ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

TRABAJO DE TITULACIÓN

"Diseño e implementación de una infraestructura inalámbrica basada en Alepo Meraki y Portal Cautivo para el control de acceso de empleados, proveedores y clientes en una entidad financiera."

PREVIO A LA OBTENCIÓN DEL TITULO DE:

Magister en Sistemas de Información Gerencial

PRESENTADO POR:

Ing. José Efraín Zamora Salazar

GUAYAQUIL - ECUADOR
2020

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y me fortalece.

Mi profundo agradecimiento a todas las autoridades y personal que hacen la Escuela Superior Politécnica del Litoral, por confiar en mí, abrirme las puertas y permitirme realizar todo el proceso investigativo y formativo dentro de su establecimiento educativo.

Finalmente quiero expresar mi más grande y sincero agradecimiento al Ing. Albert Espinal y Ing. Robert Andrade, principales colaboradores durante todo este proceso, quien con su dirección, conocimiento y enseñanza permitió el desarrollo de este trabajo.

.

DEDICATORIA

El presente trabajo investigativo lo dedico principalmente a Dios, por ser el inspirador para darme fuerza a continuar en este proceso de obtener uno de los anhelos más deseados.

A mis padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes he logrado llegar hasta aquí y convertirme en lo que soy. A mi hermano por estar siempre presente, acompañándome con apoyo moral.

A todas las personas que me han apoyado y han hecho que el trabajo se realice con éxito en especial aquellos que estuvieron dispuestos en brindarnos sus conocimientos y me abrieron las puertas de la institución financiera

TRIBUNAL DE SUSTENTACIÓN

……..

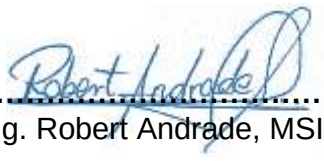
Ing. Lenin Freire C., MSIG**.**

COORDINADOR MSIG

……..

Ing. Albert Espinal S., MSIG.

DIRECTOR DEL PROYECTO DE GRADUACIÓN



……..

Ing. Robert Andrade, MSIG.

MIEMBRO DEL TRIBUNAL

RESUMEN

En la infraestructura inalámbrica podemos encontrarnos con diversos problemas, así como también con diversas soluciones, es contar con equipos de la más alta calidad y fácil de gestionar el acceso a la red, por el cual se requiere de robustecer la infraestructura inalámbrica.

A partir de las observaciones tomadas en el área de Medios Tecnológicos, se han analizado varias soluciones y alternativas para la implementación de una nueva infraestructura inalámbrica, como para poder contar con un servicio inalámbrico estable y confiable.

En el primer capítulo se indican la solución de la propuesta como el objetivo general y específico, metodología los cuales se quiere lograr mediante la nueva implementación de la infraestructura inalámbrica

En el segundo capítulo se establece el marco teórico, análisis de la situación actual, infraestructura inalámbrica centralizada, movilidad empresarial y la administración / gestión de la infraestructura, fundamentados teórica y legal en la que actualmente se establecen las bases necesarias para la implementación.

En el tercer capítulo se trata del levantamiento de la información, definiciones, equipamiento y configuración, plan de acción ADFS, inventario del direccionamiento IP y la topología a implementar

En el cuarto capítulo se desarrolla el análisis y diseño de la solución hardware (equipos a utilizar) y software (implementación del sistema).

En el quinto capítulo se desarrolla el análisis y diseño de la solución Alepo - Meraki definidas para los clientes.

En el sexto capítulo se desarrolla la implementación DNA Center, plataformas, herramientas de uso, lo beneficios, la conclusión y recomendación necesaria.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍAS

802.11ac	Versión más reciente del estándar Wifi.
AAA	Protocolos autenticación, autorización y contabilización.
ACS	Sistema de control de acceso.
Active Directory	Directorio Activo de una red distribuida de computadores.
ADFS	Active Directory Federation Services.
AES	Algoritmo del Estándar de cifrado avanzado.
ALEPO	Proveedor de soluciones tecnológicas.
AP	Access Point.
API	Interfaz de programación de aplicaciones.
BACCKUP	Respaldo, contingencia.
BYOD	Tendencia que permite realizar tareas del trabajo.
CDP	Protocolo de red propietario de nivel 2.
CISCO	Networking Academy Builds IT.
CISCO AIRONET	Access Point.
CISCO DNA	Digital Network Architecture.
CISCO FMC	Firepower Management Center.
DHCP	Dynamic Host Configuration Protocol.
DNS	Domain Name System.
FIREWALL	Cortafuegos.
GATEWAY	Puerta de enlace.
ISE	Identity Services Engine.
IP	Internet Protocol.
LAN	Red de área local de computadoras.
LDAP	Protocolo ligero de acceso a directorios.
LLDP	Protocolo de descubrimiento de capa de enlace.
MAC	Dirección Física de un medio de comunicación.
MERAKI	Líder en soluciones TI administrada en la nube.
NETFLOW	Protocolo de red.

ORION	Software de monitoreo de red.
PRTG	Software de monitoreo de red.
PXGRID	Marco de trabajo para compartir información de seguridad.
RUCKUS	Medio de comunicación inalámbrico.
SNMP	Protocolo de administración de red.
SSDI	Red inalámbrica para identificarlos.
SSH	Acceso por comando.
TI	Tecnología de la información.
VLAN	Red de área local virtual.
WAN	Red de computadoras que une varias redes locales LAN.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Con el diseño y despliegue de una red inalámbrica dentro de una entidad bancaria, utilizando una solución escalable, se implementará un medio de transmisión seguro y confiable para la transmisión de la información entre diferentes dispositivos de trabajo, tanto en lo institucional o comercial.

Esto innovará a una transformación digital con un enfoque omnicanal que mejorará la experiencia en el usuario, como uno de los propósitos estratégicos de la entidad bancaria y demostrará que las tecnologías de la información y comunicaciones pueden incidir positivamente en los indicadores de producción y eficiencia en cualquier sector privado o público, actualmente más de 85% de las transacciones del banco se realizan a través de canales electrónicos, lo que significa que los clientes se auto sirven y optimiza su tiempo en plataformas fáciles y seguras.

Se vuelve necesario poseer una red inalámbrica con el objetivo de contar con una movilidad inalámbrica bancaria para sus empleados y de brindar una experiencia digital a sus clientes, confiable y de servicio de alta calidad para que diversas aplicaciones bancarias mantengan la disponibilidad necesaria para la operación diaria, con oficinas futuristas que se enfoca en desarrollar una nueva experiencia que desarrolle el autoservicio a través de canales digitales, contando también con asesores financieros provistos con dispositivos digitales que guiaran a los clientes en el uso de los canales financieros.

Se definirá tres portales cautivos independientes y cuatro SSID en las cuales se mostrarán dependiendo del área que están ubicados los AP a nivel nacional. Para el SSID Funcionarios y el SSID Funcionarios Vip contarán con un solo portal cautivo, para el SSID Invitados contará con su portal cautivo independiente y para el SSID Clientes contará con su portal cautivo también independiente, señalizados estratégicamente con códigos QR visibles redireccionándolos a su portal cautivo del SSID invitados y clientes. Para el SSID Clientes solo serán evidenciados en el área de servicio al cliente a nivel nacional.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

En la anterior infraestructura inalámbrica de la entidad bancaria estaba diseñada por Access Point de marca Ruckus, en la cual los problemas a presentarse fueron: Se requería de 2 o más Access Point por departamento en una área muy reducida, su señal de cobertura no era muy amplia, en la controladora de los Ruckus no contaba con la compatibilidad de agregar el Active Directory, por lo tanto, se decidió habilitar SSDI protegida con WPA2. Cada vez que un usuario quería conectarse a la red inalámbrica, se requería llenar un formulario identificando la Mac de todos los dispositivos que disponía, agregándolos a la red uno por uno en la controladora Ruckus. Esto lo convierte en una red insegura, porque no estaba protegido por el firewall, es decir que se adquiría internet puro.

1.2 Descripción del Problema

La visión de la entidad financiera es ser líder en innovación en banca digital, una de las estrategias para lograr esto es la movilidad empresarial. En la actualidad cuenta con más de 2 millones de clientes y 2.000 empleados a nivel nacional, entre ellos personal de trabajo 24/7 (Standby) y proveedores externos.

El registro de control del uso de la red inalámbrica es manual. Las portátiles, los dispositivos móviles o iPad asignados, requieren la autorización de los responsables del área y de gerentes departamentales, lo que genera una documentación física. Dado que la infraestructura actual no cuenta con acceso seguro de movilidad empresarial, se puede saltar el proceso del registro físico del documento, exponiendo a los equipos a que estén en constante riesgo, y a la red como un entorno no seguro y vulnerable.

Los empleados y proveedores externos que utilizan sus propios dispositivos requieren de controles adicionales ya que están expuestos a ataques informáticos, tales como, robo de información personal, entre otros. Sin embargo, estos controles no se ejecutan por falta de recursos asignados al mismo.

1.3 Solución Propuesta

Porqué se decidió elegir una infraestructura Cisco como una solución al problema a diferencias de otras marcas, su tecnología es de la más alta calidad y está diseñada para ser fácil de gestionar; otorgándonos fiabilidad, seguridad avanzada, tecnología que pueda crecer en el negocio y garantía en sus productos. Cisco se destaca en cada una de estas áreas, ofreciendo a sus clientes un costo más bajo de propiedad y un mejor retorno de la inversión a lo ofrecida por otras marcas.

Se realizará la creación de un portal cautivo para el control de acceso de empleados y proveedores externos. La segunda fase comprende el control de acceso de los clientes a través de canales virtuales. Una vez que la solución este implementada se crearán políticas de segmentación basadas en una integración de servidores Cisco, destinadas a contener las amenazas para la red inalámbrica, facilitando la administración de implementaciones a gran escala.

Se creará un grupo de identidad de usuarios para identificar la categoría de los usuarios que se realizarán para las diversas solicitudes de acceso a la red inalámbrica. Para los empleados y proveedores se tendrá un control de acceso unificado y centralizado basado en un portal cautivo, lo que permitirá una mayor visibilidad e identificación más precisa mediante el servicio de difusión de perfiles y dispositivos. ¿Por qué no se eligió el método de autenticación Dot1x integrado con el directorio activo corporativo? Actualmente la red inalámbrica es total mente aislada de la red interna bancaria, por tal motivo su integración sería por medio de un ADFS externo en la cual no es compatible, no es soportada por un Dot1x, se tomó la decisión de elegir el portal cautivo de la propia herramienta tecnológica ISE como servidor de autenticación con el ADFS externo.

Podemos mencionar el uso de servidores de Identity Services Engine (ISE) entre las tecnologías a utilizar para mejorar la arquitectura de la infraestructura inalámbrica. Además, se tendrá como solución de control de políticas centralizada mediante autenticación de usuarios ADFS Externo como directorio activo, mediante el cual permite el acceso a la red solo a usuarios autorizados y puede aplicar políticas por perfiles de usuarios para autorizar el acceso a los servicios de la red de acuerdo al perfil que pertenece.

Adicionalmente se utilizarán dos infraestructura inalámbrica Wireless Lan Controller (WLC) en alta disponibilidad, para monitoreo y reportaría de la infraestructura de red se instalará un appliance en la cual se levanta el

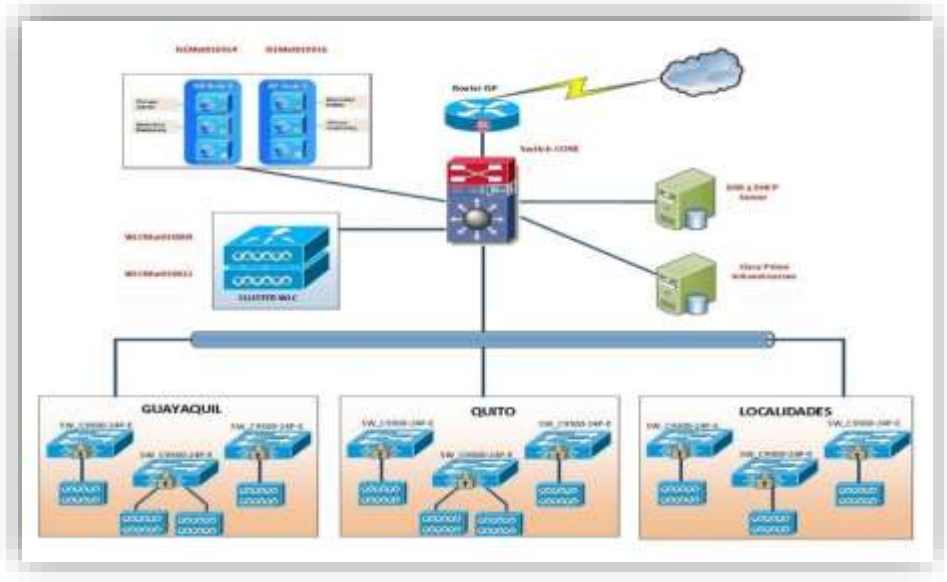


Figura 1. 1 Arquitectura de la Infraestructura Inalámbrica.

Cisco Prime Infraestructure. La arquitectura inalámbrica necesaria para el desarrollo de la solución.

Para los clientes se tendrá un control de internet diferente, con su portal cautivo mediante una nueva solución inalámbrica compatible, que se compone de dos herramientas basada en Alepo (Software) & Meraki (Software), esto permite un modelo de negocio verdaderamente seguro y estable basados en redes inalámbricas de acceso público.

El esquema de la infraestructura Alepo Meraki:

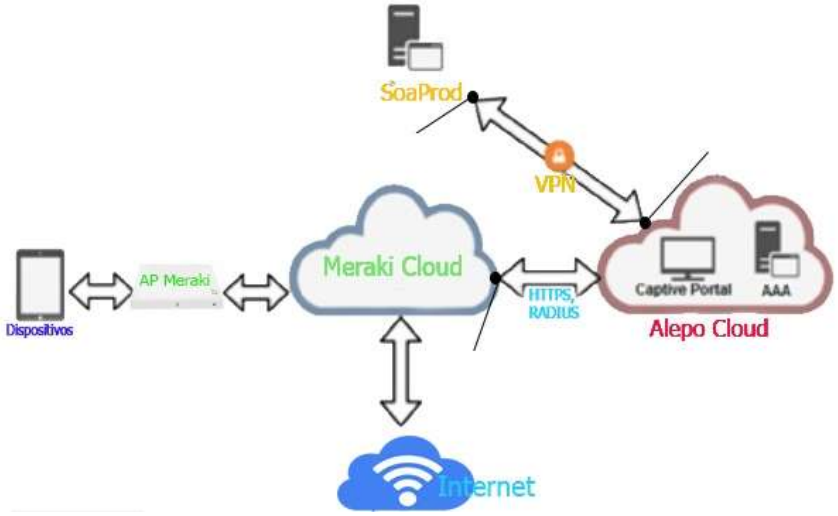


Figura 1. 2 Arquitectura del flujo de comunicación entre el Servicio Web de Alepo y el Servicio Web de la entidad bancaria (Cliente - Banco).

1.4 Objetivo General

Diseñar un nuevo modelo de infraestructura inalámbrica en una entidad financiera, para garantizar un mejoramiento en el proceso de automatización del usuario final, diseñando y desplegando una solución escalable implementando un medio de transmisión inalámbrica segura y confiable, para la transmisión de la información entre diferentes dispositivos inalámbricos de trabajo tanto en lo institucional para los empleados o comercial para los proveedores; otorgando credenciales de acceso.

Para sus clientes, los servicios bancarios o transacciones se realizan a través de canales electrónicos, lo que significa que los clientes eviten largas horas de espera se auto sirven y optimizan su tiempo en plataformas fáciles y seguras en diferentes agencias bancarias y en los centros virtuales.

1.5 Objetivos Específicos

Realizar un levantamiento de requerimientos en los clientes e identificar nuevas aplicaciones bancarias móviles para los canales virtuales dirigidos a clientes optimizando tiempos y recursos de atención presencial con cualquier funcionario de servicios bancarios.

Evaluar los resultados de las mejoras implementadas, mediante encuestas dirigidas a clientes y a funcionarios, para determinar si los cambios implementados han tenido el impacto que se buscaba, alcanzando un mejor servicio bancario en transformación digital.

Diseñar e implementar un esquema de autentificación que permita mejorar el acceso a la red inalámbrica por medio de un portal cautivo seguro para los funcionarios y proveedores, logrando un acceso seguro y controlado haciéndolo diferente al acceso inalámbrico anterior, ya que el registro de control del uso de la red inalámbrica era de forma manual (formulario), lo que generaba una documentación física de permisos de accesos.

1.6 Metodología

Con la propuesta de este proyecto que estamos haciendo con los Access Point Cisco, queremos cambiar la infraestructura inalámbrica en el banco de la siguiente manera:

- Se contrataría dos enlaces de datos dedicados con los proveedores que el banco nos proporcione. ¿Por qué enlace dedicados y no de internet? Esto se lo haría con el fin de hacer llegar una última milla de fibra óptica en el data center del banco, para que se puedan apegarse en los concentradores de fibra que tienen actualmente, haciendo todo esto se lo configuraría para que pase por la red Lan del banco y así estar con la seguridad del firewall. Un enlace principal, y uno de Backup.
- Los AP Cisco tienen mayor señal de cobertura y se podría poner un AP por departamento, a diferencia de los Ruckus.
- Se hará pruebas de señal de coberturas en todos los pisos, para poder saber con exactitud dónde ubicar cada AP para que de la cobertura suficiente a todos los usuarios.

- Estos AP soportan mayor ancho de banda, por lo que se le podría decir al proveedor el ancho de banda que necesitamos.
- Se creará un portal cautivo con la integración del ADFS Externo, los usuarios puedan acceder a internet a través de un método de autenticación, Se define cuatro SSID diferentes funcionarios – Funcionarios Vip – Invitados - Clientes.

Estos cuatro SSID estarían configurados con VLAN diferentes para poder separar el tráfico de datos de cada red, y con tres portales cautivos independientes.

El SSID funcionarios se conectan a nivel jerárquico jefes, líder, ejecutivos y todos los demás funcionarios del banco. En el SSID funcionarios Vip, se conectan todos los Gerentes, Subgerentes, Presidencia Ejecutiva, Vicepresidentes Ejecutiva y Miembros del Directorio, estos dos SSID compartirán un solo portal cautivo.

El SSID invitados, se conectan todo proveedor externo o visitas facilitándoles un código QR redireccionándolos a un portal cautivo. Estos códigos QR están ubicados estratégicamente en sala de reuniones, auditorio y oficinas departamentales.
El SSID clientes, es para poder proporcionarles internet a los clientes para que se puedan descargar los aplicativos del banco. facilitándoles un código QR redireccionándolos a un portal cautivo. Estos códigos QR están ubicados estratégicamente en áreas de atención al público, por un tiempo definido en 1 hora de conexión diaria.

Tabla 1 SSID de la Red Inalámbrica

SSID de la Red Inalámbrica			
SSID	**VLAN ID**	**NAME**	**RED**
Funcionarios	100	GYE Principal Funcionarios	10.233.000.0/00
Funcionarios VIP	200	GYE Principal VIP	10.233.000.0/00
Invitados	300	GYE Principal Invitados	10.233.000.0/00
Clientes	400	GYE Principal Clientes	10.233.000.0/00

CAPÍTULO 2

MARCO TEÓRICO

2.1 Análisis de la situación actual

En la entidad bancaria no se cuenta con una infraestructura inalámbrica robusta a nivel de seguridad tecnológica, por lo tanto, se requiere implementar una solución inalámbrica estable y así incorporar nuevas tecnologías en los servicios bancarios, como un medio de comunicación a sus funcionarios y clientes.

En toda entidad bancaria siempre quieren aumentar su agilidad la productividad de sus empleados y la satisfacción de sus clientes, se hace cada vez más importante este nivel de flexibilidad, porque ofrecer una respuesta en él mismo día ya no es suficiente ahora la respuesta tiene que darse en tiempo real. (CISCO, CISCO Movilidad excepcional con redes inalambricas, 2018)

2.2 Infraestructura Inalámbrica Centralizada

Ofrecer una ventaja competitiva que demandan en la actualidad las empresas en crecimiento, CISCO hace posible la comunicación instantánea y el uso compartido de información y también tiene el liderazgo de suministrar servicios seguros de alta calidad en movilidad avanzada. (CISCO, CISCO Movilidad excepcional con redes inalambricas, 2018)

- Voz a través de Wifi, que permite servicio de voz y mensajería inalámbricas, mejorando así la colaboración y la productividad.
- El acceso de invitados amplia para mejorar el uso compartido de la información, la productividad de los empleados y reducir al mismo tiempo los costes de soporte técnico.
- Los servicios de ubicación permiten contactar con los empleados de la forma más eficaz despendiendo de su ubicación y disponibilidad y también se hace un seguimiento coherente de los activos empresariales.
- La seguridad avanzada protege la red contra la intercepción de datos, los accesos no autorizados y otros tipos de ataques.

2.3 Movilidad Empresarial

Permitirían a los empleados desplazarse allí donde necesitan ir y obtener siempre un acceso seguro, esto permitirá obtener interacción inalámbrica en tiempo real, mensajería instantánea, alerta de texto, servicio de voz y acceso a la red tanto en oficina o en cualquier otro lugar, Ofrecer una seguridad de infraestructura inalámbrica integrada, y hacer posible conseguir una mayor productividad de los empleados, una mejor colaboración con una óptima capacidad de respuesta de atención al cliente. (CISCO, CISCO Movilidad excepcional con redes inalambricas, 2018)

La reducción de costos operativos es una de las ventajas de la red inalámbrica unificada en la administración centralizada de la red, que reduce de forma notable los gastos operativos, una mejor resolución de los problemas y el cambio permiten a los administradores de la red logar mayores índices de productividad. (CISCO, CISCO Movilidad excepcional con redes inalambricas, 2018)

Mejorar la eficiencia operativa disponer de acceso a internet desde dispositivos móviles como teléfonos o portátiles han revolucionado la

interacción entre banco y clientes. (CISCO, CISCO Movilidad excepcional con redes inalambricas, 2018)

Maximizar la capacidad de respuestas frente a los clientes es un factor esencial para mantener la competitividad, la movilidad otorga a los bancos agilidad para mantener a los clientes conectados a la información y las herramientas que necesitan. (CISCO, CISCO Movilidad excepcional con redes inalambricas, 2018)

Maximizar la seguridad inalámbrica es una consideración esencial cuando se implementa una infraestructura inalámbrica con tecnologías de protección a nivel empresarial y basadas en estándares, para evitar y solventar brechas de seguridad destacado en sistemas de detención y prevención de intrusos, que detectan y contienen estos puntos de acceso ilegales, dispositivos o clientes no autorizados, etc. (CISCO, CISCO Movilidad excepcional con redes inalambricas, 2018)

2.4 Administración / Gestión de la Infraestructura

Mediante una combinación de la red cableada e inalámbrica, la entidad financiera puede implementar las capacidades más recientes y ahorrar tiempo y costes mediante el uso del conocimiento y la formación del personal de TI, así como la infraestructura existente. Esta integración también sería útil para asegurarse de que sea cual sea el tipo de dispositivo utilizado para tener acceso a la red, los mismos servicios y capacidades estarán disponibles para todos los empleados. (CISCO, CISCO Movilidad excepcional con redes inalambricas, 2018).

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN Y SOLUCIÓN PROPUESTA

3.1 Definiciones de Alcances

Se presentan los criterios para configurar e integrar como solución inalámbrica los equipos Wireless LAN Controller (WLC), Identity Services Engine (ISE) y Cisco Prime Infrestructure, esquemas utilizados en alta disponibilidad, configuración e integración del ADFS con el Active Directory, asignación y direccionamiento IP con la topología de la infraestructura inalámbrica.

3.2 Equipamiento y configuración utilizados en la solución

El equipamiento utilizado en la solución implementada en la entidad financiera está basado en dos servidores de Identity Service Engine en alta disponibilidad en cada uno con los roles de Administración, supervisión y servicios de políticas.

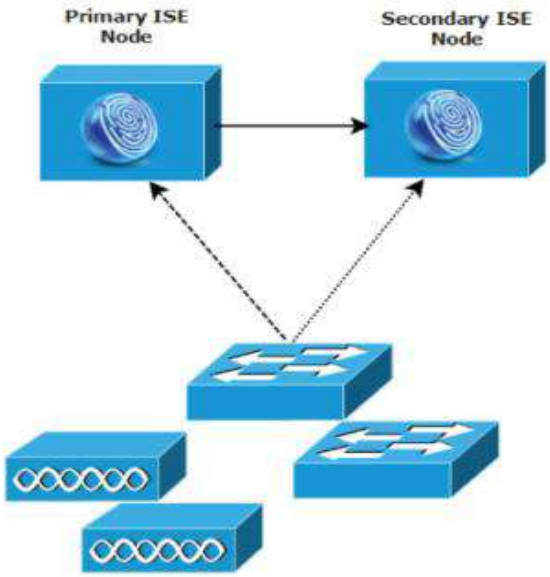


Figura 3. 1 Appliances de Identity Service en alta disponibilidad

Para la red inalámbrica, se utilizaron 2 Wireless Lan Controller de la serie 5520 en alta disponibilidad.

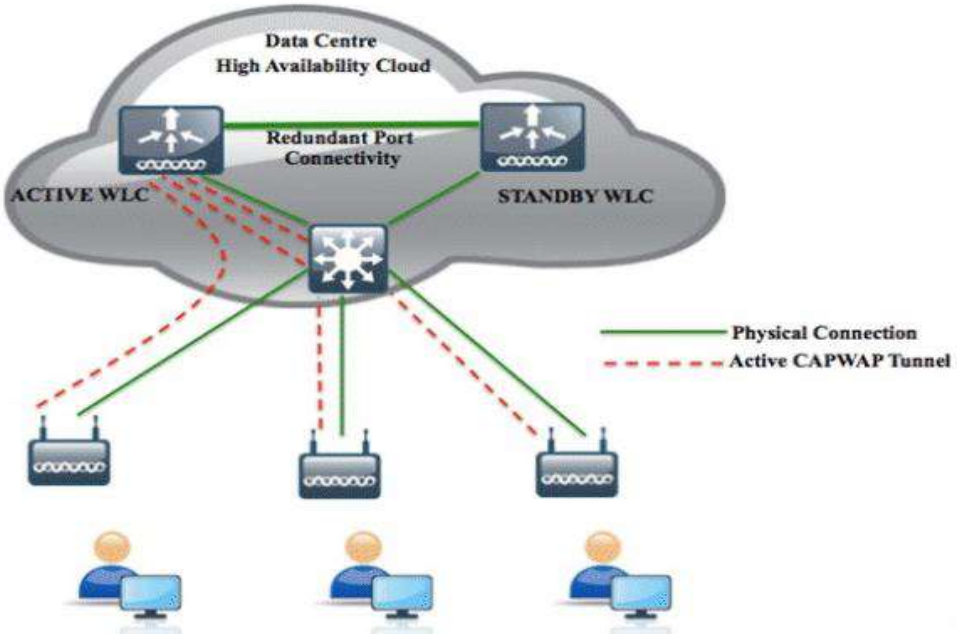


Figura 3. 2 Wireless Lan Controller en alta disponibilidad

Para monitoreo de la infraestructura se instaló un appliance en el cual se levanta el Cisco Prime Infraestructure.

