Universitat Oberta de Catalunya

uoc.edu

NAC com a solució de Seguretat dels IoTs

Nom Estudiant: Oscar Cardiel Gelabert
Pla d'estudis de l'estudiant: Màster Universitari en Ciberseguretat i Privadesa
Àrea de treball final: Seguretat empresarial

Nom Consultor/a: Amadeu Albós Raya
Nom Professor/a responsable de l'assignatura: Cristina Romero Tris

28/12/2021

FITXA DEL TREBALL FINAL

Títol del treball:	*NAC com a solució de seguretat dels IoTs*
Nom de l'autor:	*Oscar Cardiel Gelabert*
Nom del consultor/a:	*Amadeu Albós Raya*
Nom del PRA:	*Cristina Romero Tris*
Data de lliurament (mm/aaaa):	*28/12/2021*
Titulació o programa:	Màster Universitari en Ciberseguretat i Privadesa
Àrea del Treball Final:	Seguretat empresarial
Idioma del treball:	*Català*
Paraules clau	*NAC, IoT, Protecció*

Resum del Treball (màxim 250 paraules): *Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball*

La finalitat d'aquest treball ha estat la de analitzar si els sistemes de control d'accés a les xarxes de dades d'última generació (NAC) són una solució als riscos de seguretat que presenten els dispositius IoTs per les organitzacions empresarials.

Per dur a terme aquest estudi, en primer lloc s'han analitzat els riscos i vulnerabilitats que presenten els dispositius IoTs. Després, s'han estudiat els ciberatacs més comuns que pateixen els dispositius IoTs. S'han presentant els sistemes de control d'accés a les xarxes de dades (NAC) com una possible solució per protegir els dispositius IoTs, i s'ha estudiat la manera com els sistemes NAC identifiquen i protegeixen els dispositius IoTs.

Paral·lelament a l'estudi realitzat, s'ha dut a terme una recerca de quins són els principals fabricants de les solucions de control d'accés a les xarxes de dades a nivell Europeu, i s'ha finalitat l'estudi amb la realització d'una prova de concepte per tal de valorar l'efectivitat de la solució i contrastar-la amb la part teòrica estudiada.

Finalment, les conclusions obtingudes han estat que els sistemes de control d'accés a les xarxes de dades ofereixen una bona solució pel al descobriment i el control d'accés dels dispositius IoTs, així com també una molt bona solució per la protecció dels atacs dels tipus de suplantació d'identitat dels IoTs. Tanmateix, les integracions del NAC amb productes de tercers per tal d'aconseguir la protecció post autenticació dels dispositius tenen encara molt recorregut per fer.

Abstract (in English, 250 words or less):

The purpose of this Master's Thesis has been to analyse whether the latest generation data network access control systems (NACs) are a solution to the risks and security issues exposed by the IoTs devices for companies.

In order to carry out this study, firstly I have analysed the risks and vulnerabilities presented by IoTs devices. Afterwards I have looked at the most common cyberattacks suffered by these devices. Then, data network access control systems (NACs) have been presented as a possible solution to protect IoTs devices and how data network access control system works and they identify the IoTs devices.

At the same time, a market study has been carried out to find out which are the main manufacturers offering these solutions in the European market. Furthermore, a concept test has been carried out to validate the effectiveness of the operation of these safety solutions.

Finally, I can conclude that data network access control systems provide a good solution for the discovery and control of IoTs devices, as well as very good protection from attempts to supplant identity. However, NAC's integrations with third-party products to achieve post-authentication protection still have much to do.

Índex

Llista de taules

1 Introducció

1.1 Context i justificació del Treball

Cada cop les organitzacions estan més conscienciades pel que fa a la seguretat de la informació, i malgrat que no totes implementen un Sistema de Gestió de la Seguretat de la Informació (SGSI), si que apliquen alguns principis i segueixen la seva metodologia per tal aconseguir millores significatives en les seves polítiques de gestió de la seguretat, procediments i directrius, amb l'objectiu de protegir la informació i garantir la seva disponibilitat, confidencialitat, integritat, autenticitat i traçabilitat.

Dins els anàlisis de riscos que es realitzen sobre les infraestructures de xarxes privada d'una organització, un dels principals mals de caps i preocupacions dels responsables de la seguretat de la informació recau sobre els dispositius IoTs connectats en la infraestructura de xarxa privada empresarial.

En la actualitat, els dispositius IoTs estan totalment integrats dins les xarxes corporatives privades, aportant capacitats noves i innovadores a les organitzacions. Tanmateix, s'ha de tenir present que els dispositius IoTs estan dissenyats des d'un punt de vista funcional, i la majoria d'aquests dispositius no estan dotats de mecanismes de seguretat adequats, ni els fabricants ofereixen la possibilitat de resoldre vulnerabilitats mitjançant revisions i actualitzacions de software freqüents per mitigar-les.

Aquestes mancances de recursos de seguretat en els dispositius IoTs fa que les solucions tradicionals de control d'accés a les xarxes de dades, les quals utilitzen implementacions basades en 802.1x, no siguin una solució valida per aquest entorn, quedant els dispositius IoTs sense identificar, i convertint-se en un punt feble dins de la seguretat corporativa, i un dels principals vectors d'atac per explotar per part dels ciberdelinqüents.

Per un altre costat, cada cop hi ha mes dispositius IoTs connectats en l'ombra dins de les xarxes empresarials. Moltes vegades els dispositius IoTs van i venen en les xarxes corporatives portats per diferents departaments i personal de l'organització, i no es consideren part del departament de TI, evitant-se, d'aquesta manera, els controls típics de seguretat imposats per TI, i exposant la seguretat de tota la companyia sense que els responsable de la mateixa en tinguin constància.

Sobre aquesta problemàtica exposada, el present TFM pretén estudiar quines solucions tècniques es poden aplicar en les xarxes de dades de les organitzacions, per tal d'identificar i controlar l'accés dels diferents dispositius IoT que s'hi connecten, i mitigar el risc de seguretat global que suposa per les organitzacions el seu descontrol.

1.2 Objectius del Treball

L'objectiu global d'aquest TFM és la de conèixer i avaluar la efectivitat real que ofereixen les solucions actuals de control d'accés a les xarxes de dades sobre els dispositius IoTs.

1.2.1 Objectius Específics

- Estudi i investigació dels diferents mètodes utilitzats en les solucions actuals de control d'accés a les xarxes de dades pel que fa al descobriment, identificació i autorització de dispositius connectats a les xarxes, focalitzant l'estudi en les tècniques i solucions aplicades sobre els dispositius que els manquen mecanismes propis de seguretat, com són els dispositius IoTs.

- Anàlisis dels principals fabricants del mercat de solucions de control d'accés a xarxes, amb l'objectiu de conèixer quina cobertura ofereixen sobre les solucions i tècniques estudiades anteriorment pel que fa al descobriment i control d'accés dels dispositius IoTs. Analitzar també, quins trets diferenciadors pot tenir cada solució en front la seva competència.

- Disseny i realització d'una prova de concepte d'una de les solucions de control d'accés estudiades anteriorment, amb l'objectiu d'avaluar-ne la seva efectivitat real pel que fa a la descoberta, identificació i protecció dels dispositius IoTs d'una organització.

1.2.2 Objectius Personals

- Aprofundir en els coneixements tècnics, teòrics i pràctics, sobre les solucions de seguretat i de control d'accés a les xarxes privades de dades, en concret sobre la protecció dels dispositiu IoTs corporatius.

- Conèixer les dificultats i dependències tècniques a baix nivell de la implementació i la integració d'una solució de control d'accés dins d'un eco sistema de Ciberseguretat empresarial.

- Culminar els estudis del Màster Universitari en Ciberseguretat i Privadesa.

1.3 Enfocament i Mètode Seguit

Per tal de donar resposta als diferents objectius descrits en l'apartat anterior, la memòria del TFM es divideix en **tres blocs diferenciats**.

- **Un primer bloc teòric, orientat a la recerca i investigació** sobre la problemàtica presentada, on es pretén entendre les debilitats i riscos en seguretat que presenten els dispositius IoT i validar, d'aquesta manera, les preocupacions que motiven l'estudi d'aquest TFM. Seguidament, i també en aquest primer bloc, es pretén estudiar quins mètodes s'apliquen en la actualitat per a protegir els dispositius i IoTs, així com quines solucions tecnològiques hi ha en el mercat orientades a la seguretat de les organitzacions empresarials.

- **Un segon bloc pràctic i de disseny**, on es pretén realitzar una prova de concepte d'alguna de les solucions per a dispositius IoTs estudiades en el primer bloc i destinades a les organitzacions empresarials. D'aquesta manera es pretén contrastar les solucions i els mètodes de protecció per a dispositius IoTs estudiats en la teòrica amb les solucions tecnològiques que ofereixen els principals fabricants en el mercat.

- **Un tercer i últim bloc de valoracions i conclusions finals** sobre el nivell de protecció dels dispositius IoTs , on es pretén reportar els resultats obtinguts de la part d'estudi i investigació realitzats en el primer bloc en front els resultat obtinguts de la part més pràctica realitzada en el segon bloc.

1.4 Planificació del Treball

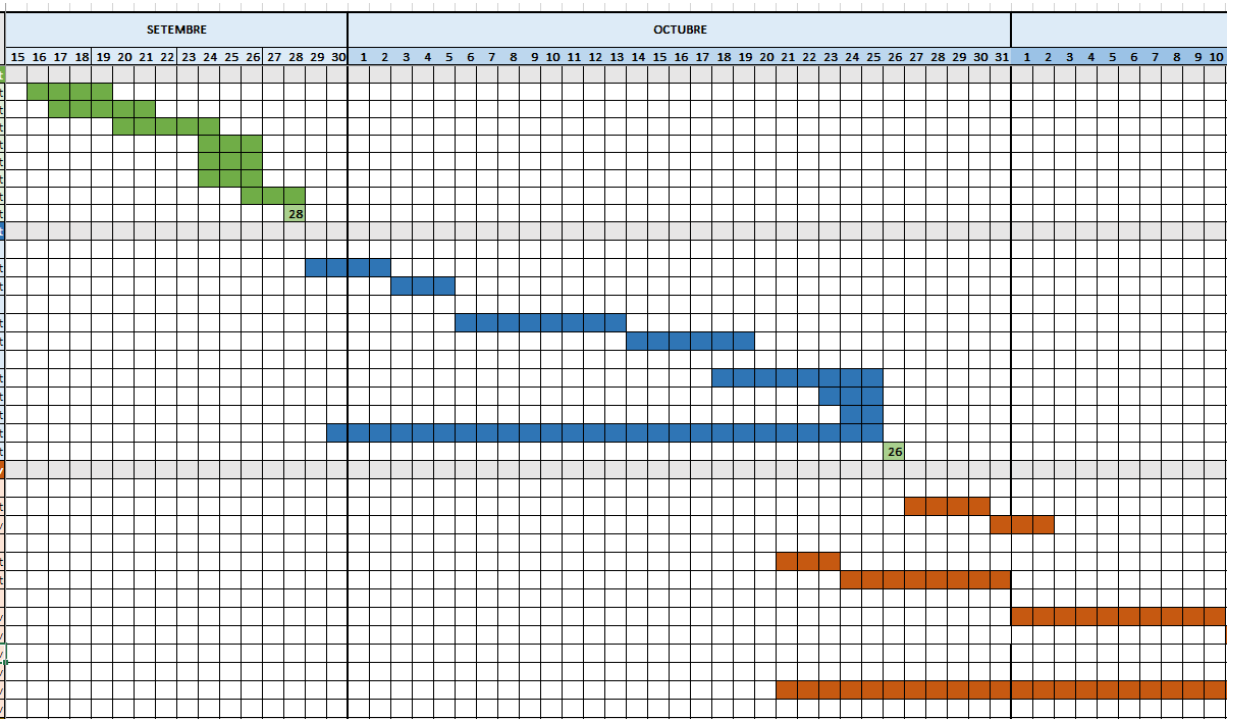
A continuació es mostra la taula de planificació per portar a terme el treball.

Cod	Activitat	Inici	Fi	
1	**Planificació**	**15-set**	**28-set**	
1.1	Definició del context i justificació del treball	16-set	19-set	4
1.2	Definició d'objectius	17-set	21-set	5
1.3	Definició de la metodologia.	20-set	24-set	5
1.4	Elaboració de la planificació	24-set	26-set	3
1.4.1	Definició de les tasques	24-set	26-set	3
1.4.2	Càlcul dels temps d'entrega	24-set	26-set	3
1.5	Redacció de l'estat d'art	26-set	28-set	3
1.6	Entrega del pla de treball - PAC1	28-set	28-set	1
2	**Recerca, estudi i investigació**	**29-set**	**26-oct**	
2.1	Estudi de la seguretat dels dispositius IoTs			
2.1.1	Debilitats en seguretats dels dispositius IoTs.	29-set	2-oct	4
2.1.2	Atacs mes comuns des del dispositius IoTs.	3-oct	5-oct	3
2.2	Estudi i investigació dels mètodes d'autenticació			
2.2.1	Mètodes d'autenticació per a usuaris i els seus dispositius	6-oct	13-oct	8
2.2.2	Mètodes d'autenticació per a dispositius IoT corporatius	14-oct	20-oct	6
2.3	Estudi de mercat de les solucions NAC			
2.3.1	Solucions de seguretat per les debilitats estudiades	18-oct	25-oct	8
2.3.2	Comparativa solucions entre fabricants punters	23-oct	25-oct	3
2.4	Justificació del fabricant escollit per la prova concepte	24-oct	25-oct	2
2.5	Redacció PEC2	30-set	25-oct	26
2.6	Entrega desenvolupament PEC2	26-oct	26-oct	1
3	**Prova de concepte**	**27-oct**	**23-nov**	
3.1	Disseny casos d'ús.			
3.1.1	Disseny autenticacions	27-oct	30-oct	4
3.1.2	Disseny de les polítiques de seguretat	31-oct	3-nov	3
3.2	Preparació de l'entorn per la prova de concepte			
3.2.1	Instal·lació de l'entorn virtual de la solució de NAC	21-oct	23-oct	3
3.2.2	Instal·lació de la resta dispositius de xarxa a utilitzar	24-oct	31-oct	8
3.3	Configuracions			
3.3.1	Configuracions del casos d'ús	1-nov	10-nov	10
3.2.2	Configuracions de les integracions.	11-nov	16-nov	6
3.4	Proves i validacions	19-nov	21-nov	3
3.5	Conclusions	19-nov	21-nov	3
3.6	Redacció PEC3	21-oct	22-nov	33
3.7	Entrega desenvolupament PEC2	23-nov	23-nov	1

4	**Presentació i defensa del TFM**	**24-nov**	**28-des**	
4.1	Configuracions pendents de la prova de concepte	24-nov	11-des	18
4.2	proves i validacions	27-nov	11-des	15
4.3	Revisió del document memòria del TFM	6-des	21-des	16
4.4	Redacció de les últimes modificacions del document memòria del TFM.	6-des	27-des	22
4.5	Entrega memòria TFM	28-des	28-des	1
5	**Presentació del vídeo del TFM**	**29-des**	**4-gen**	
5.1	Edició del vídeo	28-des	3-gen	6
5.2	Entrega del vídeo	4-gen	4-gen	1
5	**Defensa del TFM**	**29-des**	**4-gen**	
5.1	Sessió de defensa del TFM			1

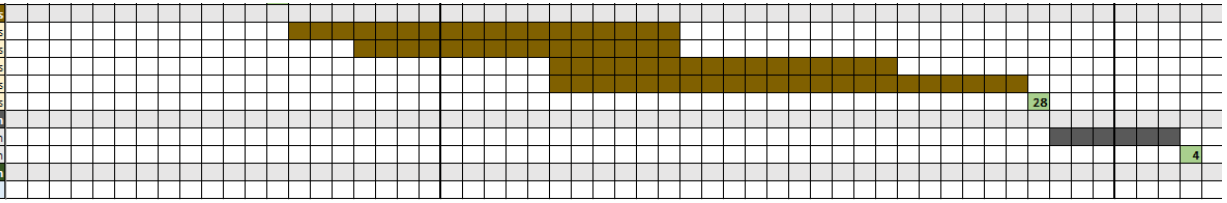
Taula 1: Planificació

	FASE/TASCA	DATA INICI	DATA FI
1	**Planifi+C5:C42cació**	**15-set**	**28-set**
1.1	Definició del context i justificació del treball	16-set	19-set
1.2	Definició d'objectius	17-set	21-set
1.3	Definició de la metodologia.	20-set	24-set
1.4	Elaboració de la planificació	24-set	26-set
1.4.1	Definició de les tasques	24-set	26-set
1.4.2	Càlcul dels temps d'entrega	24-set	26-set
1.5	Redacció de l'estat d'art	26-set	28-set
1.6	Entrega del pla de treball - PAC1	28-set	28-set
2	**Recerca, estudi i investigació**	**29-set**	**26-oct**
2.1	Estudi de la seguretat dels dispositius IoTs		
2.1.1	Debilitats en seguretats dels dispositius IoTs.	29-set	2-oct
2.1.2	Atacs mes comuns des del dispositius IoTs.	3-oct	5-oct
2.2	Estudi i investigació dels mètodes d'autenticació		
2.2.1	Mètodes d'autenticació per a usuaris i els seus dispositius	6-oct	13-oct
2.2.2	Mètodes d'autenticació per a dispositius IoT corporatius	14-oct	20-oct
2.3	Estudi de mercat de les solucions NAC		
2.3.1	Solucions de seguretat per les debilitats estudiades	18-oct	25-oct
2.3.2	Comparativa solucions entre fabricants punters	18-oct	25-oct
2.4	Justificació del fabricant escollit per la prova concepte	23-oct	25-oct
2.5	Redacció PEC2	30-set	25-oct
2.6	Entrega desenvolupament PEC2	26-oct	26-oct
3	**Prova de concepte**	**27-oct**	**23-nov**
3.1	Disseny casos d'ús.		
3.1.1	Disseny autenticacions	27-oct	30-oct
3.1.2	Disseny de les polítiques de seguretat	31-oct	3-nov
3.2	Preparació de l'entorn per la prova de concepte		
3.2.1	Instal·lació de l'entorn virtual de la solució de NAC	21-oct	23-oct
3.2.2	Instal·lació de la resta dispositius de xarxa a utilitzar	24-oct	31-oct
3.3	Configuracions		
3.3.1	Configuracions del casos d'ús	1-nov	10-nov
3.2.2	Configuracions de les integracions.	11-nov	16-nov
3.4	Proves i validacions	19-nov	21-nov
3.5	Conclusions	19-nov	21-nov
3.6	Redacció PEC3	21-oct	22-nov
3.7	Entrega desenvolupament PEC2	23-nov	23-nov



Taula 2: Diagrama Gantt de la Panificació de Setembre a Octubre

4	**Presentació i defensa del TFM**	**24-nov**	**28-des**
4.1	Configuracions Pendents de la Prova de Concepte	24-nov	11-des
4.2	Proves i Validacions	27-nov	11-des
4.3	Revisió del Document Memòria del TFM	6-des	21-des
4.4	Redacció Últimes Modificacions Document Memoria TFM.	6-des	27-des
4.5	Entrega Memòria TFM	28-des	28-des
5	**PRESENTACIÓ VIDEO DEL TFM**	**29-des**	**4-gen**
5.1	Edició del Vídeo	28-des	3-gen
5.2	Entrega del Vídeo	4-gen	4-gen
5	**DEFENSA DEL TFM**	**29-des**	**4-gen**
5.1	**Sessió Defensa del TFM**		



Taula 3: Diagrama de Gantt de la Planificació de Novembre a Gener

1.5 Estat de l'Art

Les tecnologies i solucions de control d'accés a les xarxes privades de dades intenten protegir i controlar l'accés de tots aquells dispositius que s'hi connecten. De fet, el neguit pels mètodes de controls d'accés a les xarxes de dades a format part del món del networking des de gairebé els inicis de l'Ethernet i, com succeeix en la majoria de les solucions tecnològiques, s'ha vist forçada a evolucionar per tal d'adaptar-se als requeriments de seguretat dels moments.

Sobre els principis de la dècada dels 2000, la gran majoria d'organitzacions confiaven en la seguretat i protecció que els podia oferir la autenticació del sistema operatius Windows, i es tenia aquest mètode com el mètode principal i segur per a controlar qui es connectava a la xarxa de dades.

L'aparició dels primers virus informàtics va portar la necessitat de controlar, no només l'autenticació sobre els sistema operatiu que s'utilitzava fins el moment, sinó també l'accés de la connexió física a la xarxa i als serveis que aquestes oferien. En conseqüència, va sorgir la solució de la limitació de l'accés dels dispositius a les xarxes mitjançant llistes d'adreces MAC permeses en els ports dels commutadors, combinat amb la configuració, també en els commutadors, de llistes d'accés cap als diferents serveis i recursos de la xarxa que s'oferien..

La dificultat de la gestió i manteniment d'aquesta solució de control d'accés esmentada, la debilitat de la protecció que oferia l'autenticació MAC, i l'emergent tendència per la implementació de les xarxes sense fils en les organitzacions, anys 2007 a 2010, va fer evolucionar el control d'accés cap a la utilització de protocols segurs d'autenticació com és l'estàndard 802.1x. És just en aquest moment quan la tecnologia de control d'accés a les xarxes de dades agafa identitat pròpia, i és coneguda arreu com a NAC, Network Access Control. Una de les solucions estrella de l'època va ser el que oferia el fabricant Cisco System conegut com a Access Control Server (ACS).

La evolució cap a la segona generació de la tecnologia NAC, entre els anys 2010 i 2015, va venir donada per la necessitat de gestionar i protegir l'accés dels diferents rols d'usuaris existents dins les organitzacions, sobretot, per tal de controlar l'accés dels rols d'usuaris col·laboradors i convidats, on els departaments d'IT de les organitzacions no tenien control sobre els dispositius que aquests usuaris utilitzaven, ni dels diferents softwares que hi tenien instal·lats.

Així doncs, la segona generació de NAC permetia controlar de manera dinàmicament, i segons el rol i tipus d'autenticació utilitzat per l'usuari, a quin segment de la xarxa quedaria ubicat i, en conseqüència, a quins recursos corporatius podria accedir. Per exemple, una solució de control d'accés típica en desplegaments de NAC de segona generació és la d'autenticar els usuaris corporatius mitjançant el mètode d'autenticació 802.1x i assignant dinàmicament els segments de xarxa on pertany cada usuari corporatiu. Pel que fa als usuaris no corporatius, se'ls identifica amb un protocol d'accés menys segurs, aquest pot ser per exemple un portal captiu, i se'ls assigna

dinàmicament un accés a internet fora de banda de la xarxa corporativa, o se'ls limita l'accés als diferents recursos corporatius mitjançant llistes d'accés dinàmiques.

Dins d'aquesta segona generació de NAC, i a partir dels anys 2015 cap a 2018, l'expansió de l'ús de la tecnologia mòbil i tauletes en les organitzacions, normalment dispositius no corporatius i personals dels diferents rols d'usuaris corporatius, obliga a evolucionar de nou el NAC cap a solucions de control d'accés del tipus BYODs, on els usuaris se'ls permet, per exemple, a accedir a certs recursos corporatius, o simplement se'ls dona accés a internet, prèviament registrant el dispositiu en la plataforma NAC per tal d'identificar-lo i controlar-ne el seu accés.

A partir del 2018 es dispara la incorporació i l'ús dels diferents tipus de dispositius IoTs en les organitzacions. Aquests dispositius, per les seves característiques físiques i de disseny, els manquen recursos i sistemes propis de seguretat i també per interactuar amb el sistemes de control d'accés. Conseqüentment, es disparen els d'atacs informàtics contra les organitzacions, on els ciberdelinqüents s'aprofiten de les debilitats i vulnerabilitats que els dispositius IoTs presenten per tal d'accedir a les xarxes privades amb diferents intencionalitats delictives. Es en aquest moment quan apareix la tercera generació del NAC.

En aquesta tercera generació del NAC s'introdueix la identificació de dispositius mitjançant les tècniques de perfilat, el que es coneix com a Profiling. Aquesta tècnica pretén donar solució a la identificació d'aquell dispositius, tipus IoTs, que no disposen de sistemes d'autenticació i protecció propis. Al mateix temps, s'incorpora també la funcionalitat d'auditoria, el que es coneix com a Posture, dels equips d'usuari mitjançant la instal·lació d'agents fixes o solubles, els quals determinen la salut dels dispositius, auditant si aquests disposen de les aplicacions de seguretats mínimes requerides per les organitzacions en les seves polítiques de seguretat, com poden ser, per exemple, el fet de disposar d'un antivirus instal·lat, el servei de tallafocs activat, unes actualitzacions dels sistemes operatius mínims, etc.

També és en les solucions de control d'accés de tercera generació on s'incorpora la integració del NAC amb d'altres solucions de seguretat de l'ecosistema corporatius, com són, per exemple, els dispositius IPS, tallafocs, MDMs, antivirus, així com sistemes de gestió centralitzada d'incidents, com sistemes SIEM, per tal aïllar de manera rapida i a través del NAC, els dispositius compromesos, o fins i tot, descontentant-los de la xarxa en el moment que és detecta un atacs sobre la infraestructura, dotant, d'aquesta manera, de mes visibilitat, control i seguretat de tots els dispositius connectats a la xarxa corporativa.

La nova tendència cap el teletreball, la qual s'han accelerat degut a la pandèmia del COVID-19, juntament amb la conscienciació, cada cop més generalitzada i acceptada per les empreses, de que cal aportar gestos importants per aturar el canvi climàtic, com és reduir el desplaçament dels usuaris cap els llocs de feina. La imparable integració en les organitzacions de

dispositius IoTs per infinitat de serveis i aplicacions. La diversitat de serveis en producció ubicats tan en CPDs corporatius locals o en el *Cloud*, així com el augment, també imparable, d'atacs contra organitzacions i usuaris per part dels ciberdelinqüents, esta tornant a requerir nous canvis en les solucions de control d'accés a les xarxes privades que poden evocar en la quarta generació del NAC.

La tendència de la nova generació de les solucions de controls d'accés van cap a una confiança zero, *Zero-Trust Network Acces (ZTN)*, de qualsevol dispositiu que es connecti a la xarxa privada de dades, ja sigui de forma remota o local. Cal tractar tots els dispositiu i usuaris, indiferentment de la ubicació on siguin, com amenaces potencials que poden comprometre la xarxa corporativa i, per tant, s'ha de poder identificar, autenticar i ser monitoritzat en tot moment.

S'ha vist que la identitat de l'usuari és fonamental per desenvolupar una política eficaç de control d'accés, la qual ha d'anar basada en rols d'usuari i, d'aquesta manera, assignar les mínimes polítiques d'accés cap els recursos i aplicacions necessàries per la seva funció i feina, amb un seguiment i inspecció constant de les transaccions i l'ús, i no controlar només l'accés a xarxa com fins ara.

Les empreses necessiten solucions que els donin visibilitat d'on es troba cada dispositiu, que fa i com es connecta a d'altres dispositius a través de la xarxa, ja que la maca de visibilitat, deixa una organització vulnerable als riscos invisibles.

Una veritable solució de control d'accés de confiança Zero, obligaria a tot moment a identificar, segmentar i supervisar contínuament tots els dispositius, amb la qual cosa les organitzacions podrien garantir que els seus recursos intern es mantenen segur, que les dades, les aplicacions i la propietat intel·lectual es mantenen protegits i que les operacions de xarxa i seguretat es simplifiquen en general.

1.6 Productes Finals

A continuació es detallen els productes finals que s'espera obtenir en la finalització del TFM.

- Estudi dels diferents riscos i amenaces conegudes al que estan exposats els dispositius IoTs.

- Estudi de les diferents tècniques existents en la actualitat pel descobriment, identificació i control d'accés dels diferents dispositius IoTs connectats a les xarxes empresarials.

- Comparativa de les diferents solucions de control d'accés a les xarxes de dades dels principals fabricats del mercat.

- Avaluació d'una de les solucions de control d'accés a les xarxes de dades d'última generació focalitzat a l'entorn dels dispositius IoTs.

1.7 Breu descripció dels capítols de la memòria.

En el primer capítol s'introdueix la problemàtica de seguretat dels dispositius IoTs i es justifica la motivació del seu estudi. Es marquen els objectius que es desitgen assolir durant la realització del TFM, es mostra una planificació de treball, i s'exposen els productes finals que se n'esperen obtenir al finalitzar.

En el segon capítol s'analitza en detall la problemàtica de seguretat de l'estudi que ens ocupa. Es justifiquen els motius per els quals els dispositius IoTs presenten uns riscos de seguretat tan elevats i s'analitzen les diferents vulnerabilitats, amenaces i atacs més freqüents als quals estan sotmesos en la actualitat.

En el tercer capítol es presenten els sistemes de control d'accés a les xarxes de dades d'última generació com a part d'una solució global dins l'ecosistema de seguretat d'una organització per tal de protegir-se dels diferents riscos de seguretat que presenten els dispositius IoTs.

En el quart capítol s'exposen els diferents mètodes utilitzats en la actualitat per descobrir i identificar els diferents dispositius IoTs connectat en una xarxa corporativa.

En el cinquè capítol es realitza un estudi de mercat de les diferents solucions de control d'accés a les xarxes de dades que presenten els principals fabricants a dia d'avui, amb la finalitat de corroborar en quina mesura aquestes solucions cobreixen la problemàtica de seguretat dels dispositius IoTs exposada.

En el sisè capítol es realitza el disseny i prova de concepte sobre una de les solucions estudiades de control d'accés a les xarxes de dades, per tal de validar la correspondència de la solució teòrica estudiada sobre la part pràctica.

En el setè i últim capítol s'exposen les diferents conclusions a les quals s'han arribat després dels estudis, anàlisis i proves pràctiques realitzades durant la execució del TFM.

2 Anàlisis de la problemàtica.

En aquest apartat s'estudia en detall la necessitat de disposar d'alguna tipus d'eina i solució per tal de descobrir i identificar tots els dispositius connectats en una xarxa de dades, i s'analitza en profunditat la problemàtica exposada sobre els riscos de seguretat que plantegen els dispositius IoTs.

2.1 La problemàtica del control dels dispositius

La innovació digital és fonamentals pel creixement empresarial i això inclou, per exemple, noves infraestructures de xarxa locals i/o al núvol, la introducció de dispositius mòbils, dispositius d'internet de les coses, dispositius tradicionals PCs de sobre taula, portàtil, servidors... on tots generen un volum fluxos de treball molt grans els quals els responsables de la seguretat de les organitzacions han de protegir per tal que els usuaris puguin realitzar la seva feina sense comprometre cap actiu corporatiu i, paral·lelament, complir amb les regulacions corporatives actuals i les diferents polítiques de seguretat de control d'accés i protecció de dades com, per exemple, el RGPD, entre d'altres.

Per tal protegir els actius corporatius dels diferents tipus de ciberatacs als que estan exposats, els responsables de la seguretat de les xarxes privades necessiten dotar-se d'un ecosistema sistema de seguretat on, d'entre d'altres dispositius, disposin d'eines que els facilitin la tasca d'identificar cada un dels dispositius i usuaris que es connecten a la xarxa corporativa, i d'aquesta manera, acotar l'accés als recursos que aquests poden accedir, minimitzant l'àrea de risc d'atac exposada per a cada dispositiu/usuari.

Existeixen en la actualitat diversos mètodes i mecanismes d'autenticació, la majoria estandarditzats en diferents protocols, per exemple l'EAP, que poden ser aplicats i configurats en la gran majoria de dispositius corporatius i empresarials que utilitzen normalment els usuaris d'una organització. Una vegada els usuaris i/o dispositius han estat identificats i autenticats, se'l pot limitar l'accés als diferents recursos de la xarxa corporativa, segons uns criteris i les polítiques de seguretat preestablertes per la companyia, mitjançant pel que es coneix com a un sistema de control d'accés a la xarxa de dades o NAC.

Tanmateix, i dins de les xarxes corporatives, conviuen una gran diversitat de dispositius on no tots disposen de recursos propis destinats a la seva seguretat, i molt menys encara, destinats a identificar-se enfront solucions corporatives encarregades del control d'accés a les xarxes de dades.

Així doncs, podem classificar els dispositius que es connecten en una xarxa de dades en dos grans grups, els dispositius amb capacitat d'identificar-se, i el que no disposen d'aquesta capacitat.

- Els dispositius amb capacitat d'identificar-se són aquells dispositius que suporten diversos mètodes i protocols d'autenticacions, com per exemple, EAP-TLS, EAP, PEAP, entre d'altres. Dins d'aquest grup podem trobar PCs d'usuaris, impressores d'última generació, alguns models de telèfons IP, punts d'accés a la xarxa sense fils, tauletes, telèfons mòbils etc.

- Els dispositius que no suporten cap mètode d'autenticació, com per exemple, alguns models impressores, sensors de controls de presència, maquinaria de *vending*, càmeres de vídeo seguretat, diversos dispositius departamentals propis, dispositius personals d'empleats, etc. i que es solen conèixer com a dispositius IoTs.

Són aquest últim grup nombrós de dispositius, els quals avui dia proliferen de manera molt ràpida dins de les organitzacions, els que realment preocupen als responsables de seguretat ja que, en infinitat d'ocasions, el departament d'IT no té constància ni visibilitat de l'existència d'aquests dispositius connectats a la xarxa de dades corporativa, per tant no es prenen cap tipus de mesura de seguretat, quedant exposada tota la seguretat de l'organització.

2.2 Característiques generals dels dispositius IoTs

Per entendre la problemàtica que presenten els dispositius IoTs, és important conèixer primer les característiques generals que presenten aquests tipus de dispositius, i que els fa diferents a la resta.

Els dispositius IoTs són microordinadors amb processadors i sensors per un ús molt específic. Pel que fa al software, alguns dispositius IoTs disposen de firmware i d'altres de sistemes operatius amb aplicacions amb propòsit i funcionalitats molt específiques.

La principal característica dels dispositius IoTs és que són de mida petita, disposen de sensors integrats per la realització de les tasques específiques per les quals estan dissenyats, i necessiten estar connectats a una plataforma o servidors, on integren les dades rebudes de cada un d'aquests dispositius, i on s'apliquen els diferents anàlisis per compartir la informació i abordar necessitats específiques.

Per tant, són quatre les principals característiques que defineixen els dispositius IoT.

- **Dimensions**. Dispositius molt optimitzats a nivell de dimensions, amb els mínims components per garantir-ne el funcionament i per tan, de mida petita.

- **Sensibilitat**. Disposen de sensors per tal que puguin detectar els paràmetres pels quals estan dissenyats.

- **Connectivitat**. Han de poder connectar-se a la xarxa per interrelacionar-se amb usuaris o d'altres dispositius o sistemes. Principalment fan servir connexions WI-FI, Bluetooth o Ethernet.

- **Interacció**. Els dispositius fan servir una interfície i sistema de comunicació que permet establir la relació necessària entre les persones, els dispositius i el món físic

Com es pot veure per l'exposició de les característiques que defineixen aquests dispositius IoTs, estan tan orientats al seu ús i en optimitzar recursos i dimensions físiques, que la majoria dels fabricants no tenen en compte un dels principals requeriments de les organitzacions avui en dia, la seva pròpia seguretat com a dispositiu, la seguretat de l'ecosistema on estan connectats, i la seguretat de les dades que recopilen, processen i transmeten per la xarxa.

