ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad

Maestría de Seguridad Informática Aplicada

"DISEÑO E IMPLEMENTACIÒN DEL CONTROL DE ACCESO A LA RED *CISCO IDENTIFY SERVICES ENGINE (ISE)*"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Jimmy Eduardo Jaén Solórzano

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

Agradezco a Dios sobre todas las cosas ya que por el tengo la fortaleza de seguir adelante día a día.

Agradezco a mis padres su amor, dedicación y honestidad sus valores me guían en el arduo camino de la vida.

A mis hermanos, familiares y amigos que me apoyaron en cada momento.

A mis instructores de la universidad Politécnica del Litoral, gracias por su paciencia, dedicación y motivación han hecho fácil lo difícil. Ha sido un privilegio contar con su ayuda.

DEDICATORIA

Dedico este trabajo de Tesis a Dios, él siempre está conmigo y mi familia.

De manera especial a mi hijo, su sonrisa es la motivación más importante.

A mi esposa gracias a sus consejos, paciencia, sacrifico y amor incondicional he logrado llegar hasta aquí. Mi familia es la inspiración más grande para ellos es el fruto de todo mi esfuerzo.

A mis padres con su amor, ejemplo y trabajo he logrado convertirme en lo que soy, ha sido un privilegio ser su hijo.

TRIBUNAL DE SUSTENTACIÓN

MGS. GONZALO LUZARDO	MSG. ROKY BARBOSA
PROFESOR DELEGADO POR LA	PROFESOR DELEGADO POR LA
SUBDECANA DE LA FIEC	SUBDECANA DE LA FIEC

RESUMEN

El presente trabajo pretende compartir la experiencia en el proceso de implementación de una solución de control de acceso seguro y controlado a los servicios de red de una empresa, con el objetivo primordial de brindar mayor seguridad a la red más vulnerable a ataques, que es la red de acceso, ya que facilita el acceso a intranet a los funcionarios, visitantes, contratistas, etc.

La herramienta Cisco ISE nos facilita el control de usuarios, utilizando el protocolo IEEE 802.1 x, en su validación utilizando un repositorio externo el cual es el Active Directory (AD).

Por lo antes expuesto y con la creciente evolución del acceso a la intranet a través de la movilidad de los diferentes dispositivos, se vuelve más importante en las empresas el contar con políticas de seguridad bien estructuras a nivel de la capa de acceso, ya sea en la red cableada e inalámbrica.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

802.1x	Es una norma del IEEE para el control de acceso a red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN.
AAA	Es el acrónimo de Authentication, Authorization y Accounting.
AD	Active Directory (AD), es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.
ADM	Equipo que posee el rol de administrador en la arquitectura de control de acceso a la red del CISCO IDENTITY SERVICE ENGINE - ISE.
AP	Access Point (AP) nomenclatura que describe los equipos que propagan los SSID de la red inalámbrica.
BYOD	Bring Your Own Device (BYOD), política empresarial consistente en que los empleados lleven sus propios dispositivos a su lugar de trabajo para tener acceso a recursos de la empresa.
CA	Certificate Authority (CA), Es una entidad de confianza, responsable de emitir y revocar los certificados digitales.

CWA	Central Web Authentication (CWA).
Dirección MAC	Es un identificado de 48 bits que corresponde al identificador único de la tarjeta de red (media access control).
DNS	Domain Name System (DNS) En el grupo de protocolos TCP-IP se encuentran los protocolos de resolución de nombres por direcciones IP.
DHCP	Dynamic Host Configuration Protocol (DHCP) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas.
EAP-MSCHAPV2	Protected Extensible Authentication Protocol es un protocolo que encapsula el protocolo de autenticación extensible (EAP) dentro de un cifrado y autenticado Transport Layer Security (TLS) del túnel.
HTTP	Hypertext Transfer Protocol, es el protocolo usado en cada transacción de la World Wide Web
IP	Protocolo de internet de comunicación digital a nivel de red.
ISE	Identity Services Engine
LAN	Local Area Network, red de área local

MAB	MAC Authentication Bypass, utiliza la dirección MAC de un dispositivo para determinar qué tipo de acceso se le ofrece en la red.
MON	Equipo que posee el rol de monitoreo en la arquitectura de control de acceso a la red del CISCO IDENTITY SERVICE ENGINE - ISE.
MNT	Monitoring and Troubleshooting Node
NAD	Network Access Device
NTP	Network Time Protocol
NOC	Centro de Operaciones de Redes
PAN	Policy Administration Node (PAN), nodo que permite a un administrador para realizar cambios en toda la topología de ISE
PSN	Equipo que posee el rol de políticas de servicio en la arquitectura de control de acceso a la red del CISCO IDENTITY SERVICE ENGINE - ISE.
SO	Sistema Operativo
SSID	Service Set Identifier(ssid), es el nombre de la red inalámbrica
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network
WLC	Wireless Lan Controler (WLC) controladora de Access Point.
WPA2-PSK	Wi-Fi Protected Access 2 - Pre-Shared Key, método de seguridad implementado enrede inalámbricas

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La seguridad de la información es el bien intangible más impotente de una organización, y la pérdida o difusión de la misma, puede y suele acarrear un daño económico y de prestigio que afecta a la empresa.

El presente proyecto de implementación tiene como objetivo incrementar el nivel de seguridad de la red de acceso de una empresa, implementado políticas de seguridad con la herramienta cisco ISE.

En el primer capítulo se expone el antecedente y problemática en donde se enmarca el desarrollo del presente trabajo.

El segundo capítulo se expone la situación actual del diseño de acceso a la red, la metodología de diseño a implementar, los requerimientos previa instalación y configuraciones a realizar.

El tercer capítulo se expone los resultados obtenidos pos-implementación Cisco ISE, sus mejoras obtenidas en las redes cableadas e inalámbricas, optimando el ingreso los usuarios de acuerdo a sus funciones y responsabilidades.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

La seguridad de las redes es ahora parte integral de las redes informáticas. Incluye protocolos, tecnologías, dispositivos, herramientas y técnicas que aseguran los datos y reducen las amenazas. Las soluciones de seguridad en redes surgieron en los años 1960 pero no se convirtieron en un conjunto exhaustivo de soluciones para redes modernas hasta el principio del nuevo milenio.

La mayor motivación de la seguridad en redes es el esfuerzo por mantenerse un paso más adelante de los hackers malintencionados. Del mismo modo que los médicos intentan prevenir nuevas enfermedades tratando problemas existentes, los profesionales de la seguridad en redes intentan prevenir ataques minimizando

los efectos de los ataques en tiempo real. La continuidad de los negocios es otro factor impulsor de la seguridad en redes. (Cisco)

Mantener una red segura garantiza la seguridad de los usuarios de la red y protege los intereses comerciales. Esto requiere vigilancia de parte de los profesionales de seguridad en redes de la organización, quienes deberán estar constantemente al tanto de las nuevas y evolucionadas amenazas y ataques a las redes, así como también de las vulnerabilidades de los dispositivos y aplicaciones. Esta información se utiliza para adaptar, desarrollar e implementar técnicas de mitigación.

"La necesidad es la madre de todos los inventos". (centlivre)

Este dicho se aplica perfectamente a la seguridad en redes. Cuando surgió Internet, los intereses comerciales eran insignificantes. La gran mayoría de los usuarios eran expertos en investigación y desarrollo. Los primeros usuarios raramente se involucraban en actividades que pudieran dañar a los otros usuarios. Internet no era un ambiente seguro porque no necesitaba serlo.

Con lo expuesto anteriormente surge la necesidad de contar con herramientas que mitiguen riesgos en temas de seguridad informática, en nuestro caso en especial el acceso a la red con la herramienta Cisco Identity Services Engine (ISE) la que ofrece:

Reducir las fronteras de acceso a los recursos de red, preservando políticas de acceso, reduciendo riesgos de intrusión, incrementando la seguridad de acceso, brindando mayor flexibilidad y control a personal administrativo de TI. Ya sea porque deba implementar prácticas de trabajo en las que cada empleado trae su propio dispositivo (bring your own device, (BYOD) u ofrecer un acceso más seguro a los recursos de la empresa.

1.2. Descripción del Problema

En la actualidad existen amenazas latentes que buscan atacar las redes institucionales para afectar su continuidad, extraer información y mal utilizar los recursos de red, por lo cual las redes empresariales se encuentran ante nuevos retos, como es el aseguramiento del acceso de usuarios internos y externos a los recursos de la red empresarial, debido a que a través de la red, fluye información que debe llegar a los destinatarios adecuados, velar su confidencial y garantizar el acceso oportuno a la misma.

El acceso a la red ya no solo se limita en tener acceso a un punto de red habilitado por descuido en una oficina o sala de sesiones, con la creciente demanda de movilidad el personal de TI se ve en la obligación de facilitar el acceso a través de la red inalámbrica, una herramienta muy útil para el acceso de funcionarios, pero una ventana para hackers a la intranet de una empresa, si esta no posee políticas de control de acceso adecuadas.

Uno de los principales problemas que tenemos los administradores de TI es cuando se divulga la clave de un SSID en una empresa, al manejar redes corporativas el simple hecho de cambiar la clave ya no cabe, por lo que se torna imperativo poseer una herramienta que nos facilite el control de acceso a cada uno de los dispositivos móviles de la empresa.

1.3. Descripción de la solución propuesta

Ante los retos antes mencionados es necesario implementar soluciones de seguridad que permitan brindar la visibilidad y control del acceso a los recursos de red de cada funcionario interno y externo, mitigando los riegos de seguridad.

Una estrategia de seguridad de la información es disponer de elementos de red que permitan habilitar un control de acceso perimetral, como son los firewalls y hoy es crítico implementar una solución de control de acceso a recursos de red basados en contexto, es decir que permita a los administradores de red, establecer políticas para el acceso, que identifiquen al usuario, dispositivos mediante los cuales se accede a la red, lugar y hora de ingreso a la red institucional y que los recursos habilitados sean los adecuados.

Como se dispone de una red empresarial basada en elementos del fabricante Cisco, es conveniente implementar una solución de control de acceso a la red del mismo fabricante, que garantice su completa integración y la explotación al

máximo de sus funcionalidades, reducir los tiempos de implementación y operación de la plataforma.

Los beneficios que ofrece la solución son:

Aplicación uniforme de políticas contextuales en las redes fijas e inalámbricas.

Visibilidad de todo el sistema para saber qué y quiénes están en la red fija e inalámbrica.

Autenticación, autorización y accounting (AAA) integradas, perfiles, servicios para usuarios temporales, disponibilidad de aplicar postura.

Disponibilidad de cumplimiento de normas de los dispositivos móviles basado en políticas y aprovisionamiento de aplicaciones mediante soluciones integradas de gestión de múltiples dispositivos.

Total integración con el sistema de gestión de infraestructura de red operativo actualmente, con la finalidad de mediante una sola consola tener una visibilidad de los usuarios en la red.