3.3 Plan de acción ADFS o Active Directory

Desde Cisco ISE

Importar archive XML desde ISE SP

Figura 3. 3 Importar archivo XML desde ISE SP

Configuración de ADFS Relying Party Trusts

Añadir nueva **"Relying Party Trust"**

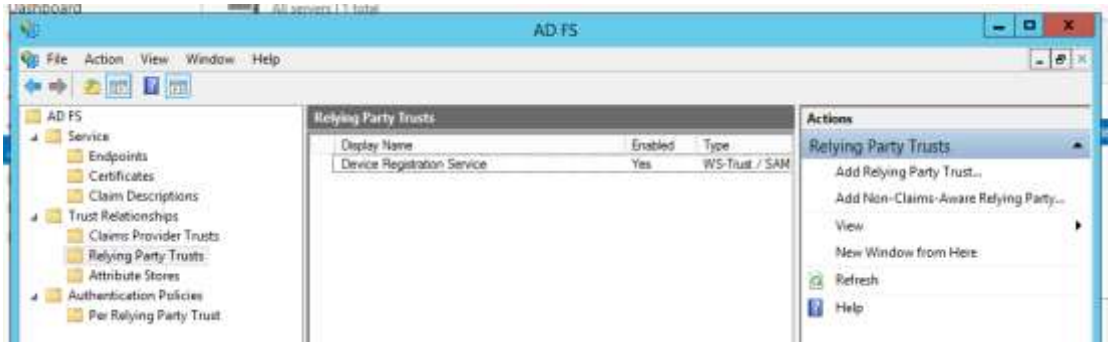


Figura 3. 4 Configuración de ADFS Relying Party Trusts

Seleccionar fuente de datos

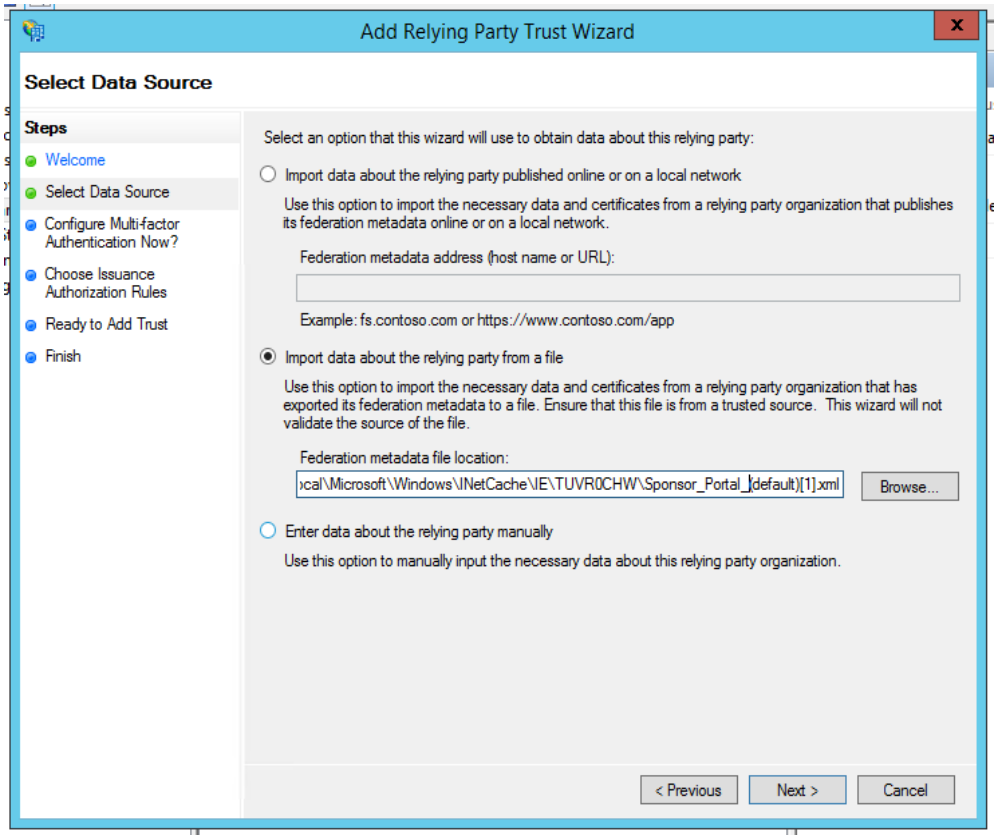


Figura 3. 5 Seleccionar fuente de datos

Se selecciona el archive XML descargado desde el ISE Asignación de nombre Choose Issuance Authorization Rules: Permit all users to access this relying party Validar check - Open Edit Claim Rues Dialog: **Ticked**

Seleccionar - **“Issuance Transform Rules”**

Añadir nueva regla: Claim Rule Template: Send LDAP Attributes as Claims

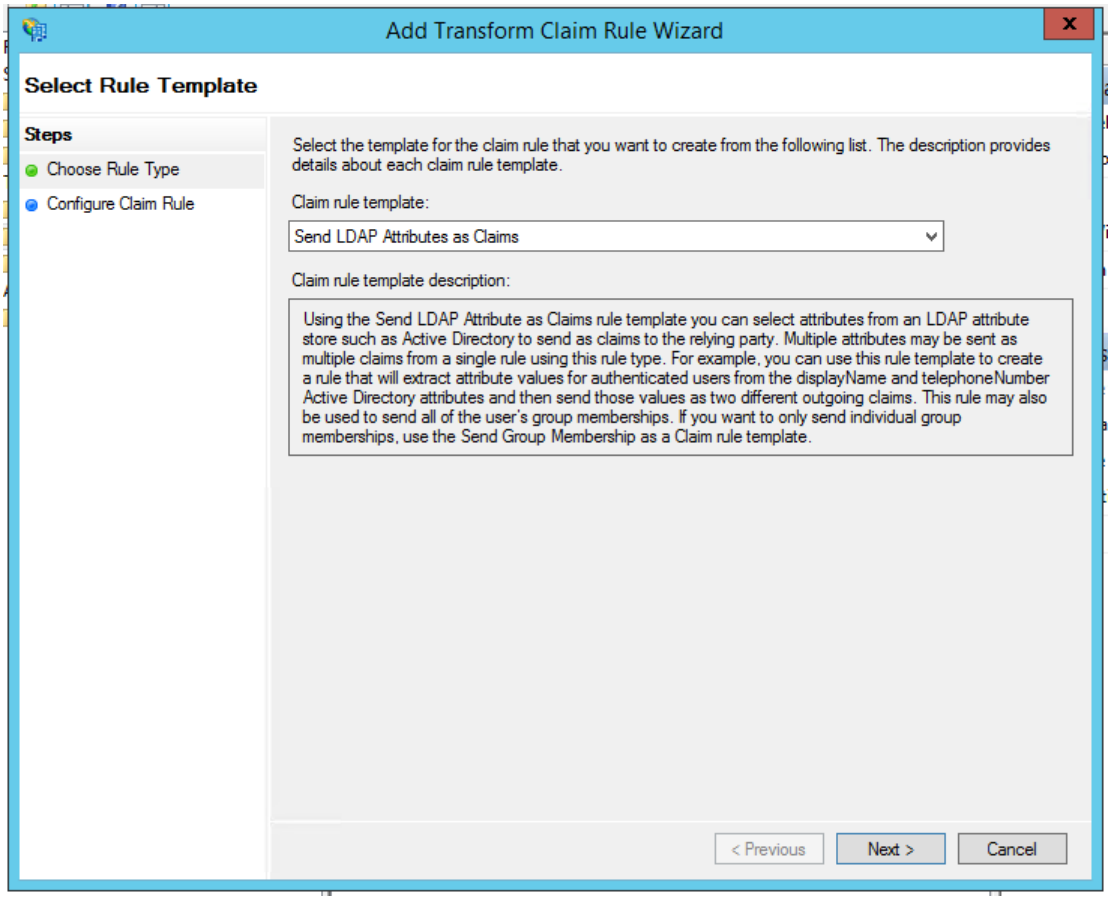


Figura 3. 6 Plantilla de regla de reclamo

Regla de reclamo

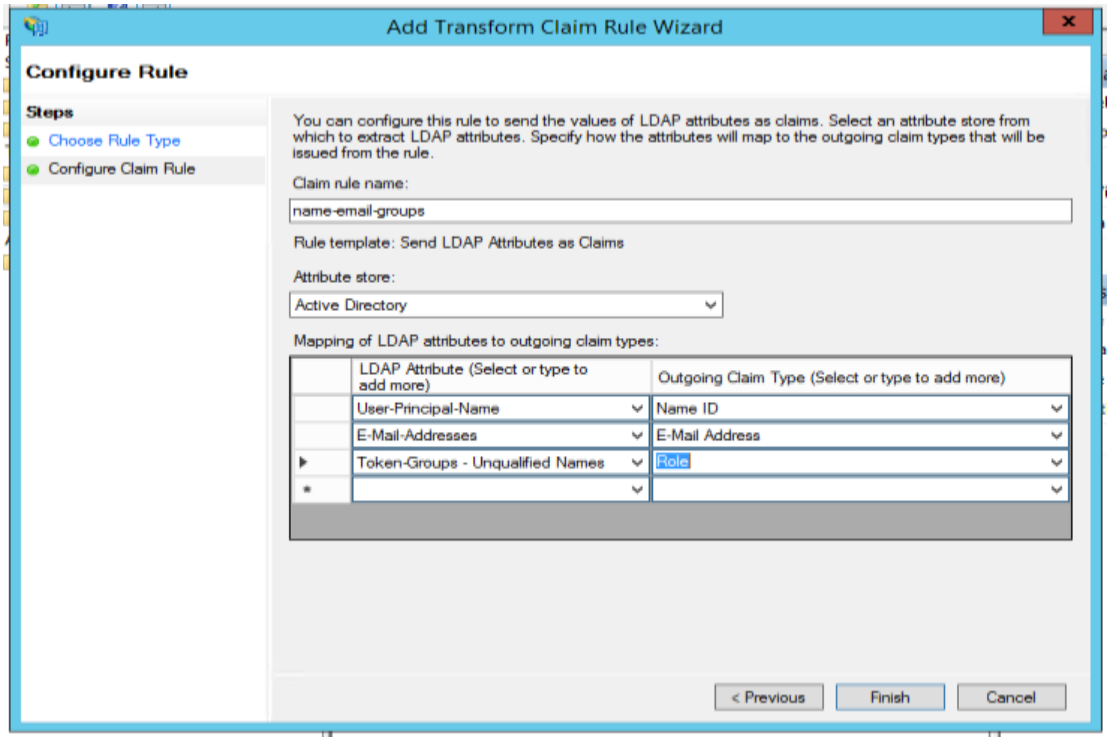


Figura 3. 7 Regla de reclamo

Aplicar – Aceptar políticas de autenticación

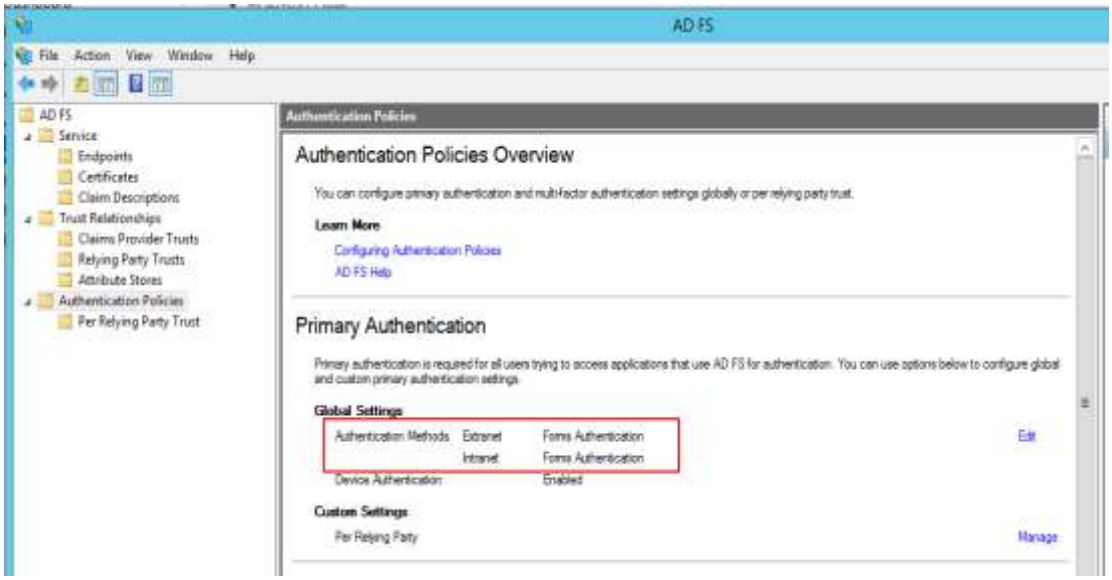


Figura 3. 8 Políticas de autenticación

Verificación de Per Relying Trust - Multifactor

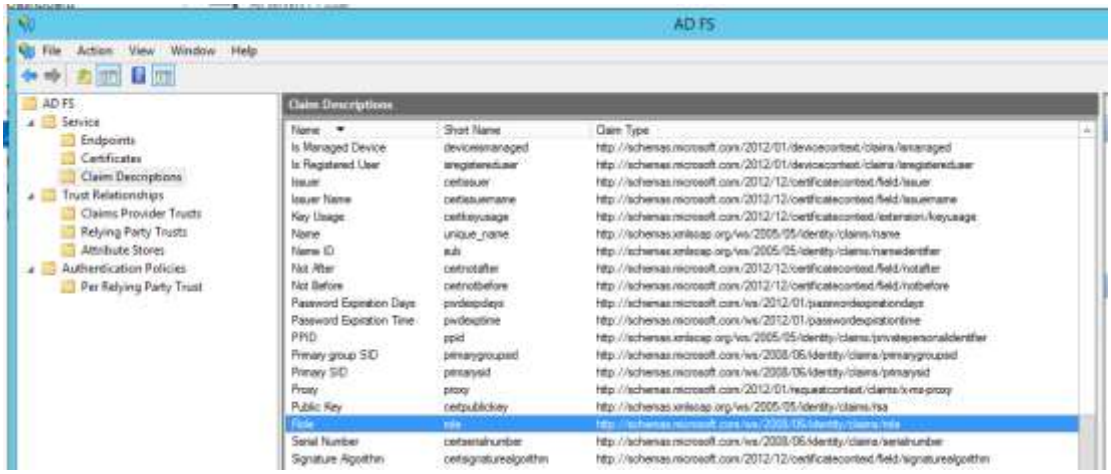


Figura 3. 9 Verificación de Per Relying Trust

3.4 Inventario y direccionamiento IP

A continuación, su inventario, direccionamiento IP y credenciales de la infraestructura instalada.

Tabla 2 Inventario

INVENTARIO			
Hostname	**Modelo**	**Serie**	**Descripción**
DNS	UCS240	FCH17330000	Servidor DHCP/DNS
VMWare	Ver 6.0		VMware
ISE Principal	SW-3515-ISE-K9	SFCH22160000	Cisco ISE Principal
ISE Secundario	SW-3515-ISE-K9	SFCH22160000	Cisco ISE Secundario
WLC Principal	AIR-CT5520-K9	SFCH22160000	Wireless LAN Controllers Principal
WLC Secundario	AIR-CT5520-K9	SFCH22250000	Wireless LAN Controllers Secundario
PRIME	PI-UCS-APL-K9	FCH2215V0000	Cisco Prime Infrestructure

Tabla 3 Direccionamiento IP

DIRECCIONAMIENTO IP			
Hostname	**Modelo**	**Descripción**	**Dirección IP**
DNS	UCS240	Servidor DHCP/DNS	10.233.000.00
VMWare	ver 6.0	VMWare	10.233.000.00
ISE Principal	SW-3515-ISE-K9	Cisco ISE Principal	10.233.000.00
ISE Secundario	SW-3515-ISE-K9	Cisco ISE Secundario	10.233.000.00
WLC Principal	AIR-CT5520-K9	Wireless LAN Controllers Principal	10.233.000.00
WLC Secundario	AIR-CT5520-K9	Wireless LAN Controllers Secundario	10.233.000.00
PRIME	PI-UCS-APL-K9	Cisco Prime Infrestructure	10.233.000.00

Tabla 4 Modelo y Versión

MODELO Y VERSIÓN		
Hostname	**Modelo**	**Versión**
ISE Principal	SW-3515-ISE-K9	2.4.0.357, patch 4,5
ISE Secundario	SW-3515-ISE-K9	2.4.0.357, patch 4,5
WLC Principal	AIR-CT5520-K9	8.8.100.0
WLC Secundario	AIR-CT5520-K9	8.8.100.0
PRIME	PI-UCS-APL-K9	3.3.0

Los Access Point instalados se muestran a continuación, las credenciales para acceso SSH y vía telnet son las mismas que se utilizan para el WLC.

Tabla 5 Direccionamiento IP Access Point

DIRECCIONAMIENTO IP ACCESS POINT			
AP Name	**IP Address**	**AP Serial Number**	**Localización**
AP_MAT002	10.233.000.00	FJC2232M000	Matriz
AP_MAT002	10.233.000.00	FJC2232M000	Matriz
AP_MAT003	10.233.000.00	FJC2232M000	Matriz
AP_MAT003	10.233.000.00	FJC2232M000	Matriz
AP_MAT004	10.233.000.00	FJC2232M000	Matriz
AP_MAT004	10.233.000.00	FJC2232M000	Matriz
AP_MAT005	10.233.000.00	FJC2232M000	Matriz
AP_MAT005	10.233.000.00	FJC2232M000	Matriz
AP_MAT006	10.233.000.00	FJC2232M000	Matriz
AP_MAT006	10.233.000.00	FJC2232M000	Matriz
AP_MAT007	10.233.000.00	FJC2232M000	Matriz
AP_MAT007	10.233.000.00	FJC2232M000	Matriz
AP_MAT008	10.233.000.00	FJC2232M000	Matriz
AP_MAT008	10.233.000.00	FJC2232M000	Matriz
AP_MAT009	10.233.000.00	FJC2232M000	Matriz
AP_MAT009	10.233.000.00	FJC2232M000	Matriz
AP_MAT010	10.233.000.00	FJC2232M000	Matriz
AP_MAT010	10.233.000.00	FJC2232M000	Matriz
AP_MAT010	10.233.000.00	FJC2232M000	Matriz
AP_MAT010	10.233.000.00	FJC2232M000	Matriz
AP_MAT011	10.233.000.00	FJC2232M000	Matriz
AP_MAT011	10.233.000.00	FJC2232M000	Matriz
AP_MAT011	10.233.000.00	FJC2232M000	Matriz
AP_MAT011	10.233.000.00	FJC2232M000	Matriz
AP_MAT012	10.233.000.00	FJC2232M000	Matriz
AP_UIO001	10.233.000.00	FJC2232M000	Quito
AP_UIO001	10.233.000.00	FJC2232M000	Quito
AP_UIO001	10.233.000.00	FJC2232M000	Quito
AP_UIO001	10.233.000.00	FJC2232M000	Quito
AP_UIO003	10.233.000.00	FJC2232M000	Quito
AP_UIO003	10.233.000.00	FJC2232M000	Quito
AP_UIO003	10.233.000.00	FJC2232M000	Quito
AP_UIO003	10.233.000.00	FJC2232M000	Quito

3.5 Topología de la nueva Infraestructura Inalámbrica

Evidenciamos perfiles de SSID con su método de autenticación conectados a un Switch Core donde mostramos la integración en alta disponibilidad de los servidores Wireless LAN Controller (WLC), Identity Services Engine (ISE) y Cisco Prime Infrestructure, conectados por un Router ISP Internet.

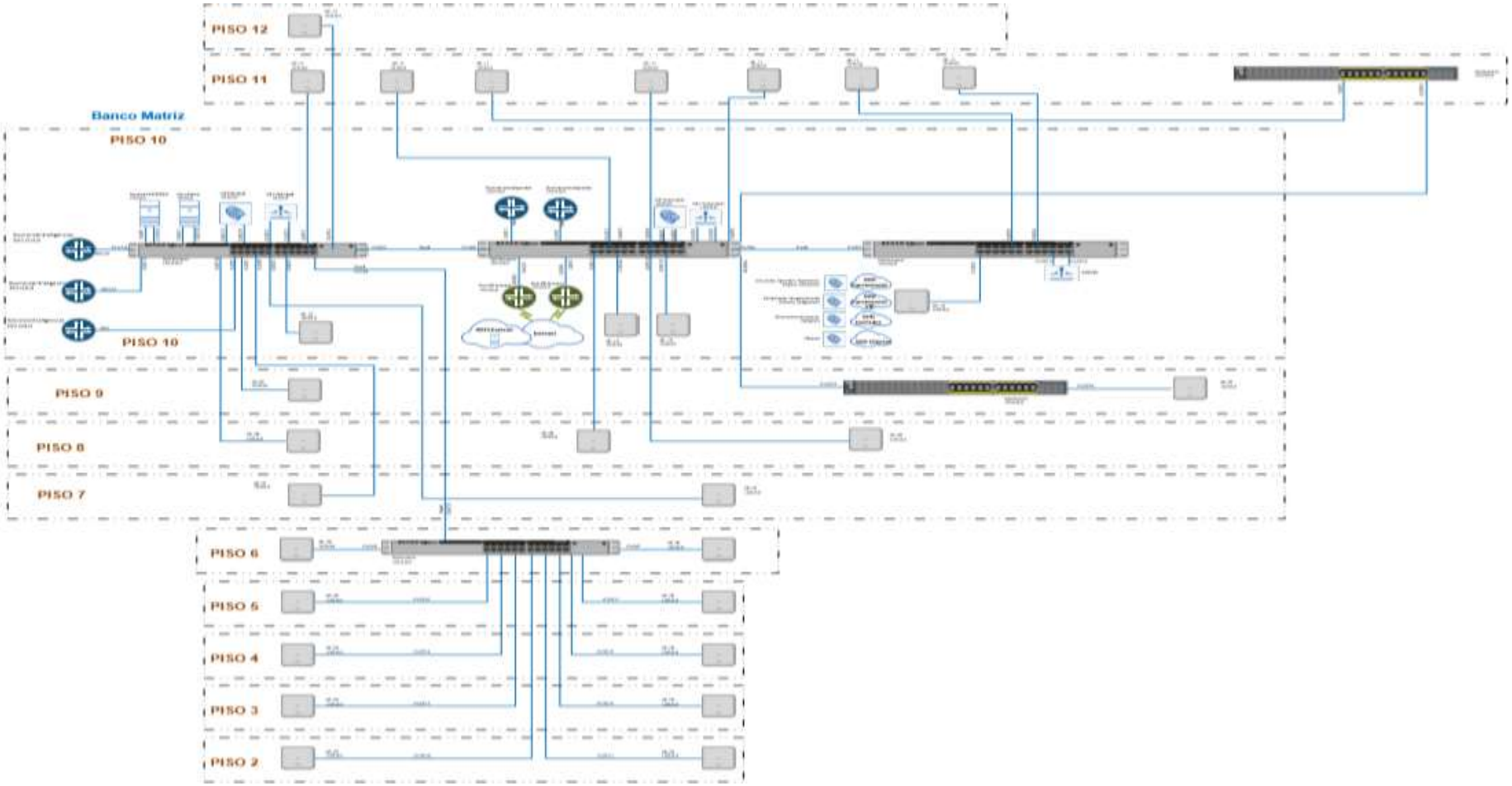


Figura 3. 10 Topología de la nueva Infraestructura Inalámbrica

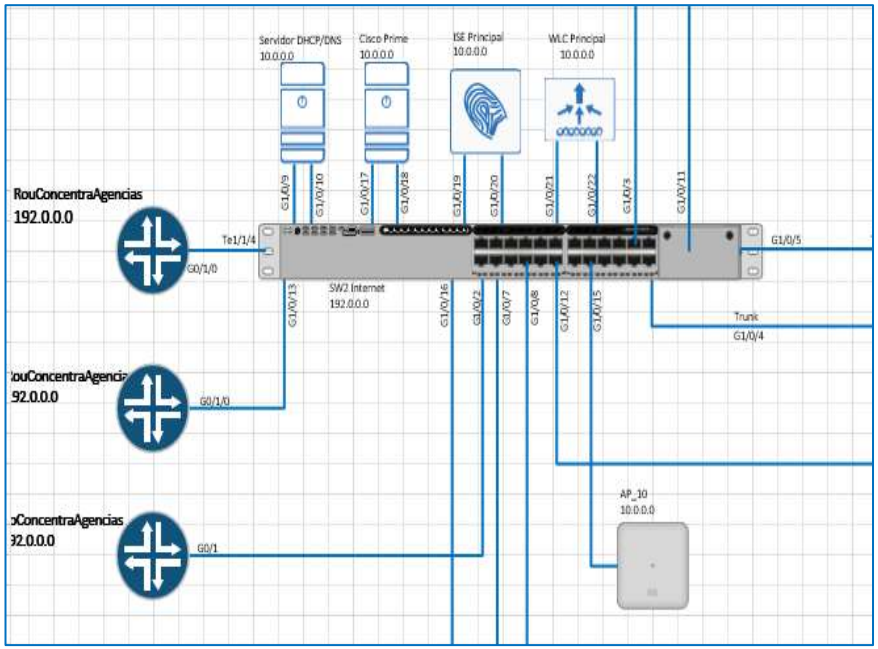


Figura 3. 12 Topología de la nueva Infraestructura Inalámbrica Concentradores – Servidores Principales – Servidor DHCP/DNS

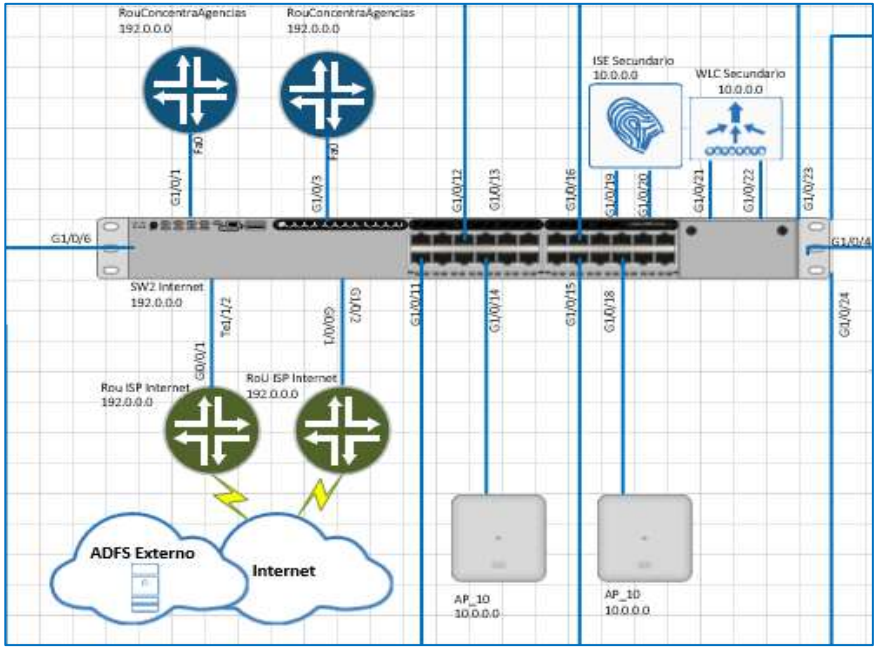


Figura 3. 11 Topología de la nueva Infraestructura Inalámbrica ISP – Servidores Secundarios

