Secure Borderless Networks
Trusted Security (TrustSec)

Timothy Snow, CCIE
Security CSE (APAC)

C97-576463-00

Table of Contents

Today's Dynamic Business Environment

Customer Challenge in Building an Access Policy in a Borderless Network

Common questions organizations ask

Authorized Access

- How can I restrict access to my network?
- Can I manage the risk of using personal PCs?
- Common access rights when on-premises, at home, on the road?
- Endpoints are healthy?

GuestAccess

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

Non-Authenticating Devices

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

Why Customer's Care:
Addressing top business initiatives with TrustSec

Enables Secure Collaboration

Dynamically authenticate and assign access based on user role, device, and location

Strengthens Security

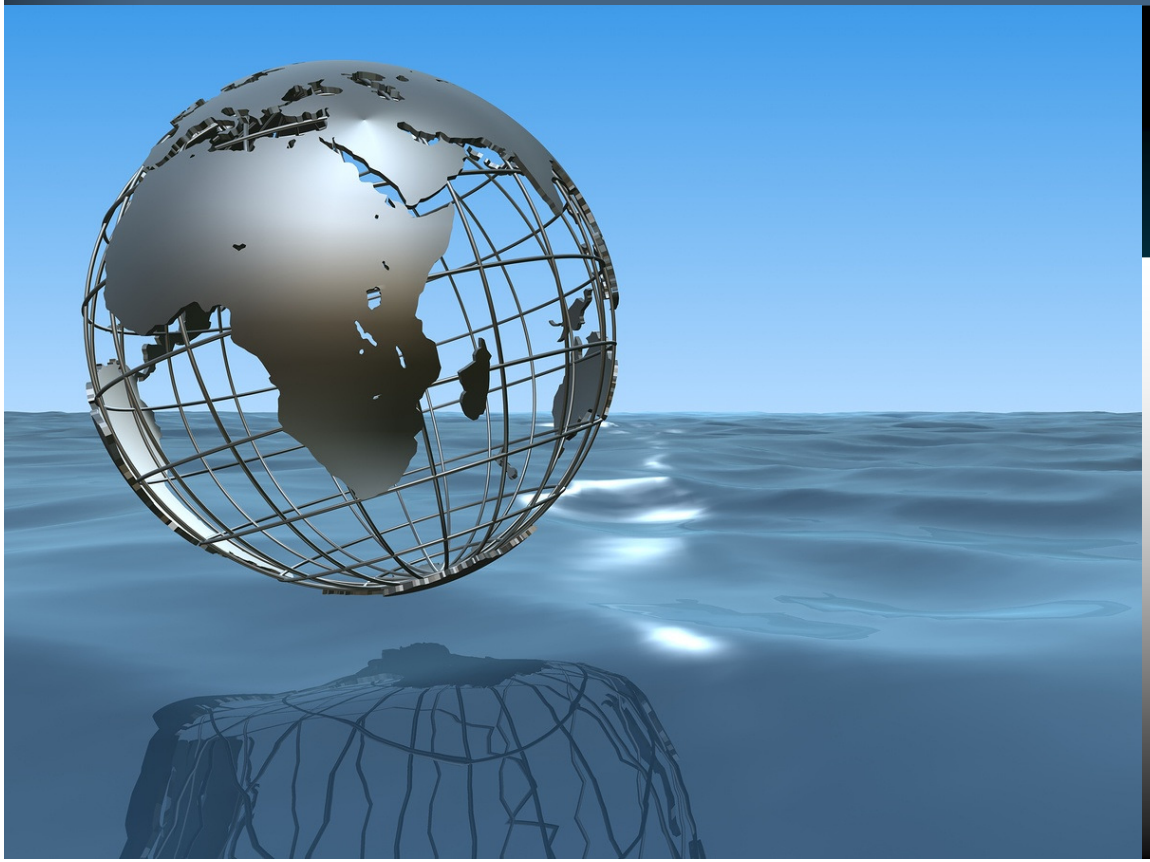
Enforce consistent security policy and ensure endpoint health

Supports Compliance

Provide real-time access visibility and audit trails for monitoring and reporting

Cisco TrustSec

Cisco TrustSec is a security solution that provides policy-based access control, identity-aware networking, and data integrity and confidentiality services



The term TrustSec has been expanded to include several methods for securing network access and control, including:

Switch infrastructure solutions:

- **Identity-Based Networking Services**
- **802.1X**
- **Security Group Tags (SGTs)**

Appliance-based solutions:

- **Network Admission Control**

Key Cisco TrustSec Functions

Policy-based Access Control

- Consistent policy for users and devices
- Distributed enforcement
- Topology- independent access control via Security Group Access Control (SGAC)

Identity-aware Networking

- Controls based on user/device identity and attributes (time, location, access methods)
- Support for Cisco Medianet and QoS for business-critical applications associated with users in specific roles

Data Integrity And Confidentiality

- Data confidentiality and integrity by securing data path in the switching environment
- IEEE 802.1AE standard based encryption with visibility into data stream to support critical security applications such as firewalls, IPS, and content inspection

Cisco TrustSec Components

Cisco TrustSec™ Technology

- Policy-based access control
- Identity-aware networking
- Data integrity and confidentiality

Topology-Independent Access Control

- Networkwide role-based access control
- Network device access control

Identity-Based Networking Services

- Flexible authentication options:
  802.1X, MAB, WebAuth, and FlexAuth
- Comprehensive post-admission control options:
  dACL, VLAN assignment, URL redirect, QoS…

Network Admission Control (NAC)

- Posture validation endpoint policy compliance

802.1X-based Network Access Control

Cisco TrustSec
Cisco 802.1X-based Authentication

- 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).

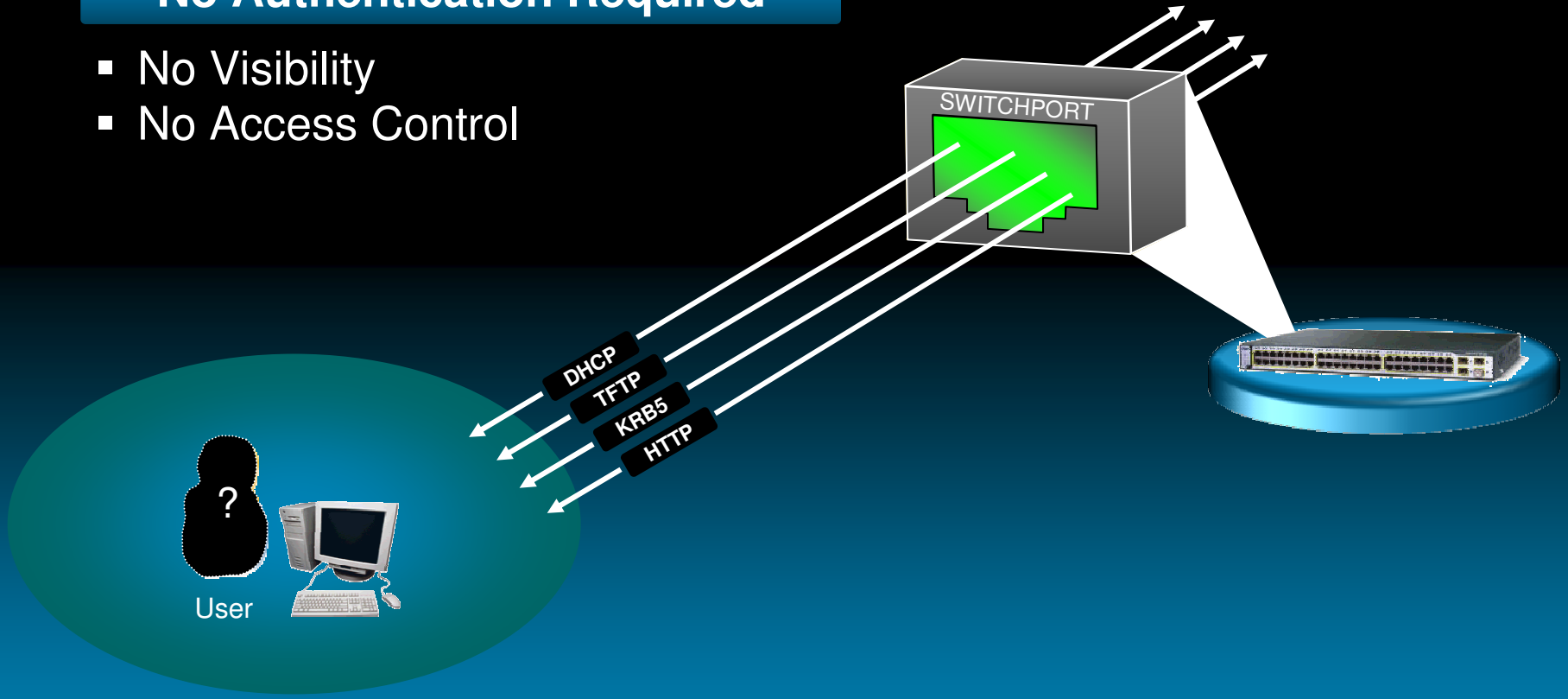
- WEB Authentication

  Guest / visitor can use web-based authentication for temporal network access.

