



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



Borderless
Experience

Always Works,
Instant Access,
Instant Response



Work, Home,
On the Go...

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

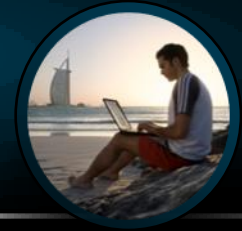
- How can I restrict access to my network?
- Can I manage the risk of using personal PCs, tablets, smart-devices?
- Access rights on-prem, at home, on the road?
- Devices are healthy?

Guest Access

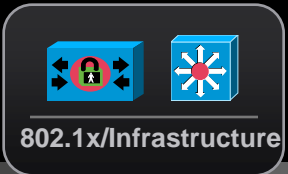
- Can I allow guests Internet-only access?
- How do I manage guest access?
- Can this work in wireless and wired?
- How do I monitor guest activities?

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



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



Worldwide [change] Search

Solutions Products & Services Ordering Support Training & Events

Cisco Systems Network Authentication

Username

Password

Continue

Please provide your visitor credentials to access this network.

Guest Access Help

Powered by [Cisco Clean Access](#)

Welcome to the human network

When we're all connected, great things happen. Web applications create new experiences. People collaborate in new ways

> Explore what is possible on the human network

Learn how the human network is changing lives every day.

Latest News

Podcast: Expanding Opportunities for Channel Partners - 04 Apr 2007

Helping Channel Partners Tap Expanding Opportunities - 04 Apr 2007

Cisco Partner Summit Blog - 03 Apr 2007

[View All News](#)

Featured Product

New for Small Businesses

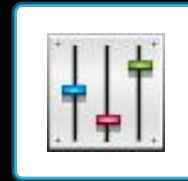
Cisco Smart Business Communications System, a complete voice, video, data, and mobility solution.

[Learn More](#)

[View All Products](#)



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



Many endpoint devices are undocumented and cannot authenticate to the network

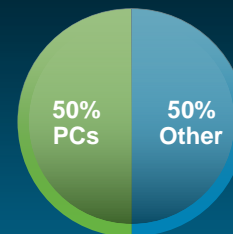
Device Identification

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

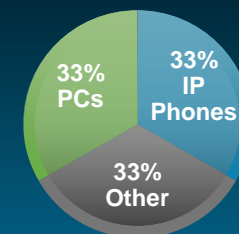
Control and Audit

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

Name	Category	Description	Active Rule(s)	LDAP	Max CF
IP Phone	Special Purpose	Based on DHCP Vendor & CDP Platform	No	Yes	40.5%
Linksys Video Cam 2	Special Purpose	Based on DHCP host name only	No	No	45%
SCADA Systems	Special Purpose	Devices with MODBUS port open	Yes	No	49.375%
Rogue Detection IP	Exceptions	Adv XML Rule: Multi MAC Vendors	No	No	50%
Hewlett-Packard JetDirect Printer	Special Purpose	Based on DHCP Vendor and/or OpenPort	Yes	No	51%
Linksys Video Cam	Uncategorized	Security Cameras	No	Yes	51%
Multi Server	GP Endpoints	Based on server banners	Yes	No	85.56%
Apple Users	GP Endpoints	Based on User Agent	No	No	92%
Windows Users	GP Endpoints	Based on User Agent and/or DHCP Vendor	No	No	96.925%



Enterprises **without** VoIP Wired Endpoints Distribution



Enterprises **with** VoIP 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 electronics 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
No-Cost Persistent & Temporal Clients for
Authentication, Posture, & Remediation



Web Agent

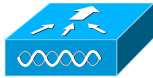
OR



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

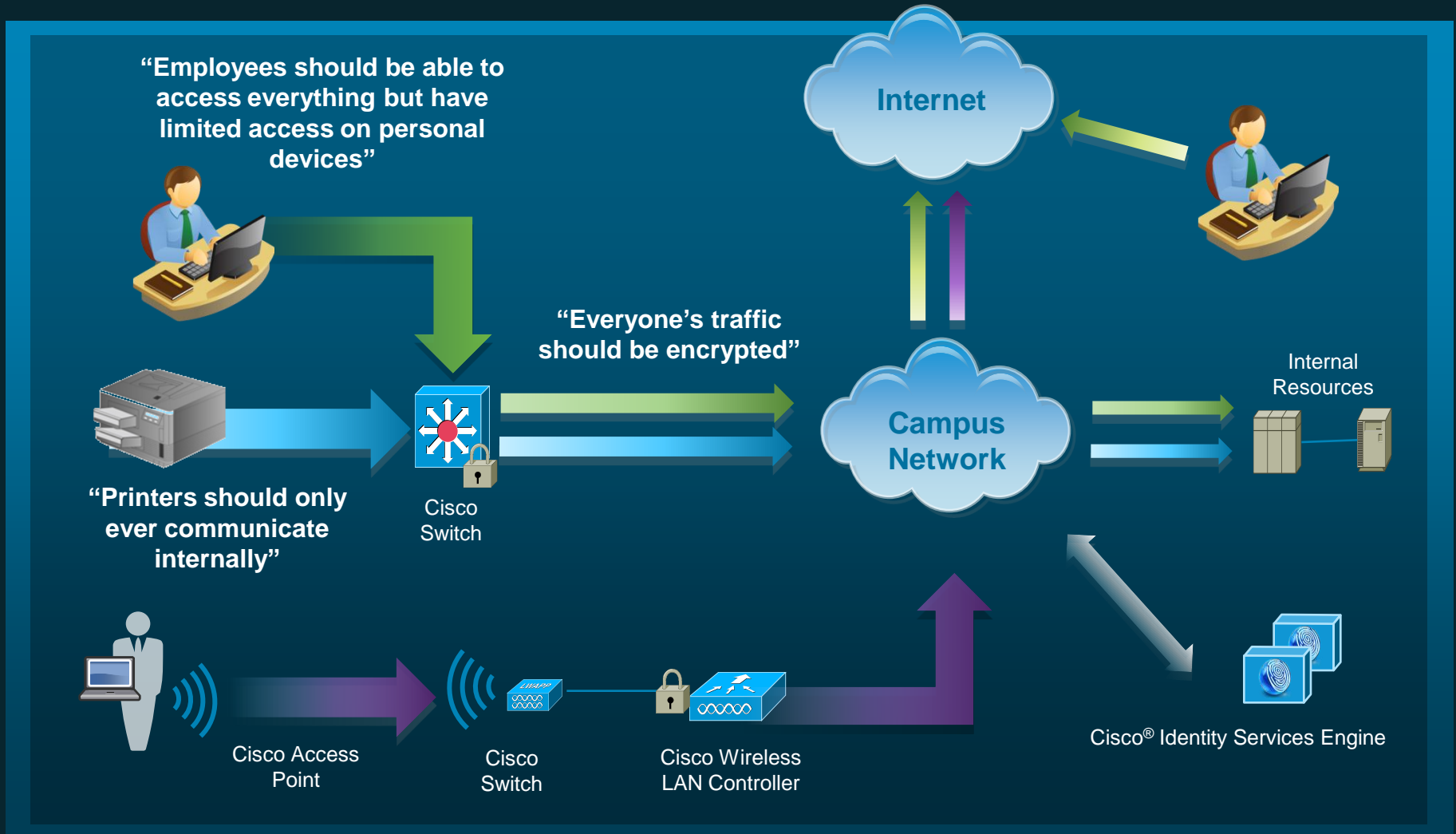
Centralized Policy Engine

for All Access to the Network

Introducing Identity Services Engine (ISE) and TrustSec 2.0



A Practical Example of Policies



Thank you.

