UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA: INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de: INGENIERO ELECTRÓNICO

TEMA:
DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE AUTENTICACIÓN Y POLÍTICAS DE SEGURIDAD MEDIANTE UN SERVIDOR AAA, HACIENDO USO DEL ESTÁNDAR IEEE 802.1X Y LOS PROTOCOLOS RADIUS Y TACACS+ PARA LA RED CORPORATIVA DE LA EMPRESA PROYECTOS INTEGRALES DEL ECUADOR PIL S.A.

AUTOR:
ÁNGEL ANDRÉS VALDIVIESO VILLAMARÍN

DIRECTOR:
JOSÉ ANTONIO PAZMIÑO SANDOVAL

Quito, mayo de 2015

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE TITULACIÓN

Yo, autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de titulación y su reproducción sin fines de lucro.

Además, declaro que los conceptos, análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

Quito, mayo de 2015

_____

Ángel Andrés Valdivieso Villamarín
CC: 1721943635

DEDICATORIA

Este trabajo de titulación lo dedico, primero a Dios por brindarme la salud y vida, a mi querida madre Roció que con sus consejos y tenacidad me ha ensañado que todo en la es posible con esfuerzo y sacrificio, además a siempre salir adelante a pesar de las dificultades que se presenten en el transcurso de la vida, a mi querido padre Ángel que me ha inculcado el valor del trabajo y de la responsabilidad para con mis actividades, a mi querida hermana Carito que siempre me ha apoyado y me ha sabido dar su comprensión en los momentos que más los he sabido necesitar, a mis compañeros de trabajo del departamento de telecomunicaciones de Proyectos Integrales del Ecuador PIL S.A. y su valioso apoyo a lo largo de este proceso.

También a mi prima Tatty por confiar en mí y siempre brindarme su ayuda en los momentos que más lo supe necesitar y esperando de todo corazón que recupere su salud satisfactoriamente.

Andrés.

AGRADECIMIENTO

Agradezco a mi director de trabajo de titulación Ing. José Antonio Pazmiño Sandoval que me brindó su tiempo, amistad, consejos, experiencia, paciencia, motivación y conocimientos para lograr terminar mis estudios con éxito.

También agradezco al lector de mi trabajo de titulación, por aportar con sus consejos, conocimiento, experiencia, amistad y sobre todo por su valioso tiempo para culminar con este proceso.

De manera muy especial agradezco a la empresa Proyectos Integrales del Ecuador PIL S.A. por brindarme la oportunidad de realizar mi trabajo de titulación en sus instalaciones y aportarme todos los recursos necesarios para la culminación del mismo.

Un agradecimiento y gratitud hacia la Universidad Politécnica Salesiana y a sus profesores que a lo largo de mi trayectoria estudiantil me han sabido guiar para formarme como un excelente profesional y persona.

A todos les manifiesto mi más sincero agradecimiento.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Proyectos Integrales del Ecuador PIL S.A., una empresa que presta servicios en el sector industrial y de las telecomunicaciones, ha tenido problemas en su red interna de comunicaciones por falta de escalabilidad y convergencia en sus servicios de red, además presenta altos tiempos de retardo en transmisión de datos y mecanismos de seguridad, debido a su infraestructura deteriorada y centralizada en un servidor UTM que brinda servicios de seguridad y de red para los usuarios.

El mecanismo de acceso seguro estaba manejado directamente por el directorio activo teniendo una arquitectura de puerto extendido hacia el usuario, además de ser asignado con VLAN estática en determinados puertos y su salida internet por otra aplicación, por que el usuario necesitaba ingresar dos veces sus credenciales para poder tener servicio de internet, presentando problemas en la administración de políticas de seguridad para el coordinador del departamento de TI.

Con lo expuesto anteriormente y por un aumento de personal dentro de la organización, pensando en una mejora a nivel de disponibilidad rendimiento y seguridad, se ha decidido realizar una reestructuración de la infraestructura, para mejorar los servicios de la red corporativa y de esta manera satisfacer las necesidades de seguridad y beneficios tecnológicos para cada uno de sus trabajadores.

Se ha decidido cambiar todos los equipos existentes de marca 3com por equipos Cisco, el acceso seguro a la red con el sistema UTM (Gestión Unificada de Amenazas) por un servidor de seguridad AAA (Autenticación, Autorización y Auditoria), que lo llevará acabo el ACS (Servidor de Control de Acceso) de Cisco para las autenticaciones de los usuarios, ya sea a través de la red cableada e inalámbrica; este estará vinculado al directorio activo de Windows, el mismo que será configurado por el departamento de TI (Tecnología de la Información), de PIL S.A.

El sistema nuevo permitirá movilidad y seguridad para el acceso a la red tanto a nivel LAN (Red de Área Local), como WLAN (Red de Área Local Inalámbrica), de modo que si un usuario desea acceder a la red de PIL S.A., deberá hacerlo mediante su cuenta de usuario y contraseña, estos datos se encontrarán registrados en el directorio

activo, manteniendo así la visibilidad y el control de acceso de cada uno de los usuarios que ingresan a la red, asignando automáticamente los permisos y recursos de red según el perfil de usuario especificado dentro de la base de datos.

Si un usuario no registrado intenta acceder a la red, el sistema se encargará de bloquear el puerto por el que se registró la anomalía, protegiendo de esta manera la red de PIL S.A. de una posible filtración de información por personas ajenas a la empresa, manteniendo la confiabilidad e integridad del sistema.

Se evaluaron diferentes tipos de usuarios y grupos con la finalidad de corroborar que cumplan con las políticas designadas en el directorio activo por parte del personal de ti de PIL S.A. Por lo tanto el usuario debe pasar por dos niveles de seguridad a través del equipo autenticador y el servidor de autenticación para poder enviar su petición al directorio activo el ACS le asigna a la VLAN a la que este está relacionado.

ABSTRACT

Proyectos Integrales del Ecuador PIL S.A., a company that provides services in the industrial sector and telecommunications, has struggled in its internal communications network for lack of scalability and convergence in their network services, also has high transmission delay times data and security mechanisms, due to his deteriorating and centralized infrastructure in a UTM server that provides services and network security for users.

The mechanism Secure Access was handled directly by the active directory having a port architecture extended to the user, in addition to being assigned static VLAN in certain ports and output internet by another application, the user needed to enter twice credentials to have internet service, presenting problems in the management of security policies for the IT department coordinator.

With the foregoing and an increase of staff within the organization, thinking about an improvement in terms of availability performance and safety, it was decided to perform a restructuring of infrastructure, to improve services to the corporate network and thus satisfy security needs and technological benefits for each of their workers.

It was decided to change all existing equipment brand 3com by Cisco equipment, secure access to network with UTM (Unified Threat Management) for server AAA (Authentication, Authorization and Audit) Security, which will take place on ACS (Access Control Server) Cisco authentications of users, either through wired and wireless network; This will be linked to Windows Active Directory, it will be configured by IT (Information Technology) of PIL S.A.

The new system will allow mobility and security for network access both LAN level (Local Area Network) and WLAN (Wireless Local Area), so if a user wants to access the network PIL S.A., you must Register through your user account and password, this information will be found recorded in the current directory, thus maintaining visibility and control of access each user entering the network, automatically

assigning permissions and network resources according to user profile within the specified database.

If an unregistered user tries to access the network, the system will block the port that the anomaly was recorded, thus protecting network PIL S.A. of a possible leak of information by persons outside the company, maintaining the reliability and integrity of the system.

Different types of users and groups in order to corroborate that meet the designated policies in the Active Directory by staff of PIL S.A. were evaluated Therefore the user must go through two security levels through the authenticator equipment and the authentication server to send your request to Active Directory ACS assigns the VLAN to which this is related.

INTRODUCCIÓN

Actualmente se sabe que los primordiales requerimientos de los sistemas informáticos que desempeñan tareas significativas, son los mecanismo de seguridad adecuados a la información que se intenta salvaguardar; el conjunto de tales mecanismos debe incluir al menos un sistema que permita identificar a los elementos activos en una red de comunicaciones (usuarios), que intenten tener acceso a los recursos de la misma, mediante procesos que impliquen credenciales como una contraseña y un nombre de usuario.

La empresa PIL S.A. pensando en la mejora continua de su desarrollo empresarial, se ha visto en la necesidad de proteger sus recursos de red incrementando el nivel de seguridad en el acceso y mejorando la infraestructura de la misma, para ofrecer a su personal todas las facilidades de desarrollo, de seguridad a nivel de acceso a la información de la empresa y seguridad perimetral, a fin de salvaguardar la integridad de sus procesos de gestión y funcionamiento.

Para permitir un acceso controlado a su red de comunicaciones y brindar la seguridad anhelada, la empresa ha decidido utilizar una solución IBNS (Seguridad de Red Basada en Identidad), para lo cual con la ayuda de un servidor ACS de marca Cisco, prestará los servicios de AAA (Autenticación, Autorización y Auditoria), con la previa configuración de los protocolos RADIUS, TACACS+ y además el uso del estándar IEEE 802.1X.

De esta manera se permitirá a los usuarios tener movilidad, seguridad en el acceso a la red y se protegerá toda información que transite a través de la misma, por lo que si un usuario desea acceder a los servicios y recursos informáticos de la empresa, deberá hacerlo mediante el uso de sus credenciales previamente asignadas (username y password) registradas en el servidor de dominio, si estos datos son correctos se le asignará automáticamente los permisos de operación según su perfil creado dentro del directorio activo. En caso de que una persona intente ingresar a la red con credenciales no autorizadas, su acceso será denegado y como medida de seguridad adicional bloqueado.

CAPÍTULO 1

SEGURIDAD DE LA RED

En este capítulo se menciona a nivel general, sobre la seguridad de acceso a la red, como también de aquellos dispositivos, protocolos y políticas que intervienen para cumplir dicho propósito.

1.1 Planteamiento del problema

Proyectos Integrales del Ecuador PIL S.A. es una empresa dedicada a la ingeniería, montaje y puesta en marcha de proyectos industriales para el sector hidrocarburífero, con énfasis en la optimización de los mismos, con sedes en Bogotá, Lima, Quito y Houston, que inició sus operaciones en el país hace aproximadamente diez años. Considerando la tecnología y la baja cantidad de personal en aquel momento, se implementó una red de datos no escalable.

Actualmente se están presentando problemas en tiempos de transmisión de datos, lo cual, principalmente se debe a su estructura de red plana, donde todas las estaciones de trabajo, teléfonos y demás periféricos que se encuentran ubicados en una sola subred IP. Adicionalmente, en el esquema de seguridad perimetral todas las funciones se concentran en un servidor del tipo UTM (Gestión Unificada de Amenazas), que realiza actividades de enrutamiento, nateo, firewall, control web, además de ofrecer servicios de aplicaciones.

Por la naturaleza, la red actual de PIL S.A. no dispone de un sistema de acceso seguro de red, el mismo que permita salvaguardar, monitorear y brindar políticas de seguridad para el adecuado manejo de información tanto al interior como en el exterior de la red corporativa de la empresa.

Considerando que la estructura actual de administración de datos, posee un promedio de 300 usuarios que realizan simultáneamente sus funciones, el esquema de servicio que ofrece esta red, se contrarresta en su eficiencia, afectando así la productividad y desarrollo de cada uno de sus colaboradores.

1.2 Justificación

La utilización de un ACS (Acceso Seguro a la Red), al administrador de la red corporativa le permitirá, controlar y autorizar el acceso, de los usuarios o grupos de usuarios, a los diferentes servicios ofrecidos por el mencionado Sistema, en base a un registro de contabilidad de todas las acciones realizadas por los usuarios en la red (Contabilización). De igual manera, el administrador de la red podrá utilizar la estructura del servidor AAA (Autenticación, Autorización y Auditoría) para gestionar (mediante TACACS+) el acceso a los equipos activos de la red (Ej.: switches y routers).

Adicionalmente es importante analizar las facilidades ofrecidas por los servidores AAA, así como también, el uso adecuado de los protocolos involucrados que permitirán el diseño del Sistema de Autenticación así como las Políticas de Seguridad que se verán involucradas para beneficio dentro de la red corporativa de la empresa Proyectos integrales del Ecuador PIL S.A.

Es imperativo contar con un Sistema de Autenticación y Políticas de Seguridad de acuerdo con los requerimientos de servicios de red basados en identidad (IBNS), mediante el uso de un servidor de control de acceso seguro a la red, de alto rendimiento como RADIUS y/o TACACS+ centralizado, el mismo puede encargarse de controlar las funciones del servidor AAA, para los usuarios que accedan a los recursos de que se encuentran en la base de datos de la empresa Proyectos Integrales del Ecuador a través de su red corporativa.

1.3 Objetivo general

Diseñar e implementar un sistema de autenticación y políticas de seguridad para la red corporativa de la empresa Proyectos integrales del Ecuador PIL S.A.

1.4 Objetivos específicos

- Establecer la situación actual del Sistema de Autenticación y Acceso Seguro de Red, con el que cuenta la red corporativa de la empresa Proyectos Integrales del Ecuador PIL S.A.

- Diseñar un sistema de seguridad de acceso a la red corporativa, basado en un servidor "AAA" (Autenticación, Autorización y Registro), que permita la aplicación de políticas de acceso a la red.

- Implementar las políticas de seguridad de acceso a la red corporativa, basado en los perfiles de usuario dispuestos por el departamento de TI de la empresa configurados en el directorio activo.

