

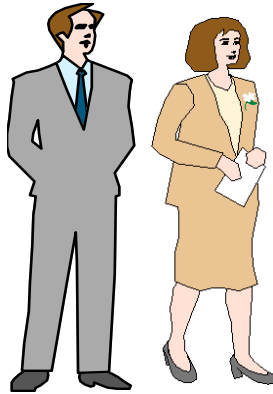


Overview of ISE vs ACS policy model

by: Krishnan Thiruvengadam

Date: 11/10/2017

What is Access Control?



APPROVED

Access control policy plan

Policy

High level business requirement with Identity, context and level of access

Model

Role Based Access control
and/or
Rule Based Access control

Mechanism

VLAN, ACL, SGT

Identity



Context



Access Level

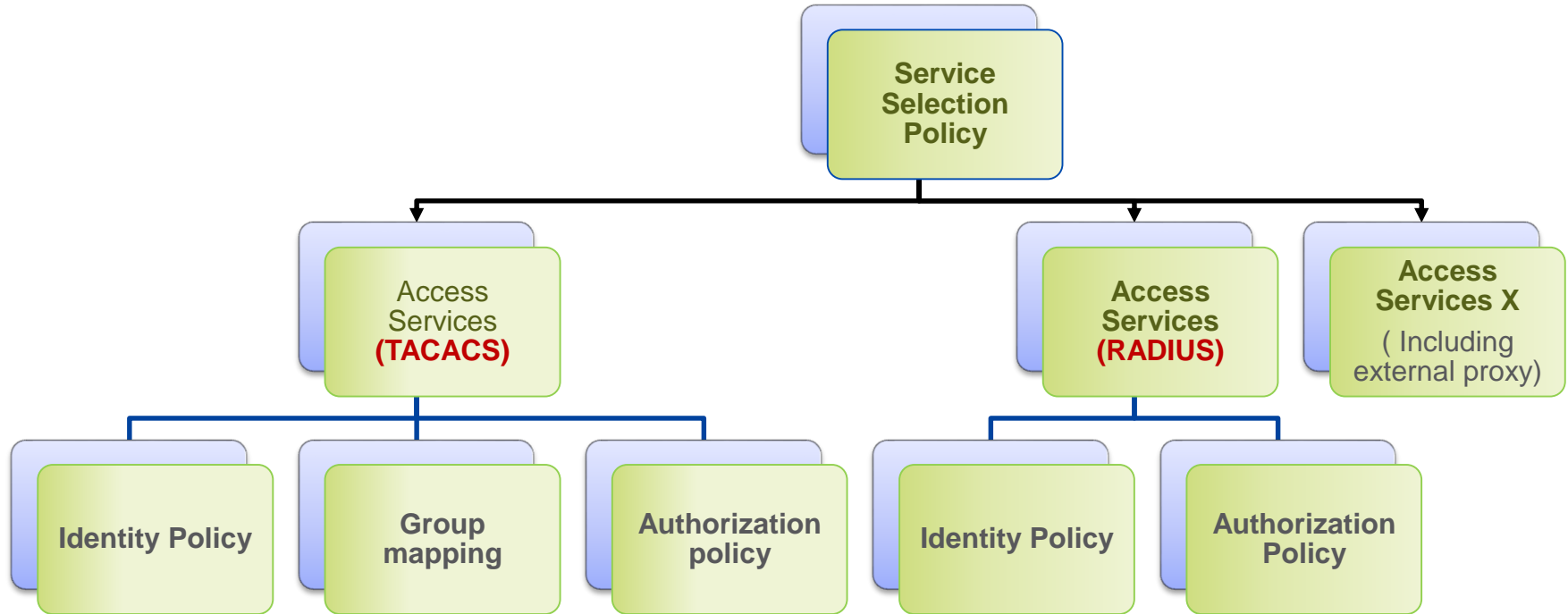
Full Access