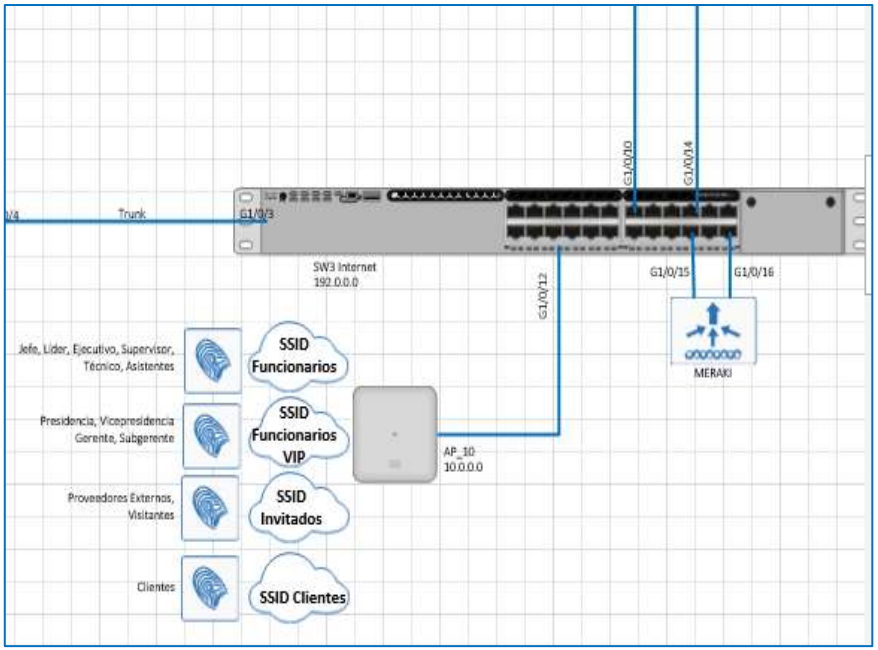


Figura 3. 13 Topología de la nueva Infraestructura Inalámbrica SSID

CAPÍTULO 4

ANÁLISIS Y DISEÑO DE LA SOLUCIÓN EMPLEADOS – PROVEEDORES

4.1 Detalle de la Solución de Hardware

Ofrecer una infraestructura inalámbrica segura y escalable logrando objetivos de resultados siendo más fácil de implementar y administrar. A continuación, se detalla la infraestructura Cisco a utilizar justificándose por su actualización de equipos tecnológicos en una infraestructura inalámbrica:

4.1.1 Servidor de red Seguro Cisco

La concesión y denegación de acceso a la red ha evolucionado más allá de las simples verificaciones de nombre de usuario y contraseña. Hoy, los atributos adicionales relacionados con los usuarios y sus dispositivos se utilizan como criterios de decisión para determinar el acceso autorizado a la red. Además, el aprovisionamiento de servicios de red puede basarse en datos como el tipo de dispositivo que accede a la red, incluido si se trata de un dispositivo corporativo o personal. (CISCO, 2019)

El servidor de red seguro Cisco es una solución escalable que ayuda a los administradores de red a satisfacer las complejas demandas de control de acceso a la red al administrar las diferentes operaciones que pueden colocar cargas pesadas en aplicaciones y servidores, que incluyen:

- Solicitudes de autorización y autenticación.
- Consultas a almacenes de identidad como Active Directory y bases de datos LDAP
- Perfil del dispositivo y comprobación de postura
- Acciones de cumplimiento para eliminar dispositivos de la red
- Informes

Figura 4. 1 Cisco Servidor de red seguro SNS-3615, SNS-3655 y SNS-3695

El servidor de red seguro de Cisco se basa en el servidor de bastidor Cisco UCS C220 y está configurado específicamente para admitir las aplicaciones de seguridad del Sistema de control de acceso (ISE) y el Sistema de control de acceso (ACS) de Cisco. El servidor de red seguro admite estas aplicaciones en dos versiones. El Cisco Secure Network Server 3615 está diseñado para implementaciones pequeñas. Secure Network Server 3655 y 3695 tiene varios componentes redundantes, como discos duros y fuentes de alimentación, lo que lo hace adecuado para implementaciones grandes que requieren configuraciones de sistema altamente confiables. (CISCO, 2019)

Al solicitar un servidor de red seguro, el cliente tiene la flexibilidad de elegir las aplicaciones de seguridad de Cisco Identity Services Engine (ISE) o del sistema de control de acceso (ACS). (CISCO, 2019).

Tabla 6 Evaluación comparativa Cisco Secure Network Server

EVALUACIÓN COMPARATIVA			
Nombre del producto	**Servidor de red seguro 3615**	**Servidor de red seguro 3655**	**Servidor de red seguro 3695**
Procesador	1 - Intel Xeon 2.10 GHz 4110	1 - Intel Xeon 2.10 GHz 4116	1 - Intel Xeon 2.10 GHz 4116
Núcleos por procesador	8	12	12
Memoria	32 GB (2 x 16 GB)	96 GB (6 x 16 GB)	256 GB (8 x 32 GB)
Disco duro	1 - 2.5 pulg. 600 GB 6 Gb SAS 10K RPM	4 - 2.5 pulg. 600 GB 6 Gb SAS 10K RPM	8 - 2.5 pulg. 600 GB 6 Gb SAS 10K RPM
RAID de hardware	No	Nivel 10 Controlador RAID modular Cisco 12G SAS	Nivel 10 Controlador RAID modular Cisco 12G SAS
Interfaces de red	2 x 10Gbase-T 4 x 1GBase-T	2 x 10Gbase-T 4 x 1GBase-T	2 x 10Gbase-T 4 x 1GBase-T
Fuentes de alimentación	1 x 770W	2 x 770W	2 x 770W

4.1.2 Cisco Identity Services Engine (ISE)

Un componente integral de la iniciativa de ciber seguridad de Cisco, Cisco Identity Services Engine (ISE) es un revolucionario producto que amplía las capacidades de acceso a la red y control de admisión ofrecida por primera vez en Cisco NAC y Cisco ACS seguro. (Cisco, S.F.) (CISCO, 2019)

Más allá del nombre de usuario y la contraseña, Cisco Identity Services Engine ofrece resultados sin precedentes habilidades para adquirir identidad de usuario y dispositivo e información de contexto para forjar políticas flexibles y poderosas que gobierna el acceso autorizado a la red. ISE es una plataforma de control de políticas empresariales todo

en uno que puede proporcionar de manera confiable acceso seguro para redes cableadas, inalámbricas y VPN. ISE también puede ayudar a TI con la incorporación segura de BYOD y permitir que TI proporcione acceso de invitado diferenciado. Identity Services Engine proporciona acciones de cumplimiento que permite a los administradores restringir los dispositivos de la red que están violando el acceso y las políticas. (Cisco, S.F.) (CISCO, 2019).

Figura 4. 2 Cisco Servidor de red seguro

4.1.3 Cisco Wireless Lan Controller (WLC)

El controlador inalámbrico Cisco 5520 proporciona control centralizado, administración y solución de problemas para implementaciones de gran escala en implementaciones de proveedores de servicios y grandes campus. Ofrece flexibilidad para admitir múltiples modos de implementación en el mismo controlador: por ejemplo, modo centralizado para campus, modo Cisco FlexConnect para sucursales lean administradas a través de la WAN y modo de malla (puente) para implementaciones donde el cableado completo de Ethernet no está disponible. Como componente de la red inalámbrica unificada de Cisco, este controlador proporciona comunicaciones en tiempo real entre los puntos de acceso de Cisco Aironet, la infraestructura de Cisco Prime y el motor de servicios de movilidad de Cisco, y es interoperable con otros controladores de Cisco. (CISCO, 2019)

La arquitectura de red digital de Cisco (Cisco DNA) es una arquitectura abierta y extensible basada en software que acelera y simplifica las operaciones de red de su empresa. La arquitectura programable libera a su personal de TI de tareas de configuración de red repetitivas que requieren mucho tiempo para que puedan centrarse en la innovación que transforma positivamente su negocio. SD-Access, como parte de Cisco DNA, permite la automatización basada en políticas de borde a la nube con capacidades fundamentales. Cisco DNA Assurance, también parte de Cisco DNA, proporciona una única fuente para monitorear, modificar y administrar su red y los datos de la aplicación. (CISCO, 2019)

Figura 4. 3 Cisco 5520 Servidor Control Inalámbrico

Tabla 7 Evaluación comparativa Cisco Wireless Lan Controller

EVALUACIÓN COMPARATIVA			
	Controlador inalámbrico 5520	**Controlador inalámbrico 8510**	**Controlador inalámbrico 8540**
General			
Despliegue objetivo	Medianas a grandes empresas	Gran empresa y proveedor de servicios	Gran empresa y proveedor de servicios
Factor de forma	Aparato 1RU	Aparato 1RU	Aparato 2RU
FlexConnect	si	si	si
Escalabilidad			
Puntos de acceso mínimos	1	300	1
Puntos máximos de acceso	1,500	6,000	6,000

Máximo soporte al cliente	20,000	64,000	64,000
Máximo rendimiento	20 Gbps	10 Gbps	40 Gbps
VLAN máximas	4095	4095	4095
Detalles de la plataforma			
Interfaces o E/S de red	Dos 10 GE	Dos 10 GE	Cuatro 10 GE
Máximo consumo de energía	190W	675W	538W
Garantía estándar de hardware	3 años	90 días	3 años
Garantía de software estándar	90 días	90 días	90 días

4.1.4 Cisco Prime Infraestructure

Simplifica la administración de redes inalámbricas, cableadas y automatizar las tareas de administración mientras aprovecha la inteligencia de sus redes Cisco, las características y capacidades del producto lo ayudan a:

- Darse cuenta de una gestión
- Consolidad productos
- Administrar la red para colaboración móvil
- Simplifica la gestión inteligente de WAN
- Extender la gestión al centro de datos
- Escala más grande

Ofrece el aprovisionamiento del día 0 y 1, así como la garantía del día N desde la sucursal hasta el centro de datos. Lo llamamos One Management, con esta vista única y este punto de control, puede obtener los beneficios de One Management en la red y en la informática. (CISCO, S.F.)

Figura 4. 4 Cisco Servidor de Reportería

4.1.5 Cisco Aironet 4800 Access Point

El punto de acceso Cisco Aironet 4800 está repleto de una gran cantidad de características que ofrecen a los usuarios una mejor experiencia, seguridad de primer nivel y conectividad de alta velocidad. Aironet 4800 facilita la resolución de problemas y mejora el contexto que se muestra en Cisco DNA Assurance.

La funcionalidad del punto de acceso se extiende a través de cuatro radios internas, por lo que estas funciones se ejecutan simultáneamente en su red. El Aironet 4800 amplía las capacidades actuales de nuestra cartera actual de Aironet (con características tales como Asignación de radio flexible incorporada, Hiperlocación y Bluetooth Low Energy [BLE]) y agrega una cuarta radio interna para proporcionar un rendimiento rico y análisis de ubicación y seguridad. Con más radios integradas en el punto de acceso, su red inalámbrica logra una mayor seguridad y análisis de datos sin degradar el rendimiento: nunca más tendrá que cambiar la seguridad por el rendimiento de la red. (CISCO, 2020)

Figura 4. 5 Cisco Aironet 4800 Punto de Acceso

802.11ac Wave 2

El Aironet 4800 extiende la velocidad y las características de 802.11ac a una nueva generación de teléfonos inteligentes, tabletas y computadoras portátiles de alto rendimiento, proporcionando una mejor experiencia para el usuario final. Ya sea que su proyecto implique cambios importantes en su red inalámbrica actual o que actualice sus implementaciones de Wi-Fi heredadas (implementaciones 802.11a/b/g/n/ ac Wave 1), el Aironet 4800 puede encargarse del trabajo. (CISCO, 2020)

El Aironet 4800 es compatible con 802.11ac Wave 2, proporcionando una velocidad de conexión teórica de hasta 5.2 Gbps, que es aproximadamente cuatro veces la velocidad ofrecida por los puntos de acceso 802.11ac de gama alta de la actualidad. El impulso lo ayuda a adelantarse a las expectativas de rendimiento y ancho de banda del trabajador móvil actual, que generalmente usa múltiples dispositivos Wi-Fi en lugar de solo uno. Como tal, los usuarios están agregando cargas de tráfico proporcionalmente más grandes a la LAN inalámbrica, que ha superado a Ethernet como la red de acceso empresarial predeterminada. (CISCO, 2020)

Tabla 8 Evaluación comparativa Cisco Aironet Access Point

EVALUACIÓN COMPARATIVA			
	Aironet 2800 Series	**Aironet 3800 Series**	**Aironet 4800 Series**
Características clave			
Despliegue de destino	Empresas medianas a grandes que requieren funciones avanzadas	Empresas medianas a grandes con tráfico de misión crítica	Grandes organizaciones empresariales con tráfico de misión crítica
Estándares de Wi-Fi	802.11a / b / g / n / acW2	802.11a / b / g / n / acW2	802.11a / b / g / n / acW2
Especificaciones de radio			
Tipo de antena	Interno (2802i); externo (2802e)	Interna, externa y profesional	Interno
Velocidad de datos máxima combinada	5Gbps	5Gbps	5Gbps
Soporte de Ethernet	2 x GE	1 x 5G mGig; 1 x GE	1 x multigigabit; 1 x GE
Clientes máximos	400	400	400
Numero de radios	Dual (XOR y 5 GHz)	Dual (XOR y 5 GHz)	Cuatro (2 x XOR, 5 GHz y BLE)
FlexConnect	si	si	si
Garantía	si	si	si

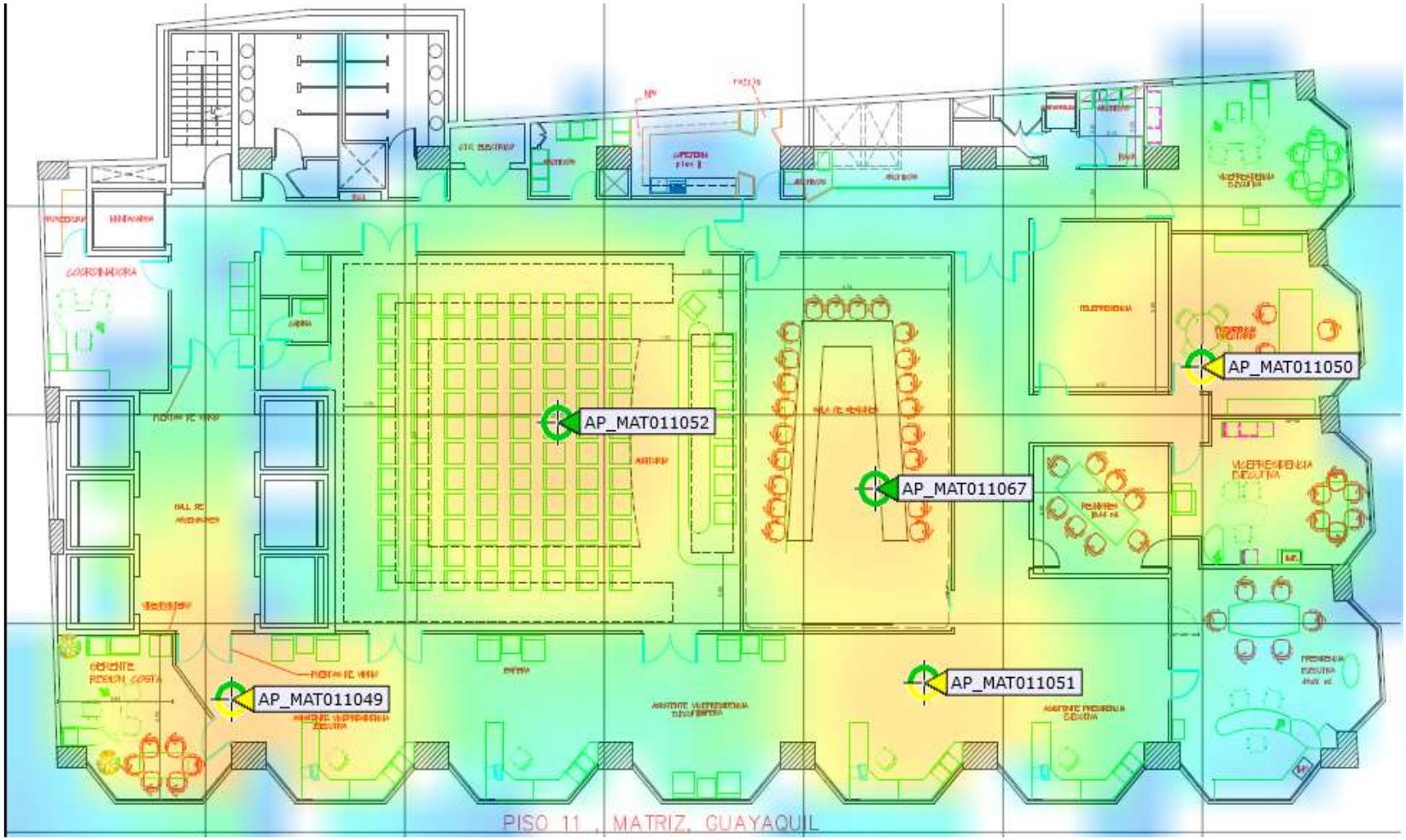


Figura 4. 6 Cisco Aironet Radio Convergente

4.2 Servicios de Identidad (ISE)

Se realiza la configuración de los 2 appliances para que operen en alta disponibilidad y con los roles de Administración, Monitoring y Policy Service Node, ninguno de ellos tiene habilitado el rol de PxGrid.

En las siguientes capturas se puede observar el detalle de la configuración realizada:

Tabla 9 Datos de los Servidores

DATOS DE LOS SERVIDORES			
Hostname	**FQDN**	**IP Address**	**Roles**
ISE Principal	ISE.abcdf.com.ec	10.233.000.00	Administration, monitoring y policy service
ISE Secundario	ISE.abcdf.com.ec	10.233.000.00	Administration, monitoring y policy

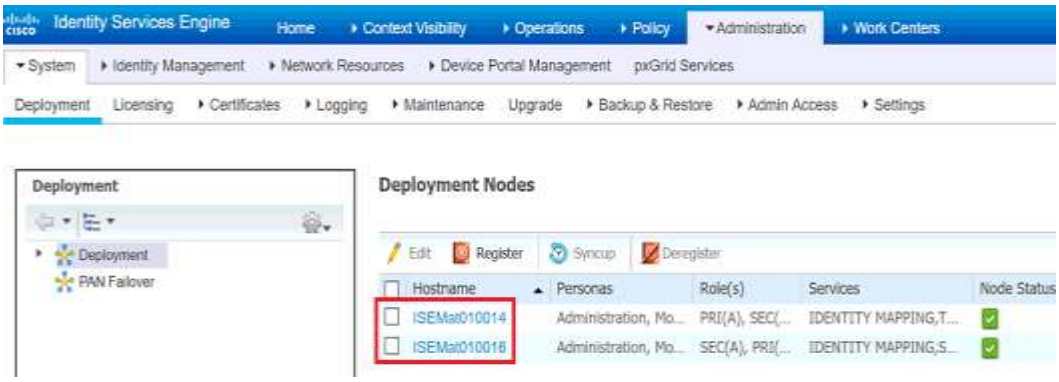


Figura 4. 7 Configuración de los Servidores ISE

4.2.1 Configuración Servidor Secundario con rol Admin, Servicio de políticas, Monitor

Se realiza la configuración del servidor 3515 ISE con los siguientes roles:

- Rol de administración: Secundario, rol de monitor: Primario, rol de políticas de servicios: Secundario.

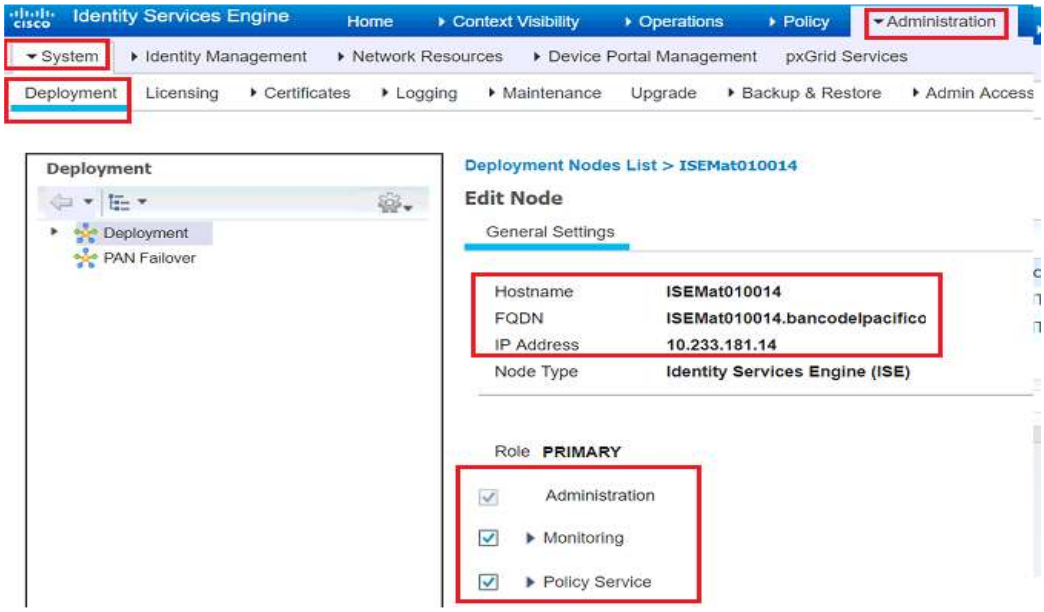


Figura 4. 8 Rol de administración

4.2.2 Configuración de Certificado

Los procedimientos mostrados a continuación se realizaron en ambos nodos o servidores ISE:

1. Administración
2. Sistema
3. Certificados
4. Importar el certificado Trusted.

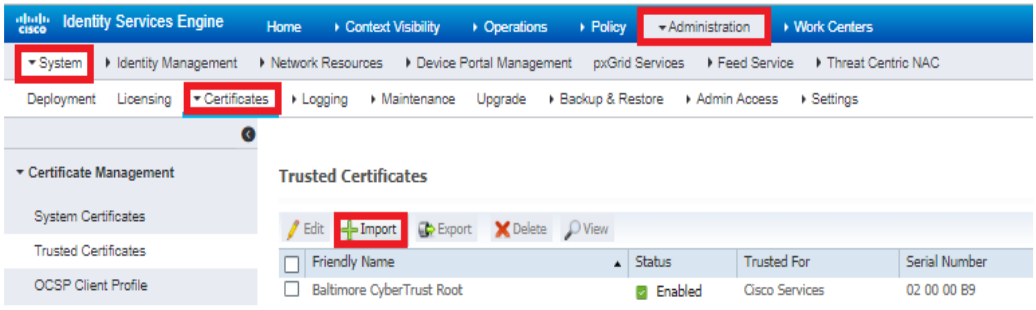


Figura 4. 9 Importar el certificado

Instalar el certificado ROOT. Para evitar advertencias por dominio no seguro, se instalan certificados de una Autoridad Certificadora de carácter Público.

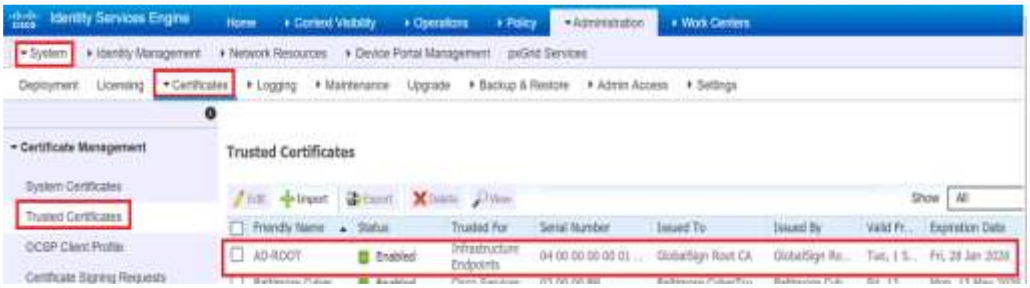


Figura 4. 10 Instalación del certificado ROOT

Para que los nodos puedan operar correctamente con los roles antes indicados, se requiere generar un Certifícate Signing Request o solicitud de firma de certificado.

