

IS YOUR NETWORK READY FOR THE MOBILE EXPERIENCE?

CISCO ISE - IDENTITY SERVICES ENGINE

**CLAUDIU ONISORU
SENIOR NETWORK SPECIALIST
22 MAR 2012**

AGENDA

- **Frontal Communication: Who we are?**
 - **Key points**
 - **Competencies Areas**
 - **Cisco Partnership**
 - **Awards**
- **ISE – Identity Services Engine. A short introduction**
- **Case Study**

KEY POINTS

- Established in 1994
- Telecom, Enterprise, Public Sector
- No.1 as IT&C SOLUTION and SYSTEM INTEGRATOR in the Romanian market (*CISCO – approx. 25 Mio. USD*)
- CUSTOMER Oriented Company
- Cisco GOLD Partner with local support
- Cisco Global Award Winner
- EMC Velocity Partner
- VMware Premier (*Infrastructure Virtualization, Business Continuity, Desktop Virtualization*)
- Authorized Cisco Training Center



COMPETENCIES AREA

DATA CENTER

Storage
Switching
Applications
Security
Network Management

NETWORK SYSTEMS

Routing
LAN Switching
Network Management

MOBILITY SOLUTIONS

Wireless LAN
Remote Access
Business Class Teleworker Solutions
Mobile Solutions for
Unified Communications

SECURITY

Firewall
Attack and Intrusion Prevention
Spam and Virus Protection
Virtual Private Networks
Network Admission Control
Security Management
Physical Security
Web and Email security
Video Surveillance

UNIFIED COMMUNICATION

IP Telephony
Applications
Contact Center
Voice Management
Vice traffic management
Call accounting

CISCO PARTNERSHIP

Certification

Cisco Gold Partner

Specialization:

Advanced Collaboration Architecture
(1st in Romania and Region)

Advanced Borderless Architecture

Advanced Routing & Switching

Advanced Security

Advanced Unified Communications

Advanced Wireless LAN

Advanced Data Center Network
Infrastructure

Advanced Data Center Storage Networking

Advanced Data Center Architecture (in
progress)

Other Authorizations:

Cisco Learning Partner Associate

Customer Satisfaction Excellence

ATP - Video Surveillance

ATP Unified Computing System
(1st in Romania and Region)

ATP Unified Contact Center (in progress)

ATP Telepresence Express

ATP Telepresence Advanced (in progress)

FRONTAL COMMUNICATION AWARDS

- Cisco Advanced Services Partner of the Year - 2011
- Cisco Service Provider Partner of the Year - 2011
- Architectural Excellence Partner of the Year - the first global award won by a Romanian company 2010
- Collaboration Partner of the Year 2010
- Customer Satisfaction Excellence 2007, 2008, 2009, 2010
- Public Sector Partner of the Year 2010
- Services Partner of the Year 2010
- Technology Excellence Borderless Network 2010
- No.1 in Romania and no. 3 in Central and Eastern Europe Training Partner 2010

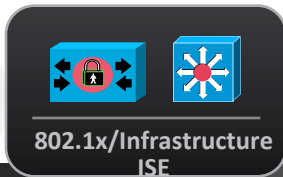
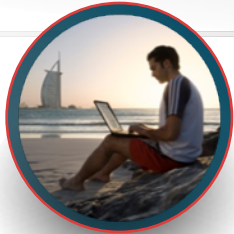


ISE – IDENTITY SERVICES ENGINE

A SHORT INTRODUCTION



ISE - AUTHENTICATION AND AUTHORIZATION



802.1x/Infrastructure
ISE

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

INTRODUCING IDENTITY SERVICES ENGINE

Identity & Access Control



Access Control Solution

Identity & Access Control +
Posture



NAC Manager



NAC Server

Device Profiling & Provisioning +
Identity Monitoring



NAC Profiler



NAC Collector

Standalone appliance or
licensed as a module on NAC
Server

Guest Lifecycle Management



NAC Guest Server



ISE



NAC Agent

FLEXIBLE AND POLICY BASED SECURITY



**Cisco
ISE**

I want to allow only authorized users access to my network

I want to allow guests into the network

I need to allow/deny iPads in my network

I need to ensure my endpoints don't become a threat vector

I need a scalable way of authorizing users or devices in the network

How can I set my firewall policies based on identity instead of IP addresses?



Authentication and Authorization



Guest Lifecycle Management



Profiling Services



Posture Services



Security Group Access Management



Identity-based Firewall

CISCO ISE AUTHENTICATION METHODS

- **IEEE802.1X User / Device Authentication**
 - Standards-based port-based authentication provides strong Layer 2 authentication methods for user and device.
- **MAC Authentication Bypass**
 - Non-802.1X device can be authenticated using MAB (MAC address-based authentication).
- **WEB Authentication**
 - Guest / visitor can use web-based authentication for temporal network access.