Network Port without 802.1X

No Authentication Required

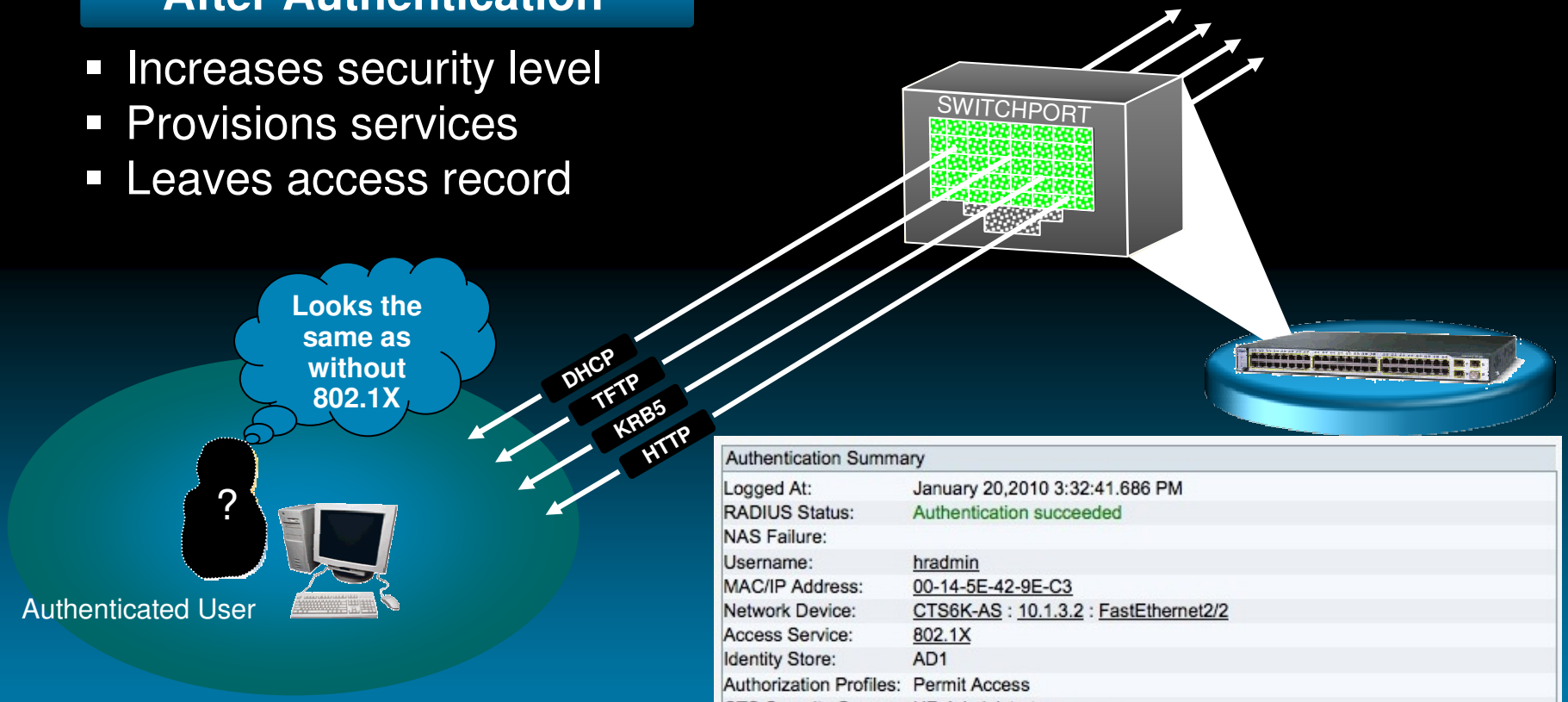
- No Visibility
- No Access Control



Network Port with 802.1X

After Authentication

- Increases security level
- Provisions services
- Leaves access record

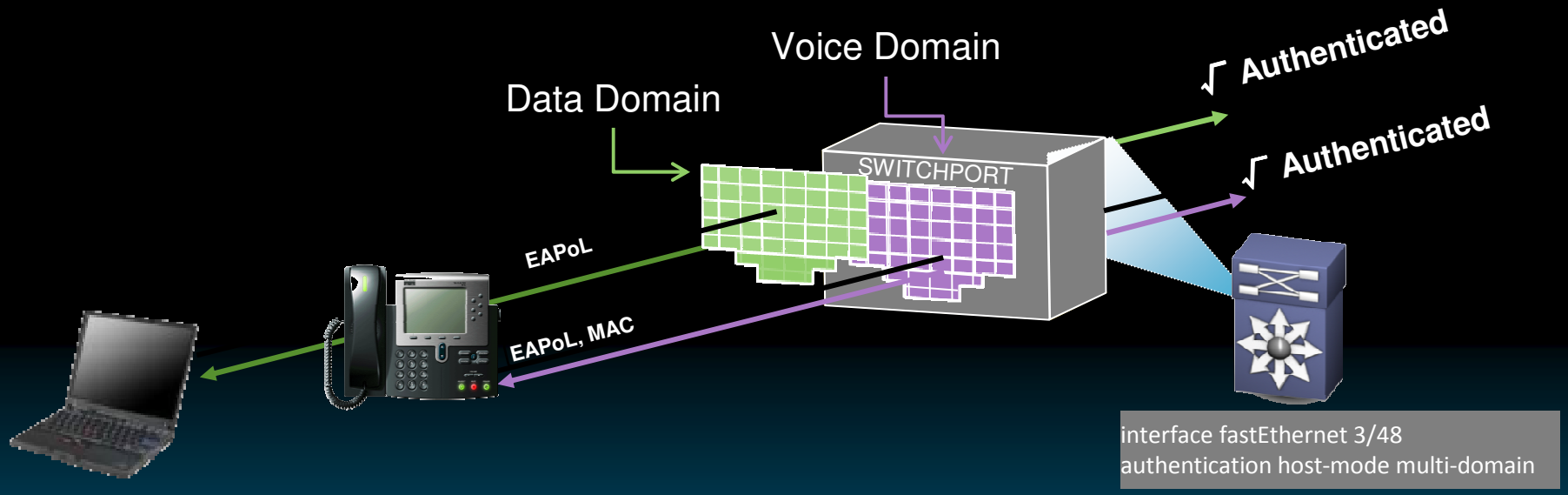


Authentication Summary	
Logged At:	January 20,2010 3:32:41.686 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	hradmin
MAC/IP Address:	00-14-5E-42-9E-C3
Network Device:	CTS6K-AS : 10.1.3.2 : FastEthernet2/2
Access Service:	802.1X
Identity Store:	AD1
Authorization Profiles:	Permit Access
CTS Security Group:	HR Administrator
Authentication Method:	PEAP(EAP-MSCHAPv2)

Cisco TrustSec Flexible Authentication

- Flexible authentication allows:
- Three different authentication methods:
  - 802.1X for supplicant-capable devices
  - MAC Authentication Bypass (MAB)
  - Web Authentication (typical user ID / password pair)
  - Provisioned per port
    - In any combination
    - In any order
- This reduces network OpEx because:
  - End users can move devices without network admin labor.
  - During transition from web auth to 802.1X, ports do not need to be reconfigured since each desktop/laptop is configured for 802.1X.

802.1X + IPT Solution: Multi-Domain Authentication (MDA) Host Mode



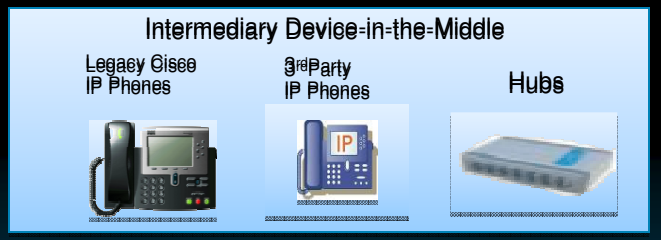
Benefits	Deployment Considerations
Secure 802.1X orMAB Authentication of the IP phone AND PC (removes CDP vulnerability)	Authentication type impacts timing, pre-deployment tasks
Compatible with IBNS features: dynamic VVID, downloadable ACLs (dACLs), Web Auth	AAA server dependency -- Centralized policy assigns phones to voice domain
Works for all phones, but retains Cisco-on-Cisco value for Cisco phones	Not all phones support 802.1X

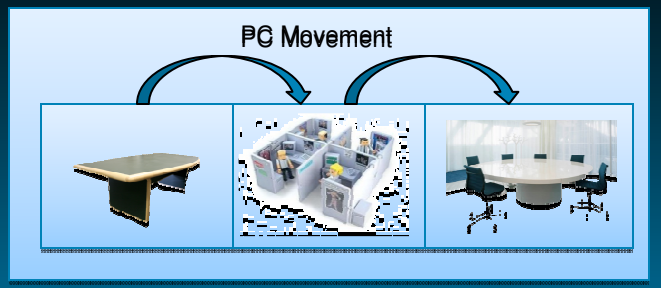
MAC Move / Replace
Problem Statement & Drivers

Customers requirement is to have Identity based access control for tighter security, as well as integrated in IP Telephony environments.