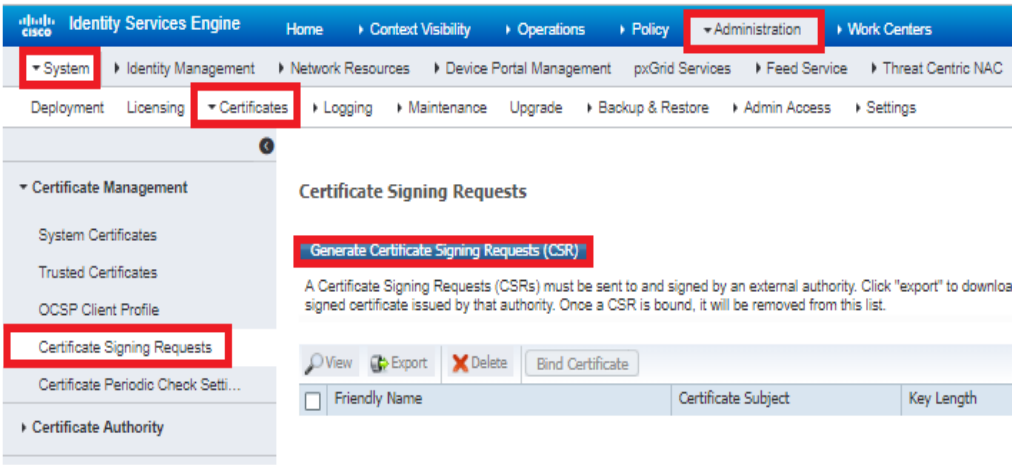


Figura 4. 11 Certificado solicitud de firma

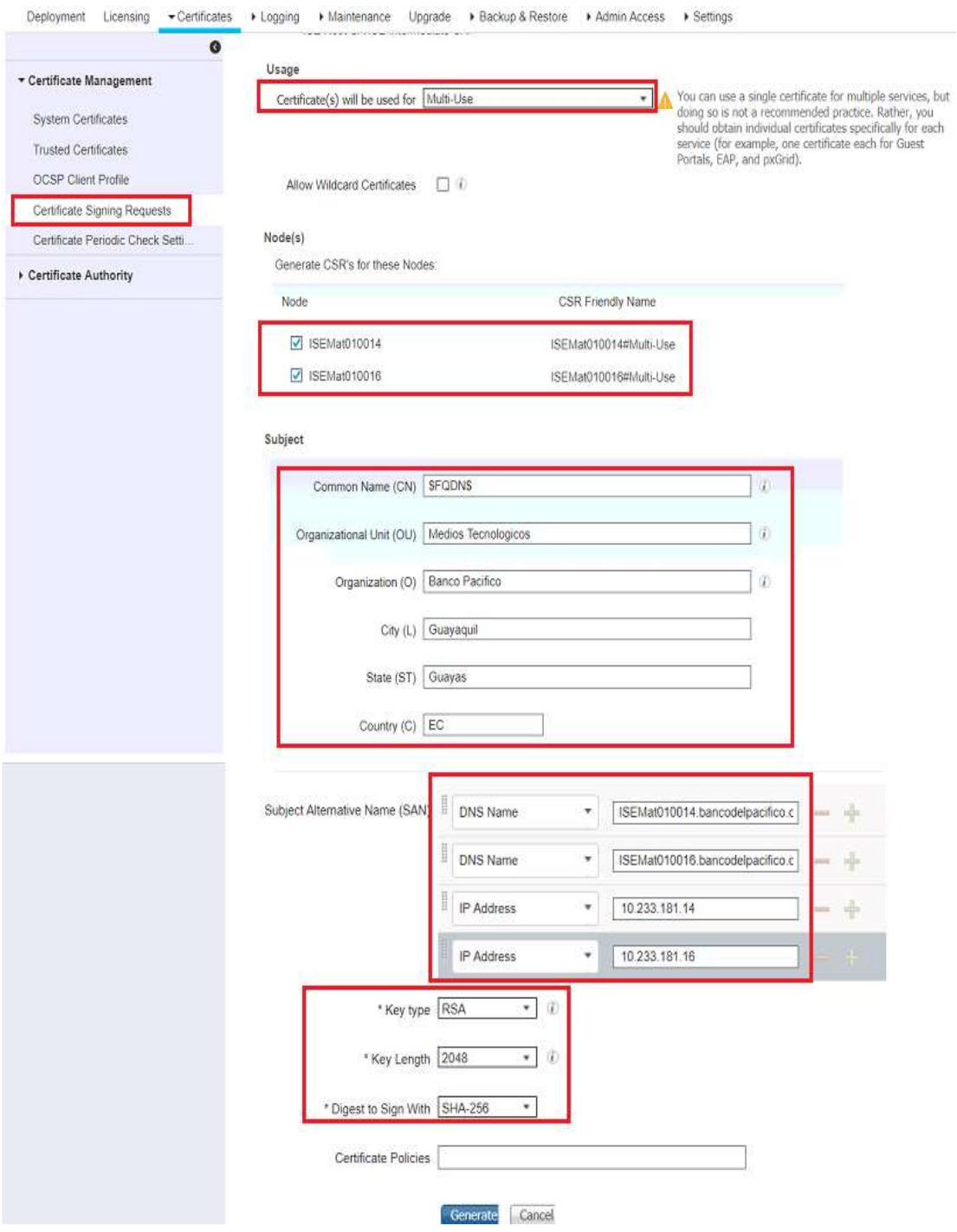


Figura 4. 12 Certificado Solicitud de firma

Se exporta y envía el archivo CSR al administrador de la CA para que sean firmados, posteriormente se realiza el binding instalando el archivo .cer

4.2.3 Configuración de Dispositivos de Red

Se configura el Wireless LAN Controller como parte de los dispositivos de red

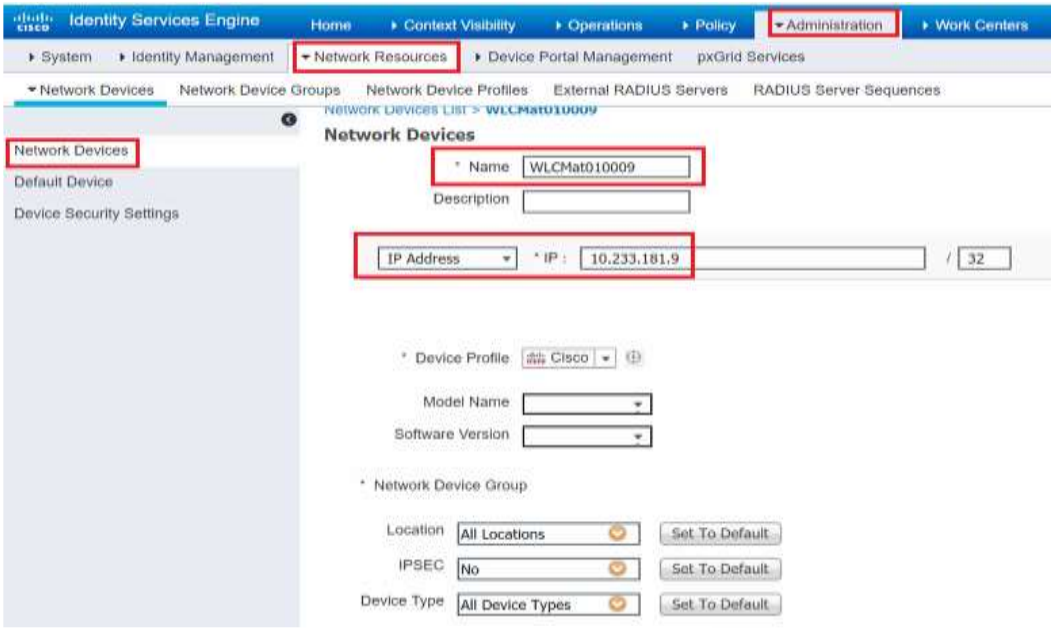


Figura 4. 13 Dispositivos de Red

4.2.4 Configuración para la Integración con el ADFS

De acuerdo con las necesidades de la solución, ya que es una red aislada a la de la entidad financiera no se tiene acceso al directorio activo interno, por lo cual se integra con el ADFS Externo del Banco. A continuación, la configuración realizada para la integración con el ADFS y los grupos definidos.

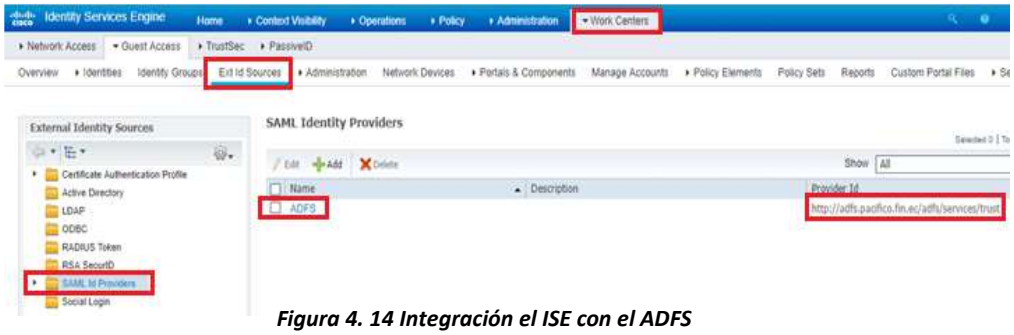


Figura 4. 14 Integración el ISE con el ADFS

Para integrar el ISE con el ADFS Externo, se exporta del ISE el archivo XML a ser instalado en el ADFS, en el consta la información de los portales disponibles, con esto se establece una relación de confianza entre el ISE y el ADFS.

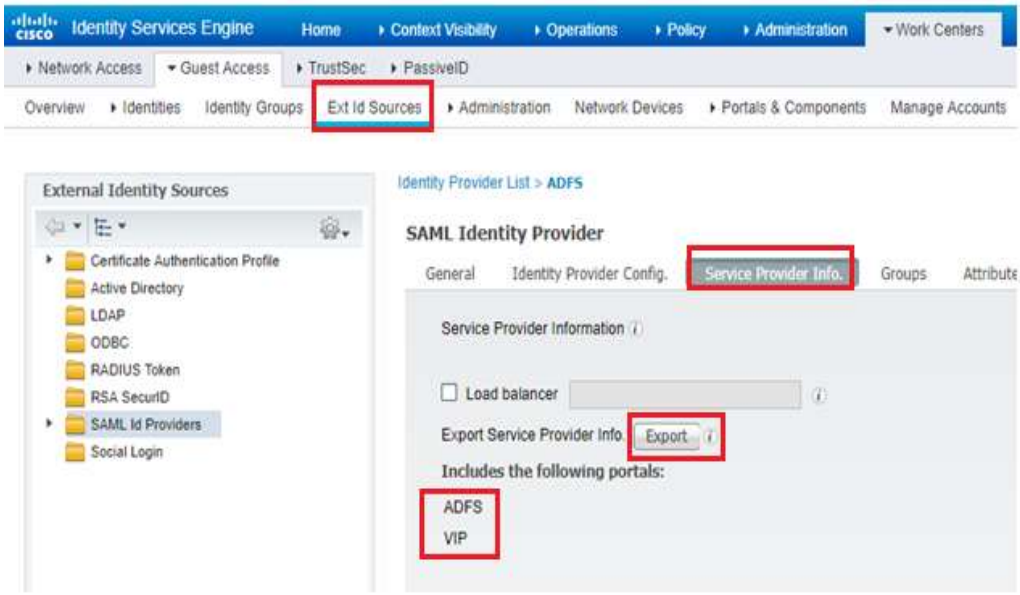


Figura 4. 15 Exportar Archivo XML

Posterior a esto, se crean los grupos con los cuales se trabajará o en este caso los usuarios que se autentificarán por este medio, los grupos definidos, tal como se muestra a continuación son GRP_funcionarios, GRP_FuncionariosVIP y GRP_Externos.

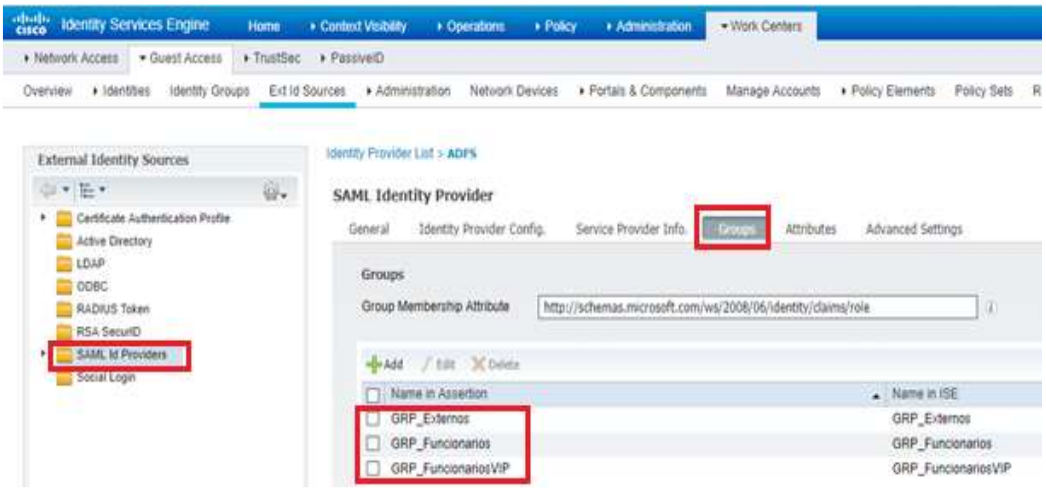


Figura 4. 16 Se crean los grupos en el ISE

4.2.5 Configuración de grupos de identidad de usuarios

La configuración de grupos de identidad de usuarios se lo realiza para identificar la categoría de usuarios que se utilizarán para las diversas solicitudes de acceso a la red.

Se crea el grupo Invitados, en este grupo se mostrarán los usuarios creados para administración del patrocinador para creación de las cuentas de los invitados.

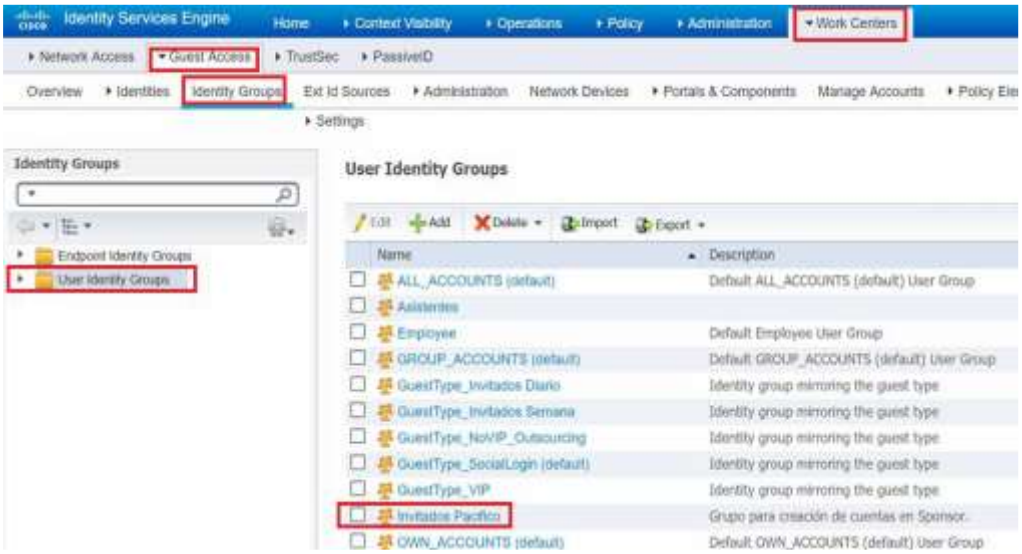


Figura 4. 17 Configuración de grupos de identidad de usuarios

4.2.6 Configuración de Endpoint Identity Groups

La configuración de grupos de identidades de puntos finales se lo realiza para identificar la categoría de dispositivos finales.

En este caso, se tiene en uso 4 grupos que fueron definidos para esta implementación, adicionalmente al grupo GuestEndpoints predefinido.

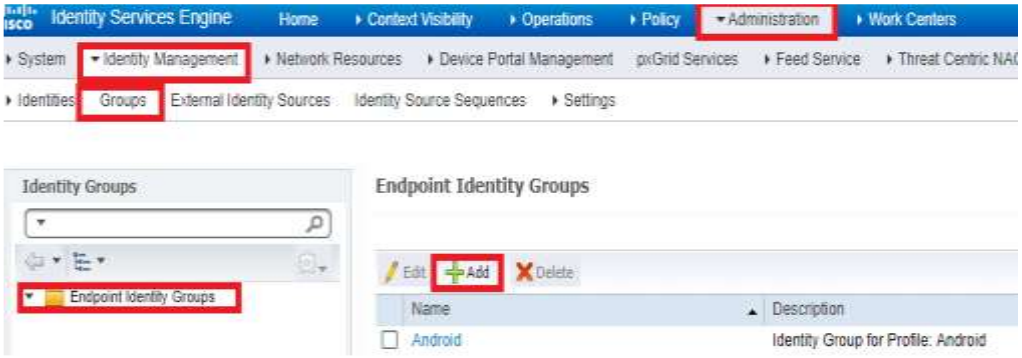


Figura 4. 18 Grupo

Los grupos creados para la solución son Externos, Funcionarios_VIP, Funcionarios_no_VIP y TV_Printers, en los cuales se registrarán el Mac de los dispositivos en los cuales se ingresen credenciales de ADFS válidas. En el grupo TV_Printers se registrarán manualmente las MAC de impresoras y televisores que no sean compatibles con el uso de un portal cautivo para autentificar.

Para agregar la MAC de un dispositivo a alguno de los grupos, se realiza lo siguiente:

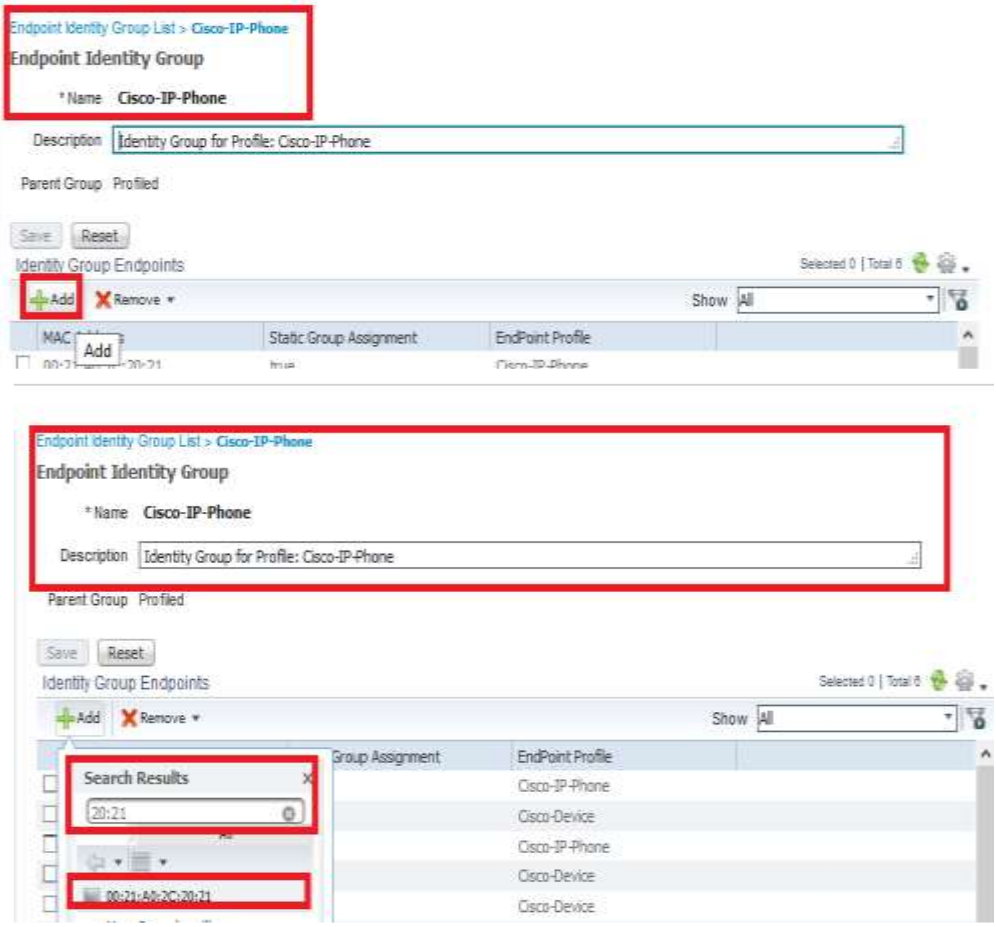


Figura 4. 19 Agregar la MAC de un dispositivo a alguno de los grupos

Figura 4. 20 Agregar la MAC de un dispositivo a alguno de los grupos

4.2.7 Configuración de Políticas de Autentificación

Dado que la red es únicamente inalámbrica, se manejan políticas de autentificación inalámbrica.

Las políticas de autorización son las encargadas de dar permisos a los equipos a diferentes roles como el caso de la asignación a un VLAN, dichas políticas están basadas en condiciones y permisos. Para cada red tiene una política de autorización como se indica en la siguiente pantalla.

En este caso se manejan políticas para Funcionarios VIP, Funcionarios no VIP e Invitados Pacífico y dependiendo de la política con la que se valide, se asignará la IP de la VLAN correspondiente.

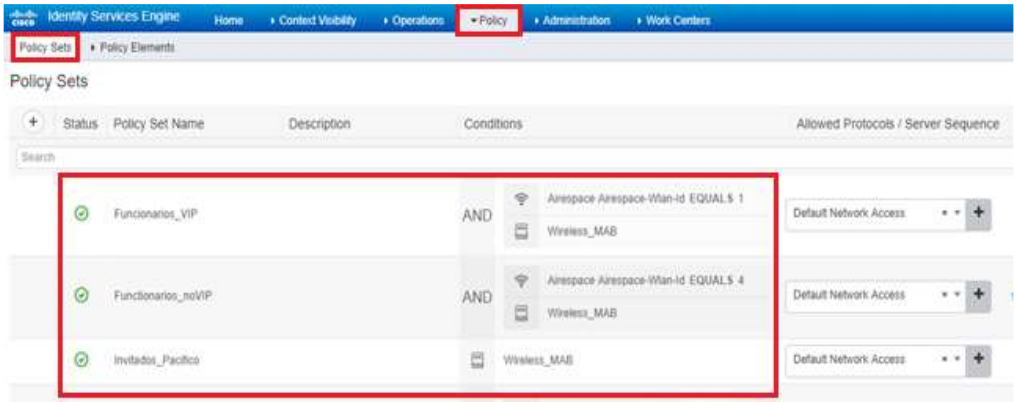


Figura 4. 21 Configuración de Políticas de Autentificación

4.2.8 Configuración del Portal Web

Se crean portales para la autentificación de los usuarios, estos portales se pueden modificar.

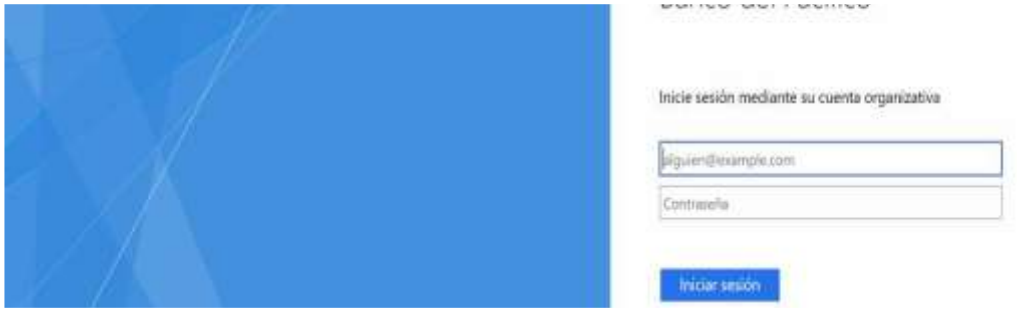


Figura 4. 22 Portal Web

4.2.9 Portal de Invitados Externos

Este portal se utiliza para invitados externos inician sesión.

Figura 4. 23 Portal de Invitados Externo

4.2.10 Licenciamiento

El ISE cuenta con licenciamiento Base, tiene disponibilidad para 4000 usuarios y las licencias son permanentes.

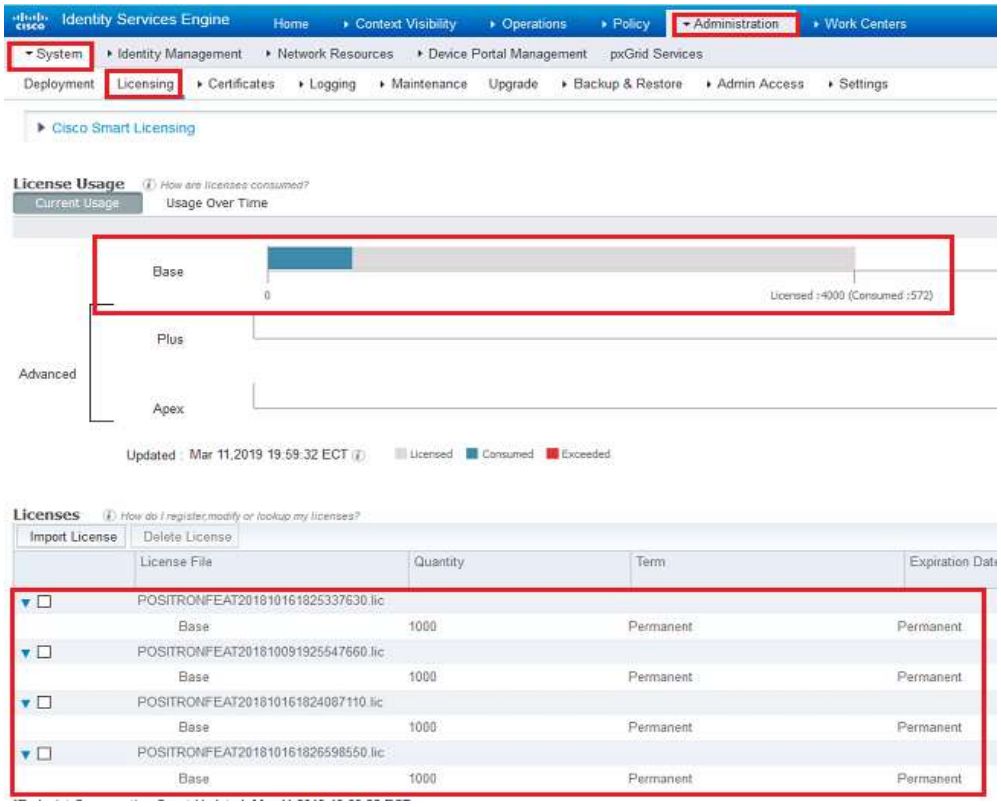


Figura 4. 24 Licenciamiento

4.3 Controlador Lan Inalámbrico (WLC)

Se instalan 2 Wireless LAN Controller en alta disponibilidad.

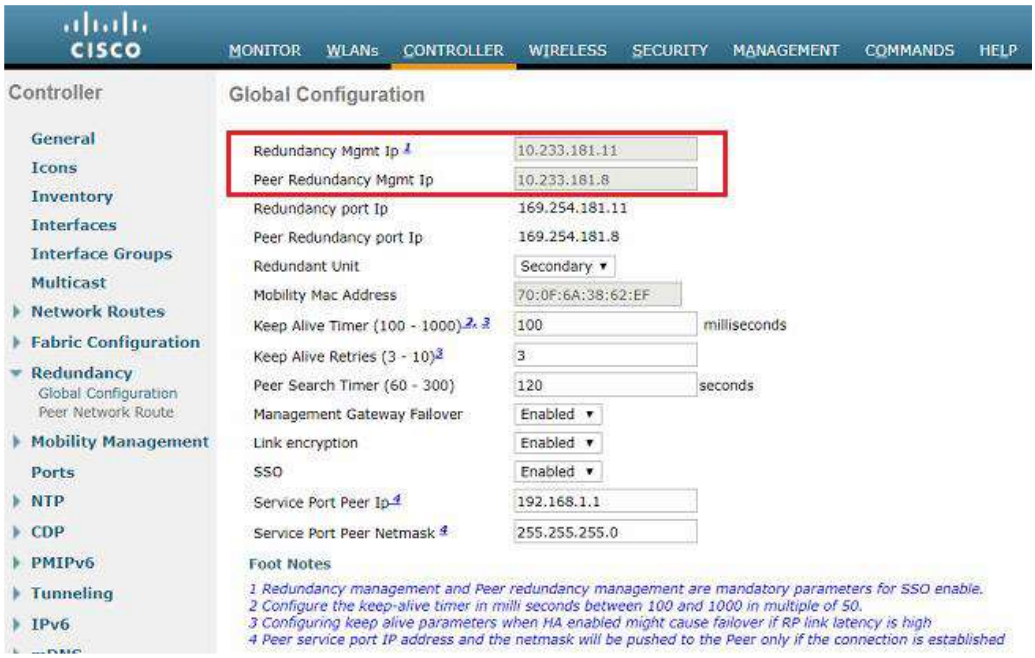


Figura 4. 25 Wireless LAN Controller en alta disponibilidad

4.3.1 Configuración de Radius (Authentication y Accounting)

Se configuran los ISE como servidores radio para autenticación y registro.