CISCO ISE ARCHITECTURE

Authorization

ACL

VLAN

Security Group
Tagging

Authentication

802.1X

WebAuth

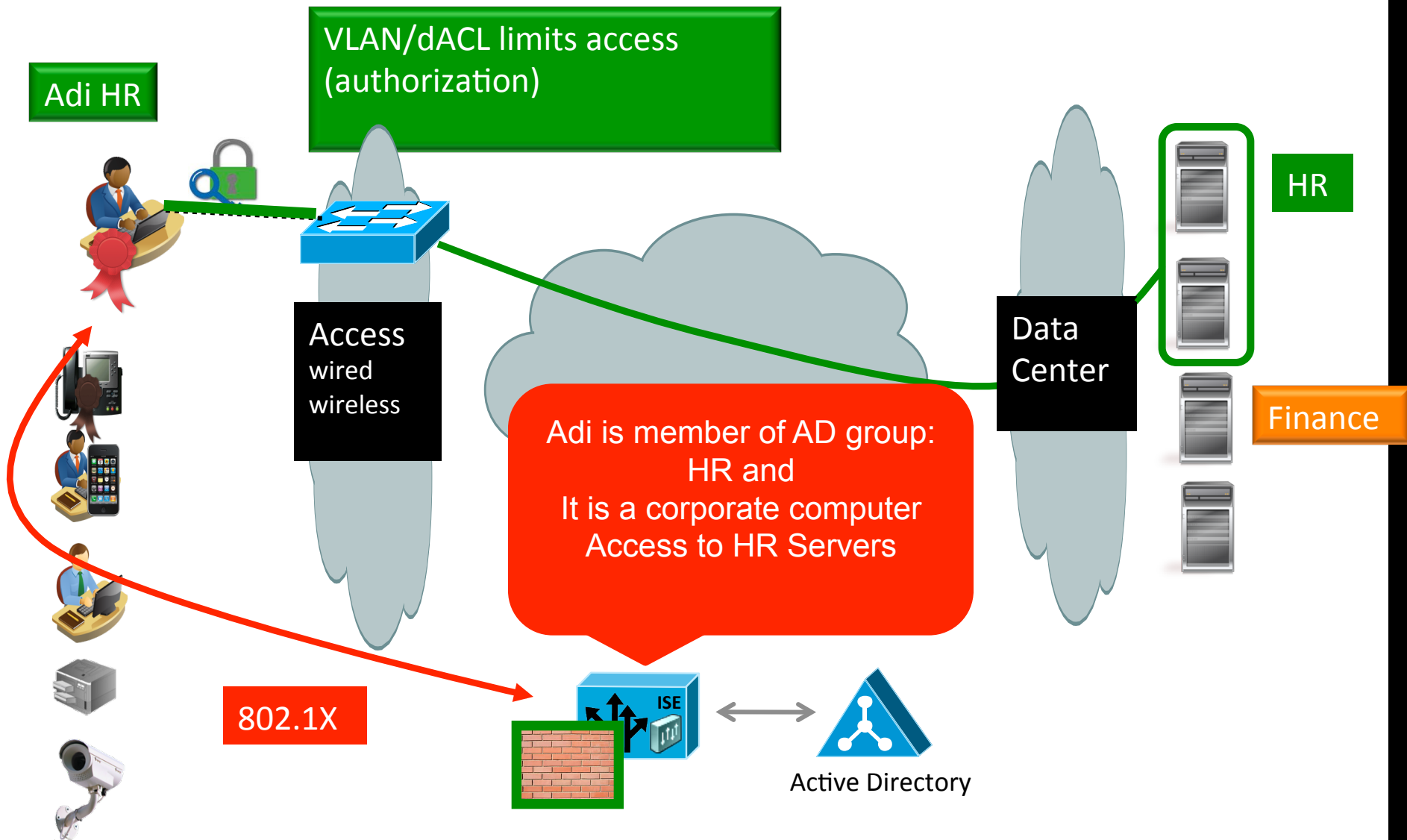
MAB



802.1X AUTHENTICATION

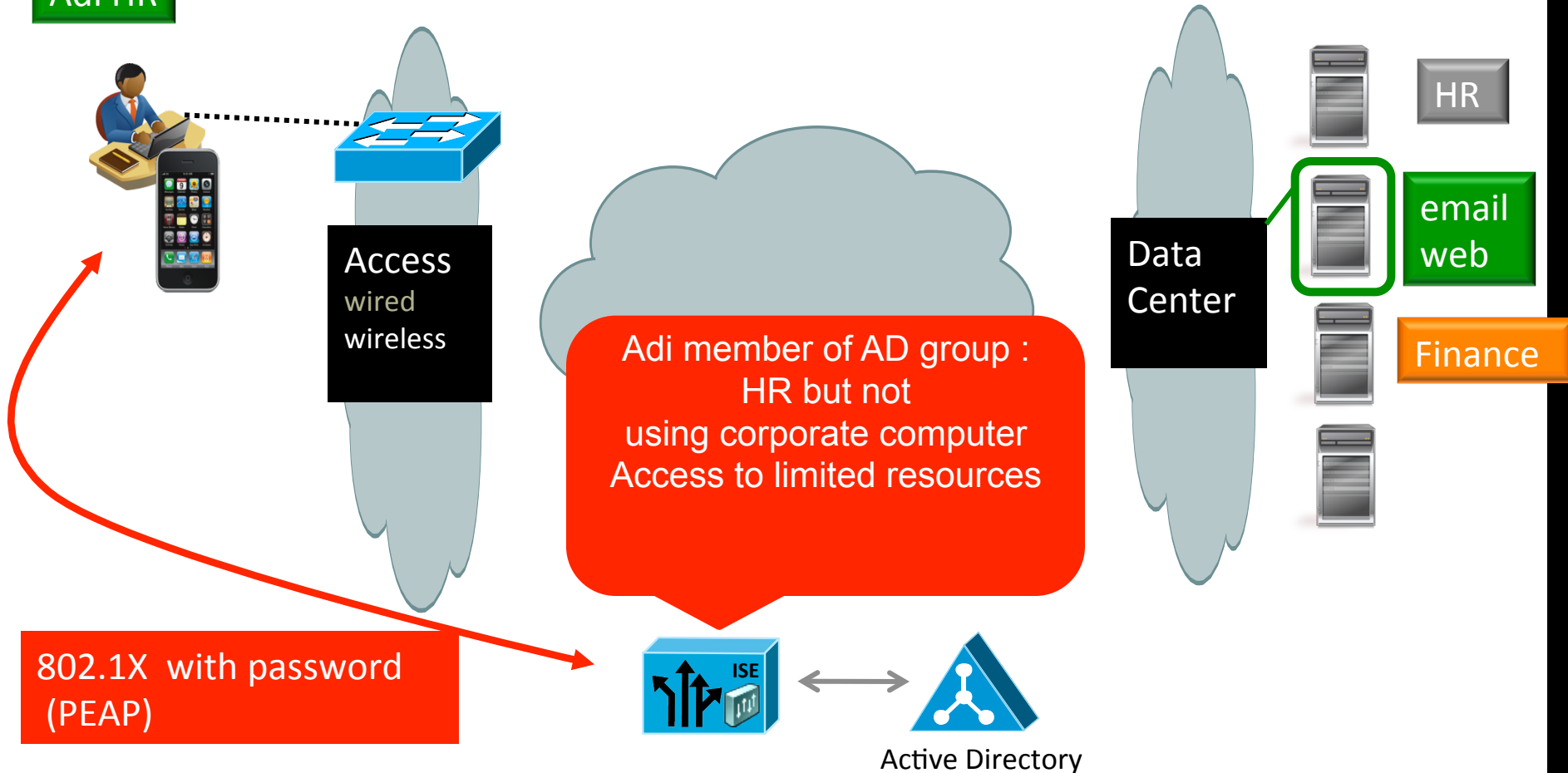


EMPLOYEES WITH CORPORATE COMPUTERS



EMPLOYEE WITH BYOD (802.1X)

Adi HR



MANAGING NON-USER DEVICES



HOW TO HANDLE NON-USER DEVICES



Monitor Mode reveals all kinds of endpoints... what to do with those now?

- Use MAC Address based authentication (MAB)
- MAB requires MAC address database to authenticate
- How to populate database?
 - ✓ Import existing asset inventory data
 - ✓ Find all unique MAC addresses in the report, and populate static entries in backend database
 - ✓ Use Profiling technology to automatically populate MAC addresses, then profile device type based on its context

OTHER DEVICES (NON-802.1X CAPABLE) MAC AUTHENTICATION BYPASS (MAB)

VLAN/downloaded ACL
controls access

Access
wired
wireless

Data
Center

HR

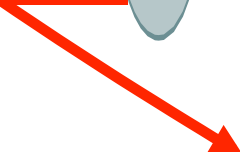
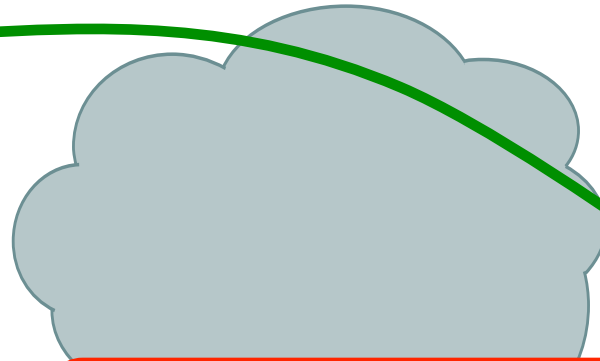
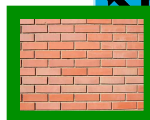
Finance

Surveillance

No 802.1X
MAC adress=.....

Check MAC adress database
(ISE internal or external)

MAC
Database

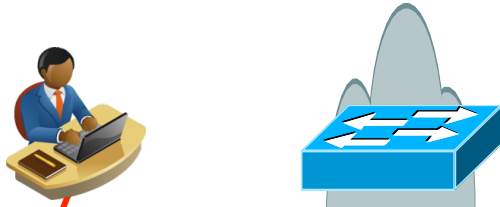


MANAGING GUEST ACCESS