2.3 Vulnerabilitats dels dispositius IoTs

A continuació, i per tal d'entendre millor les vulnerabilitats dels dispositius IoTs i com d'insegurs són, es presenta un estudi i anàlisis de les principals vulnerabilitats detectades en aquest tipus de dispositius. Bona part d'aquestes vulnerabilitats es troben publicades en el web d'INCIBE-CERTS (2019).

- **Seguretat física inadequada.** Un dels principal problemes de la seguretat en els ecosistemes IoT és que els seus components es distribueixen en l'espai o, moltes cops, s'instal·len en ubicacions públiques o insegures. Això permet als atacants tindre accés als dispositius i controlar-los localment, o fer-los servir per accedir a la resta de dispositius d'una xarxa. Per exemple, un atacant pot copiar la configuració (la IP de xarxa, l'adreça MAC..) i suplantar el dispositiu IoT per escoltar o afectar el rendiment de la xarxa.

- **Configuracions predeterminades insegures.** Molts dispositius IoTs surten al mercat amb configuracions predeterminades insegures o, bàsicament, no els és possible configurar funcionalitats destinades a la seguretat de si mateixos o de les dates que recopilen.

- **La incapacitat de controlar el dispositiu.** Els dispositius IoT solen ser una caixa negre. No se'ls implementa la capacitat de monitorització del treball que realitzen. No permeten identificar quins serveis s'estan executant i amb quins interactuen. Per un altre costat, no tots els fabricants ofereixen als usuaris dels dispositius un control total sobre el sistema operatiu i les aplicacions en execució, no permeten verificar la integritat i la legitimitat del software descarregat, ni instal·lar actualitzacions en el sistema operatiu.

- **Ús de paraules de pas a gestió inexistents, dèbils i emmagatzemades en els mateixos dispositius.** És una de les vulnerabilitats més importants dels dispositius IoTs. Hi ha una gran

quantitat de dispositius IoTs que no disposen de protecció per accedir a la seva gestió i, en cas de tenir-ne, utilitzen paraules de pas que poden ser obtingudes de manera senzilla mitjançant atacs de força bruta o cercant-les per les webs publiques d'internet dels mateixos fabricants. Al mateix temps, aquestes paraules de pas normalment sol ser la mateixa per un sol model o per tota la línia de productes. Això, i el fet que molts dispositius tenen exposats els ports de Telnet o SSH, facilitat i molt, la seva intrusió.

- **Serveis de xarxa insegurs.** Els dispositius IoTs es caracteritzaren per oferir múltiples opcions d'accessibilitat. els quals posen al descobert serveis de xarxa insegurs que s'executen en segon pla i que, en la gran majoria de les vegades, estan exposats a internet. Això, conjuntament amb la facilitat de la utilització d'escàners de descobriment de serveis i ports oberts de dispositius connectats a internet, fa que els dispositius IoTs siguin molt vulnerables al seu descobriment i a l'explotació de les vulnerabilitats associades.

- **Ecosistemes d'interfícies insegures**. Aquesta vulnerabilitat fa referència als problemes de seguretat de les eines externes dels dispositius IoTs com són, per exemple, les interfícies web, serveis en el núvols o APIs, els quals poden estar configurats de manera insegura i fan siguin susceptibles a ser compromesos.

- **Falta de mecanismes d'actualització segurs**. La impossibilitat d'actualitzar el dispositiu en si ja és tota una debilitat. Si no s'instal·la, ni hi ha possibilitat d'instal·lar cap actualització, els dispositius queden vulnerables de manera indefinida. Al mateix temps però, si el dispositiu IoT permet la actualització del seu software, la actualització en si i el firmware també poden ser insegur. Per exemple, el fet de no fer servir canals encriptats per rebre el software, si l'arxiu d'actualització no està encriptat o no es verifica la seva integritat abans de ser instal·lat, no hi ha protecció de tornada enrere a una versió mes vulnerable o no hi ha notificacions sobre canvis de seguretat degut a actualitzacions.

- **Ús de components poc segurs o inadequats**. Un component vulnerable és suficient per tal saltar-se tota la seguretat configurada. Això inclou utilitzar components o biblioteques de software obsoletes i insegures que poden comprometre els dispositius IoTs. També inclou la configuració de les plataformes dels sistemes operatius i l'ús de components de software o hardware de tercers d'una cadena de subministrament compromesa.

- **Transferència i emmagatzemant de dades insegurs.** Els dispositius IoTs recopilen i emmagatzemen dades ambientals, inclosa informació personal diversa. Una paraula de pas compromesa es pot substituir, però les dades robades, per exemple, d'un dispositiu biomètric

(empremta digital, retina, biometria facial) no. al mateix temps, els dispositius IoTs no només poden emmagatzemar dades sense xifrar, sinó també transferir-los per la xarxa. Els dispositius IoTs solen estar mancats de xifrats i control d'accés a dades confidencials en qualsevol part de l'ecosistema, això inclou l'emmagatzemat, la transmissió i el processament.

- **Protecció de la privacitat inadequada**. Totes les dades personals s'han d'emmagatzemar i transmetre de manera segura. Tanmateix, aquesta vulnerabilitat considera la privacitat en un sentit més profund i des del punt de vista de la protecció dels secrets de privacitat. Els dispositius IoTs recopilen informació sobre què i qui els envolta, això inclou també a persones les quals no en són conscients que se'ls està recopilant informació. Les dades d'usuaris robades o processades incorrectament podrien desacreditar voluntàriament o involuntàriament a una persona fent-les servir, per exemple, com a xantatge. Per tant, aquesta informació emmagatzemada en un dispositiu o ecosistema es podria utilitzar de forma insegura, inadequada o sense permís.

Com es pot apreciar, les vulnerabilitats que presenten de manera generalitzada els dispositius IoTs són molt importants i de gran consideració.

En l'apartat d'Annexos, punt 10.1 Llistat vulnerabilitats dispositius IoTs, s'ha inclòs una ampliació detallada amb el conjunt i la descripció de les vulnerabilitats detectades segons els diferents fronts per on els ciberdelinqüents podent aconseguir fer-se amb la infraestructura IoT, o amb les dades que aquests dispositius recopilen.

2.4 Amenaces i atacs a dispositius IoTs

Les motivacions que mouen a atacar i comprometre els dispositius IoTs poden ser diverses, des de simple entreteniment, aconseguir informació confidencial emmagatzemada en el dispositiu, com a punt d'entrada per atacar d'altres equips, reconfigurar-los per inhabilitar-los o canviar les seves condicions d'utilització, fins a utilitzar les seves característiques de comunicació i computació per tal d'utilitzar-los com a Botnet dins d'un sistema zombi i atacar objectius específic mitjançant la tècnica d'atac que es coneix com atacs de denegació de servei distribuïts (DDoS).

A continuació s'analitza amb mes detall les diferents amenaces i tipus d'atacs que poden patir els dispositius IoTs.

- **Suplantació d'identitat o Spoofing**. Són atacs especialment més freqüents i rellevants en l'entorn de les organitzacions i en la industria. En aquests casos, el ciberdelinqüents busquen fer-se passar per un dispositiu IoT i, d'aquesta manera, guanyar accés a la xarxa privada normalment amb diferents objectius que poden anar des d'alterar el

funcionament d'operacions, robar informació confidencials, fins el d'espionatge.

- **Botnet. Denegació de servei o DDoS**. Segurament aquest sigui l'amenaça i tipus d'atac mes generalitzat cap els dispositius IoT. Els ciberdelinqüents intentaran convertir el dispositiu IoT en un equip zombi per tal entri a formar part d'una xarxa de dispositius Botnets controlats per operadors a través de Command-and-Control-Servers (C&C Sever). Tots els dispositius zombis tenen dos característiques en comú, tenen accés a internet, i poden transferir dades automàticament a través d'una xarxa. L'objectiu final d'aquest atac és enviar milers de sol·licituds des de diferents dispositius zombi a un mateix objectius final per tal de bloquejar-lo.

- **Bloqueig i encriptació de dades**. Els ransomware han estat un dels tipus de programari mes maliciós dels últims temps. D'entrada, els ransomware no eliminen els fitxers o dades sensibles, sinó que bloqueja l'accés a aquests mitjançant el xifratge. Es en aquest moment que el ciberdelinqüent exigeix un rescat per la clau de desxifrat que desbloqueja els fitxers. Els dispositius IoTs poden ser una porta d'entrada per aquests tipus d'atacs o, directament, patir-los en el cas de ser IoTs dels quals se'l pugui aplicar aquesta tècnica d'atac i disposin de dades sensibles per les quals poder-ne demanar un rescat.

- **Manipulació d'integritat de les dades dels IoTs**. Els dispositius IoTs es caracteritzen per processar, emmagatzemar i transmetre una gran quantitat d'informació. Moltes vegades aquests dispositius envien dades recollides al núvol, sense cap xifratge. Com a resultat, un ciberdelinqüent podria accedir a un dispositiu IoT, controlar-lo i alterar les dades que recopila amb les conseqüències que això podria comportar.

- **Criptomineria amb IoT Bots**. La fabricació de criptomoneda exigeix recursos colossals de CPU i GPU. Els ciberdelinqüents han trobats en els dispositius IoTs la possibilitat de crear xarxes de IoTs infectats, bots, amb l'objectiu de no crear danys, sinó d'utilitzar els seu recursos per la criptomineria. La criptomoneda de codi obert anomenada Monero, és una de les primeres que s'explota mitjançant dispositius IoT infectats, per exemple, utilitzant càmeres de vídeo accessibles des d'internet. Tot i que una càmera de vídeo per si sola no té recursos suficients per explotar criptomonedes, si en té tot un exèrcit.

2.5 Cronologia dels atacs a dispositius IoTs

Es important conèixer la cronologia de les diferents etapes dels atacs dirigits cap els dispositius IoTs per tal de poder-los protegir correctament.

A continuació, es descriu cronològicament el cicle de vida d'un atac dirigit cap a dispositius IoTs segons publica el fabricant de solucions de seguretat, Palo Alto Networks (5 de març de 2020) The 8 Statges of the Iot Attack Lifecycle.Palo

Alto Networks: https://www.paloaltonetworks.com/resources/infographics/the-8-stages-of-the-iot-attack-lifecycle

- **Accés inicial.** Mitjançant eines d'escaneig de ports, els atacs escanegen la xarxa, internet o privada, a la recerca de dispositius vulnerables amb ports oberts. Amb les eines d'escaneig l'atacant arriba a conèixer la IP del dispositiu i la vulnerabilitat.

- **Execució**. Una vegada descoberta la vulnerabilitat del dispositiu, el següent pas és executar un payload o instrucció cap el dispositiu vulnerable mitjançant un exploit o a través de tècniques de força bruta. L'objectiu es aconseguir que es descarregui un arxiu maliciós en el IoT y executar-lo.

- **Persistència**. Una de les funcions del malware executat sol ser la crear accessos redundants al dispositiu IoT per tal de garantir l'accés de l'atacant en tot moment, com pot ser el fet de deixar el Shell obert, crear nous comptes d'usuaris en el cas que l'IoT permeti crear-los, etc.

- **Evasió.** S'apliquen diferents tècniques d'evasió per tal evitar la detecció de l'atac, per exemple, eliminar els registres de les instruccions realitzades del sistema i historial d'instruccions, ocultar i emmascarar l'arxiu malware utilitzat, desinstal·lar les eines de supervisió del dispositiu IoT, etc.

- **Recol·lecció d'informació**. Tota la informació emmagatzemada en el dispositiu es recol·lectada. Això pot incloure arxius sensibles i claus privades.

- **Command & Control**. El malware introduït pot continuar llençant diferents atacs, com poden ser inundacions TCP o UDP, la infiltració de dispositius addicionals en funció de diferents instruccions rebudes del servidor C&C. Els canals de C&C més comuns solen ser mitjançant els protocols HTTP, IRC, P2P entre d'altres.

- **Moviment lateral**. Després de comprometre un primer dispositiu, l'atacant utilitzarà tècniques de moviment lateral per tal d'accedir a d'altres dispositius de la xarxa. Per exemple, si un dispositiu enrutador perimetral ha estat compromès, l'atacant intentarà infectar i accedir a tots els dispositius IoTs connectat en aquest enrutador.

- **Impacte**. Les diferents activitats malicioses llençades des del dispositiu infectat poden tenir múltiples impactes en el dispositiu i a la xarxa de dades on pertany, per exemple, encriptació de les dades mitjançant un ransom, esborrat de les dades del disc, la utilització dels recursos del dispositiu IoT per la fabricació de criptomoneda, o el control del dispositiu com a bonet.

2.6 Exemple de casos reals d'atacs

Hi ha infinitat d'exemples i casos d'atacs a dispositiu IoTs coneguts que es podrien citar i ser objecte d'estiu. Tanmateix, per citar-ne algun de mediàtic, l'any 2018, els hackers van aconseguir infiltrar-se en un centre d'investigació i desenvolupament de la NASA, Califòrnia, i van robar uns 500 MB de dades relacionades amb la missió a Mart.

En la anàlisis i auditories per esbrinar com s'havia portat a terme l'atac, es va descobrir que el punt d'entrada utilitzat pels hackers va ser una Raspberry Pi connectada a la xarxa. També es van trobar en el centre d'investigació diferents dispositius IoTs connectades a la xarxa de dades i que eren totalment desconeguts pels personal IT. (24 de juny 2019) Raspberry Pi used to steal data from Nasa lab. BBC: https://www.bbc.com/news/technology-48743043

També podem trobar casos de ciberatacs més actuals i sonats en el nostre territori, portats a terme a finals del 2021, com han estat els atacs a la Universitat Autònoma de Barcelona, el de l'empresa de Serveis Municipals de Barcelona, el de l'empresa DAMM o, també, el de l'empresa MediaMarkt. En tots aquests últim casos no s'ha fet públic de moment si l'origen del ransomware i entrada de l'atac ha estat via un dispositiu IoT, però les primeres investigacions no ho descarten. Elisabet Escriche (11 de novembre 2021) Un atac informàtic obliga Damm a aturar la producció de cervesa. Diari ARA. https://www.ara.cat/economia/atac-informatic-obliga-damm-aturar-produccio-cervesa_1_4178698.html. Diego Pastor Sánchez (19 de novembre 2021) Los Servicios de Barcelona Serveis Municipals, en jaque por un ataque informático. La Vanguardia: https://www.lavanguardia.com/local/20211019/7799950/ataque-informatico-afecta-servicios-barcelona-serveis-municipals.html

2.7 Conclusions.

Després de l'estudi realitzat sobre les principals característiques dels dispositius IoTs, de la anàlisis de les vulnerabilitats i riscos de seguretat que aquests dispositius presenten, queda palès que cal prendre mesures de protecció i control sobre aquests dispositius.

Així doncs, cal dotar-se d'alguna solució tecnològiques i de seguretat que permetin el descobriment d'aquests dispositius dins d'una xarxa de dades, identificant-los i delimitant-los només a l'accés als recursos necessaris pel seu bon funcionament i servei que ofereixen.

3 Sistemes de control d'accés a la xarxa

En aquest apartat es presenten els coneguts sistemes de control d'accés a les xarxes de dades (NAC) com també l'actual solució de control d'accés pels dispositius IoTs desplegats en les xarxes de dades corporatives.

3.1 La necessitat d'un sistema de control d'accés

Com s'ha estudiat en l'apartat anterior, el fet que un dispositiu es connecti en un punt d'accés d'una xarxa de dades de manera no controlada i autoritzada, com pot ser la connexió de dispositius IoTs per part d'empleats d'una companyia sense informar-ne al departament d'IT, pot provocar, des de una simple molèstia en la productivitat de la organització, fins a una gran amenaça de seguretat per tota la companyia.

En aquest sentit, i degut a que es tan senzill per als usuaris connectar-se a un punt d'accés dins la infraestructura de la xarxa de dades d'una organització, els responsables de la seguretat necessiten dotar-se d'eines per protegir-se contra aquest tipus d'amenaça i risc.

Els sistemes de de control d'accés a les xarxes de dades, en anglès Network Access Control (NAC), és una combinació de hardware i software que controla, de manera dinàmica, els accessos a la xarxa de dades dels dispositius i/o usuaris en funció del compliment d'unes polítiques de seguretat establertes. Tot aquell dispositiu i/o usuari que no compleixi amb les polítiques de seguretat es quedarà aïllat o sense accés a la xarxa de dades.

3.2 Funcionalitats dels sistemes de control d'accés

Un sistema de control d'accés a la xarxa de dades, com ja s'ha comentat anteriorment, ha de garantir, per un costat, el compliment d'unes polítiques de seguretat d'accés a la xarxa de dades definides però, per un altre costat, ha de oferir també visibilitat de tots i cada un dels dispositius i/o usuaris que estan connectats a la xarxa, o que intenten accedir-hi.

En aquests sentit, les solucions de control d'accés a les xarxes de dades aporten tres funcionalitats principals al eco sistema de seguretat que es comenten a continuació.

- **Visibilitat.** Les xarxes de dades actuals estan en constant evolució, com també ho estan els equips que s'hi connecten, i on s'hi podem trobar dispositius tradicionals, com són els dispositius Windows o Linux, però també dispositius més d'última generació com poden ser tot tipus de dispositius IoTs.

  Per tal d'aconseguir visibilitat de tots els dispositius que estan connectats a la xarxa de dades, les solucions de control d'accés a les xarxes de dades ofereixen diferents mètodes o tècniques de

descobriment de dispositius que al mateix temps, recol·lecten informació específica dels dispositiu per poder-los identificar i classificar.

- **Control dinàmic d'accés**. Les solucions de control d'accés a les xarxes de dades permeten també gestionar de manera dinàmica i autònoma l'accés dels dispositius i/o usuaris que pretenen accedir-hi. Aquest control d'accés i autorització del dispositiu i/o usuari vindrà donat per una identificació o autenticació prèvia.

- **Respostes automàtiques post accés.** Per garantir la integritat i la seguretat de les xarxes de dades post un accés dels dispositius, les solucions de control d'accés a xarxes monitoritzen contínuament la xarxa i responen de manera automàtica davant possibles exposicions de la seguretat, reaccionant automàticament en temps real per tal de contenir el dispositiu compromès i notificar l'incident a les diferents eines de gestió i monitorització del eco sistema de seguretat, com podria ser un SOC o NOC.

3.3 Mètodes d'identificació i autenticació

Els sistemes de control d'accés a les xarxes de dades es basen en el principi de la verificació de la identitat dels dispositius i/o usuaris que si connecten. Per aquest motiu, ofereixen tot un seguit de mètodes i protocols d'autenticació que permeten interactuar amb els dispositius i/o usuaris que es connecten a la xarxa amb la finalitat d'identificar-los i assignar-los les corresponents autoritzacions d'accés segons unes polítiques de seguretat d'accés establertes.

Tot seguit es presenten els mètodes d'identificació i autenticació utilitzats per las solucions de control d'accés a les xarxes de dades.

3.3.1 Autenticació per suplicant

Els sistemes de control d'accés a les xarxes de dades segueixen l'estàndard del protocol definit a l'IEEE 802.1x per l'autenticació dels dispositius i/o usuaris que es connecten a la xarxa.

L'IEEE 802.1x utilitza el protocol d'autenticació (EAP) per millorar el procés d'autenticació dels dispositiu i usuaris. En el procés d'autenticació mitjançant el protocol 802.1X, intervé el que s'anomena suplicant, que és l'usuari o client que intenta accedir a la xarxa, el servidor RADIUS, que és el servidor que autentica el client, i el que s'anomena autenticador, que és el punt on el dispositiu s'està intentant connectar (port del commutador o punt d'accés de la xarxa sense fils).

A continuació es presenta una taula comparativa dels protocols d'autenticació EAP més utilitzats en les solucions de control d'accés.

Tipus de EAP ---------- Avantatges	MD5	TLS	TTLS	PEAP	FAST	LEAP
Necessita certificat de client	No	SI	No	No	NO (PAC)	No
Necessita certificat de servidor	NO	SI	Si	SI	NO (PAC)	No
Atributs d'autenticació	Unidireccional	Mutua	Mutua	Mutua	Mutua	Mutua
Característica	MD5	Seguretat nivell de transport	Seguretat nivell de transport per túnels	Seguretat nivell de transport protegit	Autenticació flexible mitjançant tunelització segura	Protocol lleuger d'autenticació ampliable

Taula 4: Taula comparativa protocols autenticació EAP

Per un ampliació sobre els diferents protocols d'autenticació utilitzats pels sistemes de control d'accés a les xarxes de dades, en l'apartat d'Annexos d'aquest document, punt 10.2 protocols d'autenticació s'ha inclòs una descripció dels protocols d'autenticació mes comuns i utilitzats a l'hora d'implementar aquest tipus de solució.

3.3.2 Autenticació per perfilat

Com a mètode de suport a l'autenticació i identificació dels diferents tipus dispositius que es connecten a les xarxes de dades, així com també per identificar aquells dispositius que, com els IoTs, no disposen de recursos per interactuar directament en un procés d'autenticació, les solucions de control d'accés actuals han incorporat el que es coneix com l'autenticació per perfilat.

L'autenticació per perfilat consisteix en la tècnica d'identificar un dispositiu segons els diferents atributs i informació que se'n pot obtenir d'aquest des de diferents serveis de xarxa habitualment desplegats, com per exemple, DHCP, SNMP, entre d'altres. Els diferents atributs que se'n pot obtenir d'un tipus de dispositiu marquen un perfil. Les solucions de control d'accés actuals disposen d'una gran base de dades de perfils que els utilitzen a l'hora d'identificar dispositius o per aportar un suport addicional a l'autenticació tradicional.

3.4 Conclusions

Els sistemes de control d'accés a les xarxes de dades ofereixen una solució d'identificació i control d'accés sobre els dispositius que suporten els mètodes d'autenticació 802.1x àmpliament utilitzada i provada en les organitzacions.

Tanmateix, com s'ha exposat en l'apartat de la anàlisis de la problemàtica, són els dispositius sense recursos per autenticar-se els que presenten actualment els riscos mes importants pel que fa a la seguretat de les xarxes de dades, i on els sistemes actuals de control d'accés a les xarxes de dades, mitjançant diferents tècniques de perfilat de dispositius, intenten donar-hi una solució.

És important doncs, conèixer i entendre el funcionament de les solucions de perfilat de dispositius que ofereixen els sistemes de control d'accés per tal valorar, per una banda, la possible efectivitat de la solució dins de les xarxes de dades reals, i per l'altre banda, la facilitat d'implantació de la solució a curt termini dins d'una xarxa de dades en producció.

4 Identificació i perfilat de dispositius IoTs

En aquest apartat s'estudien i analitzen els diferents mètodes que poden ser utilitzats pels sistemes de control d'accés per tal de determinar (perfilar) de quin tipus de dispositius es tracta quan aquest no ofereix cap mètode al sistema de control per identificar-se.

Com s'ha exposat en l'apartat de l'anàlisi de la problemàtica d'estudi, hi ha tot un seguit de dispositius corporatius i personals (IoTs), que es connecten a les xarxes corporatives i suposen un risc molt elevant per la seguretat d'una organització pel fet que, per les seves característiques de disseny, no suporten cap mètode d'autenticació estandaritzat pels quals se'l pugui identificar i controlar.

4.1 Perfilat de dispositius

Es pot definir el perfilat dels dispositius com un mètode que permet identificar dispositius segons els diferents comportaments que es poden observar d'aquest quant es connecta a una xarxa.

El perfilat dels dispositius sol estar sota un model jeràrquic de 3 elements principals derivats dels atributs descoberts, un cop els dispositius es connecten a la xarxa de dades. Aquests elements són: la categoria del dispositiu, la família del dispositiu i el nom del dispositiu.

- **La categoria del dispositiu**, és la classificació mes àmplia d'un dispositiu i la qual denota el tipus de dispositiu del qual es tracte. Per exemple, si és un ordinador, una impressora, un punt d'accés, una tauleta, etc.

- **La família dels dispositiu**, classifica els dispositiu en una categoria segons els tipus de sistema operatiu que fan servir o el tipus de proveïdor. Per exemple, *Windows Linux*, *Mac OS X* serien famílies quan la categoria de dispositiu és un ordinador. En el cas d'*Apple*, *Android* serien exemples de famílies de dispositius quan la categoria fos *SmartDevice*.

- **La versió del dispositiu**. Dins d'una família de dispositius, aquests es solen classificar de manera mes granular segons la seva versió o nom de dispositiu. Per exemple, *Windows 10*, *Windows 11*, *Windows 2012* server, els quals son nom de dispositius sota una mateixa família de dispositius.

Aquest model jeràrquic, proporciona una vista estructurada de tots els dispositius que estan connectats a la xarxa.

A part de tota aquesta informació comentada anteriorment, també se'n pot recopilar d'altre de molt útil per la identificació del dispositiu, com pot ser:

- L'adreça IP assignada
- El nom del dispositiu
- El proveïdor de la MAC
- En quin moment s'ha descobert el dispositiu
- Quin moment ha estat l'últim cop que s'ha vist els dispositiu connectat
- etc.

4.2 Col·lectors

Els col·lectors són un seguit de serveis i elements dins d'una xarxa que ajuden a recopilar dades, o atributs dels dispositius, quan es connecten a la xarxa i, d'aquesta manera, poder-los identificar i classificar, segons s'ha vist en el punt anterior.

Col·lectors	
Tècniques passives	**Tècniques actives**
Peticions DHCP	Consultes SNMP
HTTP User-Agent	Connexions SSH
TCP Empremta digital	Escaneig de xarxa (Nmap)
Netflow	Consultes LDAP
Flexible Netflow	Consultes REST
IPFix	Consultes SQL
sFlow	Cisco Device Sensor
Peticions RADIUS	
MAC OUI	

Taula 5: Col·lectors

A continuació es descriuen els col·lectors mes comuns i utilitzats, per les solucions de control d'accés, a l'hora d'identificar els dispositius connectats en les xarxes de dades.

4.2.1 DHCP

El DHCP és un protocol de xarxa client/servidor que permet als dispositius clients que es connecten a una xarxa adquirir una sèrie de paràmetres per la seva configuració a xarxa on , entre d'altres paràmetres, el mes comú i habitual és l'obtenció d'una adreça IP dinàmica.

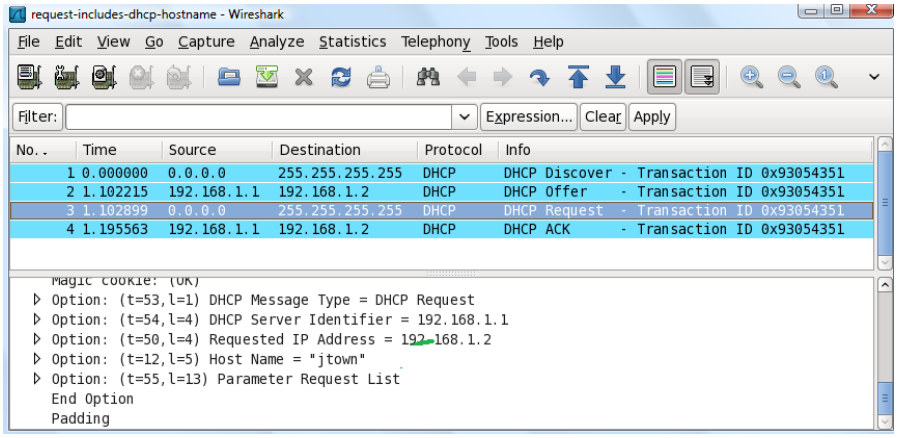
Mitjançant el protocol de DHCP, i durant el diàleg entre client i servidor, DISCOVER i REQUEST, el dispositiu client envia tot un seguit d'atributs que identifiquen el client de manera única.

Entre aquests atributs enviats podem trobar, per exemple, l'opció 55 (llista de sol·licituds de paràmetres), l'opció 60 (classe de proveïdor), entre d'altres,

Els dispositius de control d'accés d'última generació (NAC), s'aprofiten d'aquest protocol DHCP per identificar i classificar els dispositius que es connecten a xarxa, focalitzant-se, sobre tot, en aquells dispositius que no disposen o ofereixen cap sistema de seguretat per tal d'autenticar-se.

Les tècniques utilitzades per aconseguir llegir la informació dels clients de DHCP són les de Relay de DHCP, DHCP SPAN o RSPAN, cap els dispositius de control d'accés.

Com es pot evidenciar en aquest mètode, per perfilar els dispositius de xarxa, requereix que els dispositius connectats a xarxa estiguin configurats per l'obtenció dinàmica d'IP i no s'hagin configurat una IP de manera manual i estàtica. La configuració de la IP estàtica, per exemple, la podria efectuar un ciberdelinqüent en el cas de que fos coneixedor d'aquesta tècnica de detecció i perfilat de dispositius.



4.2.2 HTTP User-Agent

La aplicació de navegació web, els navegadors, també es poden utilitzar a l'hora identificar dispositius. Aquest, dins la capçalera HTTP/HTTPS, coneguda com a User-Agent, inclou tot un seguit d'informació adapta per identificar el dispositiu, com per exemple, el tipus d'aplicació, el sistema operatiu, el proveïdor de programari, etc.

Les solucions de control d'accés poden capturar aquesta informació dels navegadors web continguda en l'atribut de l'User-Agent, així com d'altres atributs HTTP dels missatges de sol·licitud, i els afegeixen a la llista d'atributs del dispositiu descobert.

Els mètodes principals que s'utilitzen els sistemes de control d'accés per tal de capturar l'User-Agent d'un client sol ser la redirecció d'URL cap un portal captiu

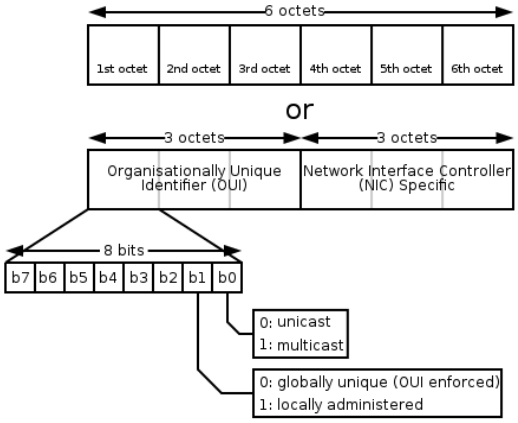
d'autenticació, o mètodes de replicació i redirecció (SPAN) de paquets del port on es troba el dispositiu client connectat, per tal analitzar-los.

```
Hypertext Transfer Protocol
  GET /cd/132/update2.132.0.exe HTTP/1.1\r\n
     Request Method: GET
     Request URI: /cd/132/update2.132.0.exe
     Request Version: HTTP/1.1
   Accept: */*\r\n
   Accept-Encoding: identity\r\n
   User-Agent: Microsoft BITS/6.6\r\n
   Host: inupdate.info\r\n
   Connection: Keep-Alive\r\n
```

4.2.3 MAC OUI

Les adreces MAC haurien de ser úniques en el mon. El valor de l'adreça MAC és el resultat directe de les normes implementades per l'IEEE amb l'objectiu de garantir adreces úniques per a cada dispositiu. L'IEEE assigna al proveïdor un codi de 3 bytes (24bits) denominat Identificador únic d'organitzador (OUI). En aquest sentit, totes les adreces MAC assignades a una NIC han d'utilitzar l'OUI que té assignat el proveïdor com els 3 primers bytes.

La utilització de la MAC OUI ja s'ha vist anteriorment que es fàcilment vulnerable, tanmateix, si que es utilitzat com a complement per la classificació dels dispositius descoberts.



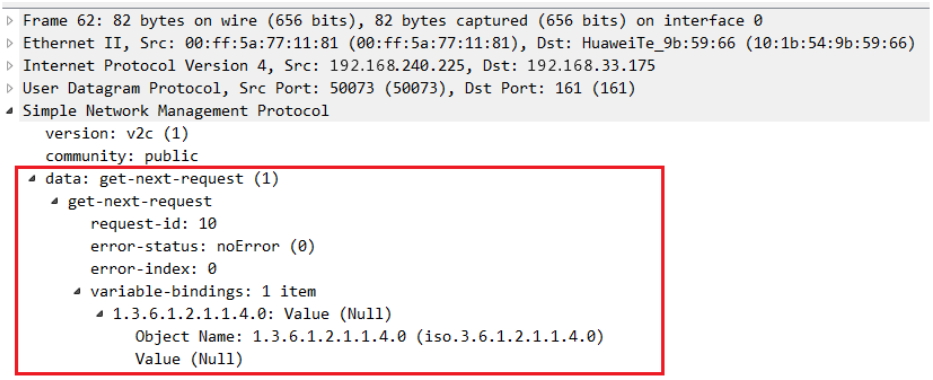
4.2.4 SNMP

L'SNMP és un protocol estàndard de capa d'aplicació, basat en IP, que intercanvia informació entre una solució d'administració de xarxa i qualsevol dispositiu, hardware o software, que tingui habilitat l'SNMP.

Un component molt important del SNMP és el que s'anomena MIB o base d'informació d'administració. Es tracte d'un arxiu de text que conté informació organitzada i jerarquitzada relativa a les dades que es poden recopilar d'un dispositiu determinat. Les MIBs estan incloses en tots els dispositius que suporten SNMP.

Aquesta informació SNMP doncs, també pot ser utilitzada com a mètode d'identificació de dispositius per un sistema de control d'accés.

Certament, el mecanisme de perfilat basat en SNMP només és capaç de crear perfils de dispositius en el cas de que els dispositiu responguin a consultes SNMP, o en el cas de que el dispositiu anuncii la seva capacitat mitjançat el protocol estàndard de descobriment LLDP, o el propietari de Cisco, CDP, en els dispositius de xarxa on estan connectats (commutador, controladors APs, routers, etc)



4.2.5 Lectura taules ARP

L'ARP és un protocol de resolució d'adreces MAC a partir d'una adreça IP. L'ús d'aquest protocol és força clar dins de les xarxes de dades. Les funcionalitat doncs, són les de resoldre direccions físiques associades a una IP, l'enviament de datagrames entre diferents dispositius de la mateixa xarxa, evitar IP duplicades, etc.

Cada dispositiu de xarxa conté una taula d'ARP que emmagatzema las adreces IP de les quals coneix la seva MAC.

En aquest sentit, les solucions de control d'accés NAC, utilitzen les taules ARP de diferents dispositius de xarxa, com poden ser els commutadors, controladors, routers, etc (equips NAS) per tal descobrir els dispositius que estan connectats en ells. Les solucions de control d'accés pregunten periòdicament mitjançant SNMP als dispositius NAS sobre les seves taules ARP.