Figura 4. 26 Configuración de Radio

4.3.2 Interfaces Inalámbrico

Se tienen definidas las interfaces según el direccionamiento establecido.

Tabla 10 Interfaces Inalámbricas

INTERFACES INALÁMBRICA				
SSID	**VLAN ID**	**NAME**	**RED**	**PUERTA DE ENLACE**
N/A	000	Administración inalámbrica	10.233.000.0/00	000
Funcionarios	000	GYE Principal Funcionarios	10.233.000.0/00	000
Funcionarios VIP	000	GYE Principal VIP	10.233.000.0/00	000
Invitados	000	GYE Principal Invitados	10.233.000.0/00	000
Clientes	000	GYE Principal Clientes	10.233.000.0/00	000

El direccionamiento indicado anteriormente está siendo utilizado por los edificios de Matriz, Anexo, en las otras agencias y sucursales se maneja otro direccionamiento por VLAN.

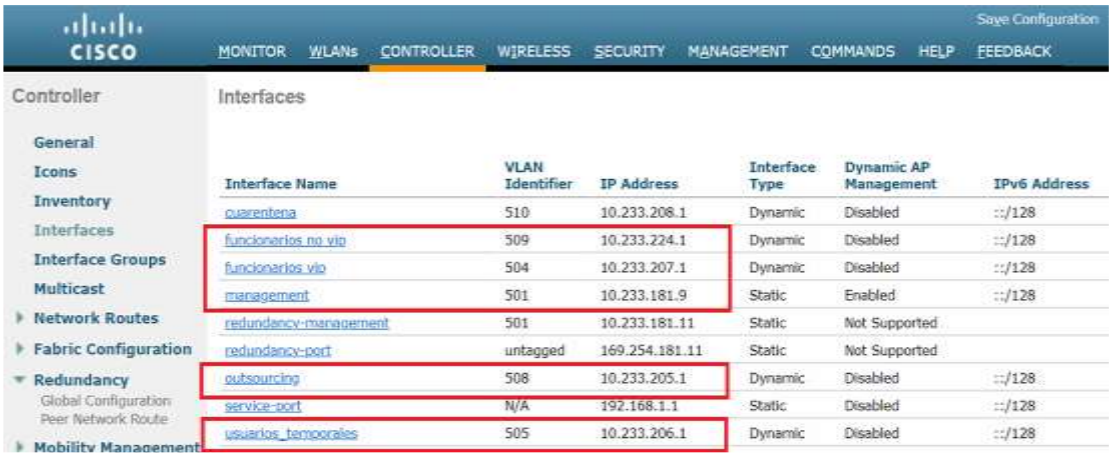


Figura 4. 27 Interfaces Inalámbricas

4.3.3 FlexConnect

FlexConnect es una solución inalámbrica para implementaciones de sucursales y oficinas remotas. Le permite configurar y controlar los puntos de acceso en una sucursal u oficina remota desde la oficina corporativa a través de un enlace WAN sin el despliegue de un controlador en cada oficina.

4.3.4 Configuración de WLAN

Se crearon los siguientes SSID, los mismos que están asociados a las interfaces indicadas en el punto anterior.

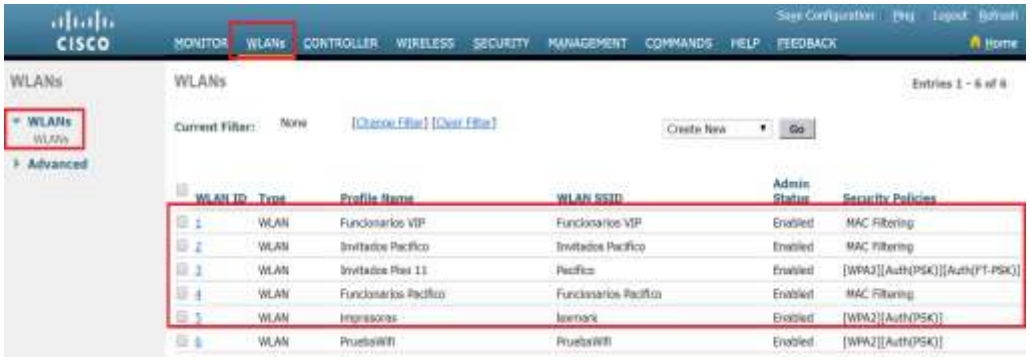


Figura 4. 28 Configuración de WLAN

Funcionarios VIP

Este SSID será utilizado por los Funcionarios VIP, el flujo definido para esta red indica que posterior a que un Endpoint se conecte a este SSID deberá saltar un portal para autenticarse en la red, si el usuario ingresado cumple con el requisito de pertenecer al grupo, hará un cambio de IP, de la VLAN de cuarentena a la VLAN asignada para los funcionarios VIP.

La interfaz utilizada es la de cuarentena, en la cual el dispositivo no tendrá acceso libre a la red, si no únicamente tendrá conectividad al ADFS, DHCP, DNS y servidores de identidad.

Como seguridad de capa 2 tiene las Mac se filtran y se definen los servidores tanto de registro como de autentificación.

Funcionarios

Este SSID será utilizado por los Funcionarios de banco y por personal outsourcing, el flujo definido para esta red indica que posterior a que un Endpoint se conecte a este SSID deberá saltar un portal para autenticarse en la red, si el usuario ingresado cumple con el requisito de pertenecer al grupo de funcionarios o de outsourcing, hará un cambio de IP, de la VLAN de cuarentena a la VLAN asignada al grupo perteneciente.

La interfaz utilizada es la de cuarentena, en la cual el dispositivo no tendrá acceso libre a la red, si no únicamente tendrá conectividad al ADFS, DHCP, DNS y servidores de identidad.

Como seguridad de capa 2 tiene las Mac se filtran y se definen los servidores tanto de registro como de autentificación.

Invitados

Este SSID será utilizado por los Invitados, el flujo definido para esta red indica que posterior a que un Endpoint se conecte a este SSID deberá saltar un portal para autenticarse en la red previo registro, si las credenciales ingresadas son correctas, tendrá acceso a la red.

La interfaz utilizada es la de usuarios temporales, previo al ingreso de credenciales el dispositivo no tendrá acceso libre a la red, si no únicamente tendrá conectividad al ADFS, DHCP, DNS y servidores de identidad. Posterior a la autentificación, se garantizará el acceso a la red, excepto a la VLAN de administración.

Como seguridad de capa 2 tiene las Mac se filtran y se definen los servidores tanto de registro como de autentificación.

Impresoras

Este SSID será utilizado para la conexión de las impresoras del área de innovación del edificio. Esta red utiliza la interfaz de outsourcing.

4.4 Reportería (Prime)

4.4.1 Reportería

Se crearon trabajos o Jobs para ser ejecutados automáticamente por el Prime, a continuación, el detalle de estos. Estos reportes se obtendrán semanalmente el sábado.

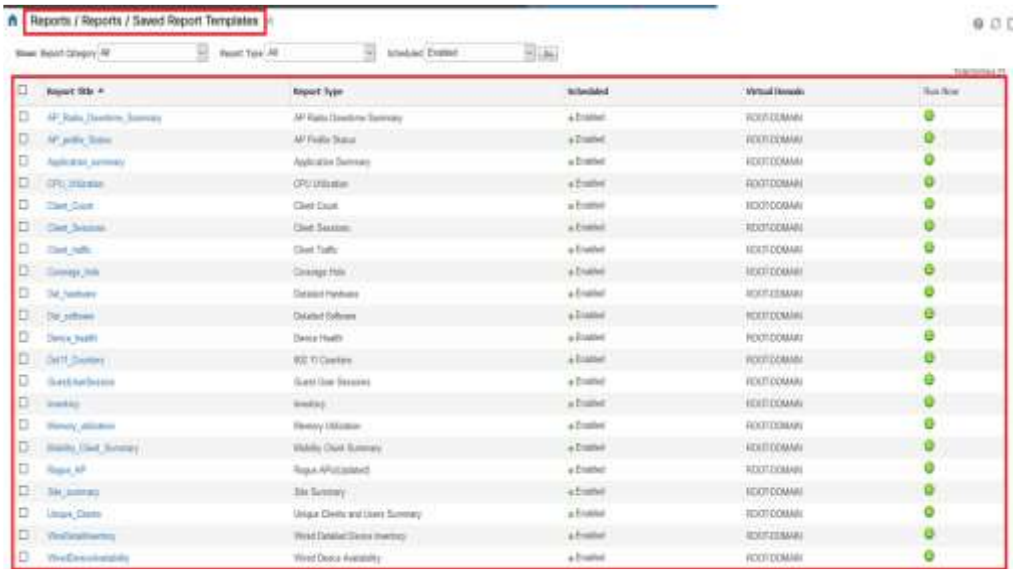


Figura 4. 29 Reportería (PRIME)

4.4.2 Licenciamiento

Actualmente el Cisco Prime Infraestructure cuenta con el siguiente licenciamiento.

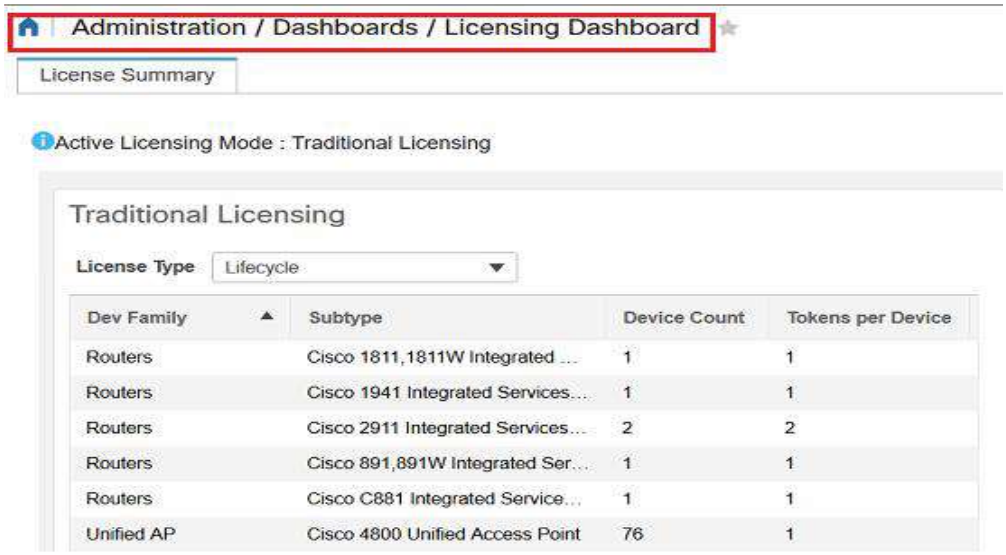


Figura 4. 30 Licenciamiento PRIME

CAPÍTULO 5

ANÁLISIS Y DISEÑO DE LA SOLUCIÓN CLIENTES

En esta solución de monetización Wi-Fi de Alepo nos permitirá administrar con eficacia modelos de negocio basados en redes Wi-Fi de acceso público con compatibilidad con equipos cisco. La solución se compone de varias herramientas (enumeradas a continuación) para permitir un modelo de negocio verdaderamente granular y extensible.

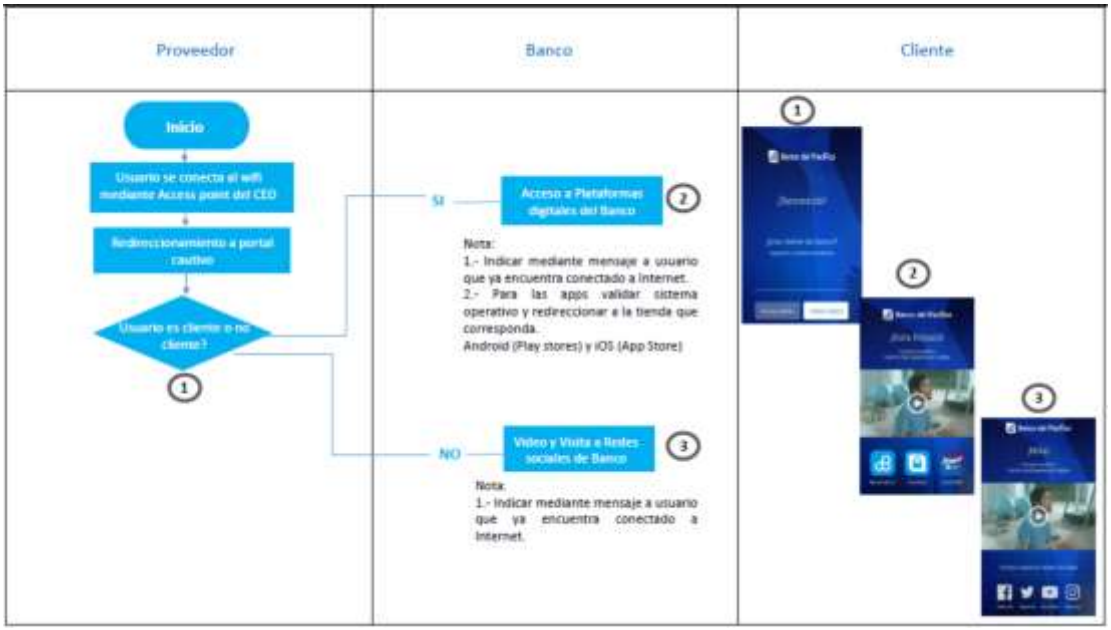


Figura 5. 1 Evaluación comparativa del Proveedor Alepo - Banco - Cliente

4.5 Detalle de la Solución de Software Alepo

Alepo hace realidad las oportunidades de datos de próxima generación. Sus soluciones y servicios avanzados de software permiten a los proveedores de servicios de comunicaciones globales acelerar el crecimiento de los ingresos, la participación en el mercado y el éxito comercial en las redes de banda ancha fija y móvil de próxima generación. Durante más de una década, Alepo ha sido el socio tecnológico de "todos los datos" en proveedores de servicios líderes como Orange, Saudi Telecom y Digicel. (Alepo, S.F.)

A medida que el mundo conectado se acerca a la masa crítica, Alepo imagina proveedores de servicios de comunicaciones delgados que están facultados para:

- Dar la bienvenida a las tecnologías disruptivas con la disposición y la agilidad para aprovechar nuevas oportunidades.
- Orquestar la experiencia del cliente en medio de una ráfaga de terceros, contenido y socios OTT.
- Crecer, adaptarse y evolucionar con la garantía de un rendimiento de red y una velocidad inquebrantables. (Alepo, S.F.)

Su innovación continua abarca políticas avanzadas y control de cobro, cobro y facturación convergentes, administración de dispositivos, BSS / OSS, monetización de puntos de acceso Wi-Fi, descarga de Wi-Fi, infraestructura AAA y más. Alepo ofrece servicios profesionales expertos: integración de sistemas, consultoría y diseño, capacitación y soporte, servicios administrados y más. (Alepo, S.F.)

La solución de monetización Wi-Fi de Alepo permitirá administrar con eficacia modelos de negocio basados en redes Wi-Fi de acceso público. La solución se compone de varias herramientas (enumeradas a

continuación) para permitir un modelo de negocio verdaderamente granular y extensible. (Alepo, S.F.)

La solución de ALEPO cuenta con 3 módulos, portal cautivo, servidor AAA y AAA EMS. (Alepo, S.F.)

4.5.1 Portal Cautivo de Alepo

El Portal Cautivo de Alepo da vida a la funcionalidad completa de la solución, lo que permite un proceso de ingreso rápido e intuitivo para todos los clientes. Cualquier cliente puede ingresar a través del diligenciamiento de un formulario o viendo un video publicitario. Además, el portal se puede personalizar fácilmente para imitar la apariencia del portal existente del banco, y sirve como una poderosa herramienta de marketing. (Alepo, S.F.)

El conjunto de características principales incluye:

- Portal cautivo avanzado basado en una arquitectura basada en complementos moderna con un conjunto de características extensible.
- La plataforma proporciona casos de uso listos para usar y pre-integrados para un tiempo de publicación más rápido.
- Fácil configuración basada en “arrastrar y soltar” para la creación de páginas en el portal.
- Portal cautivo para dispositivos móviles que se dimensiona automáticamente.
- Biblioteca disponible con plantillas de diseño de página predefinidas para elegir. (Alepo, S.F.)

Diagrama General SSDI

En el siguiente diagrama se puede visualizar la arquitectura de forma general de cómo el usuario tiene acceso a la red inalámbrica cuando es cliente o no es cliente de la entidad financiera.

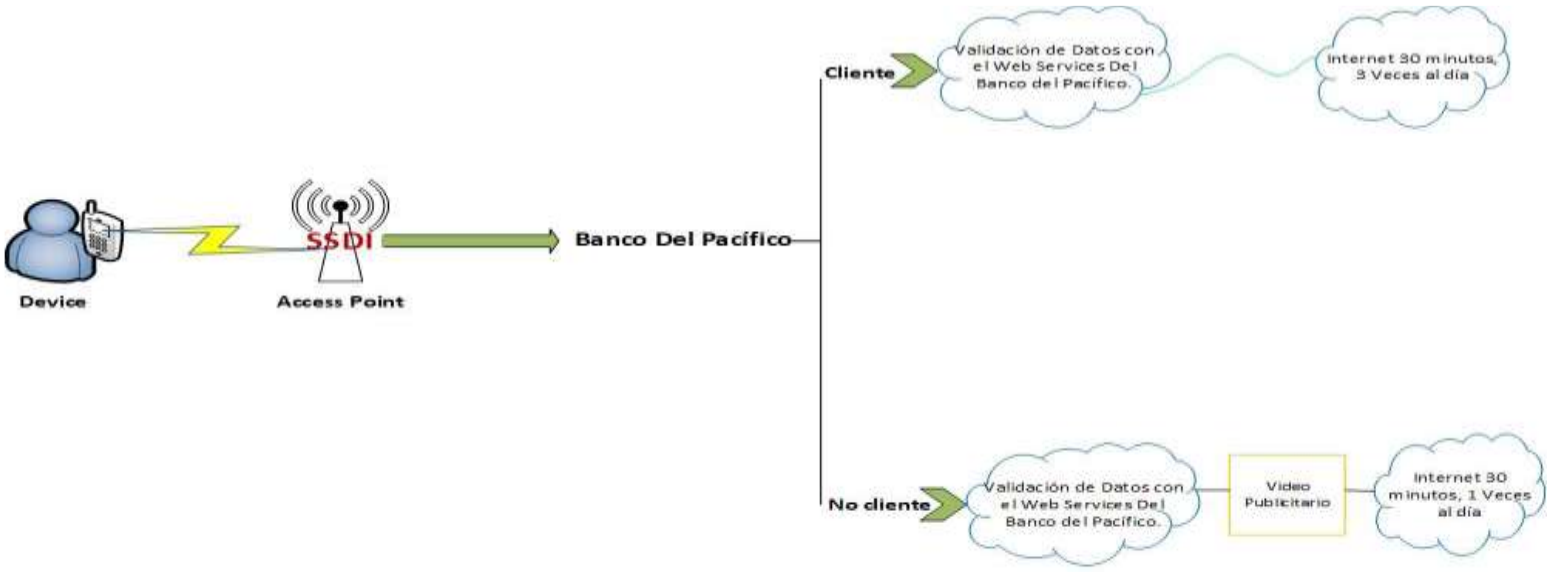


Figura 5. 2 Diagrama General SSDI

El usuario se conecta al SSDI Banco, una vez conectado, aparecerá el portal cautivo de Alepo dónde el usuario pondrá su número de cedula, ruc o pasaporte donde esos datos serán validados con el Web Services del Banco, para ver si es cliente o no es cliente.

Si el Usuario es cliente, se le dará internet por 30 minutos y con posibilidad de conectarse 3 veces en el día.

Si el Usuario no es cliente, le aparecerá un video publicitario del Banco, una vez reproducido el vídeo, podrá conectarse por 30 minutos, conectándose 1 vez al día.

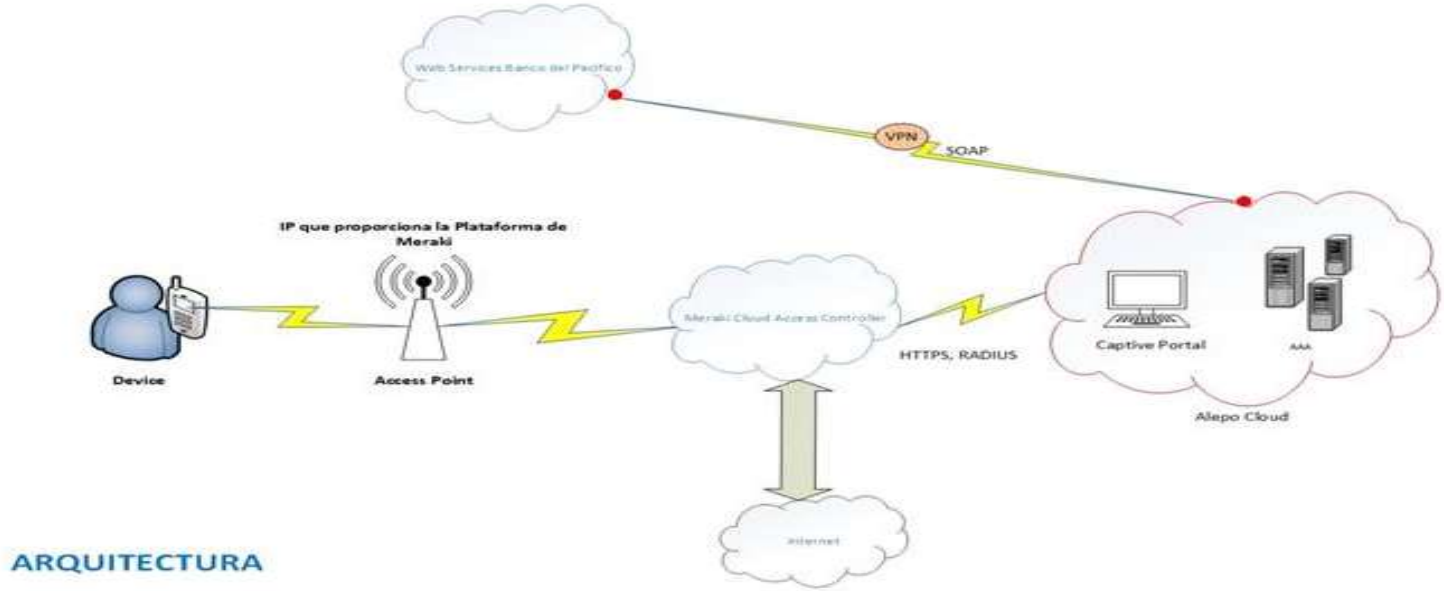


Figura 5. 3 Diagrama de Conexión

Diagrama de Conexión y Consultas al Banco

En el siguiente diagrama se puede visualizar la arquitectura de cómo el usuario tiene acceso a la red inalámbrica.

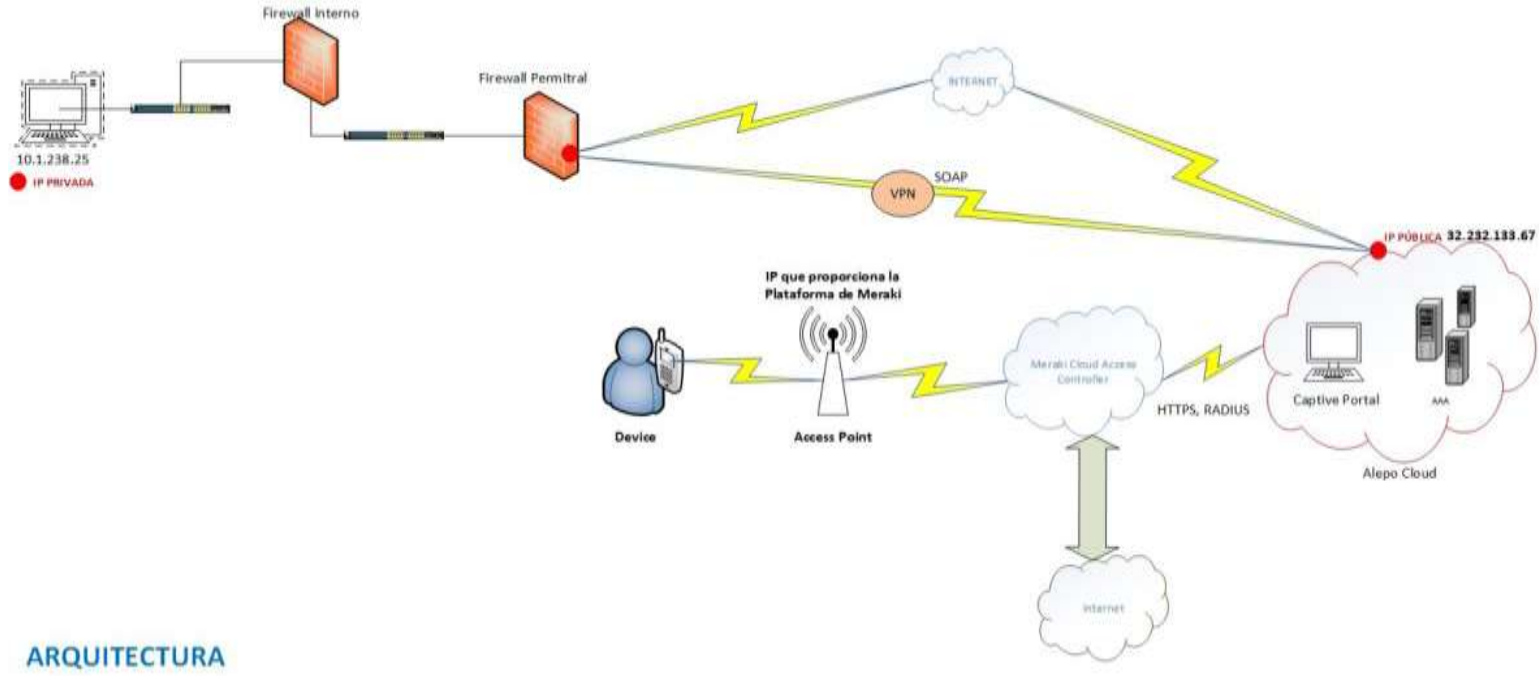


Figura 5. 4 Consultas al Banco

- El usuario se conecta al Access Point de Cisco, hace una conexión a la Nube de Meraki, dónde se le proporcionará una IP aleatoria propia de la plataforma de Meraki.
- La conexión entre la nube de Meraki y la nube de Alepo, está certificado con seguridad HTTPS, y se puede conectar también mediante un servidor radio.
- Esta conexión se la hace por un servidor radios con el siguiente host y puerto:
- Se conecta a la nube de Alepo donde está configurado el Portal Cautivo, este hace una consulta al Web Services del Banco donde se valida los datos del cliente.
- Esta consulta se la hace mediante una VPN.
- Estos datos son consultados y presentados.
- Ninguna información del Usuario queda guardada en la nube.
- Devolvemos estos datos, se valida el usuario si es cliente o no, y se le proporciona acceso al internet. (Diagrama General).

