

Cisco ISE

Cisco Identity Services Engine (ISE)

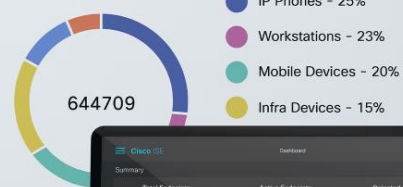
Know and control devices and users on your network

Employ intel from across your stack to enforce policy, manage endpoints, and deliver trusted access. Multicloud NAC with zero trust makes it possible.

[Watch overview \(03:48\)](#)

[Read latest news >](#)

Endpoints



Osama Raad Hateem

www.linkedin.com/in/osama-raad-9608081ba

المحتوى

Table of Contents

AAA.....	3
Change of authorization.....	3
identity source	4
802.1x and EAP	4
Authorization	6
MAC auth bypass	8
ISE PKI.....	11
User authentication certificate	11
Authorization	12
TrustSec.....	15
MacSec(802.1AE)	18
WebAuth	20
Guest service	22
الفرق بين Sponsor Portal و Guest Portal	22
Posture	23
Profiler.....	25
BYOD (bring your own device)	27

Cisco ISE (identity service engine)

هذا هو محور الكورس حول ise

Ise : هو عبارة عن policy engine كل يوزر له خصائص مثلا كل يوزر ماذا يعمل وماذا لا يعمل

AAA

Authentication : مثلا عملية تسجيل الدخول وتتم عن طريق بروتوكول

- 802.1x
- Web auth
- MAC auth bypass

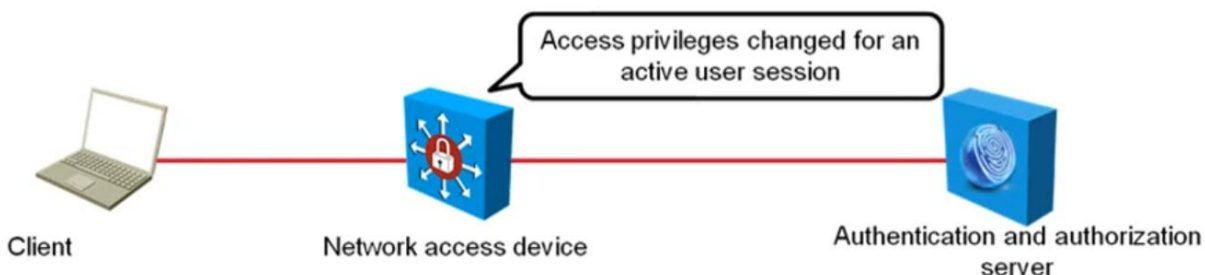
Authorization : الصلاحيات التي تعطى لليوزر عن طريق :

- Acl
- Vlan
- Security group access

Accounting : ماذا يفعل اليوزر عندما يدخل الى النيتورك وتحليل ماذا يفعل وتسجيل الاحداث وتسجيل تفاصيل الجلسة

Change of authorization

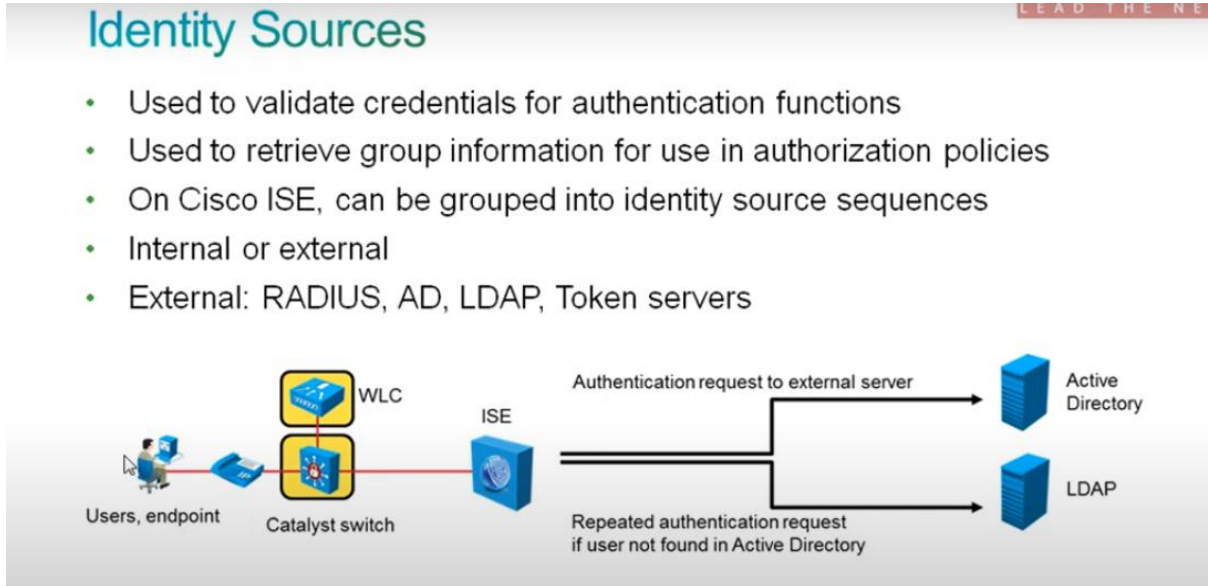
عندما يعمل الكلاينت Authentication يقوم Cisco ISE باعطاء صلاحيات الى السويتش حيث يقوم السويتش باعطاء هذا اليوزر صلاحيات واعتباره موثوق بدلا من الذهاب الى Cisco ISE كل مره لتخفيف الحمل عليه



identity source

يعني مثلا عندما اقوم بالدخول الى الشبكة من اين احصل على اليوزر والباسورد ؟
يكون اما داخلي او خارجي :

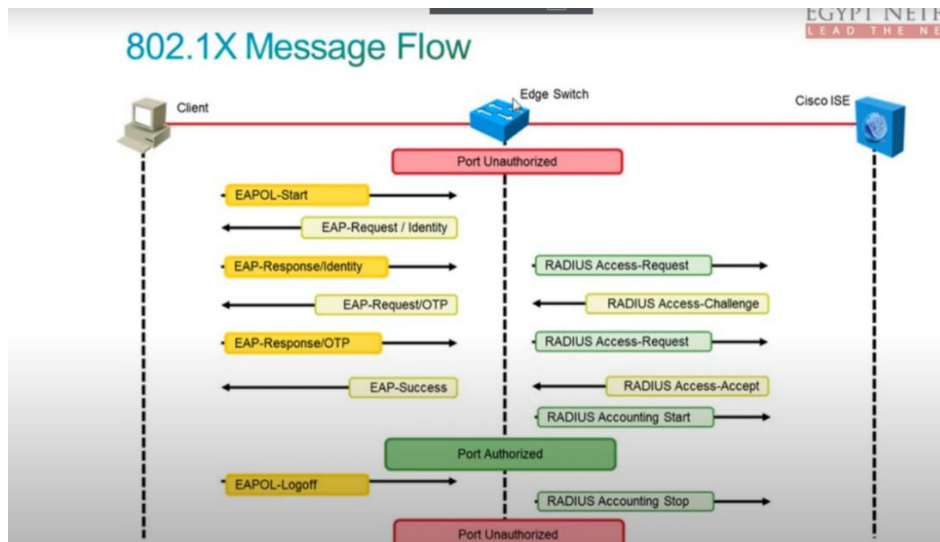
- داخلي : داخل Cisco ISE local database
- خارجي : على ويندوز سيرفر active directory او LDAP باستخدام بروتوكول RADIUS