ARP Table

IP Address	MAC Address
128.8.127.4	1C-6E-97-CF-08-DF
128.96.40.151	FD-BC-EE-7A-F1-B3
192.4.153.17	BC-C8-D0-58-3F-E5
192.4.153.90	B8-EF-9C-BA-F8-B5
10.10.10.1	46-F4-93-AF-86-B1
113.89.79.1	FC-01-31-42-FC-60
71.201.65.1	34-74-FC-72-A9-2B
22.231.5.9	75-E1-9B-43-CA-69

4.2.6 Descobriment de dispositius via escaneig de xarxa

Un altre mètode força comú utilitzats pels sistemes de control d'accés per tal descobrir dispositius amb IP estàtica, és el de realitzar exploracions o escanejos de subxarxes de dades. Per exemple, hi ha sistemes de control d'accés que utilitzen el mètode d'escaneig mitjançant l'aplicació NAMP per descobrir equips connectats a les xarxes de dades, i al mateix temps utilitzar la potència d'aquesta eina per tal de validar si els dispositius descoberts disposen del port SNMP obert, port 161, entre d'altres ports. D'aquesta manera, recopilar informació addicional que pot ser utilitzat per seguir aplicant mètodes diferents de perfilat sobre el dispositiu descobert.

```
nmap -iL hosts.txt


Nmap scan report for localhost.example.com(127.0.0.1)
Host is up (0.0000080s latency).
Not shown: 991 closed ports
PORT     STATE    SERVICE
22/tcp   filtered ssh
25/tcp   open     smtp
80/tcp   open     http
111/tcp  open     rpcbind
631/tcp  open     ipp
3000/tcp open     ppp
4000/tcp open     remoteanything
8080/tcp open     http-proxy
9090/tcp open     zeus-admin

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds


nmap 10.19.140.2

Starting Nmap 6.40 ( http://nmap.org ) at 2019-07-21 16:39 EDT
Nmap scan report for 10.19.140.2
Host is up (0.061s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
199/tcp  open  smux
443/tcp  open  https
8000/tcp open  http-alt
8181/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.18 seconds
```

4.2.7 Cisco Discovery Protocol

Igual que en el cas del protocol estàndard LLDP, Cisco Discovery Protocol és un protocol de capa 2 del model OSI, capa d'enllaç, al qual permeten als commutadors de xara aprendre dinàmicament els atributs dels dispositius connectats. En aquest cas, i a diferencia del protocol LLDP, CDP és un protocol propietari de Cisco.

Molts dispositius de xarxa, inclosos equips de vídeo IP, infraestructures de xarxa, electrodomèstics Cisco, i un nombre creixent de dispositius d'Internet de les coses (IoT), utilitzen el protocol LLDP/CDP per comunicar les seves característiques de dispositiu cap a la xarxa.

Alguna de la informació que es pot obtenir dels dispositius que suporten CDP és, per exemple, el nom del dispositiu, la plataforma, la versió del sistema operatiu, l'adreça IP, entre d'altres.

```
Switch1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Switch2          Fas 0/9           138              S I   WS-C3560- Fas 0/9
Switch3          Fas 0/11          158              S I   WS-C3560G Gig 0/11
Switch4          Fas 0/14          143              S I   WS-C3560G Gig 0/14
term-server      Fas 0/24          140                    2511      Eth 0
SEP00179462595A  Fas 0/21          157            H P M   IP Phone  Port 1
SEP0019AA56FACA  Fas 0/20          161            H P M   IP Phone  Port 1
RHN              Fas 0/2           125            R S I   3825      Gig 0/0
JNN1             Fas 0/1           159            R S I   3825      Gig 0/0
Switch1#
```

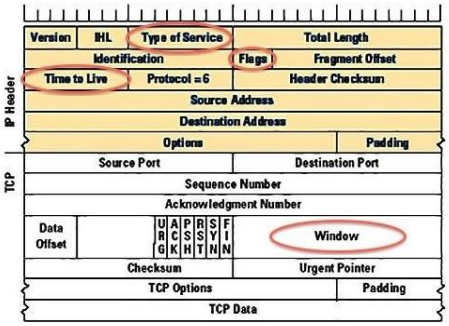
4.2.8 Empremta digital TCP/IP

L'empremta digital TCP, o també conegut com a empremta digital de pila TCP, és una tècnica d'anàlisi de camps de dades que contenen els paquets TCP/IP. Així doncs, segons cert els camps continguts en els paquets TCP/IP es pot identificar el dispositiu de xarxa que l'origina. Entre la diversitat d'informació que es pot aconseguir de l'anàlisi d'aquest paquets TCP/IP, hi ha la informació del tipus de dispositiu que ha originat el paquet, així com la informació del seu sistema operatiu.

Hi ha dos tècniques que utilitzen els dispositiu de control d'accés per analitzar les empremtes digitals TCP/IP d'un xarxa, l'escaneig passiu i l'escaneig actiu.

En un escaneig actiu, els sistemes de control d'accés envien paquets i n'esperen les seves respostes per tal de comparar-les la informació que aquests disposen en las seva base de dades i determinar-ne una identitat.

En un escaneig passiu, s'escolta el tràfic que circula per la xarda per tal d'identificar les màquines que s'estan comunicant. Aquest mètode, de vegades té l'inconvenient que cal esperar molt de temps per identificar dispositius si aquests no són molt actius.



4.3 Conclusions

Els sistemes de control d'accés a les xarxes de dades necessiten nodrir-se dels diferents serveis desplegats a les xarxes corporatives, així com integrar-se amb d'altres solucions de l'ecosistema de seguretat, per tal dotar-se de visibilitat de tots els dispositius que s'hi connecten.

No hi ha unes bones pràctiques clarament definides pel que fa a l'ús dels col·lectors. Tanmateix, si que l'experiència dels administradors apunten a utilitzar-ne tants com, la solució de control d'accés i les infraestructures de xarxes on s'apliquen, en puguin suportar. No obstant, s'ha de tenir en compte que un ús abusiu de les tècniques mitjançant col·lectors actius, escanejos, podrien provocar incidents de rendiment en la xarxa de dades.

5 Estudi de mercat de les solucions de control d'accés (NAC)

En el següent apartat es mostra un estudi de mercat de les solucions de control d'accés NAC considerades punteres en la regió europea, segons la consultora tecnològica de gran prestigi, Gartner (2021). *Network Access Control (NAC) Reviews a Ratings*.https://www.gartner.com/reviews/market/network-access-control

Així doncs, trobem que els primer 5 fabricants punters pel que fa a solucions NAC són: Cisco ISE, The Forescout Platform, Aruba ClearPass Policy Manager, Policy Secure NAC i FortiNAC.

5.1 Cisco identity Services Engine (ISE)

La solució de control d'accés ISE, de Cisco Systems, ofereix un control complert sobre qui, què, quan, on i com es permeten que els diferents dispositius es connectin a una xarxa. Entre d'altres tecnologies, l'ISE és destaca per la utilització de la segmentació definida pel protocol anomenat TrustSec, propietari del mateix fabricant Cisco Systems. Aquest protocol s'utilitza per la classificació del tràfic que hi circula per la xarxa, assignant etiquetes, amb la finalitat d'identificar-lo per permetre'l o bloquejar-lo, segons unes polítiques de seguretat prèviament definides per les organitzacions.

L'ISE és una solució que s'integra bé amb d'altres productes de Cisco, cosa que d'entrada el posiciona en entorns de xarxa d'infraestructures pro Cisco. La solució d'ISE està disponible per a dispositius físics i també per a dispositius virtual, tan per hipervisors VMWare, Red Hat i de Microsoft.

Com a solució per a validar la salut d'un dispositiu, l'ISE utilitza l'agent permanent anomenat AnyConnect, molt conegut pels usuaris ja que s'utilitza també com aplicació client per accessos remots, VPN Client.

A continuació s'enumeren algunes de les seves funcionalitats principals i destacables:

- Serveis AAA integrats i suport per a múltiples serveis d'identitat com directori Actiu, LDAP, RADIUS, RSA, OTP etc
- Gestió de polítiques centralitzada i control d'accés basat en funcions de BYOD integrat, mobilitat i gestió del cicle de vida dels convidats.
- Portals de convidats mòbils personalitzats.
- Perfilat de dispositius i servei de validació de la salut dels dispositius.

La solució d'ISE s'ofereix amb 4 tipus de llicències.

- Base (User Visibility and Enforcement, AAA and 802.1x, Guest)
- Advantge (Device Visibility, BYOD, Context Sharing, Group Based policy)
- Premier (Full Stack Compliance, Cloud Services, RTC/ANC).
- Device Admin (TACACS+ services)

Com a conclusió es pot dir que, Cisco ISE és una molt bona solució de control d'accés i, molt probablement, la mes adequada en organitzacions que han invertit en una infraestructura completa de Cisco. Tanmateix, en d'altres infraestructures de xarxa amb dispositius multi fabricant, es pot considerar fàcilment solucions NAC d'altres fabricants.

5.2 Forescout

La solució de control d'accés de Forescout, és una solució molt flexible i, al mateix temps, molt robusta, que ofereix la possibilitat del descobriment i gestió de dispositius de xarxa sense la necessitat d'instal·lar agents de software en els dispositius.

Com s'ha comentat anteriorment, la capacitat d'integració amb el programari i amb la infraestructura de xarxa existent, és un dels factors importants a tenir en compte a l'hora d'avaluar els productes NAC. En aquest cas, una de les principals característiques de la solució de Forescout és el grau elevant de possibilitats d'integració amb d'altres solucions de seguretat com IPS, SIEM, entre d'altres.

La solució de Forescout posa èmfasi en la visibilitat dels dispositius que hi ha connectats a les xarxes i, gràcies al seu accés a milions de perfils de dispositius, pot identificar-ne una gran varietat.

A través del seu motor de polítiques de seguretat, pot proporcionar control d'accés a la xarxa, segmentació i, fins i tot, donar resposta automàtica a incidents detectats.

El producte estrella de Forescout, Forescout 8.2, identifica i avalua dinàmicament els dispositius a mesura que aquest es connecten a la xarxa de dades d'una organització. Al mateix temps, proporciona la base per automatitzar i aplicar una àmplia gamma de controls basats en polítiques de seguretat i forçar-ne el seu compliment.

Els components de la solució de ForesCout inclouen:

- eyeSight: proporciona visibilitat a una xarxa mitjançant la detecció, classificació i avaluació de dispositius a mesura que estableixen una connexió sense necessitat d'agents.
- eyeControl: ajuda a aplicar i automatitzar controls basats en polítiques, així com a respondre a incidents.
- eyeSegment: proporciona segmentacions de xarxa o zones de seguretat lògiques a tota l'empresa.

La solució de Forescout es permet desplegar com a dispositiu físic o com a solució virtual. Hi ha tres nivell de suport disponibles per a clients, ActiveCare Basic ActiveCare Advanced i Forescout Premium Care. Cadascun inclou l'accés a un portal d'assistència en línia, assistència per correu electrònic i actualitzacions de programari.

Com a conclusió d'aquesta solució de control d'accés, la plataforma de Forescout NAC és una opció excel·lent per a les organitzacions que disposen d'equips de xarxa de diferents proveïdors, ja que pot recopila informació dels dispositius connectats d'una manera senzilla. Per aquest motiu, és una solució molt adequada per a grans organitzacions on solen tenir una gran varietat de dispositius multi fabricant.

5.3 HPE Aruba ClearPass Policy Manager

La solució de control d'accés d'Aruba, adquirida per HP, proporciona un control d'accés a les xarxes de dades molt segur, basat en dispositius corporatius, dispositius de col·laboradors o proveïdors, de convidats, IoTs i BYOD en qualsevol infraestructura, ja sigui de cable, sense fils i VPN.

ClearPass ofereix també mecanismes automatitzats, com som els portals d'auto registre de convidats, i aprofita dades contextuals sobre rols d'usuari, dispositius, ús de aplicacions, ubicació i períodes temporals, per desplegar BYOD i gestionar els accessos segurs a la xarxa de dades.

La solució de control d'accés de HP està disponible també com a dispositiu físic, o virtual.

Les seves funcionalitat mes destacables inclouen:

- Integració integral amb sistemes de tercers com SIEM, IPS IDS, EMM i MDM.
- Admet múltiples fonts d'autenticació i autorització, directori actiu, LDAP, SQL dins d'un mateix servei.
- Integració de dispositius d'autoservei amb una autoritat de certificació (CA) integrada per a BYOD.
- Admet la integració NAC i EMM, MDM per a avaluacions de dispositius mòbils.
- Aplicació de l'accés a la xarxa basa en rols per a xarxes heterogènies.

- Accés de convidats amb una àmplia personalització i marca.
- Informes de totes les autenticacions vàlides i fallides dels usuaris.
- Perfils integrats mitjançant empremtes digitals DHCP i TCP.

ClearPass ofereix tres mòduls funcionals diferenciats, i els quals s'activen segons el tipus de llicencia adquirida. Així doncs, en aquest podem trobar:

- ClearPass Onboard, on s'ofereix una plataforma d'auto registre de dispositius i usuaris, per tal obtenir accés a la xarxa de dades mitjançant un portal autoguiat. La configuració específica del dispositiu i de la seguretat per la seva connexió, es configura automàticament en dispositius autoritzats. La solució d'Onboarding està suportada per dispositius amb sistema operatiu Windows, iOS, Android Linux..

- ClearPass OnGuard, on s'ofereix avaluacions de la validació de la salut dels dispositius a través de connexions sense fils, per cable i VPN, mitjançant opcions de desplegament flexibles, amb agents i sense agents.

- ClearPass Guest, el qual simplifica els processos de registre dels usuaris convidats per tal de permetre el seu accés a la xarxa de dades.

Com a conclusió d'aquesta solució de control d'accés, ClearPass és una solució molt complerta, que s'adapta perfectament tan en infraestructures de xarxa basades en Cisco, com en infraestructura multi fabricant. Tanmateix, per aprofitar realment aqueta solució de control d'accés, s'ha de contemplar la compra de la totalitat, o la gran majoria, de les funcionalitat que ofereix. Això fa que pugui resultar car per empreses pimes i davant d'altres competidors del mercat.

5.4 Pulse Policy Secure

La solució NAC de Pulse Policy Secure (PPS) permet a les organitzacions tenir visibilitat dels dispositius connectat a la xarxa, així com també fer complir unes les polítiques d'accés basades en rols de seguretat per a dispositius i usuaris (corporatius, convidats, col·laboradors).

La solució PPS NAC permet a les organitzacions complir amb nombrosos requisits normatius de la indústria, des del sector governamental, fins a la sanitat. Al mateix temps, ofereix també la possibilitat remediació dels dispositius d'usuaris, la incorporació de BYOD així com una resposta automàtica a les amenaces detectades.

El PSS es pot desplegar en plataformes físiques, virtuals i al núvol. S'integra bé amb una àmplia gamma de solucions de seguretat de tercers, com són tallafocs d'última generació, IPS i SIEM de diferents fabricants.

La solució Pulse Policy Secure es compon de tres components o mòduls:

- Pulse Profiler: el qual proporciona visibilitat de la xarxa, identificació de punts finals i classificació, informes i anàlisis de comportament.
- Pulse Policy Secure: que proporciona un motor de polítiques unificat que aprofita la informació contextual dels usuaris, punts finals i aplicacions.
- Pulse Client: el client Pulse ofereix opcions d'agent i sense agent per al control previ i posterior a l'admissió i la verificació de la postura de seguretat del punt final.

Algunes de les funcionalitats mes destacables inclouen:

- Interoperabilitat: permet una fàcil integració amb dispositius de seguretat i xarxa de tercers
- Una configuració basada en l'assistent que elimina la complexitat de la configuració d'una solució NAC
- Pulse Profiler, identifica i classifica els dispositius de punt final, inclòs l'IoT
- Host Checker, identifica la postura de seguretat del dispositiu
- Suport d'accés per a convidats d'autoservei
- Gestió de polítiques centralitzada
- Suport RADIUS i TACACS +
- Resposta automàtica de les amenaces

Les opcions de llicència disponibles per a Pulse Policy Secure són les següents:

- Common Access Licenses: les llicències d'accés comuns estan disponibles com a llicències d'usuari que es poden utilitzar per a sessions d'usuari de Pulse Policy Secure (NAC) o sessions d'usuari de Pulse Connect Secure (SSL VPN).
- Enterprise Licenses: poden ser perpetues o basades en subscripcions. Les llicències perpètues tenen un càrrec únic; mentre que les llicències de subscripció ofereixen una opció més flexible i globalment valuosa amb terminis d'un, dos o tres anys.
- Altres opcions de llicència són llicències basades en rols, llicències Pulse Secure Profiler, llicències de servidor IF-MAP i llicències OAC-ADD-UAC.

De la mateixa manera, Pulse Policy Secure ofereix diferents nivells de suport en funció de les necessitats. Algunes de les opcions disponibles són:

- Gold Support: inclou l'accés a qualsevol hora i dia d'assistència globals per telèfon o en línia.
- Platinum Support: inclou tots els serveis del nivell d'assistència Gold, a més d'un accés a un equip dedicat d'enginyers superiors que gestionarà tots els casos d'assistència.

- Partner Branded Support (PAR): els clients que hagin comprat aquesta opció d'assistència es posaran en contacte amb el seu Partner quan hagin d'obrir un cas d'assistència en lloc de contactar amb Pulse Secure.

5.5 FortiNAC

FortiNAC és la solució NAC de Fortinet, la qual proporciona visibilitat, perfilat de dispositius, control i resposta automatitzada i en temps real per a tot els dispositius que es connecten a una xarxa de dades, inclosos els dispositius IoT.

FortiNAC realitza una avaluació de dispositius, estat de salut, per veure si coincideix amb perfils aprovats per la autorització de la seva connexió, com ara actualitzacions de programari i de vulnerabilitats. L'avaluació es pot fer de forma activa o passiva, i pot utilitzar agents permanents, agents solubles o sense agent (agentless).

FortiNAC és una solució flexible i escalable dirigida a mitjanes i grans empreses, i contempla àrees com la salut, l'educació, l'IdT i proveïdors de serveis gestionats.

Es pot desplegar en màquines virtuals (VMWare / AWS / Azure / KVM) o dispositius físics, appliance. FortiNAC és una solució 'fora de banda', això vol dir que no té cap impacte sobre el trànsit productiu dels usuaris i per tant, té poc o cap impacte en el rendiment de la xarxa.

La solució FortiNAC està composada de tres mòduls:

- Aplicació i control (obligatori): l'aplicació i el control proporcionen capacitats de visibilitat i configuració, així com funcions de resposta automatitzada.
- Gestió (opcional): la part de Gestió permet compartir usuaris concurrents en un desplegament de diversos servidors.
- FortiAnalyzer for Reports (opcional): FortiAnalyzer proporciona informes i anàlisis basats en la informació recollida de la xarxa a través de FortiNAC

FortiNAC ofereix tres opcions de llicència basades en les funcions i funcionalitats.

- BASE License: el nivell de llicència BASE és adequat per a organitzacions que necessiten protegir IoT i altres dispositius de xarxa, però no requereixen controls avançats d'usuari / xarxa ni resposta automàtica a les amenaces.
- PLUS License: la llicència PLUS és adequada per a les organitzacions que vulguin una visibilitat i control de punts finals complerts, però que no requereixin una resposta automàtica a les amenaces.
- PRO License: la llicència PRO és adequada per a les organitzacions que vulguin visibilitat, control i resposta automàtica del punt final complet.

Com a conclusió d'aquesta solució de control d'accés, FortiNAC és una potent solució de NAC per a la gestió de dispositius de xarxa, especialment per a dispositius BYOD i IoT. Tanmateix, tot i que admet dispositius de xarxa de tercers, es una solució orientada a entorns de xarxa que es basen, principalment, en equips de xarxa Fortinet, com són els tallafocs Fortigate, entre d'altres.

5.6 Criteris de comparació

A continuació es presenta una taula amb els criteris de comparació entre els diferents fabricants de solucions de control d'accés a xarxes segons les funcionalitats que aquestes cobreixen.

Funcionalitats	ISE	Forescout	ClearPass	PPS	Fortinac
Característiques incorporades					
Autenticació per múltiples mètodes 802.1x.	✓	✓	✓	✓	Limitat a mètodes EAP
Autenticació per portal captiu	✓	✓	✓	✓	✓
Autenticació MAC	✓	✓	✓	✓	✓
No AAA	✓	✓	✓	✓	✓
Compatibilitat amb multi fabricant	limitat	Llicencia addicional	✓	limitat	limitat
Perfilat inclòs en la llicencia bàsica	Llicencia advantage	○	✓		Llicencia plus
Alta disponibilitat actiu / actiu	✓	✓	✓	✓	○
HA failover automàtic	Requereix tasques post HA failover	○	✓	✓	✓
Eines automàtiques d'Upgrade	Requereix tasques post HA failover	Requereix el node Enterprise Manager	✓	○	✓
TACACS+	Cal llicencia addicional	○	✓	✓	○
Integracions amb tercers	limitat	limitat	limitat	limitat	limitat
Core AAA					
Autenticació SQL	✓	Llicencia addicional	✓		○
Autenticació LADP	✓	Llicencia addicional	✓		✓
Autenticació multi domini AD	✓	✓	✓		

Multi factor d'autenticació	Radius Proxy		✓		
SAML 2.0 /SP and idP) i Oauth	✓		✓		○
Suport SCEP	✓		✓		○
RadSec support RADIUS/TLS	✓		✓		○
Perfilat					
Perfils per a dispositius cablejats i sense fils	✓	✓	✓		✓
Col·lector actius i passius	✓	✓	✓		✓
Escanejos programats	○	○	✓		
Descobriment de dispositius actius	✓	✓	✓		✓
Empremtes digitals mitjançant de DHCP i TCP	✓	✓	✓		No TCP
Suport per a Netflow and IPFIX	✓	✓	✓		○
Escaneig WMI	✓	✓	✓		○
Escaneig SNMP	✓	✓	✓		✓
Escaneig SSH	✓	✓	✓		✓
Suport sFlow	✓	✓	✓		○
BYOD					
Integració basada en certificats	✓	○	✓		○
Inclou servei de certificadora interna	✓	○	✓		○
Integració amb certificadora AD de Microsoft	✓	✓	✓		○
Aprovisionament automàtic de certificats per a dispositius	✓		✓		○
Aprovisionament automàtic de perfils de xarxa	✓		✓	✓	✓
Portal per la gestió de certificats	✓		✓		○
Opció d'aprovació d'accés via patrocinador	✓		✓		✓
Convidats					
Portals personalitzats	limitat	✓	✓	✓	✓
Social login support	✓		✓		
Auto registre	✓	✓	✓	✓	✓

Registre patrocinat	✓	✓	✓	✓	✓
El patrocinador pot assignar nivell d'accés, convidat, col·laborador, etc	✓	✓	✓	✓	✓
Integració amb PMS Hotel	limitat		limitat		○
Integració amb sistemes de pagament	✓		✓		○

Taula 6: Criteris de comparació entre els diferents fabricants de NAC

5.7 Conclusions

Pel que fa a les conclusions finals obtingudes de l'estudi de mercat dels principals sistemes de control d'accés a les xarxes de dades, cal constatar que, sobre el paper, revisant les seves fitxes tècniques i portal webs dels respectius fabricants, totes les solucions suporten àmpliament tots els requisits, tècnics i de seguretat, estudiats per la protecció dels dispositius IoTs, com són, per exemple, el ventall de diferents mètodes de descobriment de dispositius, el perfilat i la classificació dels mateixos, la possibilitat de integració amb d'altres solucions i amb multi fabricant... que d'entrada, donen peu a ser a sotmetre cada solució a una prova de concepte per tal de validar-ne les seves capacitats reals.

Tanmateix, i degut a que els dos fabricants de control d'accés a les xarxes de dades implementades en el nostre territori són la solució d'ISE de Cisco Systems, i la solució de ClearPass d'HP/Aruba, s'han escollit aquestes dues solucions per la realització a continuació d'una prova de concepte dels productes, limitada a la protecció dels dispositius IoTs.

6 Prova de concepte (PoC)

Per la realització de la prova de concepte de la solució de control d'accés a la xarxa de dades per IoTs s'han escollit dues de les solucions NAC punteres en el mercat i estudiades anteriorment, la solució de ClearPass del fabricant Aruba, i la solució d'ISE del fabricant Cisco Systems.

La configuració específica i rellevant realitzada en els equips que participen en la PoC, així com les diferents captures de les evidències de les proves realitzades per la validació de la solució testejada, queden recollides en l'annex d'aquest document.

6.1 Objectius

L'objectiu principal de la prova de concepte és la de testejar i validar l'efectivitat de les diferents funcionalitats que presenten els sistemas actuals de control d'accés a les xarxes de dades com a solució davant la problemàtica d'estudi dels dispositius IoTs tractat durant en el TFM.

Paral·lelament a la validació de les funcionalitats i solucions tecnològiques per la protecció de l'entorn dels dispositius IoTs, es pretén valorar també la possible dificultat d'implementació de la solució en un entorn real i productiu.

Així doncs, a continuació es detallen en la següent taula les diferents funcionalitats de les solucions de control d'accés que es pretenen validar.

Funcionalitats NAC a testejar	
Funcionalitat	**Descripció**
Mètodes d'identificació	Utilització de diferents tipus de col·lectors per a identificar dispositius IoTs connectats a la xarxa de dades.
Mètodes d'autenticació	Autenticació de dispositius IoTs mitjançant perfilat.
Autorització	Autorització d'accés a recursos de la xarxa segons el rol de perfilat obtingut.
Integracions	Integració de la solució de NAC amb d'altres equips i dispositius de l'ecosistema de seguretat.
Gestió i monitorització	Control d'accés i monitorització dels dispositius IoTs mitjançant la solució de NAC.

Taula 7: Funcionalitat NAC a testejar - PoC

6.2 Dispositius utilitzats

Per la realització de la prova de concepte de control d'accés s'han utilitzats els dispositius que es descriuen en la següent taula.

Dispositiu per la realització de la PoC		
Dispositiu	**Model**	**Descripció**
Dispositiu (NAC)	ClearPass CLAVB (CCPM)	Solució de control d'accés a les xarxes de dades
Dispositiu (NAC)	Cisco ISE	Solució de control d'accés a les xarxes de dades
Commutador	Cisco Catalyst 3750G	Pila de tres commutadors
Tallafocs	Palo Alto 2020	Tallafocs de tercera generació.
Telèfon IP	Cisco CP7841	IoT – Telèfon IP
Punt d'accés	Cisco AP C1130	IoT - Punt d'accés per la xarxa sense fils.
Servidor	Servidor Windows 2020	Disposa dels serveis de directori actiu, de certificadora, DHCP i DNS.
PC Portàtil	Windows 10	PC portàtil per la realització de les diferents proves de suplantació identitat dels dispositius IoTs.
Entorn virtualització	ESXi 6.5	Entorn virtualització on s'ha instal·lat el ClearPass i el servidor Windows 2021

Taula 8: Dispositius - PoC

Com es comenta en la columna descripció de la taula anterior, s'han utilitzat un telèfon IP i un dispositiu punt d'accés Wi-FI com a dispositius IoTs, i un PC portàtil com a dispositiu utilitzat per la realització de les diferents proves d'atac als dispositius IoTs.

6.3 Segmentació de la xarxa

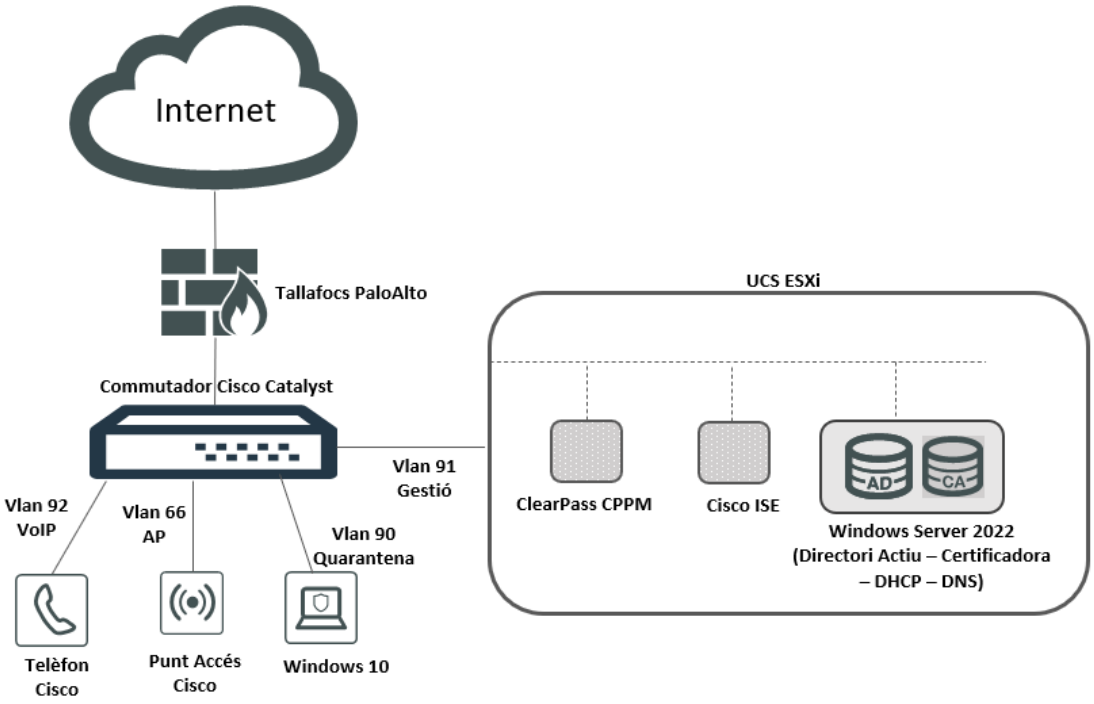
Les dades per la segmentació de la xarxa utilitzada durant la PoC són les que es mostren en la següent taula.

Entorn de xarxa		
Xarxa	**Etiqueta vlan**	**Xarxa**
Entorn Quarantena	90	192.168.115.0/24
Entorn Gestió	91	192.168.116.0/24
Dispositius VoIP	92	192.168.120.0/24
Dispositius Punt d'Accés	66	192.168.116.0/24

Taula 9: Segmentació de la xarxa - PoC

6.4 Esquema lògic de xarxa

El disseny de l'esquema de xarxa lògic de la PoC queda representat en la següent imatge.



6.5 Col·lectors de perfilat

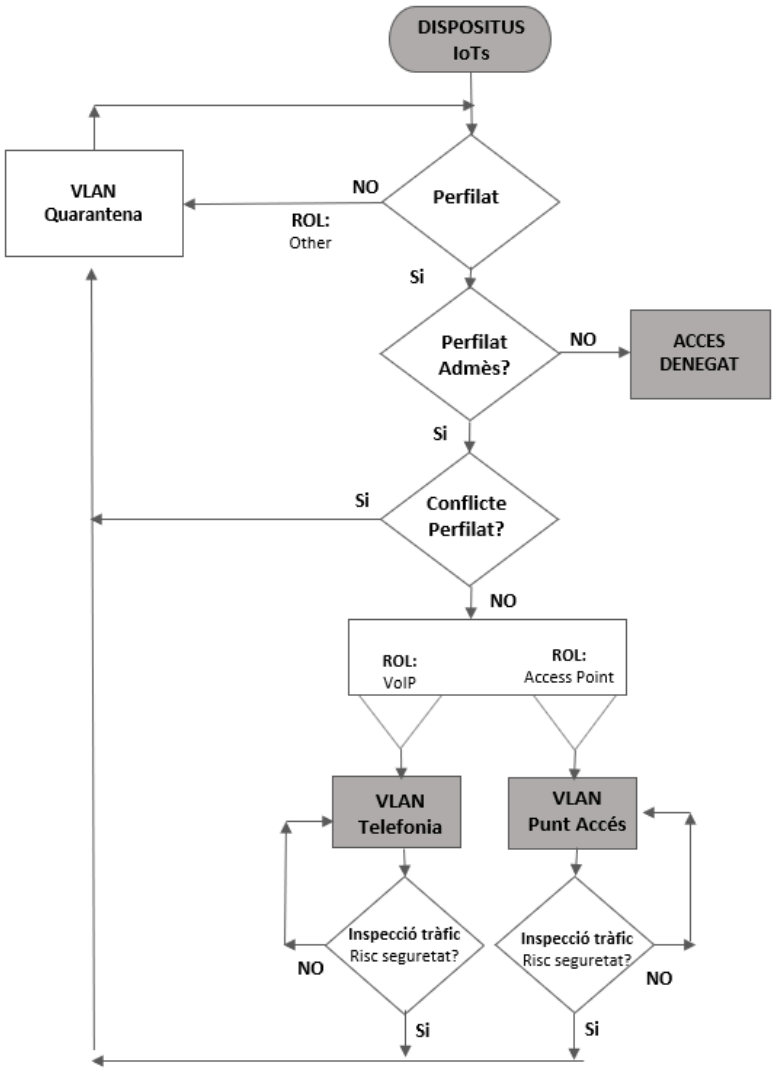
Els col·lectors configurats pel descobriment i perfilat dels dispositius IoTs en la PoC són els enumerats a continuació.

Col·lectors Perfilat dispositius de xarxa	
Col·lector	**Descripció**
DHCP	Reenviament dels paquets de DISCOVER, REQUEST i INFORM dels dispositius commutadors i tallafocs cap la solució de NAC mitjançant l'opció de configuració DHCP Relay.
SNMP	Configuració de la solució de NAC per la lectura de MIBs de SNMP per tal descobrir dispositius amb IP estàtica en la xarxa. Configuració SNMP en el commutador per tal pugui compartir la informació de la seva taula ARP amb el CPPM.
Escaneig de xarxa	Escanejos de les diferents xarxes corporatives.
LLDP	Activació del protocol de *Link Layer Discovery* en el commutador. La informació descoberta s'envia al CPPM via Radius mitjançant paquets d'accounting.
CDP	Activació del protocol de *Cisco Discovery* en el commutador. La informació descoberta s'envia al CPPM via *Radius* mitjançant paquets d'*accounting*.

Taula 10: Col·lectors perfilat - PoC

6.6 Flux de control d'accés

A continuació es detalla el flux de control d'accés dissenyat per protegir l'entorn dels dispositius IoTs, i el qual serà objecte d'estudi i validació.



- Qualsevol dispositiu IoT que es connecti a la xarxa de dades ha de ser identificat mitjançant per algun dels mètodes de perfilat configurat. Durant, i mentre no s'obtingui un perfilat del dispositiu, el dispositiu IoT quedarà ubicat en una vlan de quarantena, aïllat de la xarxa de producció.

- Un cop perfilat el dispositiu IoT, es determinarà si és un dispositiu IoT autoritzat per accedir a la xarxa corporativa de la PoC. En cas contrari, se li denega l'accés a la xarxa de dades.

- identificat que s'està davant d'un dispositiu IoT autoritzat, s'ha de validar si existeix algun tipus d'incongruència respecte a un perfilat anterior i conegut del dispositiu per tal de detectar una possible suplantació

d'identitat. En el cas d'identificar algun tipus de conflicte de perfilat, el dispositiu IoT ha de quedar ubicat en la vlan de quarantena.

- Validat de que no hi ha cap incongruència del dispositiu IoT, aquest ha de ser autoritzat per accedir als recursos corresponents, vlan, segons el seu perfilat i rol de dispositiu.

- El cas de que l'ecosistema de dispositius de seguretat detectin algun tipus de risc procedent dels dispositiu IoT que pogués comprometre la seguretat corporativa, aquest ha de ser aïllat a la vlan de quarantena.

6.7 Polítiques de seguretat aplicades

Segons el flux de control d'accés dissenyat en l'apartat anterior, es configuren unes polítiques inicials d'autenticació i autorització dels dispositius IoT de la PoC, així com també unes polítiques post autenticació , les quals es mostren en les següents taules.