- Verificar las políticas implementadas, bajo los protocolos de autenticación 802.1X, Radius, TACACS+, mediante el ingreso de usuarios registrados y no registrados a la red corporativa de la empresa Proyectos integrales del Ecuador PIL S.A.

1.5 Alcance

Este proyecto tiene por objetivo principal el diseño e implementación de un sistema de autenticación y políticas de seguridad para la empresa Proyectos Integrales del Ecuador PIL S.A.

Para lograr este objetivo se configurará en todos los equipos de red a nivel LAN como WLAN, los protocolos de acceso seguro de red haciendo uso del estándar IEEE 802.1X, los protocolos RADIUS y TACACS+, además se configurará un servidor AAA el que estará vinculado al directorio activo de Windows el mismo que será configurado por el departamento de TI de PIL S.A.

1.6 Seguridad de la red

La seguridad de la red garantiza en cierta medida que determinadas personas, no puedan leer o modificar la información dirigida a destinatarios específicos, como tampoco se permite el acceso a servicios remotos no autorizados. (Plasencia Bedón, 2012).

Los problemas de seguridad de las redes pueden dividirse en 3 áreas interrelacionadas que son la: confidencialidad, validación de identificación y control de integridad.

- La confidencialidad, tiene que ver con mantener la información fuera del alcance de los usuarios no autorizados.
- La validación de identificación, se encarga de determinar con quién se ha establecido comunicación, antes de revelar información de la red.
- El control de integridad: se asegura de que un mensaje enviado no fue modificado en la ruta hacia su destinatario final, validando que los datos recibidos fueron los exactamente enviados.

La información generada y con la que trabajan las organizaciones es confidencial, por lo que se deben tomar medidas preventivas para salvaguardar dichos datos, para llevar a cabo este fin, existen dos soluciones complementarias, la seguridad física y la seguridad lógica.

1.6.1 Seguridad física

Para proteger los datos que se almacenan y transportan a través de una red de comunicaciones, los administradores de red reconocen la necesidad de implementar un sistema de seguridad física como una solución complementaria para lograr este propósito.

La seguridad física de la red consiste en la aplicación de procedimientos de control tales como medidas de prevención y detección de amenazas a los recursos o a la información confidencial.

Tiene como principal objetivo prevenir la acción de un atacante que intente acceder físicamente a la sala de operaciones o al lugar donde están instalados los equipos de red, dentro de los cuales se encuentra almacenada la información confidencial de un determinado establecimiento, protegiendo el área donde se encuentran ubicados dichos dispositivos con la ayuda de sistemas de control de acceso y cámaras de seguridad, impidiendo así que cualquier intruso provoque daños en la información e infraestructura de la red. (Internet society, 2012).

1.6.2 Seguridad lógica

Consiste en tomar medidas para prevenir o detectar accesos no autorizados a la red, a través de la utilización de ciertos equipos que vinculados con protocolos y políticas de seguridad, permitiendo resguardar el acceso seguro únicamente a los usuarios autorizados.

Para controlar el acceso de usuarios a una red y sus respectivos permisos dentro de la misma, se utilizan algunos procedimientos que están implementados en determinados equipos que conforman la topología de red, tales como el servidores AAA (Autenticación, Autorización y Auditoria), Servidores de Directorio Activo, Switchs y además de la limitaciones de servicios y recursos determinadas por políticas de seguridad de la red. (Internet society, 2012).

1.7 ¿Qué es un servidor?

Con la creación de las redes informáticas, la necesidad de intercambiar información a grandes distancias y con grandes cantidades de personas fue incrementándose. Para dar solución a este inconveniente fue inventado el servidor que es básicamente una computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la misma. (Lescano Rodríguez, 2009).

El servidor es una aplicación en ejecución que está al servicio de los usuarios, puede estar implementado en una PC (Computador Personal), común o a su vez existen equipos con mayores prestaciones, que se encuentran diseñados para cumplir la función de servidor. (Lescano Rodríguez, 2009).

Por lo general suelen estar situados en centros de datos para proveer servicios o todo tipo de información desde archivos de texto, video, audio, imágenes, emails, aplicaciones, programas, consultas a bases de datos que son requeridas por ciertos clientes (personas, o también pueden ser otros dispositivos como ordenadores, móviles, impresoras). Es aplicable tanto a un software como a un hardware, depende de la aplicación para la cual se vaya a utilizar el mismo. (Lescano Rodríguez, 2009).

Entre algunos de los servidores que se pueden encontrar son: servidores WEB, DNS (Sistema de Nombres de Dominio), FTP (Protocolo de Transferencia de archivos), PROXY, AAA (Autenticación, Autorización y Auditoria) y LDAP (Protocolo de Acceso Ligero a Directorios). (Lescano Rodríguez, 2009).

1.8 Servidor AAA

Permite a un usuario mediante sus credenciales (usuario y contraseña) acceder a una red corporativa de comunicaciones, siempre y cuando se encuentre registrado en la base de datos (Directorio activo). De esta manera previene el acceso de personas no autorizadas a la red, limitando quién y qué recursos específicos, pueden ser utilizados una vez que se otorga el acceso a la misma.

La sigla AAA surge de las abreviaciones en inglés, Authentication, Authorization y Accounting, que en español se traduce como (Autenticación, Autorización y Auditoría). Lo que realiza este servidor es controlar a quién se le permite tener acceso a la red (autenticación), qué pueden hacer mientras están allí (autorización) y registrar qué acciones realizaron al acceder a la red (auditoría).

A continuación se definirá cada uno de los servicios que provee el servidor AAA. (Cicenia Cárdenas & Vásconez Núñez, 2011).

1.8.1 Autenticación

El servicio de autenticación es el proceso por el que una entidad que es el cliente prueba ser quien dice ser, para esto el usuario presenta sus credenciales ante el servidor de autenticación para que sean verificadas y por lo tanto permitir o no el acceso a la red y a sus recursos.

Un tipo habitual de credencial o identidad es el uso de una contraseña (o password) que junto al nombre de usuario que permite acceder a determinados recursos. Otros tipos más avanzados de credenciales son los certificados digitales. (RedUSERS, 2013).

1.8.2 Autorización

Una vez que el usuario fue autenticado, este servicio determina los recursos de la red, operaciones, ancho de banda, accesos a los archivos, servicios, aplicaciones y permisos para realizar algún tipo de configuración en la red, que dicho usuario puede efectuar. Esto se basa en los privilegios específicos que el sistema le provee. (RedUSERS, 2013).

1.8.3 Auditoría

Es la capacidad del sistema para reconocer cierto tipo de eventos ejecutados en la red, por medio de registros secuenciales que permiten determinar las acciones realizadas por una entidad activa en una red, es decir, lo que hace un usuario, los recursos a los que accede, la cantidad de tiempo que mantiene una sesión activa y cualquier cambio que realice mientras este dentro de la misma.

Toda esta información es utilizada para la correcta administración de los recursos, la planificación de la capacidad y también para la recopilación de información en caso de que un incidente la requiera. (RedUSERS, 2013).

1.9 Protocolos AAA

Los protocolos AAA más conocidos y utilizados por los administradores de TIC para efectuar el control de acceso a la red de usuarios, ya sea a través de la red cableada o inalámbrica, son el protocolo **RADIUS**, **TACACS** y su sucesor, **TACACS+**.

TACACS+ y RADIUS son protocolos de administración de acceso seguro de red, pero cada uno tiene diferentes capacidades y funcionalidades. La elección de uno de estos protocolos depende de las necesidades específicas de una determinada organización. (RedUSERS, 2013).

1.9.1 Protocolo RADIUS

RADIUS es el acrónimo en inglés de (Remote Authentication Dial-In User Server), que es un protocolo AAA abierto con aplicaciones para el acceso a las redes y movilidad IP, trabaja tanto en situaciones locales y de roaming, generalmente usado para los registros de auditoría.

El servidor de autenticación recibe la petición de acceso del usuario con sus credenciales para acceder a la red, por medio del protocolo **PPP** (Protocolo Punto a Punto), a través del Network Access Server (NAS), quien redirige la petición al servidor de autenticación que opera con el protocolo RADIUS.

El servidor de autenticación comprueba que las credenciales sean correctas mediante otros mecanismos de autenticación como **PAP** (Protocolo de Autenticación de Password), **CHAP** (Protocolo de Autenticación por Desafío Mutuo), o **EAP** (Protocolo de Autenticación Extensible). En caso de ser aceptadas se autoriza al usuario acceder a la red y recibir sus respectivos parámetros, a través del servicio de DNS, tales como una dirección IP (Protocolo de Internet).

El protocolo RADIUS encripta las contraseñas durante la transmisión, incluso con el Protocolo de Autenticación de Contraseñas PAP (Password Authentication Protocol), usando una operación bastante compleja que involucra la dispersión a

través de Message Digest 5 (MD5) y una contraseña compartida. Sin embargo, el resto del paquete se envía en texto plano.

RADIUS utiliza el puerto UDP (User Datagram Protocol), 1645 o 1812 para la autenticación y el puerto UDP 1646 o 1813 para los registros de auditoría. Este protocolo combina los servicios de autenticación y autorización en un solo proceso, es decir que cuando el usuario se autentica, también está autorizado. (Plasencia Bedón, 2012).

1.9.2 Protocolo TACACS+

TACACS es el acrónimo en inglés de (Terminal Access Controller Access Control System), es un protocolo de la propiedad de Cisco que sirve para la autenticación remota. Posteriormente surgió TACACS+, este es una mejora de su antecesor y que pese a su nombre similar es completamente nuevo y no es compatible con su versión anterior.

TACACS+ proporciona servicios AAA separados, al separar este tipo de servicios se obtiene mayor flexibilidad en la implementación, ya que realiza la autorización y registros de auditoría con un método, mientras utiliza otro para la autenticación.

La operación normal de TACACS+ es cifrar todo el cuerpo del paquete para conexiones más seguras, usa el puerto 49 con TCP (Protocolo de Control de Transmisión) en la comunicación, además es soportado por Routers de la familia Small Business (Empresa Pequeña) de la serie 2900 y Servidores de Acceso de la serie 5.4. de Cisco.

El protocolo TACACS+ fue diseñado para ampliarse a medida que crecen las redes y adaptarse a las nuevas tecnologías en seguridad, mientras el mercado evoluciona debido a que trabaja con TCP, este protocolo es más escalable y adaptable al crecimiento, así como la congestión de las redes. (Cicenia Cárdenas & Vásconez Núñez, 2011).

1.9.3 Diferencias entre el protocolo RADIUS vs TACACS+

En la figura 1 se ilustran las principales diferencias que existen entre estos dos protocolos de seguridad de acceso.

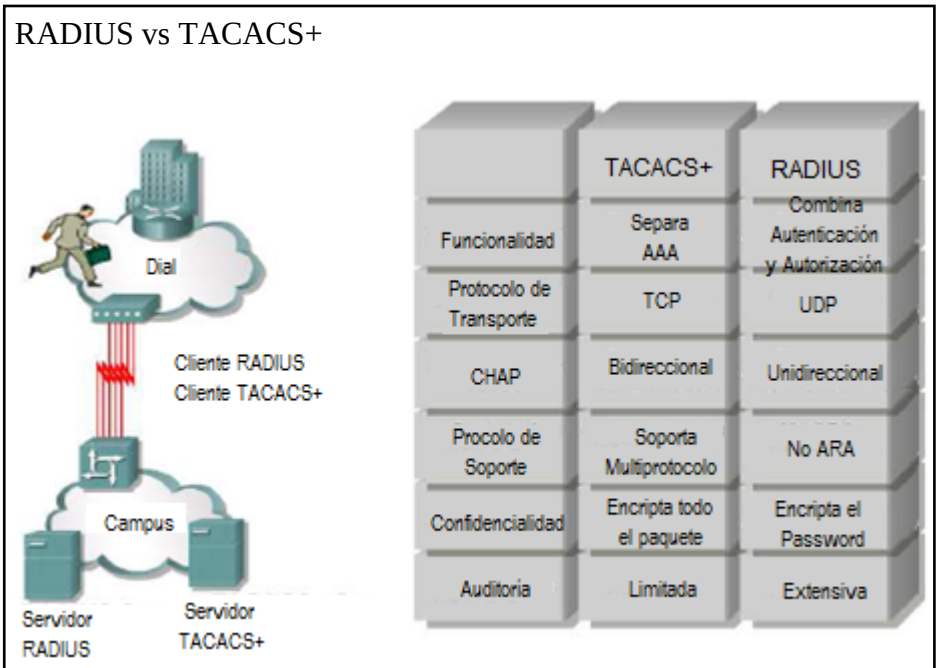


Figura 1. Diferencias entre los protocolos RADIUS y TACACS+
Elaborado por: Andrés Valdivieso.

1.10 Mecanismo para el acceso seguro a la red

El acceso seguro a la red se realiza mediante ciertos equipos como son el autenticador, el servidor AAA y la base de datos, estos están asociados entre sí para ejecutar procesos que han sido configurados para permitir tener un control de acceso en la red y una utilización correcta de sus recursos. En la figura 2 se ilustra y se explica cuál es el proceso de funcionamiento de una autenticación basada en servicios AAA.