One challenge is Link state awareness of authenticated devices connected behind legacy Cisco IP Phones, 3rd Party Phones or Hubs. Especially with respect to movement from previously authenticated MAC addresses.

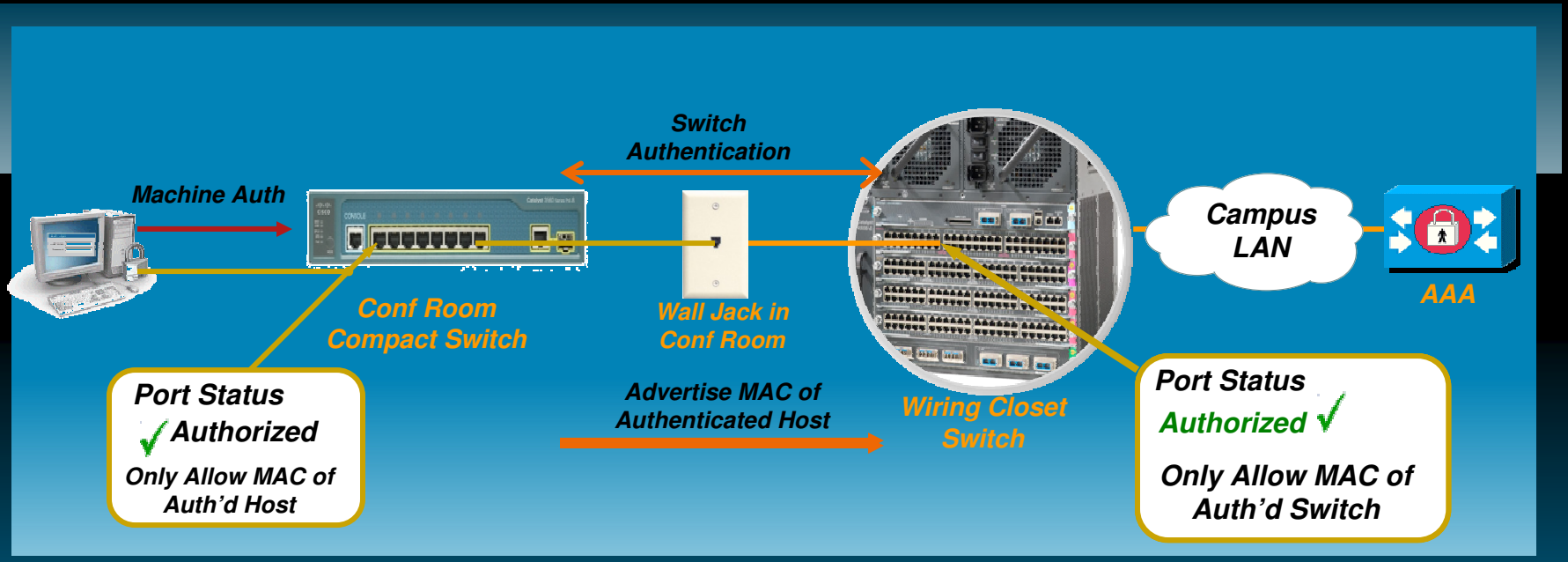
- Ability to move from location to location or new connections on previously authenticated non-direct connected ports without encountering issues or security violations





Customers want ***access control***&***mobility*** in an ***Identity Enabled Networks***

Rogue Device Mitigation: Network Edge Access Topology



- Extend trust to conference room deployment.
- Secure access control for shared media access.

Authorization and Policy Enforcement in the Network

Various Authorization Mechanisms

- TrustSec provides various authorization mechanisms for policy enforcement.
- Three major enforcement / segmentation mechanisms:
  - Dynamic VLAN assignment - Ingress
  - Downloadable per session ACL - Ingress
  - Security Group Access Control List (SGACL) - Egress
- Three different enforcement modes:
  - Monitor Mode
  - Low Impact Mode (with Downloadable ACL)
  - High-Security Mode
- Session-Based on-demand authorization:
  - Change of Authorization (RFC3576 RADIUS Disconnect Messages, ReV 5176)

Cisco TrustSec
Security Group-based Access Control

- TrustSec is a broad umbrella for security improvements based on the capability to strongly identify users, hosts and network devices within a network
- Security Group Access Control provides topology independent and scalable access controls by uniquely classifying data traffic for a particular role
- Security Group Access Control ensures data confidentiality and integrity by establishing trust among authenticated peer and encrypting links with those peers

Security Group-based Access Control Key Features

Security Group Based Access Control

- Topology independent access control based on roles
- Scalable **ingress tagging (SGT) / egress filtering (SGACL)**
- Centralized Policy Management / Distributed Policy Enforcement

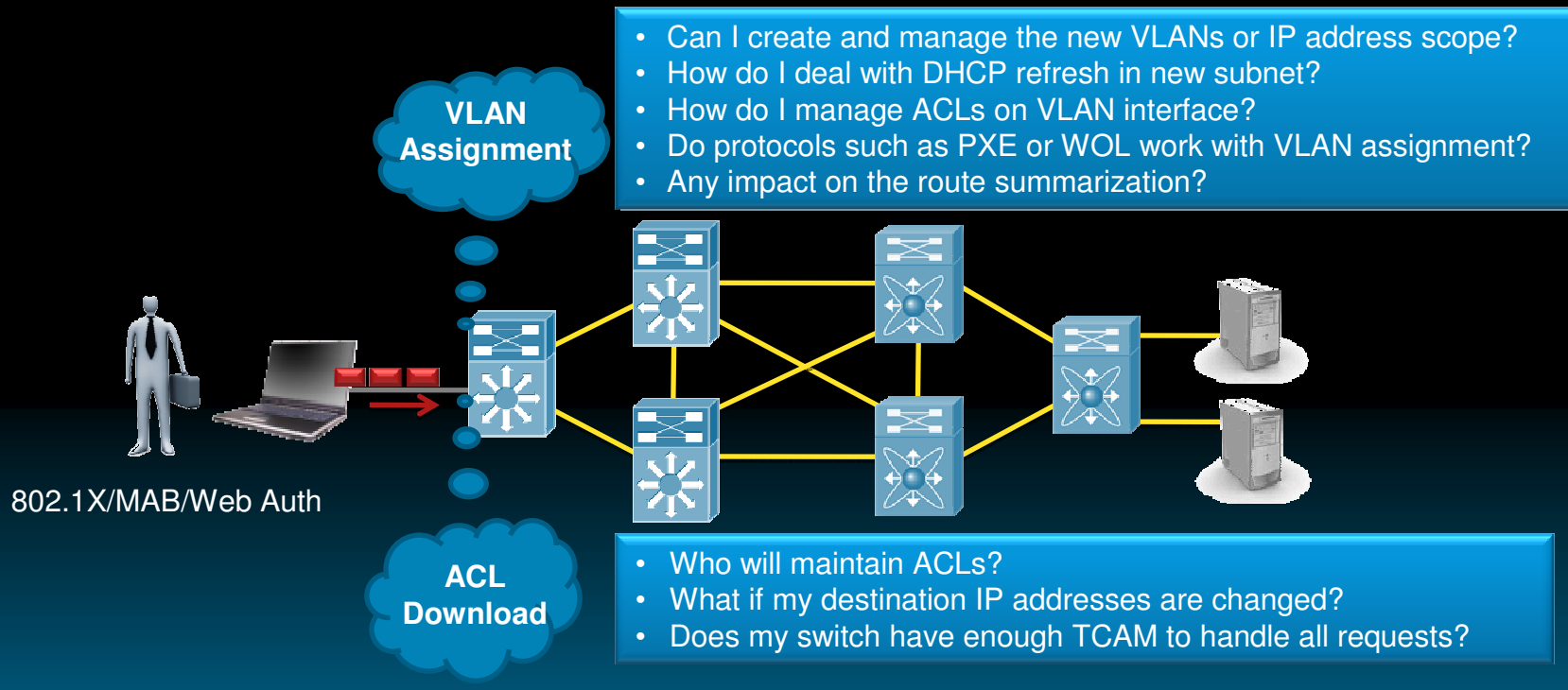
Authenticated Networking Environment

- Endpoint admission enforced via 802.1X authentication, MAB, Web Auth (Cisco Identity compatibility)
- Network device admission control based on 802.1X creates trusted networking environment
- Only trusted network imposes Security Group TAG