CAPÍTULO 2

METODOLOGÍA DE LA SOLUCIÓN

2.1. Situación actual de la red

Actualmente el acceso a los recursos de red en las diferentes localidades de una empresa, se lo realiza de forma cableada o inalámbrica. Para el acceso a la red de forma cableada no se tiene un control establecido, más que el acceso físico a los puntos de red, para el acceso a la red de forma inalámbrica se tiene un control basado en contraseñas generales; debido a que el cambio de contraseñas, involucra la reconfiguración de las portátiles, no es factible realizarlo periódicamente, lo que ocasiona que las claves sean difundidas sin autorización.

Además del control de acceso a la red, es necesario definir niveles de autorización, con el fin de que solo los usuarios autorizados accedan a los recursos asignados,

actualmente a nivel de red se tienen controles básicos de autorización basado en vlans, pero debido a que este control es basado en puertos físicos de los switches y no en las credenciales de los usuarios, el constante movimiento de los usuarios ocasiona complejidad en la gestión de los controles indicados.

Como base de referencia para la definición o creación de la metodología, se toma como referencia las mejores prácticas de instalación recomendadas por Cisco.

Previa instalación de la herramienta cisco ISE es necesario considerar que se debe poseer previamente una arquitectura de red con tecnología Cisco, la que nos permite:

• Tener una matriz corporativa única de Networking.

• Implementación de una red jerárquica.

• Mejorar las operaciones de la red mediante la utilización de soluciones propietarias, permitiendo obtener niveles altos de confiabilidad, flexibilidad, disponibilidad y escalabilidad.

• Garantizar un stock de repuestos y accesorios de una sola marca, que incide directamente en los costos de mantenimiento y operación.

• Permite una red escalable con la implementación de soluciones a nivel de servidores, si se necesitan nuevos servicios o más recursos se colocan más servidores con más aplicaciones de telefonía y automáticamente toda la plataforma queda disponible para los nuevos servicios.

• Poseen un único esquema de convergencia, redistribución y enrutamiento generando una red robusta y homogénea.

En el siguiente cuadro se muestra el cuadrante de Gartner (Diciembre de 2014) de soluciones de control de acceso a la red, observándose a Cisco dentro del cuadrante de líderes en la solución de wired y Wireless Access lan.

Figura No.2.1 Cuadrante Gartner control de acceso de red (Gartner, 2015)

2.1.1 Situación actual de acceso en red Wired.

La empresa no dispone de seguridad a nivel de acceso en la red LAN Wired. Todos los puertos de los switches de acceso, se encuentran en modo acceso perteneciente a una Vlan específica, dependiendo del servicio a ofrecer, sin

restricción alguna los puertos en cada uno de los switches de acceso se encuentran habilitados

2.1.2 Situación actual de acceso en red Wireless.

La solución de la red inalámbrica se encuentra centralizada y configurada en una WLC, la seguridad a nivel Wireless es en capa 2 con WAP2-SPK, esta seguridad se encuentra en todos los SSID de la empresa.

2.2 Requisitos de Implementación

2.2.1 Requerimientos de direccionamiento IP.

Es necesario disponer de los siguientes datos para la conexión a la red.

Username, Dirección IP, mascara, Gateway, domain, dns, ntp.

2.2.2 Disponer de Certificate Authority (CA)

Es necesario realizar el proceso de certificación con cada uno de los appliances cisco ISE con CA para que exista una relación de confianza entre Cisco ISE.

2.2.3 Requerimientos para NAD. (switches, WLC)

Para que exista una compatibilidad idónea de los equipos NAD con cisco ISE 1.2 será necesario seguir la siguiente tabla de compatibilidad, tanto en modelo y versión de IOS. Para lo cual se requieren que los equipos que se integrarán con ISE se encuentren registrados en el Cisco Prime.

Tabla 1. Compatibilidad con IOS de switches Y WLC Cisco (Cisco Systems, 2014)

Access Switches										
Device	**Recommended OS Version [1]**	**MAB**	**802.1X**	**Web Auth**		**Session CoA**	**VLAN**	**dACL/ Named ACL [2]**	**TrustSec [3]**	**Device Sensors**
				CWA	**LWA**					
Catalyst 2960, ISR EtherSwitch ES2 (Catalyst 2960-S, Catalyst 2960-C)	IOS v 12.2(55)-SE3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Catalyst 2960-SF, Catalyst 2960Plus	IOS v 15.0.2-SE (ED) LAN BASE [4]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Catalyst 2960–XR, Catalyst 2960–X	IOS v 15.0.2-EX3 (ED)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Catalyst 3560-C Catalyst 3560-E, ISR EtherSwitch ES3 Catalyst 3560-X	IOS v 15.0.2-SE2 (ED)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Catalyst 3750-G	IOS v 12.2(55)-SE3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Catalyst 3750-E Catalyst 3750-X	IOS v 15.0.2-SE2 (ED) IP BASE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Catalyst 3850, 3650 [5]	IOS XE 3.2.2 SE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Catalyst 4500 Supervisor Engine 7-E, 7L-E	IOS-XE v 3.4.0 SG (ED)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Catalyst 4500 Supervisor Engine 6-E, 6L-E	IOS v 15.1.2 SG (ED)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Catalyst 6500 (Supervisor 32/Supervisor 720)	IOS v 12.2(33)-SXJ5 (MD)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Wireless [2]										
Device	**Recommended OS Version**	**MAB**	**802.1X**	**Web Auth**		**Session CoA**	**VLAN**	**dACL/ Named ACL**	**TrustSec**	**Device Sensors**
				CWA	**LWA**					
Wireless LAN Controller (WLC) 2100 [6]	7.0.116.0(ED)	No [7]	Yes	No	Yes	Yes	Yes	Yes	No	No
Wireless LAN Controller (WLC) 4400 [6]	7.0.116.0(ED)	No [7]	Yes	No	Yes	Yes	Yes	Yes	No	No
Wireless LAN Controller (WLC) 2500 [8]	7.3.112.0.(ED), 7.4.x, 7.5	Yes[9]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Wireless LAN Controller (WLC) 5500 [8]	7.3.112.0.(ED), 7.4.x, 7.5	Yes[9]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wireless LAN Controller (WLC) 7500 [8]	7.3.112.0.(ED), 7.4.x, 7.5	Yes[9]	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Wireless LAN Controller (WLC) 8500 [8]	7.3.112.0.(ED), 7.4.x, 7.5	Yes[9]	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
WiSM1 Blade for 6500	7.0.116.0(ED)	No [7]	Yes	No	Yes	Yes	Yes	Yes	No	No
WiSM2 Blade for 6500	7.0.116.0(ED)	No [7]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
WLC 5760	IOS XE 3.2.2 SE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

2.2.4 Compatibilidad con External Identity Source.

Para que exista una compatibilidad idónea de External Identy Source con cisco ISE 1.2 será necesario seguir la siguiente tabla de compatibilidad.

Para que exista la integración de cisco ISE con AD es necesario disponer de User y Password con privilegios de agregar y borrar dispositivos en el AD.

Tabla 2. Compatibilidad con external identity Source (Cisco Systems, 2014)

External Identity Source	OS/Version
Active Directory 12 · 13 · 14	
Microsoft Windows Active Directory 2003	—
Microsoft Windows Active Directory 2003 R2	—
Microsoft Windows Active Directory 2008	—
Microsoft Windows Active Directory 2008 R2	—
Microsoft Windows Active Directory 2012	—
Microsoft Windows Active Directory 2012 R2 15	—
LDAP Servers	
SunONE LDAP Directory Server	Version 5.2
OpenLDAP Directory Server	Version 2.4.23
Token Servers	
RSA ACE/Server	6. *x* series
RSA Authentication Manager	7. *x* and 8.0 series
Any RADIUS RFC 2865-compliant token server	—

2.2.5 Sistema Operativo compatible con cisco ISE 1.2

Los equipos PCs con S.O que son soportados para validación 802.1x con cisco ISE 1.2 son los siguientes.

Tabla 3. Compatibilidad con IOS de Windows PC (Cisco Systems, 2014)

Table 6 Microsoft Windows 22

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE	Cisco NAC Agent	Cisco NAC Web Agent
Microsoft Windows 8 23,24,25					
Windows 8 Windows 8 x64 Windows 8 Professional Windows 8 Professional x64 Windows 8 Enterprise Windows 8 Enterprise x64	• Microsoft IE 10	• Microsoft Windows 8 802.1X Client	1.2.x	4.9.4.3	4.9.4.3
Microsoft Windows 726					
Windows 7 Professional Windows 7 Professional x64 Windows 7 Ultimate Windows 7 Ultimate x64 Windows 7 Enterprise Windows 7 Enterprise x64 Windows 7 Home Premium Windows 7 Home Premium x64 Windows 7 Home Basic Windows 7 Starter Edition	• Microsoft IE 9, 10 27 • Google Chrome 11, 12, 13, 14, 15, 16 • Mozilla Firefox 3.6, 4, 5, 9	• Microsoft Windows 7 802.1X Client • AnyConnect Network Access Manager	1.2.x	4.9.4.3	4.9.4.3
Microsoft Windows Vista 5					

Windows Vista SP1, SP2 Windows Vista x64 SP1, SP2	• Microsoft IE 6, 7, 8, 9 • Google Chrome 8, 9, 11, 12, 13, 14, 15, 16 • Mozilla Firefox 3.6, 4, 5, 9	• Microsoft Windows Vista 802.1X Client • Cisco Secure Services Client (SSC) 5. *x* • AnyConnect Network Access Manager	1.2.x	4.9.4.3	4.9.4.3
Microsoft Windows XP 5					
Windows XP Media Center Edition, SP2, SP3 Windows XP Tablet PC, SP2, SP3 Windows XP Home, SP2 Windows XP Professional SP2, SP3 Windows XP Professional x64, SP2	• Microsoft IE 6, 7, 8, 9 • Google Chrome 11, 12, 13, 14, 15, 16 • Mozilla Firefox 3.6, 9	• Microsoft Windows XP 802.1X Client • Cisco Secure Services Client (SSC) 5. *x* • AnyConnect Network Access Manager	1.2.x	4.9.4.3	4.9.4.3

2.2.6 Sistemas Operativos y browsers soportados para portal sponsor

Los sistemas operativos y browsers soportados para el portal sponsor son los siguientes:

Tabla 4. Compatibilidad con IOS de browsers (Cisco Systems, 2014)

Supported Operating System	Browser Versions
Google Android [29] 4.1.2, 4.0.4, 4.0.3, 4.0, 3.2.1, 3.2, 2.3.6, 2.3.3, 2.2.1, 2.2	• Native browser • Mozilla Firefox 5, 16

Apple iOS 6.1, 6, 5.1, 5.0.1, 5.0	• Safari 5, 6
Apple Mac OS X 10.5, 10.6, 10.7, 10.8	• Mozilla Firefox 3.6, 4, 5, 9, 14, 16 • Safari 4, 5, 6 • Google Chrome 11
Microsoft Windows 8[30]	3 Microsoft IE 10
Microsoft Windows 7[31]	• Microsoft IE 9, 10 [32] • Mozilla Firefox 3.6, 5, 9, 16 • Google Chrome 11
Microsoft Windows Vista, Microsoft Windows XP	• Microsoft IE 6, 7, 8 • Mozilla Firefox 3.6, 9, 16 • Google Chrome 5
Red Hat Enterprise Linux (RHEL) 5	• Mozilla Firefox 3.6, 4, 5, 9, 16 • Google Chrome 11
Ubuntu	Mozilla Firefox 3.6, 9, 16

2.2.7 Dispositivos y sistema operativo soportados para BYOD.

Los dispositivos y sistema operativo soportados para BYOD son los siguientes.

