY DEPLOYED DEVICES
30B
WEB REQUESTS
HTTP://
100M
EMAIL MESSAGES
35%
WORLDWIDE TRAFFIC
SensorBase
Threat Operations Center
Dynamic Updates


cisco
SIO
$100M
SPENT IN DYNAMIC RESEARCH AND DEVELOPMENT
24x7x365
OPERATIONS
500
ENGINEERS, TECHNICIANS AND RESEARCHERS
40+
LANGUAGES
80+
Ph.D.s, CCIE, CISSPs, MSCEs
SensorBase
Threat Operations Center
Dynamic Updates


cisco
SIO
3 to 5
MINUTE UPDATES
6,500+
IPS SIGNATURES PRODUCED
20+
PUBLICATIONS PRODUCED
200+
PARAMETERS TRACKED
8M+
RULES per DAY
SensorBase
Threat Operations Center
Dynamic Updates

Full-Spectrum User Identification

Covers Wide Breadth of Identity Use Cases

Fidelity

NTLM
Kerberos

User Authentication
- Auth-Aware Apps
- Mac, Windows, Linux
- AD/LDAP user credential

TRUSTSEC*

Network Identity

Group information
Any tagged traffic

AD/LDAP Identity
- Non-auth-aware apps
- Any platform
- AD/LDAP credential

IP Surrogate
AD Agent

Breadth

* Future

Location-based Policy Control

WHERE

HOW

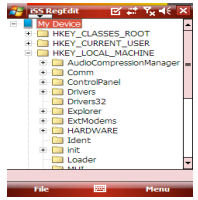
Device Identification

Information From 100,000,000 Endpoints

Device OS

OS Version

Posture*



Registry

AV

Files

AnyConnect

Identity Services Engine*

** Future*

Cisco ASA 5585-X Series High-End Lineup Solutions

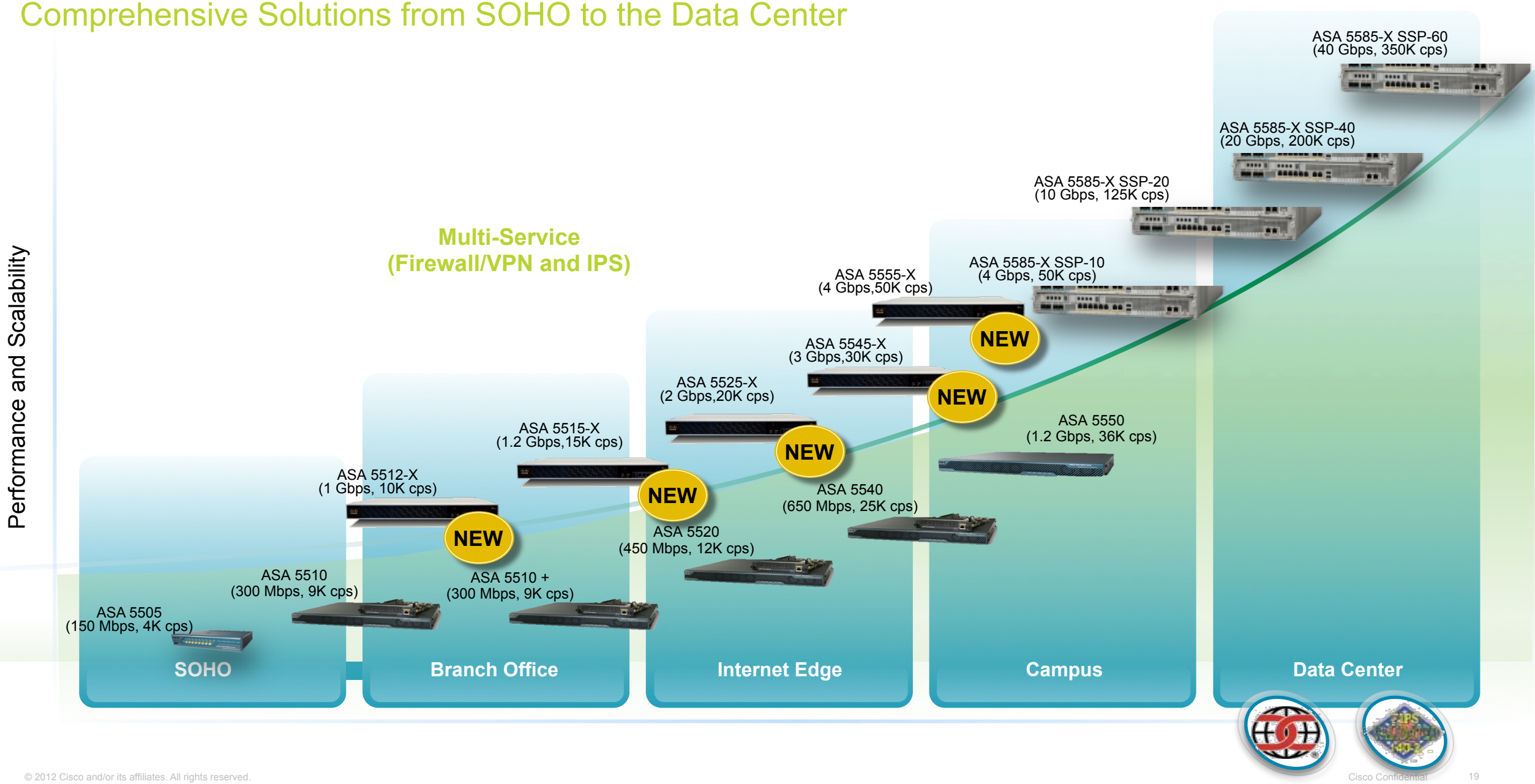
Network Location	Internet Edge/ Campus ASA 5585 SSP-10	Internet Edge/ Campus ASA 5585 SSP-20	Campus/ Data Center ASA 5585 SSP-40	Data Center ASA 5585 SSP-60
Performance				
Max Firewall	4 Gbps	10 Gbps	20 Gbps	40 Gbps
Max IPS	2 Gbps	3 Gbps	5 Gbps	10 Gbps
Max IPSec VPN	1 Gbps	2 Gbps	3 Gbps	5 Gbps
Max IPSec/SSL VPN Peers	5000	10,000	10,000	10,000
Platform Capabilities				
Max Firewall Conns	1,000,000	2,000,000	4,000,000	10,000,000
Max Conns/Second	50,000	125,000	200,000	350,000
Packets/Second (64 byte)	1,500,000	3,000,000	5,000,000	9,00,000
Base I/O	8 GE + 2 10 GE	8 GE + 2 10 GE	6 GE + 4 10GE	6 GE + 4 10GE
Max I/O	16 GE + 4 10 GE	16 GE + 4 10 GE	12 GE + 8 10GE	12 GE + 8 10GE
VLANs Supported	1,024	1,024	1,024	1,024
HA Supported	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S