GUEST ACCESS – MORE THAN JUST INTERNET ACCESS

Adi HR : Sponsors Cristi



Account Management > Guest User Accounts List > Create Guest Account

Create Guest Account

* First Name: Cristian
* Last Name: Ionescu
* Email Address: cristian.ionescu@frontalcoi
Phone Number:
* Company: Frontal Communication
* Reason for Access: guest access
Additional Comments:
* Group Role: Guest
* Time Profile: 8HoursFromCreation
* Timezone: Europe/Bucharest

* = Required fields

Submit Cancel

Adi member in AD group
HR:
may sponsor "HR-
consultants" and "Guests"



Active Directory

Data
Center



HR



email



Finance



GUEST ACCESS – MORE THAN JUST INTERNET ACCESS

Adi HR : Sponsors Cristian



Access

Data Center



HR



email



Finance



Joe member in AD group
HR:
may sponsor "HR-consultants" and "Guests"



Active Directory

Account Management > [Guest User Accounts List](#) > Create Guest Account



Successfully Created Guest Account cionescu

Username: cionescu
Password: 5Q
First Name: Cristian
Last Name: Ionescu
Email Address: cristian.ionescu@frontalcommunication.ro
Phone Number:
Company: Frontal Communication
Status: AWAITING INITIAL LOGIN
Suspended: false
Reason for Access: guest access
Additional Comments:
Group Role: Guest
Time Profile: 8HoursFromCreation