Tabla 5. Compatibilidad con IOS de dispositivos móviles (Cisco Systems, 2014)

Device	**Operating System**	**Single SSID**	**Dual SSID (open > PEAP (no cert) or open > TLS)**	**Onboard Method**
Apple iDevice	iOS 4	No	Yes[33]	Apple profile configurations (native)
Apple iDevice	iOS 5 and 6	Yes		

Android	2.2 and above[34]	Yes	Yes	Cisco Network Setup Assistant
Barnes & Noble Nook (Android) HD/HD+ [35]	—	—	—	—
Windows	Windows XP, Windows Vista, Windows 7, Windows 8	Yes[36]	Yes	SPW from Cisco.com or Cisco ISE Client Provisioning feed
Windows	Mobile 8, Mobile RT, Surface 8, and Surface RT	No	No	—
MAC OS X[37]	10.6, 10.7, 10.8	Yes	Yes	SPW from Cisco.com or Cisco ISE client provisioning feed

2.3 Desarrollo de la metodología a implementar

2.3.1 Descripción de la arquitectura propuesta

La arquitectura de control de acceso a la red propuesta, CISCO IDENTITY SERVICE ENGINE - ISE, se basa en nodos que cumplen roles específicos:

- **Rol administrador - ADM**. Permite realizar todas las operaciones administrativas. Maneja todas las configuraciones relacionadas con el sistema y las configuraciones que se relacionan con la funcionalidad de autenticación, autorización y auditoría. En un entorno distribuido, puede tener sólo uno o un máximo de dos nodos que ejecutan el rol de administración.

- **Rol Monitoreo - MON.** Permite al Cisco ISE funcionar como el colector de mensajes de registro y de repositorio de toda la información de administración creada para usuarios, grupos y dispositivos, y repositorio de la información de políticas de servicio para los nodos ISE PSN. El rol de monitoreo proporciona herramientas avanzadas de monitoreo y solución de problemas sobre los elementos de red y sus recursos. Un nodo con este rol, permite agregar y correlacionar los datos que recopila para ofrecer información significativa mediante informes. Cisco ISE permite tener un máximo de dos nodos con este rol que puede asumir funciones primarias o secundarias para alta disponibilidad.

- **Rol Politicas De Servicio - PSN**. Proporciona políticas de acceso a la red, postura, acceso de invitados, aprovisionamiento de clientes, y perfiles de servicio. Este rol evalúa las políticas y toma todas las decisiones. Puede tener más de un nodo con este rol dentro de la red. Todos los nodos de política de servicio de CISCO ISE residen detrás de un equilibrador de carga y comparten una dirección de multidifusión común, se pueden agrupar para formar un grupo de nodos. Si uno de los nodos en un grupo de nodos falla, los otros nodos detectan el fallo y restablecen las sesiones pendientes.

  De acuerdo al análisis de la topología de red, número de usuarios y distribución zonal que dispone la empresa, se recomienda adoptar un modelo con redundancia de nodos ADM+MON y PSN de respaldo centralizado, y distribuir

nodos PSN por el resto de zonas. Este modelo soporta 2 nodos ADM, 2 nodos MON y 5 nodos PSN.

Se puede concentrar en Zona Norte el rol de ADM y MON con redundancia, además de un PSN robusto que será el backup de las otras zonas considerando a la Zona Norte como el punto central de la red, debido que la topología de red de la empresa es en estrella.

En la Zona Norte se tendrá redundancia en ADM y MON, los cuales concentran la administración y monitoreo de todas las zonas, en las otras zonas se tendrán equipos ISE con el rol de Policy Service (PSN).

En este tipo de configuraciones tenemos la limitante que solo podemos manejar hasta 5 PSN los cuales ya estarían integrados.

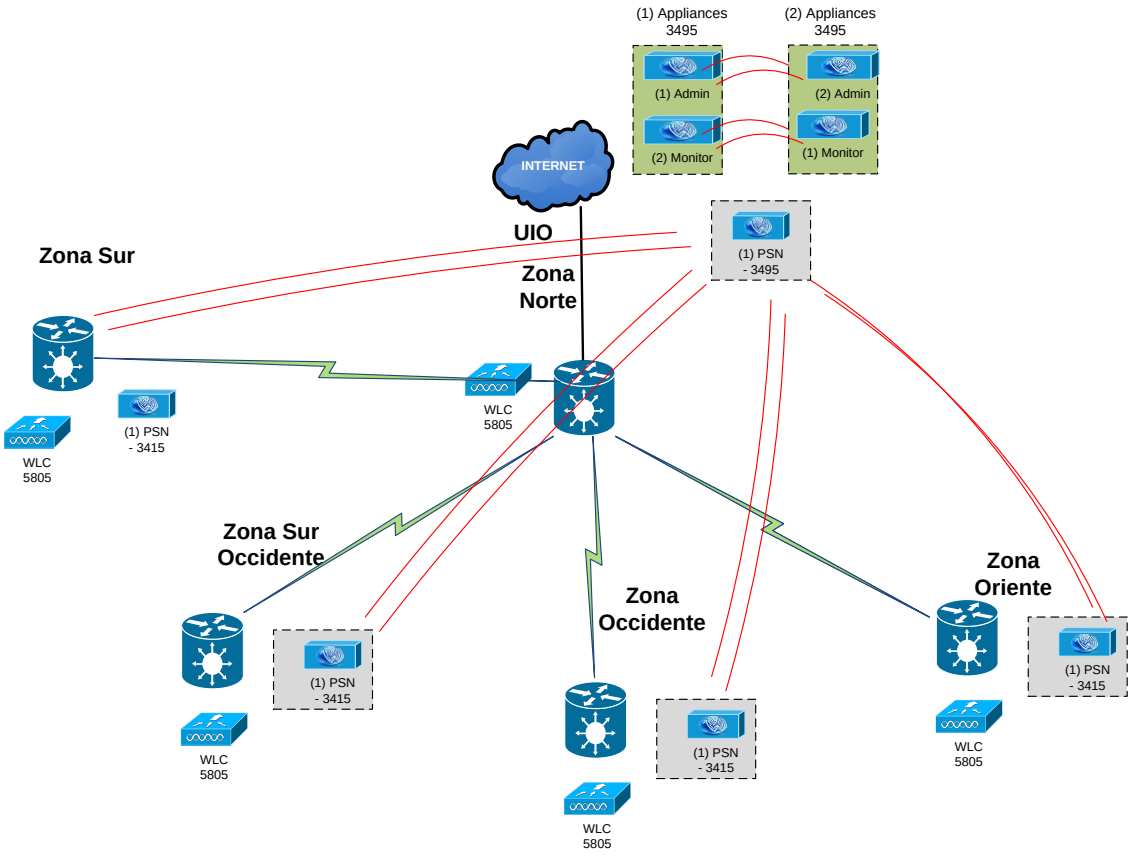

Figura No.2.2 Arquitectura y distribución de Control de Acceso a la Red

2.3.2 Diseño de la parte Core de sistema cisco ISE.

En el diseño de la parte Core del plan de implementación se propone 3 nodos cisco ISE 3495, 2 nodos cisco ISE 3495 en redundancia, cada uno de estos con el rol de Admin, Monitor, el tercer nodo 3495 como Policy Services.

Se dispondrá del nodo principal con los siguientes roles: ISE-1

Admin (Primario)

Monitor (Secundario)

Para el segundo nodo secundario se dispondrá de los siguientes roles: ISE-2

Admin (secundario)

Monitor (Primario)

Para el segundo nodo secundario se dispondrá de los siguientes roles. ISE-3

PSN (Activo)

En este tipo de configuración se tiene el server ISE-1 esta como el primario para PAN y el secundario para MNT. Server ISE-2 esta como secundario para PAN y como primario para MNT. Para el balanceo de roles entre el primario y secundario, la carga de trafico será balanceada mientras se mantiene la alta disponibilidades de la solución.

Figura No.2.3 Esquema alta Disponibilidad (Cisco Systems, 2014)

2.3.3 Esquema de trabajo de cisco ISE con NAD, External Data Base, EndPoints.

Todas las configuraciones son realizadas en Admin (PAN) y son enviadas al Policy Service (PSN), cuando un Endpoint accede a la red, El Network Access Devices (NAD) (Switche, WLC) se comunican con ISE usando RADIUS. Los dispositivos de red envían diferentes tipos de trafico como (HTTP, span, dhcp span, dhcp relay, NetFlow/ snmp QueryTraps, esta información es dirigida hacia la interface del PSN para profiling, información de Loggin de todas las personas es también intercambiado hacia el Monitor (MNT)

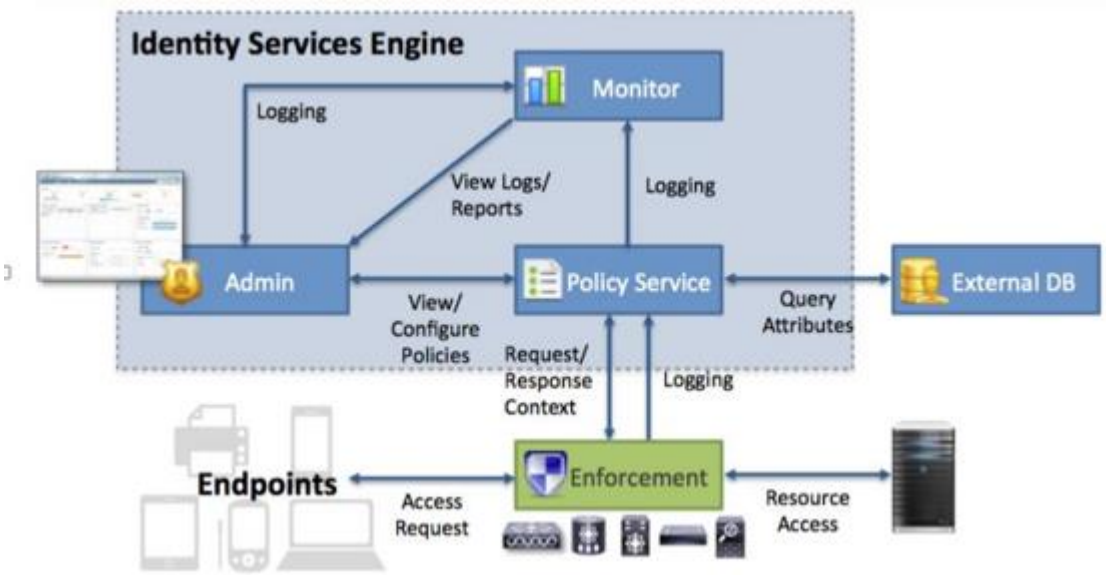

Figura No.2.4 Arquitectura ISE (Cisco Systems, 2014)

2.3.4 Parámetros iniciales de configuración cisco ISE.

A continuación se detallan los parámetros iniciales de configuración de cisco ISE para la solución requerida en autenticación y autorización.