Internet only

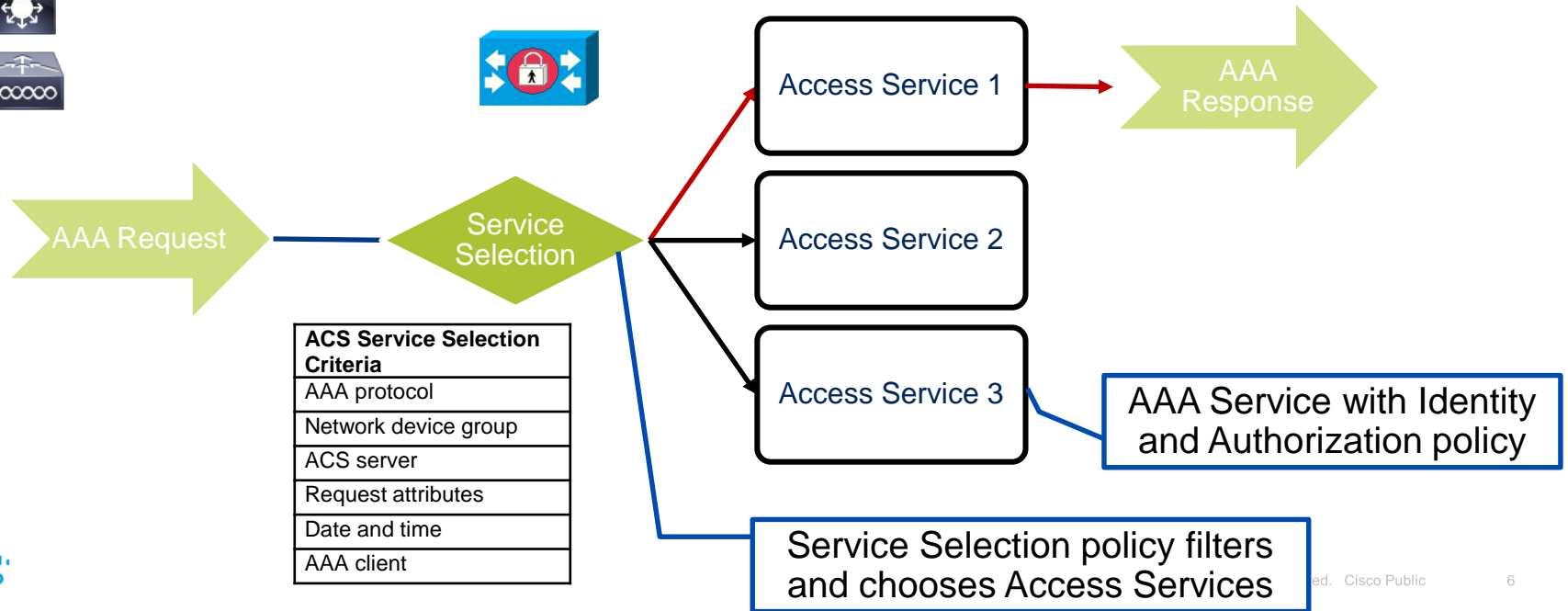
Policy example

Identity	Context (who, what, when, where, how, posture/threat)	Level of Access
Guest (including contractors)	WiFi, Weekly, verify MAC	Internet
Personal devices	WiFi, employee	Limited Access after onboarding
Device Administrators	Network operators, WLC Help desk, WLC	Full Access Monitoring access

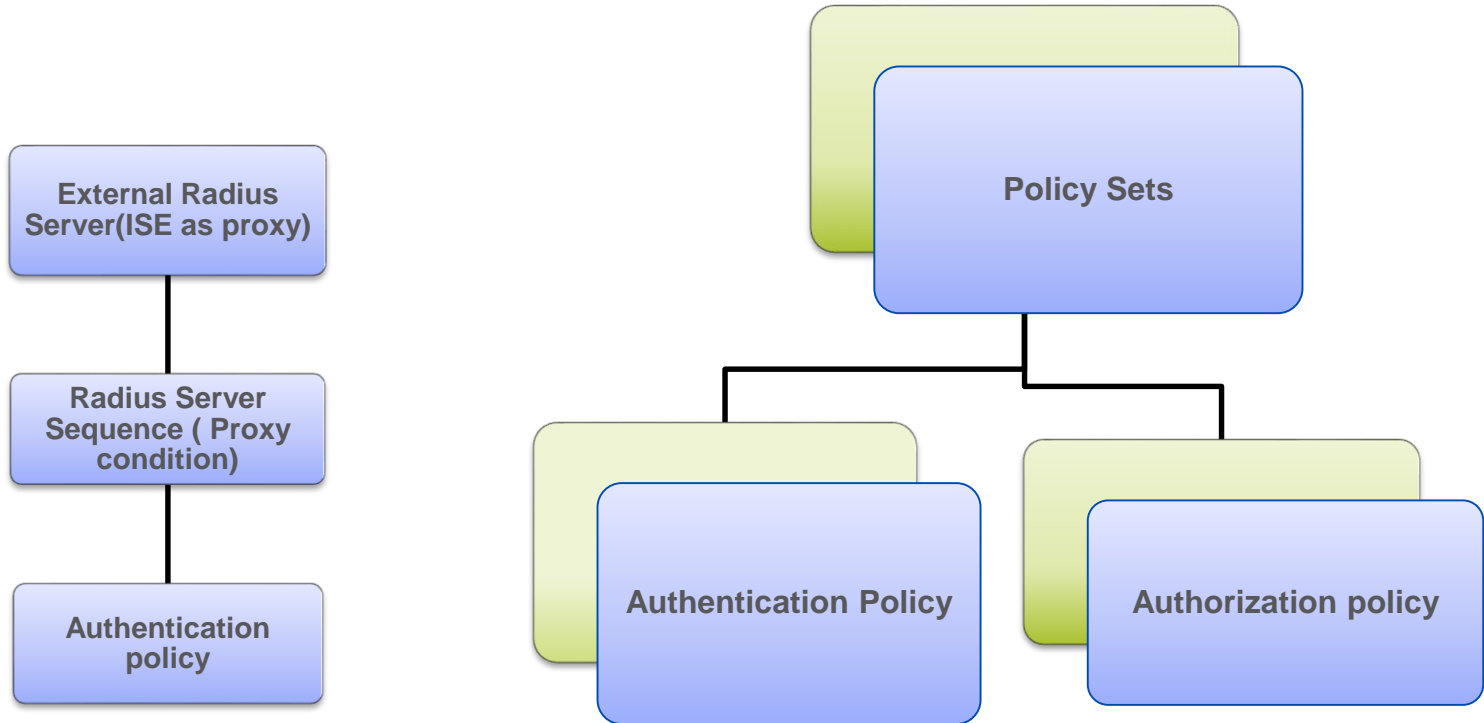
ACS Policy model – Service selection rules