البروتوكول الذي يعمل بين السويتش وال Cisco ISE هو radius

802.1x and EAP

- **Supplicant** : هو الجهاز الذي سوف يدخل للشبكة عن طريق واير او وايرلس
- **Authenticator** : الجهاز الذي سوف يعمل authentication من خلاله
- **Authentication** : هو الجهاز الذي يرى في الداتا بيس الخاصة به ويحدد اذا كان هذا اليوزر يدخل الى الشبكة او لا ويحدد صلاحياته في الشبكة



طريقه عمل 802.1x هي عمل port authentication ويساله عن اليوزر نيم والباسورد وعلى اساسه يعطي صلاحيات

Eap : هو البروتوكول الذي يرسل بين supplicant و switch (Authenticator) يقوم السويتش بالرد بانه يريد اليوزر والباسوورد يقوم السبلكينت بالرد باليوزر والباسوورد السويتش لم يملك اي قاعدة بيانات لليوزر نيم والباسوورد لذلك يقوم بارسال الطلب الى Cisco ISE ويقوم ال Cisco ISE بالتحقق مما اذا كان هذا اليوزر والباسوورد يسمح له بالدخول واعطائه الصلاحيات اذا كان اليوزر صحيح يصبح ال port authorized مصرح له بالدخول وبعد الخروج يصبح ال port Unauthorized

ويتم التواصل بين السوتش وال Cisco ISE عن طريق بروتوكول radius

Authorization

حالات اعطاء صلاحيات

802.1X Authorization

Cisco ISE can perform per-user and per-group network authorization:

- VLAN assignment: Applies a specific VLAN
- ACL assignment: Applies a specific ACL
- Time-based access: Limits network access based on time of day
- Cisco TrustSec:
 - Topology-independent, scalable access control
 - Classifies data traffic for a particular role
 - Ingress tagging via SGT
 - Egress filtering via SGACLs

vlan -1

هذه صورة للصلاحيات التي تعطى بعد ان قام اليوزر بالدخول واعطاء اليوزر نيم والباسورد بشكل صحيح
في هذه الحالة تعطى صلاحيات حسب ال vlan

- Assigned vlan : تعطى عندما ادخل بشكل صحيح وادخل لل 40 vlan مثلا وهذه ال vlan تكون لها صلاحيات محددة
- Guest vlan : يدخل لها عندما اكون لا املك يوزنيم وباسورد
- Retriected vlan : ادخل لها في حالة عمل Authentication بصورة خاطئة
- default vlan : عندما يكون Authentication صحيح ولا املك vlan
- critical vlan : تعطى عندما لا يتوفر ال cisco ise

802.1X VLAN Assignment



VLAN	Description
Assigned VLAN	Dynamically assigned by the authentication server.
Guest VLAN	Assigned if no supplicant detected and MAB does not apply.
Restricted VLAN	Assigned if the supplicant fails the authentication.
Default VLAN	Default VLAN configured on the port. Used with successful authentication when no specific VLAN is assigned.
Critical VLAN	Assigned if the authentication server is unavailable.

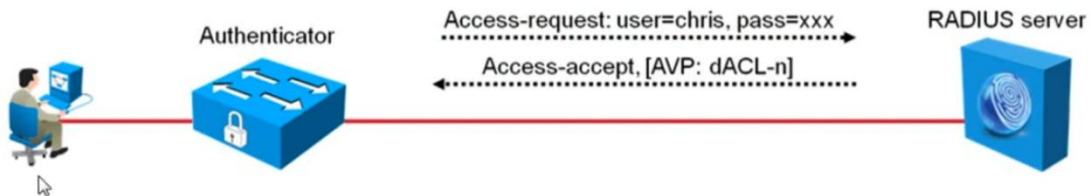
ACL -2

عندما ادخل بشكل صحيح الى شبكة يقوم ال authentication بارسال access list بالصلاحيات التي يمتلكها حيث اقوم بوضع access list لكل يوزر واعطاء صلاحيات بالدخول الى المكان المحدد في نيتورك

802.1X Downloadable ACLs

LEAD THE

- Per-user dACLs provide differentiated network access
- In RADIUS, authentication and authorization occurs in one step:
 - RADIUS server authenticates a user connected to an 802.1X port
 - RADIUS server retrieves the ACL attributes and sends them to the switch
- The switch applies the attributes to the 802.1X port for the duration of the user session.
- The switch removes the per-user ACL configuration when the session is over, if authentication fails, or if a link-down condition occurs



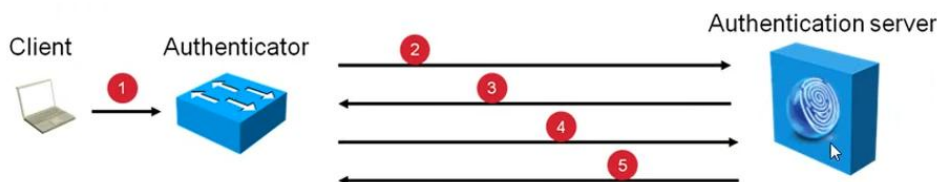
Change of authorization

عندما تتم العملية و يتم auth لأول مره تتم عن طريق السيرفر وهو Cisco ISE وبعدها يقوم Cisco ISE باعطاء تفويض الى السويتش بانه هو من يقوم بادخال اليوزر الى الشبكة بعد الوثوق باليوزر بدلا من الذهاب كل مرة الى Cisco ISE وبذلك يكون ريسورس عالي على شبكة

Change of Authorization

LEAD THE

1. Endpoint connects
2. 802.1X authentication completes successfully
3. Initial authorization policy: allow posture assessment and remediation
4. Posture assessment completes, endpoint is compliant
5. CoA message from ISE to switch, allow context appropriate access