Polítiques d'autenticació de dispositius IoT PoC			
Dispositiu IoT	**Autenticació mitjançant perfilat**	**Resultat**	**Autorització**
Telèfon VoiP	Category = VoIP Phone OS Family = Cisco Hostname contingui SEP MAC = Cisco Systems, Inc	OK	Vlan 92 (VoIP)
		KO	Vlan 90 (quarantena)
Punt d'accés	Category = Access Point OS Family = Cisco Hostname contingui ap MAC = Cisco Systems, Inc	OK	Vlan 66 (AP)
		KO	Vlan 90 (quarantena)

Taula 11: Polítiques seguretat implementades - PoC

Polítiques Post autenticació de dispositius IoT PoC		
Dispositiu IoT	**Detecció de Risc per part del Palo Alto**	**Autorització**
Telèfon VoiP	OK	Vlan 90 (quarantena)
Punt d'accés	OK	Vlan 90 (quarantena)

Taula 12: Polítiques Post autenticació implementades - PoC

6.8 Validacions de la solució

Les proves de funcionament realitzades en la PoC s'han dividit en dos escenaris d'estudi.

- Un primer escenari de connexió lícita o no mal intencionada d'un dispositiu IoT, on l'objectiu d'aquest escenari és el de validar el descobriment del dispositiu IoT, la seva correcte categorització,

l'assignació de rol corresponent i finalment, la seva autorització i informació del dispositius al ecosistema de seguretat, tallafocs.

- Un segon escenari de connexió il·lícita o mal intencionada, on l'objectiu d'aquest escenari és el de validar la capacitat de la solució de control d'accés a l'hora de detectar intents de suplantació d'identitat i amenaces des de dispositius IoTs compromesos.

6.8.1 Validació connexions lícites dels dispositius IoTs

A continuació es mostra la taula de les validacions que s'han portat a terme per a comprovar el funcionament de les solució de control d'accés a la xarxa de dades davant les connexions lícites de diferents dispositiu IoT. Les evidencies d'aquestes validacions queden recollides en l'apartat d'annexes d'aquest document.

Validacions connexions lícites dispositius IoTs				
ID	**Validació**	**Resultat**	**Descripció**	**Comentaris**
A.1.1	Perfilat Telèfon IP	**OK**	Identificació del dispositiu IoT a través d'algun dels col·lectors configurat.	En el cas del telèfon IP podem veure que s'obté informació de perfilat mitjançant els col·lector configurats de DHCP, CDP i SNMP.
A.1.2	Perfilat Punt Accés Wi-Fi	**OK**		En el cas de l'AP veiem que només s'obté informació del col·lector de DHCP
A.1.3	Perfilat descobriment dispositius desconeguts	**OK**		En la base de dades d'*Endpoint*s del CPPM es pot veure que s'han descobert molts dispositius connectat en el laboratori, que d'entrada no teníem coneixement que hi estaven connectats
A.1.4	Perfilat dispositiu no admès	**OK**		Es valida que en el cas de perfilar un dispositiu que no compleix cap política de seguretat d'admissió a la xarxa, aquest queda ubica en la vlan de quarantena.
A.2.1	Autenticació Telèfon IP	**OK**	Autenticació mitjançant el perfilat dels dispositius.	El telèfon IP, un cop perfilat, s'autentica correctament segon els atributs de perfilat definits en la política de seguretat.
A.2.2	Autenticació Punt Accés Wi-Fi	**OK**		El Punt d'Accés , un cop perfilat, s'autentica correctament segon els atributs de perfilat definits en la política de seguretat.
A.3.1	Autorització Telèfon IP	**OK**	Depenent del perfilat i rol obtingut mitjançant la autenticació, el dispositiu queda ubicat a la vlan corresponent amb l'autorització marcada per la política de seguretat implementada.	Es valida que el telèfon IP queda assignat a la vlan 92 corresponent a la xarxa de telefonia.
A.3.2	Autorització Punt Accés Wi-Fi	**OK**		Es valida que el Punt d'Accés Wi-Fi queda ubicat en el vlan 66 corresponent a la part de xarxa sense fils.

A.3.3	Autorització altres dispositius IoTs	**OK**		Es valida que els dispositius no identificat per perfilat o identificats però que no compleixen la política de seguretat establerta per ser admesos, queden ubicats a la vlan 90 de quarantena.
A.4	Integració amb Palo Alto	**OK**	El tallafocs Palo Alto disposa de polítiques d'accés basades en rols assignats als diferents dispositius per la solució de control d'accés.	Es valida que el telèfon IP en el moment que se li assigna el rol de Telefon VOIP se li apliquen les regles del Tallafocs referents a la telefonia. En el moment en que la solució de control d'accés li assigna el rol de Quarantena, es valida que en el tallafocs se li apliquen les regles corresponents als dispositius en Quarantena.
		OK		Es valida que el punt d'accés Wi-Fi en el moment que se li assigna el rol de Punt Acces WI-Fi se li apliquen les regles del Tallafocs referents aquest rol. En el moment en que la solució de control d'accés li assigna el rol de Quarantena, es valida com en el tallafocs se li apliquen les regles corresponents als dispositius en Quarantena
A.5	Post autenticació	**OK**	Per la realització d'aquesta prova s'ha utilitzat un PC per simular un IoT vulnerat com a Bonet. Des del PC s'intenta accedir a una web maliciosa que faci saltar les proteccions de seguretat del Palo Alto i aquest interaccioni amb el ClearPass (syslog) per tal bloquegi el port del dispositiu IoT (en el nostre cas un PC).	S'ha pogut validar com el Palo Alto envia mitjançant syslog la informació de la detecció de l'equip IoT compromès. La informació de syslog es interpretada correctament pel ClearPass i aquest aïlla el dispositiu assignat el seu port a la vlan 90 de quarantena.

Taula 13: Validacions connexions lícites dispositius - PoC

6.8.2 Validació connexions malintencionades

Validacions connexions il·lícites dispositiu IoT				
ID	**Validació**	**Resultat**	**Descripció**	**Comentaris**
B.1	Perfilat de dispositiu	**OK**	Connexió a la xarxa amb IP estàtica per tal no ser identificar pel col·lector d'atributs mes utilitzats, el DHCP	D'entrada el dispositiu no queda perfilat. La política d'autorització no permet accedir a la xarxa sense un perfil definit i per tan, el dispositiu queda ubicat a la vlan de quarantena, vlan 90.

B.2	Suplantació Identitat	**OK**	Intent de connexió a la xarxa de dades cablejada amb intent de suplantació d'identitat d'un dispositiu IoT conegut pel sistema de control d'accés, en aquest cas un telèfon IP, modificant la adreça MAC del dispositiu portàtil Windows 10	Les dues solucions de control d'accés han identificat mitjançant el perfilat que no es tracte d'un telèfon IP sinó d'un PC amb windows 10 i ha estat assignat a la vlan de quarantena.
B.3	Post autenticació	**OK**	Per la realització d'aquesta prova s'ha utilitzat un PC per simular un IoT vulnerat com a Bonet. Des del PC s'intenta accedir a una web maliciosa que faci saltar les proteccions de seguretat del Palo Alto i aquest interaccioni amb el ClearPass (syslog) per tal bloquegi el port del dispositiu IoT (en el nostre cas un PC).	S'ha pogut validar com el Palo Alto envia mitjançant syslog la informació de la detecció de l'equip IoT compromès. La informació de syslog es interpretada correctament pel ClearPass i aquest aïlla el dispositiu assignant la vlan 90 de quarantena al port del commutador on està connectat l'equip compromès.

Taula 14: Validacions connexions il·lícites dispositiu IoT

6.9 Conclusions

L'efectivitat del funcionament dels diferents mètodes de perfilat i de la identificació dels dispositius que ofereixen els sistemes de control d'accés d'última generació, són la clau per a protegir les xarxes de dades de la connexió de dispositius IoTs no autoritzats, i per protegir també els dispositius IoTs autoritzats d'una possible suplantació d'identitat.

En aquest sentit, s'ha pogut corroborar en la PoC que les dues solucions de control d'accés testejades, ClearPass i ISE, ofereixen la possibilitat d'utilitzar un número considerable de col·lectors pel descobriment i perfilat de dispositius IoTs, com per exemple, DHCP, ARP, SNMP, CDP, LLP, entre d'altres.

Pel que fa a l'efectivitat real del descobriment dels dispositius connectats a la xarxa de dades i la recopilació d'informació per la realització del perfilat, s'ha pogut comprovar que la integració del col·lector de RELAY de DHCP amb el sistema de control d'accés és molt rellevant a l'hora de minimitza, significativament, el temps de descobriment i classificació dels dispositius IoT en comparació amb la resta de col·lectors suportats.

Quan es descobreix un dispositiu mitjançant les peticions que aquest realitza al servidor DHCP per adquirir una adreça IP, aquestes peticiones es transmeten cap el sistema de control d'accés just en el precís moment en que el dispositiu sol·licita una adreça IP, RELAY de DHCP.
Molt diferent succeeix amb la resta de col·lectors configurables en les solucions de NAC, on podríem dir que la iniciativa de descobriment la pren la solució de control d'accés en forma de consultes programades cap els diferents col·lectors, la qual cosa provoca un retard de descobriment i perfilat notable en comparació amb el col·lector de DHCP.

No obstant això, el fet de no disposar d'un perfilat ràpid del dispositiu IoT, no provoca un problema de seguretat, sempre i quan el dispositiu no hagi estat mai perfilat anteriorment. Els sistemes de control d'accés permeten configurar una política de seguretat la qual ubica els dispositius no perfilats en una vlan de quarantena fins que hagin estat identificats o perfilats. Tanmateix, si que aquest fet podria provocar un problema de rendiment funcional del dispositiu IoT en alguns determinats casos d'ús.

Paral·lelament, si que provocaria un problema "temporal de seguretat" el cas en el que el dispositiu IoT hagi estat perfilat i catalogat prèviament, és a dir, en el cas en el que els dispositiu sigui un dispositiu conegut per la solució de control d'accés, i un atacant intenti realitzar una suplantació d'identitat, configurant-se en el seu dispositiu una IP estàtica amb la MAC dels dispositiu IoT i desconnectant-lo de la xarxa.

Els dispositius que són perfilats queden enregistrat en la base de dades del sistema de control d'accés permetent-los, d'aquesta manera, una autenticació i autorització ràpida a la xarxa. En el cas anterior de suplantació d'identitat d'un dispositiu IoT, l'atacant pot accedir a la xarxa de dades durant uns minuts fins que el sistema de control d'accés és capaç de perfilar el dispositiu mitjançant les diferents consultes programades als col·lectors. En aquest moment el dispositiu es detectat, perfilat i bloquejat en una vlan de quarantena.

Pel que fa als mètodes de descobriment de dispositius per escaneig programats, tot i que semblen efectius en la cerca massiva de dispositius, una utilització freqüent podrien provocar incidents de connectivitat i rendiment en les xarxes de dades en producció. Per tant, podríem dir que aquests mètodes d'escaneig són mètodes de descobriment per ser utilitzats de manera puntual i no com un mètode habitual.

S'ha pogut validar també que la solució de NAC de ClearPass s'integra via API XML amb la solució de tallafocs de Palo Alto. La solució de NAC de ClearPass envia la correlació de IP/Rol assignats als dispositius IoTs cap al tallafocs de Palo Alto per tal que aquest pugui utilitzar aquesta informació en les seves polítiques de seguretat.

En sentit contrari, el Palo Alto s'integra amb la solució de NAC de ClearPass, enviant els events de seguretat via syslog cap el ClearPass, el qual actua de servidor de syslog. La solució de ClearPass es capaç de llegir els events de seguretat, la IP i Rol del dispositiu que el dispara, i realitzar una acció de post autenticació per bloquejar el port on està connectat.

7 Conclusions

En aquest apartat, s'exposen les diferents conclusions a les quals s'han arribat després de l'estudi i de l'anàlisis de la utilització dels sistemes de control d'accés a les xarxes de dades d'última generació (NAC), com la solució a la problemàtica de seguretat que presenten els dispositius IoTs instal·lats dins de les organitzacions.

7.1 Descripció de les conclusions del treball

A continuació es descriuen les conclusions finals obtingudes del treball de TFM realitzat, així com també algunes lliçons apreses durant el seu desenvolupament.

- Els riscos de seguretat que presenten els dispositius IoTs, i que s'enfronten les organitzacions, van en augment a mesura que van incorporant dispositius IoTs en la seva infraestructura de xarxa com a solucions a les diferents necessitats corporatives que van sorgint.

- Actualment, hi ha ja masses dispositius IoTs en producció en les empreses, i de tipus molt diferents, per esperar a curt termini un estàndard uniforme que garanteixi la seva seguretat, i la seguretat del seu entorn.

- Es molt complicat aplicar mesures de seguretat sobre allò que no es té constància, o realitzar un manteniment de protecció individual de tots i cada un dels dispositius IoTs corporatius instal·lats en una companyia, així doncs, és crític per les organitzacions de dotar-se d'eines d'automatització per a descobrir, identificar i protegir tots els dispositius IoTs instal·lats en les seves infraestructures de xarxa de dades.

- S'ha pogut corroborar, mitjançant l'estudi teòric i pràctic realitzat, que els sistemes de control d'accés d'última generació proporcionen, a través dels diferents mètodes de perfilat de dispositius, un nivell de protecció elevat i acceptable davant els riscos de seguretat que presenten els dispositius IoTs per la seva manca de recursos destinats a l'autenticació i protecció pròpia.

- Pel que fa a l'efectivitat real del descobriment dels dispositius IoTs connectats a la xarxa de dades, i la recopilació d'informació per la realització del seu perfilat d'identificació, s'ha pogut comprovar que la integració del col·lector de RELAY de DHCP amb la solució del sistema de control d'accés a les xarxes de dades, és molt rellevant a l'hora de minimitza significativament els temps de perfilat dels dispositius IoTs descoberts.

- Les integracions de les solucions de NAC amb dispositius de tercers encara estan força limitades a determinats productes de seguretat en

concret (principals fabricants i productes del mercat) i a versions determinades dels seus sistemes operatius. Això pot crear dubtes i desconfiança a l'hora de implementar certes integracions pel fet que, una actualització freqüent d'un dels productes de l'ecosistema de seguretat, pot desmuntar la integració implementada.

- No podem aferrar-nos en que les solucions de control d'accés a les xarxes de dades són una solució complerta davant els riscos de seguretat que presenten els dispositius IoTs. Cal també que cada organització dissenyi la seva pròpia estratègia específica de seguretat per tal de reduir-ne la seva exposició i risc.

- Després d'una descoberta de dispositius IoTs en una xarxa de dades, és recomanable investigar sobre com protegir els dispositius IoTs més nombrosos trobats, i treballar aquesta estratègia de protecció amb els venedors, distribuïdor o fabricants dels dispositius IoTs.

- Una segmentació correcte de la xarxa de dades atura el moviment lateral d'exploits i redueix la superfície d'atac. Es recomanable implementar segments de xarxa aprofitant els tallafocs per tal de limitar l'accés entre segments, així com cap a Internet, aprofitant les característiques d'inspecció de tràfic que ofereixen els tallafocs actuals de tercera generació.

- Disposar d'una solució centralitzada de monitorització de tots els dispositius de seguretat que es tinguin implementats en la infraestructura de xarxa és fonamental per tal d'identificar i d'analitzar dispositius IoTs amb comportaments de risc.

7.2 Avaluació dels objectius assolits

A continuació es realitza una valoració del compliments dels objectius marcats a l'inici del TFM.

Objectius Específics

- **Estudi i investigació dels diferents mètodes utilitzats en les solucions actuals de control d'accés a les xarxes de dades pel que fa al descobriment, identificació i autorització de dispositius IoTs.**
  Aquest objectiu es pot considerar complert, ja que s'ha pogut investigar i estudiar, amb força detall i entrant en profunditat, els diferents mètodes de descobriment i identificació de dispositius que utilitzen les solucions actuals de NAC, les quals estan basades amb els diferents serveis comuns desplegats a les xarxes de dades com a col·lectors d'atributs dels dispositius IoTs descoberts, per tal de perfilar-los i identificar-los.

- **Anàlisis dels principals fabricants del mercat de les solucions de control d'accés a xarxes de dades, amb l'objectiu de conèixer quina cobertura ofereixen sobre les solucions i tècniques estudiades anteriorment pel que fa al descobriment i control d'accés dels dispositius IoTs. Analitzar també, quins trets diferenciadors pot tenir cada solució en front la seva competència.**
  Aquest objectiu a quedat cobert parcialment, ja que, per una banda, s'han pogut cercar i analitzar quins són els cinc principals fabricants de solucions de control d'accés a les xarxes de dades del mercat Europeu. Per una altra banda, s'ha presentat una descripció de les principals funcionalitats que presenten aquestes solucions a nivell individual, però a mancat la presentació d'una taula comparativa dels trets diferenciadors de cada solució en front la seva competència.
  El motiu pel qual no s'ha assolit aquest objectiu ve donat per a una maca de temps físic per extreure la informació requerida dels documents tècnics específics de la solució de cada fabricant, i enfrontant-los entre ells, per tal d'obtenir la taula comparativa que se n'esperava.

- **Disseny i realització d'una prova de concepte d'una de les solucions de control d'accés estudiades anteriorment, amb l'objectiu d'avaluar-ne la seva efectivitat real pel que fa a la descoberta, identificació i protecció dels dispositius IoTs d'una organització.**
  Aquest objectiu es pot considerar com a complert, ja que s'ha pogut portat a terme una prova de concepte de dues solucions NAC punteres en el mercat, ClearPass i ISE, i on s'ha pogut validar la part pràctica de les dues solucions de NAC, amb la part teòrica estudiada referent a la protecció dels dispositius IoTs.

Objectius Personals

- **Aprofundir en els coneixements tècnics, teòrics i pràctics, sobre les solucions de seguretat i de control d'accés a les xarxes privades de dades, en concret sobre la protecció dels dispositiu IoTs corporatius.**
  Penso que personalment he fet un avanç important pel que fa a coneixements adquirits sobre la problemàtica real de seguretat que presenten els dispositius IoTs, així com quines solucions actuals es poden aplicar per tal de mitigar-ne el seu risc.

- **Conèixer les dificultats i dependències tècniques a baix nivell de la implementació i la integració d'una solució de control d'accés dins d'un eco sistema de Ciberseguretat empresarial.**
  Durant la realització de la PoC, he ensopegat amb dificultats tècniques per a poder portar a terme les integracions de les solucions de NAC testejades amb el tallafocs de Palo Alto utilitzat en la PoC com a prova d'integració. Per una banda, la solució de NAC de ClearPass no interpretava correctament el format de syslog enviat per tallafocs. Per un altra banda, la solució de NAC d'ISE requereix d'una màquina Linux pont, amb el software anomenat Gridmeld, per tal d'integrar-se

correctament amb el tallafocs de Palo Alto, En aquest última cas, i per un tema de mancat temps per complir terminis d'entrega del TFM, he vist obligat a renunciar a la prova d'integració.

- **Culminar els estudis del Màster Universitari en Ciberseguretat i Privadesa.**
  Aquest objectiu queda pendent, a expenses de conèixer el resultat final i la nota obtinguda pel tribunal avaluador del TFM.

7.3 Seguiment de la planificació establerta

Pel que fa a la planificació establerta a l'inici del projecte, aquesta a patit un retard considerable, que a repercutit clarament en la data d'entrega final del mateix.

Aquest retard ha vingut donat per un plantejament inicial personal erroni de l'estructura del TFM que, gràcies a l'acompanyament del meu consultor i tutor assignat, s'ha pogut reconduir.

El projecte també ha patit un retard important en els seu avanç quan s'ha arribat a la part de la integració de les solucions de NAC amb la solució de tallafocs de Palo Alto. Com s'ha comentat en el punt anterior referent a l'avaluació dels objectius assolits, han sorgits dificultats tècniques que han retard la culminació del projecte.

7.4 Línies de treball futur

Assolits gairebé la totalitat dels objectius inicials marcats en aquest TFM, a continuació es presenten varies línies de treball que es podrien seguir en un futur per tal de millorar i ampliar els estudis realitzats.

- Ha quedat pendent, pel que fa a l'apartat de la realització de la PoC, la implementació amb èxit de la integració de la solució NAC de Cisco ISE amb el tallafocs de Palo Alto, per tal de validar el correcte funcionament de la una solució de seguretat post autenticació dels dispositius IoTs.

- L'estudi de les solucions de Maching learning, o de l'aprenentatge automàtic de patrons de comportament, que ajudin a determinar amb mes fiabilitat el tipus de dispositius connectat a la xarxa, així com el seu està de salut, podria ser una línia nova d'estudi per ampliar la part de perfilat estudiat en aquest TFM.

- El concepte de confiança cero dels dispositius connectats a la xarxa de dades d'un organitzacions, conjuntament amb les solucions de microsegmentació per aturar els atacs laterals dels dispositius infectats, podrien ser també dos línies futures de treball molt interessants a realitzar.

8 Glossari

BYOD: Porta el teu propi dispositiu **(**Bring Your Own Device) és una política empresarial la qual els empleats poden utilitzar els seus propis dispositius personals en el seu lloc de treball i tenir accés als recursos de l'empresa

CAGR: Tassa de creixement anual compost (Compound Annual Growth Rate) és un terme específic de negocis e inversió que fa referència al guany anualitzat d'una inversió sobre un període de temps.

Ciberamenaces: activitats malicioses que tenen lloc en un entorn digital, ja sigui un ordinador de sobretaula, portàtil, mòbil, tauleta…

Ciberseguretat: Àrea relacionada amb la informàtica i la telemàtica que s'enfoca en la protecció de la infraestructura computacional i tot el vinculat amb aquesta.

COVID-19: Coronavirus Disease y 2019. Malaltia provocada pel coronavirus SARS-CoV-2.

CPU: Unitat Central de processament (Central Processing Unit), és el component de l'ordinador i d'altres dispositius, que interpreta les instruccions contingudes en els programes i processa les dades.

DDoS: Atac de denegació de servei (distribuited denial of service attack) és una incursió contra la seguretat informàtica.

DHCP: (Dynamic Host Configuration Protocol) és un protocol de xarxa que permet als nodes d'una xarxa IP obtenir els seus paràmetres de configuració automàticament.

EAP: Protocol d'autenticació extensible (Extensible Authentication Protocol) es un marc arquitectònic que proporciona extensibilitat pels mètodes d'autenticació per les tecnologies d'accés a les xarxes protegides, com són els accessos a les xarxes sens fils, cablejades, xarxes privades virtuals.

GPU: Unitat de Procés Gràfic (Graphic Processing Unit) és un dispositiu dedicat a la generació de gràfics per a ordinadors personals, estacions de treball o consoles de videojocs.

IEEE: Institut d'Enginyers Elèctrics i Electrònics (Institute of Electrical and Electronics Engineers), una associació tècnico-professional mundial dedicada a l'estandardització, entre altres coses.

IPS: Sistema de Prevensió d'Intrusos (intrusion Prevention System) és un software que s'utilitza per protegir els sistemes d'atacs i intrusions.

IoT: EL Internet de les coses (Internet Of Things) és un concepte que es refereix a un interconnexió digital d'objectes quotidians amb internet.

IT: Departament de Tecnologia de la informació, sovint s'anomena al departament que s'encarreguen de l'equipament de telecomunicacions d'una organització.

MAC: (Media Access Control) és una adreça Unicast que identifica a una interfície de xarxa de maquinari quasi de manera única.

MDM: Gestor d'aplicacions Mòbils (Mobile Device Management) és un administrador de dispositiu mòbils.

NAC: Control d'accés a xarxa (Network Access Control) és un enfoc de la seguretat en xarxes de computadors que intenta unificar la tecnologia de seguretat en els equips finals, usuaris o sistema d'autenticació i reforçar la seguretat d'accés a la xarxa.

NOC: Centre d'operacions de xarxes (Network Operation Center) és un centre on els analistes de Ciberseguretat treballen per supervisar els sistemes de telecomunicacions.

PC: Ordinador Personal (Personal Computer) és qualsevol ordinador amb un preu, mida i possibilitats que el fan útil per a persones individuals, i que està pensat per ser operat directament per l'usuari final, sense intervenció de cap operador/a.

PoC: Prova de Concepte (Proof o concept) és una implementació, sovint resumida o incompleta, d'un mètode o d'una idea, realitzada amb el propòsit de verificar que el concepte o la teoria en qüestió és susceptible de ser explotada d'una manera útil.

RADIUS: (Remote Authentication Dial-In User Server) és un protocol d'autenticació i autorització per a aplicacions d'accés a la xarxa o mobilitat.

RGPD: Reglament General de Protecció de Dades, és un reglament europeu mitjançant el qual l'Eurocambra, el Consell de la Unió europea i la Comissió Europea pretenen enfortir i unificar la protecció de dades del tots els països del a Unió europea, controlant també la transferència de dades fora de la Unió.

SGSI: Un Sistema de Gestió de la Seguretat de la Información és un conjunt de polítiques d'administració de la informació.

SIEM: Informació de Seguretat i Gestió d'Esdeveniment (Security Information Event Management) són productes i serveis de programari que combinen la gestió de la informació de seguretat amb la gestió d'esdeveniment de seguretat. Aquests productes i serveis proporcionen anàlisis en temps real de les alertes de seguretat generades per aplicacions i maquinari de xarxa.

SMNP: (Simple Network Management Protocol) és un protocol de capa d'aplicació basat en IP que intercanvia informació d'administració entre dispositius de xarxa.

SOC: Centre d'Operacions de la Seguretat (Security Operation Center) és un centre on els analistes de Ciberseguretat treballen per supervisar els sistemes de telecomunicacions.

TFM: Treball Final de Màster

UART: Transmissor-Receptor Asíncron Universal (Universal Asynchronous Receiver Transmitter) és el dispositiu que controla els ports i dispositius sèrie. Es troba normalment integrat en la placa base o en la targeta adaptadora d'un dispositiu.

VLAN: Xarxa d'Area Local Virtual (Virtual LAN) és un mètode de crear xarxes lògicament independents dins d'una mateixa xarxa física.

9 Bibliografia

9.1 Llibres consultats

- Aaron Woland, Vivek Santuka, Chad Mitchell, Jamie Sanbower. “Integrated Security Technologies and Solutions”. Cisco Press. Apr.6.

- Aaron Woland, Katherine McNamara. “CCNP Security Indentity Management”. Cisco Press. Dec 22, 2020

9.2 Planes web consultades

Comparatives de solucions NAC

- Aruba. “Aruba ClearPass versus Cisco ISE”. URI:https://afp.arubanetworks.com/afp/index.php/Competitive:_Aruba_ClearPass_versus_Cisco_ISE

- Aruba: “Fortinet and ClearPass”. URI: https://afp.arubanetworks.com/afp/index.php/Fortinet

- Cisco. “Compare Network Access Control Solutions”. URI: https://www.cisco.com/c/en/us/products/security/identity-services-engine/competitive-comparison.html#~competitive=0+1+2+3

- Fortinet. “Data Sheets FORTINAC”. URI:https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf

- Forescout. “Control de acceso a la red moderno”. URI: https://forescouttechnologies.es/resources/control-de-acceso-a-la- red-moderno/

Guies d’instal·lació

- Aruba. “Aruba ClearPass Policy Manager Deployment Guide”. URI:https://www.arubanetworks.com/techdocs/ClearPass/6.9/Aruba_DeployGd_HTML/Content/home.htm

- Aruba. “ClearPass and Palo Alto Networks Integration Guide”. URI: https://www.paloaltonetworks.com/resources/techbriefs/aruba-networks-clearpass-integration-guide

- Cisco. “Cisco Identity Services engine Installation Guide, Release 3.0”. URI:https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/install_guide/b_ise_InstallationGuide30.html

- Cisco. “ISE Security Ecosystem Integration Guide”.

URI:https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216120-ise-security-ecosystem-integration-guide.html#anc88

Mercat solucions control d'accés

- CCN. "Taxonomia de productos STIC-Anexo A.1: Dispositivos de Control de Acceso a Red" URI: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3869-guia-140-anexo-a-1-control-de-acceso-a-red-nac/file.html

- Fortinet . "FortiNAC:Control de acceso a red" URI: https://www.fortinet.com/lat/products/network-access-control

- Gartner. "Market Guide for Network Access Control". URI:https://www.gartner.com/doc/reprints?id=1-26B9LRC6&ct=210603&st=sb

- Genians. "Genians Responds to Garrner's May 202 Maket Guide for Netowkr Access Control". URI: https://www.genians.com/learn-more/insights/genians-responds-to-gartners-may-2020-market-guide-for-network-access-control/

Seguretat en dispositius IoTs

- Barbara. "recomendaciones para garantizar la Seguridad en IoT industrial". URI:https://barbaraiot.com/blog/recomendaciones-para-garantizar-seguridad-iot-industrial/

- CCN-CERT. "Buenas Practicas – Internet de las Cosas". URI: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2258-ccn-cert-bp-05-internet-de-las-cosas/file.html

- INCIBE. "La importància de la Seguridad en IoT. Principales amenazas". URL:https://www.incibe-cert.es/blog/importancia-seguridad-iot-principales-amenazas

- INCIBE. "Temáticas IoT". URL: https://www.incibe.es/protege-tu-empresa/tematicas/iot

- PALO ALTO. "8 Stages of the IoT Attacl Lifecycle" URL: https://www.paloaltonetworks.com/resources/8-stages-of-the-iot-attack-lifecycle

- FORESCOUT. "IoT Security". URI: https://www.forescout.com/resources/internet-things-solution-brief/

10 Annexos

10.1 Llistat vulnerabilitats dispositius IoTs

A continuació, és mostra una taula detallada amb el conjunt i la descripció de les vulnerabilitats detectades segons els diferents fronts per on els ciberdelinqüents podent aconseguir fer-se amb la infraestructura IoT, o amb les dades que aquests dispositius recopilen.

Superfície d'atac	Vulnerabilitat
Control d'accés a l'ecosistema	Confiança implícita entre tots els components del sistema.
	(In)Seguretat en el registre de components (enrollment)
	La retirada o jubilació d'equips (desmantellament)
	Pèrdua de credencials i procediments d'accés.
Memòria del dispositiu	Noms d'usuari i contrasenyes en clar.
	Credencials de tercers en clar
	Claus de xifratge en clar.
Interfícies físiques del dispositiu	Extracció del firmware
	Interfície de línia d'ordres d'usuari i administrador
	Possibilitats d'escalar privilegis
	Esborrat (Reset) a un estat insegur.
	Extracció dels medis d'emmagatzematge
	(No)Resistència a les manipulacions físiques del dispositiu
	Presència de ports de depuració (per exemple, JTAG17)
	Exposició de número de sèrie o identitat del dispositiu
Interfície Web del dispositiu	Injecció SQL, Cross-site scripting i Cross-site Request Forgery
	Extracció i llistat de noms d'usuari vàlids
	La presència de contrasenyes febles
	Possibilitat de bloquejar comptes
	Existència de credencials per defecte
El firmware del dispositiu	Credencials incrustades en el codi
	Divulgació d'URL i informació sensible
	Presència de claus d'encriptació clares
	El Alteració de xifratge (simètric i asimètric)
	Visualitza la versió de microprogramari i/o la data de l'última actualització
	Comptes d'usuari oblidats que actuen com a backdoors
	Serveis vulnerables actius (web, ssh, tftp, etc.)
	Exposició de les API de seguretat del dispositiu
	Possibilitat de tornar a una versió anterior insegura
Serveis de xarxa del dispositiu	Divulgació d'informació
	Interfície de línia per a usuaris i per a l'administrador
	Possibilitats d'injecció de codi
	Denegació de servei

	L'existència de serveis no xifrats
	L'ús de xifratges mal implementats
	presència de serveis de prova i/o desenvolupament no suprimits en escenaris de producció
	Problemes de desbordament de la memòria intermèdia en el programari
	UPnP18 i serveis udp vulnerables
	Les possibilitats d'èxit en els atacs DOS (denegació del servei)
	L'actualització On The Air (OTA) del firmware i del dispositiu
	Falta de verificació de dades o càrregues de codi
	No verificar la integritat dels missatges, ja siguin dades o ordres
Interfície administrativa	Injecció SQL, Cross-site scripting i Cross-site Request Forgery
	Mecanismes vàlids de descobriment de noms d'usuari
	La presència de contrasenyes febles i credencials per defecte conegudes
	Possibilitat de bloqueig de comptes
	L'absència d'opcions de seguretat/xifratge i logging segur
	La no autenticació amb doble factor
	Incapacitat per netejar amb seguretat el dispositiu (wipe)
Emmagatzematge local de les dades	La presència de dades no xifrades i/o xifrat amb claus compromeses
	La manca de controls d'integritat de dades
	L'ús de la mateixa clau de xifratge/desxifratge per a totes les dades
Interfície Web amb el Cloud	Injecció SQL, Cross-site scripting i Cross-site Request Forgery
	El descobriment de noms d'usuari vàlids
	Presència de contrasenyes febles i credencials per defecte
	El possible bloqueig de comptes
	El no xifrat del que es transporta o es comunica
	La presència d'un mecanisme de recuperació de claus i contrasenyes que és insegur
	La no autenticació amb doble factor
Backend API de terceres parts	Enviament no xifrat d'informació personal
	El mode d'encriptació d'informació personal i d'identificació
	La divulgació d'informació dins del dispositiu
	Divulgació de la ubicació del dispositiu
Mecanismes d'actualització	Aquestes actualitzacions s'envien sense xifrar
	Que les actualitzacions no vinguin signades correctament
	Que l'URL de les actualitzacions sigui modificable
	que no existeix o sigui ineficaç la verificació d'actualitzacions, o la falta d'autenticació de les mateixes
	Possibilitat d'instal·lar actualitzacions malicioses
	La pèrdua temporal o permanent del mecanisme d'actualització
	Absència d'un mecanisme d'actualització manual
Aplicació mòbil	L'existència de credencials per defecte i/o l'acceptació o ús de contrasenyes febles
	Emmagatzematge insegur de dades

	L'absència o encriptació inadequada del que es transporta
	Un mecanisme insegur de recuperació de contrasenyes i claus
	Absència d'autenticació de doble factors
Backend API de proveïdors	Acceptar com a confiança inherent en el núvol o les aplicacions mòbils
	Mecanismes d'autenticació febles
	Controls d'accés inexistents o febles
	Possibilitat d'atacs d'injecció amb èxit
	La presència de serveis ocults i funcionalitats indocumentades
Comunicació de l'ecosistema	L'absència o l'abús dels controls de l'estat de salut total del sistema
	Proves de funcionament correcte (Heartbeat) del sistema.
	La (in)seguretat de les ordres que operen l'ecosistema
	La desprovisionament de recursos o capacitats
	El forçat de les actualitzacions
Tràfic de xarxa	La pròpia xarxa local (LAN)
	El salt de la LAN a Internet (router, proxy, tallafocs, etc.)
	Trànsit de xarxa Connexions aèries de curt abast
	La no estandardització de protocols i/o procediments
	Les pròpies xarxes sense fils (Wi-Fi, Z-wave, Zigbee, Bluetooth)
	La possibilitat d'analitzar els dispositius amb tècniques de Protocol fuzzing
Autenticació i autorització	La divulgació de valors relacionats amb l'autenticació/autorització de claus de sessió, token, galetes, etc.
	La reutilització de claus de sessió, fitxes, etc.
	Autenticació i absència d'autenticació dispositiu a dispositiu
	La nul·la o feble autenticació del dispositiu amb l'aplicació i entre el dispositiu i el núvol, i viceversa.
	La no autenticació de l'aplicació amb el núvol, i viceversa
	La manca d'autenticació d'aplicacions web amb el sistema cloud
	Manca de tècniques d'autenticació dinàmic
Privacitat	La divulgació de les dades de l'usuari
	La publicació de la ubicació de l'usuari a través del seguiment del seu dispositiu
	La possibilitat de sistemes amb privacitat diferencial, en els quals uns pocs monitoritzen a tothom i ningú els monitoritza a ells

Taula 15: Llistat de Vulnerabilitats

10.2 Protocols d'autenticació

L'autenticació es el procés de verificació de la identitat d'un usuari o dispositiu que es connecta a un sistema. La efectivitat d'aquest procés ve determinat pels protocols d'autenticació i els mecanismes que s'utilitzen.