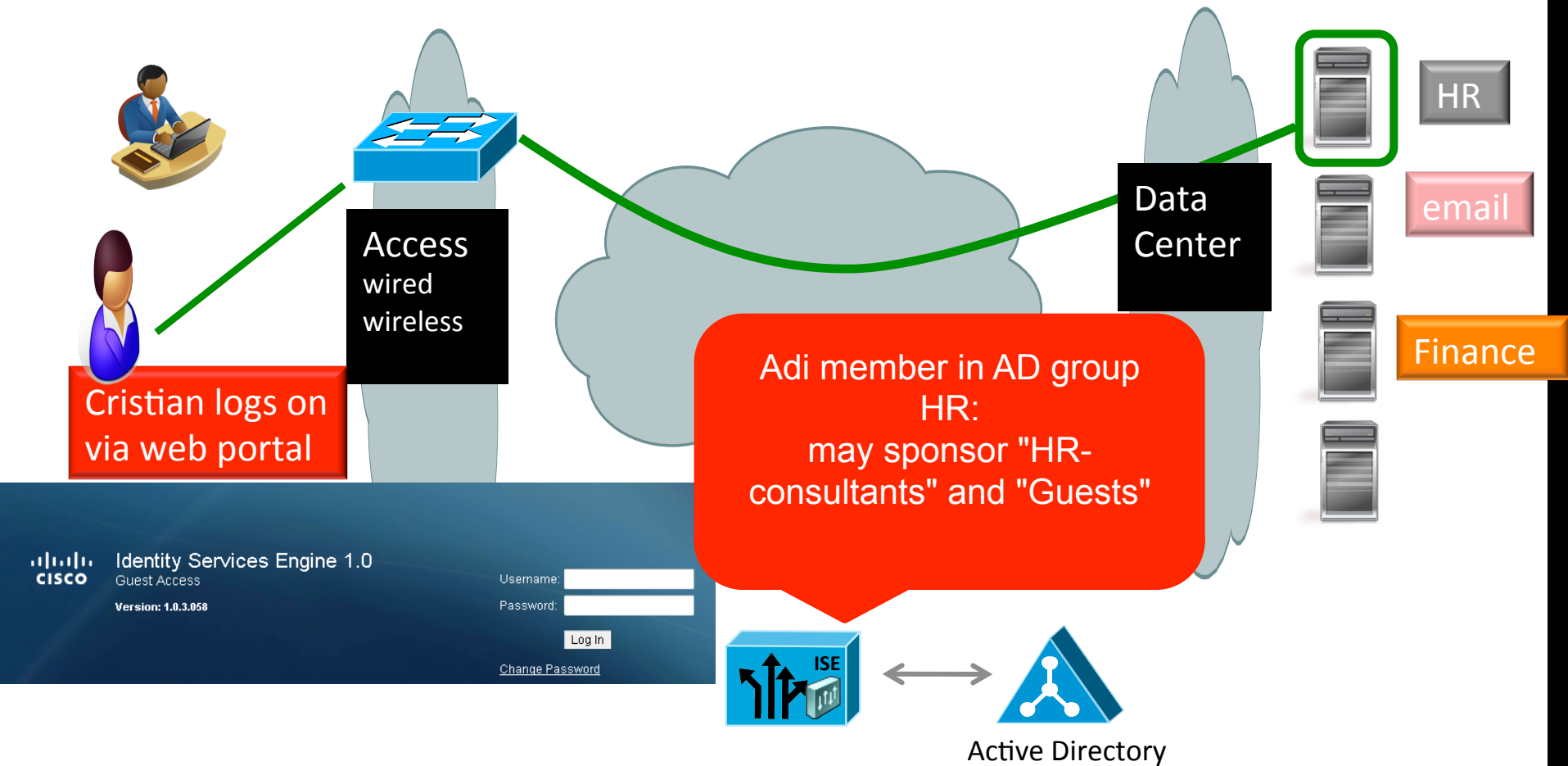
Timezone: Europe/Bucharest

Account Start Date: 2012-03-19 17:13:25 EET

Account Expiration Date: 2012-03-20 01:13:25 EET

[Email](#) [SMS](#) [Print](#) [Create Another Account](#) [View All Accounts](#)

GUEST ACCESS – MORE THAN JUST INTERNET ACCESS



ISE PROFILING



DO YOU KNOW YOUR MAC ADDRESSES?

- Number of "other devices" often exceeds number of computers
- Do you know every MAC address?
 - Process to add MAC addresses when purchasing devices
 - Process to remove MAC addresses when removing devices
- Some organization already may have processes in place and be in full control
- For others, *Profiling*, will help discover and categorize devices, effectively enabling a successful implementation of 802.1X