MAC auth bypass

طريقة تستخدم لاعفاء الاجهزة من عمل 802.1x

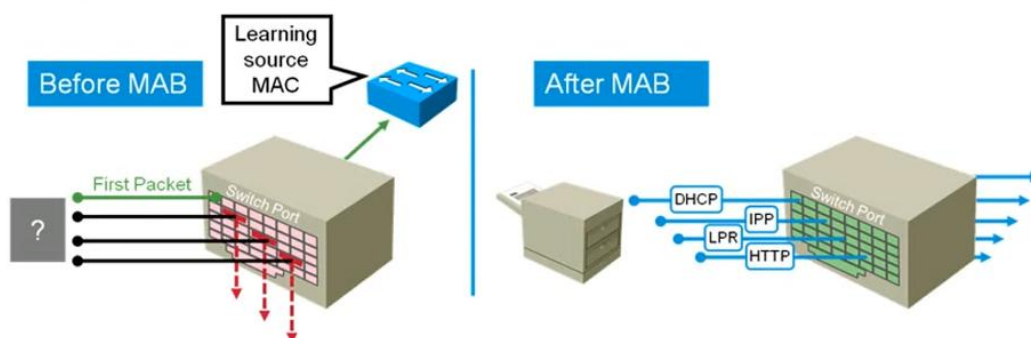
انا قولت للسويتش اي احد يتوصل اليك يجب ان يعطيك يوزرنيم وباسورد

في المثال في الاسفل يوجد printer في هذه الحالة كيف سوف تقوم printer من عمل Authentication في هذه الحالة سوف نعطي mac address للسويتش ونقول له بان هذه الماكات لا تحتاج الى عمل auth خل يعبر مباشرة بدون Authentication

EGYPT NE
LEAD THE

MAC Authentication Bypass

- A method to allow exemptions from 802.1X authentication
- Certain MAC addresses skip the regular authentication process
- MAC address sent in RADIUS Access-Request message
- Exempted MAC addresses defined as endpoints on the server



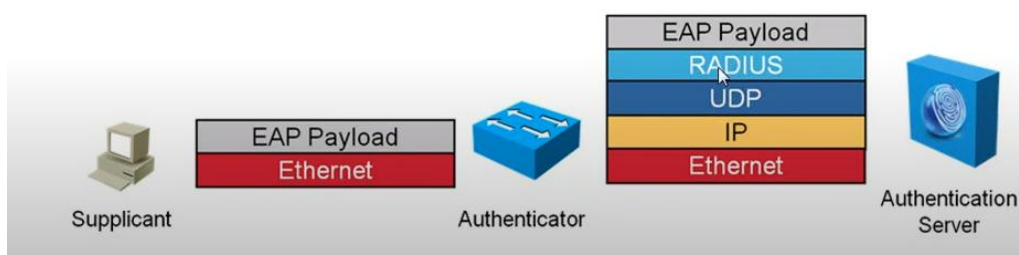
EAP : هو البروتوكول الذي يعمل بين سبلكينت و اوثنكتيتر

radius : هو البروتوكول الذي يعمل بين اوثنكتيتر و اوثنكتيشن هو بروتوكول

EGYPT NE
LEAD TH

Extensible Authentication Protocol

- Authentication exchange direct between the supplicant and the authentication server
- Encapsulation:
 - Between supplicant and authenticator - in the edge LAN protocol (EAPOL: Ethernet, 802.11)
 - Between authenticator and authentication server - inside RADIUS

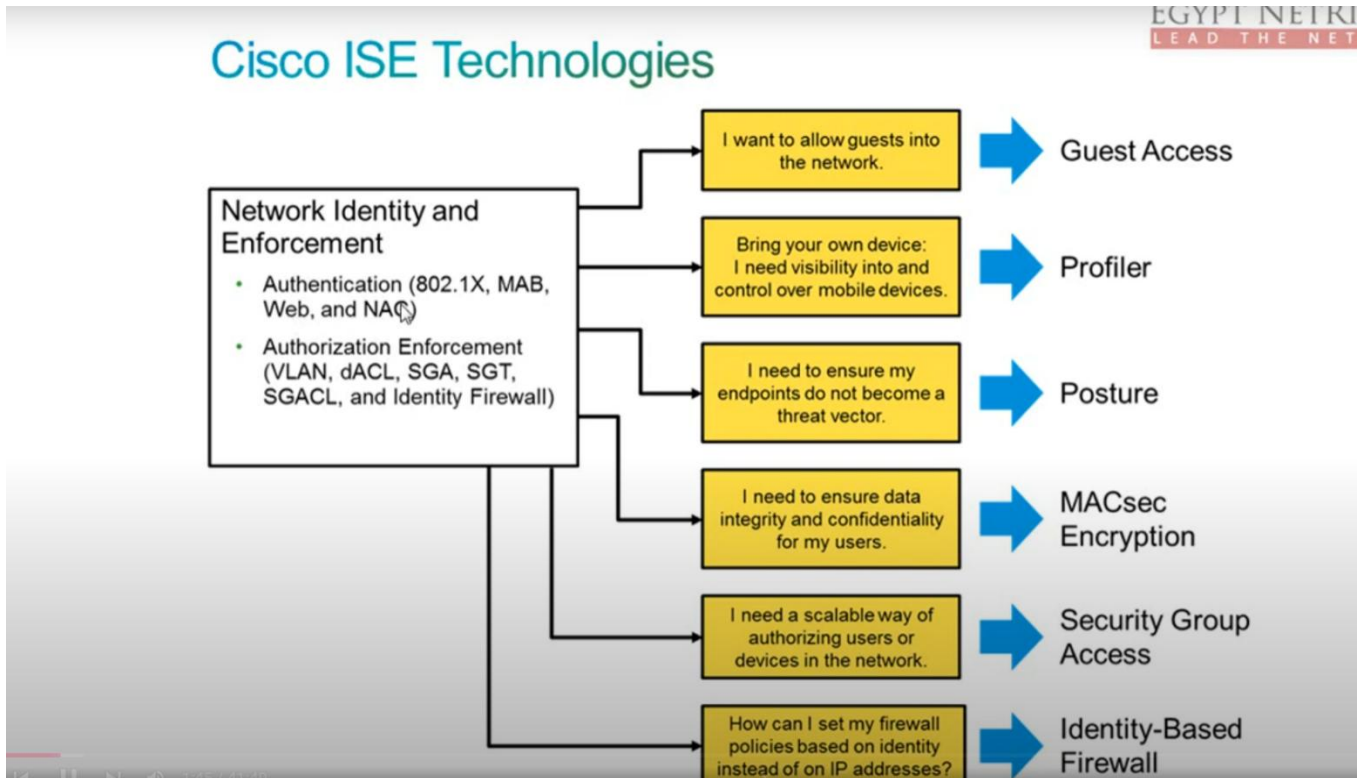


باختصار بروتوكول 802.1x : هو البروتوكول الذي يطلب منك ادخال يوزرنيم وباسورد قبل الدخول الى الشبكة