Superior Edge Performance

	ASA CX SSP-10	ASA CX SSP-20
Throughput (Multi-protocol)	2 Gbps	5 Gbps
Concurrent Connections	500,000	1,000,000
New Connections / Second	40,000	75,000

Cisco ASA 5500 Series Portfolio

Comprehensive Solutions from SOHO to the Data Center



ASA-CX Demo 

Agenda

- ASA-CX Gennemgang
- ASA-CX Demo
- ASA 9.0 (SGA / Cisco Cloud Web Sec)
- ASA 9.0 med CCWS Demo
- Pause
- Unified Access Gennemgang
- Unified Access Demo – BYOD/SGA/ PRIME
- Cisco Security ELA (Enterprise License Agreement)
- Diverse Nyheder

Agenda

Security Contexts

- Dynamic Routing
- VPN for Site to Site
- Mixed Mode Firewall Support

Scansafe Integration

SGAcl

IPv6 Firewall and VPN

- Integrated IPv4 and IPv6 security policy
- NAT 66/64 and DNS 64
- DHCPv6 relay
- OSPFv3 (dynamic routing for IPv6)

Clustering

Remote Access VPN

Cisco Trustsec: Identity Services Engine

ISE: Policies for people and devices

Authorized Access

- How can I restrict access to my network?
- Can I manage the risk of using personal PCs, tablets, smart-devices?
- Access rights on-prem, at home, on the road?
- Devices are healthy?

Guest Access

- Can I allow guests Internet-only access?
- How do I manage guest access?
- Can this work in wireless and wired?
- How do I monitor guest activities?

Non-User Devices

- How do I discover non-user devices?
- Can I determine what they are?
- Can I control their access?
- Are they being spoofed?

Authentication and Authorization

802.1x/Infrastructure

Vicky Sanchez
Employee, Marketing
Wireline
3 p.m.

Frank Lee
Guest
Wireless
9 a.m.

Security Camera G/W
Agentless Asset
MAC: F5 AB 8B 65 00 D4

Francois Didier
Consultant
HQ—Strategy
Remote Access
6 p.m.

Identity Information

Group:
Full-Time Employee

Group:
Contractor

Group:
Guest

Other Conditions (Context)

Time and Date

Posture

Location

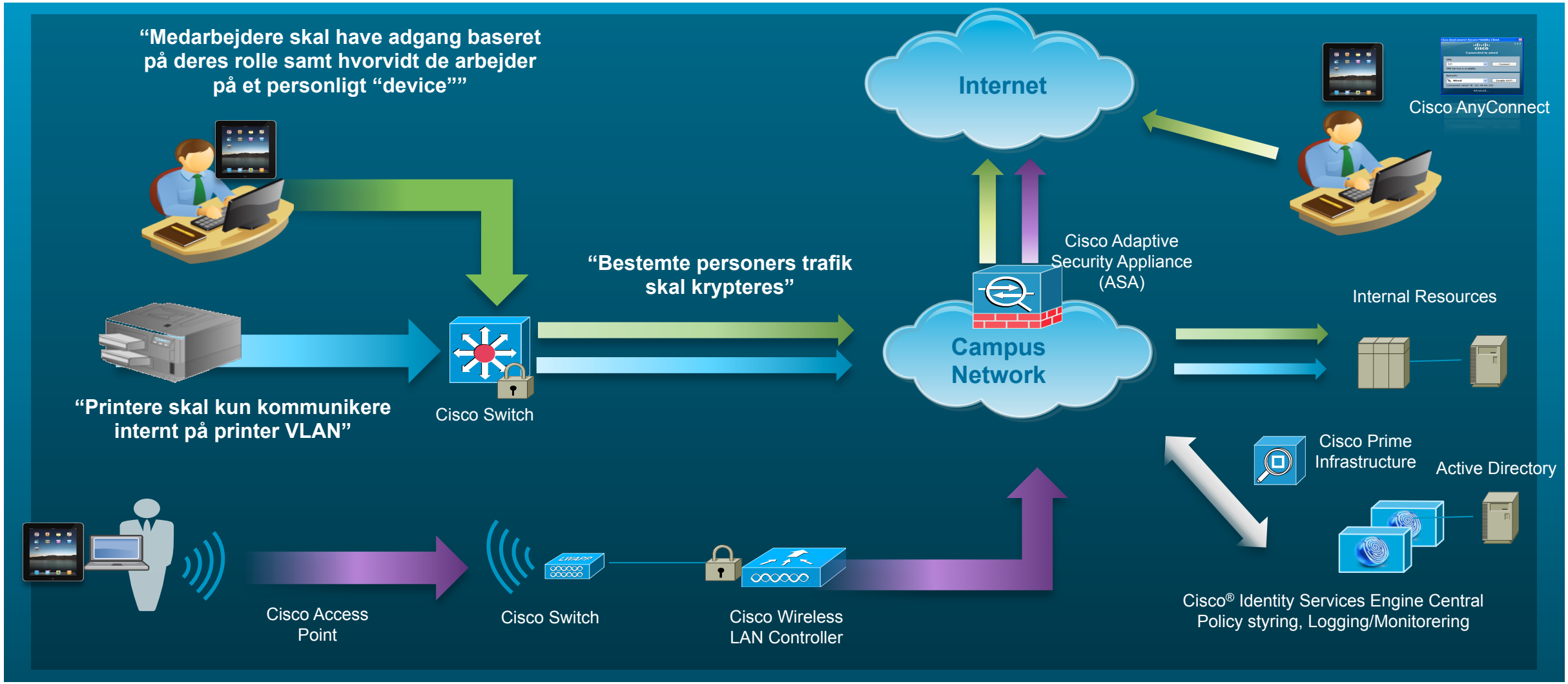
Device Type Access Type

Authorization (Controlling Access)