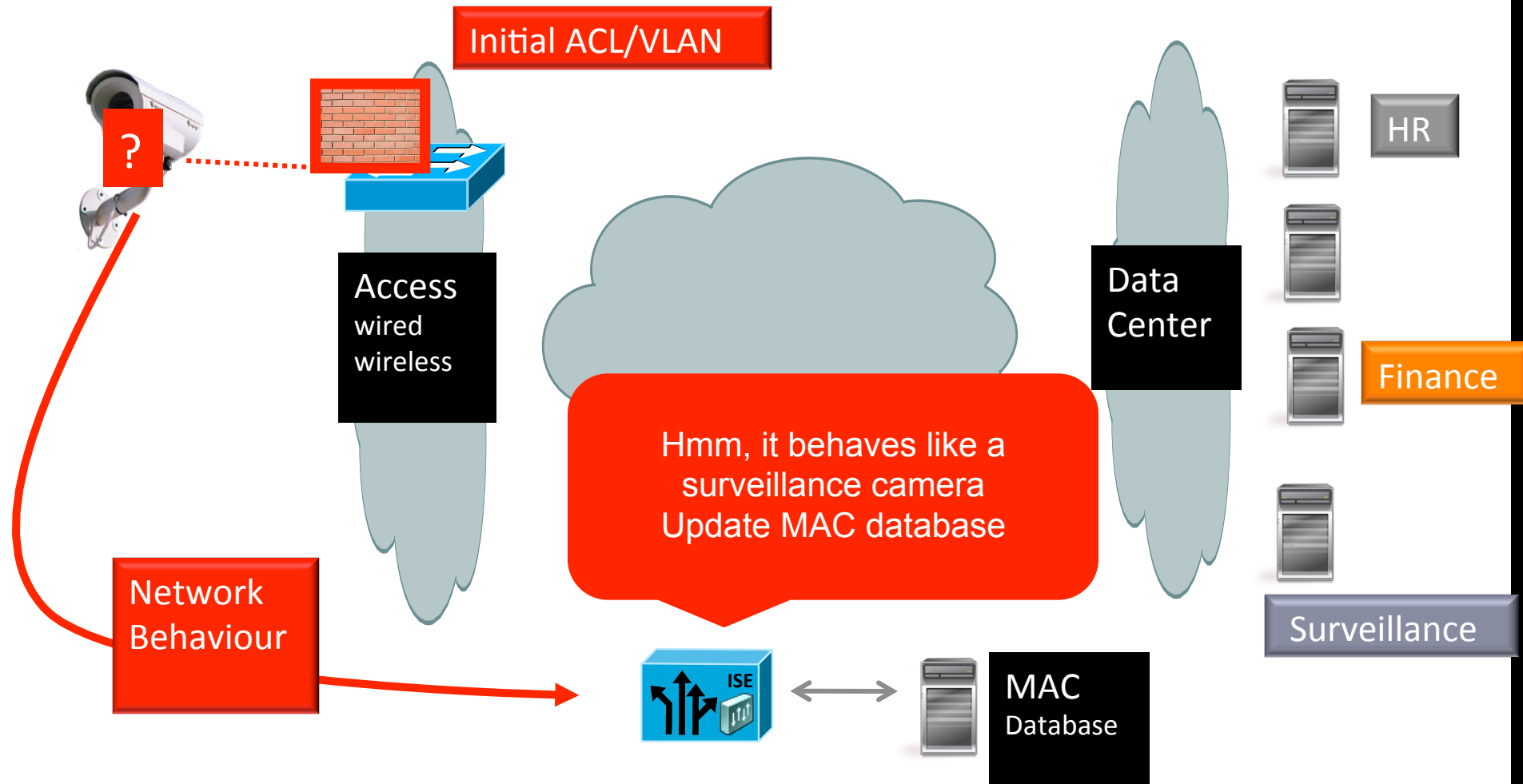


Advanced
License

ISE PROFILING



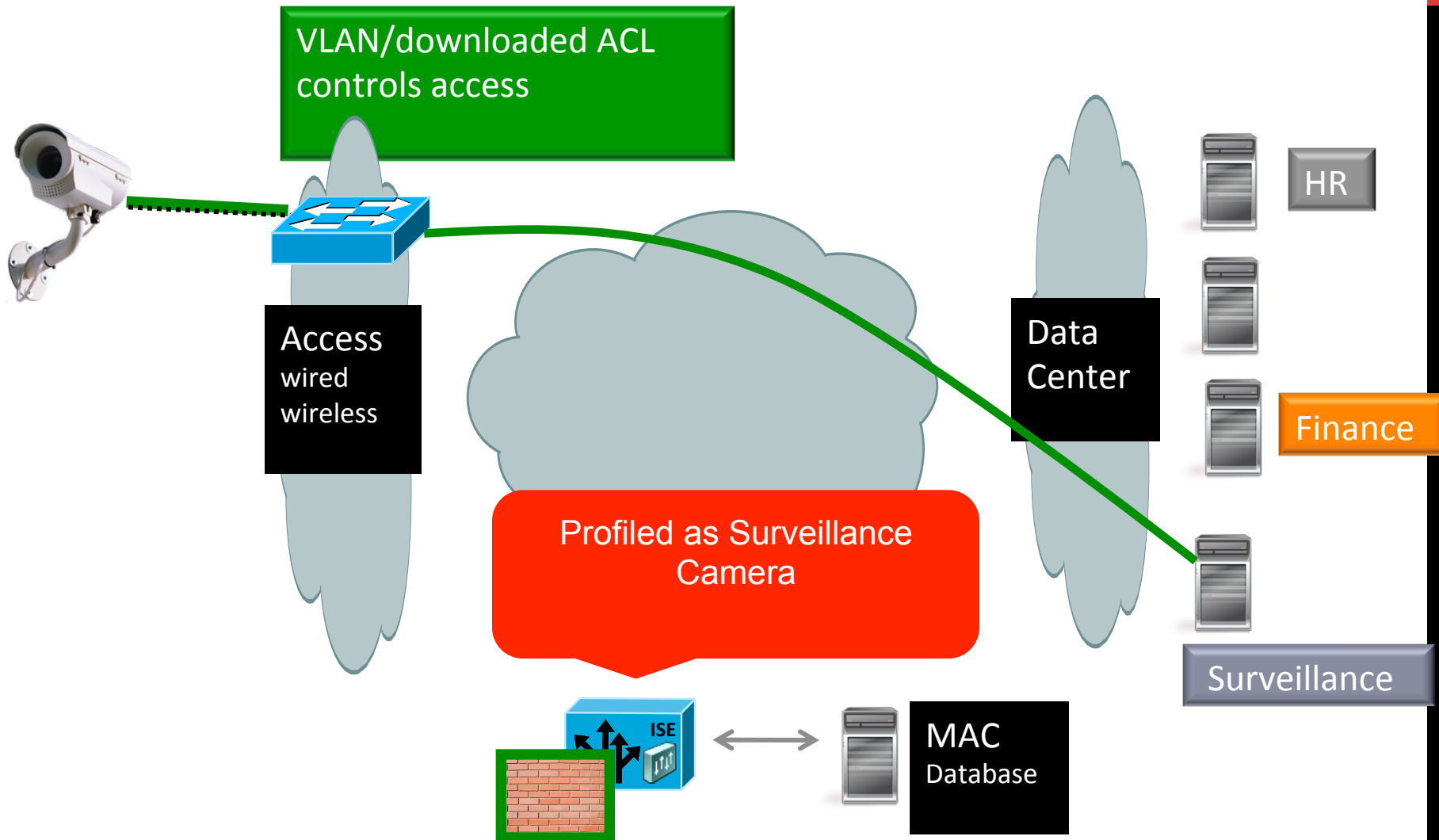
Advanced
License



ISE PROFILING



Advanced
License