1.10.1 Funcionamiento de la autenticación AAA

Procedimiento del sistema de autenticación AAA

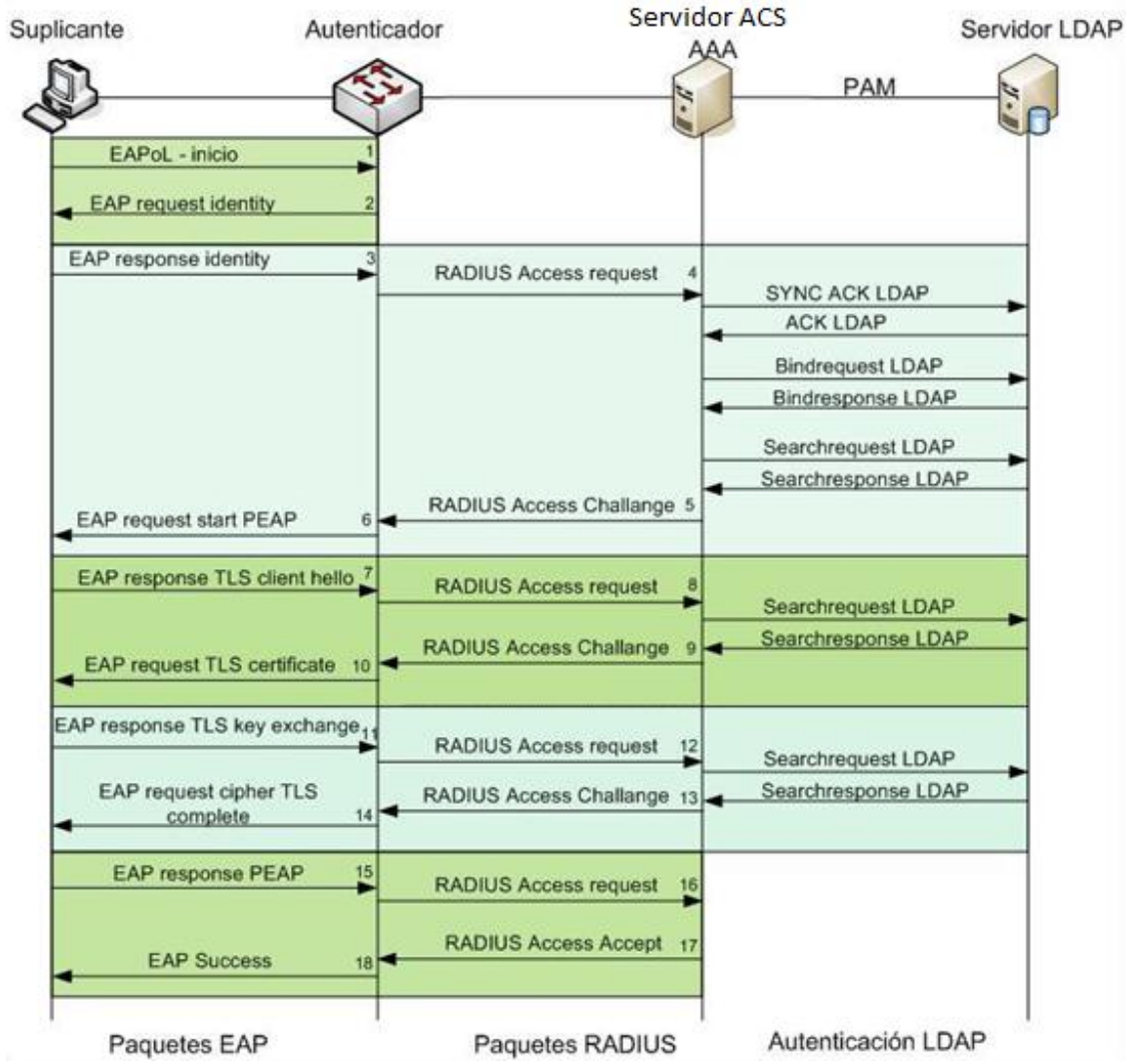


Figura 2. (Plasencia Bedón, 2012).

El de acceso a la red, mediante la autenticación del usuario a través de un servidor consta de los siguientes elementos:

- el suplicante (cliente),
- el autenticador (Switch o Access Point),
- el servidor autenticador,
- la base de datos.

La comunicación se establece cuando el suplicante envía una solicitud conjuntamente con sus credenciales hacia el equipo autenticador, este recibe la

información y realiza la petición al servidor de autenticación para la asignación de servicios de red que el suplicante solicita, el servidor de autenticación a su vez a través del protocolo LDAP consulta con el servidor de directorios si la información recibida concuerda con su base de datos, si el resultado es positivo el servidor de autenticación a través del equipo autenticador, permitirá el acceso al suplicante a los servicios de red requeridos.

En el caso de que las credenciales del suplicante no concuerden con la base de datos del servidor de directorios no le permitirá el acceso a los servicios de red al mismo.

A continuación se analiza este proceso a nivel de tramas.

1. El proceso de autenticación RADIUS, empieza desde que el suplicante solicita acceso a la red, enviando un mensaje EAPOL (Protocolo de Autenticación Extensible sobre LAN), al equipo autenticador. En la figura 3 se puede observar la trama de inicio EAPoL. (Plasencia Bedón, 2012).

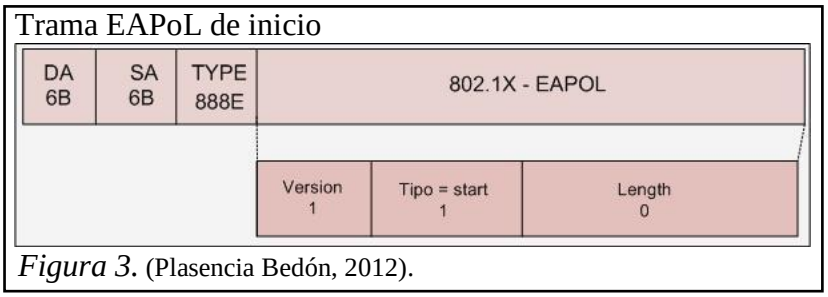


Figura 3. (Plasencia Bedón, 2012).

2. El autenticador recibe el mensaje de inicio y responde al suplicante con un mensaje de solicitud de identidad (EAP request identity) del usuario que intenta acceder a la red, en la figura 4 se muestra la trama EAP request identity. (Plasencia Bedón, 2012).

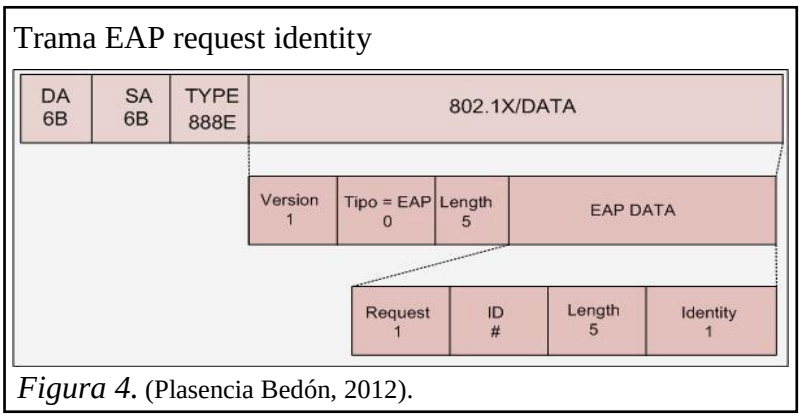


Figura 4. (Plasencia Bedón, 2012).

3. El suplicante envía su identidad de usuario en un mensaje EAP al autenticador (EAP response identity), en la figura 5 se muestra la trama EAP response identity. (Plasencia Bedón, 2012).

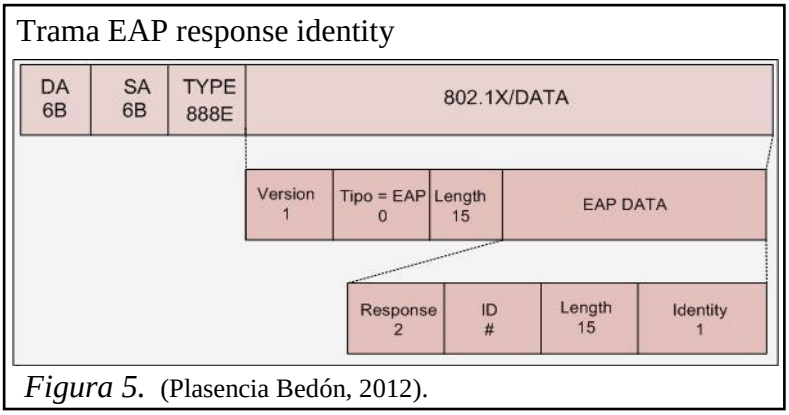


Figura 5. (Plasencia Bedón, 2012).

4. La trama EAP response identity llega al autenticador y es encapsulada en un mensaje RADIUS para ser enviada a través de este, al servidor RADIUS cuando le haga la petición de acceso a la red mediante un mensaje, (RADIUS access request), en la figura 6 se muestra la trama RADIUS access request. (Plasencia Bedón, 2012).

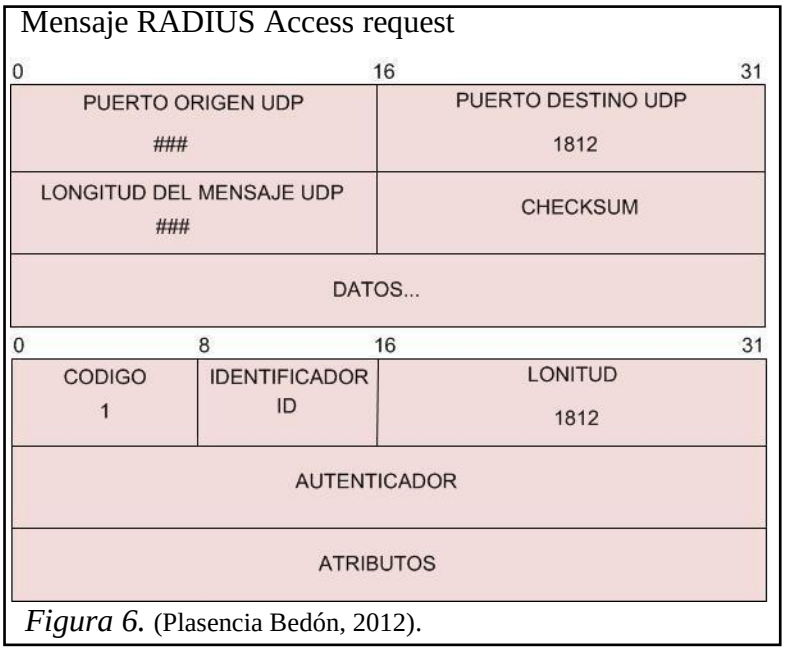


Figura 6. (Plasencia Bedón, 2012).

El mensaje RADIUS Access request llega al servidor RADIUS, para que las credenciales del usuario sean consultadas en la base de datos. A continuación se describe una consulta que le hace el servidor RADIUS a la base de datos:

La consulta que le hace el servidor RADIUS a la base de datos donde se encuentran registrados los usuarios que pueden tener acceso a la red y tener ciertos privilegios dentro de la red, lo realiza mediante conexiones TCP al puerto 389. Para que el servidor RADIUS pueda realizar consultas a la base de datos primero se autentica con las credenciales de la cuenta configurada en el módulo LDAP (Protocolo Ligero, Simplificado de Acceso a Directorios), de RADIUS (bindrequest/bindresponse) y luego se procede a realizar comandos de búsqueda para verificar la autenticidad del usuario (searchrequest/searchresponse). (Plasencia Bedón, 2012).

5. El servidor RADIUS envía una trama RADIUS Access-challenge para iniciar la negociación del método EAP que será utilizará para el establecimiento del canal seguro. En la figura 7 se muestra la trama RADIUS Challenge. (Plasencia Bedón, 2012).

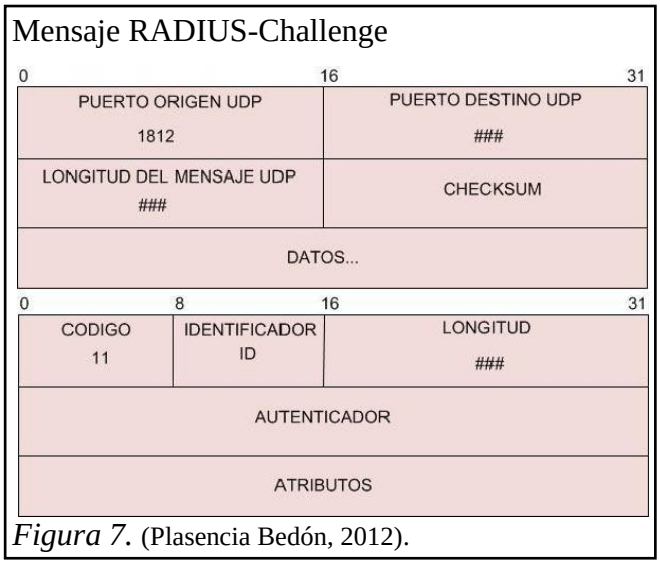


Figura 7. (Plasencia Bedón, 2012).

6. El autenticador envía al suplicante un EAP con petición para el establecimiento del canal seguro con EAP de tipo PEAP (Protocolo Protegido de Autenticación Extensible). En la figura 8 se muestra la trama PEAP. (Plasencia Bedón, 2012).

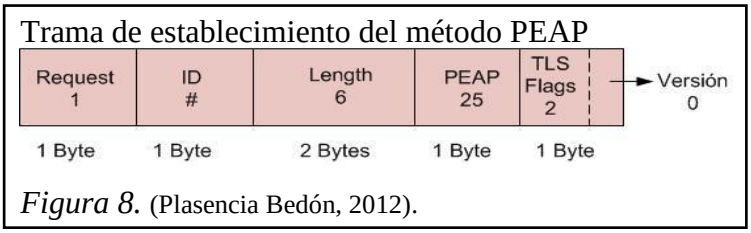


Figura 8. (Plasencia Bedón, 2012).