- **PAP.** Password Authentiacion Protocol (PAP), és un protocol d'autenticació que es caracteritza per enviar la contrasenya dels usuaris a través de la xarxa al servidor d'autenticació en clar. Això ofereix un risc de seguretat important, ja que un usuari no autoritzat podria capturar paquets de dades mitjançant un analitzador (sniffer) i veure la contrasenya.

  L'avantatge de PAP és que es compatible amb molts tipus de servidors de diferents sistemes operatius. Tanmateix, es recomana de fer-se servir PAP només en cas necessari a nivell de requeriments de compatibilitat.

- **MSCHAP / MSCHAP v2.** És un protocol estàndard d'autenticació que utilitza MD5, un mètode de xifrat unidireccional, que realitza una operació hash en la contrasenya i transmet el resultat hash, en lloc de la contrasenya en sí, a través de la xarxa.

  L'algoritme hash garanteix que la operació no es pugui realitzar mitjançant enginyeria inversa per aconseguir la contrasenya original a partir dels dos resultats hash. Però, CHAP és vulnerable a la suplantació d'un servidor remot. MS-CHAP és la versió de Microsoft de CHAP. MS-CHAPv2 utilitza autenticació bidireccional per tal validar la identitat del servidor, així com la del client. D'aquesta manera s'intenta protegir la vulnerabilitat de la suplantació d'identitat- MS-CHAP també augmenta la seguretat mitjançant l'ús de claus criptogràfiques independents per les dades enviades.

  Les especificacions del CHAP es poden trobar en la RFC 1994.

- **EAP.** Extensible Authentication Protocol (EAP), és un protocol de capa 2 que admet múltiples mètodes d'autenticació. No és un mecanisme d'autenticació com a tal. Les especificacions es poden trobar en la RFC 5247.

  Originalment EAP va ser dissenyat per a comunicacions PPP (punt a punt) però mes endavant es va actualitzar per a control d'accés 802.1X basat en ports. Alguns tipus de EAP són propietat de fabricants i alguns tipus de EAP són estàndards. Per exemple, LEAP és propietat de Cisco Systems i PEAP és un estàndard públic. Alguns EAP només poden proporcionar autenticació unidireccional i alguns EAP poden proporcionar autenticació mútua.

  A continuació es detalles el tipus de protocols EAP.

- **EAP-MD5.** Aquest protocol utilitzat el nom d'usuari i contrasenya com a credencials, on només la contrasenya va xifrat per l'algoritme MD5. En aquest cas l'autenticació es unidireccional, només s'autentica el client, no el servidor. Es considera un protocol dèbil a nivell de seguretat.

    - Basat en TLS.
    - Autenticació unidireccional
    - Hash MD5 dèbil

- **EAP-LEAP**. El protocol Lightweight Extensible Indentity Authentication utilitza claus del tipus WEP generades dinàmicament per xifrar la transmissió de dades i realitza un tipus d'autenticació pseudo mútua.

    - Basat en TLS.
    - Autenticació pseudo mutua
    - Hash MS-CHAPv2 dèbil

- **EAP-PEAP.** El protocol d'autenticació extensible protegit per EAP (EAP-PEAP) és un protocol que crea un canal xifrat abans que es produeixi l'autenticació basada e contrasenya. PEAP és un mètode d'autenticació 802.1X que utilitza el certificat de clau pública del servidor per establir un túnel segur en què el client s'autentica amb el servidor.

    L'autenticació PEAP crea un túnel SSL/TLS xifrat entre el client i el servidor d'autenticació. L'intercanvi d'informació es xifra i s'emmagatzema al túnel, garantint que les credencials d'usuari es mantinguin segures.

    - Basat en TLS.
    - Amaga l'intercanvi EAP
    - Requereix autenticació de servidor i client
    - Desenvolupat per Microsoft, Cisco i RSA Security
    - Es va convertir en MS PEAP i EAP GTC

- **EAP-TTLS.** El protocol de túnel de la capa de transport protegit per EAP, igual que PEAP, també fa servir un túnel TLS per a protegir el mètode d'autenticació i proporciona una seguretat similar a l'EAP-TLS, però cada usuari no necessita emetre cap certificat. Els certificats només s'emeten als servidors d'autenticació. Semblant a PEAP, però permet qualsevol protocol d'autenticació EAP. Les especificacions es poden trobar en la RFC 5281.

- **EAP-TLS.** El protocol de capa de transport protegit per EAP (EAP-TLS) requereix un intercanvi de proves d'identitat mitjançant criptografia de clau pública com ara certificats digitals. EAP-TLS assegura aquest intercanvi amb un túnel TLS xifrat que ajuda a resistir atacs de diccionari o d'altres.

    - Basat en TLS i definit en la RFC 5216
    - Utilitza certificats de client i servidors
    - Ofereix autenticació mútua.
    - Suportat en múltiples sistemes operatius.

- **EAP-FAST.** El protocol EAP-Flexible authentication via Secure Tunneling va ser dissenyat per Cisco System per tal reemplaçar el EAP-LEAP el qual s'havia vist es podia desxifrar de manera senzilla.

  EAP-FAST proporciona autenticació mútua i autenticació túnel però en aquest cas no es fa servir un certificat digital basat en l'estàndard X.509 per tal establir el túnel, sinó que utilitza PAC (credencial d'autenticació protegida), es a dir, una espècie de certificat digital, que en realitat es una clau compartida.

    - Basat en TLS i definit en la RFC 4851
    - Utilitza PAC
    - Ofereix autenticació mútua.
    - Suportat en múltiples sistemes operatius.

10.3 Mètodes d'autenticació

A continuació es descriuen el mètodes d'autenticació mes utilitzats en les xarxes corporatives i es fa la anàlisis del seu nivell de seguretat.

- **SSID.** El Service Set Identifier és un ID o nom arbitrari que es configura en les xarxes sense fils per tal segmentar-les lògicament. Tots els dispositius sense fils d'un subconjunt WLAN específic cal que estiguin enganxats en el SSID en concret.

  Tot i que el SSID no està dissenyat per utilitzar-se com un mecanisme de seguretat, ni proporciona privadesa ni autenticació, pot privar l'accés no autoritzat d'usuaris que no tinguin configurat un SSID vàlid per connectar-se a la xarxa WLAN.

- **Autenticació MAC**. L'autenticació basada amb l'adreça fisca, MAC, permet l'accés a la xarxa de tots aquells dispositius amb una adreça MAC coneguda definida en alguna base de dades local o remota. S'utilitza per aquells clients o dispositius sense possibilitat de disposar

d'una solució amb autenticació 802.1X o agent integrat, per exemple dispositius IoTs.

Aquest tipus d'autenticació és molt dèbil donada la facilitat que presenta el fet de suplantar qualsevol adreça MAC d'un dispositiu a nivell de configuració de la targeta de xarxa, per tan, és una tipus d'autenticació gens recomanable en xarxes amb requeriments estrictes de seguretat.

L'autenticació MAC, de vegades anomenada MAC Auth Bypass (MAB), s'utilitza habitualment com a error d'autenticació per a dispositius heretats sense cap capacitat, no compatibles amb 802.1X, com per exemple equips IoTs o usuaris convidats on, en aquest últim cas, es combina amb l'autenticació mitjançant portal captiu. De fet, considerar la autenticació MAC com una autenticació és un error, ja que d'entrada, no s'intercanvien mai credencials d'usuari ni viceversa entre el client i el servidor d'autenticació.

Com que l'autenticació MAC es produeix entre el commutador i el servidor d'autenticació (per exemple RADIUS), no hi ha configuració del client ni interacció. A causa d'aquesta senzillesa, l'autenticació MAC sovint es desplega com a primer pas d'autenticació de xarxa cap a un solució amb 802.1X o com alternativa per a dispositius no compatibles amb 802.1X.

Exemples habituals de dispositius on s'utilitza aquest tipus d'autenticació MAC són majoritàriament dispositius IoTs.

- Controls d'edifici, (climatització, accés de portes, etc)
- Càmeres IPs.
- Reproductors multimèdia
- Impressores-
- Punts d'accés a la xarxa sense fils
- Dispositius VOIP.
- Dispositius mèdics.

- **WPA/WPA2.** Wi-Fi Protected Access (WPA) i la seva versió 2, són protocols d'autenticació de les xarxes sense fils que, no només compleixen el propòsit d'evitar connexions i accessos a les xarxes privades sense fils, si no que al mateix temps també xifren les dades enviades per la xarxa.

  Actualment el protocols WPA es considera un protocol molt dèbil i vulnerable a nivell de seguretat. Per aquesta raó, no es recomana el seu ús i si el del protocol WPA2, el qual aporta l'estàndard de encriptació AES que és molt mes fort que l'estàndard d'encriptació RC4 que fa servir WPA i que ha estat vulnerat infinitat de vegades.

- **Portal Captiu.** Un portal captiu és una pàgina web a la qual s'accedeix amb un navegador web i que es mostra als usuaris recentment

connectats a xarxa, ja sigui una xarxa sense fils o per cable, abans que se'ls concedeixi accés als recursos de la mateixa.

En el moment en que un client es connecta a la xarxa, el sistema de portal captiu redirecciona la petició http o https cap el servidor de portal captiu del sistema. D'aquesta manera, se li presenta a l'usuari un formulari per la autenticació fent servir un nom i pas de clau, o realitzant un auto registre. El servidor del portal captiu descartarà la majoria del tràfic generat per l'usuari fins que aquest no s'autentiqui correctament en el sistema.

- **802.1x.** És un estàndard IEEE i mètode d'autenticació utilitzat en les xarxes cablejades i sense fils per tal d'autenticar la identitat d'un usuari abans de proporcionar-li accés a la xarxa.

  Hi ha tres elements bàsics que intervenen en l'autenticació 802.1X.

  - **Sol·licitant**. Un client de software que s'executa en l'estació de treball o dispositiu.
  - **Autenticador**. El punt d'accés a la xarxa, ja sigui un WI-FI (un AP) o un port de xarxa cablejada (un commutador).
  - **Servidor d'autenticació**. Una base de dades d'autenticació normalment un RADIUS contra un LDAP o Directori Actiu.

  S'utilitza el protocol d'autenticació EAP per passar la informació d'autenticació entre el sol·licitant (estació de treball o PC) i el servidor d'autenticació (LDAP, AD). El tipus de EAP és qui realment controla i defineix l'autenticació. El punt d'accés, ja sigui un AP o commutador, que actua com a autenticador, és només un proxy que permet la comunicació entre el sol·licitant i el servidor d'autenticació.

  El tipus de EAP a implementar en el mètode 802.1X dependrà del nivell de seguretat que és vulgui aplicar i es necessiti. Com s'ha comentant en l'apart de protocols d'autenticació, es pot utilitzar EAP-PEAP, EAP-TTLS, EAP-TLS, etc

  Exemples habituals de dispositius capaços d'autenticar-se mitjançant 802.1X serien:

  - Portàtils i ordinadors de sobre taula que executen els sistemes operatius Windows, macOS i la majoria de distribucions Linux.
  - Impressores d'última generació.
  - Dispositius de VOIP
  - Alguns punts d'accés a la xarxa sense fils d'última generació.
  - etc

- **IPSEC / VPN**. El protocol IPSEC és un dels protocols de seguretat més importants i àmpliament utilitzat en entorns empresarials. IPSEC proporciona tots els serveis necessaris per tal que una comunicació sigui segura, autenticació, confidencialitat i integritat.

  A nivell d'autenticació, el protocol IPSEC ofereix diferents tipus d'autenticació, com per exemple EAP-TLS, EAP-PEAP, EAP-MSCHAPv2, etc per tal garantir la identitat de l'usuari.

  Pel que fa a la confidencialitat, IPSEC suporta tots el xifrats simètrics actuals, AES i Blowfish així com d'altres menys segurs i recomanables com 3DES, per tal xifrar les comunicacions extrem a extrem.

  Al mateix temps, el protocol IPSEC pot assegurar que la informació no ha estat modificada entre l'origen de la comunicació fins el destí, Integritat. El protocol IPSEC permet a l'equip receptor verificar que els camps de capçalera del datagrama i la carga útil xifrada no han estat modificats mentre el datagrama estava de ruta cap el destí. Els algoritmes suports per IPSEC per assegurar la integritat de les dades can des de MD5 fins a SHA-512 i AES.

10.4 Configuracions dispositius PoC.

10.4.1 Col·lectors perfilat

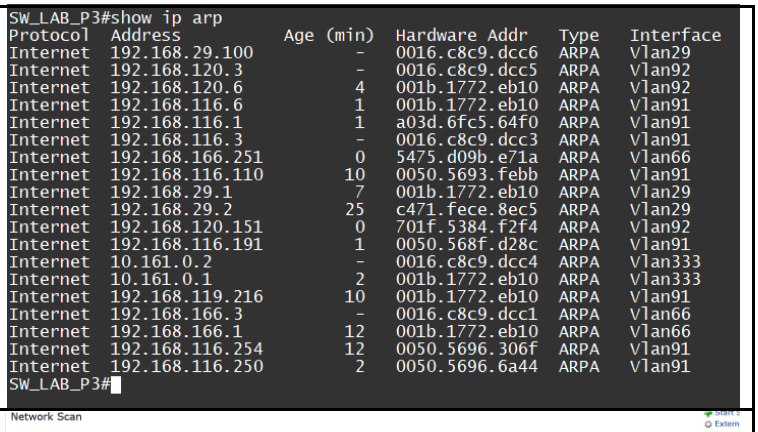
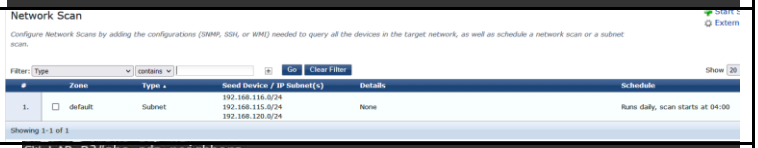
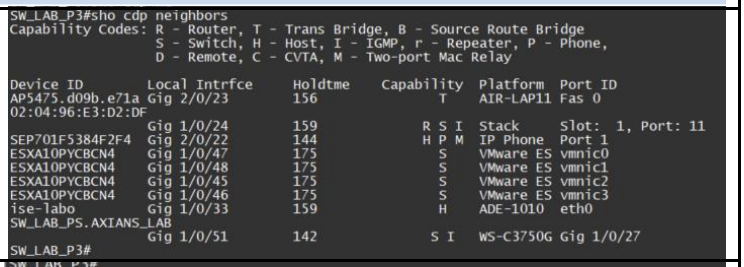
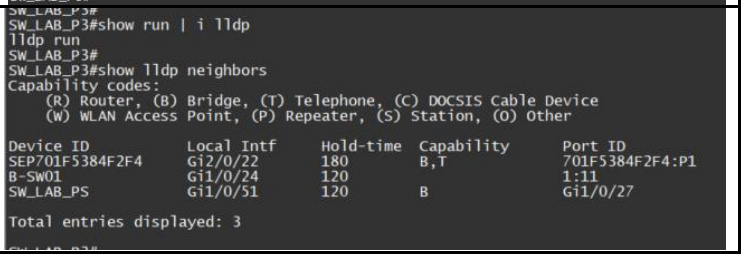
Ha continuació es mostren les captures de pantalla de la configuració realitzada dels diferents col·lector utilitzats en la PoC.

<table>
<tr><th colspan="3">Configuracions Col·lectors</th></tr>
<tr><th>Dispositiu</th><th>Descripció</th><th>Captura</th></tr>
<tr><td>Commutador Cisco</td><td>DHCP Relay commutador.</td><td>
<pre>
SW_LAB_P3#show run int vlan 91
Building configuration...

Current configuration : 119 bytes
!
interface Vlan91
 ip address 192.168.116.3 255.255.252.0
 ip helper-address 192.168.116.250
 no ip mroute-cache
end

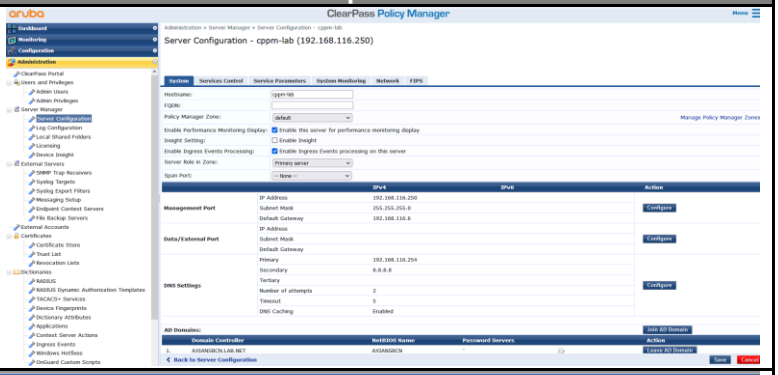
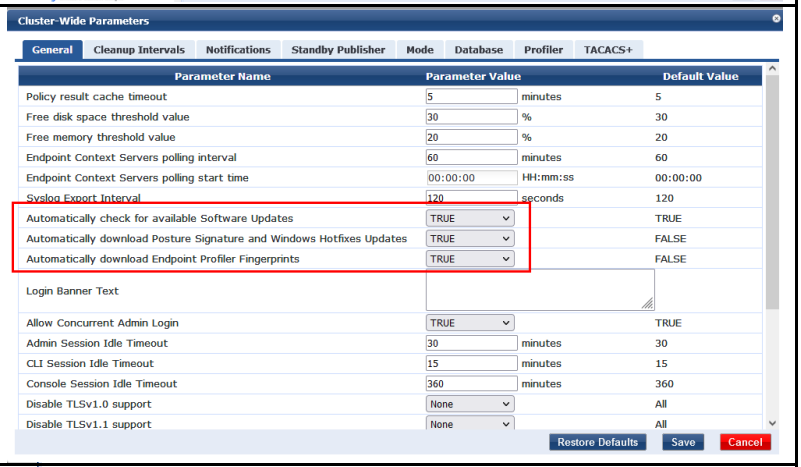
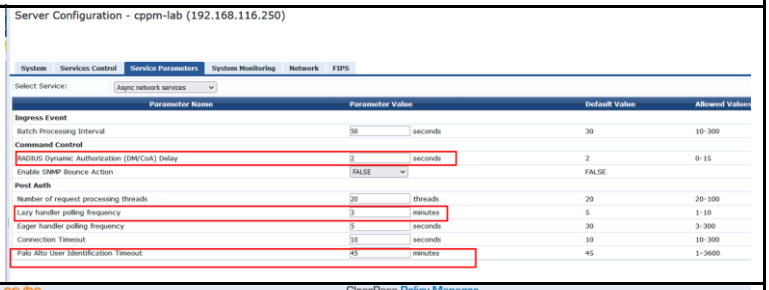
SW_LAB_P3#
</pre>
</td></tr>
<tr><td>Tallafocs Palo Alto</td><td>DHCP Relay tallafocs.</td><td>
Dashboard | ACC | Monitor | Policies | Objects | Network | Device
DHCP Server | DHCP Relay
Interface | IPv4 Enabled | IPv4 Servers
ethernet1/1.66 — 192.168.116.250, 192.168.116.254
ethernet1/1.92 — 192.168.116.250, 192.168.116.254
ethernet1/1.90 — 192.168.116.250, 192.168.116.254
</td></tr>
<tr><td>ClearPass</td><td>SNMP en el CPPM per consultar la taula ARP dels commutadors.</td><td>
System | Services Control | Service Parameters | System Monitoring | Network | FIPS
Parameter Name | Parameter Value | Default
SnmpService
SNMP Timeout: 4 seconds — 4
SNMP Retries: 1 retries — 1
LinkUp Timeout: 5 seconds — 5
IP Address Cache Timeout: 600 seconds — 600
Uplink Port Detection MAC Threshold: 5 — 5
SNMP v2c Trap Community: •••••• — public
SNMP v3 Trap Username: aruba — aruba
SNMP v3 Trap Authentication Protocol
SNMP v3 Trap Privacy Protocol
SNMP v3 Trap Authentication Key
SNMP v3 Trap Privacy Key
Device Info Poll Interval: 60 minutes — 60
Certificate Auth

Edit Device Details
Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes
Allow SNMP Read: Enable Policy Manager to perform SNMP read operations
Policy Manager Zone: default
SNMP Read Setting: SNMP v1 with community strings
Community String: •••••••••••••• Verify: ••••••••••••••
Read ARP Table Info: Read ARP table from this device
Copy | Save | Cancel
</td></tr>
<tr><td>Commutador</td><td>SNMP en el commutador.</td><td>
<pre>
SW_LAB_P3#
SW_LAB_P3#
SW_LAB_P3#show run | i snmp
snmp-server community public RO
SW_LAB_P3#
SW_LAB_P3#
</pre>
</td></tr>
</table>

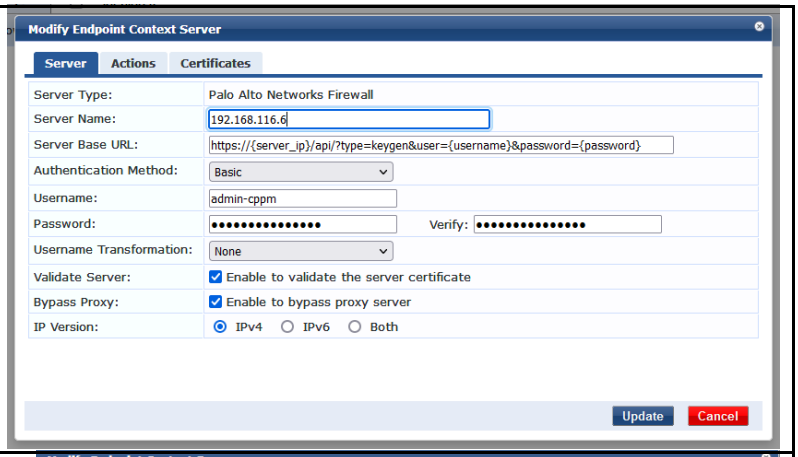
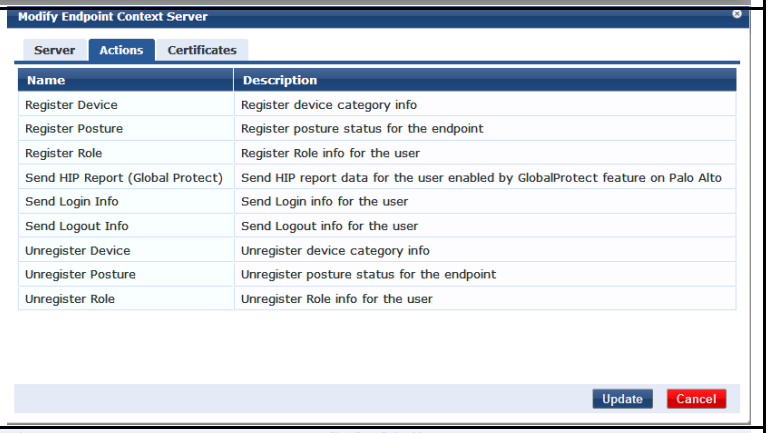
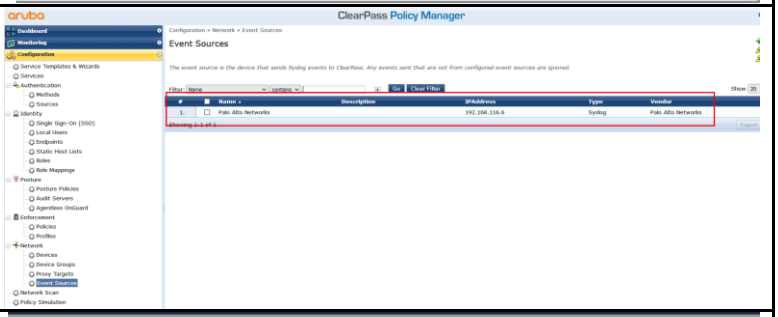
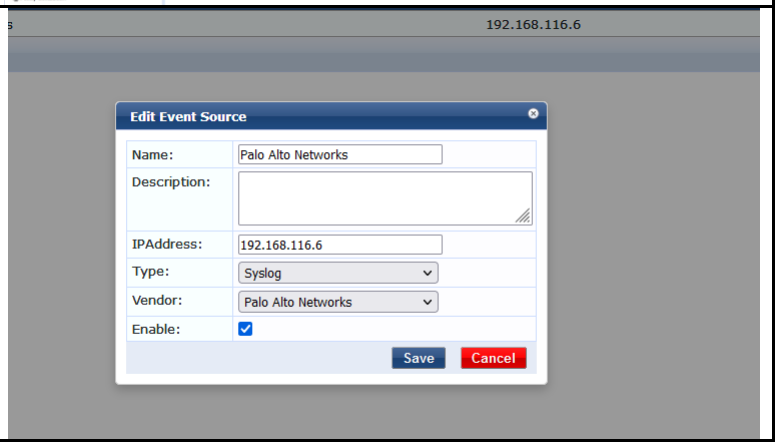
Commutador	Taula ARP del commutador compartida per SNMP	
ClearPass	Escanejos diaris de la xarxa en hores no productives	
Commutador	Activació CDP	
Commutdor	Activació LLDP	

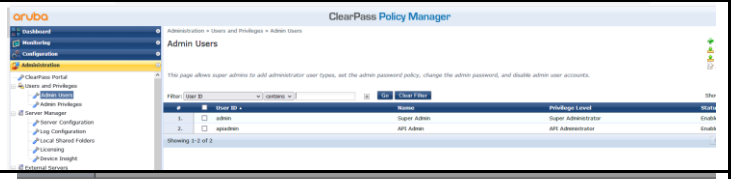
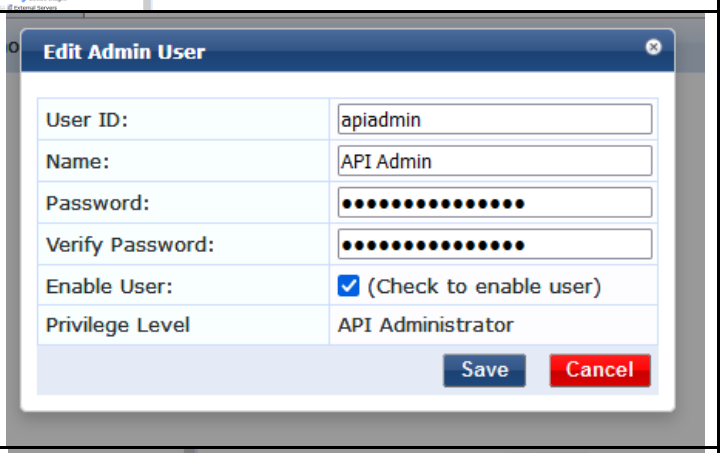
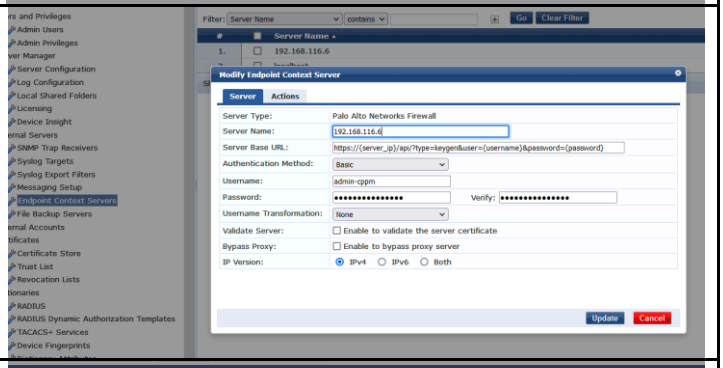
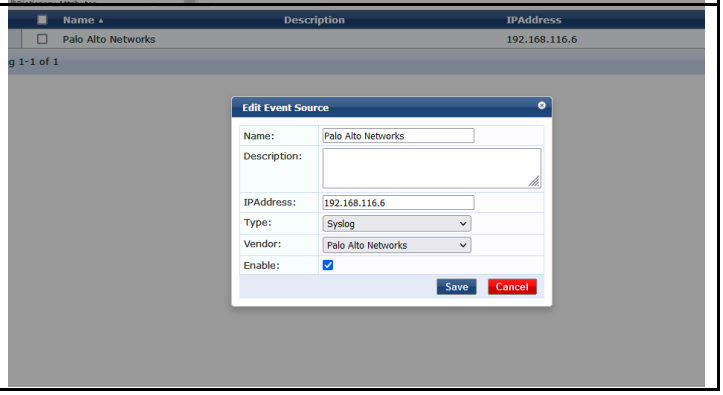
Taula 16: Configuracions Col·lectors

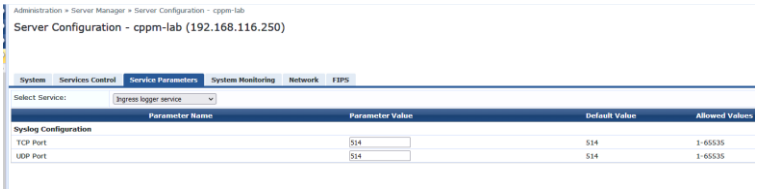
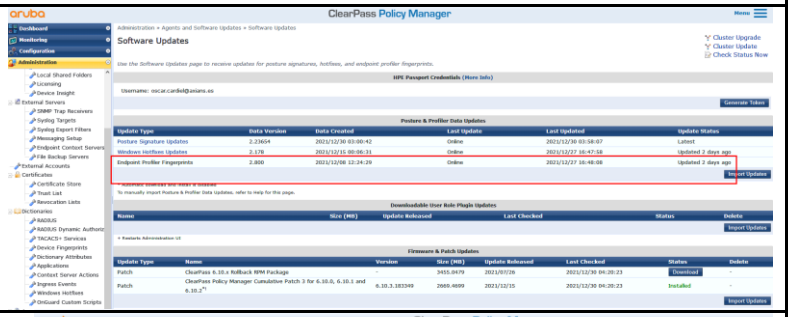
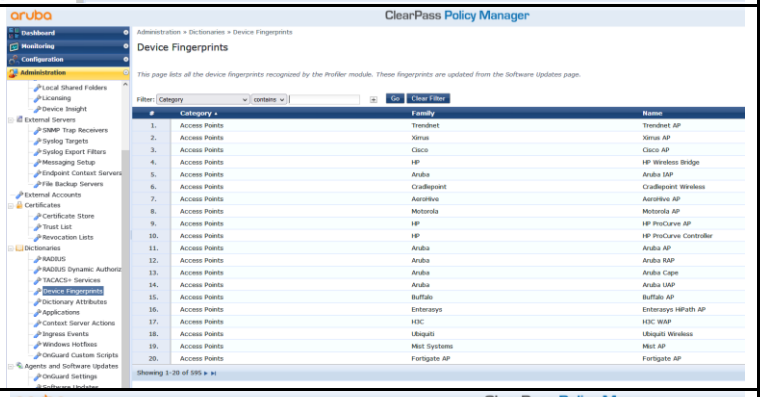
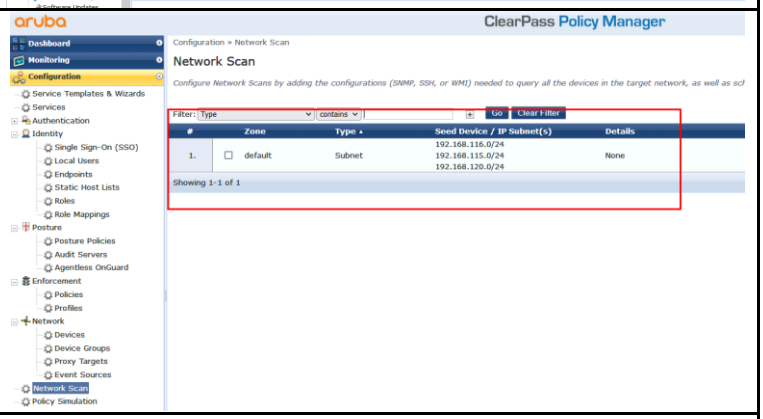
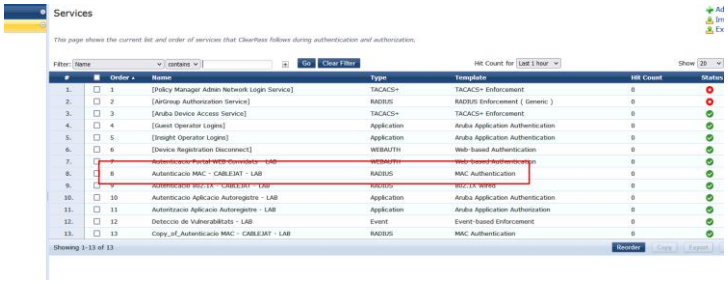
10.4.2 Configuració ClearPass