CASE STUDY



REQUESTS FOR THE CASE STUDY



Enterprise Client with HQ and Branches

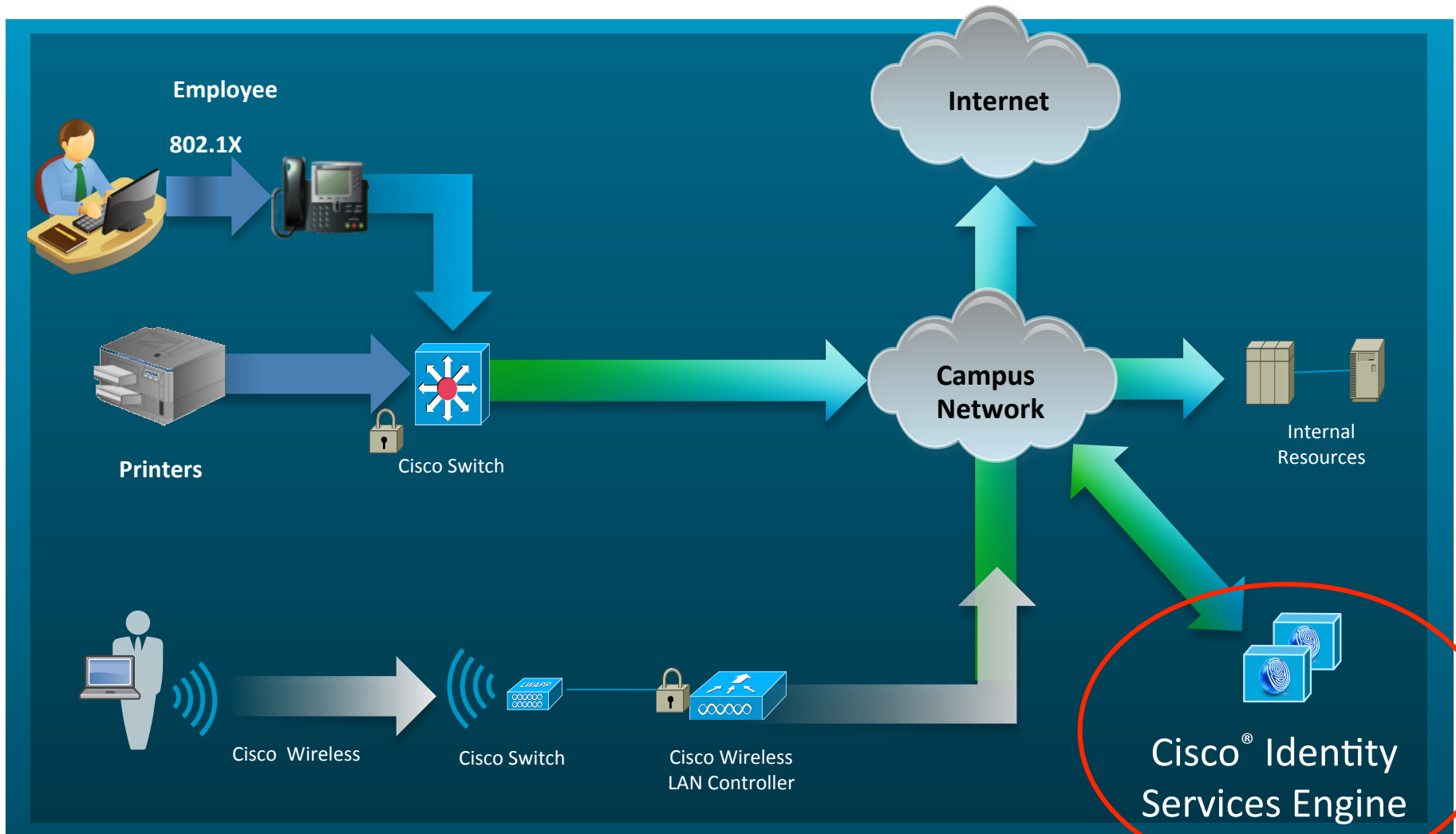
Client asked this pilot only for HQ

Requests:

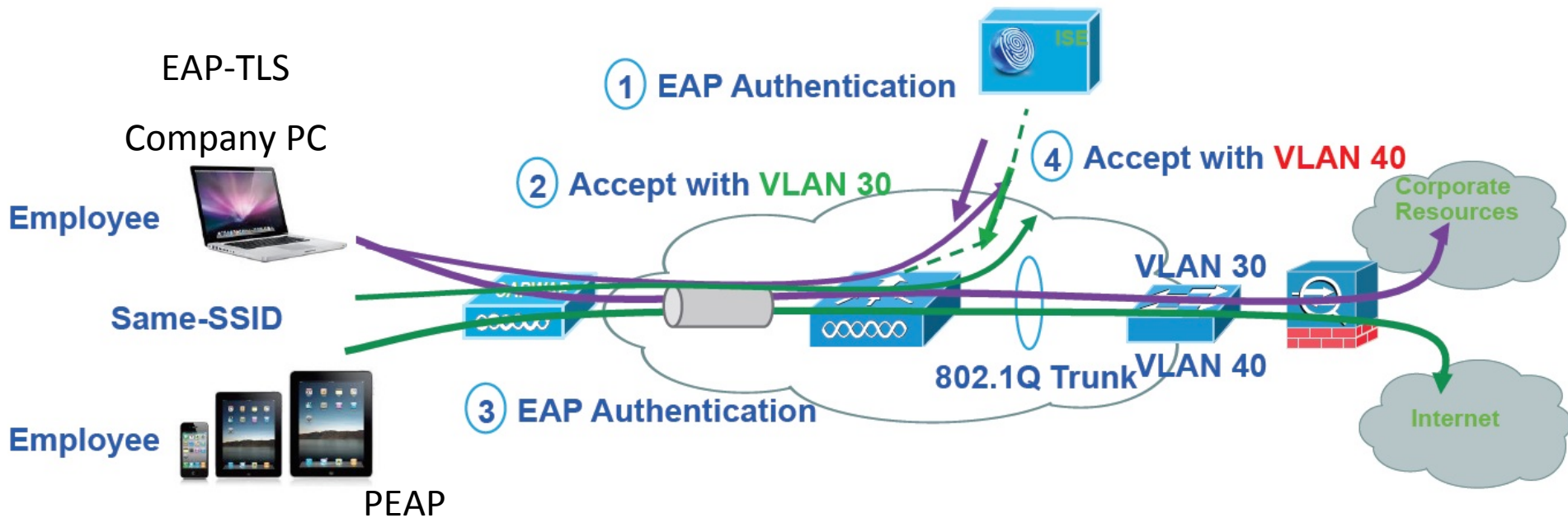
1. Secure wireless access for employees both with company devices and own devices – SSID1
2. Secure wireless access for guests (only internet access) – SSID2
3. Secure wired access only for employees
4. Other devices like network printers, IP phones, must be authenticated