Acceso a la red inalámbrica para las IPADS

Como solución de la conexión inalámbrica para los dispositivos (iPads) que van a estar en la “Sucursal del Futuro”, se va a crear una credencial de dominio (SFuturo@abcdf.fin.ec) donde se van a poder conectar todos los iPads.

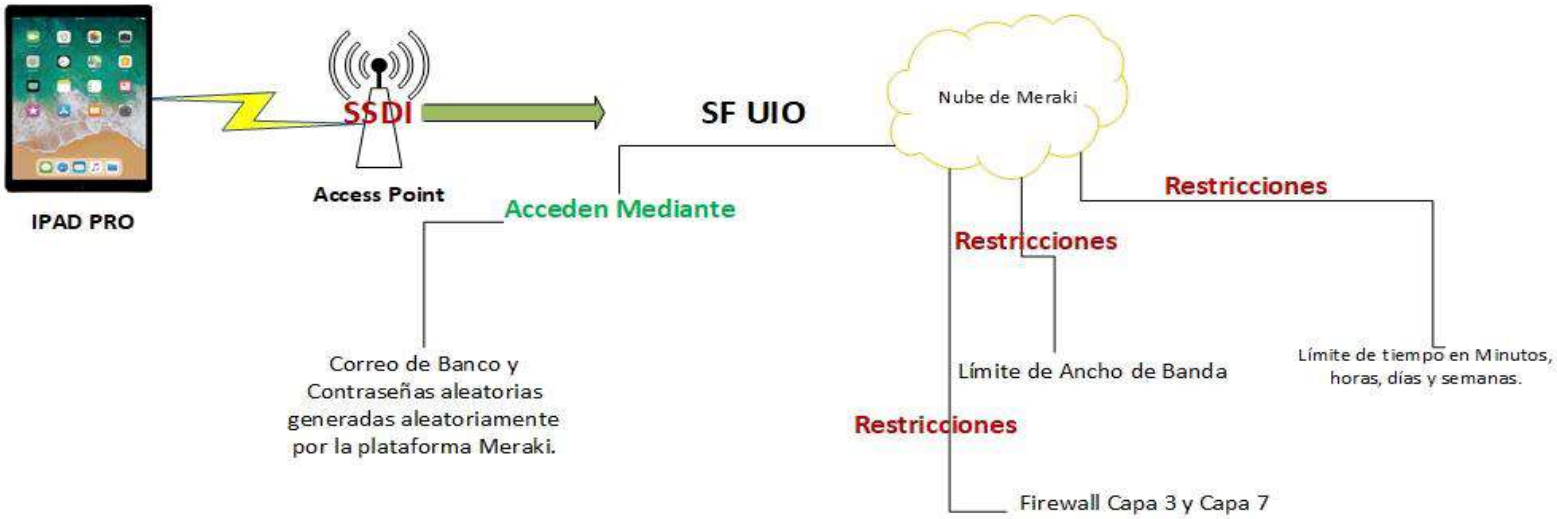


Figura 5. 5 Acceso Red Inalámbrico en las IPADS

4.5.2 Servidor AAA

El servidor AAA de Alepo funciona con elementos de red para autenticación de servicios, autorización, contabilidad y control de puerta de enlace. (Alepo, S.F.)

Especificaciones

1. Admite la redirección de un usuario a un portal cautivo en lugar de rechazar una solicitud de acceso.
2. Admite el envío de una copia del paquete de contabilidad RADIUS a uno o varios destinos RADIUS. Basándose en el destino los mensajes de contabilidad se pueden modificar (agregar / actualizar / eliminar) antes de enviar la copia de la solicitud de contabilidad.
3. Admite el envío de paquetes de Autenticación RADIUS y / o Contabilidad RADIUS a un servidor AAA asociado. Opcionalmente, los paquetes de contabilidad reenviados se pueden almacenar localmente en Alepo AAA CDR Store.
4. Admite el almacenamiento de datos de la sesión RADIUS con la información de uso
5. Admite el registro de todas las solicitudes de autenticación, todos los rechazos o rechazos específicos enviados.
6. Incluye un motor de scripting de alto rendimiento que le permite escribir e implementar reglas personalizadas de autenticación / autorización internamente y ejecutarlas sin tener que volver a compilar o "ensuciar" el código fuente.
7. Admite contadores Alepo SNMP personalizados para la aplicación RADIUS que se pueden interconectar con cualquier sistema de gestión basado en SNMP para monitorizar los parámetros de la aplicación AAA.

8. Admite las siguientes bases de datos
    - MySQL
    - Oracle
    - LDAP como base de datos de autenticación (Alepo, S.F.)

4.5.3 AAA EMS

Alepo EMS Portal es la interfaz para el sistema AAA que permite a los administradores del sistema obtener acceso al sistema para las configuraciones AAA y la gestión diaria de los suscriptores. (Alepo, S.F.)

Especificaciones

1. Soporta la gestión del suscriptor AAA.
2. Soporta interfaz basada en web para ver las sesiones en línea RADIUS y CDR.
3. Soporta una interfaz basada en web para gestionar y configurar el Alepo AAA.
4. Soporta configuración de NAS basada en web.
5. Soporta la configuración de IPs para grupos.
6. Soporta perfiles de acceso y la configuración de políticas de restricciones para un grupo de usuarios AAA. (Alepo, S.F.)

4.5.4 Sistema de Gestión de Contenidos (CMS)

El CMS de Alepo permite la creación de páginas de Portal cautivo a través del poderoso Divi Builder en WordPress. Literalmente convierte la pantalla en un lienzo organizado en bloques, y cualquier elemento que desee agregar a su página se puede agregar en la alineación que elija.

- Centraliza todas las operaciones en una sola plataforma
- El diseñador de páginas de arrastrar y soltar ofrece flexibilidad para modificar el portal cautivo y reduce el tiempo de comercialización

- Proporciona una biblioteca de plantillas de portal cautivo con casos de uso preconfigurados para que los operadores satisfagan las necesidades del mercado
- Asociar páginas con ubicaciones para proporcionar ofertas basadas en la ubicación y anuncios alineados con la marca del operador
- Informes y análisis: integración con Google Analytics
- Estilo personalizable que satisface los requisitos de afiliados con complementos y temas adicionales con la ayuda de la tecnología de WordPress.
- Permite a los operadores personalizar el portal de acuerdo con sus necesidades de marketing con menos tiempo de comercialización. Reutilice plantillas existentes o cree diseños personalizados utilizando el generador de páginas Divi.
- Cree su página personalizada con texto enriquecido, videos, campos de formulario enriquecido, código personalizado.
- Agregue contenido de marca en pocos clics, active los servicios y las ofertas de implementación.
- Reducción de errores al modificar la configuración.
- Los módulos de arrastrar y soltar ofrecen simplicidad en la modificación de las plantillas de portal cautivas

Permite crear ofertas personalizadas y categorizarlas para que estén disponibles para portales cautivos selectivos o por ubicaciones

4.6 Redundancia para Sistemas Alepo

4.6.1 Alepo Portal Cautivo

Alepo configurará el balanceador de carga para lograr alta disponibilidad para Portales cautivos Alepo.

4.6.2 AAA Redundancia

Alepo tendrá 2 nodos de AAA que se conectarán al Controlador de acceso de Cisco Meraki en arquitectura Activo - Standby. Dado que el tráfico a AAA se rige por el controlador de acceso Cisco Meraki, este debe configurarse para el balanceo de carga entre nodos AAA. Es decir, cuando un servidor AAA Activo este fuera de servicio, el controlador de acceso Cisco Meraki debe desviar el tráfico hacia el servidor AAA Standby. El equipo Alepo puede estar disponible para realizar pruebas de redundancia para Alepo AAA.

4.6.3 Redundancia del EMS

Alepo tendrá 2 nodos para AAA EMS. Alepo si configurará estos nodos en el software balanceador de carga.

4.6.4 Redundancia de la Base de Datos

Alepo configurará la replicación de MySQL entre los dos nodos de la base de datos Alepo.

Criterios de Aceptación

Dados al menos dos servidores de bases de datos configurados en modo de redundancia, el sistema podrá acceder a la base de datos en cuestión de minutos después de desconectar cualquiera de los servidores de bases de datos de la red.

4.7 Detalle de la Solución Hardware

4.7.1 Descripción de la Instalación

Cisco Meraki lleva la simplicidad de gestión a los puntos de acceso inalámbricos, Switch’s y dispositivos de seguridad gestionándolos de

Figura 5. 6 Cisco Meraki Punto de Acceso AP MR42

forma centralizada desde la nube. Además, ofrece a los administradores de red la visibilidad y el control que necesitan, sin el coste ni la complejidad de las arquitecturas de red tradicionales. (Cisco Meraki, 2018)

4.7.2 Diagrama de red de la Infraestructura

La siguiente arquitectura funcional proporciona una descripción general de la plataforma Wifi Cloud de Alepo, incluidas las interfaces con otros sistemas.

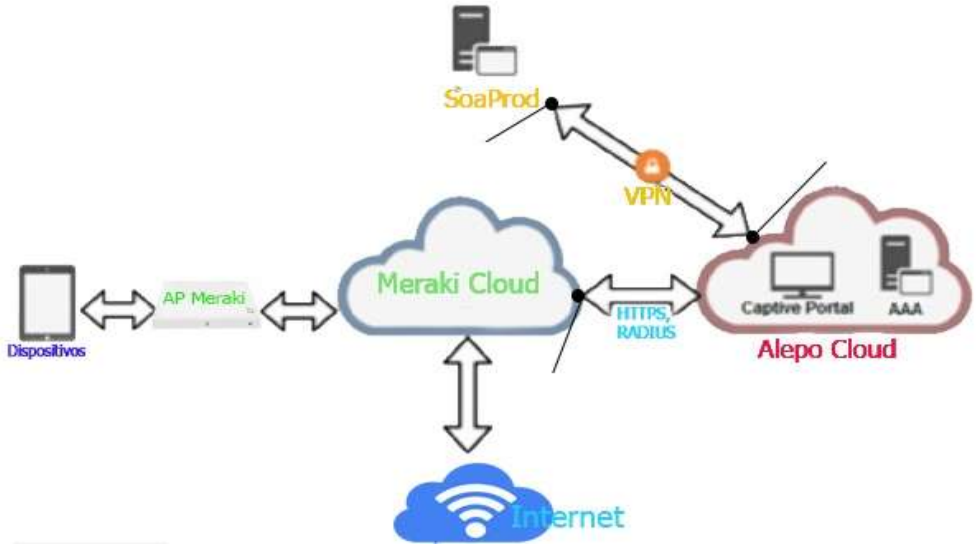


Figura 5. 7 Descripción general de la arquitectura de la solución Wi-Fi Cloud (Cliente - Banco)

Red e Integración

Propuesta de arquitectura de alto nivel:

Figura 5. 8 Alepo AAA y Plataforma de Portal Cautivo

4.7.3 Detalle de la configuración de equipos instalados

Para la visualización o administración de la plataforma inalámbrica, se debe acceder al menú Meraki, este paso se lo puede realizar mediante el siguiente enlace.

https://account.meraki.com/login/dashboard_login

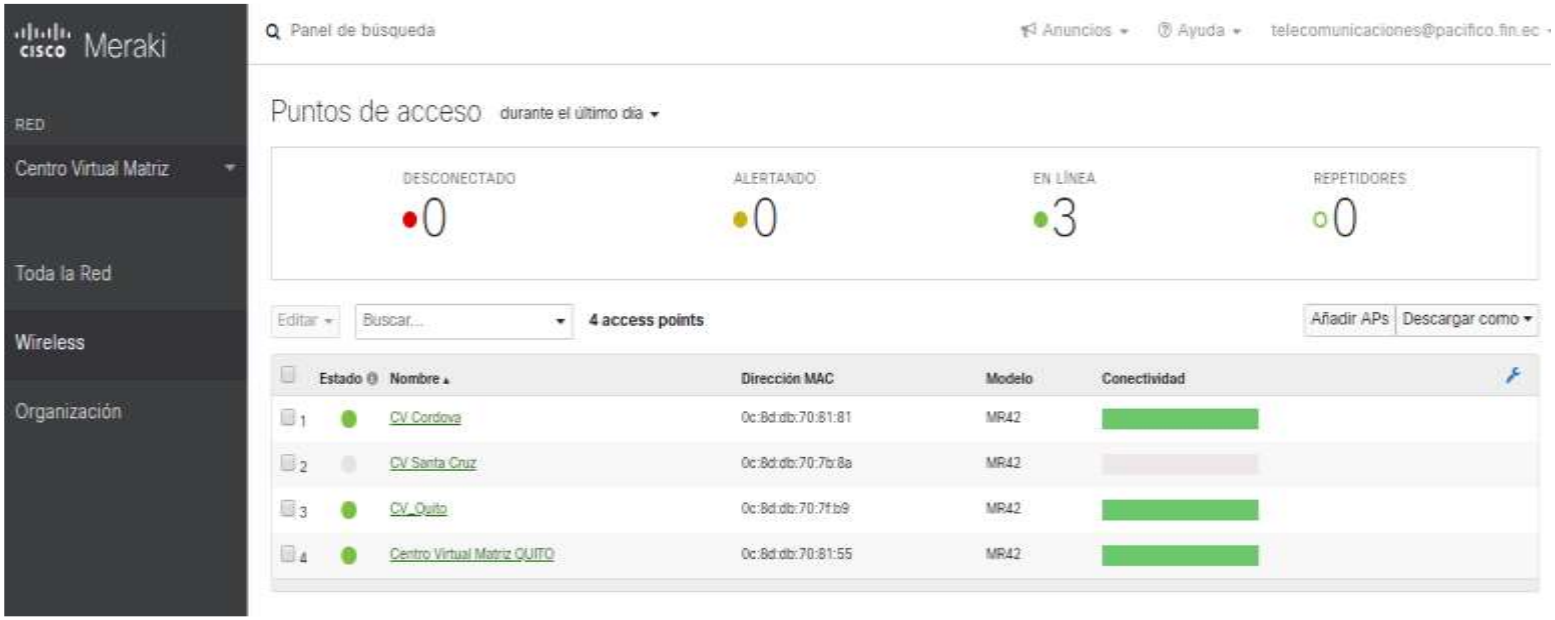


Figura 5. 9 Ventana Meraki

4.7.4 Uso de Funcionalidades de Meraki

Rendimiento

El Dashboard ofrece una amplia variedad de formas de recopilar información sobre la red inalámbrica. A través de Live Tools y el registro de eventos, los administradores de red pueden rastrear un dispositivo específico, sus movimientos y el estado 802.11. (Cisco Meraki, 2018)

Todos los productos de Cisco Meraki tienen un gráfico de conectividad que puede abarcar horas, días y semanas, lo que permite detectar rápidamente interrupciones o cualquier cambio en el estado del dispositivo, también es posible monitorear los usuarios que se han conectado a la red. (Cisco Meraki, 2018).

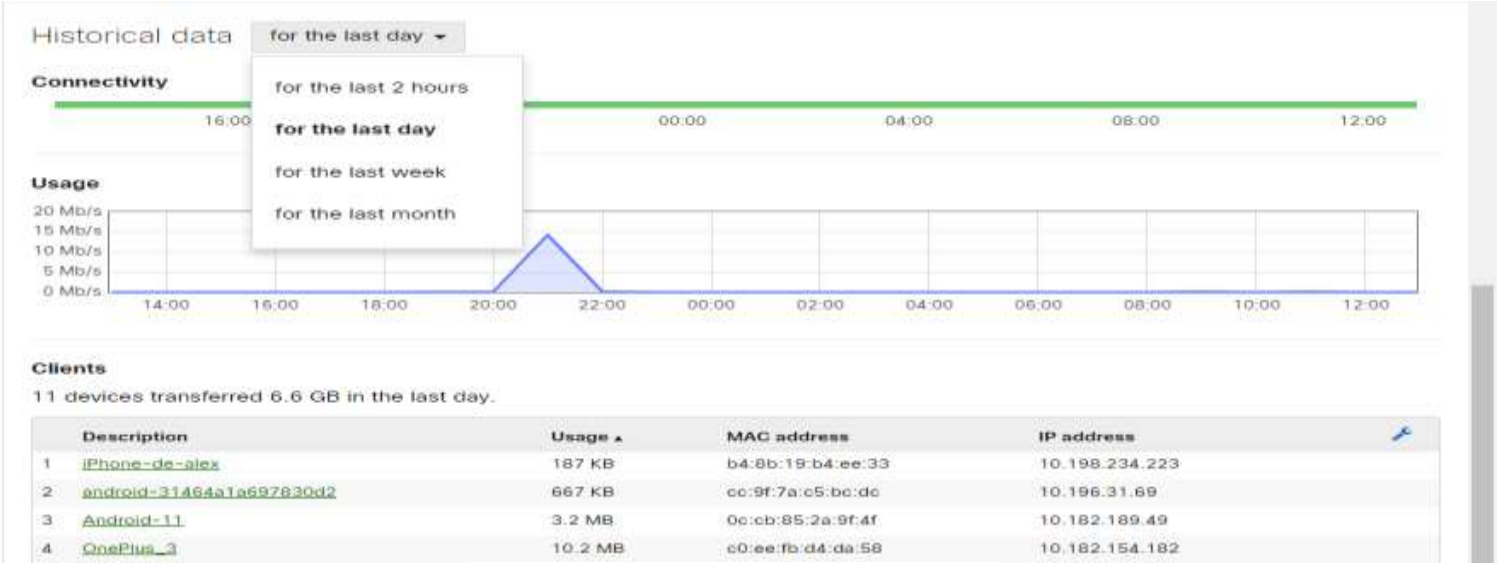


Figura 5. 10 Gráfico de conectividad y clientes

También existe un gráfico histórico para la utilización del canal que se puede ver de la misma manera que el gráfico de conectividad. El gráfico de utilización del canal puede ayudar a identificar un pico temporal o una saturación constante de un canal a lo largo del tiempo. Se lo encuentra en la pestaña RF. (Cisco Meraki, 2018)

Figura 5. 11 Gráfico histórico de la utilización del canal

Para los problemas en los que la utilización del canal muestra una gran cantidad de interferencia, ya que la mayor parte del tráfico es 802.11, es importante consultar la página Configure → Radio ajustes. Ahí se puede mostrar el número de puntos de acceso de Cisco Meraki y No-Cisco Meraki que se encuentran en los mismos canales que los puntos de acceso de la red, así como la intensidad máxima de la señal de interferencia. Si el gráfico de utilización muestra duraciones prolongadas de alta utilización del canal y la página Configuración → Radio muestra varios puntos de acceso en el mismo canal con una intensidad de señal alta, es probable que se deba cambiar el canal. (Cisco Meraki, 2018)

Dentro de las funcionalidades también se encuentra Air Marshal, la cual recopila una gran cantidad de información, incluso si un AP no es un Air Marshal dedicado. También está en la capacidad de detectar paquetes, así como SSID falsificados. (Cisco Meraki, 2018)

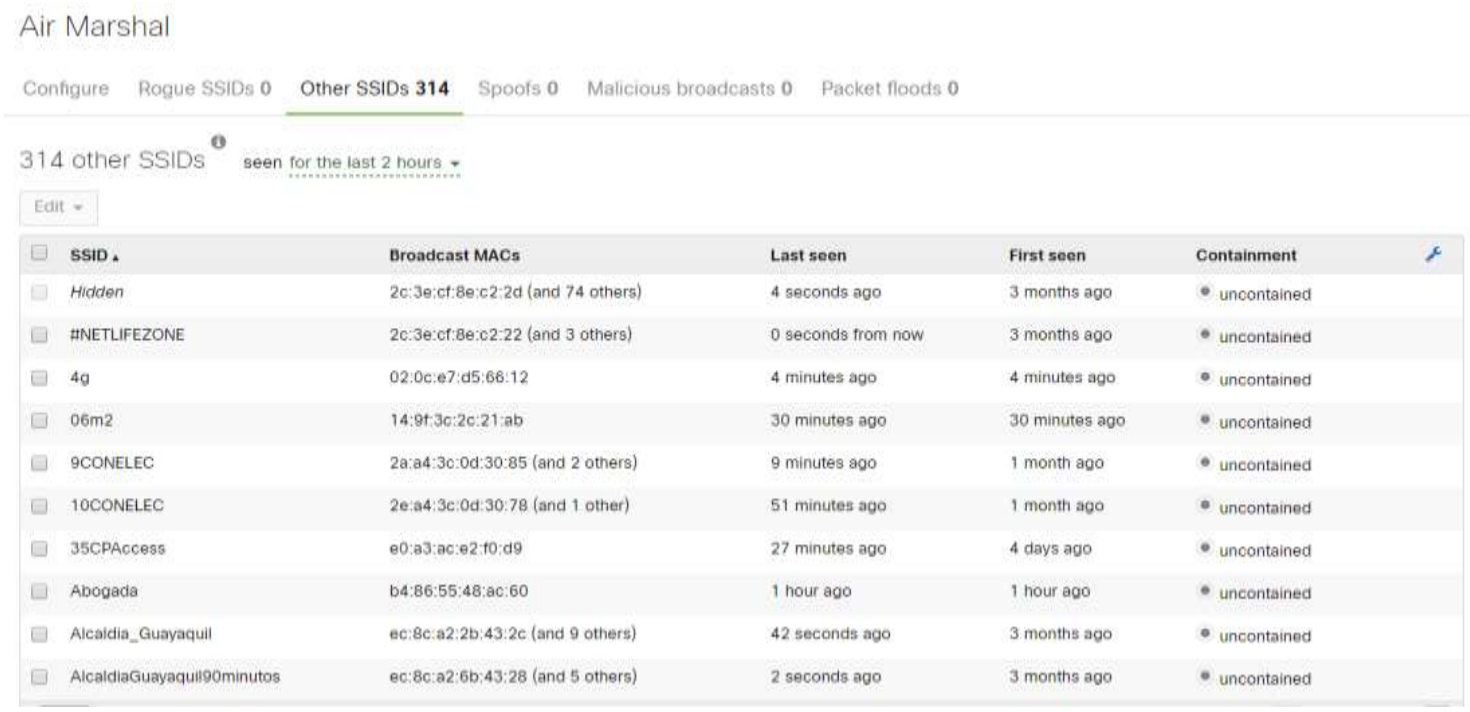


Figura 5. 12 Funcionalidades Air Marshal

También es posible monitorear el intento de acceso a la red, se puede realizar filtros por SSID, Dispositivo Meraki, tiempo y tipo de autorización (Ok o Fallida)

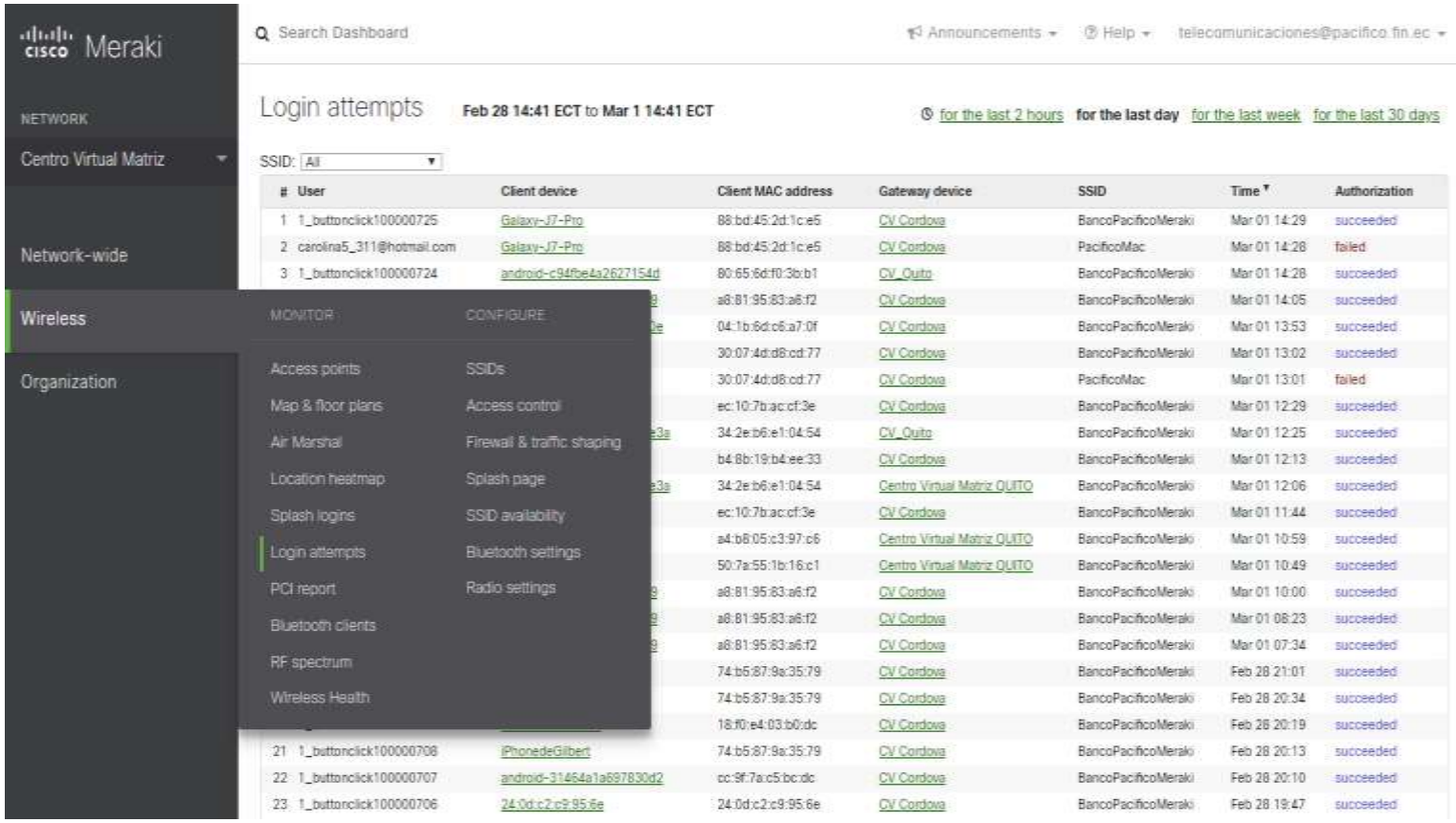


Figura 5. 13 Funcionalidades Intentos de Accesos

Con el informe resumido, se puede generar el resumen de todo lo mencionado anteriormente en un tiempo definido, este puede ser exportado en la PC local o enviado mediante un correo electrónico. (Cisco Meraki, 2018)

