Adgangskontrol med Cisco Identity Services Engine (ISE)

Rasmus Kamper Mathiasen
Systems Engineer

Cisco Danmark

rkamperm@cisco.com

Today's Environment

USER ENTITLEMENT

- Device freedom
- Work from anywhere
- Application of choice

IT BURDEN

- Securing any device
- Supporting any location
- Ensuring application quality

The Transformation
New Borderless Enterprise

Anyone

Employee,
Partner,
Customer
Communities

Anything

Person / Device,
Device / Device
Information

Work, Home,
On the Go…

Always Works,
Instant Access,
Instant Response

Anywhere

Anytime

Policy Evolving with Borderless Network

Anyone

The RIGHT Person

Any Device

An approved Device

Anywhere

In The Right Way

Anytime

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?

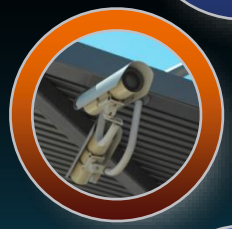
Authentication and Authorization

802.1x/Infrastructure

Identity Information	Other Conditions	Authorization (Controlling Access)

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.

Group:
Full-Time Employee

Group:
Contractor

Group:
Guest

+

Time and Date

Posture

Location

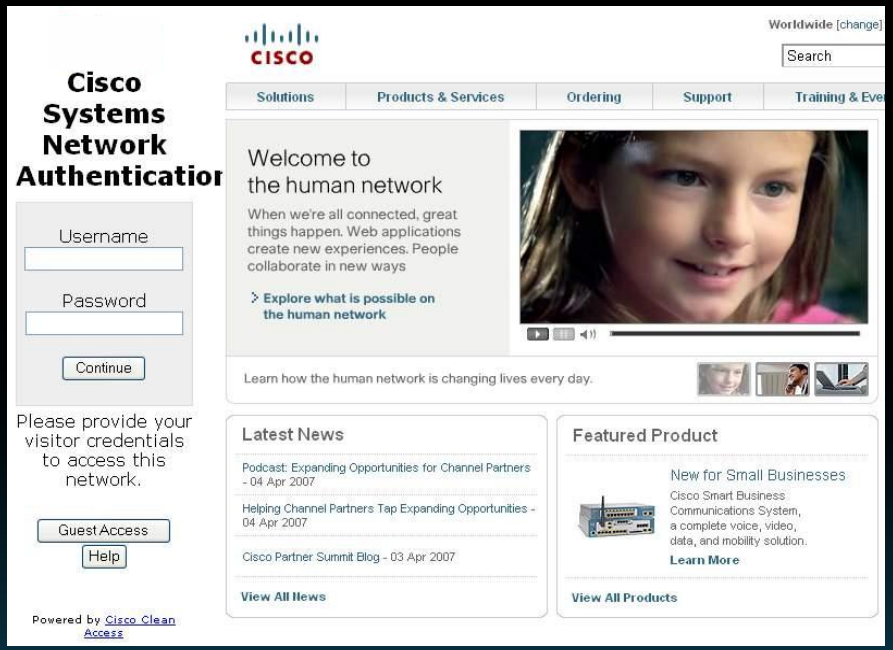
Device Type

Access Type

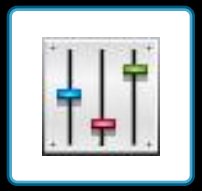
- Broad Access
- Limited Access
- Guest/Internet
- Quarantine
- Deny Access

Access Compliance Reporting

Access Policy: Guest Access



Provision: Guest accounts via sponsor portal



Manage: Sponsor privileges, guest accounts and policies, guest portal

Notify: Guests of account details by print, email, or SMS

Report: On all aspects of guest accounts

Access Policy: Non-Authenticating Devices

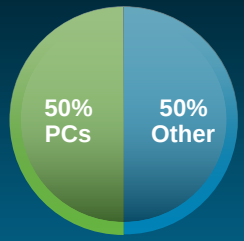
Device Identification

- Determine device type
- Centralized device discovery and inventory
- Uses network device tables and analyzes endpoint traffic

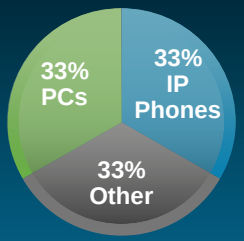
Control and Audit

- Authorize based on device role
- Monitor and audit to prevent spoofing

Many endpoint devices are undocumented and cannot authenticate to the network



Enterprises withoutVoIP Wired Endpoints Distribution



Enterprises withVoIP Wired Endpoints Distribution

Consumerization

"Consumerization is a stable neologism that describes the trend for new information technology to emerge first in the consumer market and then spread into business organizations, resulting in the convergence of the IT and consumer elctronics industries.