Confidentiality and Integrity

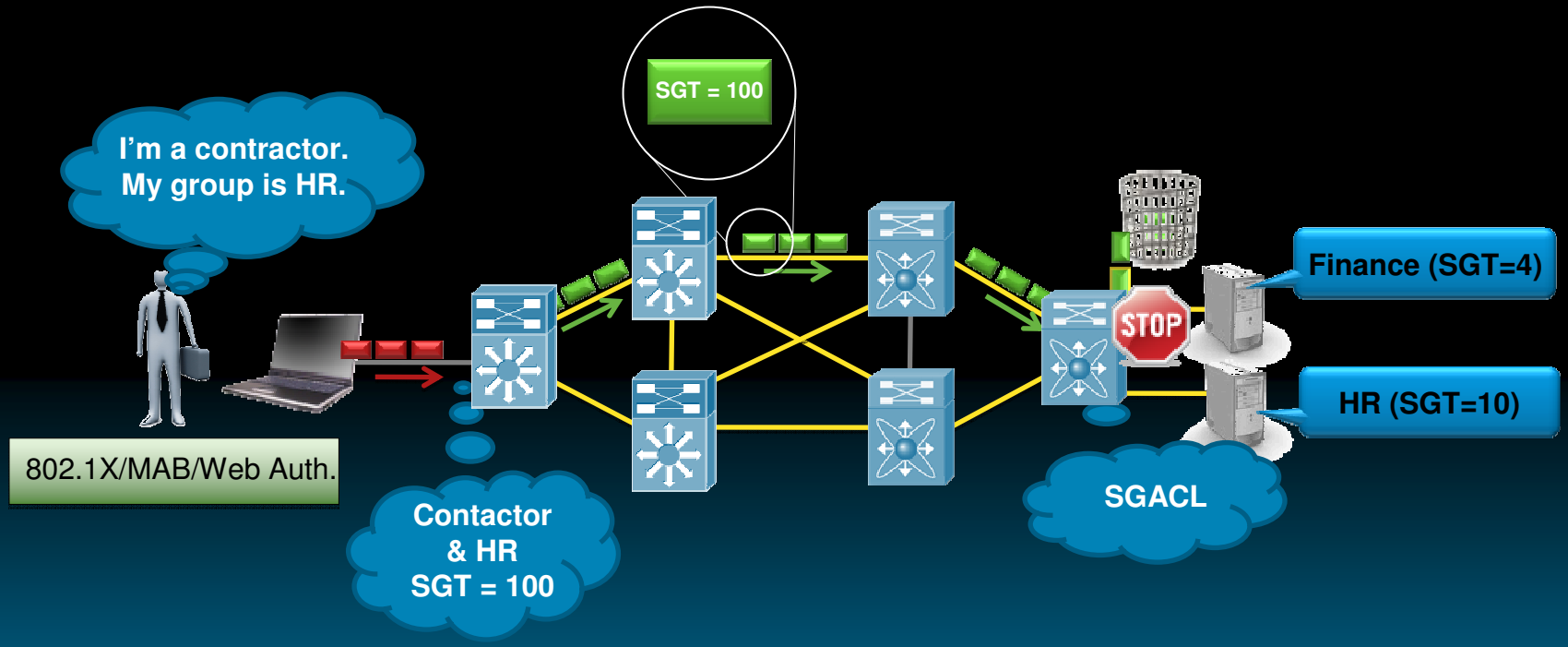
- Encryption based on **IEEE802.1AE** (AES-GCM 128-Bit)
- **Wire rate** hop by hop layer 2 encryption
- Key management based on 802.11n (SAP), standardization in 802.1X-REV

Ingress Access Control



- Traditional access authorization methods leave some deployment concerns:
  - Detailed design before deployment is required, otherwise…
  - Not so flexible for changes required by today's business
  - Access control project ends up with redesigning whole network

Security Group–Based Access Control



- Security group–based access control allows customers:
  - To keep existing logical design at the access layer
  - To change / apply policy to meet today's business requirements
  - To distribute policy from a central management server

SGT and SGACL Enforcement

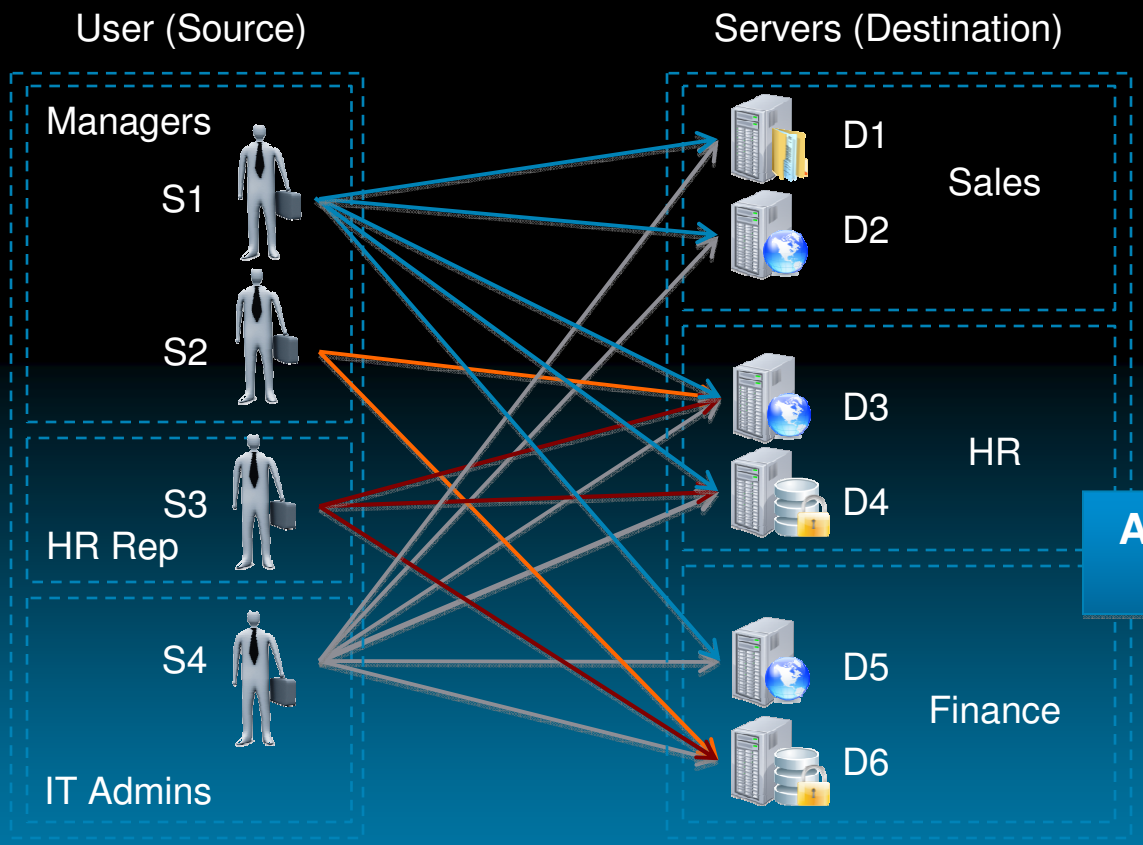
- **Unique 16 bit (65K)** tag assigned to **unique role**
- Represents **privilege of the source user, device, or entity**
- **Tagged at ingress** of TrustSec domain

- **Filtered (SGACL) at egress** of TrustSec domain
- **No IP address required in ACE** (IP address is bound to SGT)
- Policy (ACL) is **distributed from central policy server (ACS)** 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**