2.3.4.1 Parámetros básicos de acceso a red.

En la configuración inicial de los dispositivos cisco ISE es necesario una dirección IP, Host Name, DNS, NTP.

2.3.4.2 Configuración de Certificados.

Para esta tarea es necesario realizar una relación de confianza entre cisco ISE y la unidad certificadora como un trusted root CA.

Es necesario realizar la configuración de Certificados con todos y cada uno de los equipos cisco ISE.

2.3.4.3 Integración de cisco ISE con AD.

Para esta tarea es necesario contar con una cuenta Admin con permisos suficientes para integrar el equipo cisco ISE con AD, la cuenta proporcionada tiene que tener permisos de agregar o quitar equipos del AD, para ello

necesitamos **Domain Name (eppec.ec)** para conectarse con el **Identity Store Name. (AD_EPPEC)**

Es necesario realizar la configuración de AD con todos y cada uno de los equipos cisco ISE.

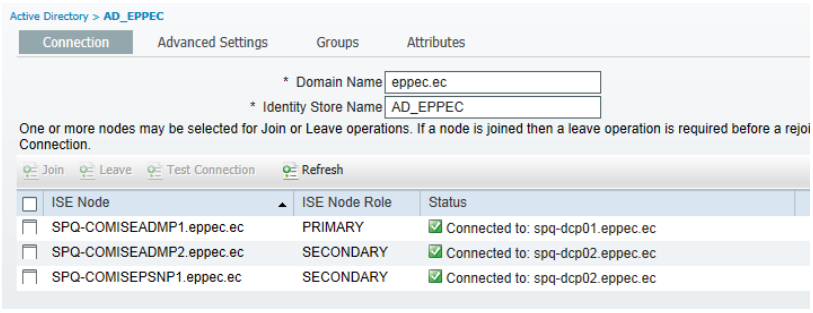

Figura No 2.5 Integración AD

Con esta integración podemos seleccionar los grupos en el AD necesarios para aplicar las políticas de autenticación y autorización.

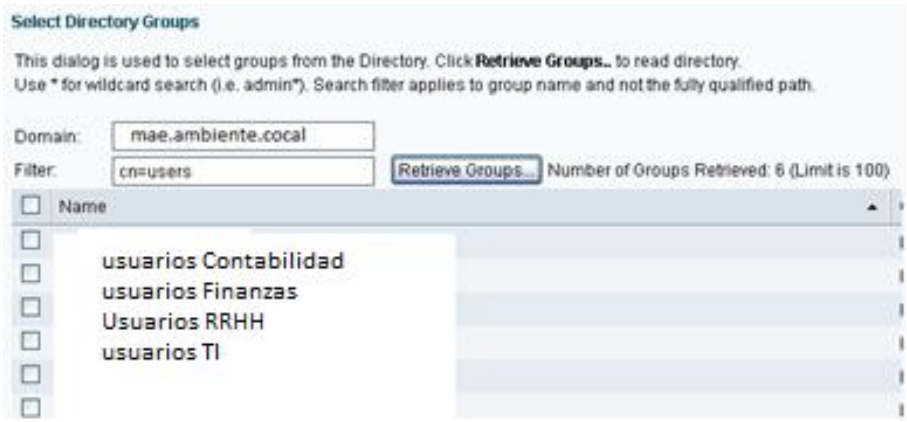

Figura No 2.6 Integración con el AD

2.3.4.4 Ingreso de los equipos cisco ISE en DNS.

Ingresar los equipos cisco ISE en sus servidores DNS.

Tabla No6 Equipos cisco ISE en DNS

HOST NAME	DIRECCION IP	Zona
SPQ-COMISEADMP1	172.17.17.40	Zona Centro
SPQ-COMISEADMP2	172.17.17.41	Zona Centro
SPQ-COMISEPSNP1	172.17.17.42	Zona Centro
SRS-COMISEPOLP1	172.17.24.135	Zona oriente
SRE-COMISEPOLP1	172.17.20.135	Zona occidente
SSG-COMISEPOLP1	172.20.97.6	Zona Sur

2.3.5 Requerimientos de diseño

El diseño se lo realiza en base a los requerimientos y lineamentos de la empresa con el fin de establecer en detalle las características y configuraciones que debe tener la nueva infraestructura de seguridades de acceso a red Wired y Wireless.

A continuación se detallan los requerimientos del diseño a ser implementado.

- Acceso de usuarios por Wired utilizando capa de autenticación EAP-MSChap2 para maquinas con autenticación 802.1x.
- Autenticación de usuarios externos con MAB, utilizando cuentas internas de usuarios Invitados y contratistas.
- Se dispone de un total de 2450 usuarios alámbricos e inalámbricos.

- Acceso de **n** impresoras por MAB
- Acceso de **n** Video Conferencia por MAB
- Acceso de **n** APS con MAB
- Capa de autenticación WLAN con WLC
- Acceso de usuarios Wireless utilizando capa de autenticación EAP-MSChap2 para maquinas con autenticación 802.1x,
- Acceso de usuarios invitados por Wireless utilizando MAB y portal cautivo.
- Acceso BYOD para dispositivos móviles

2.3.5.1 Capa de autorización con asignación de Vlans.

- Empleados: todos los servicios any to any tanto en red Wired y Wireless.
- Usuarios externos contratistas con acceso any to any.
- Usuarios externos Wired invitados con acceso de Internet.
- Usuarios externos Wireless invitados con acceso de Internet.
- Usuarios BYOD Wireless con acceso de Internet.

2.3.5.2 Procedimiento para invitados.

El acceso a la red Wireless Invitados se utilizara CWA portal cautivo y con acceso único a internet, los usuarios serán creados internamente en el portal sponsor de cisco ISE.

2.3.5.3 Profiling

Para todos los dispositivos soportados con cisco ISE (PCs, Impresoras, Videoconferencia, Aps, etc) se aplicara Profiling.

2.4 Detalle de Configuraciones

A continuación se detallan los parámetros de configuración para usuarios de con acceso a red Wired.

2.4.1 Acceso Wired

2.4.1.1 Acceso Wired Empleados

Se dispone de un total de **2650** usuarios de red Wired que se encuentran distribuidos en las cuatro Zonas (Norte, Sur, Occidente, Oriente).

La asignación de Vlan a la red LAN se dará de acuerdo al grupo que pertenecen los usuarios de cada departamento.

2.4.1.2 Validación de usuarios Wired para Autenticación y Autorización.

En la red Wired exclusivamente se validara usuarios por IEEE 802.1x.

Para el acceso a la red Wired se utilizara autenticación basada en 802.1x protocolo EAP-MSChap2.

En primera instancia se validará el hostname del equipo PC, el equipo se validara en el AD con lo cual validamos que el equipo pertenece la empresa, caso contrario el equipo que no se encuentre en el AD este no será autenticado en esta primera fase, por lo tanto el equipo quedara fuera de la red LAN.

En segunda instancia se validara los usuarios para autenticación y autorización se realizara por grupos en el AD, es decir los usuarios estarán separados en grupos de usuarios en el AD de acuerdo al departamento que pertenecen.

La autenticación y autorización de los usuarios se lo realizara por los grupos del AD, cisco ISE validara el usuario que pertenece al grupo de usuarios del AD, y ese usuario será asignado a la Vlan de usuarios que pertenece.

La creación de grupos de usuarios y la organización de los usuarios a los grupos que pertenecen debe estar realizada en el Active Directory.

Los usuarios serán autorizados de acuerdo al grupo de AD que pertenecen y asignados a la Vlan correspondiente.

Será necesario la estandarización de Vlan Name en todos y cada uno de los switches de acceso en los cuales se integraran con cisco ISE.

2.4.1.3 Grupos de Vlans a utilizar para usuarios.

Se dispone de la siguiente tabla de Vlans, la misma que es definida por la empresa y depende de las necesidades de diseño de la misma, esta tabla será estándar para cada una de las localidades a ser implementadas en cisco ISE.

Tabla No7 Vlan ID, grupo del AD

GRUPO AD	Descripción	VLAN	VLAN ID
ggiseImpresora	Impresoras	EPP_impresoras	501
ggiseNetwkg	Equipos de Networking	EPP_networking	502

ggiseVideoConf	Equipos de Video Conferencia	EPP_videoconferencia	503
ggiseVideoSeg	Equipos de Video Seguridad	EPP_videoseguridad	504
ggiseWebBasico	Funcionarios Básicos	EPP_webbasico1	530
ggiseWebDescargas	Áreas que requieren descargas de software.	EPP_webdescargas	535
ggiseWebMultimedia	Áreas que requieren streaming.	EPP_webmultimedia	536
ggiseWebSocial	Áreas que requieren redes sociales.	EPP_websocial	537
ggiseWebVip1	Gerencia, personal Vip	EPP_webvip1	538
ggeppcuarentena	Proceso de autenticación, para equipos que no validen su identidad	EPP_cuarentena	541
ggeppwfuncionarios		EPP_wfuncionarios	542
ggeppwvip		EPP_wvip	543
ggeppwbyod		EPP_wbyod	544
ggeppwinvitados		EPP_winvitados	545
ggeppwcontratistas		EPP_wcontratistas	546
ggiseTelefonia	Equipos de Telefonía	EPP_telefonia	547
ggeppwtelefonia		EPP_wtelefonia	548

2.4.1.4 Acceso Wired a usuarios externos (Contratistas e Invitados).

Existen usuarios externos que no pertenecen a la empresa y que necesitan ingresar a la red LAN, por tal motivo se creará dos grupos de usuarios para el acceso a red LAN.

Estos usuarios externos serán autenticados por Mac Addres Bypass (MAB), además de autenticados en un portal sponsor, con credenciales internas de cisco ISE.

Los usuarios Contratistas serán autenticados con credenciales internas de cisco ISE con privilegios de red **any to any**, además serán asignados a una Vlan específica de contratistas.

Los usuarios Invitados serán autenticados con credenciales internas de cisco ISE con ciertos privilegios de red, además serán asignados a una vlan específica de Invitados.