- Broad Access
- Limited Access
- Guest/Internet
- Quarantine
- Deny Access

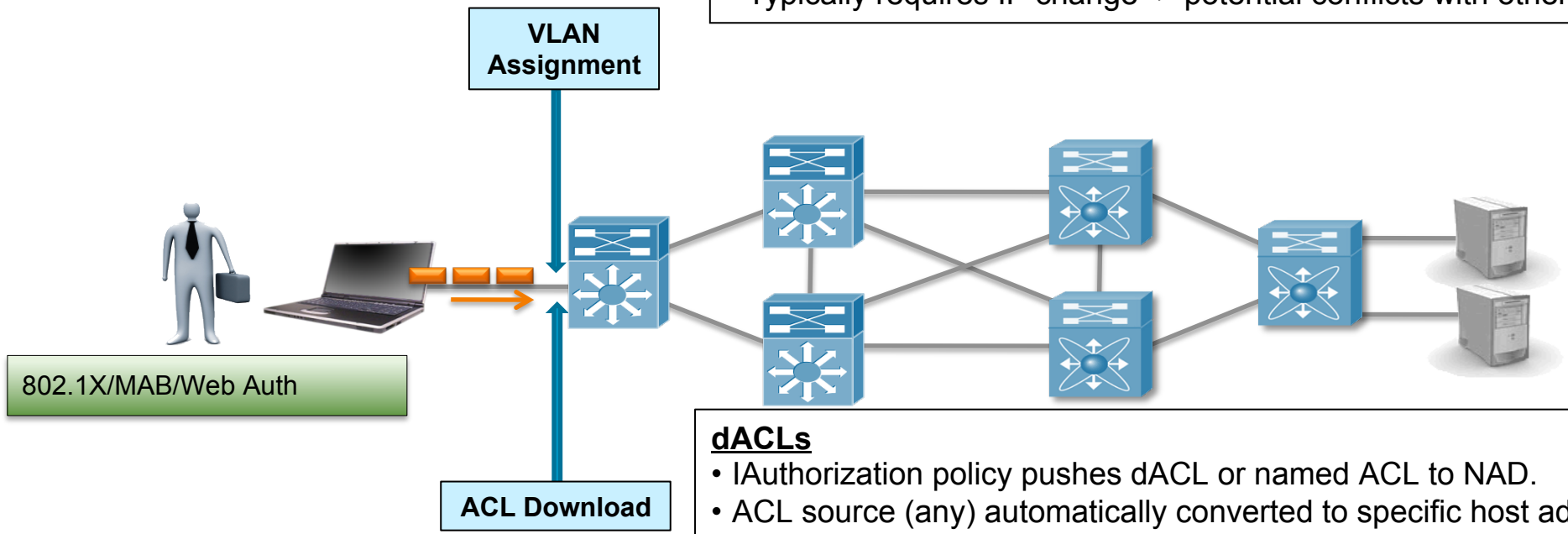
Access Compliance Reporting

A Practical Example of Policies



Policy Enforcement
VLANs and dACLs

VLANs
- Authorization policy sets VLAN. Infrastructure provides enforcement
- Typical VLAN examples:
  - Quarantine/Remediation VLAN
  - Guest VLAN
  - Employee VLAN.
- Typically requires IP change -> potential conflicts with other endpoint processes.



dACLs
- IAuthorization policy pushes dACL or named ACL to NAD.
- ACL source (any) automatically converted to specific host address
- No IP address change required, thus typically less disruptive to endpoint and improved user experience.

TrustSec Security Group Access
Marking traffic with business context

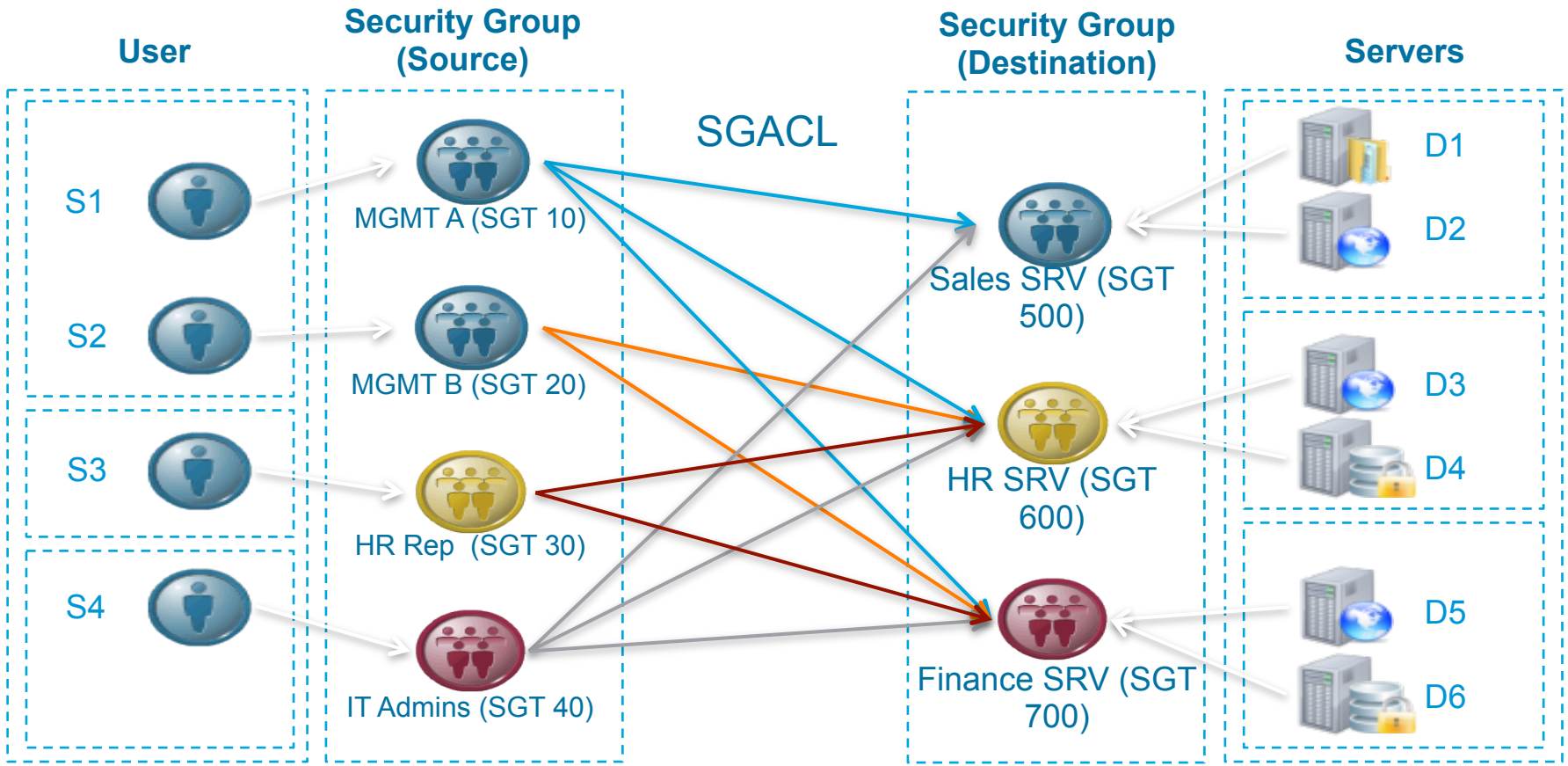
TrustSec SGA is a **context-based firewall or access control** solution :