7. El suplicante lo que hace es negociar el método de conexión y envía al autenticador un EAP-Response de respuesta con el saludo (client-hello), para el establecimiento del canal TLS (Seguridad en la Capa de Trasporte). En la figura 9 se muestra la trama EAP Response. (Plasencia Bedón, 2012).

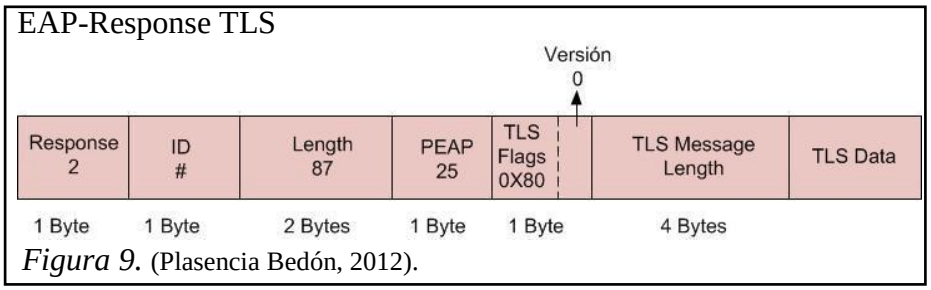


Figura 9. (Plasencia Bedón, 2012).

8. El autenticador encapsula el mensaje EAP-Response enviado por el suplicante en un mensaje RADIUS-Request para enviarlo al servidor RADIUS. (Plasencia Bedón, 2012).

9. EL servidor RADIUS verifica el mensaje que fue enviado por el usuario y le responde con su certificado en un mensaje RADIUS-Challenge. El mensaje contiene un server hello + server certificate + server hello done. (Plasencia Bedón, 2012).

10. "El autenticador recibe el mensaje RADIUS y lo reenvía el certificado del servidor RADIUS al usuario en un EAP-request TLS de credencial del usuario". (Plasencia Bedón, 2012). En la figura 10 se muestra la trama EAP Request.

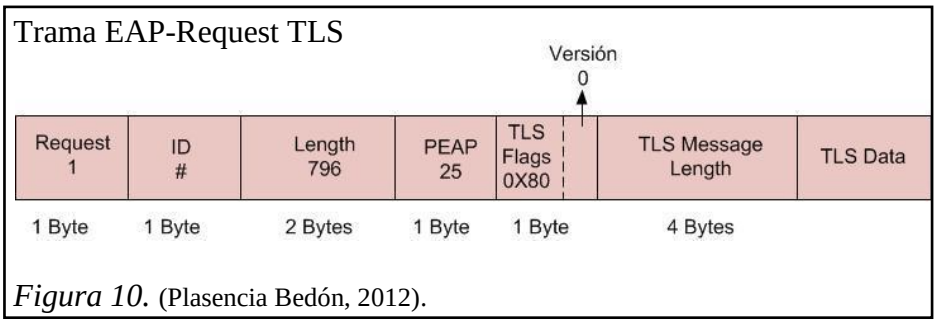


Figura 10. (Plasencia Bedón, 2012).

11. "El usuario responde con un mensaje EAP intercambiando la contraseña en el canal cifrado. El mensaje EAP-response TLS contiene el client key Exchange, change cipher spec y encrypted handshake message". (Plasencia Bedón, 2012).

12. “La trama EAP-Response TLS se encapsula en un mensaje RADIUS-Request, para enviarle al servidor RADIUS, el mensaje llega encriptado con la contraseña del usuario y es verificada en la base de datos LDAP”. (Plasencia Bedón, 2012).

13. El servidor puede tener dos respuestas válidas dependiendo del caso:

    - Si las credenciales del usuario son correctas, el servidor RADIUS responde con un mensaje RADIUS-Challange para finalizar el establecimiento del canal TLS. (Plasencia Bedón, 2012).
    - Caso contrario, si las credenciales no son correctas, el servidor RADIUS rechaza la conexión con un mensaje RADIUS-Reject y por lo tanto el puerto del Switch al que se conecta el usuario se pone en estado down. (Plasencia Bedón, 2012).

14. “El autenticador recibe un mensaje RADIUS-Challange desde el servidor RADIUS con la finalidad de establecer un canal TLS y le envía al usuario un EAP-Request de canal cifrado completo”. (Plasencia Bedón, 2012).

15. El usuario solicita acceso a la red enviando un mensaje EAP-PEAP de respuesta. (Plasencia Bedón, 2012).

16. La solicitud de acceso a la red desde el autenticador es enviada al servidor RADIUS mediante un mensaje RADIUS-request. (Plasencia Bedón, 2012).

17. El servidor RADIUS responde al autenticador con un mensaje de RADIUS-ACCEPT a la petición de acceso a la red que fue recibida, en la figura 11 se muestra la trama de RADIUS Accept. (Plasencia Bedón, 2012).

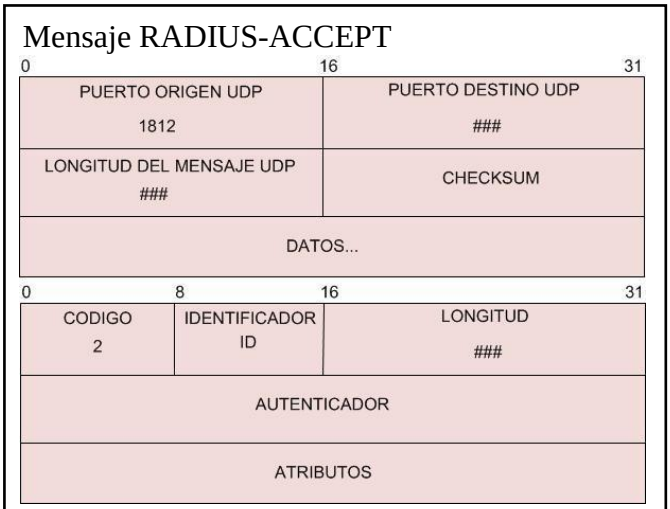


Figura 11. (Plasencia Bedón, 2012).

18. El autenticador envía un mensaje EAP-Succsess al usuario y este ya se encuentra habilitado para usar los recursos de la red, en la figura 12 se muestra la trama EAP Success. (Plasencia Bedón, 2012).

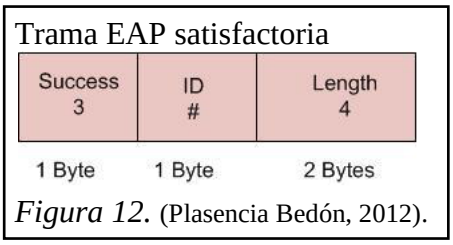


Figura 12. (Plasencia Bedón, 2012).

1.11 Estándar IEEE 802.1X

El estándar IEEE 802.1X fue aprobado en junio de 2001, este define el control de acceso a la red basado en puertos, facilita la autenticación y autorización de dispositivos que están conectados a un puerto de LAN (red cableada), a través de redes inalámbricas y a través de puertos virtuales, ya sea para permitir o denegar el acceso a dicho puerto. (Lescano Rodríguez, 2009).

El proceso de autenticación 802.1X tiene 3 componentes principales:

1. El Autenticador.- Este puede ser un Switch o un punto de acceso, su función es forzar el proceso de autenticación y enrutar el tráfico. (Lescano Rodríguez, 2009).

2. El Suplicante.- Este es el cliente, es decir el usuario que por medio de un software solicita tener acceso a la red. (Lescano Rodríguez, 2009).

3. El Servidor de autenticación.- Es el que procesa la autenticación de las credenciales del usuario. (Lescano Rodríguez, 2009).

1.11.1 Proceso de autenticación con 802.1X

En la figura 13 se ilustra los elementos de red y se describe el proceso que realiza el estándar 802.1X para la autenticación. (Lescano Rodríguez, 2009).

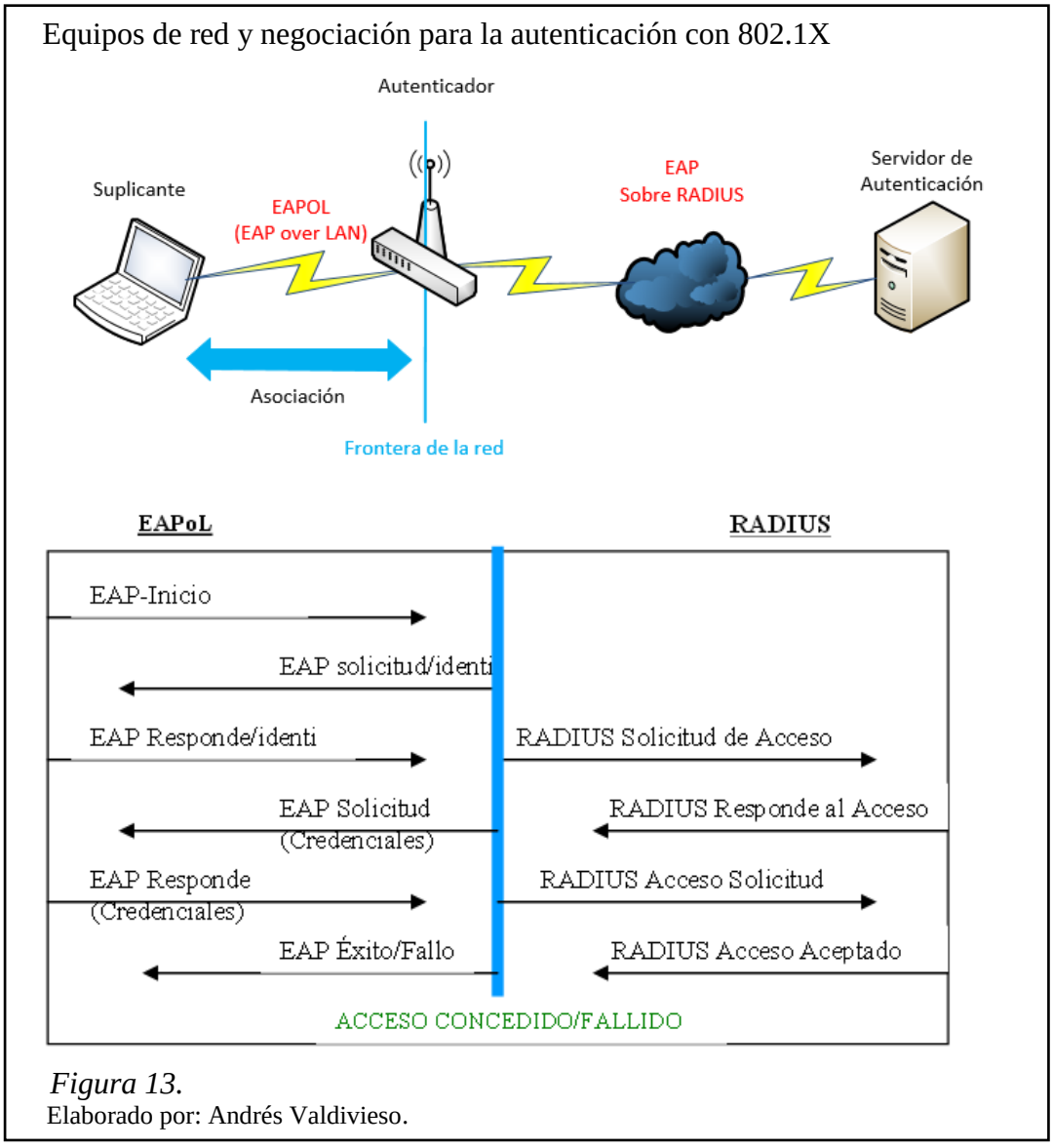


Figura 13.
Elaborado por: Andrés Valdivieso.

1. El suplicante inicia la comunicación enviando un mensaje en un paquete EAP-start hacia el autenticador, solicitando tener acceso a la red. (Lescano Rodríguez, 2009).

2. El autenticador le responde con un EAP-resquest identy a través de su puerto pidiendo las credenciales del usuario.
   EAP es el "Protocolo de Autenticación Extensible" es la encapsulación correspondiente al protocolo de autenticación de red local. (Lescano Rodríguez, 2009).

   El servidor de autenticación que se encuentra en la red cableada, pone al puerto en estado no autorizado hasta que sean verificadas las credenciales del usuario mediante el servidor de autenticación, el autenticador bloquea cualquier tipo de tráfico como paquetes HTTP (Protocolo de Transferencia de Híper Texto), DHCP (Protocolo de Configuración Dinámica de Host), y POP3 (Protocolo de Oficina Postal). (Lescano Rodríguez, 2009).

3. El suplicante le responde al autenticador con las credenciales. (Lescano Rodríguez, 2009).

4. El autenticador reenvía las credenciales al servidor de autenticación. (Lescano Rodríguez, 2009).

5. El servidor de autenticación le responde al autenticador con un mensaje indicando si las credenciales fueron autenticadas o no. (Lescano Rodríguez, 2009).

6. Si las credenciales son las correctas, el autenticador abre su puerto para permitir otro tipo de tráfico, caso contrario no lo hará. (Lescano Rodríguez, 2009).

El estándar 802.1X utiliza el protocolo de autenticación EAP (Extensible Authentication Protocol), este admite distintos métodos de autenticación como certificados, tarjetas inteligentes, NTLM (NT LAN Manager), KERBEROS y LDAP. El protocolo EAP actúa como intermediario entre un solicitante y un motor de validación permitiendo la comunicación entre ambos. (Lescano Rodríguez, 2009).