ACS Service Selection Policy

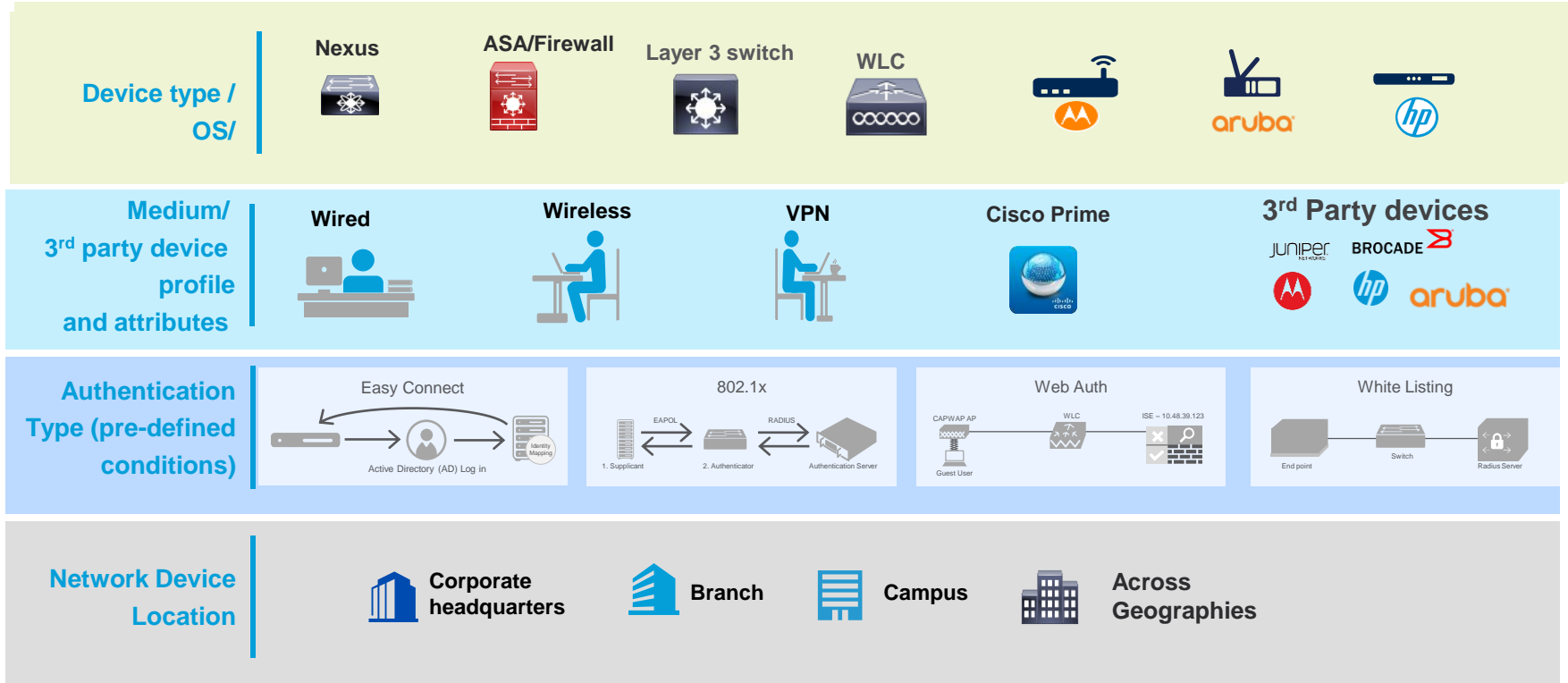


ISE Policy model – Policy sets



Policy Sets

Policy set conditions/ criteria



Conditions supported in ISE Policy sets



Policy Set Conditions (Network Access)

- Network devices
- Basic Network access
- 3rd party NAD
- Network device profiles
- Radius/ TACACS+ attribute
- Pre-defined conditions



Policy Set Conditions (Device Administration)

- Network devices
- Basic Network access
- TACACS+ attribute
- Pre-defined conditions



Device Administration Best Practices

The screenshot displays the Cisco Prime Network Device Groups (NDG) interface. On the left, a tree view shows the hierarchy: Groups > All Device Types > Firewall, Loadbalancer, Prime Infrastructure, Raritan, RAS, Router, Switch, WAAS, WLAN; and All Locations > APAC, CORP. On the right, a list of NDG names is shown with checkboxes: Name, All Device Types, All Locations, and All Migrated_NDGs. The interface includes a search bar, navigation icons, and action buttons like Edit, Add, Duplicate, and Delete.

Network Device Groups

Groups

- All Device Types
 - Firewall
 - Loadbalancer
 - Prime Infrastructure
 - Raritan
 - RAS
 - Router
 - Switch
 - WAAS
 - WLAN
- All Locations
 - APAC
 - CORP

Network Device Groups

Edit Add Duplicate Delete

- Name
- All Device Types
- All Locations
- All Migrated_NDGs

USE NDG'S!

Different Policy Sets for
IOS than AireSpace OS

Different for Security
Apps than Routers

Different for ASA

Differentiate based on
location of Device

Use Policy Sets Based on Device Type

Identity Services Engine Home

TrustSec Device Administration

Overview Identities User Identity Groups

Policy Sets

Search policy names & descriptions.

Summary of Policies
A list of all your policies

Global Exceptions
Rules across entire deployment

Access Switches
Set for T+ on Switches

Wireless LAN Controllers
WLCs

Default
Tacacs_Default

Save Order Reset Order

Policy Sets

Search policy names & descriptions.