CoA : هنا يقوم Cisco ISE بتسليم عهده الى السويتش

ما الذي يستطيع Cisco ISE فعله




1. Authentaction and authorization
 2. guest access نعطيهم صلاحيات محددة ولا يدخلون للنيتورك
 3. Profiler معرفة الجهاز الذي دخل للشبكة اذا كان ويندوز 10 او 7 او نظام لينكس او اندرويد او ماك وغيره
 4. Posture التأكد من الجهاز الداخل للشبكة انه محدث وعليه انتيفايروس ولا يوجد عليه ثريت (عمل scan للجهاز)
 5. MACsec Encryption ان يكون للداتا CIA
 6. Security group access عمل كروب لكل قسم في شبكة مثلا hr it
 7. النقطة الاخيرة هي التحكم في البورت الخاصه بالجهاز
- هذه كلها متوفرة في cisco ise



ثلاث persona او ثلاث اوضاع لل Cisco ISE هذه هي الاوضاع :

Cisco ISE Nodes, Personas, and Roles

LEAD THE N

Persona	Description	Symbol
Administration	<ul style="list-style-type: none">Interface for configuring policiesPolicies automatically distributed to other components	
Policy Services	<ul style="list-style-type: none">Engine that makes policy decisionsAttribute retrieval and evaluation	
Monitoring	<ul style="list-style-type: none">Interface for logging and reporting dataReport and alarm generation	

ليس شرطاً عمل الثلاث بيرسونه على Cisco ISE

يمكنني تقسيمها الى اكثر من ماشين مثلاً: 1- بيرسونه الادمن والمونيتور في machine

2- والبوليسي سيرفس في machine واحدة

الفكرة من هذه هي تخفيف الحمل على machine

ISE PKI

EAP : بهذه الحالة يسمى clear EAP بمعنى انه من غير شهادة توثيق

EAP-TLS : عندما يكون عليه شهادة او authentication يكون هذا البروتوكول به TLS

عند سماع TLS يعني وجود شهادة

يتم عمل (certificate Authority) CA عن طريق ويندوز سيرفر

سوف نقوم باصدار شهادتين

شهادة صادرة من ويندوز سيرفر لل Cisco ISE

وشهادة صادرة من Cisco ISE للويندوز سيرفر

بهذه الحالة يكون الاتصال بينهم secure او امن

سوف نقوم بعمل ربط بين active directory و cisco ise ليقوم ال Cisco ISE باخذ الطلب من السبلكينت والتحقق من اليوزر نيم والباسورد عن طريق الاكتف دايركتوري

ملاحظه مهمه : عند ربط اي جهاز بالاكتف دايركتوري يجب ان يكون DNS الجهاز هو ip الخاص بالاكتف دايركتوري ليتم ترجمة domain

الذهاب الى administration وبعدها الى external identity source ونكتب الدومين الخاص بالاكتف دايركتوري

User authentication certificate

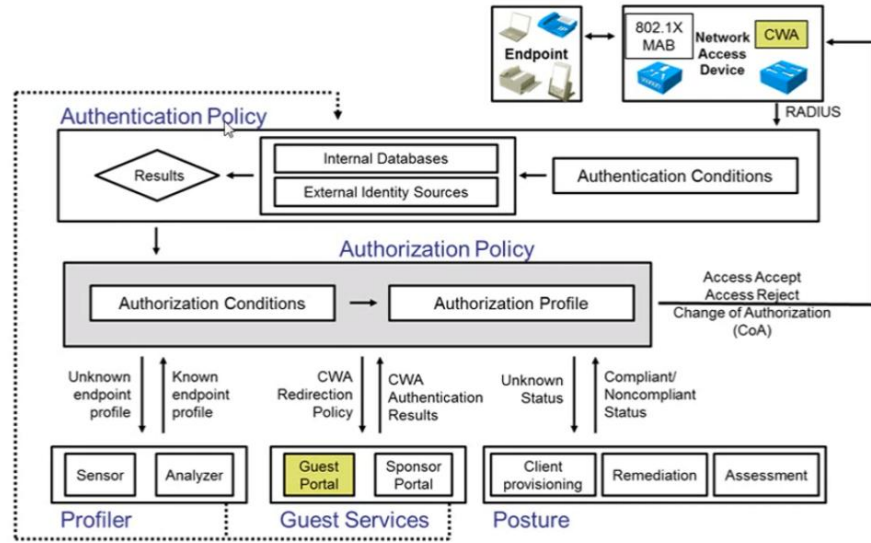
نستطيع ان نعمل authentication لليوزر عن طريق اصدار شهادة له ولل Cisco ISE

ويقوم الويندوز سيرفر بهذه المهمه حيث سوف يقوم باصدار شهاده لهم

Authorization

بعد عمل Authentication نرى ما هي صلاحيات هذا اليوزر الذي دخل الى الشبكة
هنا له صلاحيات للوصول الى كل شي ام له limitation

Authorization in Cisco ISE



Authorization تعتمد على ثلاثة مكونات رئيسية:

1. Authorization Policies :

- تحدد الشروط التي يجب تلبيةها لمنح الوصول.
- تعتمد على عوامل مثل هوية المستخدم، نوع الجهاز، موقعه، أو حالة الجهاز (Compliance Status).

2. Authorization Profiles :

- تحدد الإجراءات التي يجب اتخاذها عند استيفاء الشروط.
- أمثلة:

- السماح بالوصول الكامل.
- تقييد الوصول.
- إعادة التوجيه إلى بوابة ويب (Captive Portal).

يتم تطبيق ال Authorization بناء على الشروط التي تم استيفائها من قبل اليوزر

إعداد Cisco ISE في Authorization :

الخطوة 1: إعداد Authorization Profiles

1. اذهب إلى:

Policy > Policy Elements > Results > Authorization > Authorization Profile

2. اضغط على **Add** لإضافة ملف جديد.
3. قم بتحديد الخيارات التالية:
 1. **Name** : اسم الملف مثل Full Access أو Guest Access
 2. **Access Type** : اختر نوع الوصول (Access-Accept) أو (Access-Reject).
 3. **VLAN** : لتحديد VLAN للجهاز.
 4. **ACL** : لتطبيق قائمة تحكم في الوصول.
 5. **Redirection** : لإعادة التوجيه إلى بوابة معينة مثل بوابة تسجيل BYOD أو Captive Portal

الخطوة 2: إنشاء Authorization Policy

1. اذهب إلى:

Policy > Policy Sets.

2. اختر مجموعة السياسات المراد تعديلها أو اضغط على **Add Policy Set** لإنشاء مجموعة جديدة.
3. في قسم **Authorization Policy**:
 - اضغط على **Add Rule** لإضافة قاعدة جديدة.
 4. حدد الشروط:
 - **Identity Group** : مجموعة المستخدمين أو الأجهزة (مثل موظفين، ضيوف).
 - **Device Type** : نوع الجهاز (مثل هاتف ذكي، حاسوب لوحي).
 - **Location** : الموقع الجغرافي.
 - **Compliance** : حالة الجهاز من حيث الامتثال (متوافق أو غير متوافق).
 5. اختر ملف التفويض المناسب (**Authorization Profile**) لتطبيقه على هذه الشروط الذي فعلناها في الأعلى

أنواع السياسات في Authorization

1. **Full Access**:
 - يتم منح المستخدم أو الجهاز وصولاً كاملاً إلى الشبكة.
2. **Limited Access**:
 - يتم تقييد الوصول إلى موارد معينة.
3. **Guest Access**:
 - يتم منح الضيوف وصولاً محدوداً إلى الإنترنت أو موارد محددة.
4. **Redirect Access**:
 - يتم توجيه المستخدم إلى بوابة ويب مثل بوابة تسجيل BYOD أ
5. **Quarantine Access**:
 - يتم تقييد الوصول للأجهزة التي لم تستوف شروط الأمان أو الامتثال.