Existen múltiples tipos de protocolos EAP, algunos son estándares y otros son soluciones propietarias de empresas, entre los tipos de EAP están:

1. EAP-TLS.- Es un sistema de autenticación fuerte que se basa en certificados digitales, tanto del cliente como del servidor, es decir, requiere una configuración PKI (Public Key Infraestructure) en ambos extremos. TLS (transport Layer Security) es el nuevo estándar que sustituye a SSL (Secure Socket Layer). (Lescano Rodríguez, 2009).

2. EAP-TTLS.- Es un sistema de autenticación que se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir que se crea un túnel mediante TLS para transmitir el nombre de usuario y la contraseña. A diferencia de EAP-TLS sólo requiere un certificado de servidor. (Lescano Rodríguez, 2009).

3. PEAP.- El significado de PEAP corresponde con Protected EAP y consiste en un mecanismo de validación similar a EAP-TTLS, basado en usuario y contraseña también protegidos. (Lescano Rodríguez, 2009).

1.12 LDAP

LDAP es el acrónimo en inglés de (Lightweight Directory Access Protocol), en español Protocolo ligero de acceso a directorios, es un conjunto de protocolos abiertos utilizados para acceder a la información almacenada a través de la red.
Consolida la información de forma jerárquica y categorizada, donde pueden incluirse nombres, directorios y números telefónicos dentro del servidor. (Red Hat Enterprise Linux, 2012).

Este tipo de servidor es capaz de propagar su consulta a otros servidores LDAP del mundo, proporcionando un repositorio de información ad-hoc global. (Red Hat Enterprise Linux, 2012) .

LDAP es un protocolo modelo cliente/servidor, en el que el servidor puede usar una variedad de bases de datos para guardar un directorio. Cuando una aplicación cliente

LDAP se conecta a un servidor LDAP puede consultar un directorio o intentar modificarlo. Si es una consulta, el servidor puede contestarla localmente o puede dirigir la consulta a un servidor LDAP que tenga la respuesta y si la aplicación cliente está intentando modificar la información en un directorio LDAP, el servidor verifica que el usuario tenga permisos para efectuar el cambio y después añade o actualiza la información. (Red Hat Enterprise Linux, 2012).

Una de las ventajas de utilizar LDAP, es que se puede consolidar información para toda una organización dentro de un repositorio central. Por ejemplo, en vez de administrar listas de usuarios para cada grupo dentro de una organización, se puede usar LDAP como directorio central, accesible desde cualquier parte de la red. (Red Hat Enterprise Linux, 2012).

LDAP soporta la Capa de conexión segura (SSL) y la Seguridad de la capa de transporte (TLS). (Red Hat Enterprise Linux, 2012).

1.13 Servidor de control de acceso de red

1.13.1 Introducción

El servidor de control de acceso Cisco (ACS) provee servicios AAA a los dispositivos que estén conectados a la red como Routers, servidores de acceso, PIX, concentradores VPN. Ofrece a una infraestructura control de acceso, escalabilidad y rendimiento alto, además de ser un componente importante de la arquitectura Identity Based Networking Services (IBNS) de Cisco. (Cicenia Cárdenas & Vásconez Núñez, 2011).

El ACS utiliza los protocolos RADIUS, TACACS+ y su antecesor, utiliza un nivel de seguridad básico que es Password Authentication Protocol (PAP), con el que los usuarios se autentican una sola vez, el Challenge Handshake Authentication Protocol (CHAP) permite un nivel de seguridad mayor, con contraseñas encriptadas cuando el cliente se comunica con el NAS. (Cicenia Cárdenas & Vásconez Núñez, 2011).

Además combina la autenticación, el acceso de usuario o administrador y el control de políticas, para mayor flexibilidad y movilidad del usuario. Con una base de datos central para todas las cuentas de usuario, el ACS centraliza el control de los privilegios de usuario y los distribuye a cientos o miles de puntos de acceso a lo largo de la red. (Cicenia Cárdenas & Vásconez Núñez, 2011).

1.13.2 Autenticación y bases de datos de usuarios

El ACS soporta métodos modernos para ofrecer más seguridad basándose en tecnologías como OTP (One – Time Passwords), incluyendo PAP para el acceso de nodos remotos. (Cicenia Cárdenas & Vásconez Núñez, 2011).

Además autoriza el uso de la red basándose en un grupo de parámetros de una base de datos de usuario. Todos los usuarios autenticados por el ACS o bases externas tienen una cuenta en la base de datos de usuario ACS. A menos de que esté configurado para la autenticación de usuarios con una base de datos externa, se usa la base de datos de ACS para la autenticación. (Cicenia Cárdenas & Vásconez Núñez, 2011).

1.13.3 Funcionalidades del ACS de CISCO

"El ACS de Cisco tiene muchas funciones de alto rendimiento y escalabilidad, entre las que se presentan:" (Cicenia Cárdenas & Vásconez Núñez, 2011).

- **Facilidad de uso.-** La interfaz de usuario basada en web simplifica y distribuye la configuración para perfiles de usuario, perfiles de grupo y configuración.
- **Escalabilidad.-** Tiene la capacidad de la creación y almacenamiento de usuarios y grupos en su base de datos local, así como importar estos datos de base de datos remotas brindando la posibilidad de incrementar la capacidad del número de perfiles con los que puede trabajar.

- **Extensibilidad.-** Soporta la autenticación de perfiles de usuario que se almacenan en servidores LDAP, de diversas marcas líderes en servicios de directorios.
- **Administración.-** Cuenta con la capacidad de proveer diferentes niveles de acceso, creación y gestión de grupos, con la finalidad de facilitar el control del cumplimiento y cambios de las políticas de seguridad propuestas por el administrador de red.
- **Soporte a Terceros.-** Ofrece soporte de servidor token a cualquier empresa de contraseñas de una sola vez OTP (one-time password) que proporciones una interfaz RADIUS que se atenga a las RFC, como RSA, PassGo, Secure Computing, Active Card, Vasco o Crypto Card.
- **Control.-** Proporciona cuotas dinámicas para restringir el acceso en base a la hora, el uso de la red, el número de sesiones iniciadas y el día de la semana.

1.14 Identidad basada en servicios de red

La Identidad Basada en Servicios de Red (IBNS) es una solución moderna e innovadora de seguridad. Esta solución unificada de Cisco proporciona la base para la autenticación, control de acceso y aplicación de políticas en el borde de la red, para esto incluye varios dispositivos para permitir la autenticación, control de acceso y aplicación de políticas de usuarios (basados en identidad) para acceder de forma segura (conectividad) a la red y sus recursos, el figura 14 se puede apreciar la solución IBNS. (Lescano Rodríguez, 2009).

Permite a las empresas el manejo seguro de la movilidad de sus empleados (acceso remoto), como la asignación de los usuarios a su correspondiente segmento de red basados en su identidad. También permite que los clientes refuercen su seguridad al tiempo en que aumenta la productividad del usuario, reduciendo los costos de operación, mejorando la visibilidad y abordando el cumplimiento. (Lescano Rodríguez, 2009).

Uno de los elementos centrales de la solución IBNS es el uso de la tecnología IEEE 802.1X. Los avances recientes de la IBNS tienen que ver con la solución de la

usabilidad y la capacidad de despliegue de 802.1X mediante la introducción de una innovadora estrategia por etapas y basada en escenarios de implementación que puede utilizar para desplegar IBNS con un impacto mínimo a los usuarios finales. (Cicenia Cárdenas & Vásconez Núñez, 2011).

Ingreso basado en servicios de red (IBNS) de CISCO

Figura 14. (Lescano Rodríguez, 2009).

1.14.1 Funcionalidades del IBNS

El IBNS se basa en estándares de seguridad de puerto al igual que el estándar IEEE 802.1X y el protocolo EAP (Extensible Authentication Protocol), este extiende la seguridad desde el perímetro de la red a todos los puntos de conexión dentro de la LAN. Con esta nueva arquitectura, pueden desplegarse nuevas políticas de control, como cuotas por usuario y asignación de las VLAN y ACL. Esto es posible gracias a las funciones extendidas de los Switches y puntos de acceso inalámbricos que los habilitan para consultar al ACS a través del protocolo RADIUS. (Cicenia Cárdenas & Vásconez Núñez, 2011).

Esta solución ayuda a las empresas para que puedan gestionar mejor la movilidad de los empleados, permite reducir los gastos de acceso a la red y aumentan la productividad global al tiempo que reduce los costos. (Cicenia Cárdenas & Vásconez Núñez, 2011).

1.14.2 Beneficios de la solución IBNS

"Mejora la capacidad del negocio sin comprometer la seguridad: las políticas están asociadas con los usuarios y no con los puertos físicos, que no solo ofrece a los usuarios una mayor movilidad, sino que también simplifica la administración de personal". (Cicenia Cárdenas & Vásconez Núñez, 2011).

Logra una mayor flexibilidad y movilidad: creación de perfil es el usuario y de grupo o con las políticas que definen las relaciones de confianza entre los usuarios y recursos de la red, facilita las opciones de autentificar, autorizar y dar cuentas a todos los usuarios de redes inalámbricas y cableadas. (Cicenia Cárdenas & Vásconez Núñez, 2011).

> Aumentar la eficiencia y administrar los costos: tener la flexibilidad necesaria para ofrecer acceso seguro a la red y proveedores cuando la política basada en la administración reduce el tiempo, la complejidad y el esfuerzo asociado a las técnicas de la protección en el control de acceso a los medios de comunicación. (Cicenia Cárdenas & Vásconez Núñez, 2011).

Los componentes que intervienen en esta solución IBNS de Cisco son:

- El cliente, por ejemplo: la PC,
- El intermediador, por ejemplo: el Switch, el WLC,
- El servidor AAA, por ejemplo: el ACS,
- El directorio activo, la base de datos (roles y perfiles).

En la figura 15 se ilustran el orden en que van conectados los componentes antes descritos.

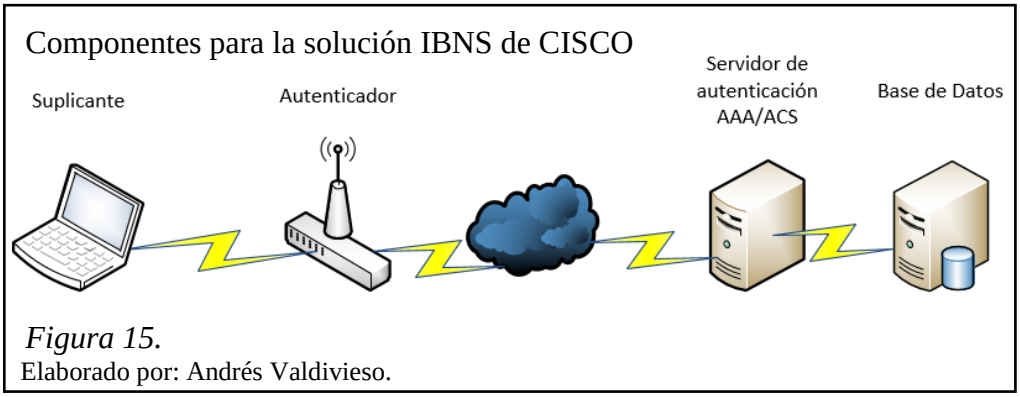


Figura 15.
Elaborado por: Andrés Valdivieso.

1.15 Método de autenticación por MAB

MAB viene de (MAC Authentication By Pass), este método de autenticación permite el control de acceso basado en puerto utilizando la dirección MAC (Control de Acceso al Medio), del punto final. Un puerto habilitado por MAB se puede activar de forma dinámica basada en la dirección MAC del dispositivo que se conecta a este. En la figura 16 se ilustra el comportamiento predeterminado de un puerto MAB habilitado. (CISCO, 2008).

Autenticación de un puerto por MAB

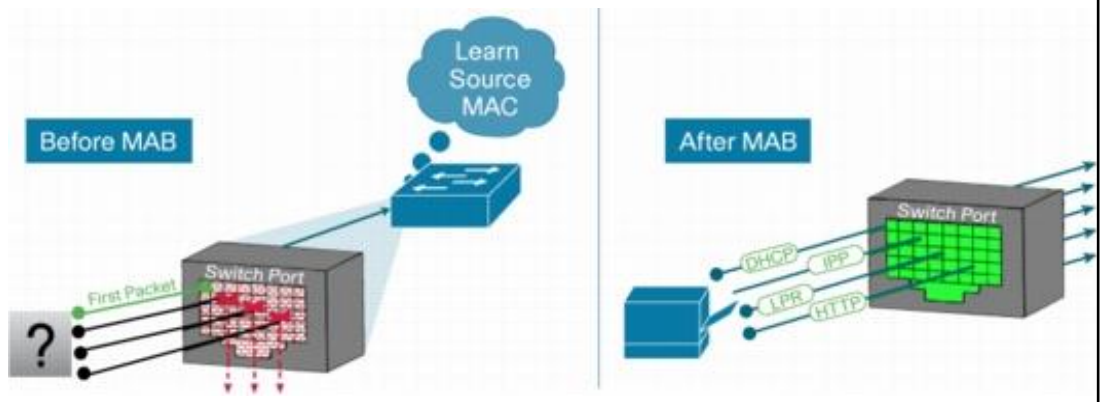


Figura 16. (CISCO, 2008).