Summary of Policies
A list of all your policies

Global Exceptions
Rules across entire deployment

Access Switches
Set for T+ on Switches

Wireless LAN Controllers
WLCs

Default
Tacacs_Default

Save Order Reset Order

Cisco IOS
Switches

Airspace WLCs

ACS - Service Selection rules (custom conditions)

ACS UI: Access Policies → Access Services → Service Selection rules → **Customize**

Access Policies > Access Services > Service Selection Rules

Single result selection Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

	<input type="checkbox"/>	Status	Name	Protocol	Compound Condition	Results
1	<input type="checkbox"/>	🟢	RadiusAuthentication	match Radius	-ANY-	PA - RAS Access
2	<input type="checkbox"/>	🟢	TACACSPRimeAuth	match Tacacs	NDG:Device Type in All Device Types:Prime Infrastructure	PA - Prime Access
3	<input type="checkbox"/>	🟢	TACACSApac	match Tacacs	NDG:Location in All Locations:APAC	PA - APAC Network Dev
4	<input type="checkbox"/>	🟢	TACACSAmericas	match Tacacs	(NDG:Location in All Locations:NORAM Or NDG:Location in All Locations:LATAM)	PA - AMERICAS Network
5	<input type="checkbox"/>	🟢	TACACSEMEA	match Tacacs	NDG:Location in All Locations:EMEA	PA - EMEA Network Dev
6	<input type="checkbox"/>	🟢	TACACSCORP	match Tacacs	NDG:Device Type not in All Device Types:Raritan	PA - CORP Network Dev

Customize Hit Count

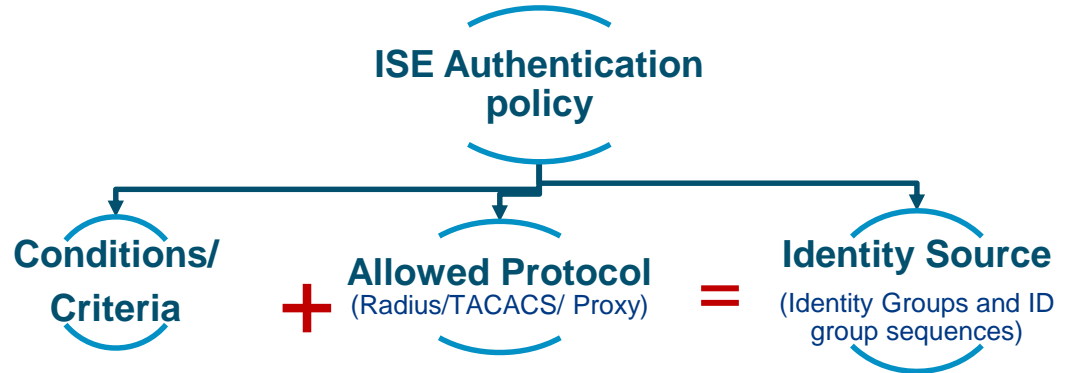
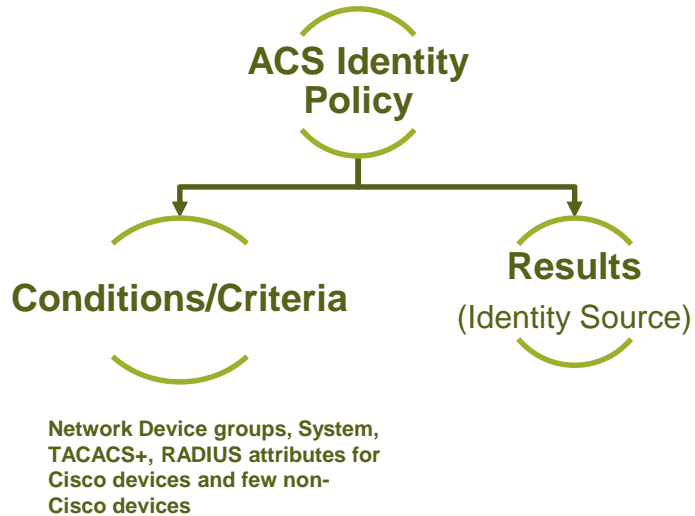
ISE - Policy set criteria (Compound Conditions)

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The navigation menu at the top includes: Home, Context Visibility, Operations, Policy, Administration, and Work Centers (circled in red with a '1'). Below this, the main navigation bar includes: Network Access (circled in red with a '2'), Guest Access, TrustSec, BYOD, Profiler, Posture, and Device Administration. The left sidebar contains a 'Conditions' section with the following items: Authentication Simple Conditions, Authentication Compound Conditions (circled in red with a '3'), Authorization Simple Conditions, Authorization Compound Conditions, and Time and Date Conditions. The main content area is titled 'Authentication Compound Conditions' and includes a sub-header: 'For Policy Export go to Administration > System > Backup & Restore > Policy Export Page'. Below this, there are action buttons: Edit, Add, Duplicate, and Delete. A table lists the following conditions:

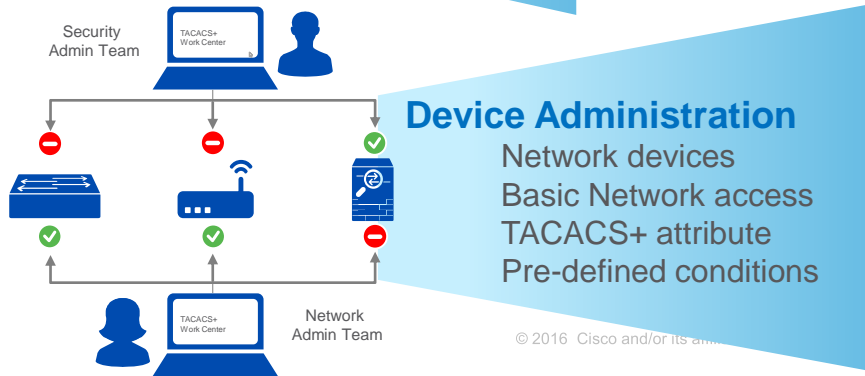
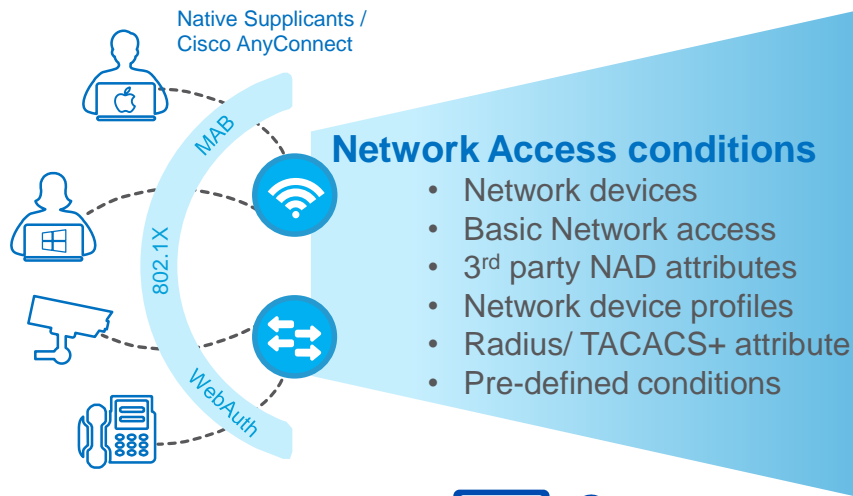
<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Switch_Local_Web_Authentication	
<input type="checkbox"/>	Switch_Web_Authentication	All Profiles
<input type="checkbox"/>	TACACSAMERICAS_comp_cond_1	
<input type="checkbox"/>	TACACSAMERICAS_entry_rule_1	