- **Classification** of systems/users based on **context** (user role, device, location, access method) as they connect
- The context-based classification **propagates** using Security Group Tags
- Context/classification can be used by firewalls, routers and switches to make intelligent forwarding or blocking decisions
- **No IP address required in ACE** (IP address is bound to SGT)
- Policy is **distributed from central policy server (ISE)** or configured locally on TrustSec device

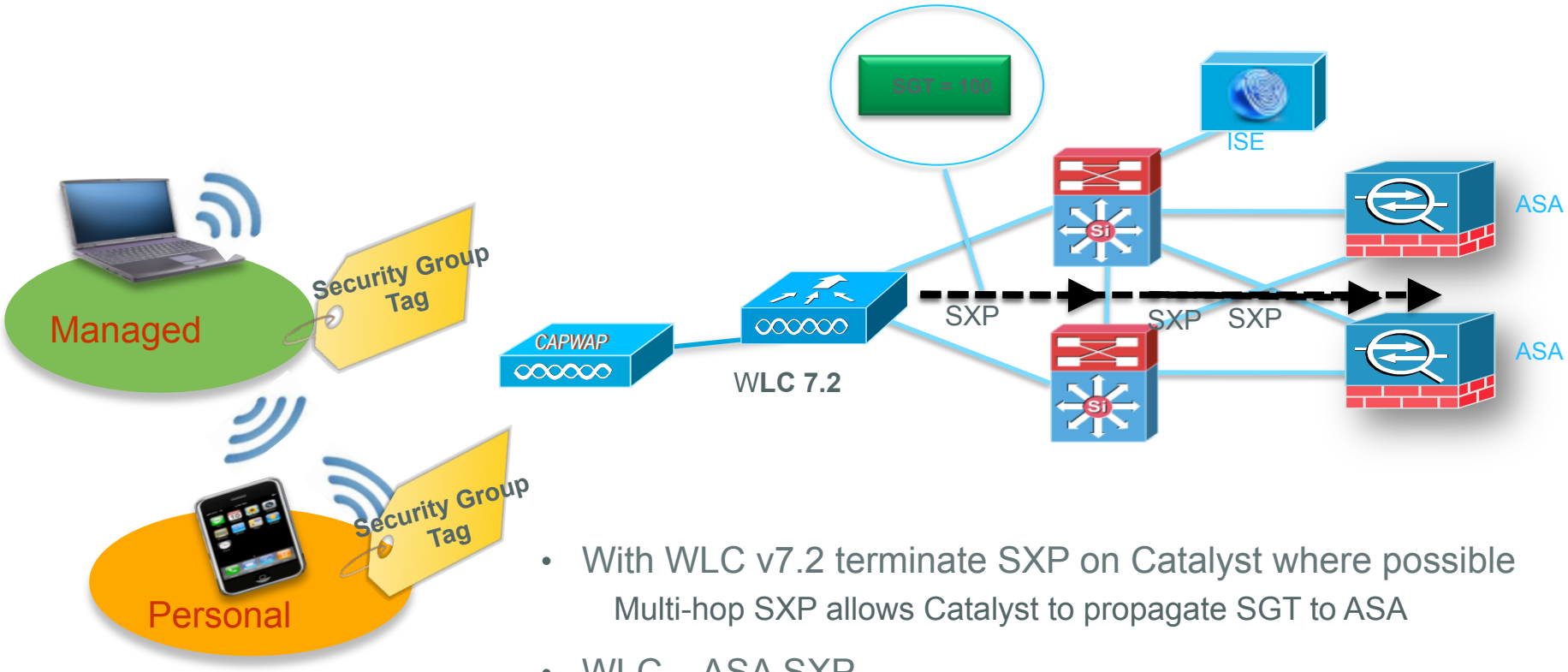
Benefits

- Provides **topology-independent** policy
- Flexible and scalable policy based on user role
- **Centralized policy management** for dynamic policy provisioning
- Egress filtering **results to reduce TCAM impact**