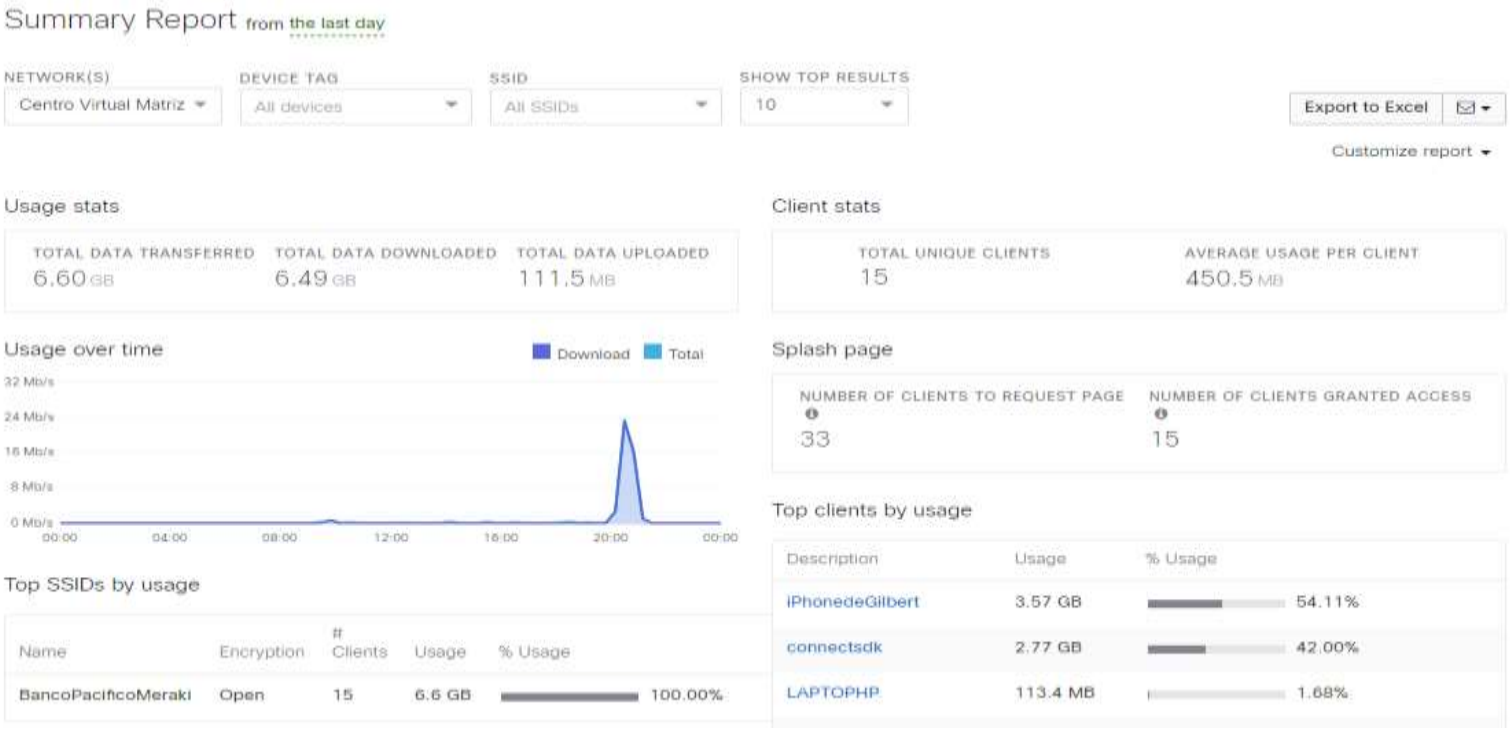


Figura 5. 14 Reporte Resumido

Existen más vías para obtener estadísticas de las conexiones de los usuarios en la opción Organización → Locación Analytics, aquí es posible saber según el tempo determinado la cantidad de personas que se conectaron cuantas están actualmente activas cuanto tiempo estuvieron conectadas de forma general, etc. (Cisco Meraki, 2018)

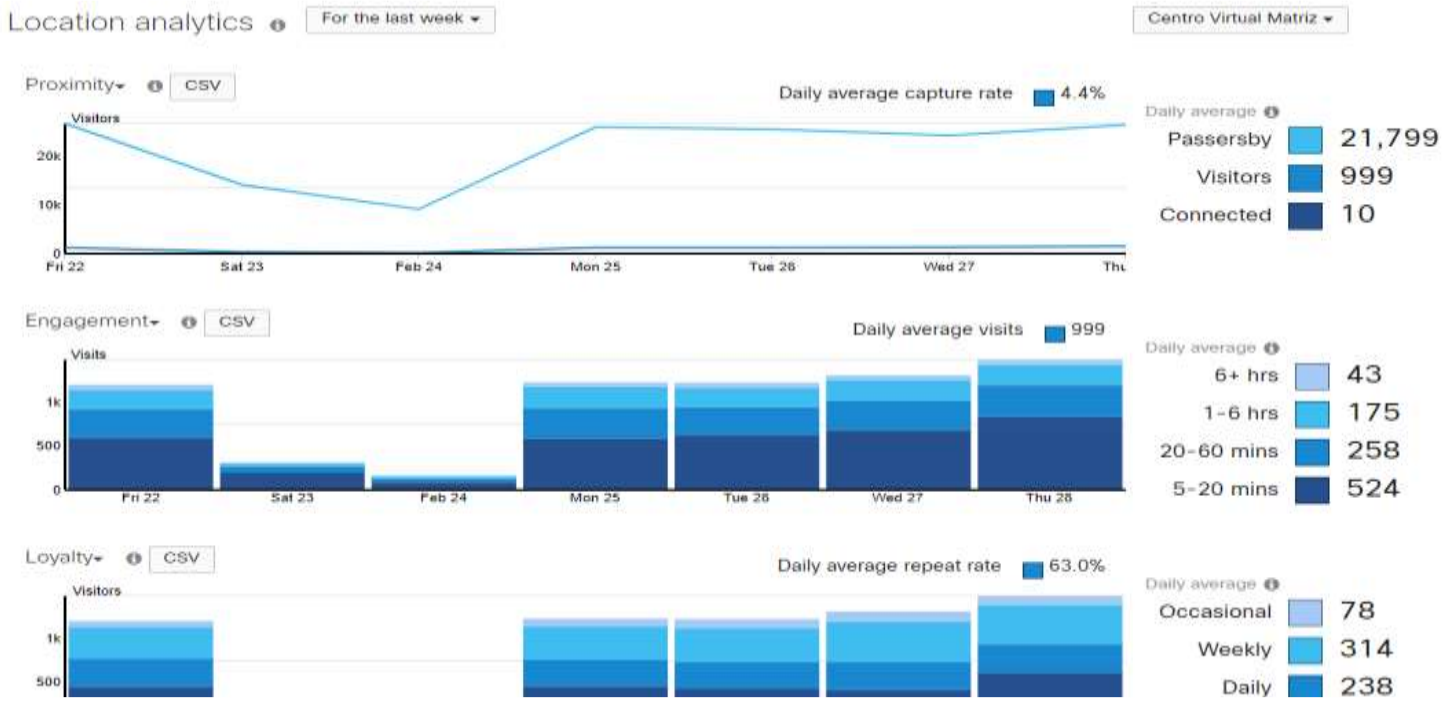


Figura 5. 15 Solución DNA CenterFigura 60 Análisis de Localización

CAPÍTULO 6

DNA CENTER

DNA Center es el software que administra y analiza eventos de la infraestructura, trae la utiliza aprendizaje automático para correlacionar las métricas de la red desde los dispositivos hasta los usuarios. (Cisco, S.F.) (CISCO, 2020)

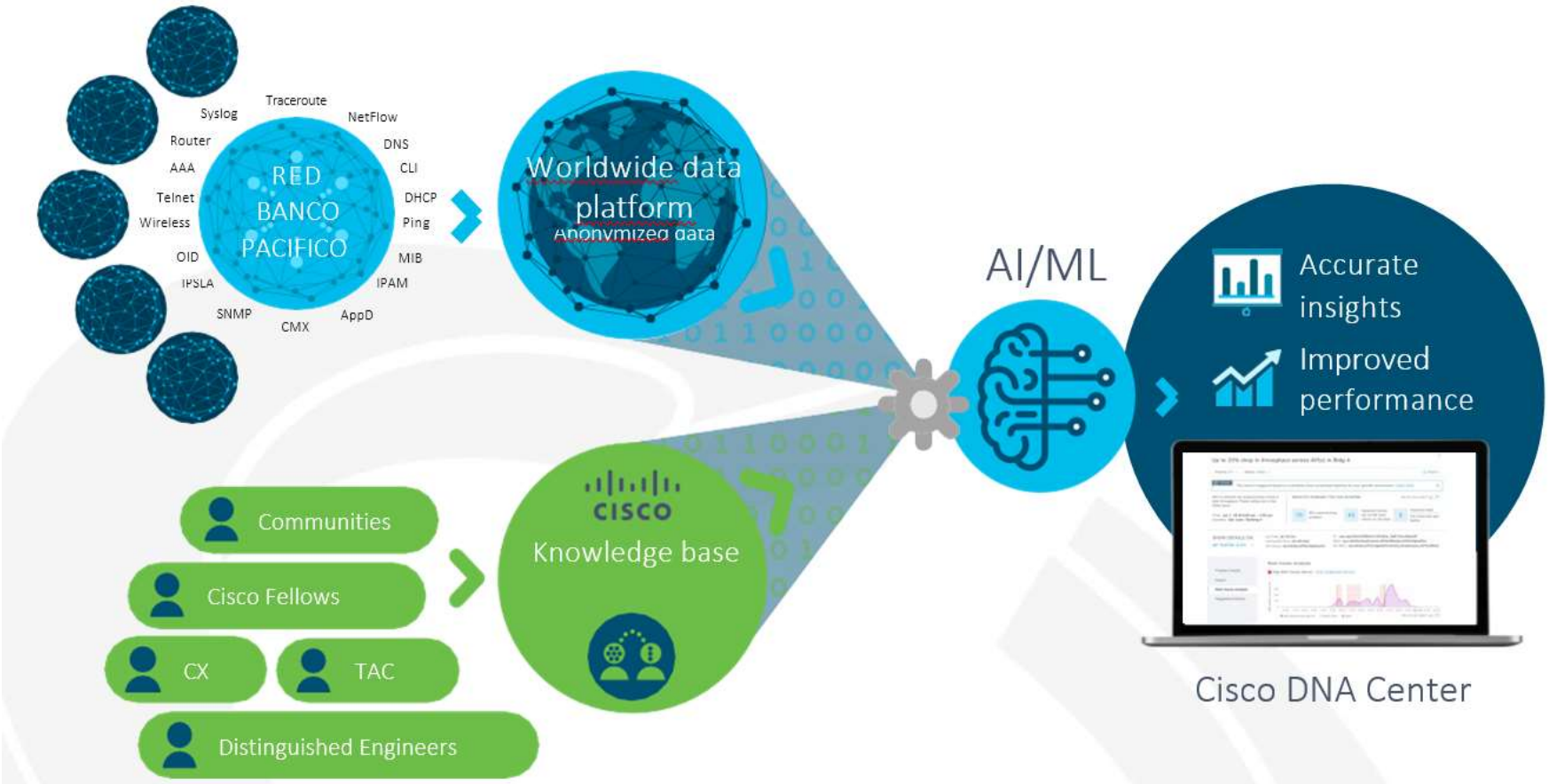


Figura 6. 1 Solución DNA Center

5.1 Redes Intuitivas

Durante el paso de los años, la demanda de servicios en la infraestructura empresarial se mantiene creciente, la arquitectura de las compañías se vuelve más robustas fortaleciendo su seguridad y su capacidad para soportar la comunicación de sus nuevos edificios y localidades. (CISCO, 2020)

La salud de la infraestructura depende en gran parte por la Operación, Mantenimiento, soporte y Mejora continua que le da su equipo de Ingenieros de IT, los cuales tienen como tarea principal, mantener la estabilidad de la red cableada o inalámbrica. (CISCO, 2020)

Como tal, esta infraestructura se vuelve más compleja al tener que combinar el soporte para mayor cantidad de servicios y sucursales. (CISCO, 2020)

Las actuales herramientas de monitoreo no abarcan todas las características de la red y pueden llegar a haber más de 3 servidores que cumplen funciones distintas.

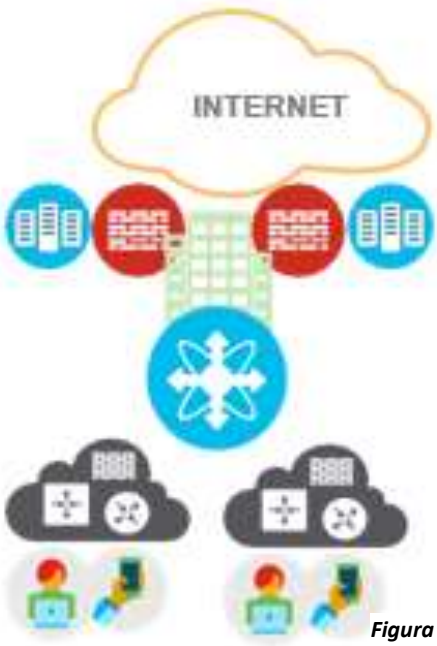


Figura 6. 2 Red Básica

El solucionador de problemas dentro de la infraestructura depende de la visibilidad que se tiene de ella y de la alta experiencia del personal encargado de administrarla.

Esta visibilidad se encuentra limitada y en ciertos puntos resulta prácticamente nula al no cubrir detalles que pueden afectar directamente a la Salud de la red.

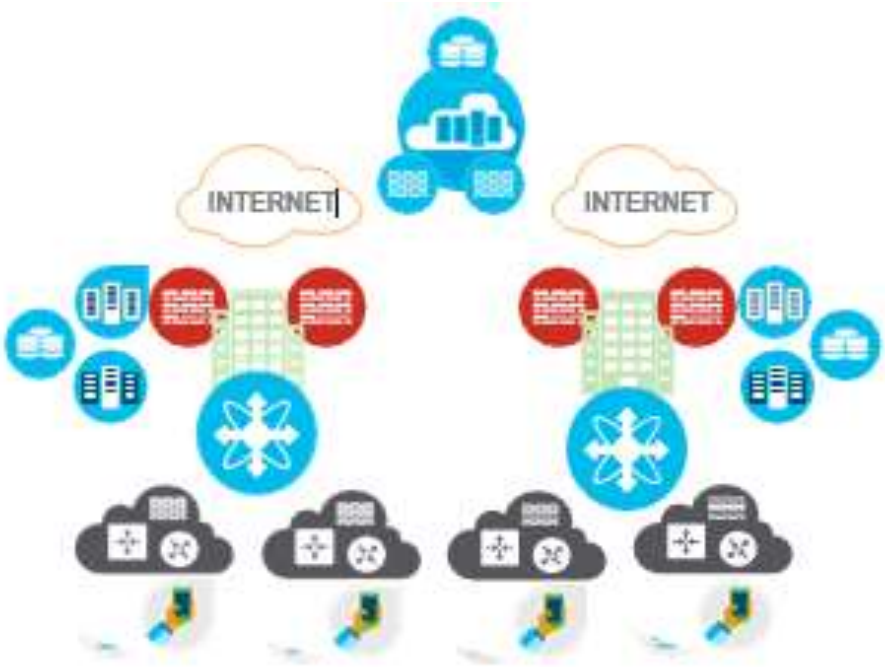


Figura 6. 3 Red Avanzada

El monitoreo de la infraestructura se realiza con servidores para SNMP, Syslog o Netflow, los cuales administran la información que obtienen de la red por separado lo que complica el análisis de los resultados.

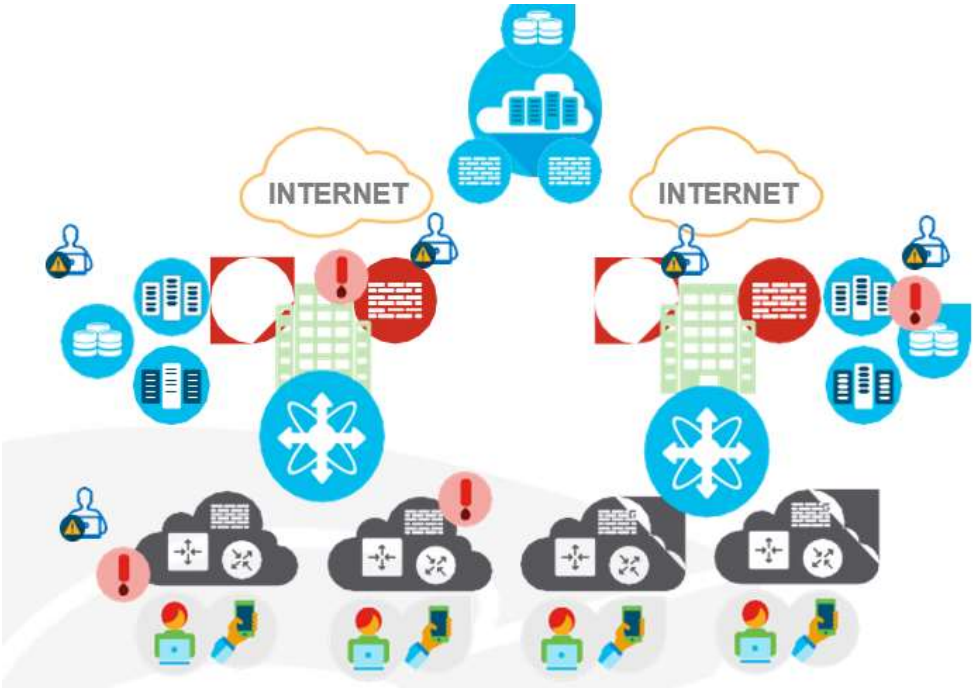


Figura 6. 4 Infraestructura con despliegue de ingeniería en solucionador de problemas

En búsqueda solucionar un problema, se puede llegar a tener un despliegue del personal a lo largo de toda la infraestructura lo cual disminuye productividad.

5.2 Infraestructura de la Entidad Financiera

La infraestructura inalámbrica de la entidad financiera se encuentra implementada de la siguiente manera:

- Campus con Acceso en L2 en su mayoría con Cat9K.
- Enlaces a Agencias se comunican con WAN por túneles GRE.
- El protocolo IGP es OSPF.
- Se monitorea la infraestructura por PRTG, ORION, y PRIME.
- Las localidades remotas tienen su propio direccionamiento.
- Los AP remotos se encuentran en modo FlexConnect.

Cuando no se logra identificar el origen del problema puede llegar a ser necesario realizar varias capturas de paquetes para mayor análisis debido a la limitada visibilidad que se posee. (CISCO, 2020)

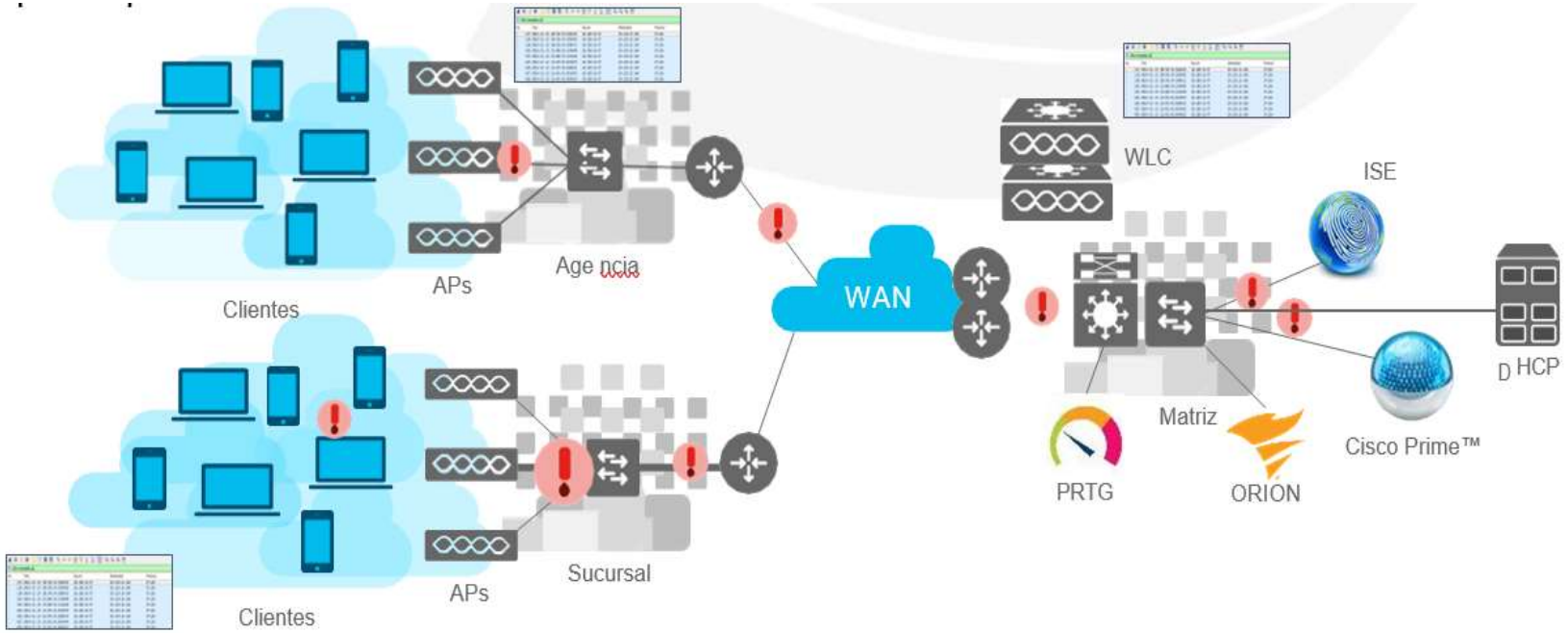


Figura 6. 5 Infraestructura resumida con tipos de tshoot aplicados

5.3 DNA Center Entidad Financiera

DNA Center se sincroniza activamente con las bases de datos de conocimiento de Cisco y utiliza Inteligencia Artificial junto con aprendizaje automático para correlacionar los eventos de la red y proporcionar de forma proactiva alertas que ayudan a la mejora operativa y de performance de la infraestructura. (Cisco, S.F.) (CISCO, 2020)

Existen dos tipos de despliegue para DNA Center, el primero aprovecha analítica sobre la infraestructura, tomando información desde todos los puntos de contacto de los dispositivos y Endpoint para identificar problemas y diagnosticar la salud de la infraestructura, a esta característica la llamamos Assurance. (Cisco, S.F.) (CISCO, 2020)

DNA Center también puede ser desplegado como gestor de políticas y automatización de la red, para esto es necesario cumplir con varios requisitos entre los cuales están la integración con Identity Service Engine, y un diseño de la red siguiendo las mejores prácticas para el despliegue de esta solución. (CISCO, 2020) (Cisco, S.F.)

El Banco en su infraestructura inalámbrica adoptó el despliegue de Assurance para el análisis y mejora de su red, de tal forma que se cumpla el objetivo de expandir la visibilidad de la salud y comportamiento de su infraestructura y que esto le ayude a mejorar su performance orientado a la productividad.

5.4 Implementación DNA Center

Los componentes instalados fueron los siguientes.

- Hardware:
- DNA Center Server DN1 UCS 220 M4
- Software Versión: DNAC 1.3.1.5
- Serial Number: FCH22030000

Figura 6. 6 Servidor Instalado DNA Center

5.5 Parámetros del Despliegue

Se solicitaron un conjunto de parámetros para realizar el despliegue del DNA Center. Es necesario

- **Enterprise port.:** 192.168.00.000 255.255.000.0 **Gateway:** 192.168.00.0
- **Puerto Cluster** 192.168.000.000 255.255.000.0
- **Parámetros Generales DNS:** 8.8.8.8 **NTP:** pool.ntp.org
- **Credenciales**

Adicionalmente DNA Center para comunicarse con los servidores de Cisco, utiliza la autenticación con la cuenta inteligente del Banco, habilitado por medio del usuario.

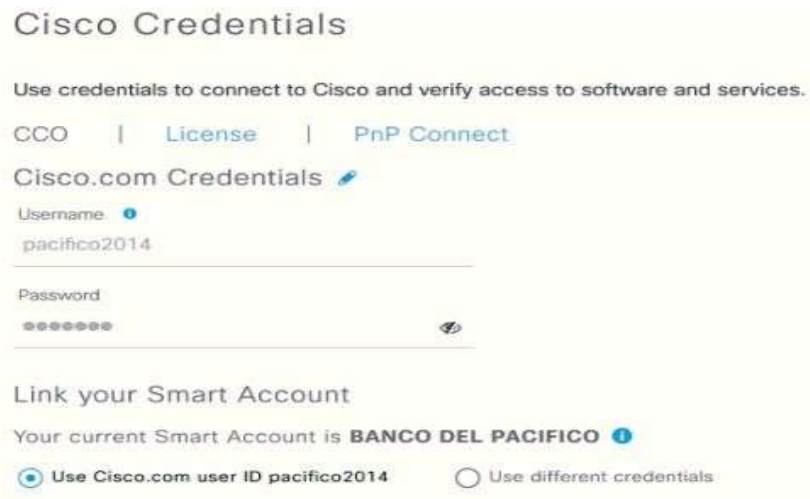


Figura 6. 7 Registro de DNA Center en cuenta inteligente

5.6 Plataforma DNA Center

Para acceder a la solución lo podemos hacer vía web por medio de https://192.000.00.000. La vista principal de se mostrará de la siguiente forma:

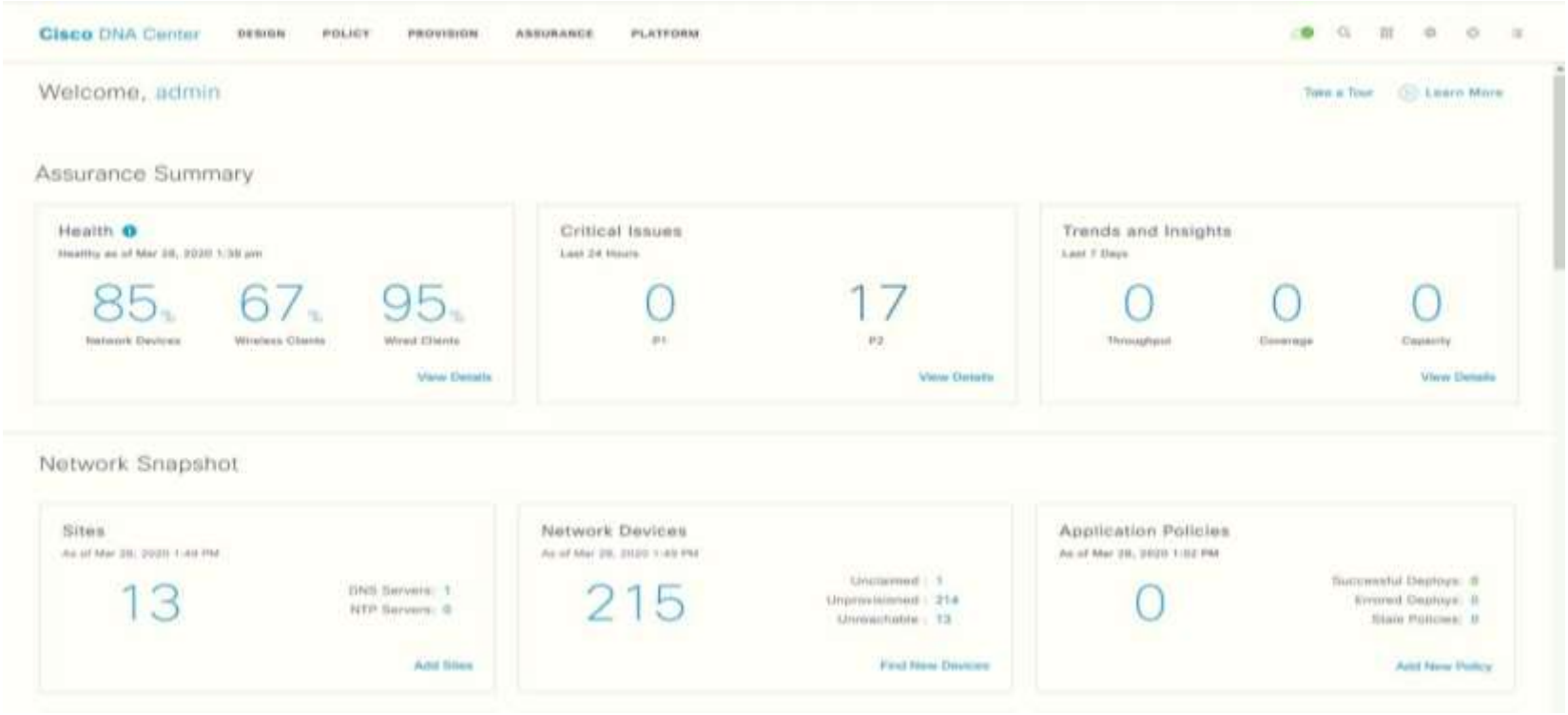


Figura 6. 8 Ventana Principal de DNA Center

En el Dashboard principal se muestra un resumen general de la salud de la infraestructura monitoreada, así como el estatus actual como una instancia de lo que tenemos monitoreado. Las Aplicaciones principales se muestran en la parte superior:

- Diseño.
- Política.
- Provisión.
- Garantía.