Tabla No8 Vlan ID, Vlan Name usuarios Contratistas, Invitados

Departamento	Dispositivo	Vlan Id	Vlan Name
Winvitados	Desktop PC	Vlan 545	EPP_winvitados
Wcontratistas	Desktop PC	Vlan 546	EPP_wcontratistas

2.4.1.5 Acceso Wired para dispositivos Estáticos Impresoras.

Se dispone impresoras de varias marcas como HP, Xerox, Canon, Lexmark etc, las cuales están conectadas por red Wired ubicadas en cada uno de los departamentos.

Estos dispositivos estarán autenticados por MAC Address Bypass (MAB) asignados a la vlan **501** cada impresora está siendo asignadas a la vlan **501** en cualquier departamento en que se encuentre.

Tabla No9 Vlan ID, Vlan Name para impresoras

Dispositivo	Vlan ID	Vlan Name
Impresoras	Vlan 501	EPP_impresoras

2.4.1.6 Acceso Wired para dispositivos Estáticos Videoconferencias.

Estos dispositivos estarán autenticados por MAC Address Bypass (MAB) asignados a la vlan **503** cada VideoConferencia está siendo asignadas a la vlan **503** en cualquier departamento en que se encuentre.

Tabla No10 Vlan ID, Vlan Name para Videoconferencia

Dispositivo	Vlan ID	Vlan Name
VideoConferencias	Vlan 503	EPP_videoconferencia

2.4.1.7 Acceso Wired para dispositivos Estáticos Telefonía.

Se dispone de telefonía cisco las cual están conectado por red Wired ubicadas en cada departamento de la empresa.

Estos dispositivos estarán autenticados por MAC Address Bypass (MAB) asignados a la vlan **547** cada teléfono estará siendo asignado a la vlan **547** del departamento en que se encuentran.

Tabla No11 Vlan ID, Vlan Name para telefonía

Dispositivos	**Vlan ID**	**Vlan name**
Teléfonos	Vlan 547	Telefonía

2.4.1.8 Acceso Vlan de cuarentena.

Todos los dispositivos PCs que se conecten a la red Wired serán asignados momentáneamente a la Vlan de cuarentena Vlan los equipos permanecerán en esta Vlan momentáneamente hasta que sean autenticados y autorizados a la Vlan de departamento o servicio.

Esta Vlan tiene que ser lo bastante grande para asignar direccionamiento IP a todos los usuarios de cada locación.

Tabla No12 Vlan ID, Vlan Name para cuarentena

Dispositivos	Vlan Cuarentena	Vlan Name
Pcs	Vlan 541	Cuarentena

2.4.2 Acceso Wireless.

Se dispondrá de seis SSID wireless con sus respectivos niveles de acceso y grupos de autenticación predefinidos.

Tabla No13 Vlan ID, SSID, authenticacion para wireless

SSID	Vlan	Autenticación	Postura	Validación
Funcionarios	Vlan 542	802.1x	no	AD
Funcionarios_VIP	Vlan 543	802.1x	no	AD
BYOD	Vlan 544	802.1x	no	AD
Telefonos_WIFI	Vlan 547	MAB	no	MAB
Contratistas	Vlan 546	MAB / portal Cautivo	no	Interna cisco ISE
Invitados	Vlan 545	MAB / portal Cautivo	no	Interna cisco ISE

2.4.2.1 Acceso Wireless IEEE 802.1x

En primera instancia se validará el hostname del equipo PC, el equipo se validara en el AD con lo cual validamos que el equipo pertenece al domino de la empresa, caso contrario el equipo que no se encuentre en el AD este no podrá ser autenticado en esta primera fase, por lo tanto el equipo quedara fuera de la red LAN.

Se dispondrá de dos SSID para personal de la empresa (Funcionarios, Funcionarios_VIP)

2.4.2.2 Validación de usuarios Wireless Funcionarios para Autenticación y Autorización.

En la red Wireless Funcionarios exclusivamente se validara usuarios de la empresa por IEEE 802.1x.

- Para el acceso a la red Wireless se utilizara autenticación basada en 802.1x protocolo EAP-MSChap2.

- Validación de usuarios por grupos de AD, la empresa deberá agrupar los usuarios de acuerdo a los permisos de utilizar la red Wireless.

- El acceso al SSID Funcionarios estarán permitidos únicamente los dispositivos PCs de la empresa así como también usuarios con credenciales del AD.

- El acceso a la red será any to any.

- Otros dispositivos que no pertenecen a la empresa no se permitirá el acceso.

- Sera necesario crear un grupo de usuarios en AD para para la validación de usuarios (Funcionarios) los cuales tendrán acceso exclusivo al SSID de Funcionarios, esta tarea se realizara asignando los usuarios al perfil de acceso wireless.

Tabla No14 Vlan ID, SSID, validación para funcionarios

SSID	Vlan	acceso	Postura	Validación
Funcionarios	Vlan 542	802.1x	no	AD

2.4.2.3 Validación de usuarios Wireless Funcionarios-VIP para Autenticación y Autorización.

En la red Wireless Funcionarios_VIP exclusivamente se validara usuarios por 802.1x, los usuarios que no pertenecen al grupo que tienen permiso a la red de Funcionarios-VIP no se permitirá el acceso a dicha red.

- Para el acceso a la red Wireless se utilizara autenticación basada en 802.1x protocolo EAP-MSChap2.
- Validación de usuarios por grupos de AD, la empresa deberá agrupar los usuarios de acuerdo a los permisos de utilizar la red Wireless.
- El acceso al SSID Funcionarios-VIP estarán permitidos únicamente los dispositivos PCs así como también usuarios con credenciales del AD.
- El acceso a la red será any to any.
- Otros dispositivos que no pertenecen a la empresa no se permitirá el acceso.
- Sera necesario crear un grupo de usuarios en AD para para la validación de usuarios (Funcionarios_VIP) los cuales tendrán acceso exclusivo al SSID de Funcionarios_VIP.

Tabla No15 Vlan ID, SSID, validación para VIP

SSID	Vlan	acceso	Postura	Validación
Funcionarios-VIP	Vlan 543	802.1x	no	AD

2.4.2.4 Validación de usuarios Wireless teléfonos_wifi para Autenticación y Autorización.

En la red Wireless telefonos_wifi exclusivamente se validara teléfonos cisco por MAB.

- El acceso al SSID telefonos_wifi estarán permitidos únicamente los dispositivos telefónicos cisco wifi.

La autenticación a ser utilizado se utilizara el modo de seguridad EAP-FAST con user y password interno de cisco ISE.

Tabla No16 Vlan ID, SSID, validación para teléfonos

SSID	Vlan	Vlan ID	acceso	Postura	Validación
Telefonos_wifi	Vlan 547	Telefonos_wifi	MAB	no	MAB

2.4.2.5 Validación de usuarios Wireless BYOD para Autenticación y Autorización.

En la red Wireless BYOD exclusivamente se validara usuarios de la empresa por 802.1x, los usuarios que no pertenecen al grupo que tienen permiso a la red de BYOD no se permitirá el acceso a dicha red.

- Para el acceso a la red Wireless se utilizara autenticación basada en 802.1x protocolo EAP-MSChap2.

- Validación de usuarios por grupos de AD, la empresa deberá agrupar los usuarios de acuerdo a los permisos de utilizar la red Wireless.

- El acceso al SSID BYOD estarán permitidos únicamente los dispositivos Móviles del personal de la empresa con credenciales del AD del grupo de Dispositivos BYOD.

- El acceso a red LAN será únicamente con permisos de Internet.

- Sera necesario crear un grupo de usuarios en AD para la validación de usuarios (BYOD) los cuales tendrán acceso exclusivo al SSID de BYOD.

- El acceso al SSID BYOD será exclusivamente para dispositivos Móviles.

Tabla No17 Vlan ID, SSID, validación para BYOD

SSID	Vlan	acceso	Postura	Validación
BYOD	Vlan 544	802.1x	no	AD

2.4.2.6 Acceso Wireless Invitados, Contratistas.

El acceso a la red Wireless Invitados será únicamente a dispositivos PCs externos que no perteneces a la empresa y por ende no están agregados al dominio, estos equipos serán autenticados por MAB con portal cautivo.

Se crearan dos grupos de usuarios internos de cisco ISE, los cuales serán validados para el acceso de usuarios Invitados y usuarios Contratistas.

2.4.2.7 Validación de usuarios Wireless Invitados para Autenticación y Autorización.

En la red Wireless Invitados exclusivamente se validara usuarios que no son de la empresa y serán autenticados por MAC Address Bypass (MAB) con portal cautivo.

- Para el acceso a la red Wireless se utilizara autenticación basada en MAB utilizando credenciales internas del portal Sponsor de cisco ISE.

- El acceso al SSID Invitados estarán permitidos únicamente los dispositivos PCs externos que no pertenecen a la empresa.

- El acceso a la red LAN será únicamente con permisos de Internet.

- El acceso a la SSID Invitados será exclusivamente para dispositivos PCs externos.

Tabla No18 Vlan ID, SSID, validación para invitados

SSID	Vlan	Acceso	Postura	Validación
Invitados	Vlan 545	MAB	no	Sponsor

2.4.2.8 Validación de usuarios Wireless Contratistas para Autenticación y Autorización.

En la red Wireless Contratistas exclusivamente se validara usuarios que no son de la empresa y serán autenticados por MAC Address Bypass (MAB) con portal cautivo.

- Para el acceso a la red Wireless se utilizara autenticación basada en MAB utilizando credenciales internas del portal Sponsor de cisco ISE.

- Validación de usuarios se realizara con usuarios internos de cisco ISE del portal Sponsor.

- El acceso al SSID Contratistas estarán permitidos únicamente los dispositivos PCs externos que no pertenecen al domino de la empresa.

- El acceso a la red LAN será con acceso total a la red.

- El acceso a la SSID Contratistas será exclusivamente para dispositivos PCs externos.

Tabla No19 Vlan ID, SSID, validación para contratistas

SSID	Vlan	Acceso	Postura	Validación
Corporativos	Vlan 546	MAB	no	Sponsor

2.4.2.9 Configuración cisco WLC para integración con cisco ISE.

En configuraciones básicas para la integración del WLC con cisco ISE se tiene la configuración del cisco ISE como servidor AAA. Para los dos equipos cisco ISE.

Cada locación se configura dos servidores radius, principal y secundario.

172.17.17.42 preshared key COM.rad.ise2014

172.20.97.6 preshared key COM.rad.ise2014

Figura No 2.7 configuración RADIUS

Para cada SSID con autenticación en 802.1x con cisco ISE se tiene la siguiente configuración de seguridad en capa2.