How SGACL Simplifies Access Control

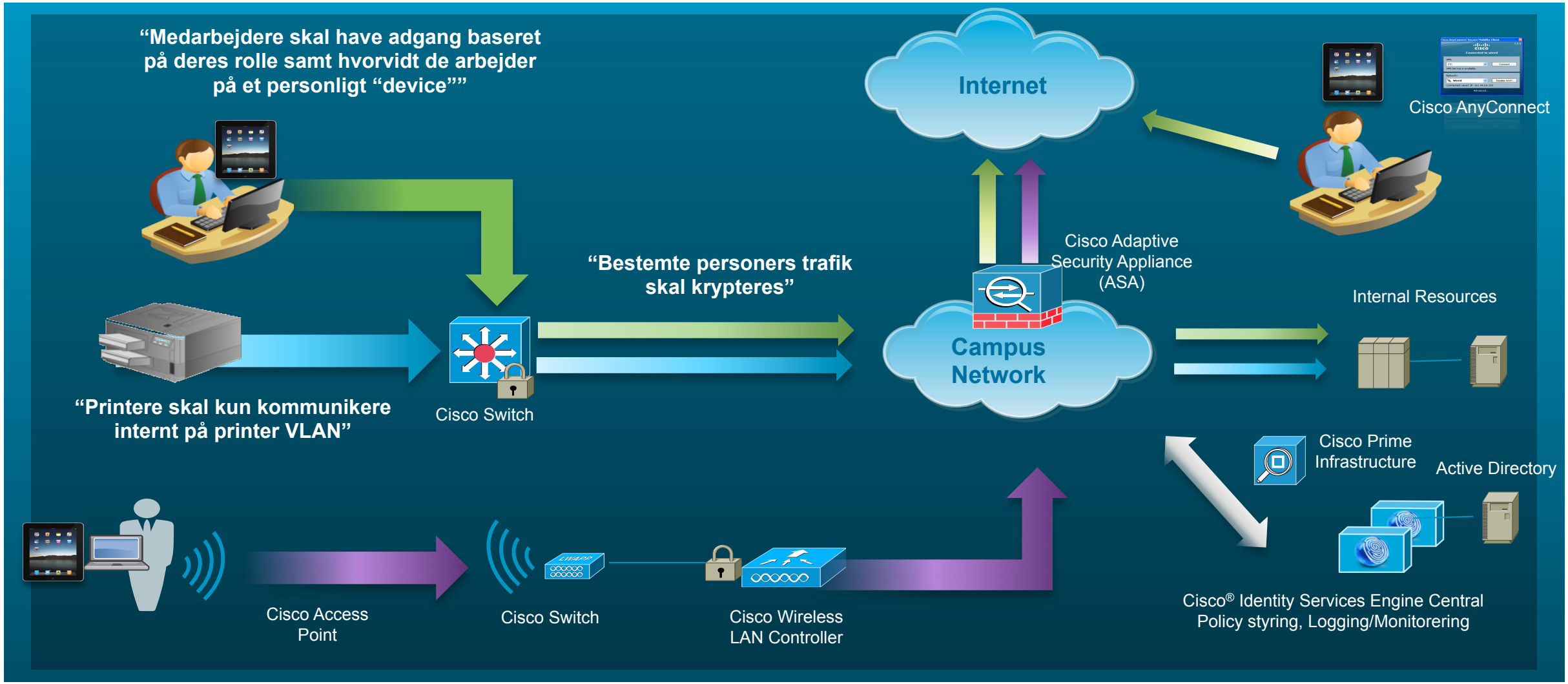


Firewalling BYOD access with ASA v9.0
Context-based policy decisions in ASA



- With WLC v7.2 terminate SXP on Catalyst where possible
  - Multi-hop SXP allows Catalyst to propagate SGT to ASA
- WLC – ASA SXP
- Differentiated BYOD access with single SSID, single VLAN design

A Practical Example of Policies



Cisco ScanSafe Cloud Services

Web Filtering

- Web Usage Controls
- Application Visibility
- Bi-directional control

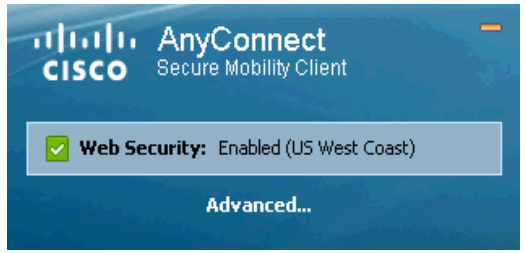
Web Security

- Anti-malware protection
- Web content analysis
- Script emulation

Centralized Reporting

Secure Mobility

Cisco Security Mobility with ScanSafe



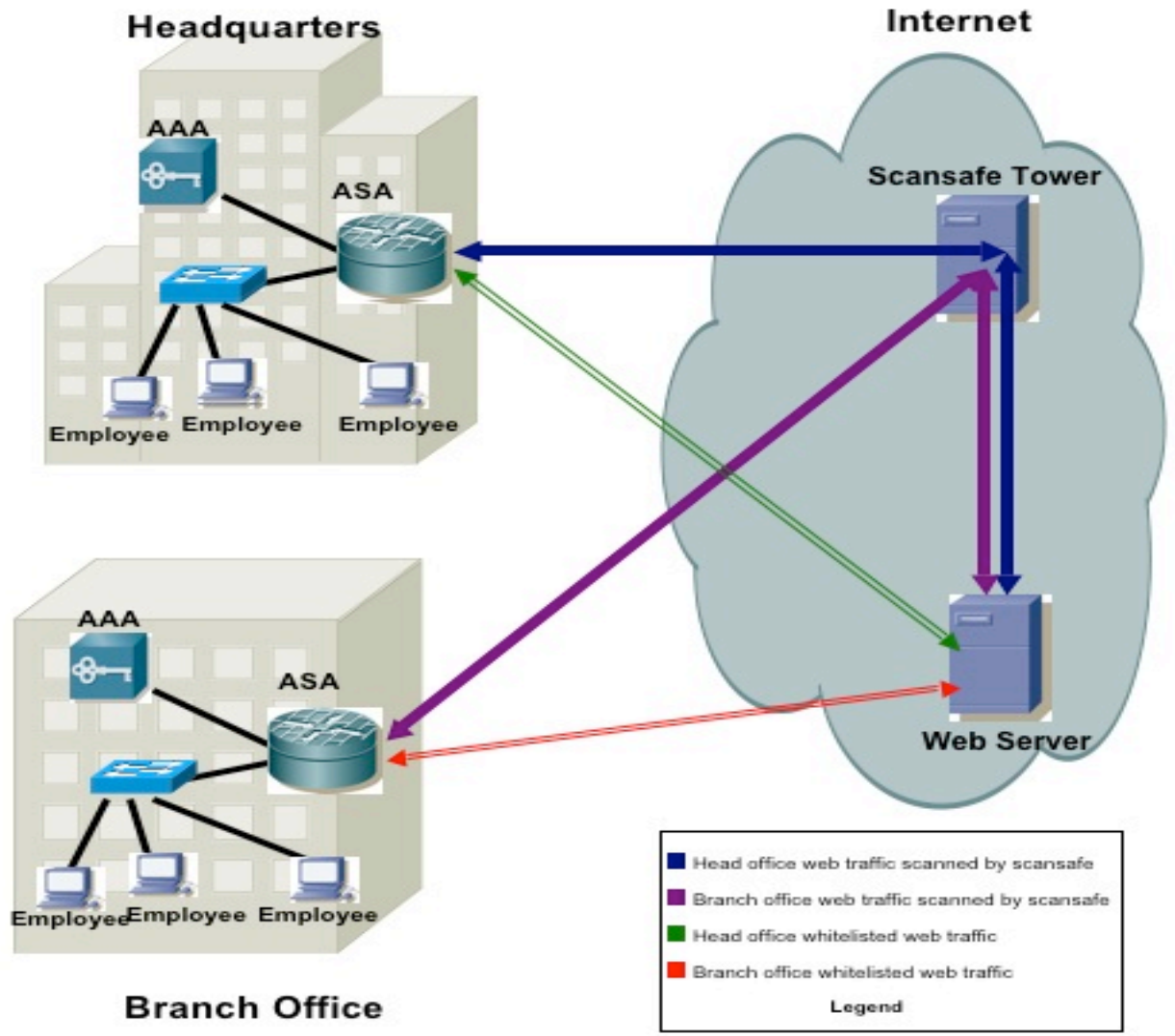
Mobile Worker

Public Wi-Fi

Home Office

- Security & policy even when off-network and off-VPN
- Connects to closest datacenter
- Seamless integration with Cisco AnyConnect client and interface

Cisco Cloud Web Security With ASA



Security Portfolio

Deployment Flexibility for Ubiquitous Security

Powered By

Cisco SIO

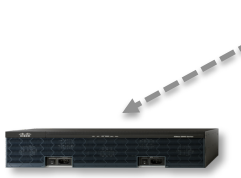
Telemetry

Intelligence

ASA CX

Cloud Web Security

Web Security Appliance
(Physical & Virtual)