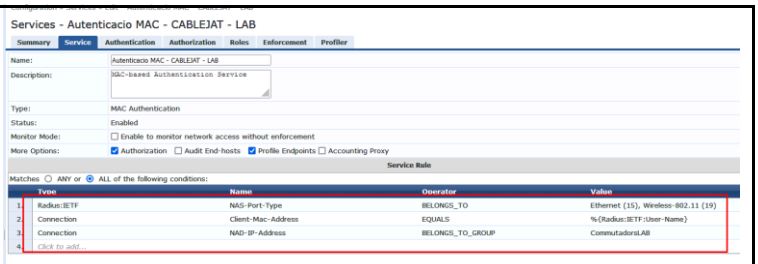
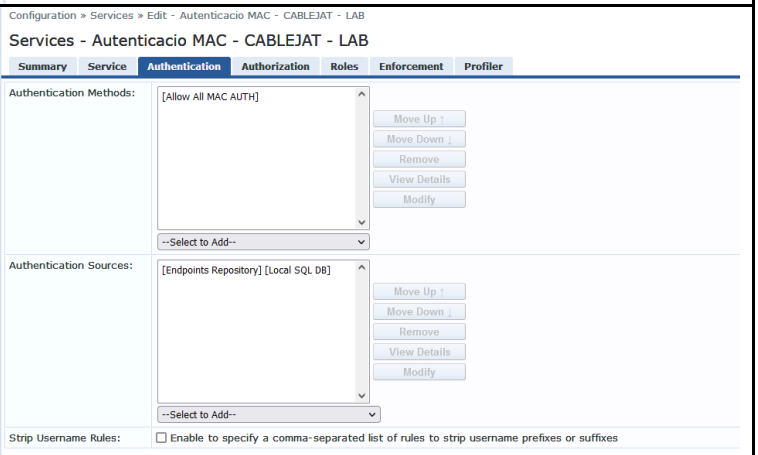
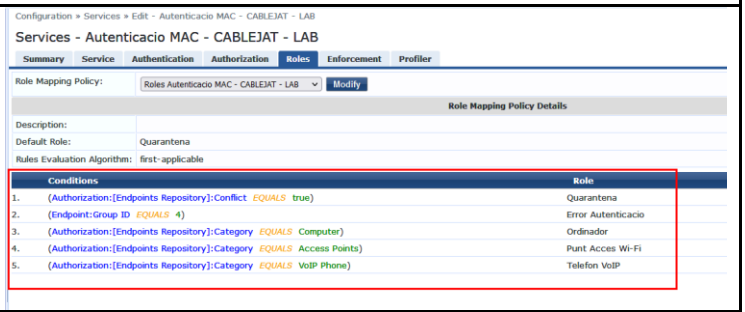
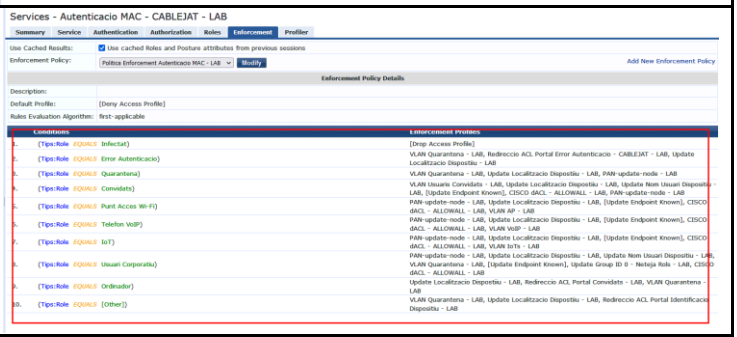
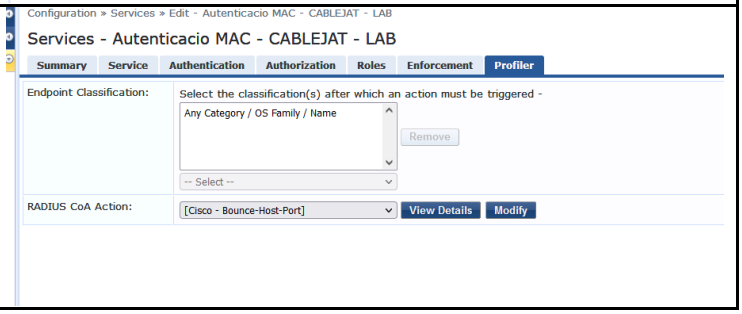
<table>
<tr><th colspan="2">Configuració ClearPass</th></tr>
<tr><th>Descripció</th><th>Captura</th></tr>
<tr><td>Configuració bàsica del node</td><td> 
</td></tr>
<tr><td>Activació automàtica (núvol d'Aruba) dels updates de la base de dades de perfilatge de dispositius</td><td> 
</td></tr>
<tr><td>Configuració integració ClearPass amb el Tallafocs Palo Alto</td><td> 

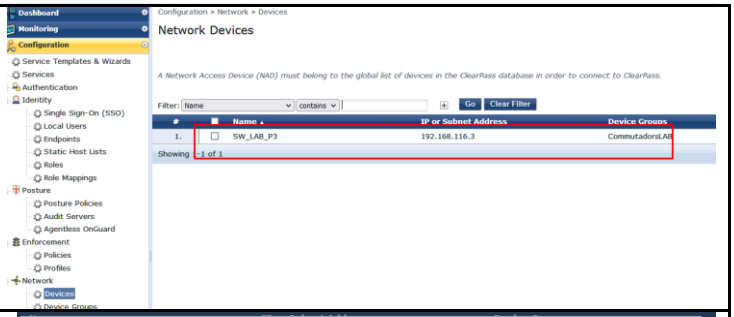
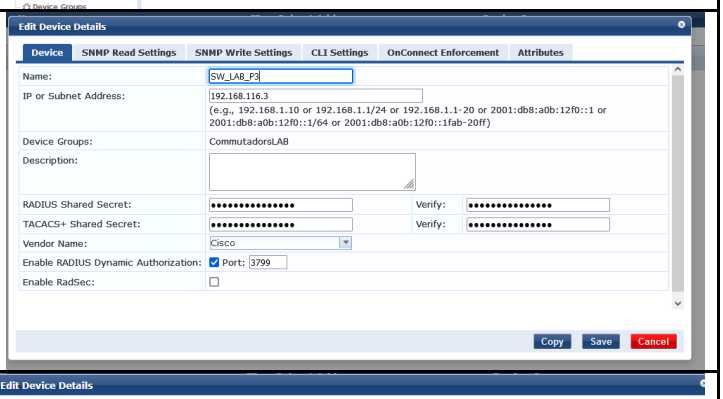
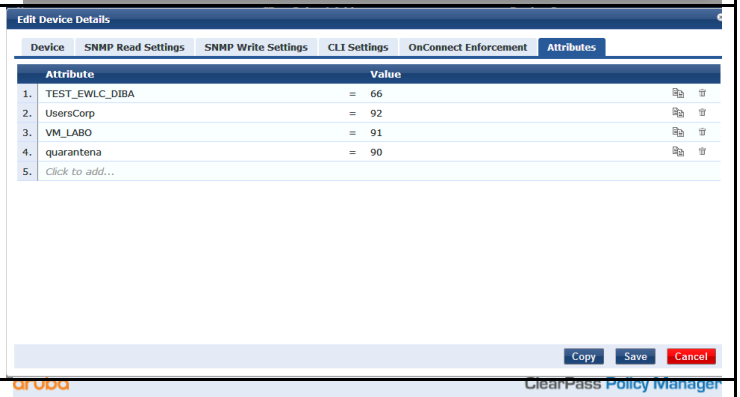
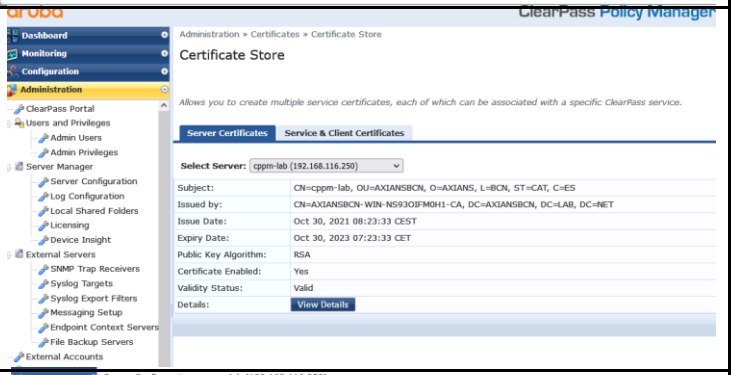
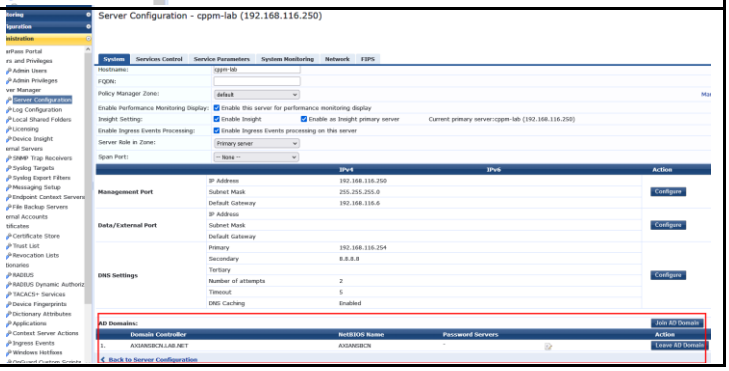

</td></tr>
</table>

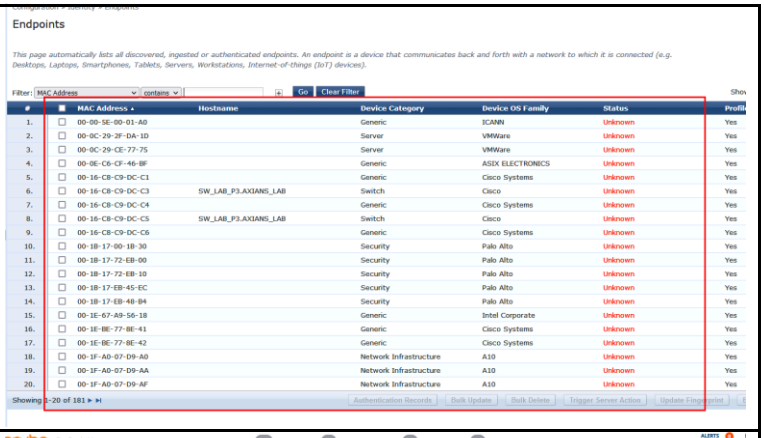
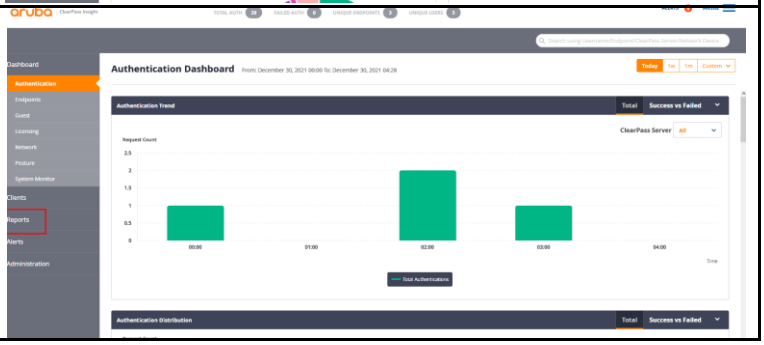
	
Configuració integració ClearPass amb el Tallafocs Palo Alto	
	
	

Arrancar els serveis de Ingress logger per tal actuar com a syslog server y rebre els logs del tallafocs.	
Usuari xml per accés via API al tallafocs de palo alto	
Usuari xml per accés via API al tallafocs de palo alto	
Integració via API amb el tallafocs de Palo Alto	
Integració amb el tallafocs de Palo Alto per la interpretació dels logs enviats pel tallafocs	

Configuració servidor syslog port TCP/UDP per la lectura del logs del tallafocs Palo Alto per identificar bloquejos de dispositius en cas de detecció d'incidents de seguretat.	
Activació subscripció actualització patrons per a perfilats de dispositius	
Base de dades de perfilats de dispositius	
Escanejos de xarxa programats o manuals per al descobriment de dispositius	
Panel de configuració de les polítiques de seguretat implementades	

Política de seguretat lot implementada – Servei accés	
Política de seguretat lot implementada - Autenticació	
Política de seguretat lot implementada - Roles	
Política de seguretat lot implementada - Enforcement	
Política de seguretat lot implementada - Profiler	

Alta dispositius NAS	
NAS - Commutador Cisco Catalyst laboratori	
NAS - Commutador Cisco Catalyst laboratori	
Integració amb la certificadora de laboratori	
Integració amb el directori actiu del laboratori	

Visibilitat dels dispositius descoberts en la xarxa pels diferents mètodes configurats	
Informes – ClearPass Insight	 

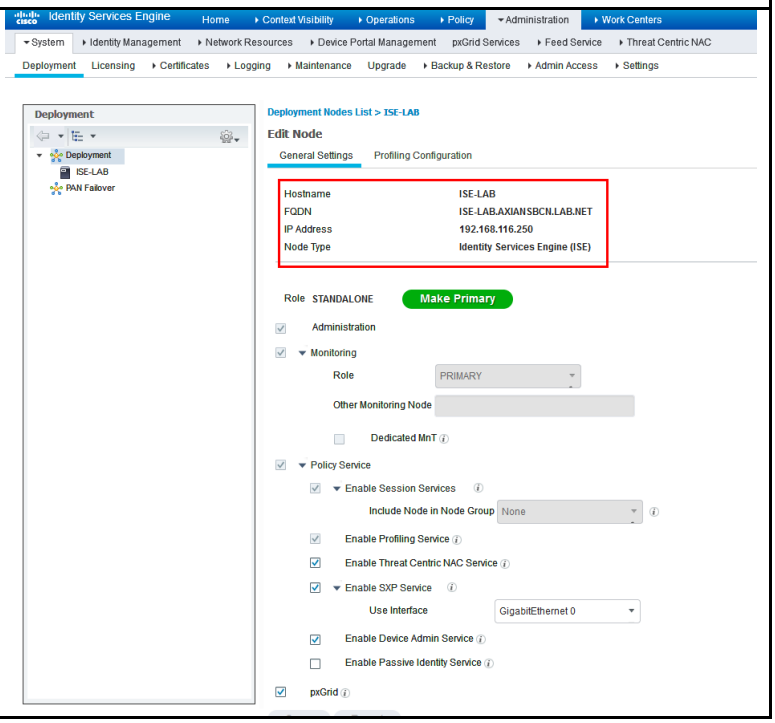
Taula 17: Configuració ClearPass

10.4.3 Configuració Cisco ISE

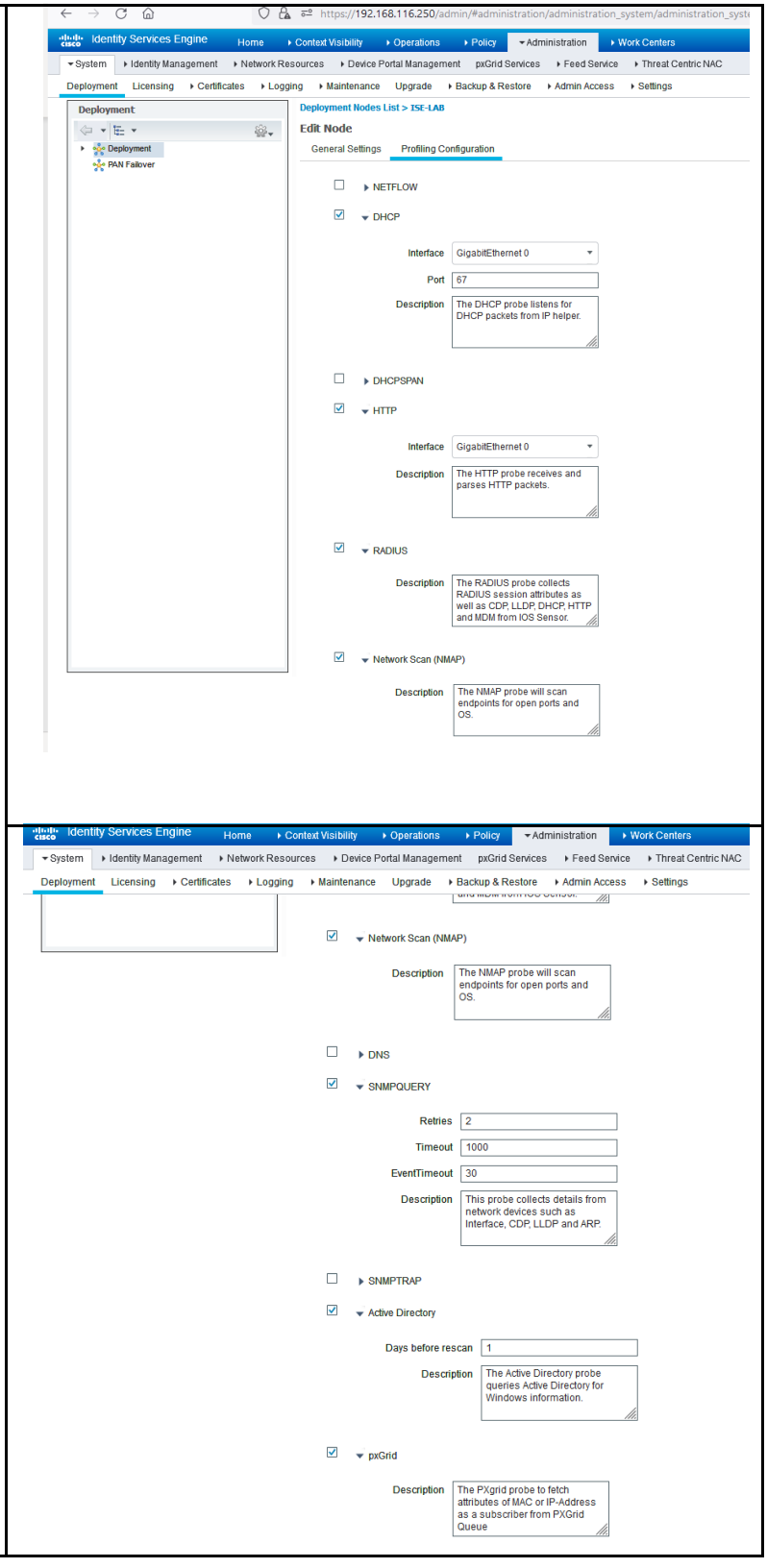
A continuació es mostren les captures de pantalla de la part de configuració mes rellevants que s'ha realitzat en el dispositiu Cisco ISE per la prova de concepte.

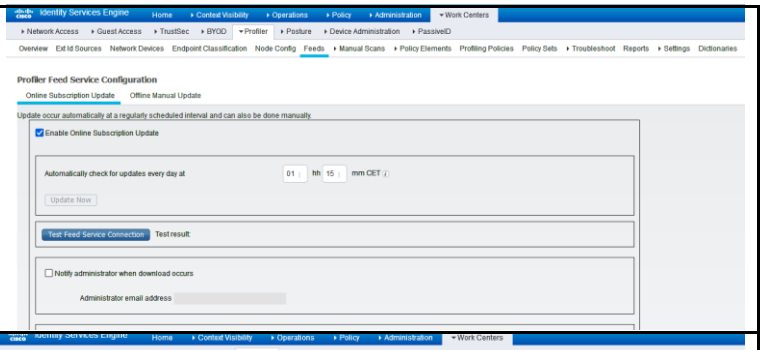
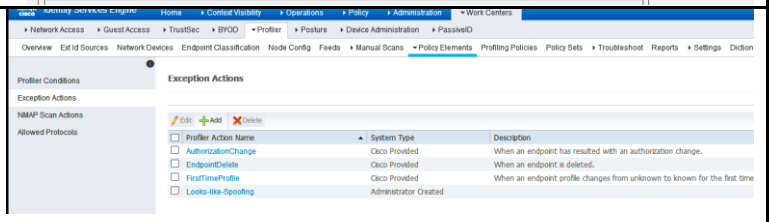
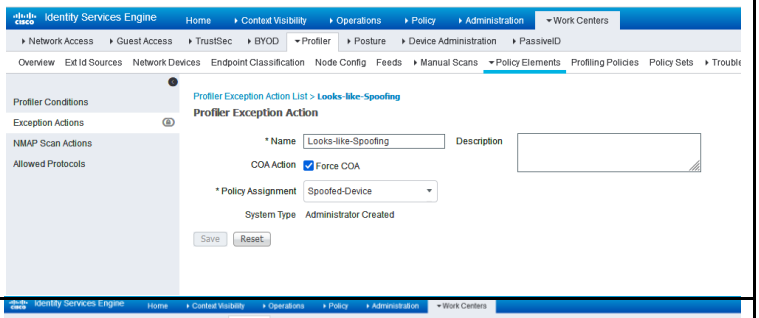
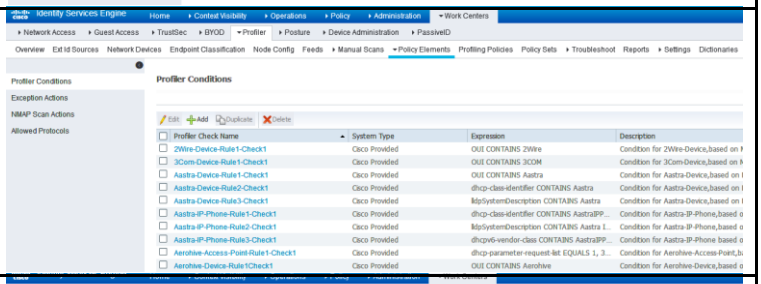
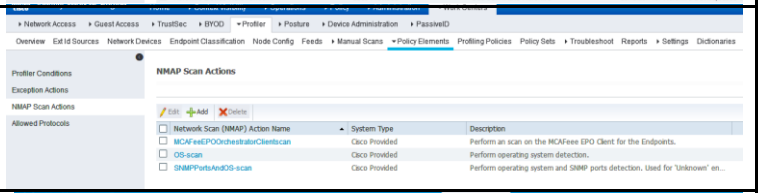
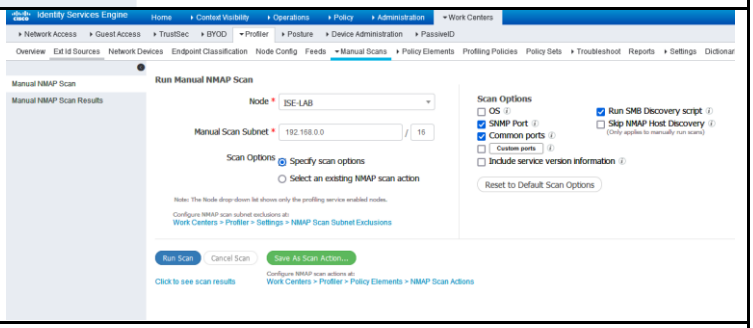
Configuració ISE	
Descripció	**Captura**
Configuració CLI del node	ISE-LAB/admin# show run Generating configuration... ! hostname ISE-LAB ! ip domain-name AXIANSBCN.LAB.NET ! ipv6 enable ! interface GigabitEthernet 0 ip address 192.168.116.250 255.255.255.0 ipv6 address autoconfig

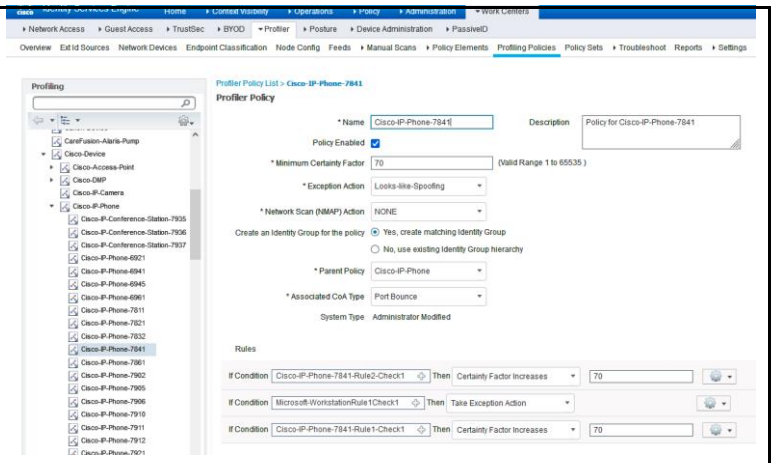
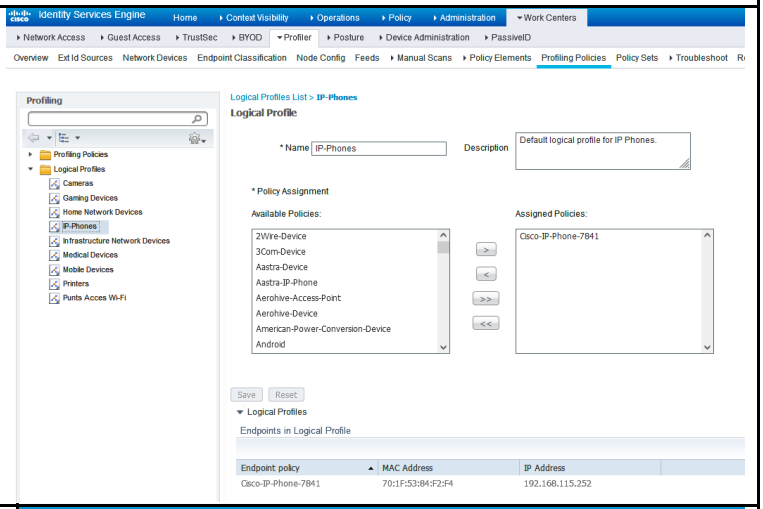
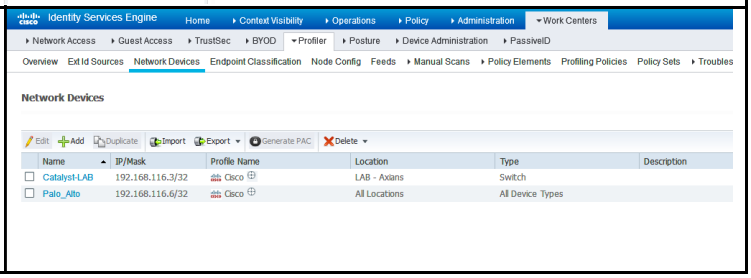
```
  ipv6 enable
!
ip name-server 192.168.116.254
!
ip default-gateway 192.168.116.6
!
clock timezone Europe/Madrid
!
ntp server es.pool.ntp.org
!
username admin password hash $5$yMC.XaVJ$qvtV8wxCHpQGsTOkjxjaHjd1eSc/1aEDffL8O1aBHt5 role admin
!
max-ssh-sessions 5
!
service sshd enable
service sshd encryption-algorithm aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes256-gcm@openssh.com aes128-ctr aes256-ctr
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  no-previous-password
  min-password-length 4
  password-lock-enabled
  password-lock-timeout 15
  password-lock-retry-count 3
!
logging loglevel 6
!
conn-limit 30 port 9060
conn-limit 5 port 9061
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
!
ISE-LAB/admin#
hostname ISE-LAB
!
ip domain-name AXIANSBCN.LAB.NET
!
ipv6 enable
!
interface GigabitEthernet 0
  ip address 192.168.116.250 255.255.255.0
  ipv6 address autoconfig
  ipv6 enable
!
ip name-server 192.168.116.254
!
ip default-gateway 192.168.116.6
!
clock timezone Europe/Madrid
!
ntp server es.pool.ntp.org
!
username admin password hash $5$yMC.XaVJ$qvtV8wxCHpQGsTOkjxjaHjd1eSc/1aEDffL8O1aBHt5 role admin
!
max-ssh-sessions 5
!
service sshd enable
service sshd encryption-algorithm aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes256-gcm@openssh.com aes128-ctr aes256-ctr
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  no-previous-password
```

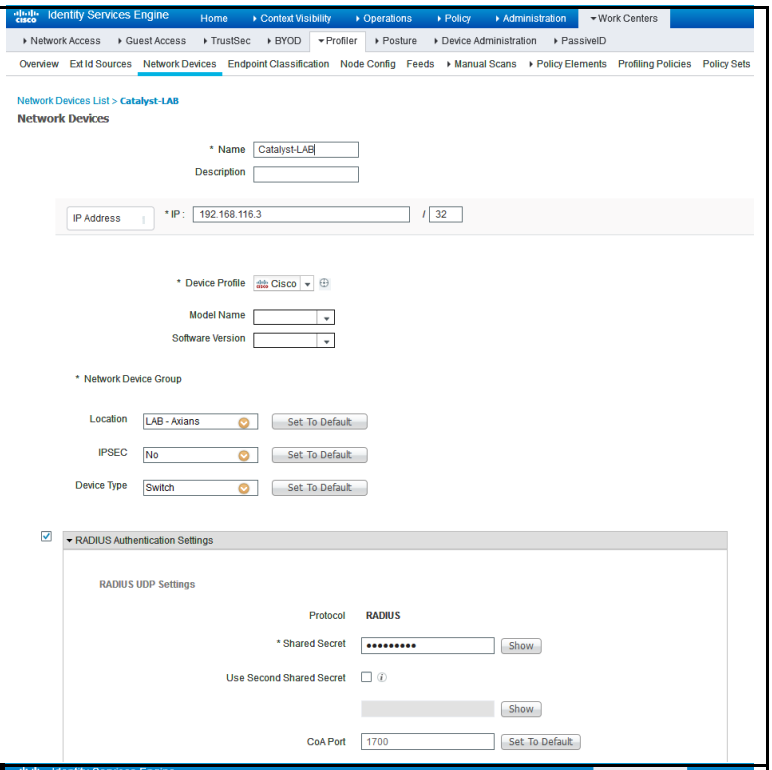
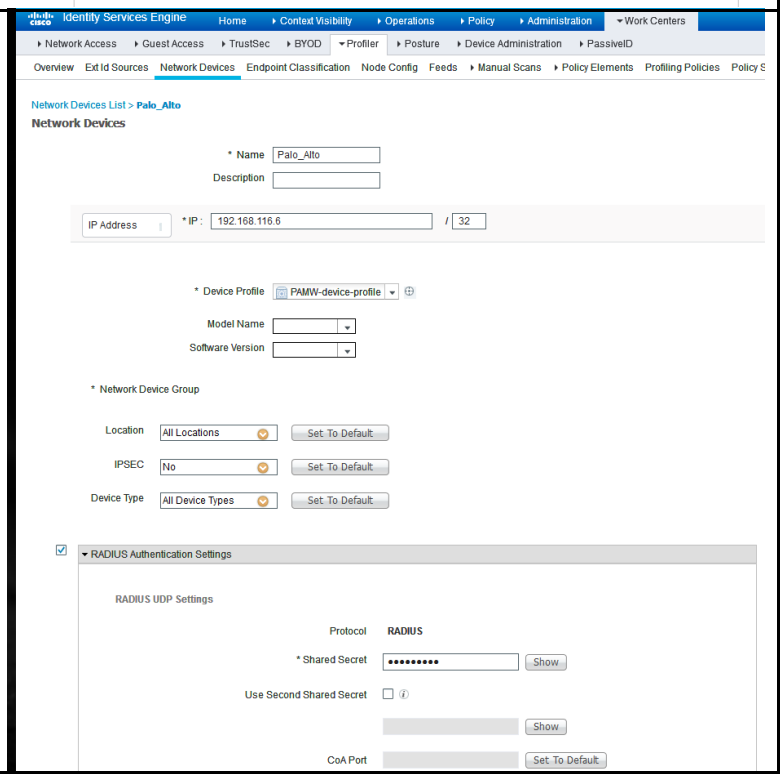
	min-password-length 4 password-lock-enabled password-lock-timeout 15 password-lock-retry-count 3 ! logging loglevel 6 ! conn-limit 30 port 9060 conn-limit 5 port 9061 ! cdp timer 60 cdp holdtime 180 cdp run GigabitEthernet 0 ! icmp echo on ! ISE-LAB/admin#
Imatge configuració principal del node - GUI	

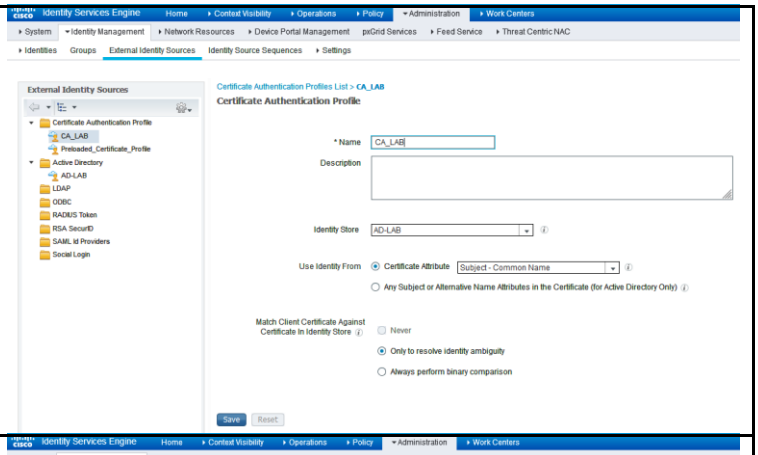
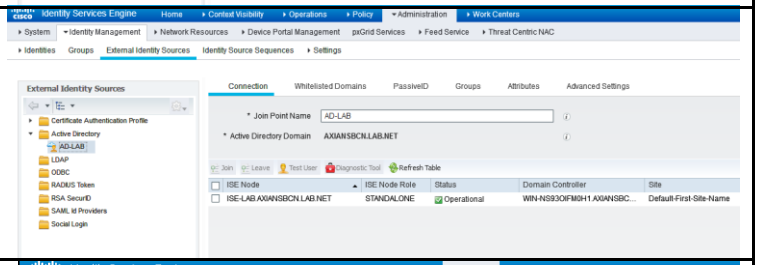
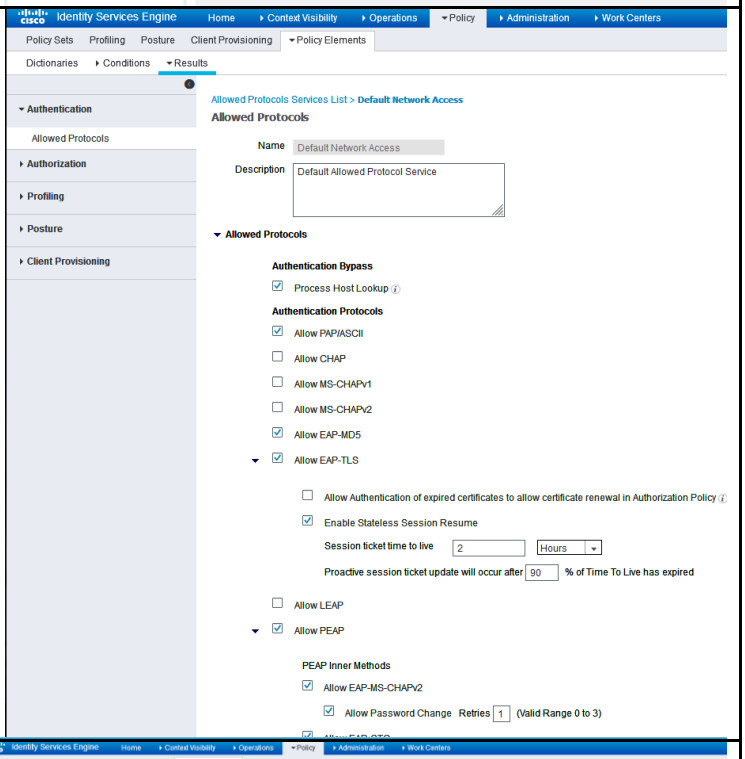
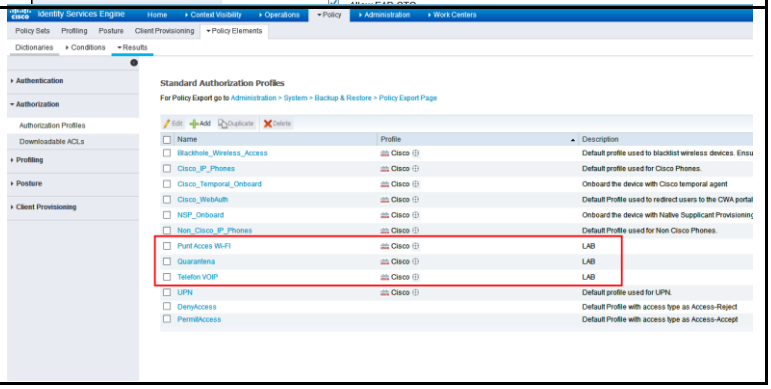
Activació i configuració dels diferents col·lectors per realitzar el perfilat.