Figura 6. 9 Herramientas DNA Center

5.7 Herramientas DNA Center

DNA Center utiliza varias herramientas incorporadas que ayudan a descubrir, operar y validar características de la red, a continuación, analizaremos varias de ellas.

5.7.1 Descubrimiento

Podemos ejecutar tareas de Discovery en la red que nos ayuden a agregar mayor cantidad de equipos.

El Discovery puede ser utilizado de 3 formas distintas: CDP, Rango de IP, LLDP. El procedimiento consiste en:

- Asignar un nombre al Discovery.
- Seleccionar el tipo de Discovery.
- Ingresar una IP o Rango de IP.
- IP de administración.
- Credenciales del equipo.

Las credenciales pueden ser de uso local en el Discovery o puede ser utilizada una credencial Global

Figura 6. 10 Descubrimiento de Red

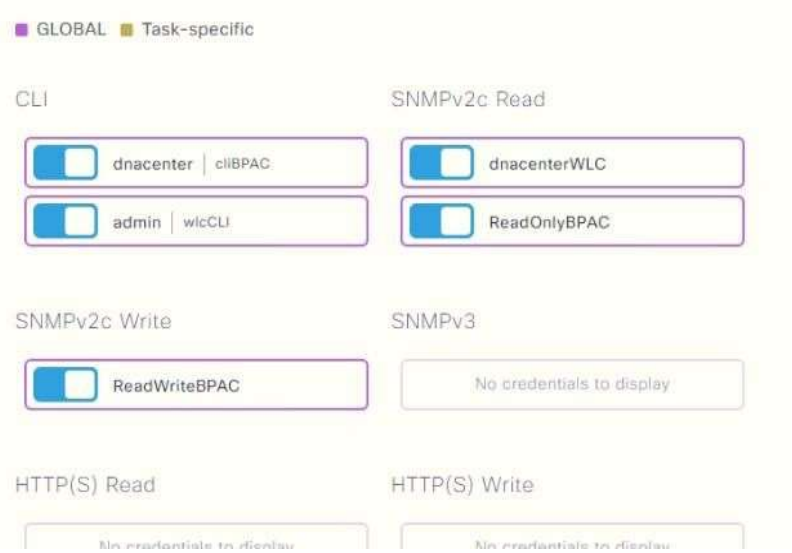


Figura 6. 11 Uso de Credenciales para realizar Descubrimiento

5.7.2 Topología

Por medio de esta herramienta tenemos una vista Gráfica mostrando la salud en un diagrama de topología o en un Mapa Geográfico.

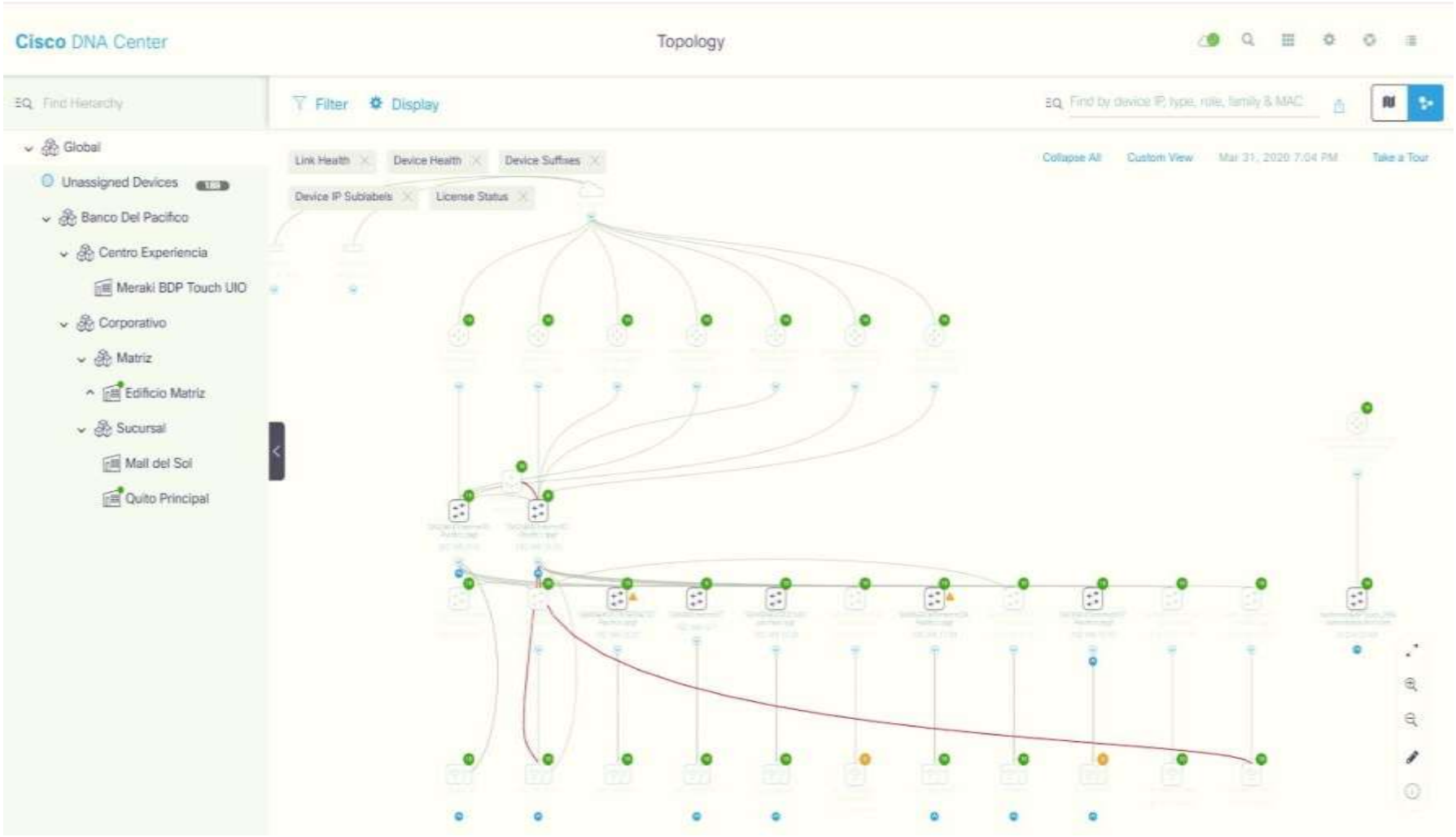


Figura 6. 12 Vista de Topología de la Red

5.7.3 Divisores de Seguridad

En esta herramienta podemos observar advertencias de Seguridad basadas en las versiones de software actuales de los productos monitoreados por DNA Center.

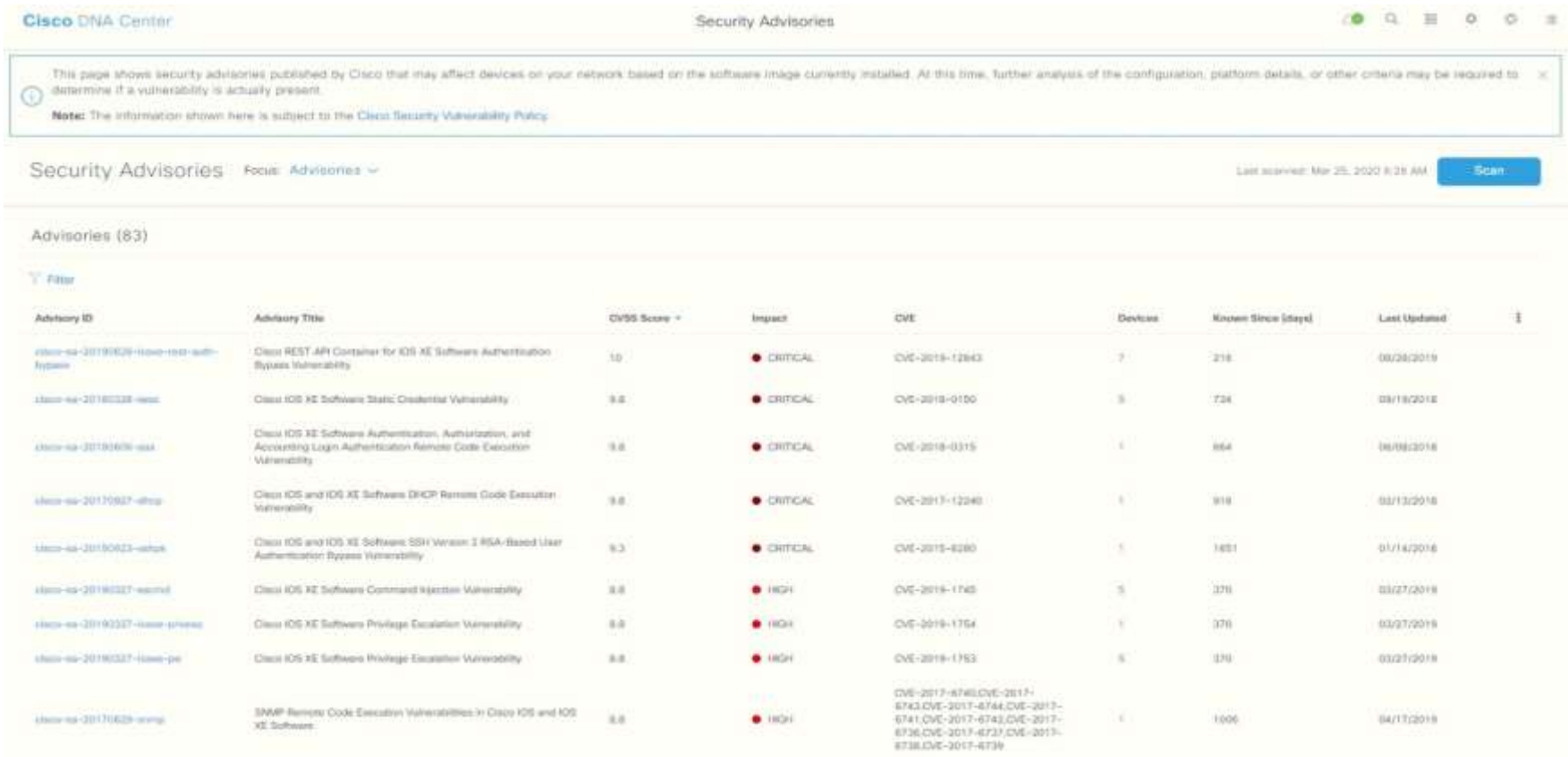


Figura 6. 13 Herramienta Avisos de Seguridad

5.7.4 Administrador Licencia

Al estar sincronizado con la cuenta inteligente de la entidad financiera, podemos monitorear el uso de las licencias inteligente que se están utilizando.

Esta información la pueden validar en software.cisco.com.

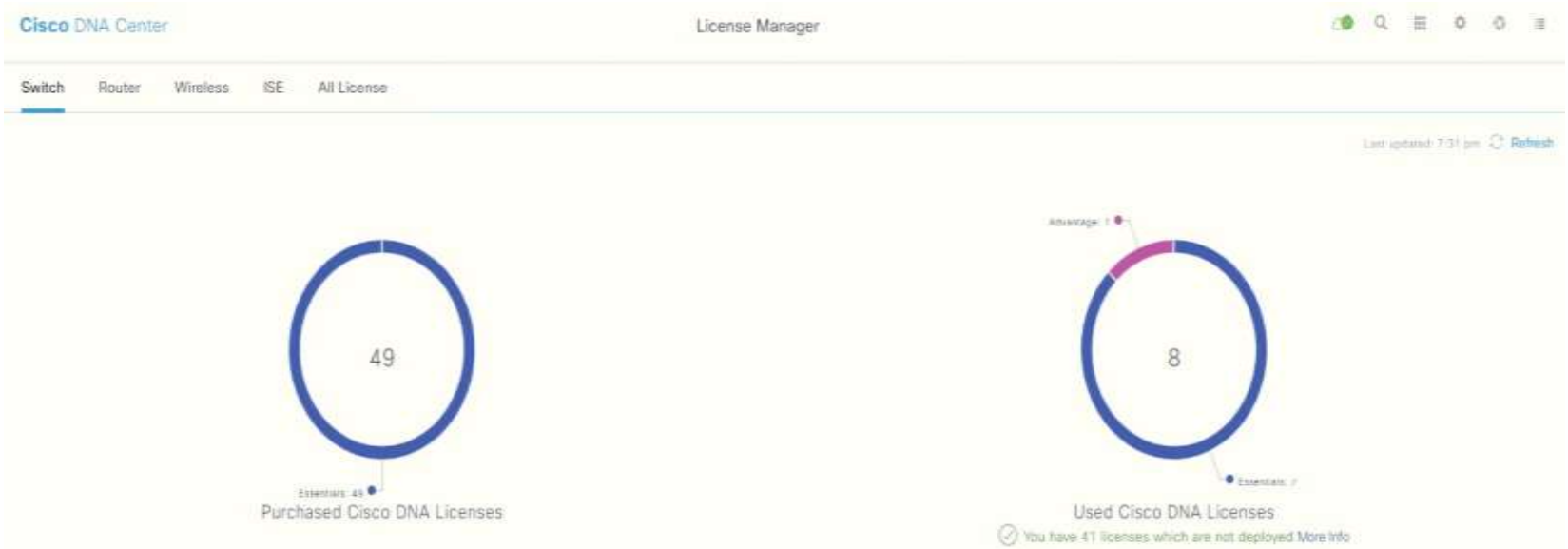


Figura 6. 14 Consumo de Licencias en DNA Center

5.7.5 Datos e informes

DNA Center por el momento DNA Center no realiza reportes de las estadísticas antes vistas en las aplicaciones como garantía sin embargo puede generar reportes ordenados de Inventario, Clientes o Software actualizaciones.

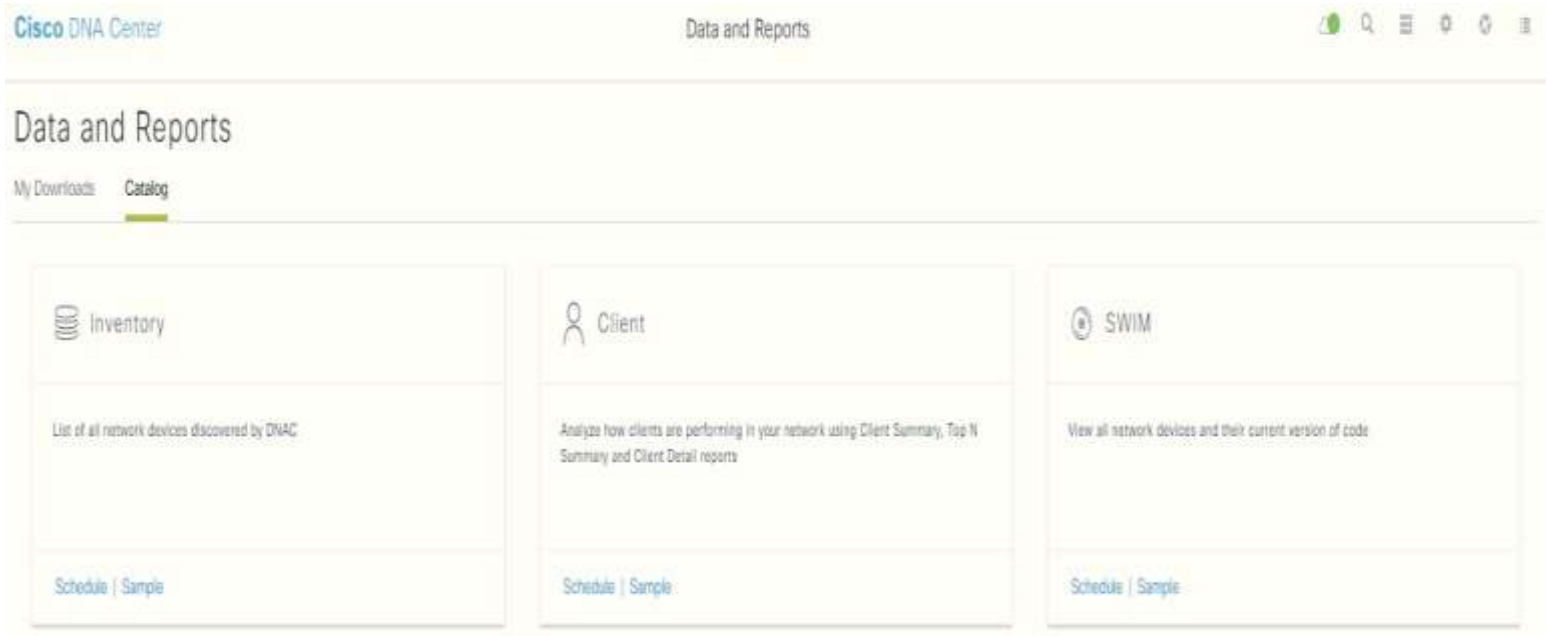


Figura 6. 15 Reportería desde DNA Center

5.8 Herramientas Generales

5.8.1 Datos e informes

DNA Center adicionalmente puede realizar monitoreo a si mismo por medio de sistema 360.

Figura 6. 16 Sistema 360 es la forma como DNA Center realiza monitoreo a sus propios módulos o aplicaciones

5.8.2 Usuarios

Existen varios tipos de usuarios para administrar la plataforma, se lo puede realizar por medio de un servidor AAA o de forma local.

Los tipos de usuarios son:

- **Administrador (Super-Admin-Rol)** Acceso Total a todas las funciones de DNA Center, incluso crear usuarios sin embargo no puede cambiar la clave de otros usuarios.
- **Network Administrador (Network-Admin-Role)** Acceso solo a funciones relacionadas a la Red, no tienen acceso a funciones o configuraciones del sistema.
- **Observador (Observador-Rol)** Solo tienen acceso de observador a las funciones del DNA Center, no pueden realizar configuración alguna.
- **Telemetría-Admin-Role** Utilizado solamente para funciones a nivel del sistema Dentro del DNA Center.

5.9 Beneficios de la Nueva Infraestructura

- **Aumento de la productividad gracias a un acceso de red seguro e independiente de su ubicación:** comunicación y mejoras de la productividad cuantificables.
- **Flexibilidad adicional de la red:** se usan redes inalámbricas en las ubicaciones con dificultad para su conexión por cable sin costosas estructuras.
- **Implementación rentable:** adopción de tecnologías visualizadas dentro de la arquitectura inalámbrica general.
- **Administración y usos sencillos:** desde un punto de administración centralizada, control de un entorno inalámbrico distribuido desde un solo lugar.

- **Implementación Plug and Play:** aprovisionamiento automático cuando un punto de acceso está conectado a la red por cable de apoyo.
- **Diseño flexible y tolerante a fallos:** conectividad inalámbrica fiable en entornos vitales, incluida la administración de todo el espectro de RF.
- **Transmisión eficaz del tráfico de multifunción:** compatibilidad con muchas aplicaciones de comunicación en grupo, como de video y pulsar para hablar. (CISCO, Resumen del diseño de tecnología de red LAN inalámbrica de campus, 2014)

Proporcionar conectividad de datos y voz en cualquier parte a los empleados y acceso inalámbrico de internet a los invitados y clientes independiente mente de su ubicación en la organización, los usuarios de la conexión inalámbrica disfrutarían de la misma experiencia cuando se conecten en los servicios de voz, video y datos.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Este proyecto detalla el diseño de la red inalámbrica en la entidad financiera, mediante la infraestructura tecnológica Cisco, que la constituye una infraestructura robusta para brindar todos los beneficios y ventajas ofrecidas para funcionarios y nuestros clientes.
2. El análisis previo del problema nos facilitó establecer mejores resultados para la solución inalámbrica en lo que se requería ofreciendo las mejores alternativas, adoptando medidas activas para salvaguardar la seguridad y la confiabilidad de la red inalámbrica.
3. Estar comprometidos con asegurar y proteger a nuestros clientes y sus datos, contar con un control de acceso unificado y centralizado basado en roles, independiente del medio (inalámbrica, red cableada o incluso VPN).
4. Mayor visibilidad e identificación más precisa de los dispositivos mediante el servicio de difusión de perfiles de dispositivos y la definición de perfiles, simplicidad en la experiencia de los invitados y clientes para lograr conectarlos y administrarlos de forma más sencilla, creando políticas de segmentación basadas en software destinadas a contener las amenazas para la red.
5. Con DNA Center se puede realizar un inventario de dispositivos obteniendo una revisión periódica y de las posibles vulnerabilidades, manteniendo todos los equipos actualizados, copias de seguridad y procedimiento de recuperación probados.
6. Meraki tiene su gestión alojada en la nube, eliminando controladores de hardware, cada punto de acceso de repetidor en una red de Cisco Meraki transmite y recibe la señal que recibe de su punto de acceso cableado. El tráfico de datos enviado entre dispositivos en una red de

Cisco Meraki se cifra mediante el algoritmo del Estándar de cifrado avanzado (AES)

RECOMENDACIONES

1. Implementar un sistema de detención de instrucciones (IDS), para la detención de posibles anomalías que generen alarmas. Monitorice el trafico de la red y realizar una búsqueda periódica de anomalías.
2. Implementar la opción de poder configurar en el Identity Services Engine (ISE) para la integración con un servidor del Directory Access Protocol de Cisco (LDAP). Esto quiere decir, que podemos integrar el Directorio Activo de la red LAN de usuarios de la entidad bancaria en la controladora, eliminando la configuración del ADFS Externo.
3. Crear un portal cautivo, con la finalidad de integrar el Directorio Activo en el ISE donde la controladora haría la consulta a la base de datos LAN del banco, y si está en el directorio le proporcionaría internet.
4. DNA Center utiliza todos los parámetros que se encuentren configurados para realizar análisis y correlación de eventos por lo que es importante actualizar las configuraciones de la herramienta cuando haya cambios en la infraestructura.
5. Se puede extender y potenciar la visibilidad de dispositivos que se conectan a la infraestructura inalámbrica por medio de integración de una herramienta adicional.
6. DNA Center puede expandir su funcionamiento por medio de la integración de su propia API con otras plataformas. DNA Center fue actualizado a la versión más estable del producto, a pesar de existir una versión más actual, se recomienda no actualizarla y de hacerlo, validar la matriz de compatibilidades con el Hardware.

BIBLIOGRAFÍA

[1] Alepo. (S.F.). AAA | Optimize and modernize carrier networks. Obtenido de AAA | Optimize and modernize carrier networks: https://www.alepo.com/products-services/aaa-infrastructure/

[2] Alepo. (S.F.). About Us. Obtenido de About Us: https://www.alepo.com/about-us/

[3] CISCO. (2014). Resumen del diseño de tecnología de red LAN inalámbrica de campus. Resumen del diseño de tecnología de red LAN inalámbrica de campus, 19.

[4] CISCO. (2018). CISCO Movilidad excepcional con redes inalambricas. CISCO Movilidad excepcional con redes inalambricas, 6.

[5] CISCO. (20 de Junio de 2019). Cisco 5520 Wireless Controller Data Sheet - Cisco. Obtenido de Cisco 5520 Wireless Controller Data Sheet - Cisco: https://www.cisco.com/c/en/us/products/collateral/wireless/5520-wireless-controller/datasheet-c78-734257.html

[6] CISCO. (08 de Agosto de 2019). Cisco Identity Services Engine - Cisco Identity Services Engine Data Sheet - Cisco. Obtenido de Cisco Identity Services Engine - Cisco Identity Services Engine Data Sheet - Cisco: https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html

[7] CISCO. (09 de Agosto de 2019). Cisco Identity Services Engine - Hoja de datos del servidor de red segura de Cisco - Cisco. Obtenido de https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/datasheet-c78-726524.html

[8] CISCO. (04 de Marzo de 2020). Cisco Aironet 4800 Access Point Data Sheet. Obtenido de Cisco Aironet 4800 Access Point Data Sheet: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-4800-access-point/nb-09-air-4800-acces-ds-cte.html

[9] CISCO. (10 de Febrero de 2020). Cisco DNA Center - Cisco DNA Center 1.3.3.0 Data Sheet. Obtenido de Cisco DNA Center - Cisco DNA Center 1.3.3.0 Data Sheet: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.html

[10] Cisco Meraki. (10 de Abril de 2018). Meraki Cloud Architecture. Obtenido de Meraki Cloud Architecture: https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Meraki_Cloud_Architecture

[11] Cisco. (S.F.). Cisco DNA Center: Administración y automatización de redes de Cisco. Obtenido de Cisco DNA Center: Administración y automatización de redes de Cisco: https://www.cisco.com/c/es_ar/products/cloud-systems-management/dna-center/index.html

[12] Cisco. (S.F.). Cisco Identity Services Engine (ISE). Obtenido de https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

[13] CISCO. (S.F.). Cisco Prime Infrastructure. Obtenido de Cisco Prime Infrastructure: https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/index.html