ISR

WSA

ASA

AnyConnect

Cloud Connectors

ASA 9.0 med CCWS Demo

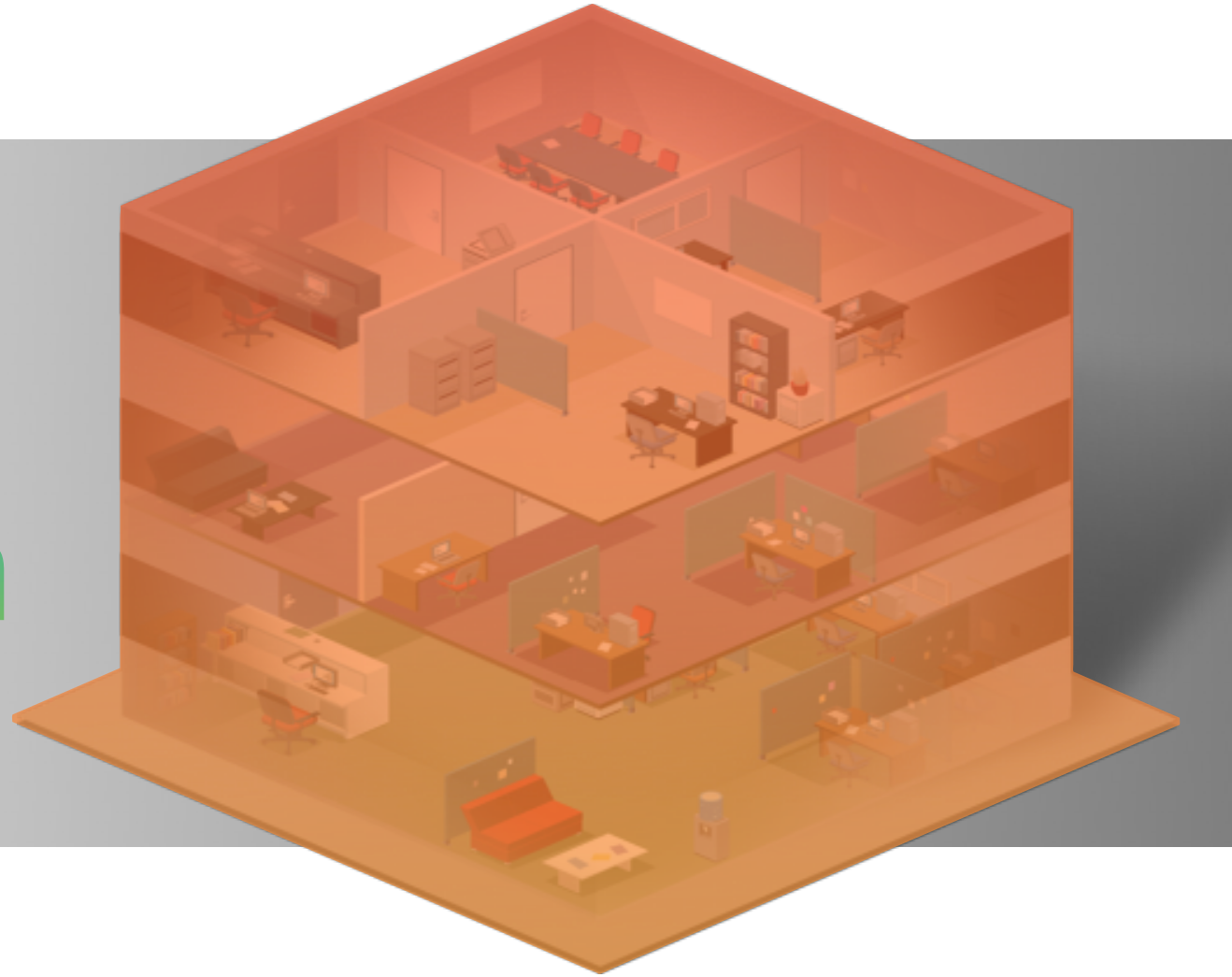
Agenda

- ASA-CX Gennemgang
- ASA-CX Demo
- ASA 9.0 (SGA / Cisco Cloud Web Sec)
- ASA 9.0 med CCWS Demo
- Pause
- Unified Access Gennemgang
- Unified Access Demo – BYOD/SGA/ PRIME
- Cisco Security ELA (Enterprise License Agreement)
- Diverse Nyheder

Agenda

- ASA-CX Gennemgang
- ASA-CX Demo
- ASA 9.0 (SGA / Cisco Cloud Web Sec)
- ASA 9.0 med CCWS Demo
- Pause
- Unified Access Gennemgang
- Unified Access Demo – BYOD/SGA/ PRIME
- Cisco Security ELA (Enterprise License Agreement)
- Diverse Nyheder

"100% of IT Is Struggling to Keep Up With Trends."