Cuando se desconoce la identidad del punto final, el tráfico para este está bloqueado, se examina un solo paquete para aprender y autenticar la dirección MAC de origen, si el método de autenticación por MAB tuvo éxito, la identidad del punto final se conoce y se le permite todo el tráfico. El Switch realiza un filtrado de direcciones MAC para ayudar a garantizar que sólo permita enviar tráfico al punto final MAB-autenticado. (CISCO, 2008).

El método MAB valida las direcciones MAC que se almacenan en un sistema centralizado, por lo cual es de más fácil administración ya que se puede consultar mediante el protocolo RADIUS. (CISCO, 2008).

1.15.1 Secuencia funcional de alto nivel

La secuencia funcional de alto nivel, es la forma como funciona MAB cuando se configura como un mecanismo de reserva para 802.1X y se ilustra en la figura 17.

Si 802.1X no está activado, la secuencia es la misma, excepto que el MAB se inicia inmediatamente después de la relación en vez de esperar a que 802.1X tenga un tiempo de espera. (CISCO, 2008).

Secuencia funcional de alto nivel

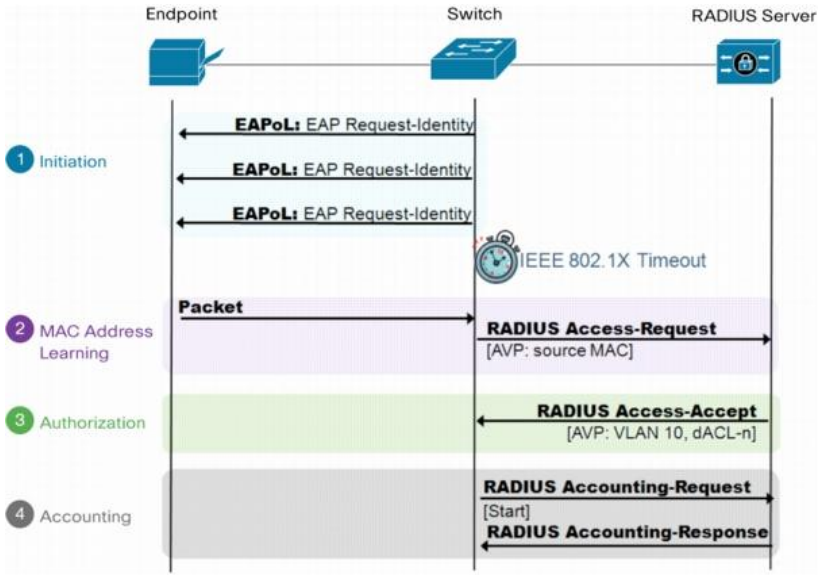


Figura 17. (CISCO, 2008).

1.15.2 Beneficios y limitaciones de MAB

1.15.2.1 Beneficios.- Algunos de los beneficios que ofrece MAB sobre las redes son (CISCO, 2008):

- **Visibilidad.-** MAB ofrece visibilidad de la red ya que el proceso de autenticación proporciona una forma de vincular la dirección IP de un dispositivo, direcciones MAC, switch, y el puerto. Esta visibilidad es útil para las auditorías de seguridad, análisis forense de redes, el uso de la red estadística, y resolución de problemas.

- **Control de acceso en el borde.-** MAB actúa en la capa 2, que le permite controlar el acceso a la red en el borde de acceso.
- **Repliegue o autenticación independiente.-** En una red que incluye tanto dispositivos que admiten y dispositivos que no soportan 802.1X, el MAB se puede implementar como un mensaje, o complementario mecanismo para 802.1X. Si la red no tiene ningún dispositivo compatible con 802.1X, el MAB puede ser desplegado como un mecanismo de autenticación independiente.
- **Autenticación de dispositivo.-** MAB puede utilizarse para autenticar dispositivos que no soportan 802.1X o que no tienen un usuario.

1.15.2.2 Limitaciones.- MAB tiene ciertas limitaciones sobre las redes que son (CISCO, 2008):

- **Base de datos MAC.-** Como requisito previo para el MAB, se debe tener una base de datos preexistente de direcciones MAC de los dispositivos que se permiten en la red. Creación y mantenimiento de una base de datos de direcciones MAC hasta la fecha es uno de los principales desafíos de la implementación del MAB.
- **Retraso.-** Cuando se utiliza como mecanismo de reserva para 802.1X, MAB realiza un tiempo de espera antes de la validación de la dirección MAC. Los retrasos en el acceso a la red pueden afectar negativamente a las funciones del dispositivo.
- **Sin autenticación de usuario.-** MAB puede utilizarse para autenticar sólo los dispositivos, y no los usuarios. Diferentes usuarios registrados en el mismo dispositivo tendrán el mismo acceso a la red.
- **Fuerza de autenticación.-** A diferencia de 802.1X, el MAB no es un método de autenticación fuerte. MAB puede ser derrotado por la suplantación de la dirección MAC de un dispositivo válido.
-

CAPÍTULO 2

SITUACIÓN ACTUAL DE LOS MECANISMOS PARA EL ACCESO SEGURO A LA RED CORPORATIVA DE LA EMPRESA PROYECTOS INTEGRALES DEL ECUADOR PIL S.A.

En este capítulo se detallará como actualmente se encuentra distribuida la infraestructura de los mecanismos para el acceso seguro a la red corporativa cableada e inalámbrica de la empresa Proyectos Integrales del Ecuador PIL S.A., tanto a nivel de topología física como de topología lógica.

2.1 Descripción del área física de Proyectos Integrales del Ecuador PIL S.A.

La empresa PIL S.A. tiene su agencia principal ubicada en la ciudad de Quito en la Av. Amazonas N39-82 y Pereira, edificio Casa Vivanco, tercer piso oficina 302, sexto piso oficina 601 y 602, séptimo piso oficina 701 (Recepción) y 702, octavo piso oficina 802.

Área física de Proyectos Integrales del Ecuador PIL S.A., Quito – Agencia Principal

Figura 18. Google Maps.

Con su sucursal ubicada en la Av. Amazonas N39-149 y José Arizaga, tercer piso.

Área física de Proyectos Integrales del Ecuador PIL S.A.,Quito – Sucursal

Figura 19. Google Maps.

Su bodega de equipos y materiales ubicada en la Av. Eloy Alfaro E5-52 y De Los Aceitunos.

Área física de Proyectos Integrales del Ecuador PIL S.A.,Quito – Bodega

Figura 20. Google Maps.

2.2 Topología física de la red

2.2.1 Data center

El data center de la red corporativa de Proyectos Integrales del Ecuador PIL S.A. está ubicado en la agencia principal, en el octavo piso, aquí se encuentran instalados los equipos principales que componen la infraestructura para el mecanismo de acceso seguro de red.

En él se encuentran instalados 2 racks:

- Rack de comunicaciones cerrado de 40UR (Rack Core).
- Rack de comunicaciones abierto de 45UR (Rack Acceso Piso 8).

Dentro de los cuales se tienen los siguientes equipos instalados descritos en las tablas 1 y 2.

2.2.1.1 Rack core

Tabla 1.
Distribución de rack de core

Item	Cantidad	Descripción	Número de Parte	Fabricante	Posición UR
1	1	Switch gigabit de 24 Puertos para rack de 1UR (Switch de Core).	2928-SFP PLUS	3COM	37
2	1	Servidor para rack de 1UR (SRV-01).	POWER EDGE R310	DELL	19
3	1	Servidor para rack de 2UR (SRV-04).	POWER VAULT NX3100	DELL	17 - 16
4	2	Servidor de piso (SRV-02, SRV-03).	PROLIANT ML110	HP	6

Nota.
Elaborado por: Andrés Valdivieso.

2.2.1.2 Rack acceso piso 8

Tabla 2.
Distribución de acceso piso 8

Item	Cantidad	Descripción	Número de Parte	Fabricante	Posición UR
1	1	Switch de 48 puertos para rack de 1UR.	SF200-48	Cisco	34
2	1	Switch de 48 puertos para rack de 1UR.	V1905-48	HP	29

Nota.
Elaborado por: Andrés Valdivieso.

2.2.2 Cuartos de equipos de comunicaciones (Acceso de red)

Dentro de la agencia principal, sucursal Jocay y bodega de materiales de PIL S.A., se encuentran ubicados los cuartos de comunicaciones, donde están instalados los equipos que conforman el mecanismo de acceso seguro de red.
A continuación se detallan los equipos que conforman la parte de acceso por cada edificio que conforma PIL S.A.

2.2.2.1 Agencia principal

En la agencia principal de PIL S.A. los cuartos de equipos de comunicaciones se encuentran ubicados en cada piso, en los cuales la empresa cumple sus funciones, a continuación se detallan los equipos instalados en los cuartos de comunicaciones mencionados anteriormente.

2.2.2.1.1 Tercer piso

Se encuentra instalado 1 rack:

- Rack de comunicaciones abierto de 24UR (Rack Acceso Tercer Piso).

Dentro del cual se tienen los siguientes equipos instalados descritos en la tabla 3.

Tabla 3.
Cuarto de comunicación, piso tres, oficina 302

Item	Cantidad	Descripción	Número de Parte	Fabricante	Posición UR
1	1	Switch de 48 puertos para rack de 1UR.	4500-50-PORT	3COM	20

Nota.
Elaborado por: Andrés Valdivieso.

2.2.2.1.2 Sexto piso

Se encuentra instalado 1 rack:

- Rack de comunicaciones abierto de pared de 16UR (Rack Acceso Sexto Piso).

Dentro del cual se tienen los siguientes equipos instalados descritos en la tabla 4.

Tabla 4.
Cuarto de comunicación, piso seis, oficina 601

Item	Cantidad	Descripción	Número de Parte	Fabricante	Posición UR
1	2	Switch de 48 puertos para rack de 1UR.	2250-SFP-PLUS	3COM	12 ; 4
2	1	Switch de 24 puertos para rack de 1UR.	2126-G	3COM	1

Nota.
Elaborado por: Andrés Valdivieso.

2.2.2.1.3 Séptimo piso

Se encuentra instalado 1 rack:

- Rack de comunicaciones abierto de 45UR (Rack Acceso Séptimo Piso).

Dentro del cual se tienen los siguientes equipos instalados descritos en la tabla 5.

Tabla 5.
Cuarto de comunicación, piso séptimo, oficina 701

Item	Cantidad	Descripción	Número de Parte	Fabricante	Posición UR
1	1	Switch de 48 puertos para rack de 1UR.	2250-SFP PLUS	3COM	41
2	1	Switch de 48 puertos para rack de 1UR.	4500-50-PORT	3COM	36
3	1	Switch de 48 puertos para rack de 1UR.	4210-52-PORT	3COM	31

Nota.
Elaborado por: Andrés Valdivieso.

2.2.2.2 Sucursal

En el edificio Jocay tercer piso, se ubica la sucursal de PIL S.A., aquí está ubicado el cuarto de equipos de comunicaciones, está instalado un rack abierto de 45UR, a continuación se detallan los equipos instalados dentro del rack mencionado anteriormente en la tabla 6.

2.2.2.2.1 Rack acceso sucursal

Tabla 6.
Cuarto de comunicación, piso tres, oficina 201

Item	Cantidad	Descripción	Número de Parte	Fabricante	Posición UR
1	1	Switch de 48 puertos para rack de 1UR.	4500-50-PORT	3COM	41

Nota.
Elaborado por: Andrés Valdivieso.

2.2.2.3 Bodega de materiales

En el interior de la Bodega de materiales de PIL S.A., se encuentra ubicado el cuarto de equipos de comunicaciones, donde está instalado un rack abierto de 45UR, a continuación se detallan los equipos instalados dentro del rack mencionado anteriormente en la tabla 7.

2.2.2.3.1 Rack acceso bodega

Tabla 7.
Cuarto de comunicación, bodega de materiales

Item	Cantidad	Descripción	Número de Parte	Fabricante	Posición UR
1	1	Switch de 48 puertos para rack de 1UR.	4500-50-PORT	3COM	38

Nota.
Elaborado por: Andrés Valdivieso.

2.2.3 Diseño de la LAN

El diseño de la red corporativa de PIL S.A. está basada en una topología de red tipo estrella, esto se ilustra en la figura 21.