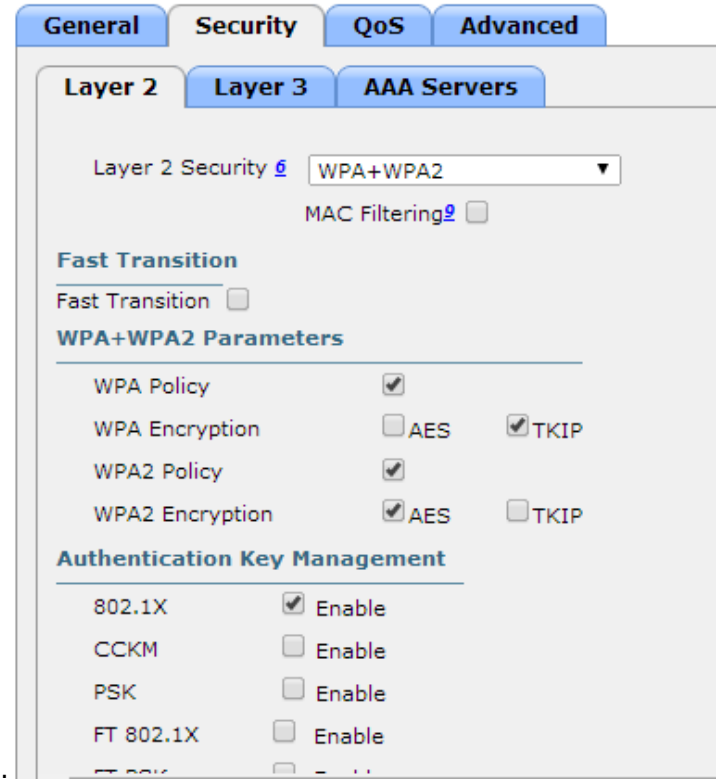

Figura No 2.8 configuración seguridad wlc

La siguiente configuración en la parte avanzada del SSID con 802.1x

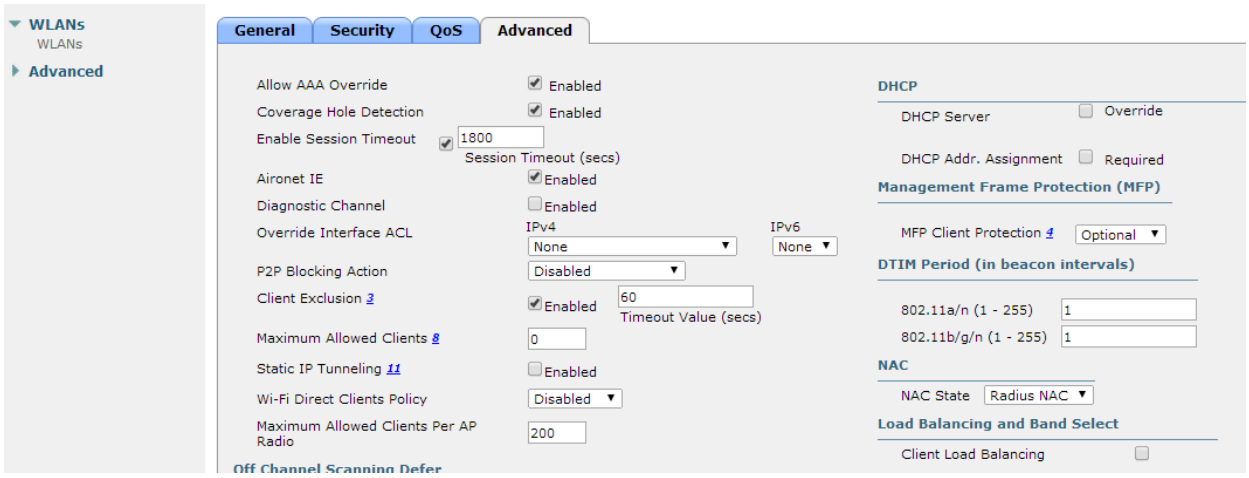

Figura No 2.9 configuración 802.1x

Luego de estas configuraciones básicas tenemos varias configuraciones extras en la configuración de cisco WLC con cisco ISE.

2.4.3 Configuración AnyConnect en PC.

Para realizar una conexión segura de equipos de computación a la red de la empresa cuando se está utilizando la herramienta de cisco ISE, la cual nos permite realizar autenticación en equipos corporativos los cuales tienen que cumplir los siguientes pre-requisitos para ser autenticados en la RED LAN.

2.4.3.1 Requisitos de autenticación de equipos PC Windows.

Los equipos de la empresa tienen que cumplir los siguientes requisitos antes de ser autenticados para el ingreso a la red LAN.

- Activado en la configuración de red la asignación dinámica de direccionamiento IP DHCP.
- Verificación de servicio de autenticación IEEE 802.1x en los equipos clientes.
- Verificación de tarjeta de red con autenticación.
- Instalación del agente de cisco AnyConnect.
- Usuario a ser autenticado debe pertenecer al grupo correspondiente del AD.

2.4.3.2 Habilitar autenticación IEEE 802.1x en equipos clientes.

Se habilita el servicio de autenticación IEEE 802.1x en los equipos clientes, este servicio será el encargado de habilitar la autenticación en la tarjeta de red Wired.

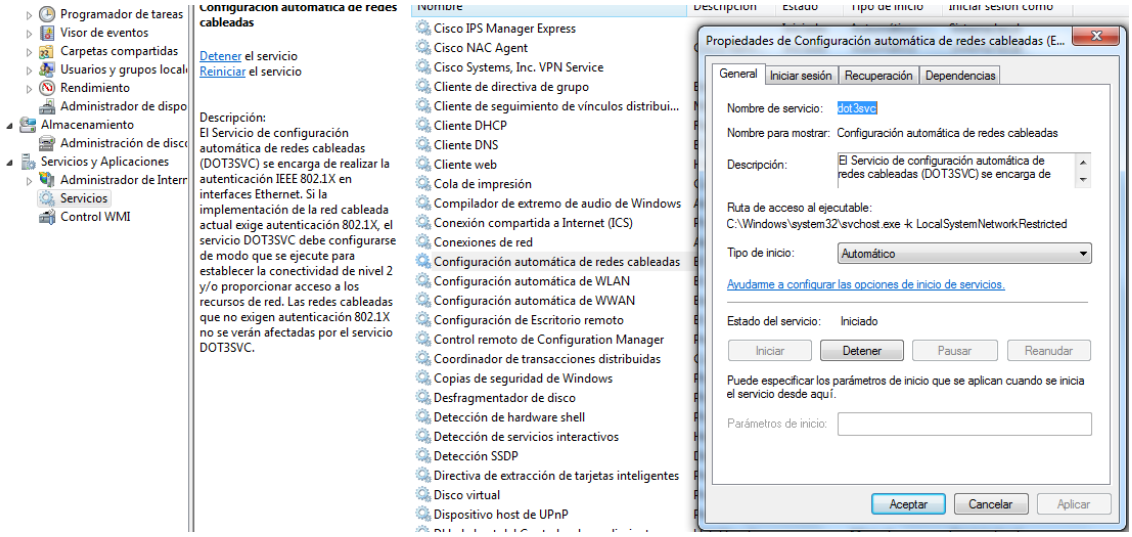

Figura No 2.10 configuración 802.1x PC

2.4.3.3 Configuración de tarjeta de red con autenticación.

Se configura la tarjeta de red Wired con los siguientes parámetros de autenticación.

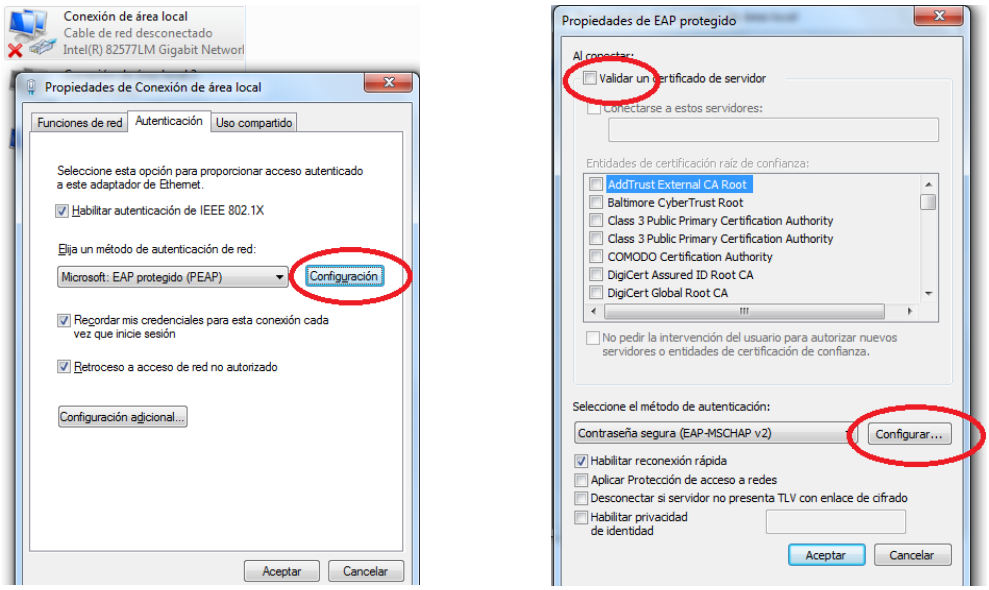

Figura No 2.11 configuración tarjeta de red PC

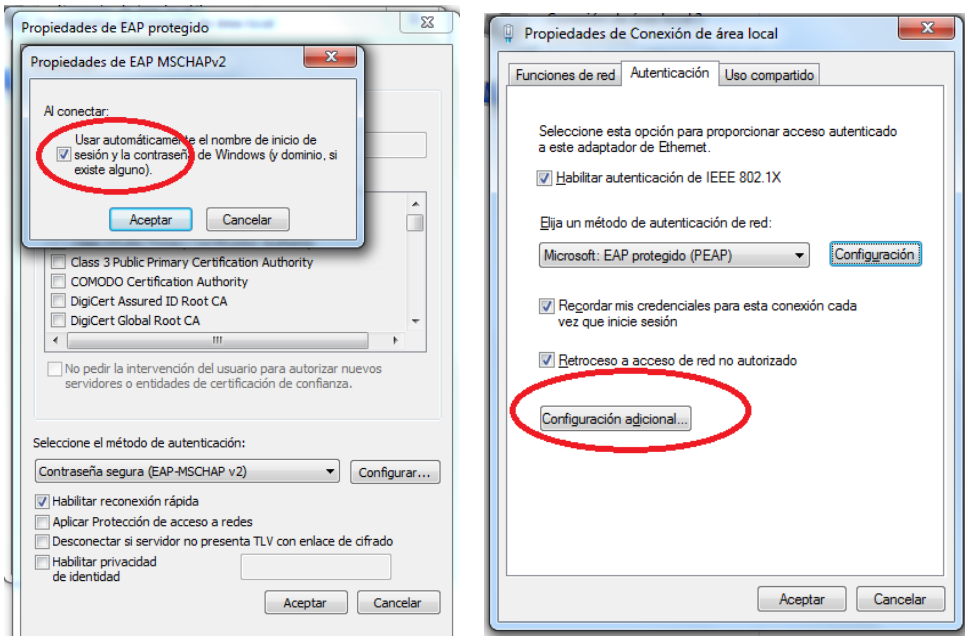

Figura No 2.12 configuración tarjeta de red PC

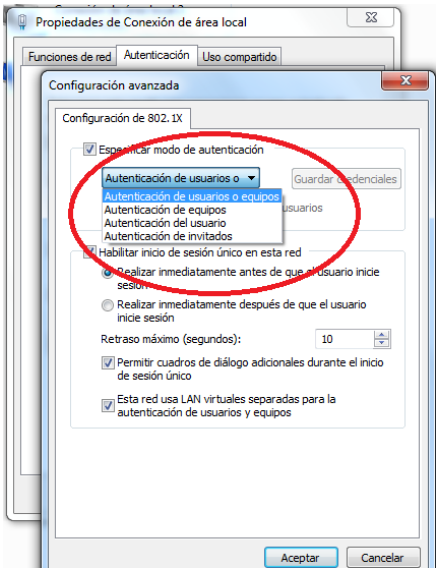

Figura No 2.13 configuración tarjeta de red PC

Esto está habilitado por política del Dominio. En caso de problema se debe verificar.