Authentication Policy

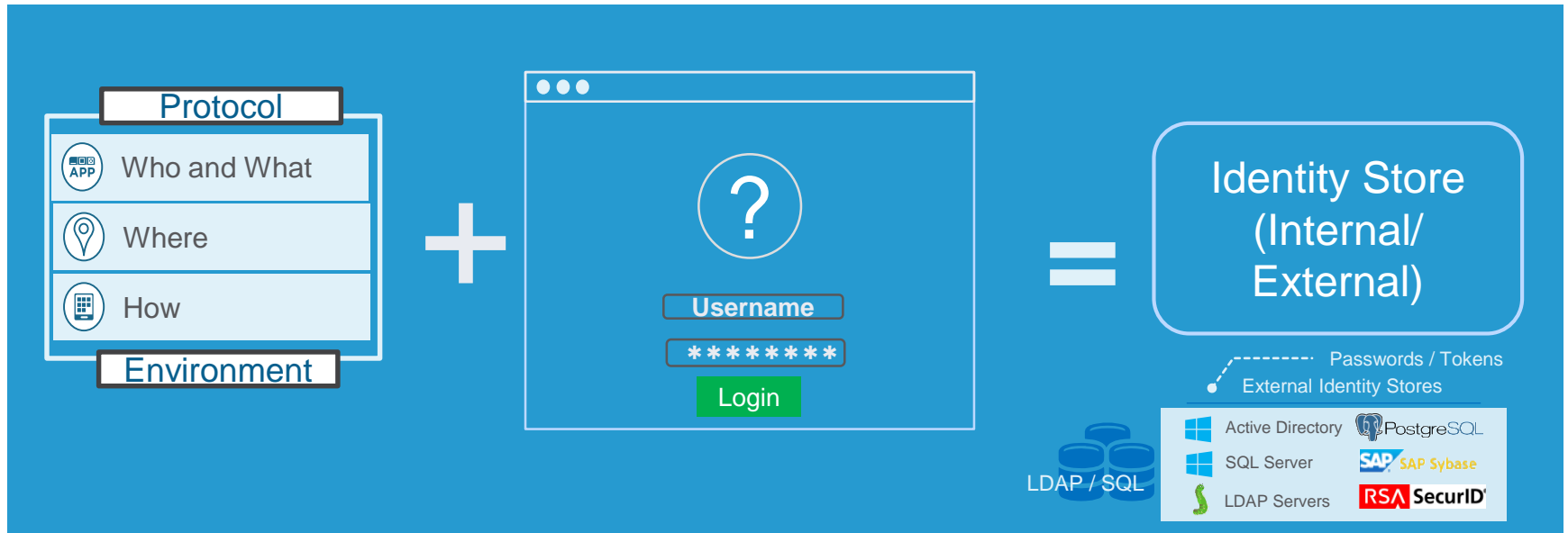
ACS vs ISE Authentication policy



Conditions supported in ISE Authentication policies

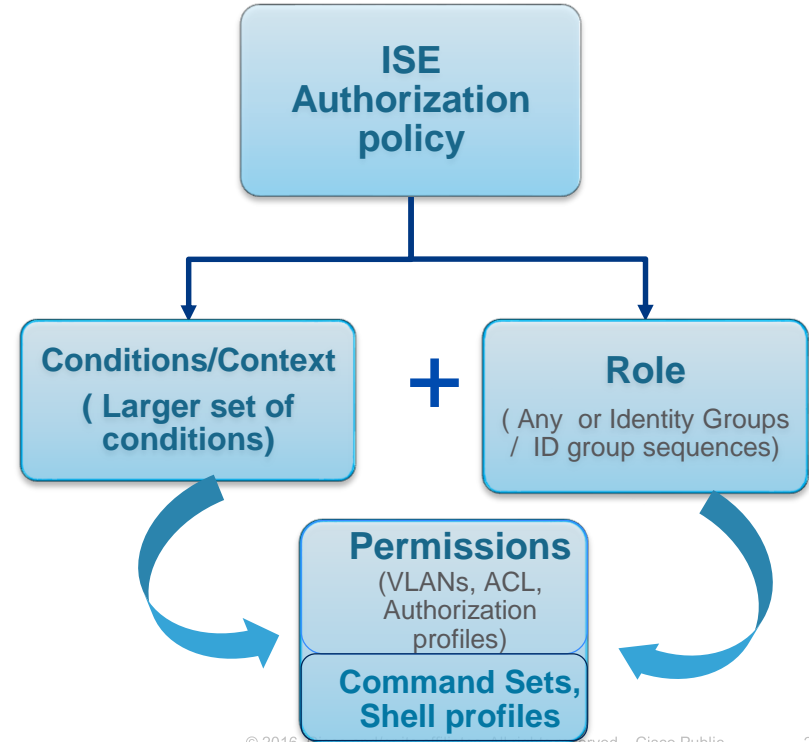
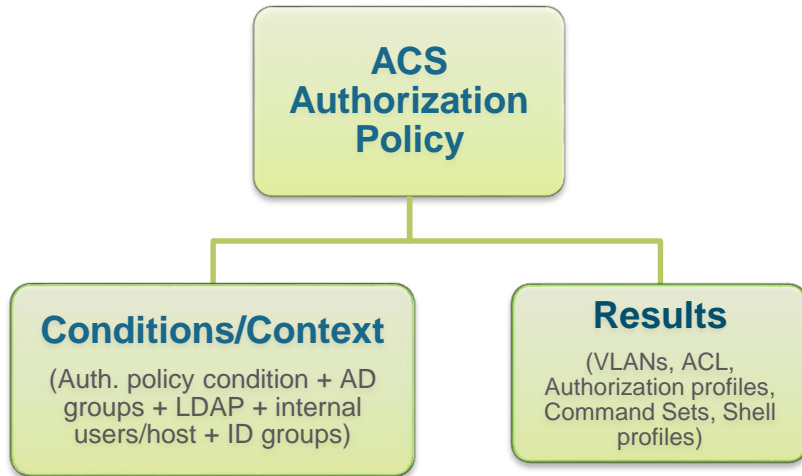


How does ISE authenticate users?

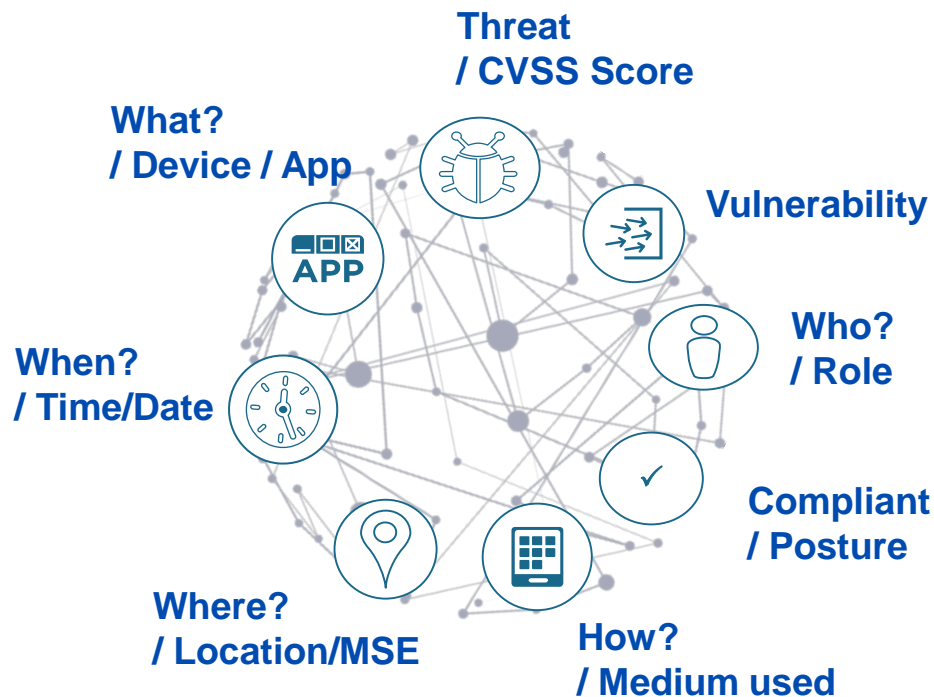


Authorization policy

ACS vs ISE Authorization policy



Authorization Policy Conditions/Context



Context /Conditions

- Network devices
- Basic Network access
- 3rd party NAD
- Network device profiles
- Radius/ TACACS+ attribute
- Pre-defined conditions
 - Time and Date Conditions
- Active Directory
- LDAP
- Endpoints
- Guest
- CWA
- Session
- MSE
- Passive ID
- Internal Users/ Groups