Topología de la red PIL S. A. existente

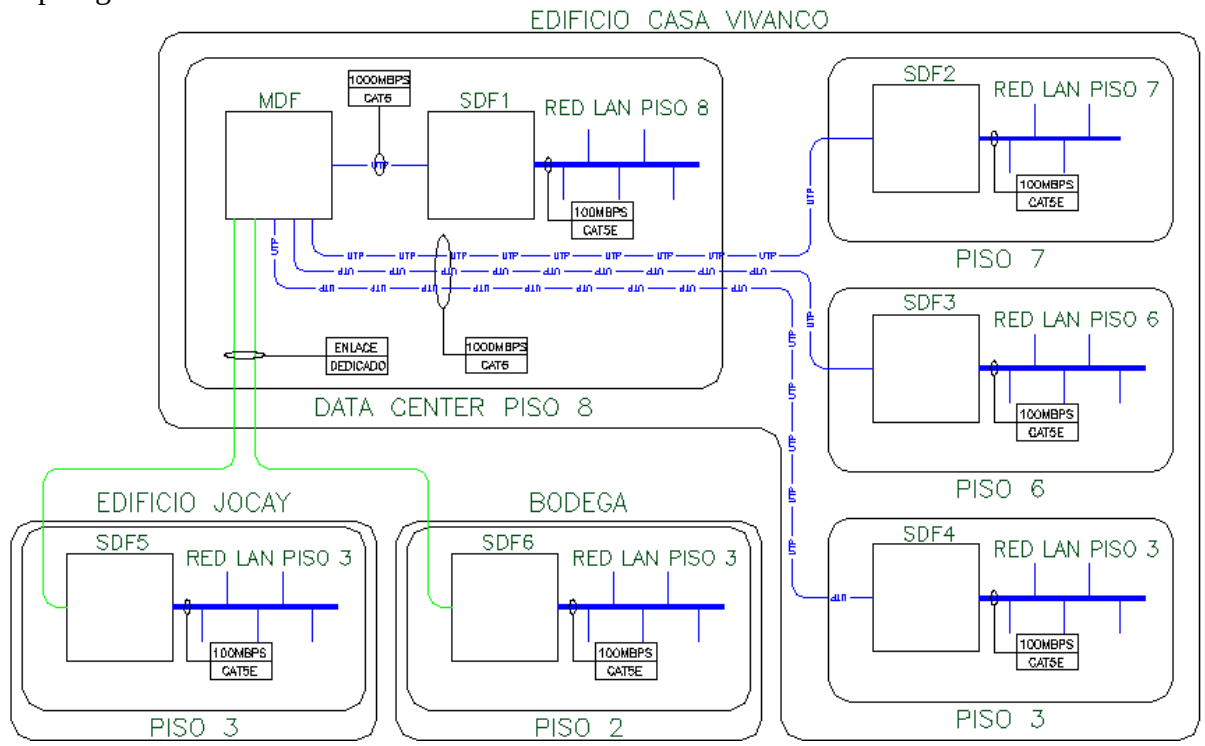


Figura 21.
Elaborado por: Andrés Valdivieso.

Está conformada por dos tipos de servicios de distribución:

1. MDF (Main Distribution Facility).
2. SDF (Sub-Distribution Facility).

Estos sistemas de distribución, se han instalado de acuerdo a las diferentes necesidades demandadas por los usuarios.

El MDF es el punto central de la red de PIL S.A., se encuentra ubicado en el data center desde donde se derivan los SDF ubicados en los demás sitios.

Los SDF están ubicados en cada uno de los pisos y lugares que se describen a continuación en la tabla 8.

Tabla 8.
Sistema de distribución SDF

SDF	Departamento	Locación
SDF1	Ingenierías	Edif. Vivanco – P3
SDF2	Servicios	Edif. Vivanco – P6
SDF3	Administrativo	Edif. Vivanco – P7
SDF4	Sistemas	Edif. Vivanco – P8
SDF5	Eléctrica	Edif. Jocay – P3
SDF6	Materiales	Bodega – P2

Nota.
Elaborado por: Andrés Valdivieso.

2.2.4 Comunicación de los servicios de distribución

Los servicios de distribución se encuentran interconectados de la siguiente manera:

Desde el MDF que se encuentra instalado en el Data Center ubicado en la agencia principal de PIL S.A. se derivan los enlaces hacia los SDF ubicados en los diferentes departamentos y lugares y como se detalló en la tabla 8.

La interconexión entre estos diferentes tipos de distribución se realiza por medio de cable UTP Categoría 6 (cableado vertical) con una configuración Etherchannel, en el caso de la agencia principal.
Para integrar la sucursal y la bodega se utilizan enlaces dedicados por medio de ISP autorizados.
La conexión de los puntos de voz y datos (cableado horizontal) hacia los patch panels de cada rack de acceso, se realiza por medio de cable UTP categoría 5E. En la figura 22 se ilustra la conexión de todos los equipos de red.

Comunicación de los equipos de red

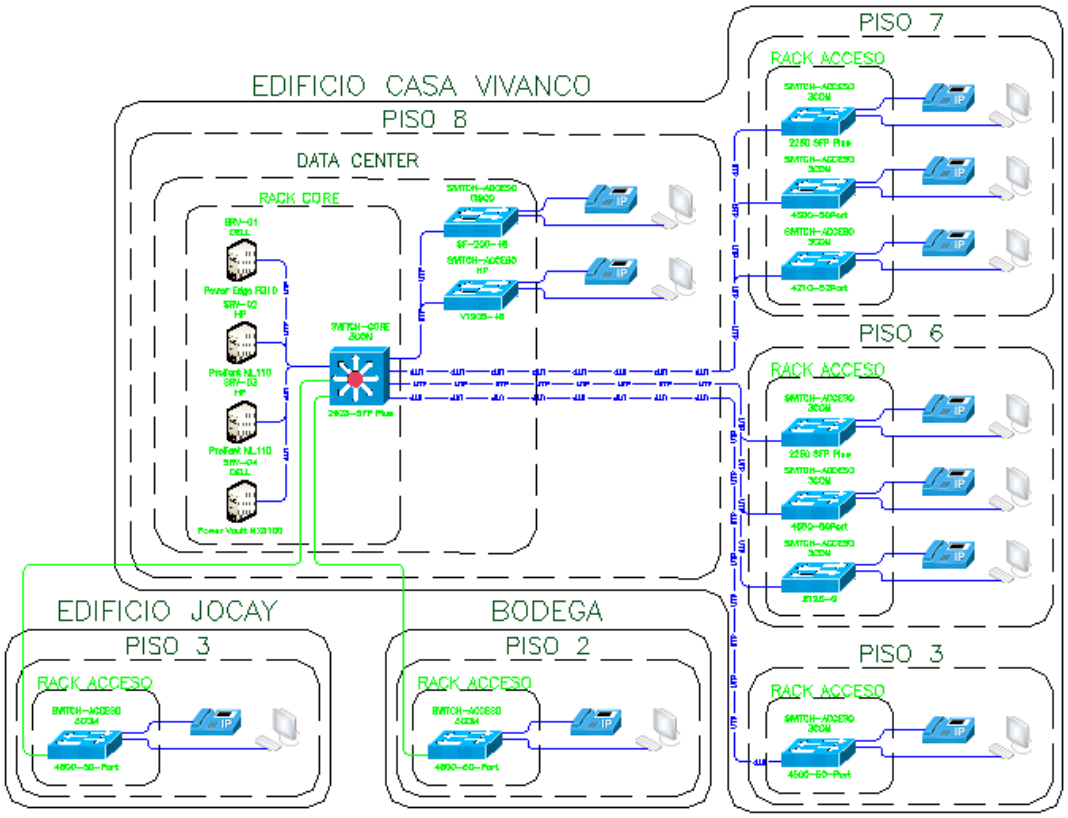


Figura 22.
Elaborado por: Andrés Valdivieso.

2.2.5 Dispositivos que conforman la WLAN

Los dispositivos que integran la WLAN se encuentran ubicados únicamente en el séptimo piso de la agencia principal de PIL S.A., donde se encuentra las oficinas de los gerentes general y administrativo de la empresa, ya que solo ellos tienen acceso a este servicio.

Está conformada por dos Access Point los cuales brindan el servicio de red inalámbrica, mismos que están directamente conectados hacia el primer Switch de acceso de este piso, especificado en la tabla 5.

A continuación se detallan los Access Point que brindan el servicio de red inalámbrica en PIL S.A.

- 2 Access Point, marca TP-LINK, modelo TL-WA901ND.

2.3 Topología lógica de la red

2.3.1 Redes

Dentro del Switch Core se encuentran configuradas 5 VLAN, las mismas que permiten tener un tipo de acceso específico y distribuido de acuerdo a la necesidad de cada usuario en la red, donde las VLAN de Acceso están configuradas estáticamente a cada puerto dependiendo del servicio que este requiera.

Las VLAN que se encuentran configuradas en el Switch de Core se detallan en la tabla 9.

Tabla 9.
VLAN creadas en Switch de core

VLAN	Nombre	Status
0	DEFAULT	Active
1	TRUNK	Active
5	DATOS	Active
8	VOZ	Active
10	WIFI	Active

Nota.
Elaborado por: Andrés Valdivieso.

2.4 Mecanismos de acceso seguro a la red

Para proteger la información generada por PIL S.A., se utilizan dos mecanismos de acceso seguro de red complementarios, tanto a nivel de red local como de Internet.

2.4.1 Acceso seguro red local

El dispositivo principal para el funcionamiento del mecanismo de acceso seguro a la red local de PIL S.A. es el servidor SRV-01(HP Proliant ML110), dentro del cual se encuentra instalado el directorio activo de Windows de la empresa en su versión 2008, que ha sido configurado por el departamento de TI de la misma.
Para el proceso de autenticación, autorización y registro de un usuario se debe cumplir el siguiente procedimiento:

1. Para que un usuario pueda tener acceso a los recursos de red, debe ser registrado por el personal del departamento de TI bajo el dominio de PIL S.A. en el directorio activo de la empresa, donde se le asignará un usuario y contraseña (podrá cambiar su contraseña cuando el usuario lo considere necesario).

2. El host del usuario debe conectarse a la red cableada de PIL S.A. en el punto de datos designado en su puesto de trabajo, se recuerda que las Vlans de acceso que están distribuidas por la red, están designadas estáticamente en cada puerto FastEthernet de cada Switch.

3. Una vez establecida la conexión física entre el host del usuario y el Switch de acceso, se envía sus credenciales a través de la Vlan troncal hacia el Switch de Core.

4. El Switch de Core envía los datos de las credenciales a través de un enlace capa 3 hacia el Servidor SRV-01.

5. El Servidor SRV-01 mediante LDAP, compara en su base de datos local si estos datos son correctos y concuerdan con las credenciales del usuario.

6. Si la comparación resulta positiva se asignará una dirección IP a través del DNS instalado dentro del mismo servidor y el usuario estará registrado y tendrá autorización para ingresar a la red y acceder a los servicios requeridos, de acuerdo a su perfil creado en la base de datos, caso contrario no podrá acceder a la misma.

2.4.2 Acceso seguro red conexión a internet

La empresa PIL S.A., tiene salida a Internet por medio de dos enlaces:

- El principal a través de Punto Net con un ancho de banda de 4Mbps.
- El de backup a través de Tv cable con un ancho de banda de 2Mbps.

Para la integración de la bodega y la sucursal a la red de PIL S.A., se utilizan dos enlaces dedicados de datos por medio del ISP Punto Net con un ancho de banda de 1Mbps respectivamente, como se ilustra en la figura 23.

Mecanismo de acceso seguro conexión a Internet

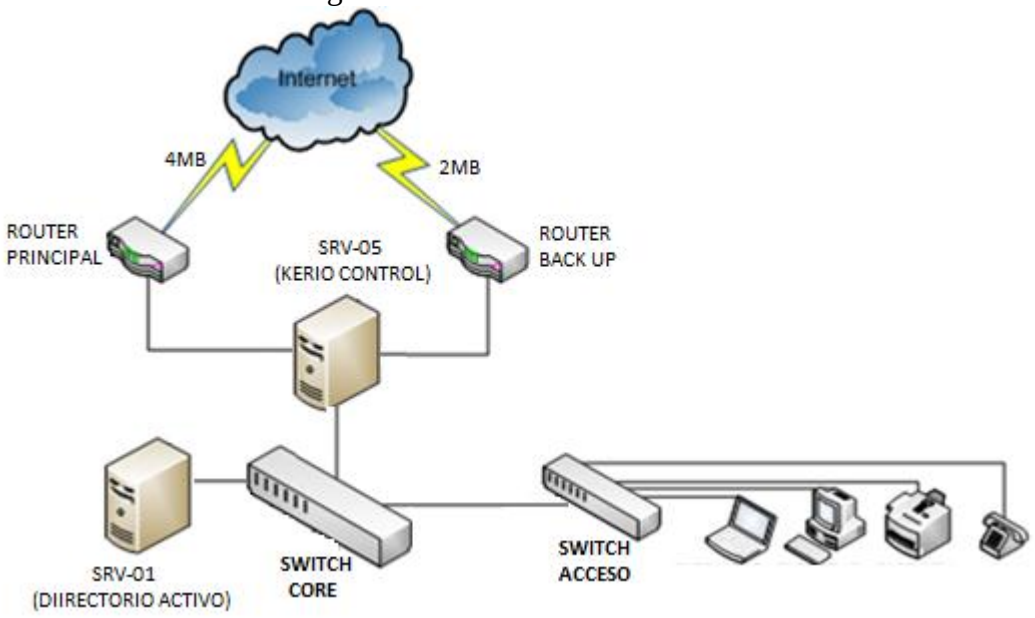


Figura 23.
Elaborado por: Andrés Valdivieso.

El dispositivo principal para el mecanismo de acceso seguro a la conexión de Internet de PIL S.A. es el servidor SRV-05 (Clone Core I7, 8 RAM, 500G), dentro del cual se encuentra instalado el Firewall de cuarta generación, Kerio Control, que ha sido configurado por el departamento de TI.

Para observar las políticas de autenticación utilizadas actualmente por los usuarios, se tuvo que seguir el siguiente procedimiento conjuntamente con el personal de TI de PIL S.A.

2.4.2.1 Acceso al servidor de autenticación Kerio Control

El administrador de red, debe ingresar su usuario y contraseña al portal cautivo generado para el ingreso a las configuraciones del Kerio Control, como se muestra en la figura 24.

Portal cauitivo para configuración de Kerio

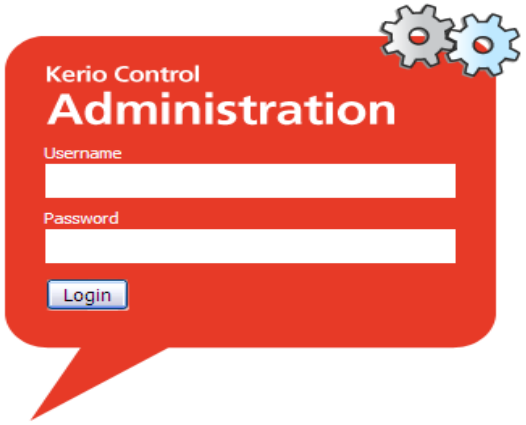


Figura 24.
Elaborado por: Andrés Valdivieso.