2.4.3.4 Instalación cisco AnyConnect.

Se realiza la instalación del agente de cisco (**cisco AnyConnect 3.1)** el cual será instalado de forma manual en todos y cada uno de los equipos clientes de la empresa.

Instalación de del paquete pre-deploy.

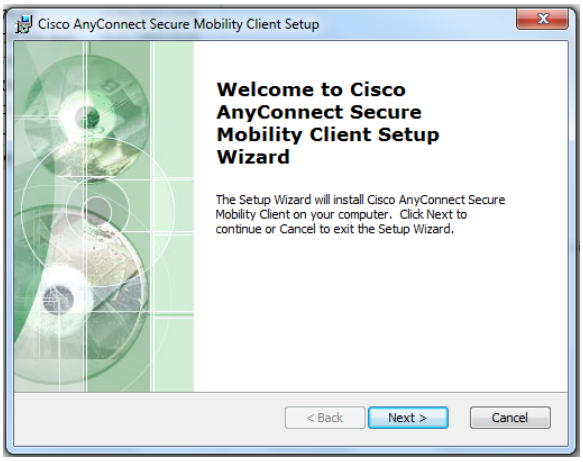

Figura No 2.14 Instalación Software AnyConnect

2.4.3.5 Acceso a red Wired y Wireless.

Para el acceso a la red Wired y Wireless serán administrados por cisco anyconnect el cual manejara todos los perfiles de conexión.

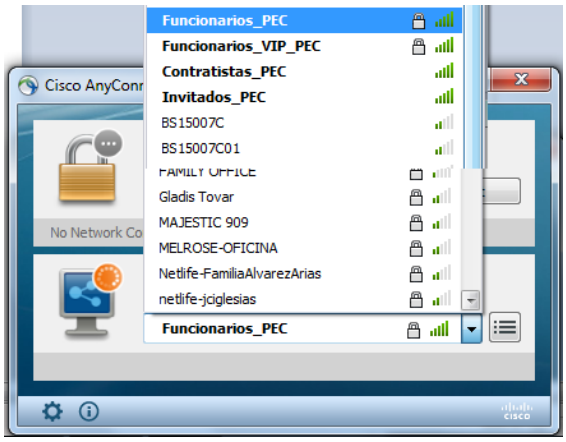

Figura No 2.15 visualización de software AnyConnect Wireless

Al momento de la conexión a la red Wired cisco anyconnect enviara las credenciales de autenticación es decir username y hostname del equipo, con estos parámetros será autenticado el equipo y el usuario a la Vlan que correspondiente.

Hay que tener en cuenta que el usuario debe pertenecer al grupo de AD que corresponde de acuerdo al grupo del departamento que pertenece para que sea asignado a la vlan correspondiente.

Al realizar una sesión de autenticación satisfactoria en la ventana de cisco anyconnect indicara la red a la cual está siendo autenticado, en nuestro caso será **WIRED** con su respectiva dirección IP y el estado de **connected.**

Figura No 2.16 visualización de software AnyConnect Wired

Al momento de la conexión a la red Wireless cisco anyconnect enviara las credenciales de autenticación es decir username y hostname del equipo,

con estos parámetros será autenticado el equipo y el usuario a la Vlan de Wireless que corresponde.

Hay que tener en cuenta que el usuario debe pertenecer al grupo de AD que corresponde es decir al grupo de Funcionarios o Funcionarios_VIP.

Al realizar una sesión de autenticación satisfactoria en la ventana de cisco anyconnect indicara la red a la cual está siendo autenticado, en nuestro caso será **Funcionarios_VIP** con su respectiva dirección IP y el estado de **connected.**

En caso de que el usuario no se encuentre en el grupo de acceso a red Wireless o Wired tendremos un error de autenticación como el siguiente.

A pesar que se ingrese el usuario y contraseña correcta se tiene el mensaje de autenticación fallida por varias ocasiones.

En caso de presentarse dicho inconveniente es necesario validar que el usuario se encuentre el grupo de AD correspondiente.

Figura No 2.17 visualización de error de conexión AnyConnect

Según el tipo de conexión a la plataforma ISE será: mediante la red cableada y la red inalámbrica.

CAPÍTULO 3

RESULTADOS DE LA IMPLEMENTACIÓN DEL CISCO ISE

Como resultado de la implementación de Services Engine Cisco (ISE), y la aplicación de políticas basadas en la identidad, se obtiene mayor control en el acceso a la red wired y Wireless.

3.1 Mejoras control de acceso a la red Wired

Previo al cambio radical de acceso a la red, se realizó una campaña de concientización exponiendo el proceso que debía realizar cada funcionario de la empresa para validar sus credenciales en cada uno de sus dispositivos finales.

Para evitar contratiempos con el personal VIP de la empresa (Gerentes, Subgerentes y Asesores) se verifica que cada usuario esté identificado y validado en el AD en los perfiles de: VIP wired, VIP Wireless, BYOD.

Se valida que el equipo PC se encuentre en el Active Directory, con lo cual garantizamos que solo equipos que pertenecen al dominio de la empresa sean autenticados en esta primera instancia.

En la segunda instancia validaremos el UserName del usuario en el Active Directory, con este parámetro de autenticación daremos el acceso definitivo al usuario a su respectiva Vlan, correspondiente a su área, dependencia o gerencia.

Para dispositivos que no manejen autenticación IEEE 802.1x se validara el acceso por MAC Address Bypass (MAB) esto en el caso de dispositivos estáticos (impresoras, Video Conferencia, Access Point, etc)

Los dispositivos PCs que no manejen autenticación IEEE 802.1x se validara el acceso por MAC Address Bypass (MAB), esta autenticación es para usuarios externos (Invitados y Contratistas) de la empresa, los grupos de usuarios contratistas e invitados serán autenticados por portal sponsor de cisco ISE, cada uno de estos grupos tendrá su nivel de privilegios.

Como beneficio debido al cambio de la condición de ingreso de los usuarios internos y externos a la red cableada de la empresa con la herramienta cisco ISE, por medio del protocolo IEEE 802.1x validado por las políticas de control de acceso de la herramienta, se obtiene un control de acceso a la intranet definido por usuario, reduciendo los riesgos de intrusión, incrementamos la seguridad de ingreso a la intranet, brindando mayor flexibilidad y control al personal administrativo de TI.

3.2 Mejoras control de acceso a la red Wireless

El cambio de políticas de acceso en la red Wireless fue la que más resistencia género en los usuarios, ya que la ser la red de más fácil acceso para a los diferentes dispositivos como tabletas, teléfonos inteligentes y computadoras portátiles personales, de cada funcionario o visitante.

Se han implementado nuevas redes inalámbricas para la plataforma ISE, las cuales son detalladas con su nivel de acceso a continuación:

Son tres SSID con autenticación IEEE 802.1x y tres SSID con autenticación por MAB (Mac Address Bypass).

Usuarios Funcionarios con autenticación IEE802.1x con acceso total a la red en el segmento de red asignado.

Usuarios Funcionarios_VIP con autenticación IEE802.1x con acceso total a la red en el segmento de red asignado.

Equipos BYOD la autenticación se la realizara con IEEE802.1x, con acceso restringido a la red en el segmento de red asignado, además de acceso a internet, este servicio será solo para funcionarios de la empresa.
Teléfonos WIFI autenticación por MAB con acceso total a la red en el segmento de red asignado.

Usuarios Invitados estos usuarios se realizara la autenticación por MAB ya que estos equipos son externos y no manejaran IEEE 802.1x, además serán autenticados por un portal cautivo manejando por cisco ISE, las credenciales serán creadas internamente en cisco ISE, el acceso será restringido a toda la red LAN y con acceso solo a internet.

Usuarios Contratistas estos usuarios se realizara la autenticación por MAB ya que estos equipos son externos y no manejaran IEEE 802.1x, además serán autenticados por un portal cautivo manejando por cisco ISE, las credenciales serán creadas internamente en cisco ISE, el acceso será restringidos a la red LAN.

El incremento de seguridad en el acceso a la red inalámbrica por medio de la autenticación 802.1x en cada uno de los SSID empresariales, incluyendo la creación de la red BYOD para control de acceso de los dispositivos móviles como teléfonos inteligentes, tabletas, relojes inteligentes, computadoras personales, etc.

Facilito la administración y el control de acceso de los dispositivos a cada SSID, limitando el ingreso solo a los usuarios con permisos para ingresar a cada SSID.

Limitar el acceso por usuario, es garantizar la disponibilidad del servicio de red inalámbrica, al no tener control de cuantos y que equipos ingresen a una determinada red, los rangos de direccionamiento quedaban insuficientes para la cantidad de equipos que ingresaban a una determinada red, ya que fueron diseñados para acceso de equipos móviles empresariales.

3.3 Estadísticas post-implementación

A continuación se muestran las estadísticas de la implementación del Services Engine Cisco (ISE) que tienen por finalidad optimizar el ingreso dispositivos finales de red de acuerdo a sus funciones y responsabilidades.

La figura 3.1 muestra el informe del perfil de endpoints y sirve para 2 propósitos
Compara los cambios de perfil para un punto final determinado y comparar los cambios de perfil de los mismos.