—Gartner

Driving the Transformation

Mobile Devices

IT Resources

- Billions of New Networked Mobile Devices in Next 3 Years

Mobility

Video

- 60% of All Cisco Network Traffic Today Is Video

Workspace Experience

Healthcare Data

- Blurring the Borders : Consumer ↔ Workforce; Employee ↔ Partner

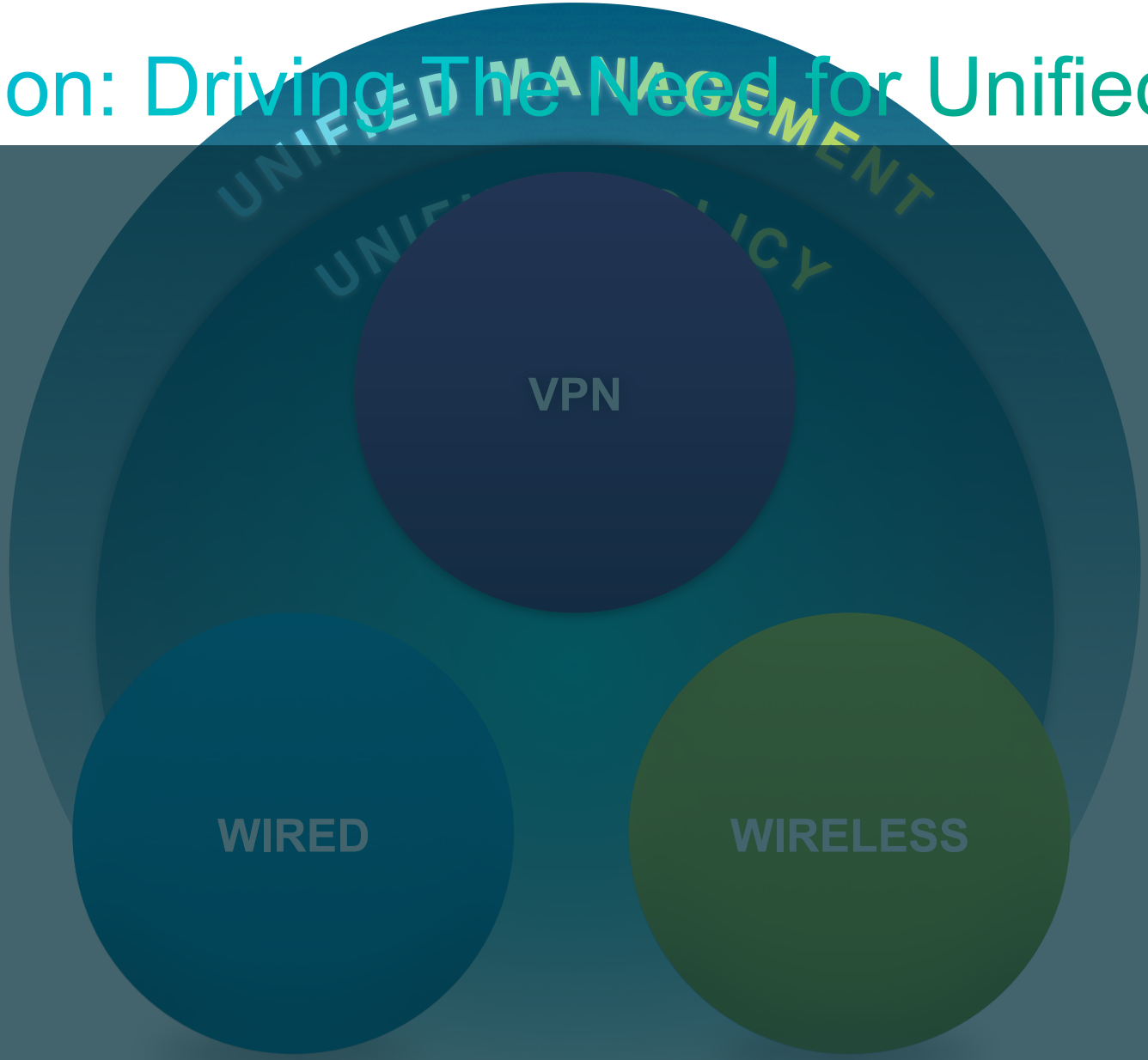
Industry Change

The New “Wired and Wireless” Magic Quadrant

The “platform chaos” has arrived

MS own the desktop - Android king of Smartphones - Apple rules the tablet market

Transformation: Driving The Need for Unified Access



Any device – Any user – Any Service

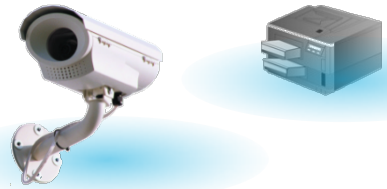
BYCD
Bring your Corporate Device

Smart devices which are managed and controlled by IT

BYOD
Bring Your Own Device

Smart Devices which are unmanaged by IT

Any Device / Service



WebEx, Collaboration service etc….

Units with limited intelligence, services like WebEx, and video

Users

Different types of users: Guests, Company users, Consultans

Cisco TrustSec™ platform

Overview

One Policy

Deliver a single source of policy across wired, wireless, and remote access

- **Cisco Identity Services Engine** Release 1.1.1 (aka Release 1.1 MR)

One Management

Provide a converged platform for integrated lifecycle management and application visibility

- **Cisco Prime Infrastructure** version 1.2

One Network

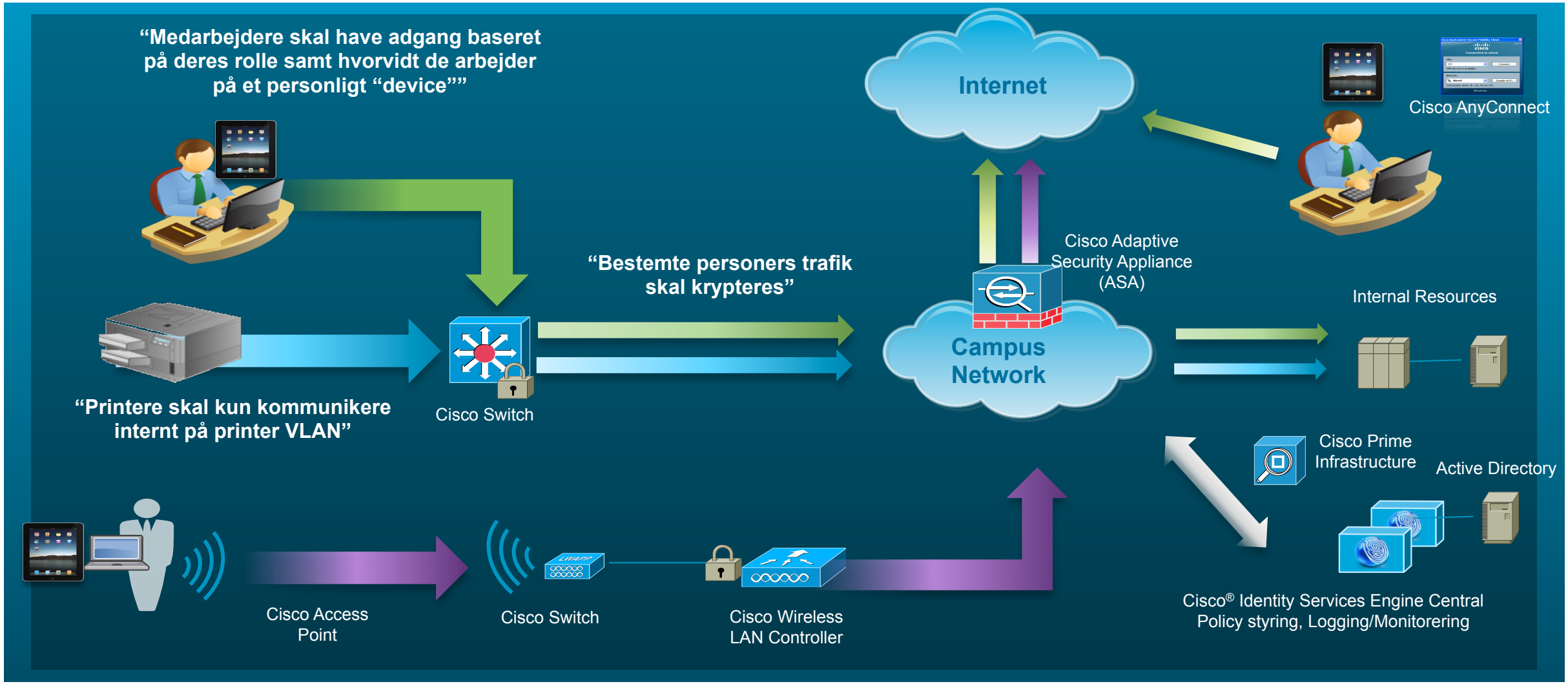
Smarter, faster access layer to handle the onslaught of new devices and applications