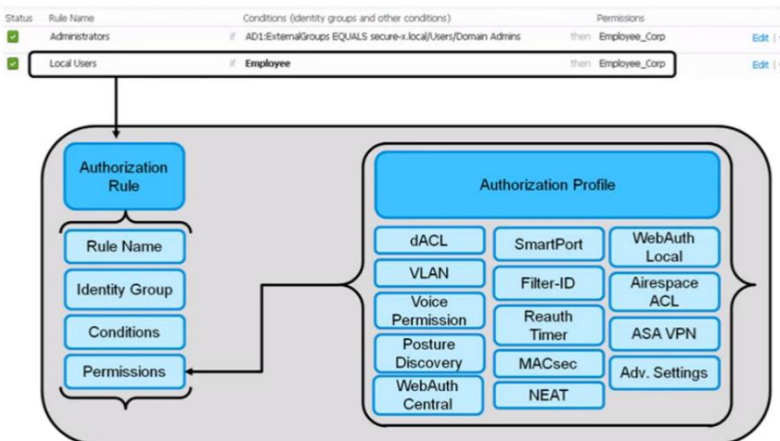
Profiler : اشوف الويندوز اصداره شنو وشنو هي الثغرات الي بي وشنو الحل الي انطي الك ممكن تحديث او تنزيل برنامج معين (يوجد شرح عنه في الاسفل بتفصيل اكثر)

Posture : الجهاز الذي يدخل اليك فقط ويندوز 10 مثلا او ويندوز 11 (يوجد شرح عنه في الاسفل بتفصيل اكثر)

```
Switch(config)#aaa authorization exec default group radius ifa
Switch(config)#aaa authorization exec default group radius if
Switch(config)#aaa authorization exec default group radius if-authenticated
```

بهذا الامر لا يدخل الى authorization الا بعد عمل authentication

Authorization Policy Overview



اعطاء صلاحيات عن طريق ACL

يتم تطبيق authorization على البورت الذي يدخل منه اليوزر

TrustSec

TrustSec : هي تقنية تقوم بإدارة أمان الشبكة بناءً على Security Group Tags (SGTs) بدلاً من الاعتماد على إعدادات VLAN أو ACL التقليدية.

يعتبر فريمورك ليتم تطبيق سكيورتي اكثر على Cisco ISE

ويتكون من :

-1 SGTs (security Group Tag)

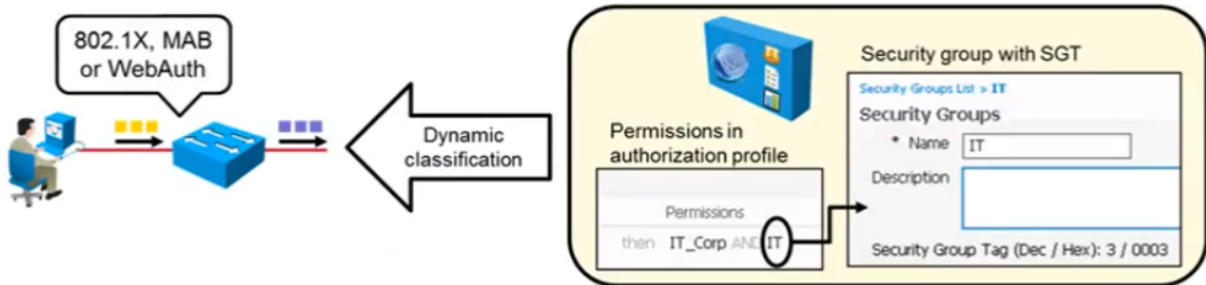
-2 MACsec

طرق عمل Dynamic SGT او static كما موضح بالصور

SGT Classification

LEAD THE

- Dynamic:
 - 802.1X
 - MAC Authentication Bypass
 - Web Authentication
- Static mappings, such as:
 - IP host or subnet to SGT
 - VLAN to SGT



إعدادات TrustSec Authorization في Cisco ISE

1. تفعيل TrustSec:

- اذهب إلى:

Administration > TrustSec > Settings.

- قم بتنفيذ TrustSec وتأكد إعدادات الشبكة.

2. إعدادات Security Groups:

- اذهب إلى:

Policy > Policy Elements > Results > Security Groups.

- أضف Security Groups مثل "Employees" و "Guests".

3. تعيين SGTs عبر السياسات:

- اذهب إلى:

Policy > Policy Sets.

- في Authorization :

○ إذا كان المستخدم ينتمي إلى "Employee AD Group" ، يتم تعيين SGT بقيمة 10.

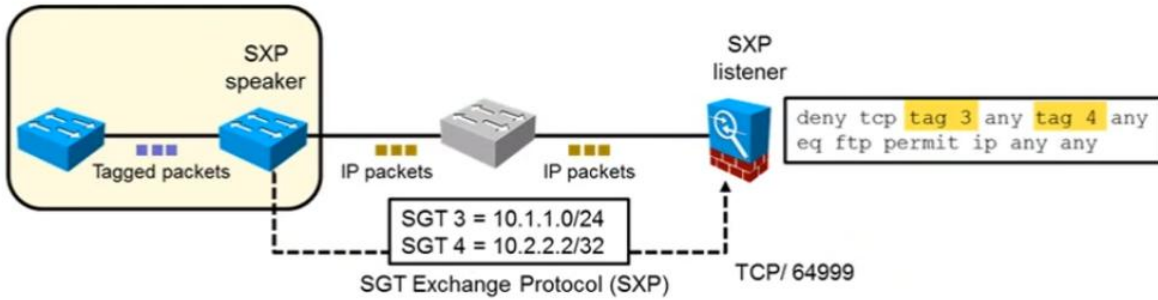
○ إذا كان المستخدم ضيفاً، يتم تعيين SGT بقيمة 20.

4. تطبيق السياسات عبر الشبكة:

- يتم استخدام الأجهزة الداعمة لـ TrustSec مثل سويتشات Cisco وأجهزة التوجيه لتطبيق سياسات الأمان بناءً على SGTs.