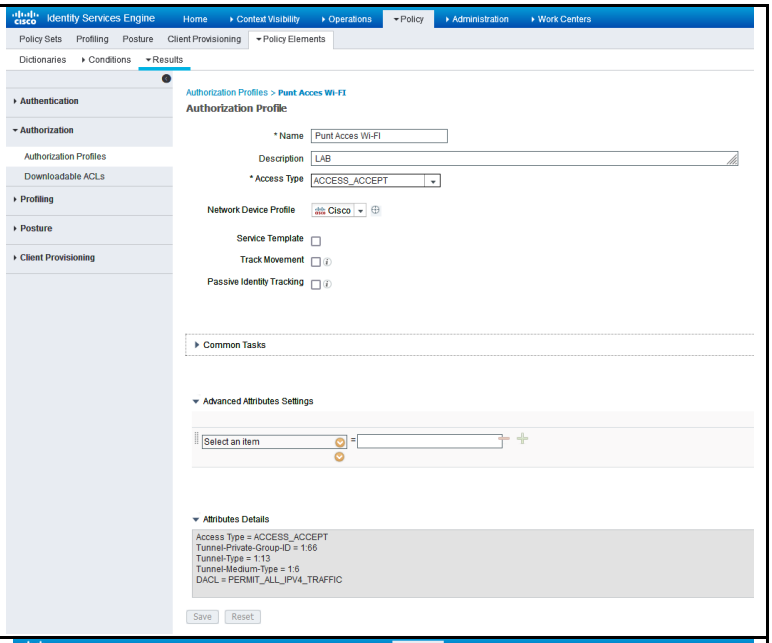
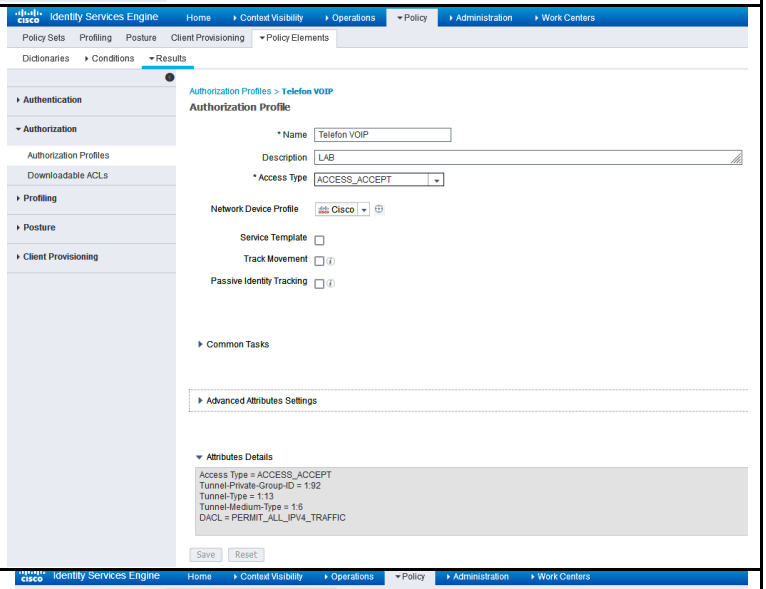
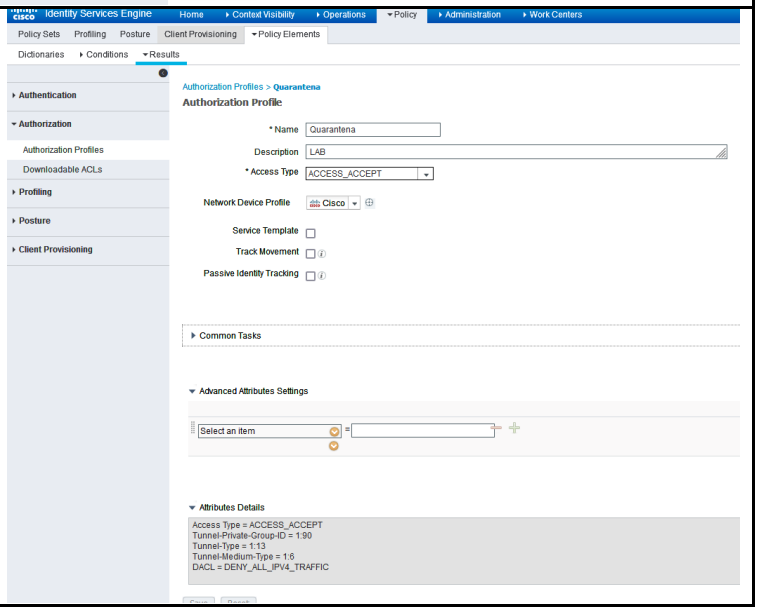


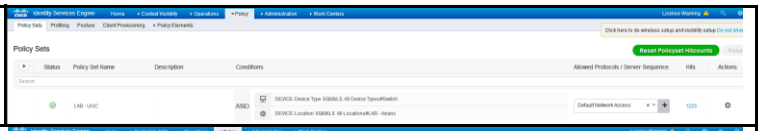
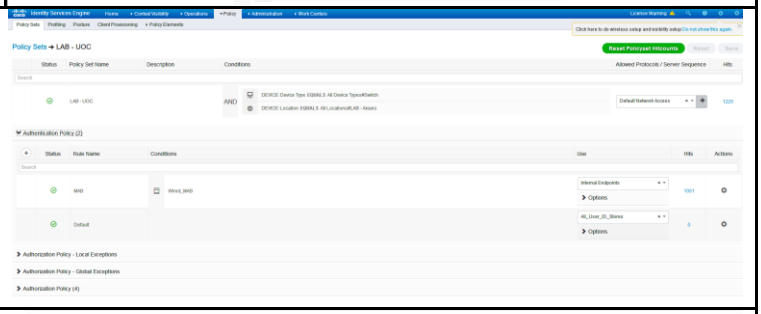
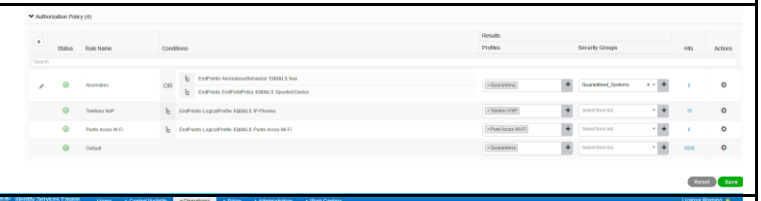
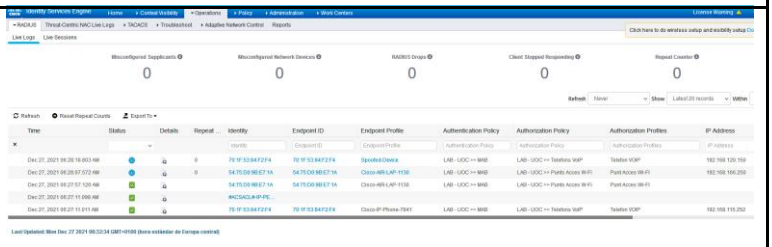
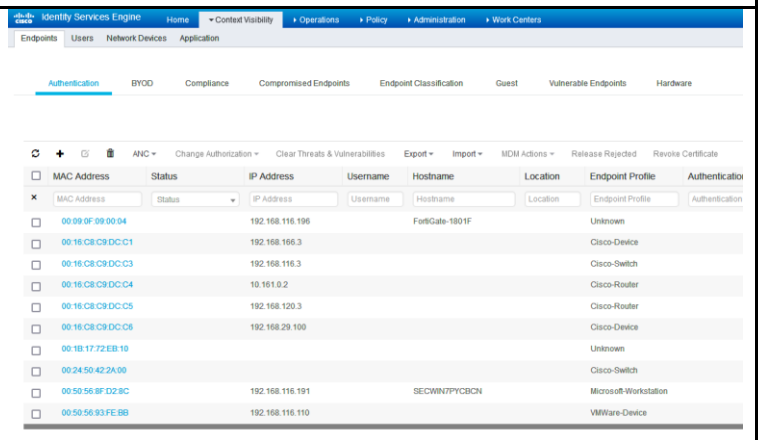
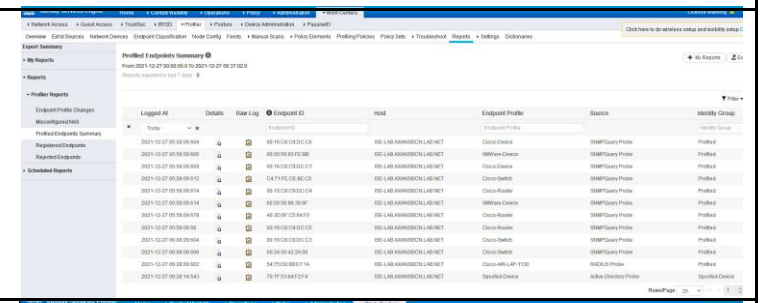
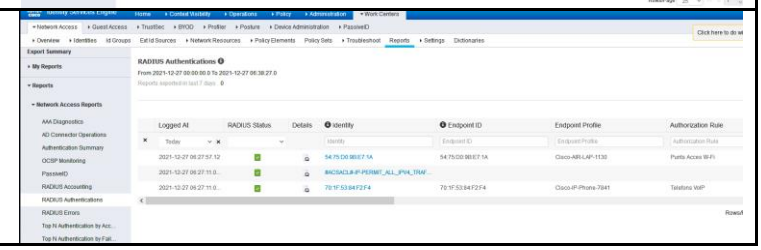
Activació subscripció actualització patrons per a perfilats de dispositius	
Polítiques perfilat – Excepcions	 
Elements predefinits per la realització del perfilat	
Escanejos de xarxa programats per a descobriment de dispositius	
Escanejos manuals	

Política perfilat específica pel telèfon IP utilitzat en la PoC	 
Alta dispositius NAS	

NAS - Commutador Cisco Catalyst laboratori	
NAS – Tallafocs Palo Alto laboratori	

Integració amb la certificadora de laboratori	
Integració amb el directori actiu del laboratori	
Protocols d'autenticació utilitzats	
Autoritzacions de perfilat personalitzats	

Autoritzacions de perfilat Punt Accés Wi-Fi	
Autoritzacions de perfilat Telèfon VoIP	
Autoritzacions de perfilat Quarantena	

Polítiques de control d'accés configurades	  
Gestió logs autenticacions i autoritzacions	
Visibilitat dels dispositius descoberts en la xarxa pels diferents mètodes configurats	
Informes	 

Taula 18: Configuració ISE

10.4.4 Configuració commutador

Servidor Radius i autorització dinàmica	
Instrucció	**Descripció**
! aaa group server radius NAC server 192.168.116.250 auth-port 1812 acct-port 1813 ! radius-server host 192.168.116.250 auth-port 1812 acct-port 1813 key xxxxx. !	Configuració del ClearPass com a servidor radius
! aaa server radius dynamic-author client 192.168.116.250 server-key Axians01. port 3799 auth-type all !	Activació de la autorització dinàmica (CoA)
! ip radius source-interface VlanXX !	Interface utilitzat la comunicació Radius

Taula 19: Configuració Servidors Radius - Commutador

Configuració AAA	
Instrucció	**descripció**
! aaa new-model ! aaa session-id common ! aaa authentication dot1x default group NAC aaa authorization config-commands aaa authorization network default group NAC aaa authorization auth-proxy default group NAC aaa accounting update newinfo aaa accounting dot1x default start-stop group NAC !	Configuració general Activació AAA per a control d'accés a Xarxes
dot1x system-auth-control !	Activació global del control d'accés per port.
radius-server vsa send accounting radius-server vsa send authentication !	Enviament de missatges d'autenticació i accounting
radius-server attribute 11 default direction in radius-server dead-criteria time 30 tries 3 radius-server deadtime 30 !	Acceptació d'IEFT per a ACLs

Taula 20: Configuració AAA - Commutador

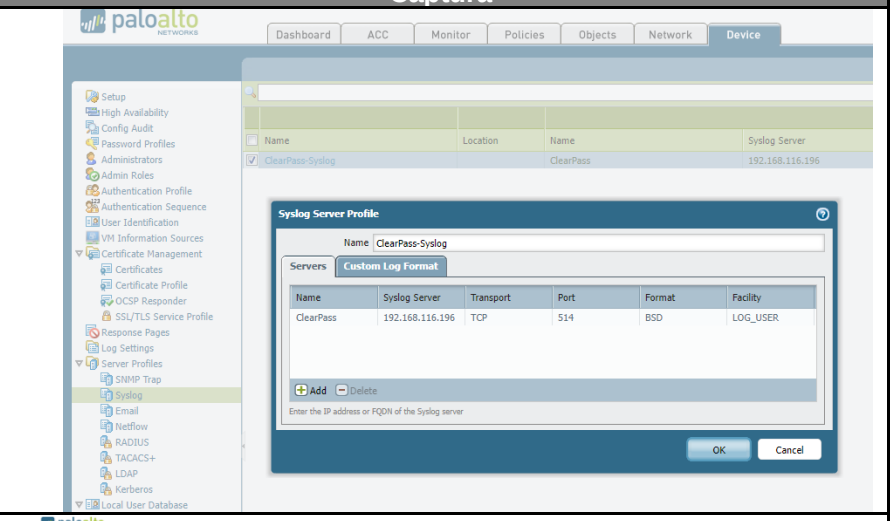
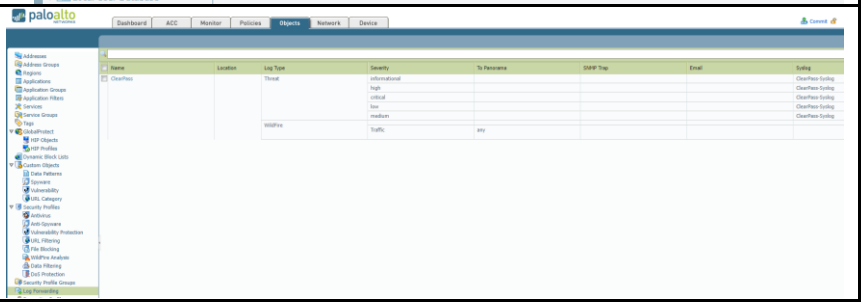
Configuració dels ports del commutador	
Instrucció	**descripció**
Interface XXXXXXXXX description PC	Interface a configurar
switchport access vlan 91 switchport mode access	Vlan assignada per defecte
switchport voice vlan 92	Vlan assignada pels dispositius de Veu
ip access-group default-port-acl in	ACL aplicada per defecte en cada port
authentication event fail retry 0 action next-method	Número d'intents d'autenticació fallits abans d'assignar la vlan d'autenticació fallida.
authentication event server dead action authorize voice	Assignació de la vlan de veu en cas no hagi resposta del servidor NAC
authentication event server alive action reinitialize	Assignació de la vlan de dades en cas no hagi resposta del

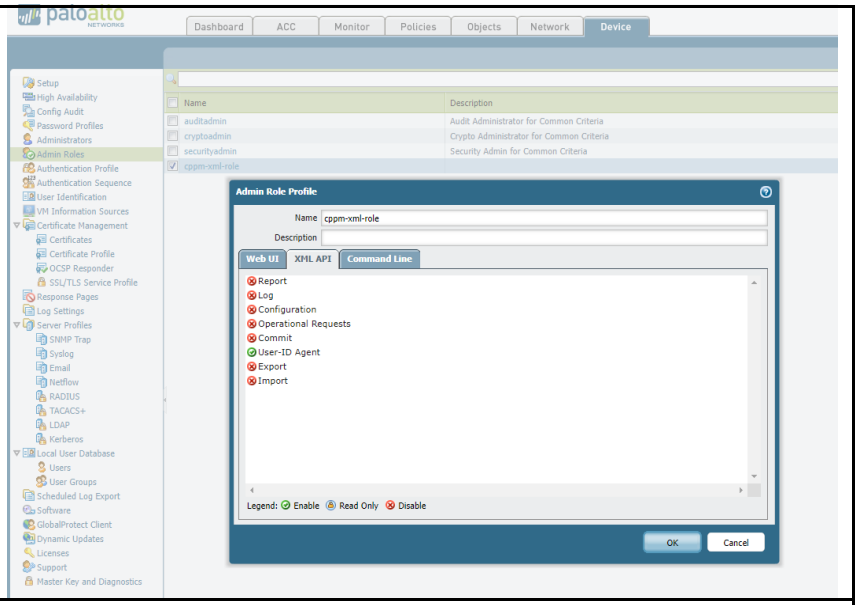
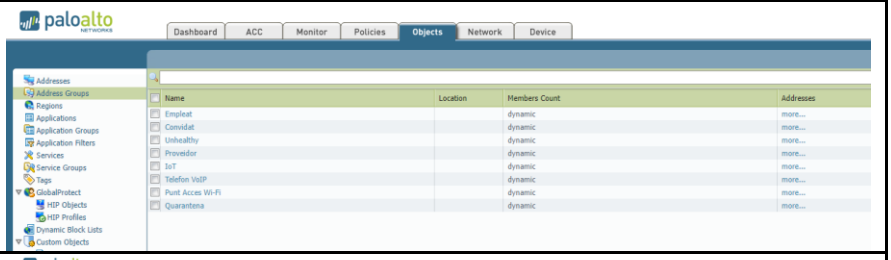
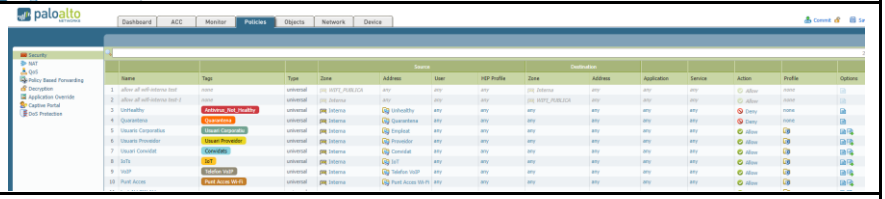
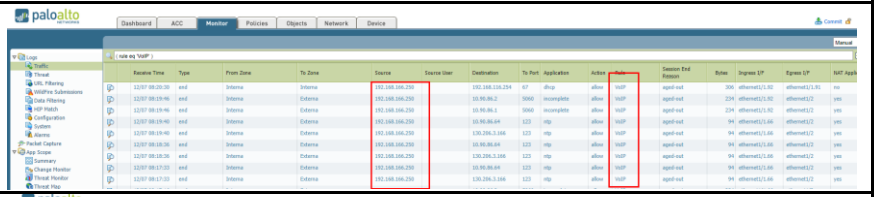
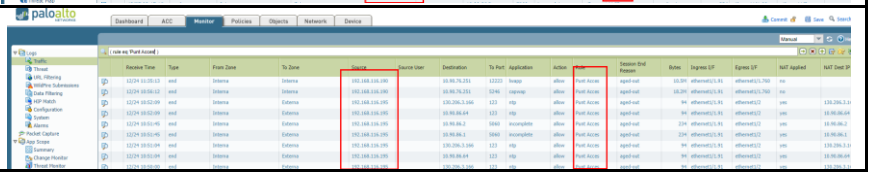
	servidor de NAC
authentication host-mode multi-auth	Suport per veu i dades en un mateix port
authentication order dot1x mab	Seqüencia d'autenticació
authentication priority dot1x mab	Prioritat pel mètode d'autenticació
authentication port-control auto	Activació de l'autenticació en el port
authentication periodic authentication timer reauthenticate server	Activació de la re-autenticació
Mab	Activació del MAC auth bypass
dot1x pae authenticator	Activació del port del commutador com a autenticador
dot1x timeout tx-period 3	Segons que espera el commutador per la resposta d'autenticació

Taula 21: Configuració ports - Commutador

10.4.5 Configuració Tallafocs Palo Alto

A continuació es mostren les captures de pantalla de la part de configuració mes rellevants que s'ha realitzat en el tallafocs de Palo alto per la prova de concepte.

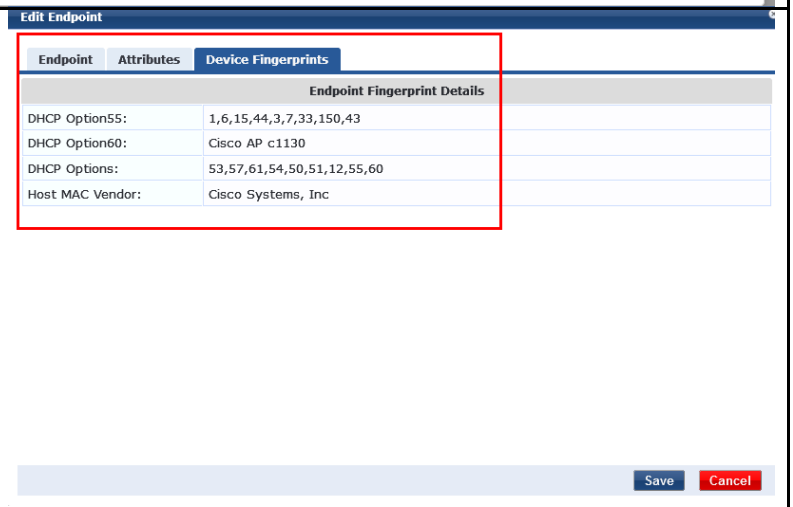
Configuració Palo Alto	
Descripció	**Captura**
Enviament events de syslog per integració amb ClearPass. Activació polítiques del ClearPass post-autenticació (detecció malware en punt final o comportaments anòmals)	 

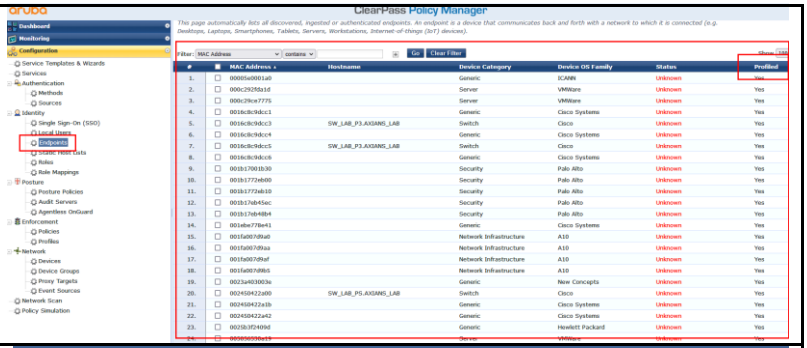
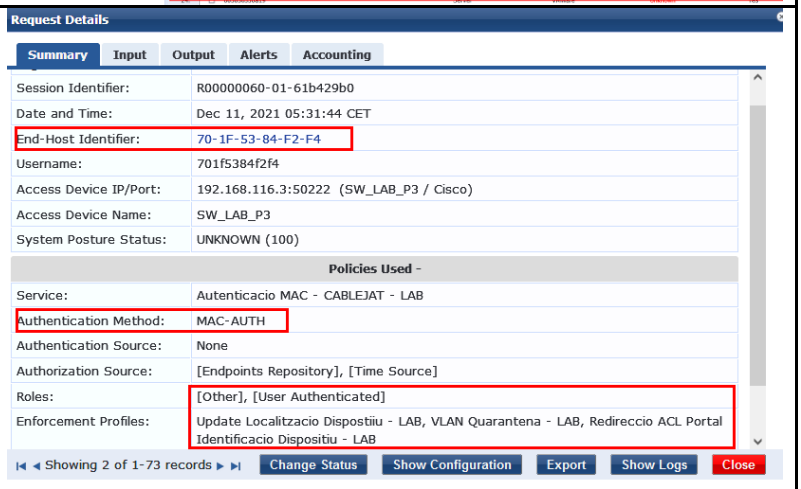
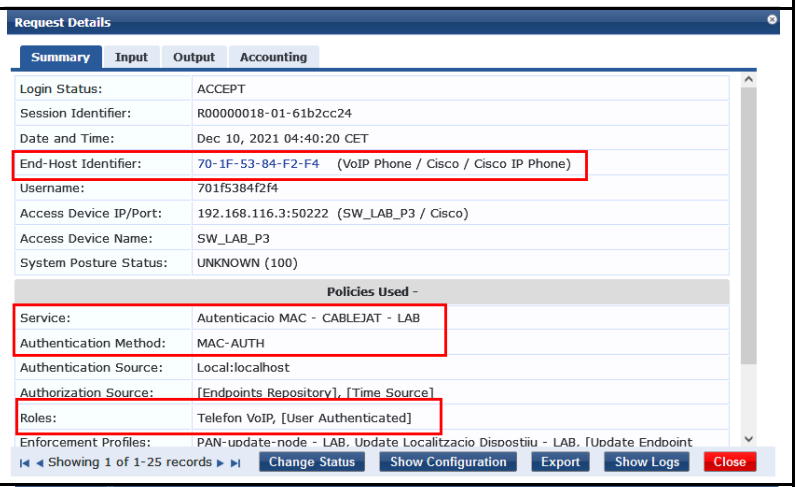
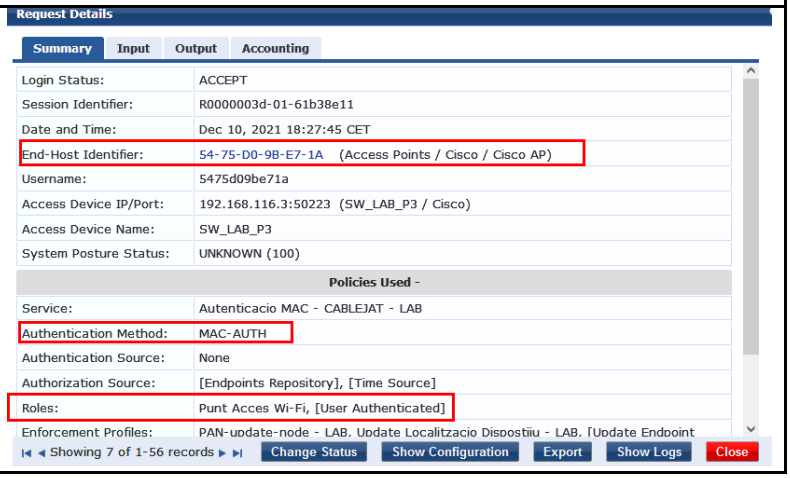
Integració del tallafocs amb el ClearPass via XLM API. ClearPass informe via API del tipus de dispositiu IoT perfilat per tal aplicar les polítiques d'accés corresponents en el tallafocs segons perfilat.	
Definició de adreces dinàmiques comunes amb els perfilats de ClearPass	
Polítiques d'accés segons el tipus de dispositiu perfilat	
Logs de perfilat de dispositius en el tallfocs de PaloAlto segons la informació obtinguda del ClearPass	 

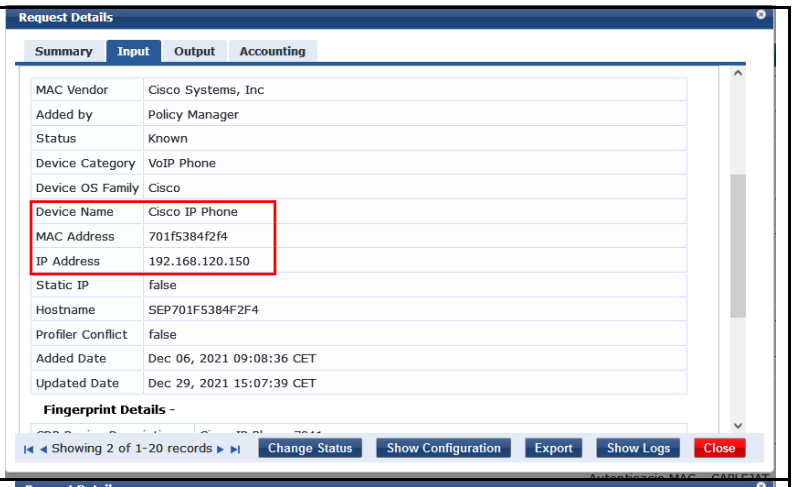
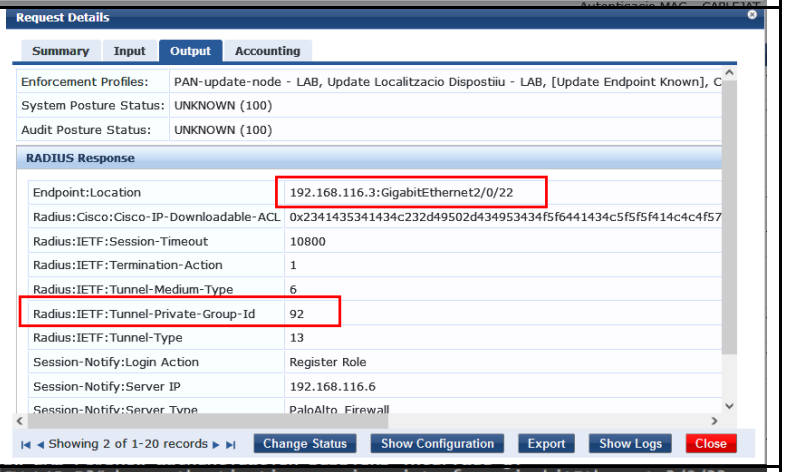
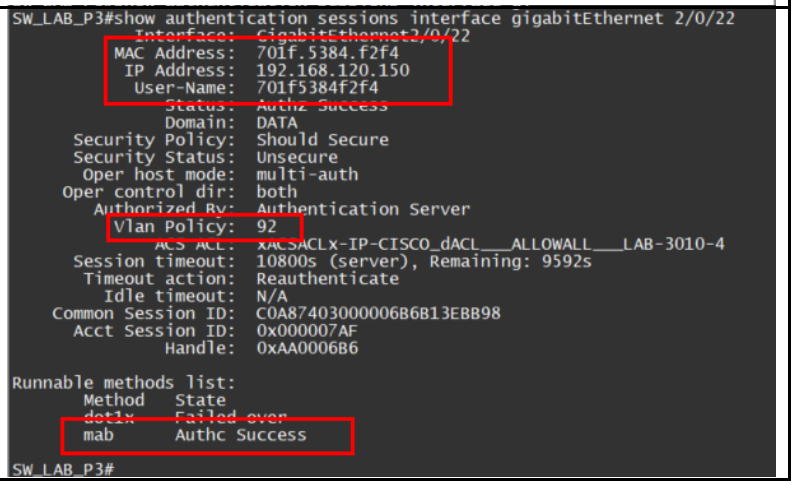
Taula 22: Configuracio Tallafocs

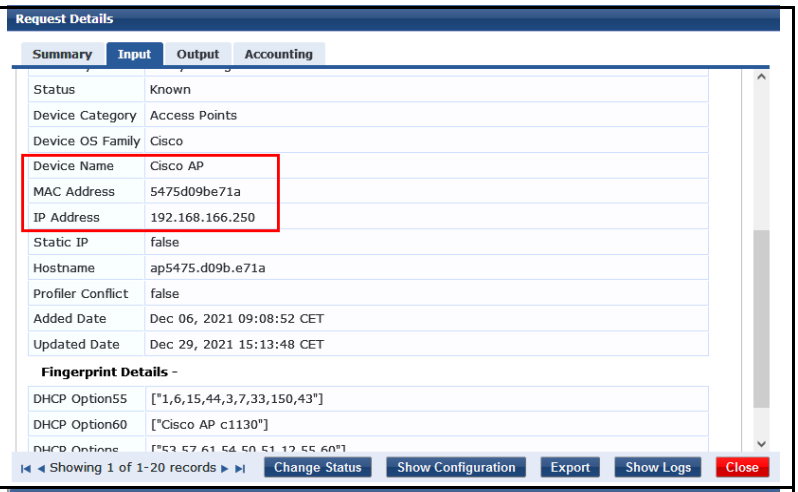
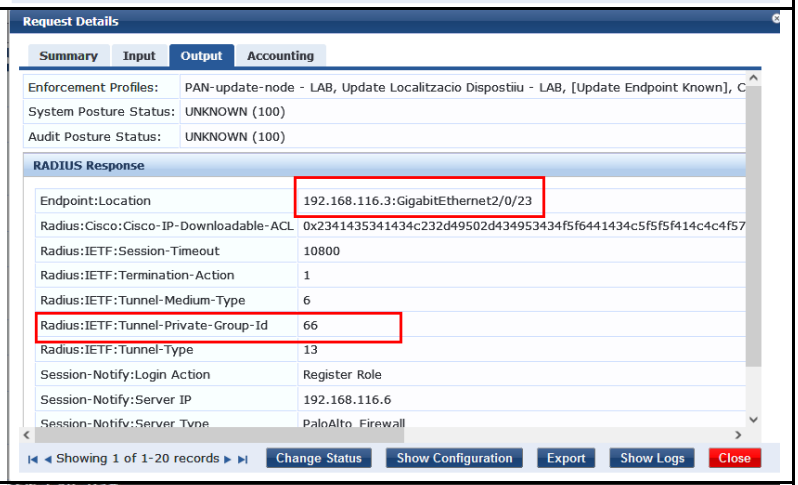
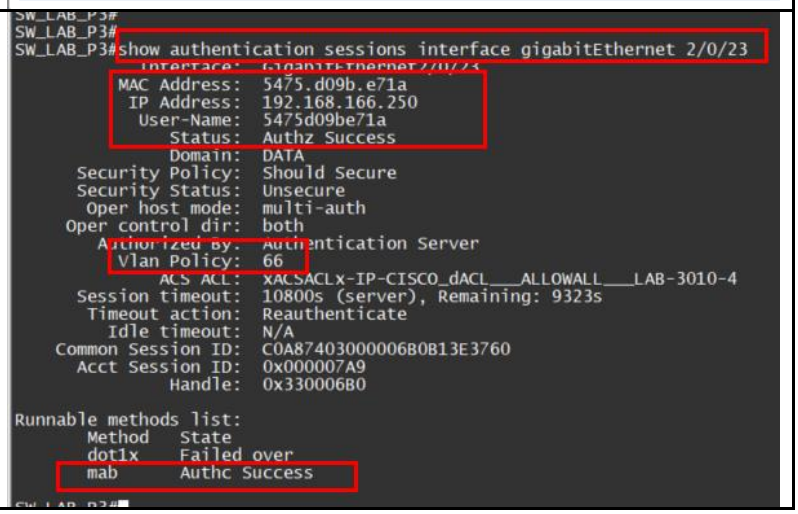
10.5 Evidències PoC

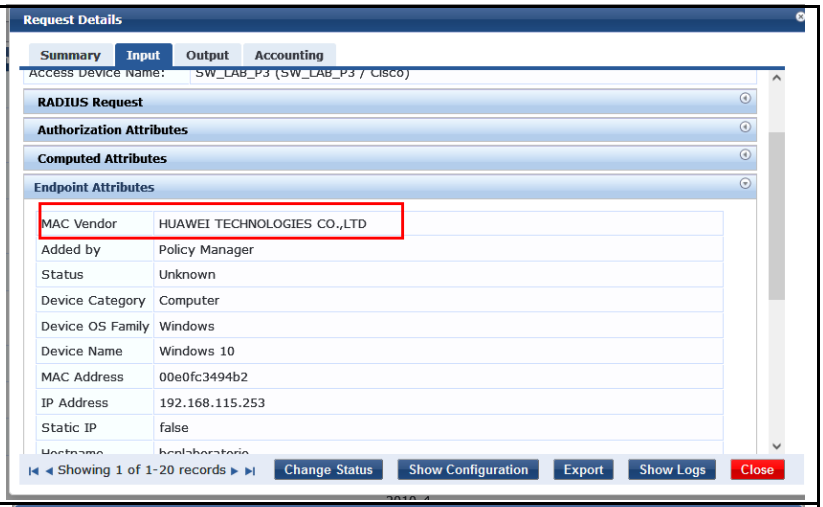
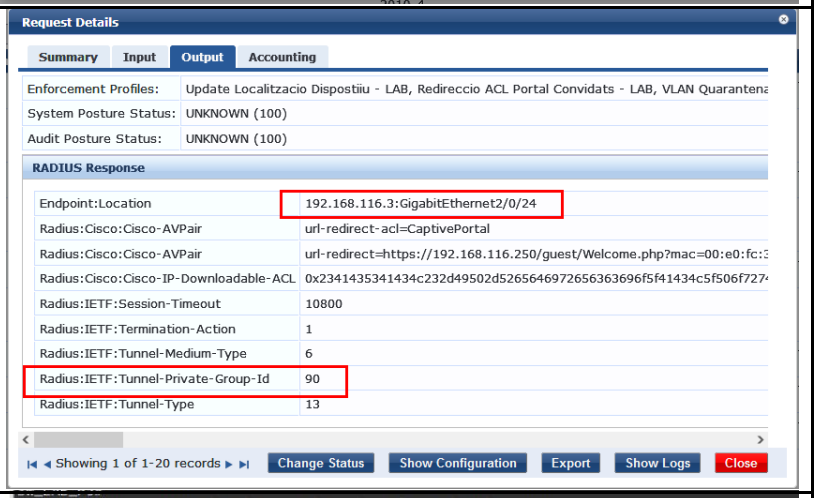
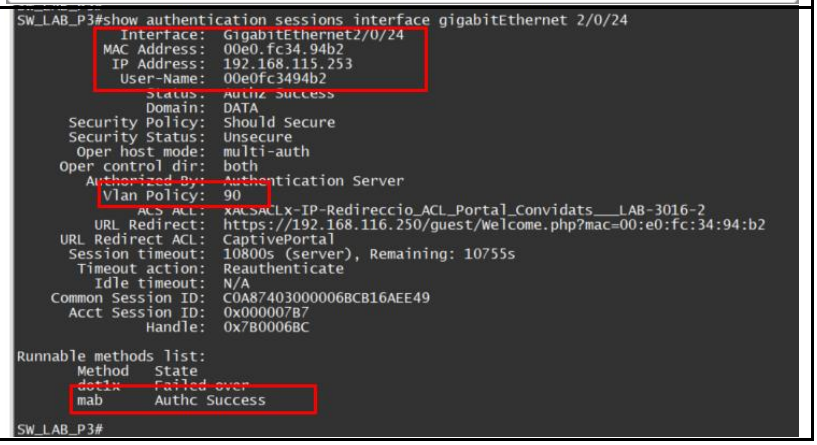
10.5.1 Evidències ClearPass - connexions lícites dels dispositius IoTs