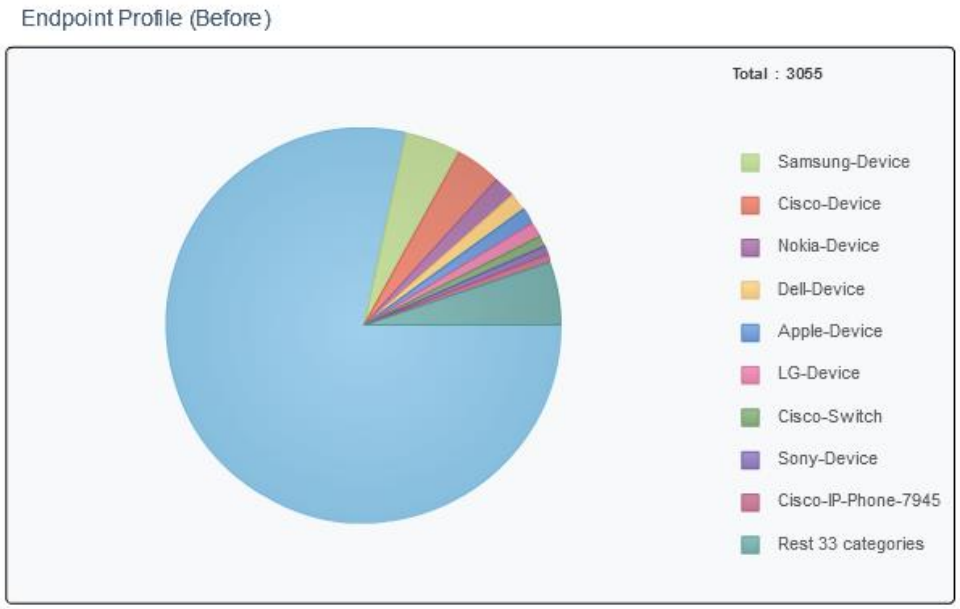

Figura 3.1. Estadísticas cambios de perfil por dispositivo en la red

La figura 3.2 se basa en las autenticaciones RADIUS. Se le permite identificar las autenticaciones más comunes y las razones de los fallos de autenticación de los dispositivos móviles o wireless.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status
2015-07-28 10:43:50.167	✓			EPPEC\rrendon >	34:17:EB:B6:28:48	Dell-Device	SW_PREV_14	GigabitEthernet1/0/47	Autho_WebBasico1_...	Dell-Device	NotApplicable
2015-07-28 08:34:37.506	✓			#ACSACL#-IP-Ad			SW_PREV_14				
2015-07-28 08:34:37.466	✓			host/GYEPRVPAC	34:17:EB:B6:28:48	Dell-Device	SW_PREV_14	GigabitEthernet1/0/47	Autho_AD_LOGIN_...	Dell-Device	NotApplicable
2015-07-28 08:31:32.454	✓			#ACSACL#-IP-Ad			SW_PREV_14				
2015-07-28 08:31:32.415	✓			host/GYEPRVPAC	34:17:EB:B6:28:48	Dell-Device	SW_PREV_14	GigabitEthernet1/0/47	Autho_AD_LOGIN_...	Dell-Device	NotApplicable
2015-07-28 08:31:08.560	✓			EPPEC\jbrown >:	34:17:EB:B5:9B:82	Dell-Device	SW_PREV_14	GigabitEthernet1/0/2	Autho_WebBasico1_...	Dell-Device	NotApplicable
2015-07-28 08:29:23.508	✓			#ACSACL#-IP-Ad			SW_PREV_14				
2015-07-28 08:29:23.472	✓			host/GYEPRVPAC	34:17:EB:B5:9B:82	Dell-Device	SW_PREV_14	GigabitEthernet1/0/2	Autho_AD_LOGIN_...	Dell-Device	NotApplicable
2015-07-28 08:17:53.221	✓			EPPEC\jvera >> I	34:17:EB:B5:FD:46	Dell-Device	SW_PREV_14	GigabitEthernet1/0/39	Autho_WebBasico1_...	Dell-Device	NotApplicable
2015-07-28 08:16:55.032	✓			#ACSACL#-IP-Ad			SW_PREV_14				
2015-07-28 08:16:54.994	✓			host/GYEPRVPAC	34:17:EB:B5:FD:46	Dell-Device	SW_PREV_14	GigabitEthernet1/0/39	Autho_AD_LOGIN_...	Dell-Device	NotApplicable
2015-07-28 08:04:21.623	✓			EPPEC\frecalde >	B8:CA:3A:BD:83:C2	Dell-Device	SW_PREV_14	GigabitEthernet1/0/43	Autho_WebBasico1_...	Dell-Device	NotApplicable
2015-07-28 07:57:24.225	✓			EPPEC\prazo >>	34:17:EB:B5:91:F8	Dell-Device	SW_PREV_14	GigabitEthernet1/0/45	Autho_WebBasico1_...	Dell-Device	NotApplicable

Figura 3.2. Lista de autenticaciones por Usuarios

La figura 3.3 y la figura 3.4 muestra la cantidad total de autenticaciones en la red por dispositivo.

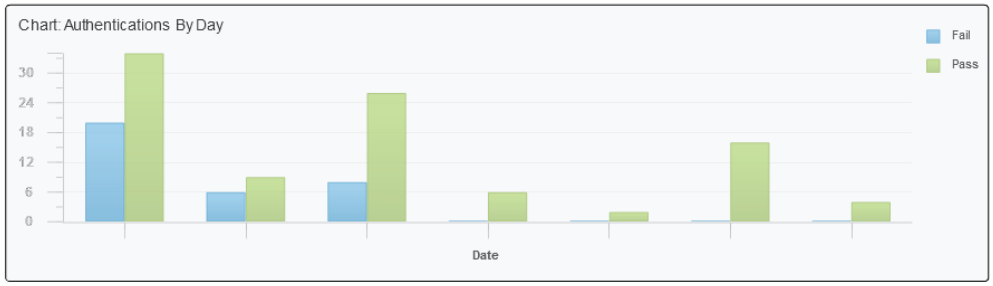

Figura 3.3. Autenticaciones totales de los Usuarios

Authentications By Day and Quick Links

Day	Passed	Failed	Total	Failed %	Avg Response Time (ms)	Peak Response Time (ms)
2015-07-28 00:00:0	4	0	4	0	14.25	18
2015-07-27 00:00:0	16	0	16	0	17.00	20
2015-07-26 00:00:0	2	0	2	0	19.00	19
2015-07-25 00:00:0	6	0	6	0	30.83	69
2015-07-24 00:00:0	26	8	34	8	20.06	58
2015-07-23 00:00:0	9	6	15	6	18.93	31
2015-07-22 00:00:0	34	20	54	20	20.43	29

Figura 3.4. Autenticaciones totales de los Usuarios

CONCLUSIONES

1. La implementación de CISCO IDENTIFY SERVICES ENGINE (ISE), nos permitió realizar una automatización en la gestión y seguridad, ejecutando un control centralizado de políticas, visibilidad, resolución de aplicar políticas para el control de acceso, basados en identificación del usuario y dispositivos, permitiendo monitorear el lugar y hora de ingreso a la red institucional, facilitando el control de todos los dispositivos que ingresan a la red, manteniendo un seguimiento de dispositivos.

2. La herramienta Cisco ISE permite al administrador de red, controlar de forma centralizada las políticas de acceso en base a implementación de políticas basadas en roles, optimizando la asignación de accesos de los recursos empresariales tales como: aplicaciones, perfiles de navegación, telefonía, Acceso a redes inalámbricas, etc., establecidas en el perfil de cada usuario, el que es creado o modificado en el active directory de la empresa.

3. Con la creciente evolución del acceso a la intranet a través de la movilidad, las empresas de hoy están evolucionando rápidamente, especialmente cuando se trata de la movilidad de los empleados. Los empleados ya no están atados a las estaciones de trabajo de escritorio, sino que acceden a recursos de la empresa a través de una variedad de dispositivos: tabletas, teléfonos inteligentes y computadoras portátiles personales, la herramienta facilita y controla el acceso de estos equipos a solo los usuarios que tengan permitido ingresar sus gatnets a la red empresarial, garantizando la disponibilidad del servicio a través del a red BYOD configurada en la WIC de la empresa.

RECOMENDACIONES

1. Previa implementación de la herramienta cisco identify services engine (ISE), se recomienda realizar una campaña de concientización a los funcionarios de la empresa vía correo electrónico o por charlas impartidas por el personal de TI, ya que se realizara un gran cambio en la manera como el usuario ingresa a la intranet de la empresa, y es necesario la colaboración de los funcionarios en facilitar al personal técnico el acceso a sus dispositivos empresariales para las configuraciones e instalación del software Cisco anyconnect.

2. Se recomienda tomar precauciones en la definición de tiempos de implementación de la herramienta, ya que previa puesta en marcha de la solución, es necesario tener una matriz corporativa única de Networking, poseer una red jerárquica claramente definida, la red pasiva de cableado estructurado bien identificada, un sistema estandarizado de dominio donde todos los equipos empresariales y usuarios estén migrados.

3. Como experiencia post implementación recomiendo no descuidar la migración de las impresoras ya que la implementación de Cisco ISE, recomienda que se migren a una Vlan independiente, y como la gran mayoría de las compañías las impresoras están en la misma Vlan de los usuarios, lo que implica un cambio en el direccionamiento de cada impresora. Como administrador de la red le puse mucho énfasis y cuidado a la migración de los usuarios y el cambio de perfil basado en el rol del usuario, cerciorándome en dejar habilitado servicios empresariales, pero al realizar el profiling a las impresoras y cambiar las ips y la vlan, el servicio de impresión de cada área se vio afectado, creando un caos. El problema radicaba en que las PC`s y laptops están asociadas a un servidor de impresión, en donde se asocia cada Impresora por su IP y al cambiar la misma se desconecta del server provocando que se pierda la conexión.

4. Con la implementación de Cisco ISE, el active directory toma un papel fundamental en la red corporativa ya que el AD es el encargado de validar al usuario. Es fundamental que el servidor que contiene al active directory este en constante monitoreo de su CPU, memoria y disponibilidad ya que si por algún motivo el appliance ISE pierde conexión con el AD, por errores de autenticación envía a todos los usuarios empresariales a la Vlan de cuarentena, por ende pierden los servicios y aplicaciones empresariales, afectando la disponibilidad y operación de la empresa.

5. Es recomendable documentar toda la implementación de la herramienta Cisco ISE con la experiencias, errores de operación, políticas de acceso, a fin de tener que evitar errores y contratiempos en futuras implementaciones como nuevos edificios administrativos, nuevos terminales de la empresa.

BIBLIOGRAFÍA

1. Ariganello, Barrientos «Redes Cisco CCNP a Fondo » 2012.

2. CISCO. Informe anual de seguridad CISCO 2015. Obtenido de:www.cisco.com/web/ES/assets/pdf/asr_final_os_ah_es.pdf

3. CISCO. Informe anual de seguridad CISCO 2014. Obtenido de:*www.cisco.com/assets/global/ES/.../sc01casr2014_cte_lig_es_35330.pdf*

4. CISCO. Manuales de implementaciòn Cisco Service Engine (ISE) de:http://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-design.html
5. Cisco. (s.f.). CCNA Security. San Francisco, California, Estados Unidos.

6. Cisco Systems. (2014). Data sheet . San Fransico, California, Estados Unidos .

7. Gartner. (2015). *blogscisco*. Obtenido de http://blogs.cisco.com/enterprise/cisco-positioned-as-a-leader-in-the-gartner-magic-quadrant-for-wired-and-wireless-lan-access-infrastructure-for-the-3rd-time-in-a-row