Traditional Access Control



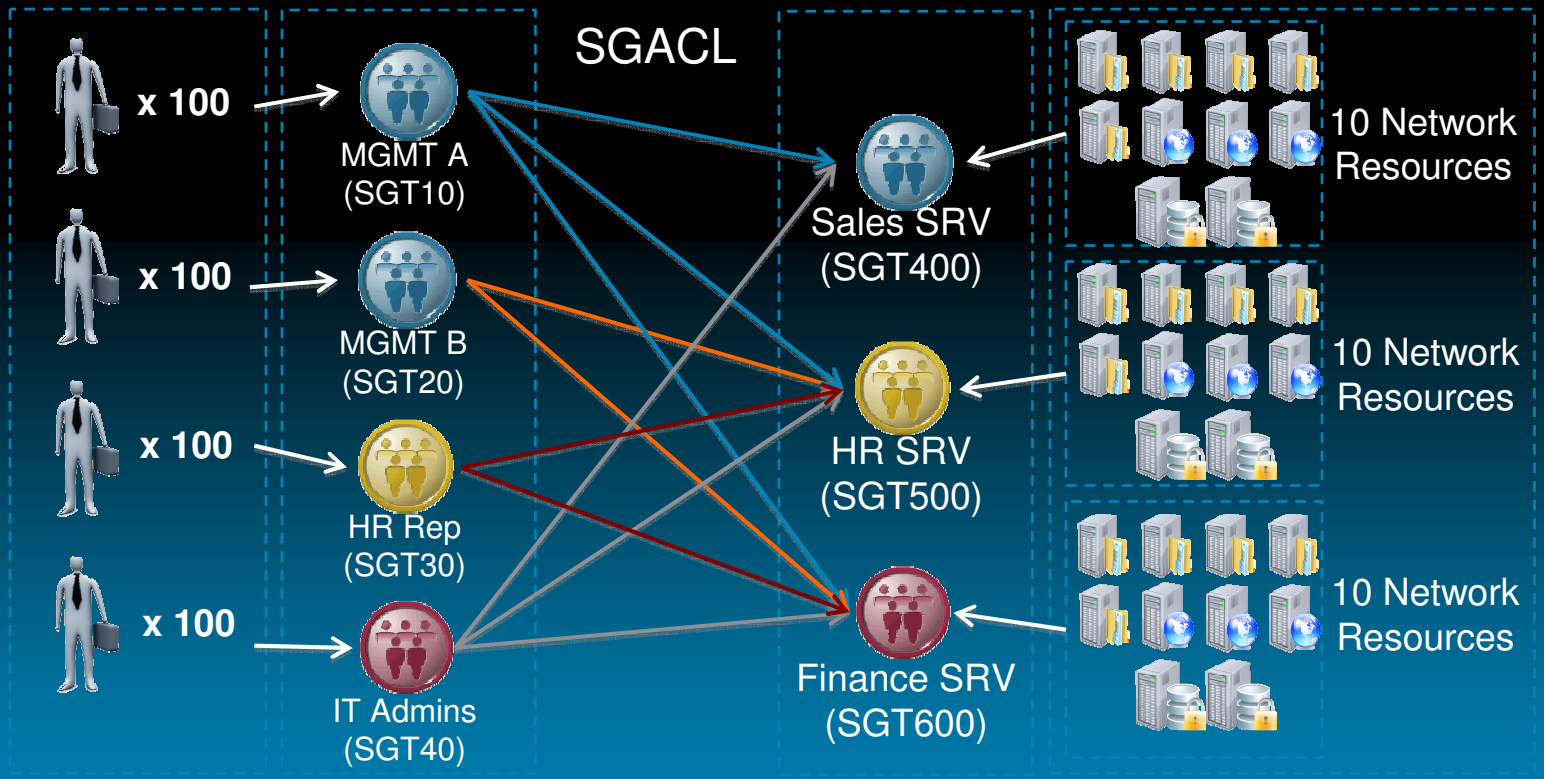
S1 to D1 Access Control

```
permit tcp S1 D1 eq https
permit tcp S1 D1 eq 8081
permit tcp S1 D1 eq 445
deny   ip   S1 D1
```

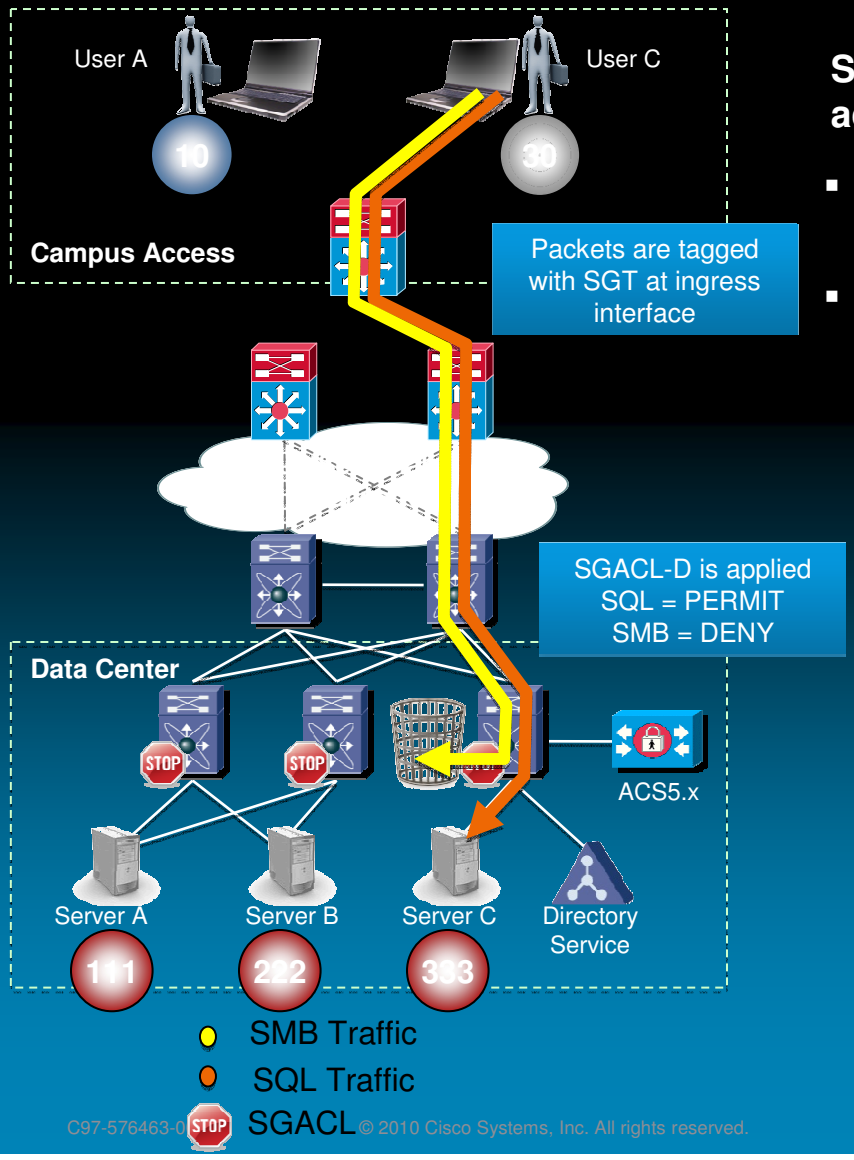
ACE # grows as # of permission statement increases

# of ACEs = (# of sources) * (# of Destinations) * permissions

How SGACL simplifies Access Control



SGACL Enforcement – LAN Enforcement



SGACL allows topology independent access control:

- Even if another user accesses on the same VLAN as previous example, his traffic is tagged differently.
- If traffic is destined to restricted resources, packet will be dropped at egress port of TrustSec domain.

SRC\ DST	Server A (111)	Server B (222)	Server C (333)
User A (10)	Permit all	Deny all	Deny all
User B (20)	SGACL-B	SGACL-C	Deny all
User C (30)	Deny all	Permit all	SGACL-D

SGACL-D

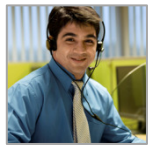
```
permit tcpsrcdsteq 1433
#remark destination SQL permit
permit tcp srceq 1433  dst
#remark source SQL permit
permit tcpsrcdsteq 80
# web permit
permit tcpsrcdsteq 443
# secure web permit
deny all
```

SGACL in Action

Access Policies > TrustSec Access Control > Egress Policy

Egress Policy

Destination / Source	Internal Server (9 / 0009)	IT Servers (4 / 0004)	Public Server (8 / 0008)	Record DB (10 / 000A)
Doctor (7 / 0007)	Permit_Web_Only	Deny IP	Permit_Web_Only	Permit_Web_WinFileShare
Guest (15 / 000F)	Deny IP	Deny IP	Permit_Web_Only	Deny IP
IT Administrator (5 / 0005)	Permit IP	Permit IP	Permit IP	IT_Maintenance_ACL
Staff (11 / 000B)	Permit_Web_Only	Deny IP	Permit_Web_Only	Deny IP