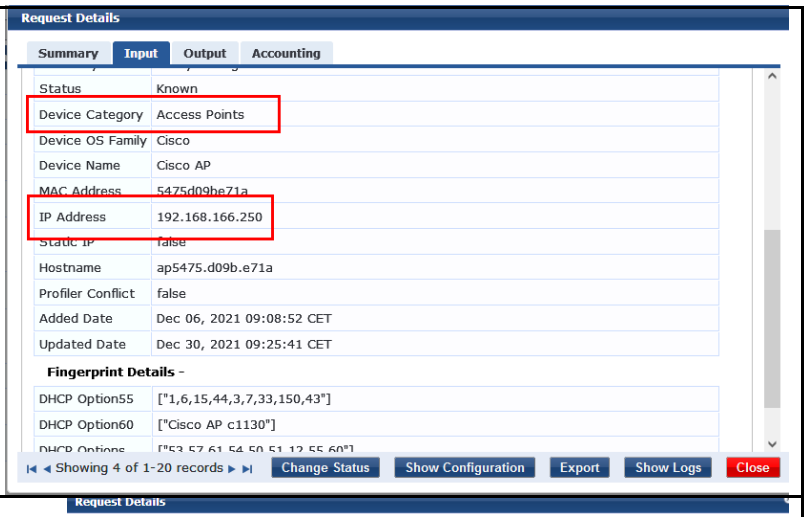
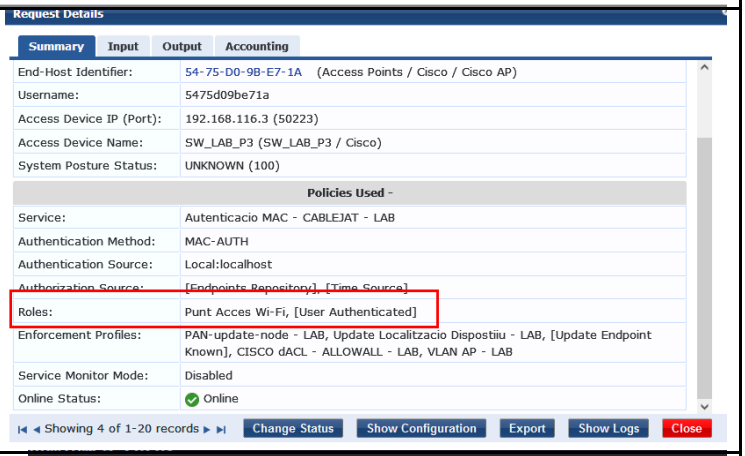
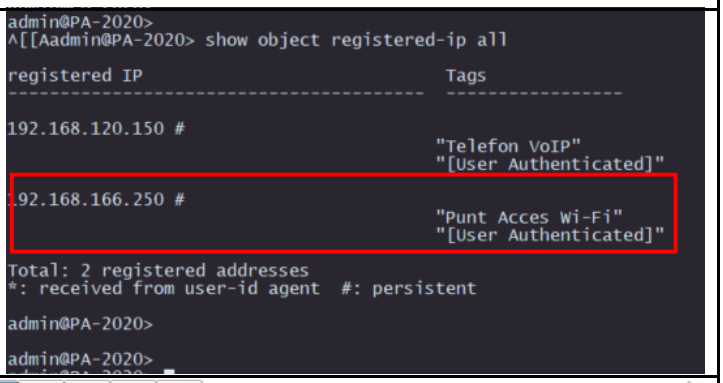
<table>
<tr><th colspan="3">Evidències connexions il·lícites de dispositius IoTs</th></tr>
<tr><th>Nº</th><th>descripció</th><th>Evidències</th></tr>
<tr><td>A.1.1</td><td>Informació obtinguda del perfilat del dispositiu telèfon IP segons col·lector.</td><td> 
</td></tr>
<tr><td>A.1.2</td><td>Informació obtinguda del perfilat del dispositiu punt d'accés segons col·lector.</td><td> 
</td></tr>
</table>

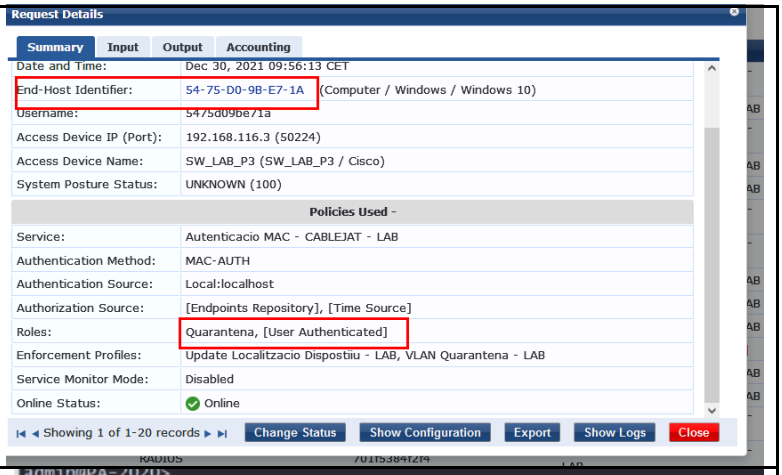
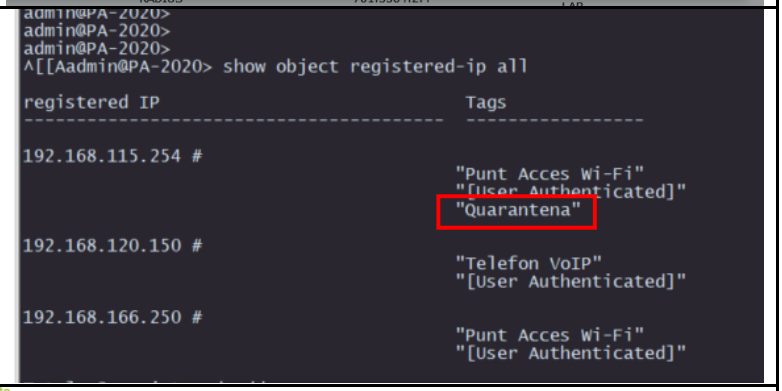
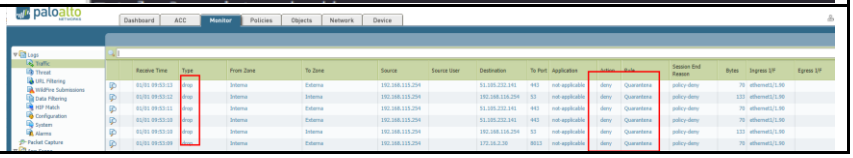
A.1.3	Dispositiu descoberts per les diferents tècniques de perfilat configurades, els quals no es tenia constància que estaven connectats.	
A.1.4	Es valida que en el cas de perfilar un dispositiu que no compleix cap política de seguretat d'admissió a la xarxa, aquest queda ubica en la vlan de quarantena.	
A.2.1	El telèfon IP, un cop perfilat, s'autentica correctament segon els atributs de perfilat definits en la política de seguretat.	
A.2.2	El Punt d'Accés , un cop perfilat, s'autentica correctament segon els atributs de perfilat definits en la política de seguretat.	

A.2.1 A.3.1	El telèfon IP, un cop perfilat, s'autentica correctament i s'ubica a la Vlan corresponent de telefonia. (Vlan 92)	  

A.2.2 A.3.2	El Punt d'Accés , un cop perfilat, s'autentica correctament i s'ubica a la Vlan corresponent de telefonia. (Vlan 66)	  

A.1.4 A.3.3	Es valida que, en el cas de perfilar un dispositiu que no compleix cap política de seguretat d'admissió a la xarxa, aquest queda ubicat en la vlan de quarantena (vlan 90)	  

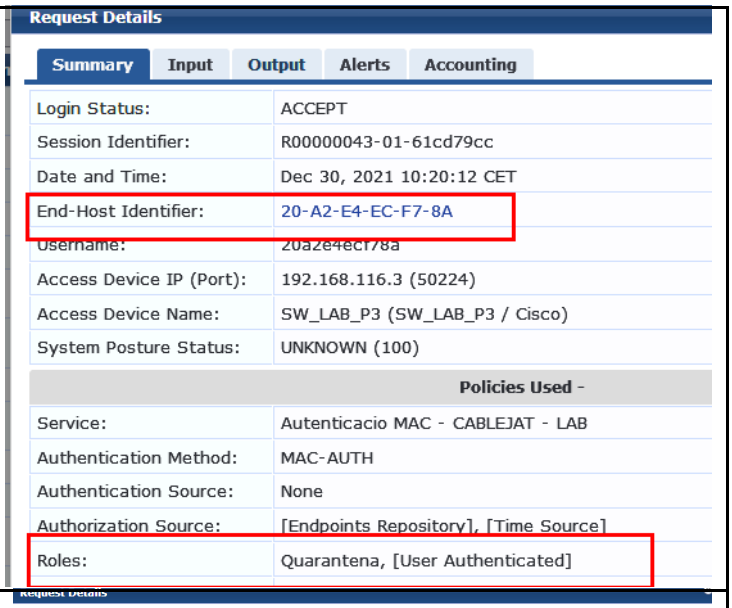
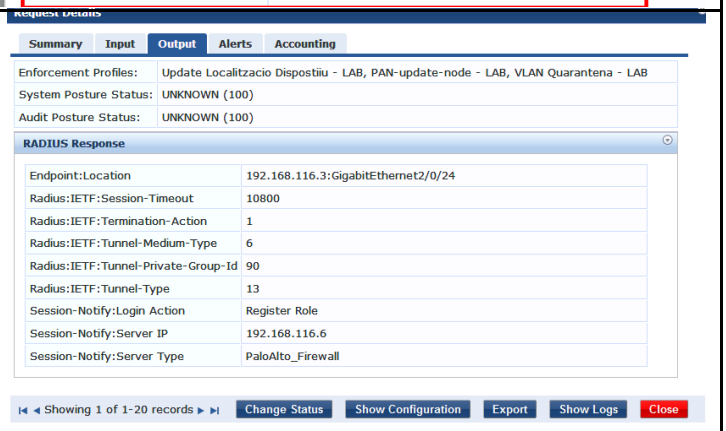
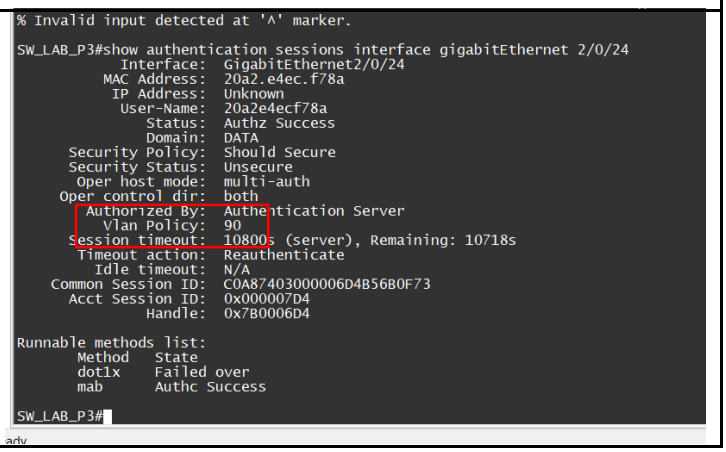
A.4	Es valida que els rols assignats per NAC de ClearPass als IoTs s'envien als Tallafocs amb la informació de la IP, per tal s'apliquin les regles de seguretat definides.	   

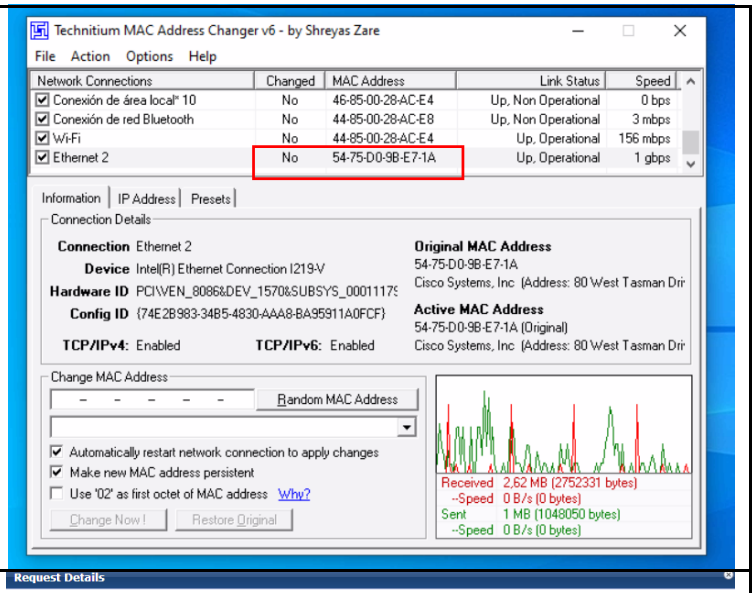
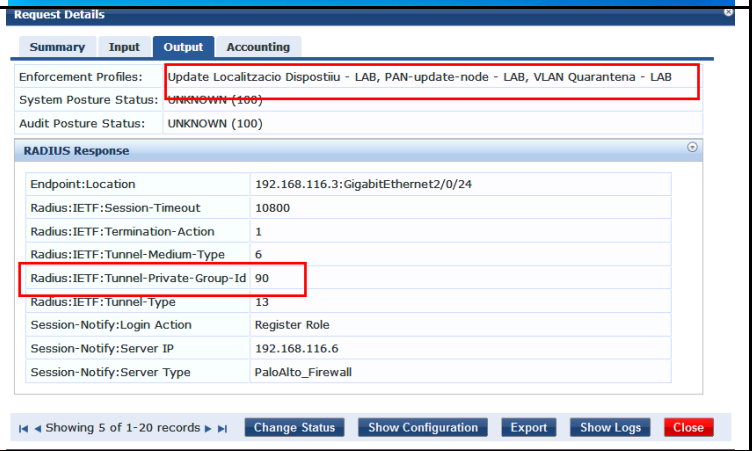
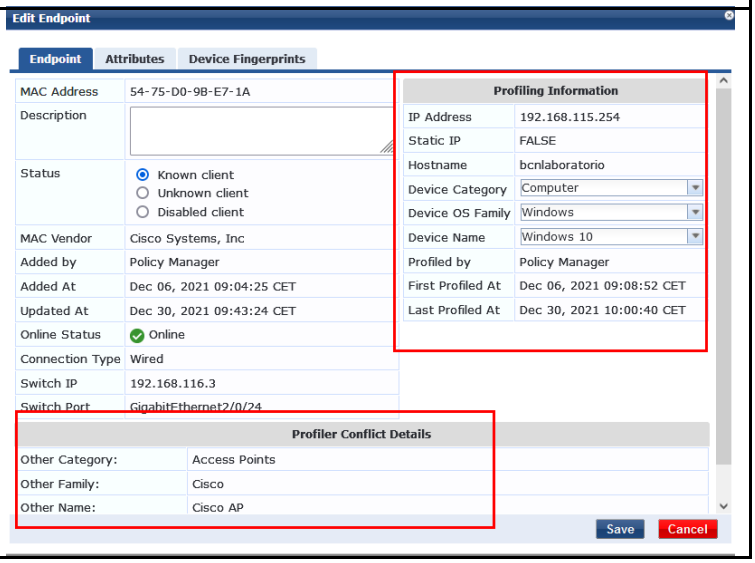
A.4	En el moment en que el ClearPass assigna un nou Rol al dispositiu, Quarantena, aquest s'envia al Palo Alto per tal apliqui les resgles corresponents	  

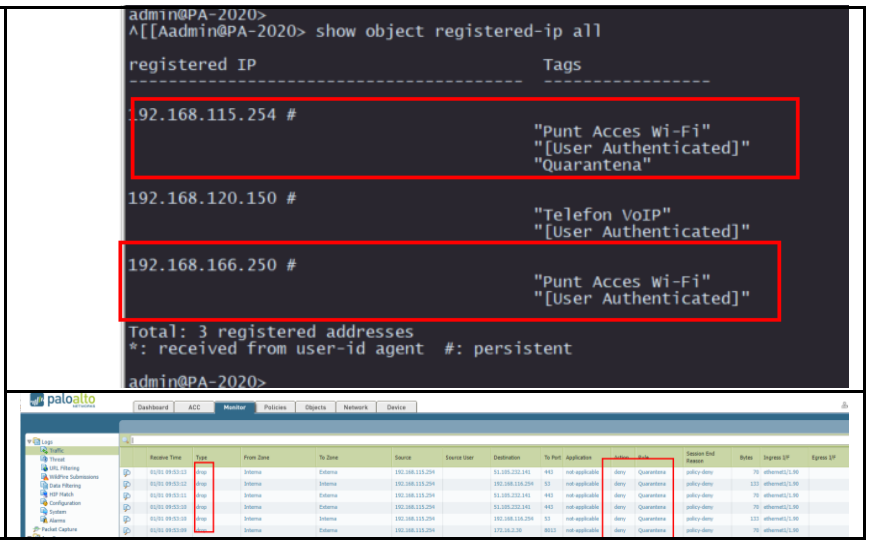
Taula 23: Evidències ClearPass - Connexions lícites

10.5.2 Evidències ClearPass - connexions malintencionades

Evidències connexions il·lícites de dispositius IoTs		
Nº	**descripció**	**Evidències**
B.1	Connexió a la xarxa amb IP estàtica. El dispositiu inicialment no té perfil i queda ubicat en la vlan quarantena.	

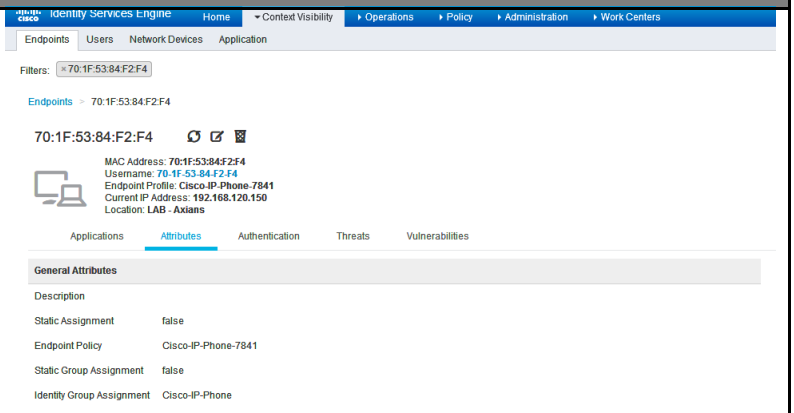
B.1	Connexió a la xarxa amb IP estàtica. El dispositiu inicialment no té perfil i queda ubicat en la vlan quarantena.		
			
			

B.2	Suplantació MAC d'un dispositiu IoT	  



Taula 24: Evidencies ClearPass - Connexions il·lícites

10.5.3 Evidències ISE - connexions lícites dels dispositius IoTs

Evidències connexions lícites de dispositius IoTs		
Nº	**descripció**	**Evidències**
A.1.1	Informació obtinguda del perfilat del dispositiu telèfon IP segons col·lector.	

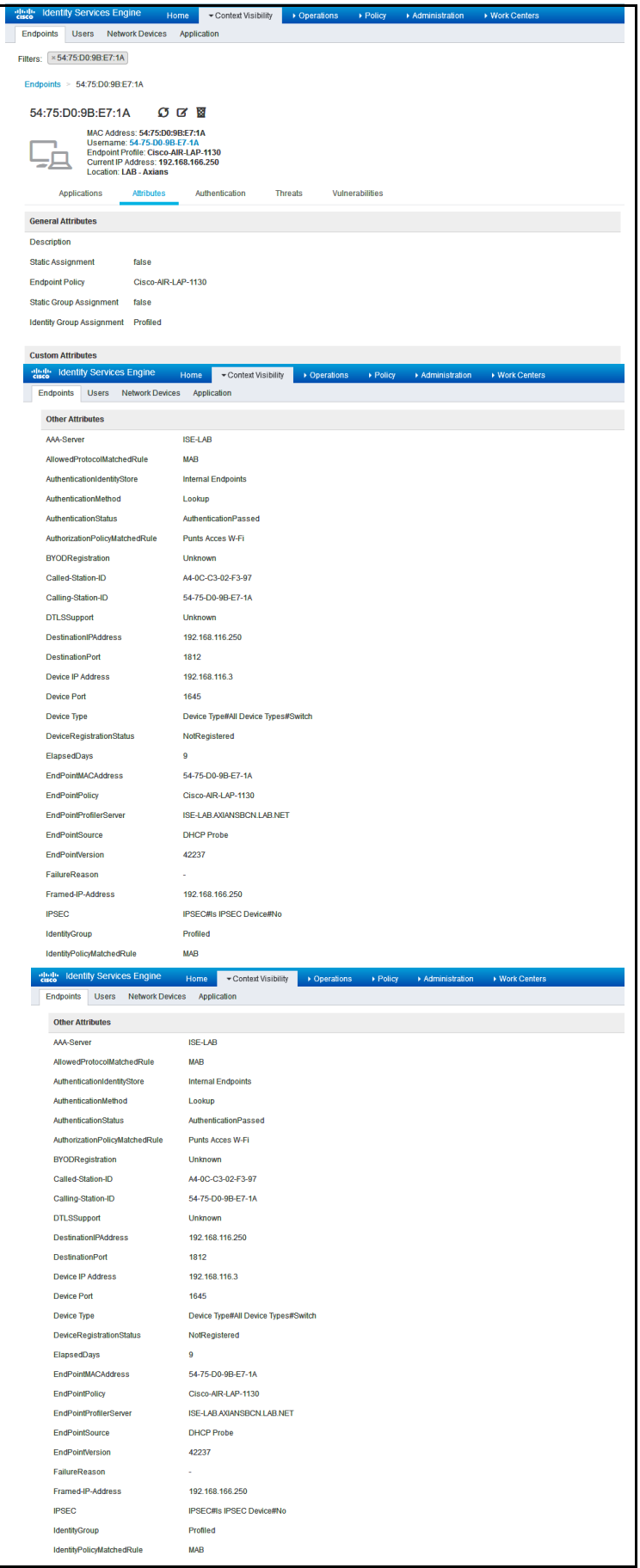
Endpoints | Users | Network Devices | Application

Other Attributes

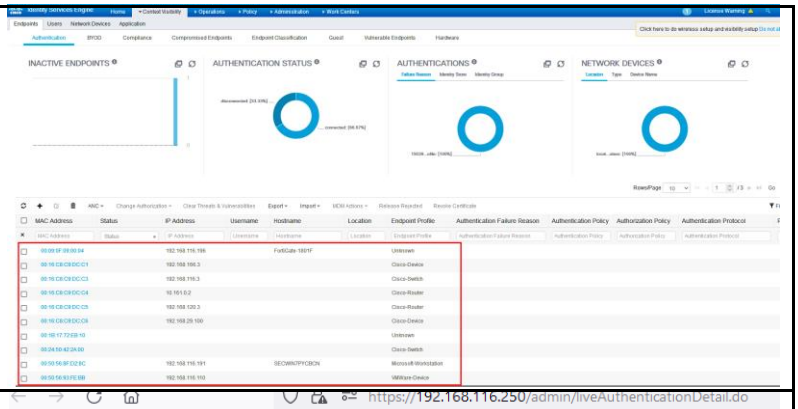
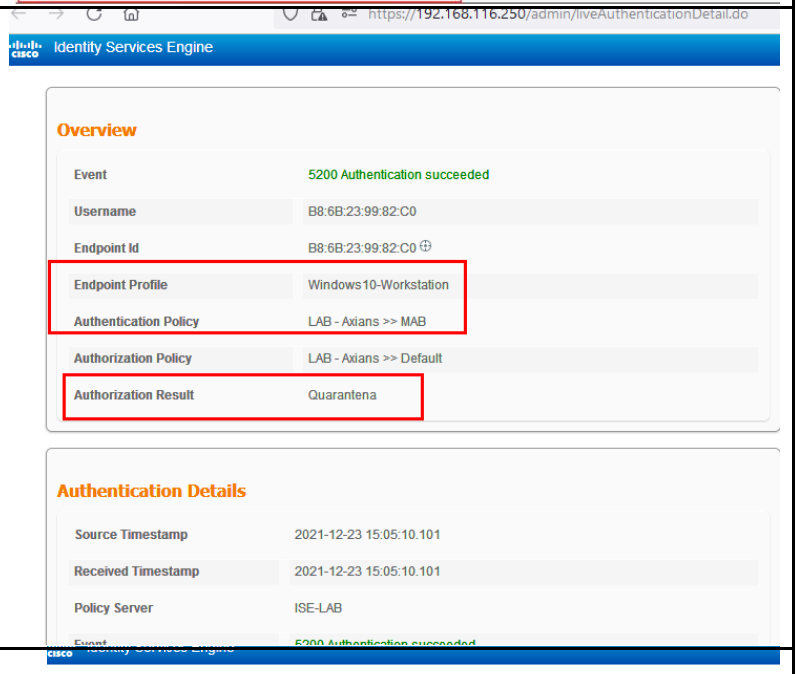
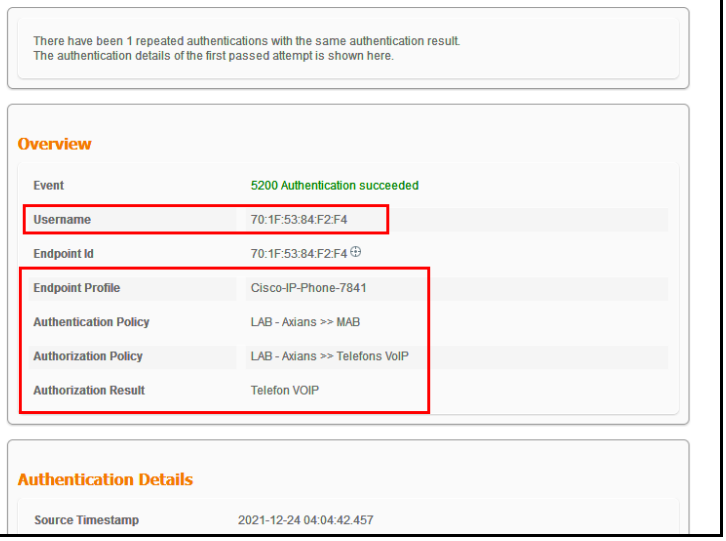
161-udp	snmp
162-udp	snmptrap
AAA-Server	ISE-LAB
AllowedProtocolMatchedRule	MAB
AuthenticationIdentityStore	Internal Endpoints
AuthenticationMethod	Lookup
AuthenticationStatus	AuthenticationPassed
AuthorizationPolicyMatchedRule	Telefons VoIP
BYODRegistration	Unknown
Called-Station-ID	A4-0C-C3-02-F3-96
Calling-Station-ID	70-1F-53-84-F2-F4
DTLSSupport	Unknown
DestinationIPAddress	192.168.116.250
DestinationPort	1812
Device IP Address	192.168.116.3
Device Port	1645
Device Type	Device Type#All Device Types#Switch
DeviceRegistrationStatus	NotRegistered
ElapsedDays	8
EndPointMACAddress	70-1F-53-84-F2-F4
EndPointPolicy	Cisco-IP-Phone-7841
EndPointProfilerServer	ISE-LAB.AXIANSBCN.LAB.NET
EndPointSource	DHCP Probe
EndPointVersion	904
FailureReason	-
Framed-IP-Address	192.168.120.150
IPSEC	IPSEC#Is IPSEC Device#No

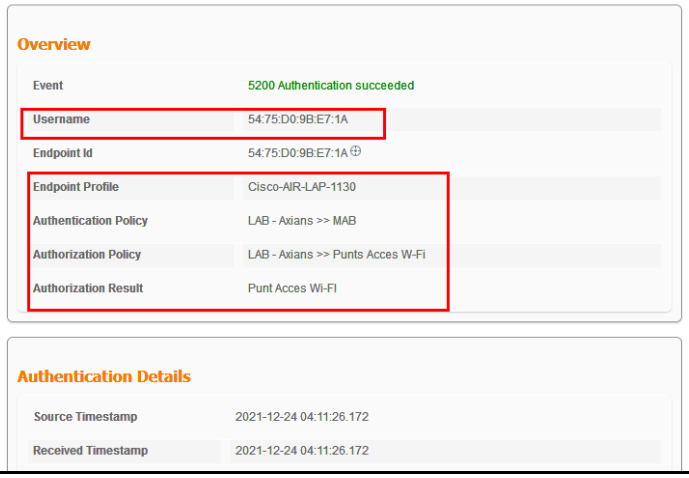
Endpoints | Users | Network Devices | Application

UserType	Host
allowEasyWiredSession	false
cdpCacheAddress	192.168.116.195
cdpCacheCapabilities	H;P;M
cdpCacheDeviceId	SEP701F5384F2F4
cdpCachePlatform	Cisco IP Phone 7841
cdpCacheVersion	sip78xx.11-5-1-18.loads
chaddr	70:1f:53:84:f2:f4
ciaddr	0.0.0.0
dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7841
dhcp-client-identifier	01:70:1f:53:84:f2:f4
dhcp-message-type	DHCPREQUEST
dhcp-parameter-request-list	1, 42, 66, 6, 3, 15, 150, 35
dhcp-requested-address	192.168.120.150
dot1xAuthAuthControlledPortControl	2
dot1xAuthAuthControlledPortStatus	2
flags	0x8000
giaddr	192.168.120.6
hlen	6
host-name	SEP701F5384F2F4
htype	Ethernet (10Mb)
ifDescr	GigabitEthernet2/0/22
ifIndex	10622
ifOperStatus	1
ip	192.168.120.150
op	BOOTREQUEST
yiaddr	0.0.0.0

A.1.2	Informació obtinguda del perfilat del dispositiu punt d'accés segons col·lector.	

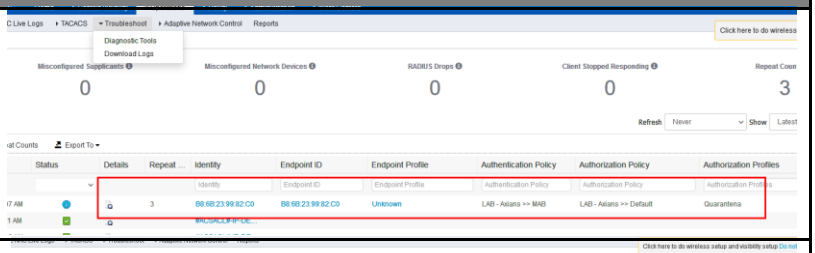
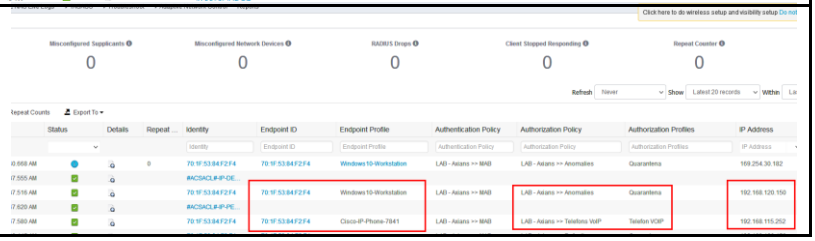
Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Endpoints
Users
Network Devices
Application
Other Attributes
AAA-Server ISE-LAB
AllowedProtocolMatchedRule MAB
AuthenticationIdentityStore Internal Endpoints
AuthenticationMethod Lookup
AuthenticationStatus AuthenticationPassed
AuthorizationPolicyMatchedRule Punts Acces W-Fi
BYODRegistration Unknown
Called-Station-ID A4-0C-C3-02-F3-97
Calling-Station-ID 54-75-D0-9B-E7-1A
DTLSSupport Unknown
DestinationIPAddress 192.168.116.250
DestinationPort 1812
Device IP Address 192.168.116.3
Device Port 1645
Device Type Device Type#All Device Types#Switch
DeviceRegistrationStatus NotRegistered
ElapsedDays 9
EndPointMACAddress 54-75-D0-9B-E7-1A
EndPointPolicy Cisco-AIR-LAP-1130
EndPointProfilerServer ISE-LAB.AXIANSBCN.LAB.NET
EndPointSource DHCP Probe
EndPointVersion 42237
FailureReason -
Framed-IP-Address 192.168.166.250
IPSEC IPSEC#Is IPSEC Device#No
IdentityGroup Profiled
IdentityPolicyMatchedRule MAB

A.1.3	Dispositiu descoberts per les diferents tècniques de perfilat configurades i els quals, d'entrada, no es tenia constància que estaven connectats a la xarxa	
A.1.4 A.3.3	Es valida que, en el cas de perfilar un dispositiu que no compleix cap política de seguretat d'admissió a la xarxa, aquest queda ubicat en la vlan de quarantena (vlan 90)	
A.2.1 A.3.1	El telèfon IP, un cop perfilat, s'autentica correctament i s'ubica a la Vlan corresponent de telefonia. (Vlan 92)	

A.2.2 A.3.2	El Punt d'Accés , un cop perfilat, s'autentica correctament i s'ubica a la Vlan corresponent de telefonia. (Vlan 66)	

Taula 25: Evidencies ISE - Connexions lícites

10.5.4 Evidències ISE - connexions malintencionades

Evidències connexions il·lícita de dispositius IoTs		
Nº	**descripció**	**Evidències**
B.1	Connexió a la xarxa amb IP estàtica. El dispositiu inicialment no té perfil i queda ubicat en la vlan quarantena.	
B.2	Suplantació MAC d'un dispositiu IoT	

Taula 26: Evidencies ISE - Connexions il·lícites