SGT Exchange Protocol

- Communicates IP-to-SGT mappings "out of band" of IP packet
- Used to propagate SGT across devices that are not inline capable
- Unidirectional, speaker transmits to listener via TCP/64999
- Configured on a per-peer connection basis



SGT : هو البروتوكول الي ينقل الكلام بين سويتش و Cisco ISE وهو الذي يقوم بنقل صلاحيات يعني ان Cisco ISE هو الذي اكتب بداخله الاكسس لست لكن السويتش هو من يقوم بتنفيذها ليمنع اليوزر من الوصول الى شبكة معينة

نقوم بعمل مثال بمنع employee من الوصول الى الى telnet مثلا :

نقوم بعمل كروب ل source وكروب ل destination عن طريق trustSec الموجودة في work centers وبعدها نطبق Security group tag وهذه البوليسي تمنع اليوزر من عمل telnet على السيرفر مثلا ومسموح بعمل اي شي ثاني ونقوم بعمل بالذهاب الى matrix الموجوده في trustSec

MacSec(802.1AE)

MACsec (Media Access Control Security) • هي تقنية تقوم بتأمين الروابط بين الأجهزة على طبقة الوصلة Layer 2 باستخدام تشفير.
تعمل على منع:

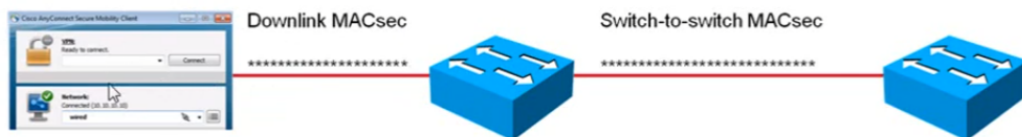
- التنصت على البيانات.
- التلاعب بالبيانات.
- الهجمات من الداخل (Insider Attacks).

فائدته عمل encrypted لل layer 2

MAC Security

LEAD THE

- Layer 2 Encryption (802.1AE)
- Downlink MACsec:
 - Industry Standard Extension to 802.1X
 - Uses MKA
 - Enabled by Cisco AnyConnect supplicant
 - Supports per-device security associations (for example PC and IP phone)
- Switch-to-switch MACsec:
 - NDAC
 - SAP



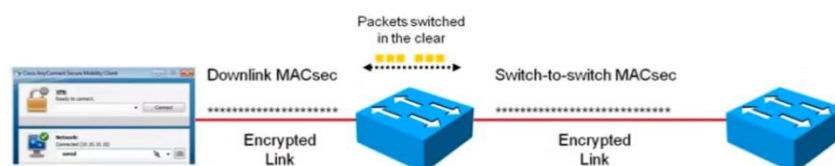
Hop by hop : يعني دائما تكون انكربشن

فائدتها inspection and filter and Qos

MACsec Hop-by-Hop Operation

LEAD THE

- "Bump-in-the-wire" model
 - Packets are encrypted on egress
 - Packets are decrypted on ingress
 - Packets are in the clear across the backplane
- Network can perform all packet processing features:
 - Inspection
 - Filtering
 - QoS



يتم تفعيل macSec عن طريق Cisco ISE عن طريق authorization يوجد شيء اسمه MACSec policy ويكون لها ثلاث خيارات كما موضح بالصورة

▼ Common Tasks

☐ Reauthentication

☒ MACSec Policy

should-secure

must-not-secure

must-secure

should-secure

☐ NEAT

▼ Advanced Attributes Settings

تفعيل خاصية macSec على سويتش كما في الصورة في الأسفل

```
HQ-Sw(config)#  
interface GigabitEthernet0/1  
macsec  
mka default-policy  
authentication linksec policy should-secure
```

ويتم تفعيله على pc عن طريق cisco any connect

WebAuth

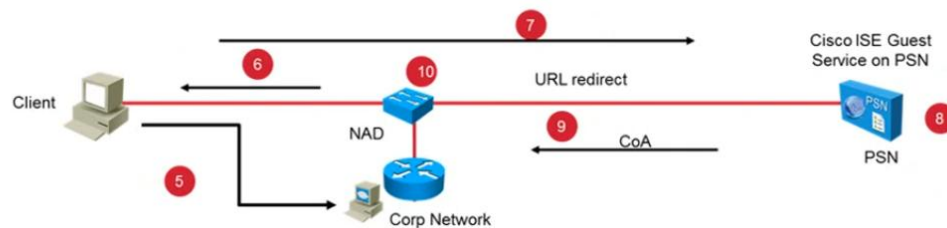
عمل authentication and authorization عن طريق http and https عن طريق صفحة ويب

يستخدم أكثر شي عندما يكون لدي ضيوف في شركة او المؤسسه لانه من غير الممكن ان اضع يوزر وباسورد لكل ضيف على Cisco ISE

واكون مخلي policy تقول ان الي دخلوا من ويب authentication لهم صلاحيات بالوصول الى نيتورك معين او شي معين

Central WebAuth Operation (Cont.)

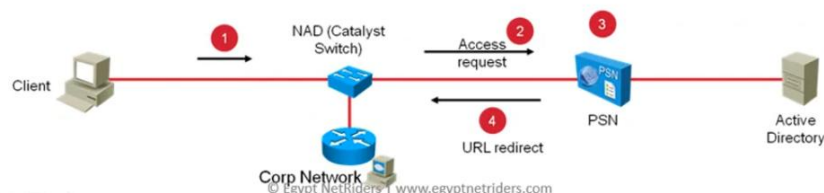
5. User attempts to connect to any URL.
6. NAD redirects client browser.
7. Redirected client browser connects to portal on ISE.
8. ISE authenticates the user.
9. ISE sends a CoA to the NAD.
10. NAD applies new authorization settings.



Central WebAuth Operation

LEAD THE NE

1. Client connects to NAD; may or may not have 802.1X supplicant
2. NAD initiates an access request
 - MAB request (no 802.1X supplicant)
 - Regular user access request (802.1X supplicant)
3. ISE configured to continue operation
 - Upon "MAB failure" or "User not found"
 - To allow the Central WebAuth process to proceed
4. ISE sends access-accept message with URL-redirect to WebAuth service



خطوات عمل webAuth :

- 1- الكلاينت يريد access على نيتورك عن طريق الواير مثلا ويدز الطلب للسويتش
- 2- السويتش يدز طلب للسكو ايس
- 3- ال Cisco ISE يشوفه وحيكون جاهز انو يستقبل url redirect
- 4- اليوزر من بيدي يفتح اي صفحة الطلب حيروح للسويتش
- 5- السويتش حيرد عليه ب صفحة web authentication حتى لكلاينت يدخل يوزر وباسوورد
- 6- السويتش حيدز اليوزر نيم والباسوورد للسكو ايس حتى يتأكد اذا كان يوز وباسوورد صحيحات
- 7- بعدها ال Cisco ISE يدز للسويتش حينطلي الصلاحيات لليوزر الي دخل
- 8- يسوي apply policy



Central WebAuth Configuration Procedure

1. Configure a switch for WebAuth.
2. Configure the MAB to continue when user not found.
3. Tune the WebAuth identity source sequence (situational).
4. Configure Pre-WebAuth dACL.
5. Configure traffic redirect to WebAuth: authorization profile.
6. Configure traffic redirect to WebAuth: authorization policy.
7. Configure authorization policy for clients authenticated via WebAuth.