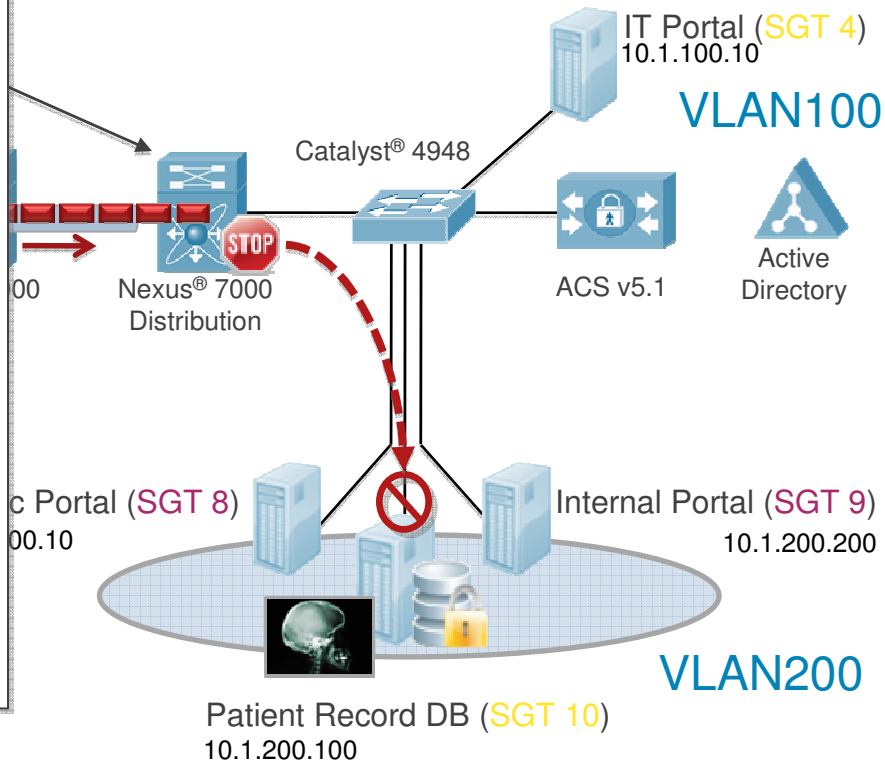


IT Admin (SGT 5)

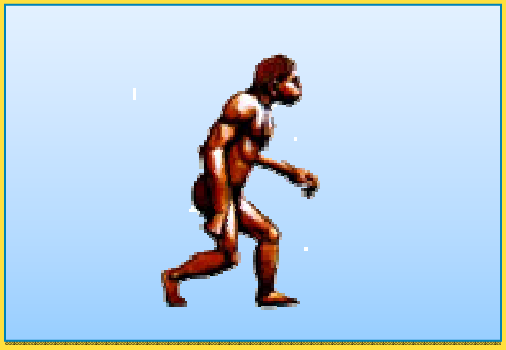
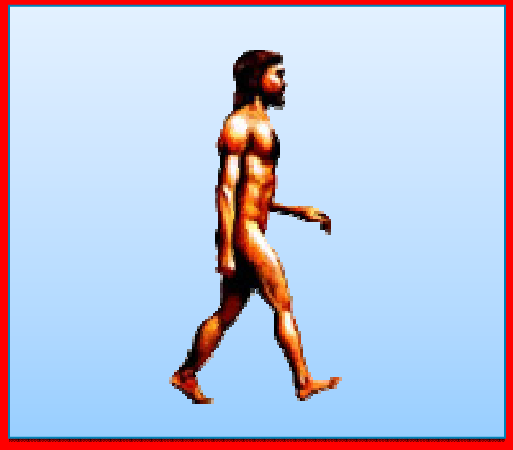
Users, Endpoints

802.1X

```
CTS7K-DC# show cts role-based policy

sgt:5
dgt:4   rbacl:Permit IP
        permit ip

sgt:5
dgt:8   rbacl:Permit IP
        permit ip

sgt:5
dgt:9   rbacl:Permit IP
        permit ip

sgt:5
dgt:10  rbacl:IT_Maintenance_ACL
        permit tcp dst eq 20 log
        permit tcp dst eq 21 log
        permit tcp dst eq 22 log
        permit tcp dst eq 445 log
        permit tcp dst eq 135 log
        permit tcp dst eq 136 log
        permit tcp dst eq 137 log
        permit tcp dst eq 138 log
        permit tcp dst eq 139 log
        permit tcp dst eq 3389 log
        permit icmp log
        deny ip
<skip>
```



Deployment Modes
Campus Deployability

Monitor Mode	Low Impact Mode	High Security Mode
Primary Features ▪ Open mode ▪ Multi-Auth ▪ Flex Auth **Benefits** ▪ **Unobstructed Access** ▪ No Impact on Productivity ▪ Gain Visibility AAA Logs	**Primary Features** ▪ Open mode ▪ Multi-Domain ▪ Port & dACLs **Benefits** ▪ Maintain Basic Connectivity ▪ No design changes ▪ Increased Access Security/Visibility ▪ Differentiated Access	**Primary Features** ▪ Traditional Closed Mode ▪ Dynamic VLANs **Benefits** ▪ Strict Access Control
		

Data Integrity and Confidentiality

Confidentiality and Integrity 802.1AE based Encryption

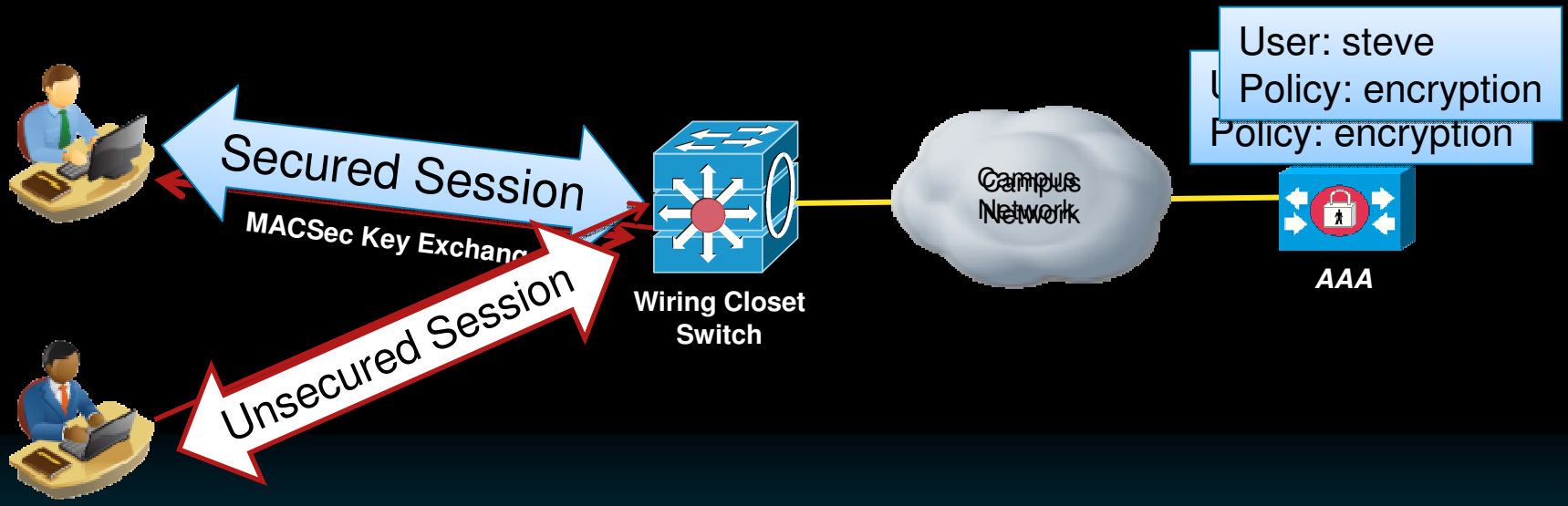
- TrustSec provides Layer 2 hop-by-hop encryption and integrity, based on IEEE 802.1AE standard
- 128bit AES-GCM (Galois/Counter Mode) – NIST Approved *
- Line rate Encryption / Decryption for both 10GbE/1GbE interface
- Replay Protection of each and every frame
- Announced already on new Cat 3K (3750-X), SUP 2T for C6k, Nexus7

Customer Benefits

- Protects against man-in-the-middle attacks (snooping, tampering, replay)
- Standards based frame format and algorithm (AES-GCM)
- Network service amenable hop-by-hop approach compared to end-to-end approach (e.g. Microsoft Domain Isolation/IPsec)

* NIST Special Publication 800-38D (http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf)

802.1AE (MACSec) and 802.1X-REV (MKA)



1. User bob connects.
2. Bob's policy indicates endpoint must encrypt.
3. Key exchange using MKA, 802.1AE encryption complete.
   User is placed in corporate VLAN.
   Session is secured.
4. User steve connects
5. Steve's policy indicates endpoint must encrypt.
6. Endpoint is not MACSec enabled.
   Assigned to guest VLAN.