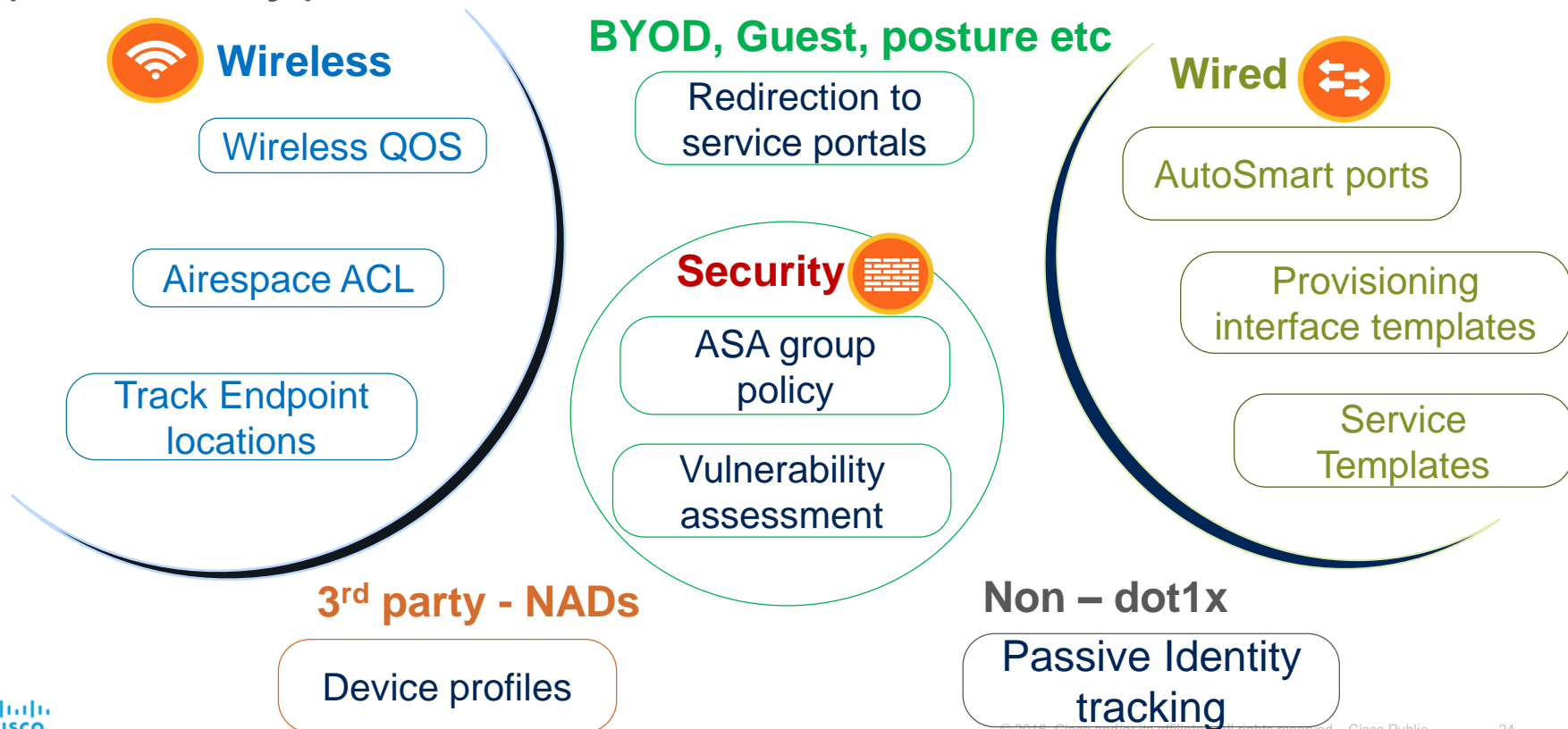
Reference:

<https://communities.cisco.com/docs/DOC-67894>

Authorization policy – Permissions (Network Access)

ACS	ISE
Downloadable ACL (Static/Dynamic from AD, Internal users/hosts, LDAP)	Downloadable ACL with syntax check(Static / Dynamic supported in ISE 2.1 p 2(internal users/AD)
Authorization profile	
Downloadable ACL Filter ID ACL Proxy ACL	Downloadable ACL Filter ID ACL
Linksec Security policy: Should, must, must-not secure	MACSec policy: Should, must, must-not secure
Reauthentication timer (Static/Dynamic from AD, Internal users/hosts, LDAP)	Reauthentication timer (static) (Use Advanced setting to map it to AD attribute)
VLAN (Static/Dynamic from AD/internal users/host/LDAP) with configurable ID only	VLAN (AD support via Advanced setting- create RADIUS attributes for VLAN and map the value to AD attribute)
QOS (Input and Output policy map)	Not supported

Authorization policy – Authorization profile (ISE only)



Authorization Policy Example

SGT can also be used for enforcement

Authorization Profile Details

Name **InternetGuest_Policy**
Description
Attributes Details
Service Template **false**
Access Type **ACCESS_ACCEPT**
DACL Name **ACL_Internet-Only**
Airespace-ACL-Name **wACL_Guest_Internet_Only**

<input checked="" type="checkbox"/>	Hotspot_InternetAccess	if GuestEndpoints AND (Wireless_MAB AND Radius:Called-Station-ID ENDS_WITH :DEMO-Hotspot)	then InternetGuest_Policy
<input checked="" type="checkbox"/>	Hotspot_Redirect	if (Wireless_MAB AND Radius:Called-Station-ID ENDS_WITH :DEMO-Hotspot)	then Hotspot_Redirect
<input checked="" type="checkbox"/>	Guest_InternetAccess	if (Wireless_MAB AND Radius:Called-Station-ID ENDS_WITH :DEMO-Guest AND Network Access:UseCase EQUALS Guest Flow)	then InternetGuest_Policy
<input checked="" type="checkbox"/>	Guest_Redirect	if (Wireless_MAB AND Radius:Called-Station-ID ENDS_WITH :DEMO-Guest)	then GuestAccess_Redirect

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Redirection to Guest Portal, Different portals are used here for different guest flows

Hot Spot

ACL

wACL_WEBAUTH_REDIRECT

Value

Hotspot Guest Portal (default)

Hotspot Guest Portal (default)

Guests do not require username and password credentials to access the network, but you can optionally require an access code

Used in 1 rules in the Authorization policy

Authorization policy – Shell Profiles(Device Administration)

ACS

General **Common Tasks** Custom Attributes

Privilege Level

Default Privilege:

Maximum Privilege:

Shell Attributes

Access Control List:

Auto Command:

No Callback Verify:

No Escape:

No Hang Up:

Timeout:

Idle Time:

Callback Line:

Callback Rotary:

ISE – IOS devices

TACACS Profiles > New

TACACS Profile

Name:

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type:

Default Privilege (Select 0 to 15)

Maximum Privilege (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout Minutes (0-9999)

Idle Time Minutes (0-9999)

TACACS+ Profile Types (ISE Only)