هذه الصورة شرح شلون نسوي عمل web auth على Cisco ISE

لو اليوزر غير موجود نعمل continue من ال authentication

Guest service

طرق الدخول للنيتورك هي عن طريق 802.1x او MAB والطريقه الثالثه هي webAuth وهي تكون مخصصه للضيوف الذين ياتون الى الشركة وتستخدم احيانا للموظفين الذين لا يستطيعون الدخول عن طريق 802.1x او عن طريق MAB

اول شي افعله هو تهيئه صفحه للجيسيت لكي يقوموا بتسجيل الدخول

Sponsore portal : بوابه يستخدمها موظفين الاستقبال او HR لادارة حسابات الضيوف واعطاءهم صلاحيات مؤقته

وظيفتها

- إنشاء وتعديل وحذف حسابات الضيوف.
- تعيين صلاحيات ومدة الوصول المسموح بها للضيوف.
- إرسال تفاصيل الحساب (مثل اسم المستخدم وكلمة المرور) إلى الضيوف.

*يمكن تخصيصه ليشمل مستويات مختلفة من الصلاحيات لموظفي المؤسسة الذين يديرون عملية تسجيل الضيوف.

Guest Portal : هي الي استخدمها للضيوف حتى يوصلون للشبكة لتسجيل الدخول باستخدام الحساب الي قدمه اله Sponsore portal

وظيفته

- تسجيل الدخول إلى الشبكة.
- يمكن أن يتضمن بعض شروط الاستخدام أو السياسة التي يجب على الضيف الموافقة عليها قبل الوصول.

*يمكن تخصيص واجهة الضيوف لتتوافق مع العلامة التجارية للشركة وتقديم تجربة مميزة للزوار.

الفرق بين Guest Portal و Sponsor Portal

- **Sponsor Portal** مخصص لإدارة حسابات الضيوف من قبل الموظفين المخولين داخل الشركة.
- **Guest Portal** مخصص لاستخدام الضيوف الفعليين الذين يريدون الوصول إلى الشبكة بناءً على الصلاحيات الممنوحة لهم من خلال Sponsor Portal

اي جهاز Cisco ISE يعمل ك standalone فهو admin Portal

Posture

هي ميزة يقدمه Cisco ISE للتأكد من ان الجهاز الداخل الي الشبكة يطبق السياسات الخاصه بالشركة مثلاً

- النظام محدث باخر تحديث
- لديك انتي فايروس
- لديك فايروول

NAC agent : برنامج يتم تثبيته على ال endpoint يقوم بالتحقق ان هذا الكمبيوتر يلبي سياسات الامان لدى المؤسسه قبل منحه الوصول الكامل للشبكة

Posture Policy : هنا يتم وضع القواعد من كل نواحي ويتم الدخول في العمق يعني معرفة نوع واصدار نظام التشغيل مثلاً :

- وجود برنامج مكافحة الفيروسات وتشغيله.
- تحديثات النظام وبرامج الحماية.
- إعدادات الفايروول

مثال : يقوم موظف بالدخول الى الشبكة عن طريق Windows xp هذا غير ممكن لان هذه النسخه بها الكثير من الثغرات وتمثل خطر على شبكة

المعالجة:(Remediation)

- إذا كان الجهاز لا يتوافق مع سياسات الأمان، يمكن للـ **NAC Agent** مساعدة المستخدم في تصحيح المشكلة من خلال إرشادات واضحة.
- مثال: إذا كان برنامج مكافحة الفيروسات غير محدث، يوجه البرنامج المستخدم لتحديثه.

Remediation Actions.

- تحديث برنامج مكافحة الفيروسات.
- تثبيت تحديثات النظام.
- تمكين إعدادات الأمان مثل الفايروول.

Client Provisioning : تنزيل اخر التحديثات واخر الحاجات الي نزلت الخاصه بسكويرتي على Cisco ISE

حتى عندما يقوم الكلاينت بالدخول اسوي scan او مقارنه بين الانتي فايروس الي عندي والي موجود على Cisco ISE ولازم يكون عندي حتى اطبق سياسات الشبكة او المؤسسه

مثلا : Cisco ISE يكول لازم عندي انتي فايروس avira لمن يسوي سكان على على اليوز الي دخل للشبكة راح يلكه عنده مثلا Kaspersky هنا Cisco ISE راح ينطي alert رابط يلكه نزل avira

Autorization Plocy

يحدد ما إذا كان الجهاز **Compliant** (متوافق) أو **Non-Compliant** غير متوافق

- بناءً على النتيجة، يتم منح الجهاز مستوى الوصول المناسب إلى الشبكة.
- اما اذا كان Unknown يعني اول مره يدخل الى شبكة نقوم بتوجيهه الى Client provisioning portal ويقوم بتنزيل NAC agent وبعدها يحدد اذا كان **Compliant** (متوافق) أو **Non-Compliant**

سيناريو عملي:

1. يتصل جهاز جديد بالشبكة لأول مرة.
2. يتم اكتشاف أن الجهاز لا يمتلك برنامج AnyConnect.
3. يتم إعادة توجيه الجهاز إلى بوابة التوفير.
4. يقوم المستخدم بتنزيل وتثبيت AnyConnect Posture Module.
5. يتم إعادة تقييم الجهاز من قبل ISE.
6. إذا كان الجهاز متوافقاً، يُمنح وصولاً كاملاً للشبكة.

- وجود برنامج مكافحة الفيروسات مع تمكينه وتحديثه.
- تمكين الفايرول.
- تثبيت آخر التحديثات الأمنية لنظام التشغيل.

EGYPT NE
LEAD THE

Cisco ISE Posture Service Overview

- Functionality to determine the security status of the endpoints
- Leverages NAC agents

Configuration area	Function
Client provisioning	Automates NAC agent installation and updates
Posture policy	Defines the "health" requirements of endpoints
Authorization policy	Considers the posture status: <ul style="list-style-type: none">• If unknown, redirect to client provisioning portal• If compliant, grant controlled access• If noncompliant, enforce appropriate security policy

Profiler

تكلما سابقا عن Posture والان هذه الخاصية هي تكملة لل Posture

Profiler : هي خاصية تحديد نوع الجهاز ومن اي شركة تم صنعه وتصنيفها اذا كانت كاميرات مراقبة او طابعات او كمبيوتر او هاتف