- **New line of 2nd generation 802.11n access points (Cisco Aironet 1600 & 2600 APs)**
- **New Cisco Wireless 8500 Series Controller**
- **New Cisco Virtual Wireless Controller**
- **Cisco Wireless 7.3 Software Release**
- **Cisco IOS Release 15.0(2)SE for Catalyst 3K-X switches**
- **Additional Products**

Services for Unified Access from Cisco and Our Partners

Unified Access Demo

A Practical Example of Policies



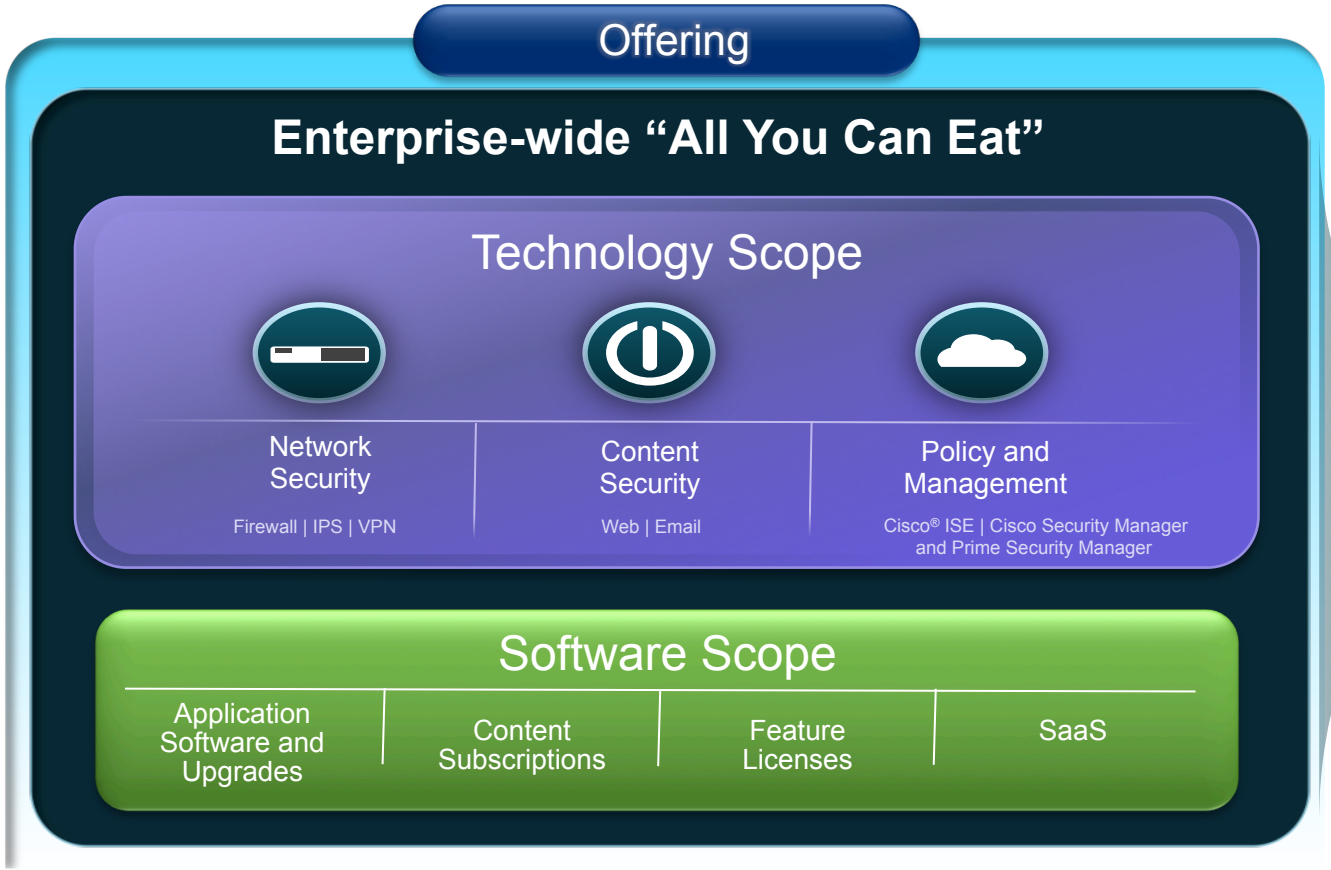
Agenda

- ASA-CX Gennemgang
- ASA-CX Demo
- ASA 9.0 (SGA / Cisco Cloud Web Sec)
- ASA 9.0 med CCWS Demo
- Pause
- Unified Access Gennemgang
- Unified Access Demo – BYOD/SGA/ PRIME
- Cisco Security ELA (Enterprise License Agreement)
- Diverse Nyheder

Cisco Security Enterprise License Agreement

Jesper Dromph, Security PSS

Cisco Security Enterprise License Agreement Overview



Customer value

- Design flexibility
- Cost savings
- Easier to buy and manage
- Vendor consolidation
- Budget predictability and needs alignment

Outside scope of Cisco® Security ELA

- Hardware
- Technical support

Agenda

- ASA-CX Gennemgang
- ASA-CX Demo
- ASA 9.0 (SGA / Cisco Cloud Web Sec)
- ASA 9.0 med CCWS Demo
- Pause
- Unified Access Gennemgang
- Unified Access Demo – BYOD/SGA/ PRIME
- Cisco Security ELA (Enterprise License Agreement)
- Diverse Nyheder

Diverse Nyheder

- ISE 1.1.1 – NSP – EAP-Chaining
- Cisco AnyConnect Secure Mobility Client for Apple iOS
- Cisco AnyConnect Secure Mobility Client for Android (Generic Support from 4.0. For other versions check release notes)
- AnyConnect 3.1
- ASA1000v
- SGT/SGAcl Support on 3560-X & 3750-X & N5K & 6500 Sup2T
- SXP Support on 2960-S & N1K & WLC 7.2 & ASA 9.0
- IPS 4510 & 4520 max 5 / 10 Gb 3,8 / 8,4 Mill Conn 72K / 100K CPS
- BYOD Smart Solution Cisco Validated Design Guide 2.2
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html
- Cisco Security Manager 4.3
  http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.3/release/notes/csmrn43.html
- ASA-CX på ASA 5500-X

Cisco Live London 2013 (28 jan – 1 feb)

- CVU ASA 9.0 onsdag 12 dec www.cisco.dk - lokale seminare eller seminar materialer

God Jul!