802.1X-Rev Components

- MACSec enabled switches
- AAA server 802.1X-Rev aware
- Supplicant supporting MKA and 802.1AE encryption

Network Device Admission Control

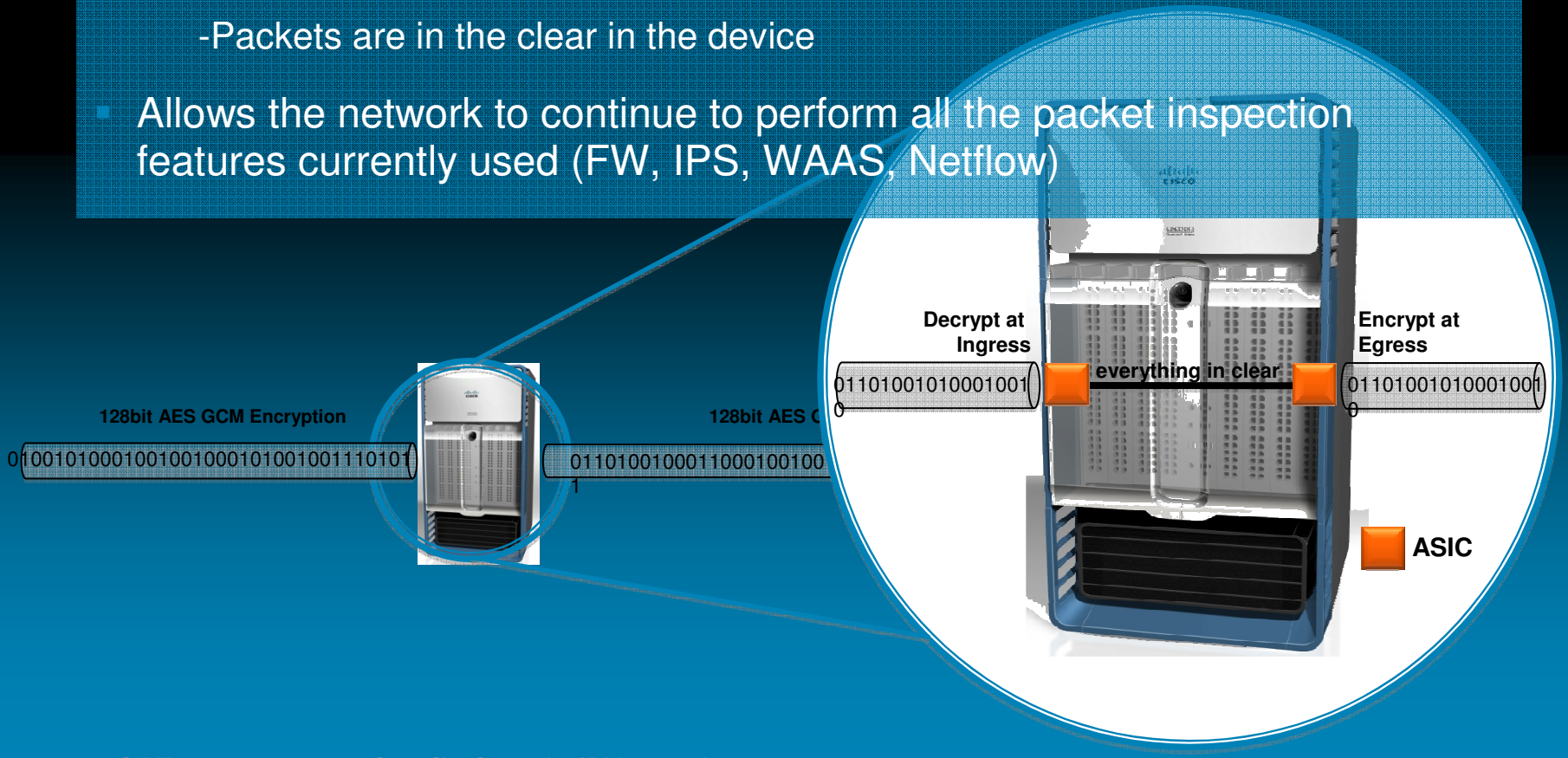
- Network Device Admission Control (NDAC) provides strong **mutual authentication (EAP-FAST) to form trusted domain**
- Only SGT from **trusted peer is honored**
- Authentication leads to **Security Association Protocol (SAP)** to negotiate keys and cipher suite for encryption automatically (mechanism defined in 802.11i)
- 802.1X-REV will succeed and replace SAP
- Trusted device acquires trust and policies from ACS server

Customer Benefits

- Mitigate rogue network devices, **establish trusted network fabric** to ensure SGT integrity and its privilege
- Automatic key and cipher suite negotiation for **strong 802.1AE based encryption**

Hop-by-Hop Encryption via IEEE802.1AE

- "Bump-in-the-wire" model
  - -Packets are encrypted on egress
  - -Packets are decrypted on ingress
  - -Packets are in the clear in the device
- Allows the network to continue to perform all the packet inspection features currently used (FW, IPS, WAAS, Netflow)



The Secure Network Fabric

802.1x/Infrastructure

NDAC

- Prevents rogue endpoints and network devices from connecting to the network
- Network Device Admission Control (NDAC) enforces strong mutual authentication of network devices before joining the fabric (NEAT)

802.1AE

- Provides data confidentiality & integrity for wired Ethernet throughout the Enterprise
  - Mitigates packet eavesdropping, tampering, and injection
- Standards-based technology
  - Strong (128-bit AES-GCM), NIST-approved, 10Gb line-rate encryption
  - Leverages IEEE standards including the MACsec Key Agreement (MKA) protocol
- Deployment versatility
  - Hop-by-hop approach supports existing packet inspection technologies (IPS, Firewall, Caching, WAN optimization/acceleration, Network monitoring)
  - Works in shared media environments (IP Phones, Desktops)