GENERIC NETWORK DIAGRAM

ISE: authentication/authorization for users and devices

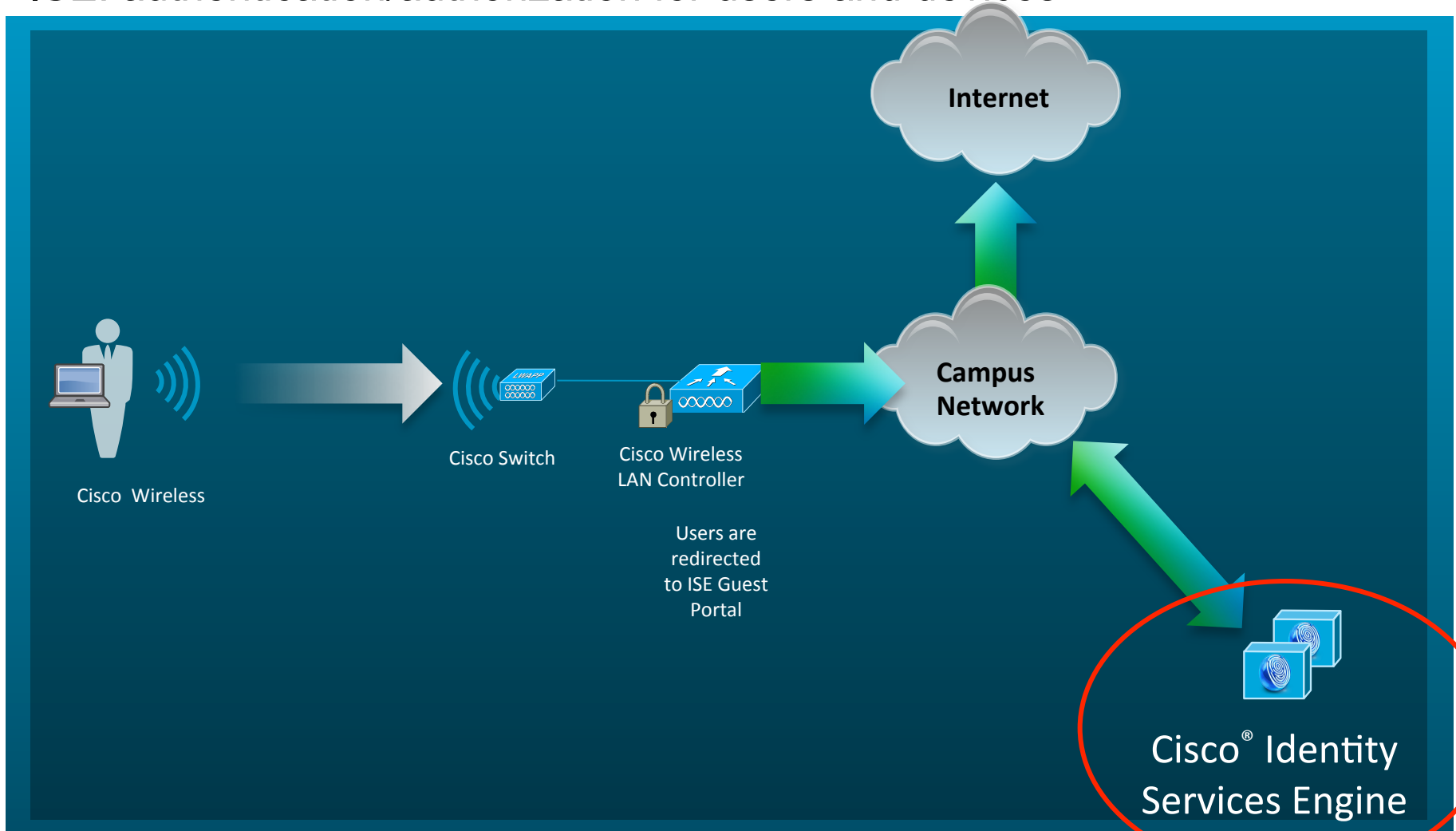


SECURE WIRELESS ACCESS FOR EMPLOYEES



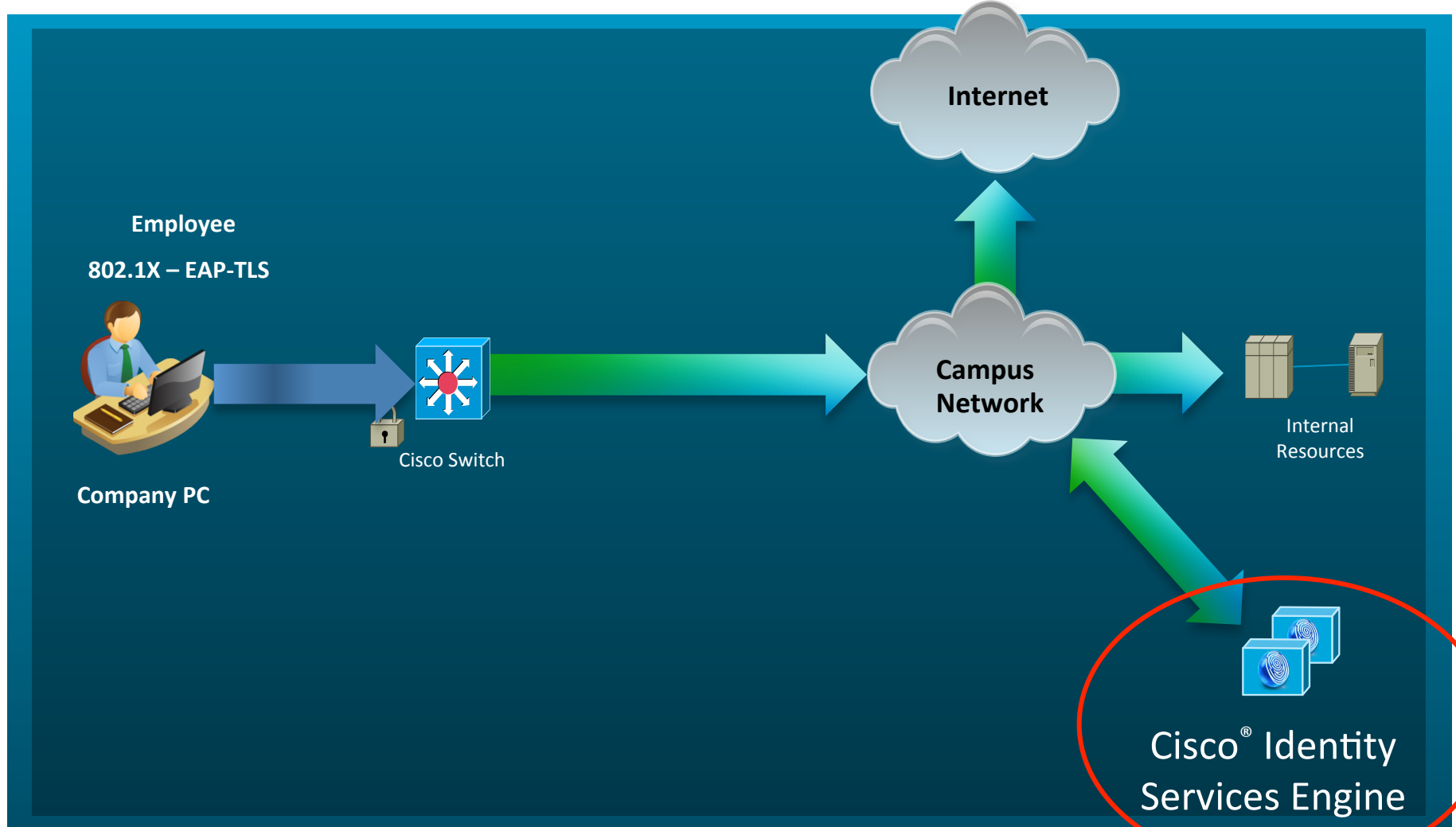
SECURE WIRELESS ACCESS FOR GUESTS

ISE: authentication/authorization for users and devices



SECURE WIRED ACCESS ONLY FOR EMPLOYEES

ISE: authentication/authorization for users and devices



OTHER DEVICES LIKE NETWORK PRINTERS, IP PHONES, MUST BE AUTHENTICATED

ISE: authentication/authorization for users and devices