http://en.wikipedia.org/wiki/Consumerization

Cisco TrustSec Portfolio

Appliance Policy Components

NAC Manager
Admin, Reporting, and Policy Store

NAC Server
Posture, Services, and Enforcement

OR

ACS
Identity & 802.1x Access Policy System

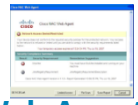
+

NAC Profiler
Profiles Non-Authenticating Devices

NAC Guest
Full-Featured Guest Provisioning Server

Endpoint Components (Optional)

NAC Agent



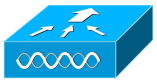
Web Agent

No-Cost Persistent & Temporal Clients for Authentication, Posture, & Remediation

OR

802.1x Supplicant
AnyConnect or OS-Embedded Supplicant

ISE Identity Services Engine

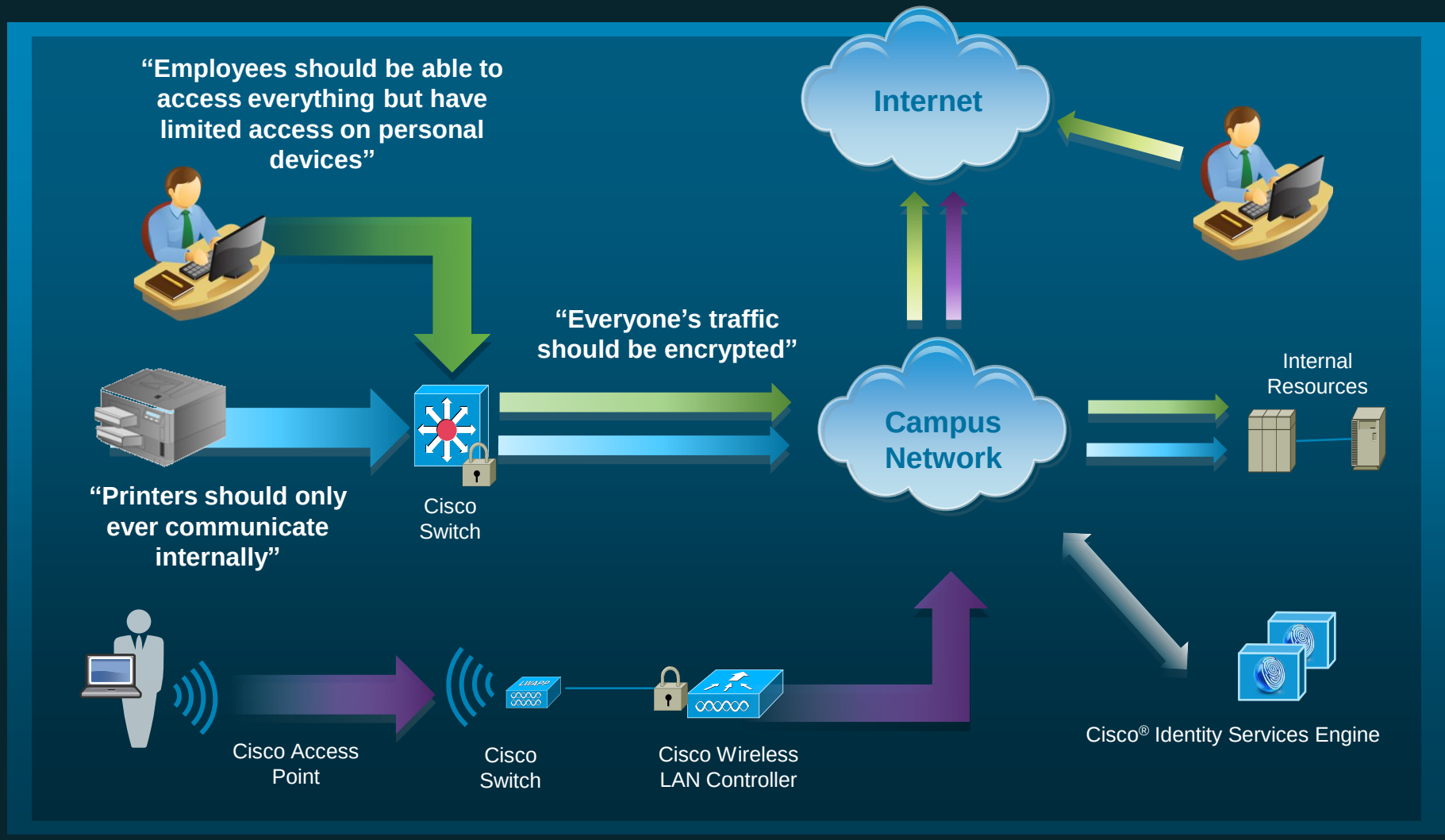




Cisco 2900/3560/3700/4500/6500 and Nexus 7000 switches, Adaptive Security Appliance (ASA), Wireless and Routing Infrastructure

Centralized Policy Engine for All Access to the Network

Introducing Identity Services Engine (ISE) and TrustSec 2.0

A Practical Example of Policies



Thank you.