ISE – WLC devices

Common Task Type

All
 Monitor
 Lobby
 Selected

WLAN Controller Wireless Security Management Commands

The configured options give a mgmtRole Debug value of: 0x0 ⓘ

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Monitor

- Summary
- Access Points
- Cisco CleanAir
- Statistics

Summary

12 Access Points Supported



Cisco 5508 Series Wireless Controller
Model 5508

ISE – Nexus devices

TACACS Profiles > New

TACACS Profile

Name

Description

Task Attribute View Raw View

Common Tasks

Common Task Type

Set attributes as

Network role

- None
- Operator (Read Only)
- Administrator (Read Write)

VDC role

- None
- Operator (Read Only)
- Administrator (Read Write)

Authorization policy Device administration

IOS-SecOps-NoConfig
Deny_Always Config *
Permit Everything Else

IOS-PermitAllCommands
Permit *

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	StackCommandSets	if Any and Domain-Admi...	NoShow ...	IOS-Priv15
<input checked="" type="checkbox"/>	Security-Priv15-NoConfig	if (SecOps OR SecAdmin)	IOS-SecOps-NoConfig	
<input checked="" type="checkbox"/>	NetOps-Priv13	if NetOps	IOS-PermitAllCommands	
<input checked="" type="checkbox"/>	NetAdmin-Priv15	if NetAdmin		
<input checked="" type="checkbox"/>	EmployeeNoShow	if Employees		
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAllCommands	

ISE Public Resources

ISE Public Community:

<http://cs.co/ise-community>

Customer Connection Program:

<http://cisco.com/go/ccp> > Security

ISE Compatibility Guides:

<http://cs.co/ise-compatibility>

ISE Design & Integration Guides:

<http://cs.co/ise-guides>

ISE Licensing / Ordering Guide:

<http://cs.co/ise-licensing> | <http://cs.co/ise-ordering>



The screenshot displays the Cisco Communities page for Identity Services Engine (ISE). At the top, there are navigation links for 'Welcome, Guest', 'Help', and 'Login', along with a search bar. Below this, a breadcrumb trail reads: 'Cisco Communities > Technology > Cisco Security Community > Policy and Access > Identity Services Engine (ISE)'. The main heading is 'Identity Services Engine (ISE)', followed by a prompt to 'Log in to follow, share, and participate in this community. Not a member? Join Now!'. The page is divided into several sections: 'Overview', 'Content', and 'People'. A 'Contact a Cisco Sales Rep' box includes a profile picture, an email icon, and contact information: 'Call us: 1-866-432-1783 EXT 114' and 'US/Can | 5am-5pm Pacific Other Countries'. Below this is an 'Ask the Community' section with a search bar and an 'Ask it' button. A 'Watch This Community to Stay Up-to-Date' section features a tip about email notifications and options to 'Subscribe (Login Required)' and 'View feeds'. A 'Take Action' section contains 'View feeds', 'Post and Share (Login Required)', and 'View feeds'. The 'Navigate to Other Community Forums' section lists various forums like 'Security Forums', 'Threat-Centric Security', 'Security Solutions', 'Advanced Threats', 'Policy and Access', and 'Security Forums Security Home'. The main content area is titled 'What can we help you with?' and includes a search bar and a 'Search' button. Below this are 'Quick Links to ISE Resources' categorized into: 'Get Started' (with links to ISE 2.1 Release, Streamlined Visibility Wizard, Contact Visibility, Easy Connect, Rapid Threat Containment, Threat Centric NAC, Threat Centric NAC with Qualys, Profiler Work Center Overview, BYOD Work Center Overview, Network Access Work Center, and Quick Start Videos); 'Device Admin' (with links to ISE Device Administration (TACACS+), ISE Device Administration Attributes, and ISE & MACsec); 'Network Access' (with links to ISE Compatibility Guides (CCO), ISE Design & Integration Guides, ISE Third-Party NAD Profiles, ISE Easy Connect, ISE Network Access Attributes, Phone Authentication Capabilities, ISE Authentication & Authorization Policies, How To: Troubleshoot ISE Failed Authentications & Authorizations, and ISE & MACsec); 'Demos' (with links to ISE Demo, CiscoISE @ YouTube > Demos, and TechWiseTV: Inside Cisco ISE); 'Documentation' (with links to ISE Product Documentation (CCO), Release Notes, Compatibility Guides, Administrator Guides, ISE 2.1: Release Notes, Network Component Compatibility, ISE Administrator Guide, ISE API Reference Guide, ISE CLI Reference Guide, ISE Hardware Installation Guide, ISE Upgrade Guide, ISE Migration Tool Guide, ISE My Devices Portal FAQs, ISE Sponsor Portal User Guide, ISE Certificate Provisioning Portal FAQs, ISE Active Directory Integration, and ISE Open Source Used); 'Training' (with links to ISE Training, ISE Partner Training, Cisco IT and ISE [Blog] (CCO), Cisco Live: Sessions Library, ISE @ LabMinutes, ISE Training Partners: FastLane, and Global Knowledge); 'Profiler' (with links to ISE Profiling, ISE Endpoint Profiles, Tag: ise-nad-profiles, and Cisco Medical NAC (CCO)); 'Guest Access' (with a link to ISE Guest & Web Authentication); 'BYOD' (with a link to ISE BYOD); 'Posture / Compliance' (with links to ISE Posture and ISE EMM & MDM); and 'Integrations' (with links to ISE Compatibility Guides (CCO), ISE Design & Integration Guides, ISE Location Base Services with Mobility Services Engine, ISE & MACsec, Network as a Sensor and Enforcer Config Examples and TechNotes (CCO), Rapid Threat Containment (RTC) (CCO), Security Technology Partners (CCO), and Technology Partner Marketplace). At the bottom, there is a 'TrustSec' section with a link to 'Simplify Network Segmentation with Cisco TrustSec - YouTube'.

Thank you.