802.1X-2010

ACS for Policy-Based Access Control

More Flexible Policy with Role-Based Access Control

Policy for Today's Business Requirement

Identity Information

Identity:
Network Administrator

Identity:
Full-Time **Employee**

Identity:
Guest

+

Other Conditions

Time and Date

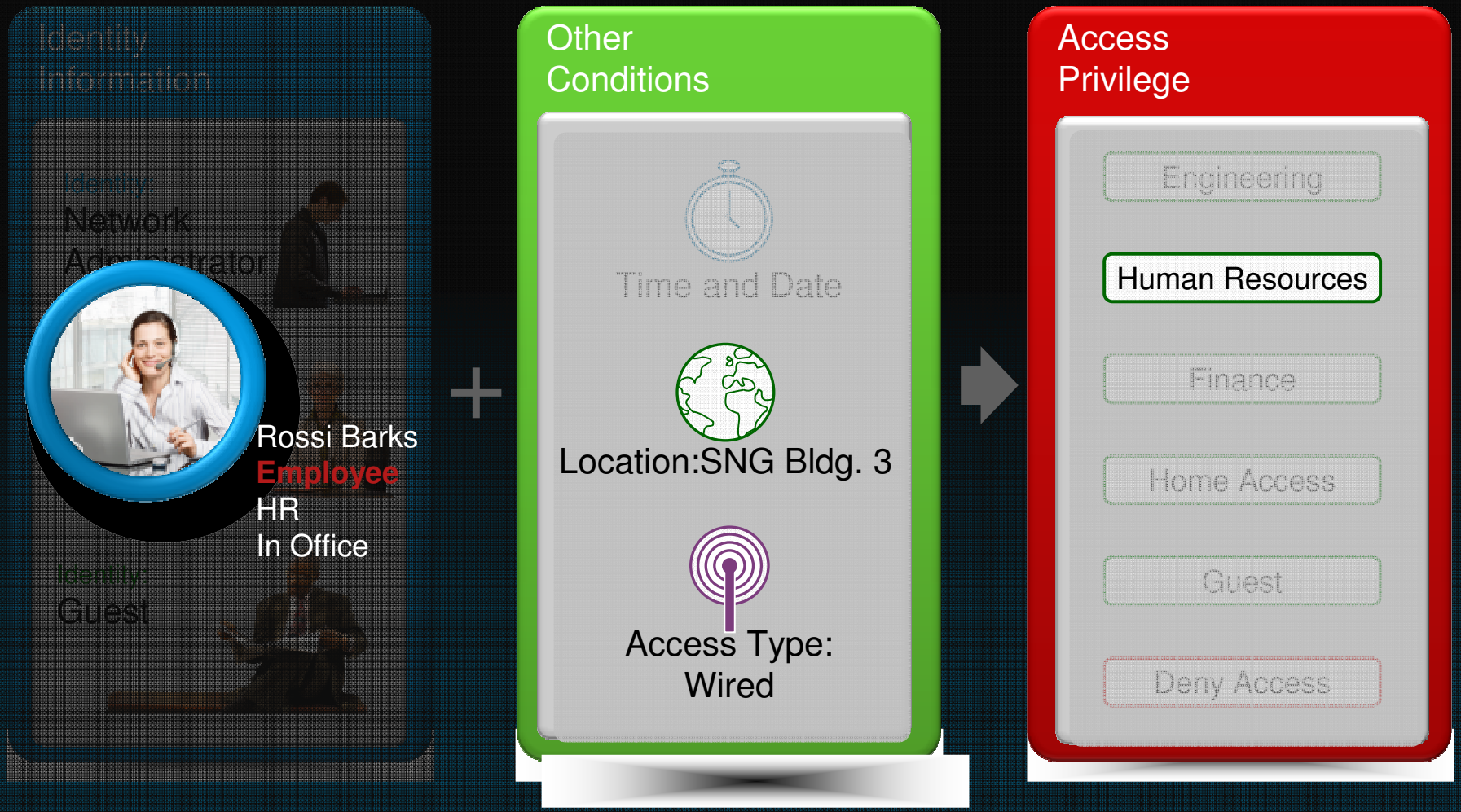
Location

Access Type

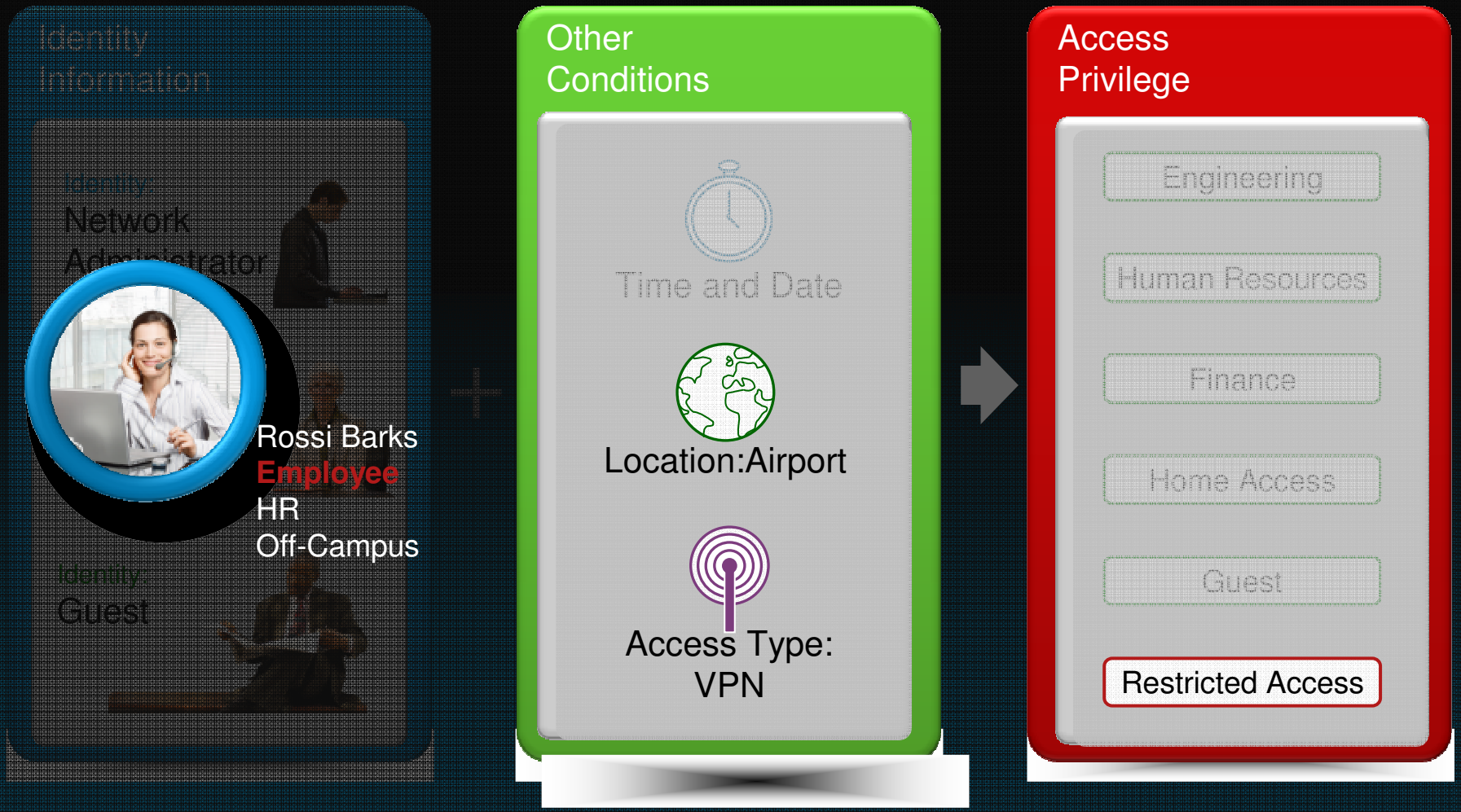
Access Privilege

- Consultant
- Human Resources
- Finance
- Marketing
- Guest
- Deny Access

Role + Rule–Based Access Control Example: Human Resources Role



Role + Rule–Based Access Control Example: Human Resources Role



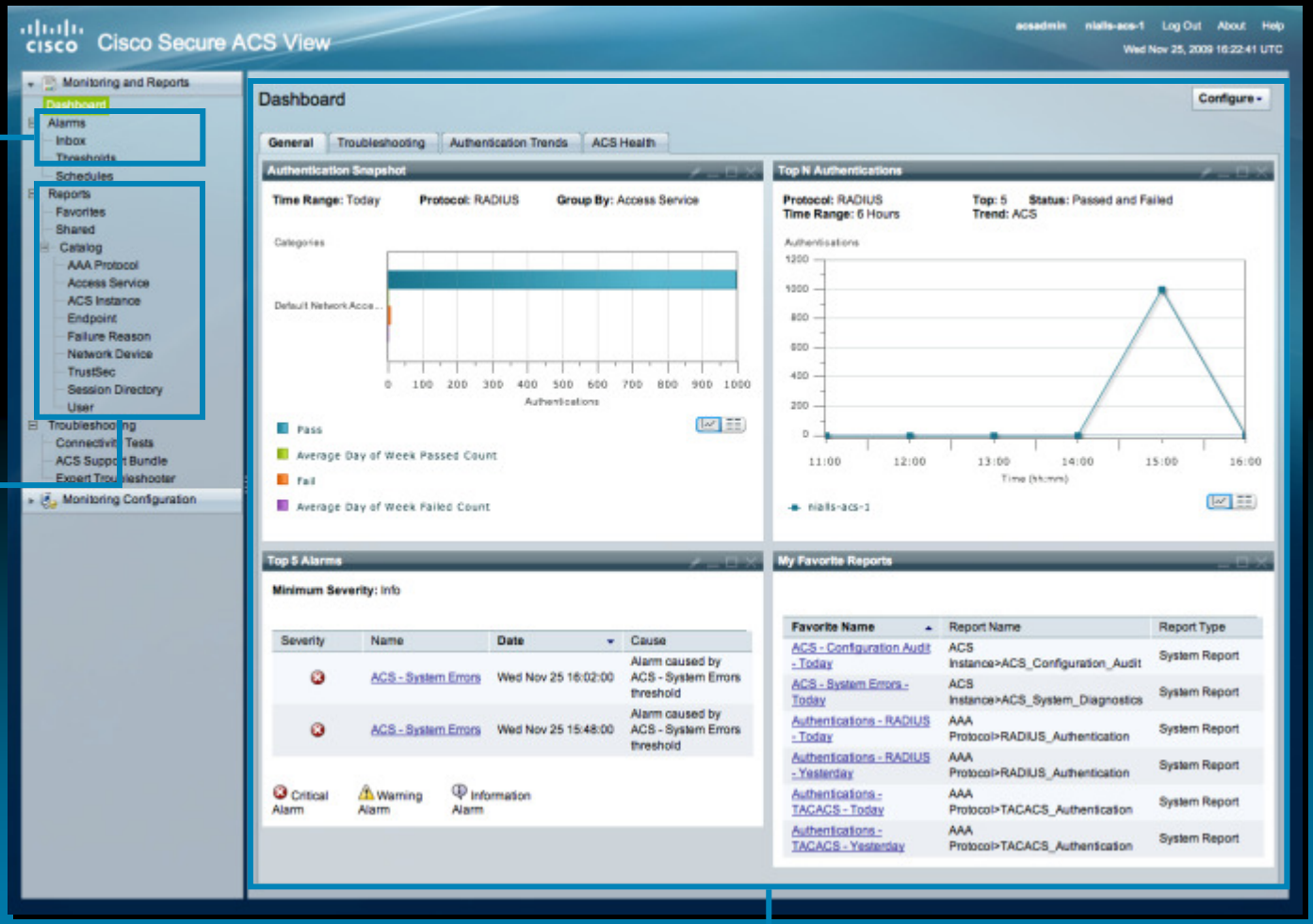
Cisco ACS
Monitoring & Troubleshooting Tool

Alarms and Notifications

- Custom Triggers
- Alerts via Email and Syslog

Comprehensive Reporting

- Standard Reports
- Templates
- Customized Reports



Fully Configurable Dashboard

Cisco TrustSec End to End

Client	IP Telephony	Campus Access	Servers
Cisco® Identity • Cisco Secure Services Client • Identity Agent • Built in 802.1X in OS	Cisco IP Telephony • IP phones Cisco IOS® Software (most robust) • Cisco and third-party support	Cisco LAN Switches • Cisco Catalyst® Switches Cisco WLAN • Cisco access points and controllers	Cisco RADIUS • Cisco Secure ACS 5.0 NAC • Profiler or guest
			

Solution Expertise

Compatibility/Support

Vendor Stability


CISCO