ويتم تحديد نوع الشركة المصنعه بناء على MAC الجهاز

مثل Dell or HP or Apple or Lenovo

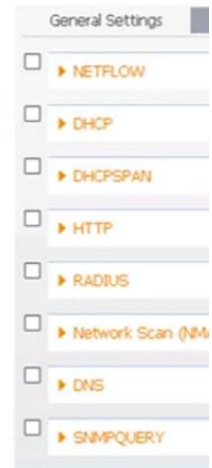
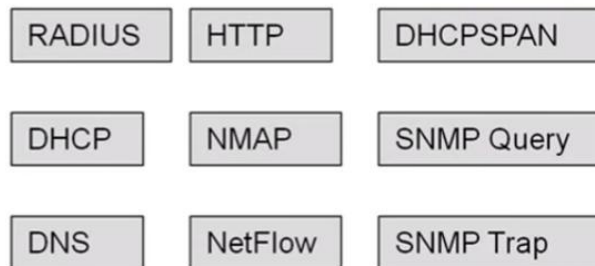
مثلا تكون جميع اجهزة مؤسسه معينه هي Lenovo عندما ارى ان جهاز HP دخل الى الشبكة يعني ان هذا الجهاز يجب ان لا يدخل

اعطاء صلاحيات عن طريق نوع الجهاز : مثلا ان جهاز هواوي وسامسونج له صلاحيات معينه جهاز ابل له صلاحيات معينه جهاز ويندوز له صلاحيات معينه وهكذا

كيفية عمل profiler : يعمل عن طريق هؤلاء البروتوكولات

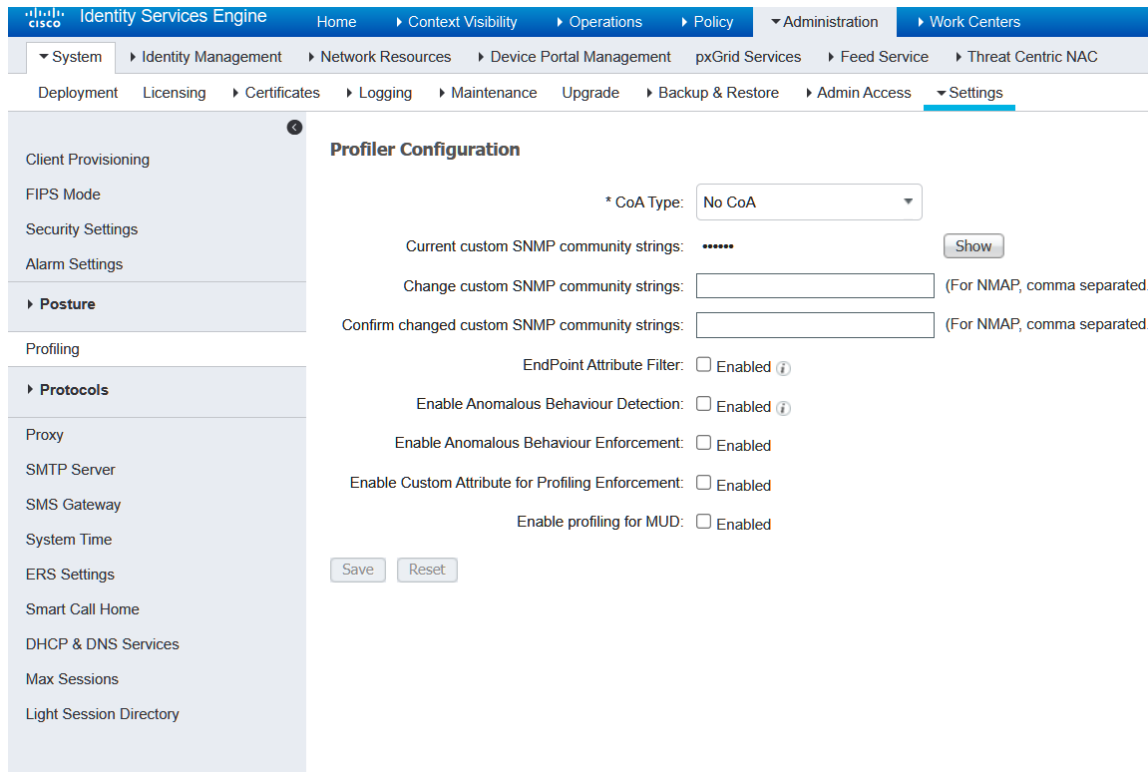
Cisco ISE Probes

- All probes are disabled by default
- Enabled individually to meet profiling requirements
- Probes are enabled on policy service nodes



Probes : هي التي تستخدم لتحديد نوع الاجهزة في profiler وتستخدم ايضا في عمل كروب لكل نوع واعطاءه صلاحيات مختلفة

مثلا اجهزة ابل تكون في كروب مختلف عن اجهزة اندرويد وتكون لكل كروب صلاحيات مختلفة



تفعيل Coa type وانوعه

1. Reauthenticate:

- يُجبر الجهاز على إعادة المصادقة (Reauthentication) مع خادم RADIUS.
- تُستخدم عندما يحتاج ISE إلى التحقق مرة أخرى من بيانات الاعتماد أو تحديث السياسات استنادًا إلى تصنيف جديد للجهاز.

2. Port Bounce:

- يقوم بإعادة تشغيل منفذ الشبكة (Interface) الذي يتصل به الجهاز.
- تُستخدم عندما تحتاج إلى إعادة تعيين الاتصال بشكل كامل.
- قد يكون مفيدًا لتحديث VLANs أو تطبيق سياسات جديدة عند تغيير نوع الجهاز.

من هذه القائمة التي في الاسفل ننتبه ان لا نعمل checked على nmap لانها تستهلك بروتوكول عالي

BYOD (bring your own device)

هي تقنية او سياسته يستطيع الموظفون من خلالها استخدام اجهزتهم الشخصية مثل الهواتف والكمبيوتر للوصول الى شبكة المؤسسة مع توفير الامان لهذه الاجهزة

• يوجد كورس خاص من سيسكو لل BYOD فقط

*يفضل عمل VLAN مخصصه لاجهزة BYOD لضمان عزل هذه الاجهزة عن البيانات والموارد الحساسه

Single and Dual SSID Design

- Single SSID:
 - Provisioning and network access on a single SSID
 - Uses secured SSID
 - Does not work for guests
 - Less common
- Dual SSID:
 - Separates provisioning and network access
 - Similar to traditional approach:
 - Protected SSID for employees
 - Open SSID for guests
 - Uses open SSID for provisioning
 - Works for guests and employees
 - More common

حينما يأتي ضيوف الى شركة ونريد ربطهم wireless يوجد طريقتين لتوصيل الاجهزة

Single SSID BYOD -1

يتم استخدام ssid واحده للشبكة بمعنى اسم واحد

- Ssid : هي اسم الشبكة التي تبحث عنها طريق الهاتف من الواي فاي

لا انصح باستخدامها

Dual SSID BYOD -2

في اكسس بوينت الخاص ب سسكو توجد خاصية ان تقوم بعمل اكثر من ssid في نفس الاكسس بوينت

واعطي لكل ssid صلاحيات وفيتشر مختلفه عن ssid الثاني

هي الافضل والتي انصح باستخدامها