Si el usuario y contraseña ingresados son correctas aparecerá el mensaje que se muestra en la figura 25.

Acceso Kerio Control

Figura 25.
Elaborado por: Andrés Valdivieso.

2.4.2.2 Usuarios y grupos

En esta opción de configuración del servidor de Autenticación se tiene tres pestañas, estas ayudaran a configurar los parámetros necesarios para el acceso seguro hacia el Internet.

2.4.2.2.1 Grupos

En la figura 26 se observa que dentro de la pestaña de **grupos**, se importan todos los que han sido creados en el Directorio Activo mediante el dominio pilec.com, se comprueba en la descripción que función desempeña cada uno dentro de la empresa.

Grupos importados desde pilec.com

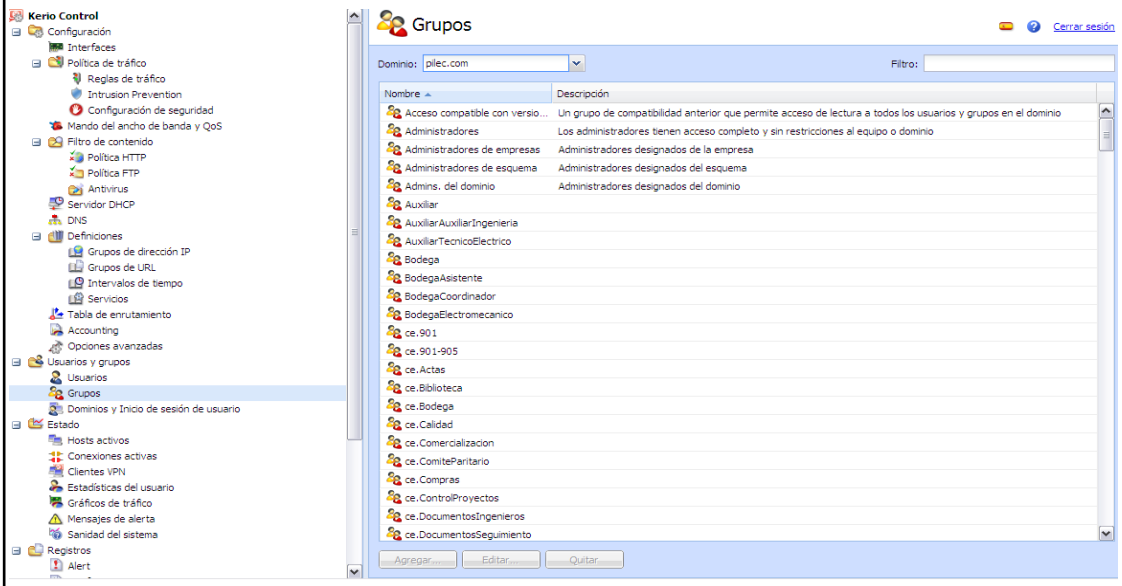


Figura 26.
Elaborado por: Andrés Valdivieso.

En la figura 27 se observa que dentro de la pestaña **grupos**, es necesario crear en la base de datos local el grupo de gestión, esto es si por algún tipo de eventualidad la comunicación con el directorio activo se perdiera, permitiendo la gestión del servidor localmente.

Grupo cerado en base de datos local

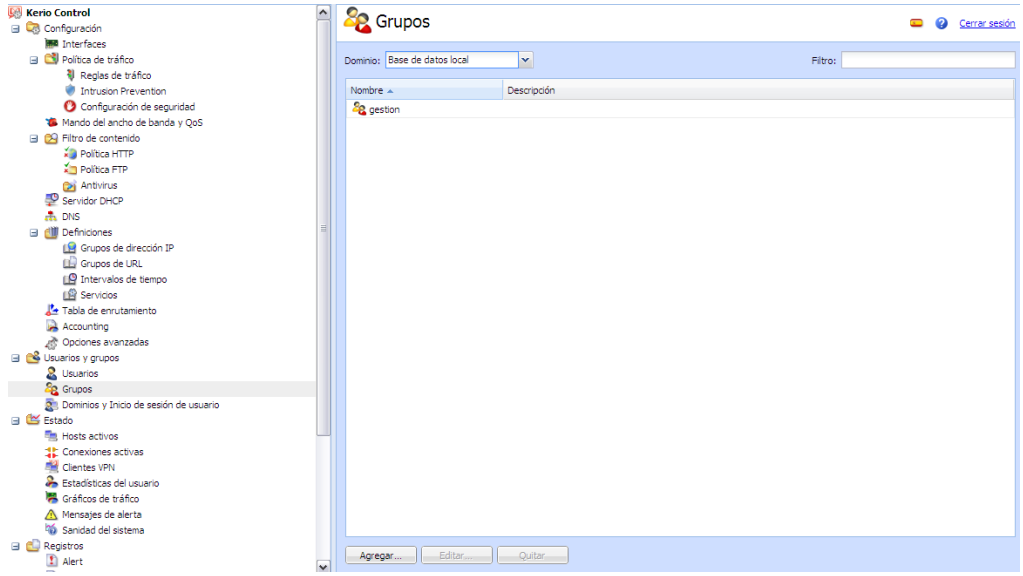


Figura 27.
Elaborado por: Andrés Valdivieso.

2.4.2.2.2 Usuarios

En la figura 28 se observa que dentro de la pestaña **usuarios**, se importan todos los perfiles creados en el Directorio Activo mediante el dominio pilec.com, se comprueba los nombres completos y los grupos a los que respectivamente pertenecen.

Usuarios importados desde pilec.com

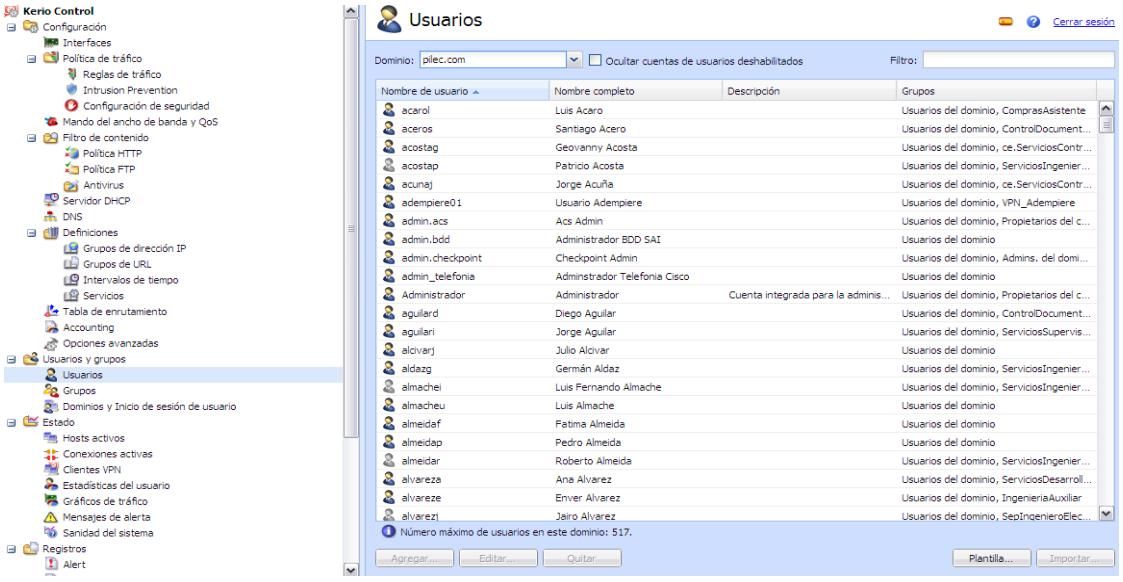


Figura 28.
Elaborado por: Andrés Valdivieso.

En la figura 29 se observa que dentro de la pestaña **usuarios**, existe la necesidad de crear en la base de datos local dos perfiles: de administración y de gestión, esto es si por algún tipo de eventualidad la comunicación con el directorio activo se perdiera, permitiendo la administración del servidor localmente.

Usuarios creados en base local

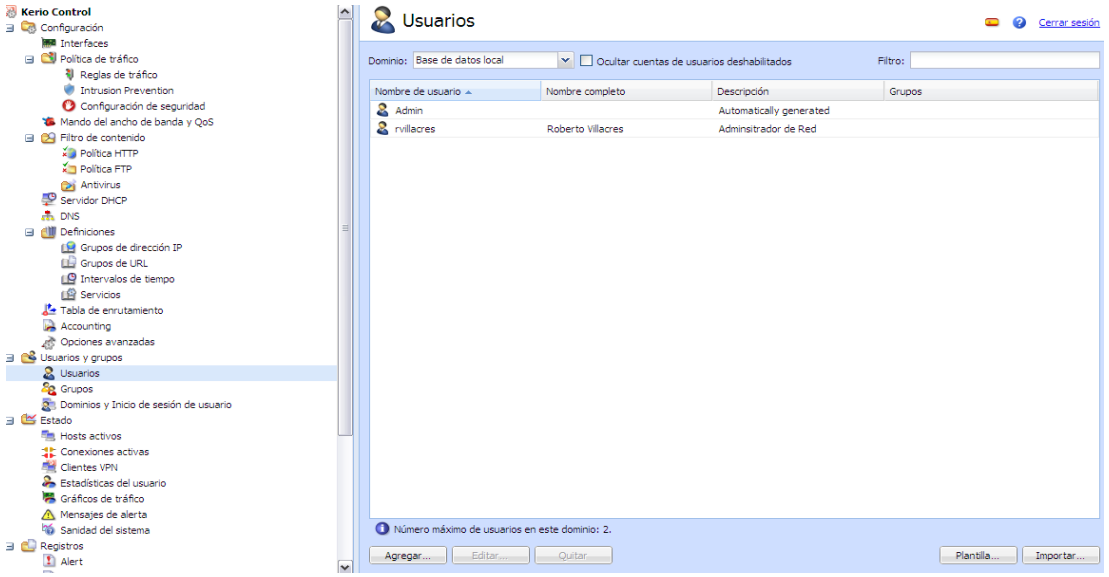


Figura 29.
Elaborado por: Andrés Valdivieso.

2.4.2.2.3 Dominios e inicio de sesión de usuario

Como se puede observar en la figura 30, en la pestaña **dominios e inicio de sesión de usuario**, dentro de las opciones de autenticación web, están activos los parámetros: siempre requerir autenticación de los usuarios al acceder a páginas web y el tiempo de inactividad en el cual el servidor requerirá que los usuarios ingresen nuevamente sus credenciales.

Opciones de autenticación

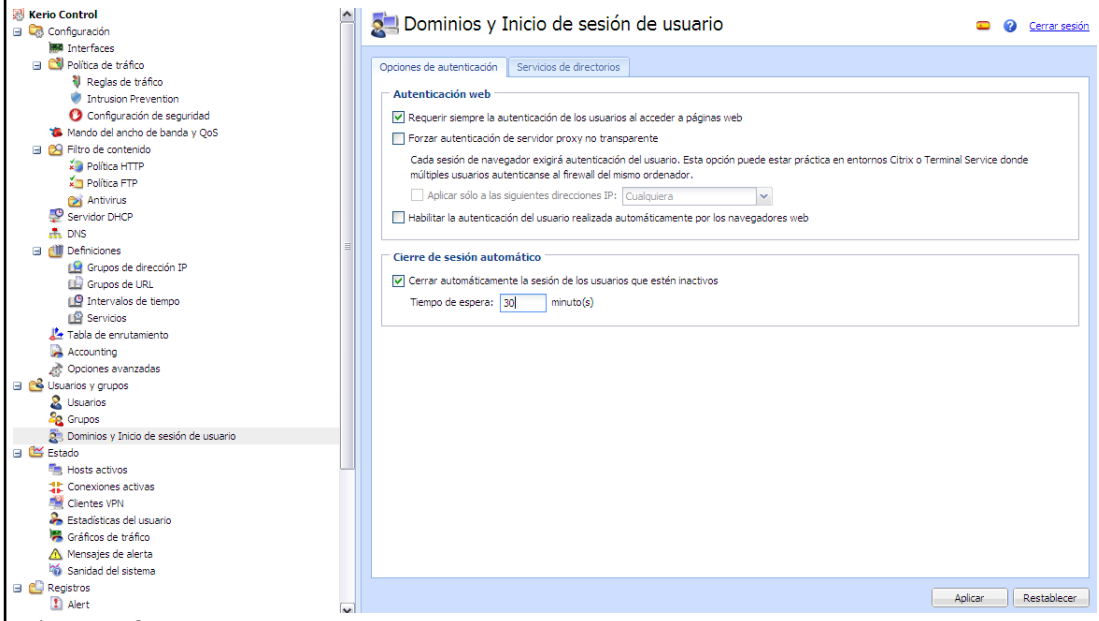


Figura 30.
Elaborado por: Andrés Valdivieso.

En la figura 31, en la pestaña **dominios e inicio de sesión de usuario**, dentro de los servicios de directorios, se observa los parámetros del directorio activo, desde el cual se importan y comparan los usuarios y grupos respectivamente, además de la creación de una cuenta de lectura que permita acceso hacia el mismo.

Servicios de directorios

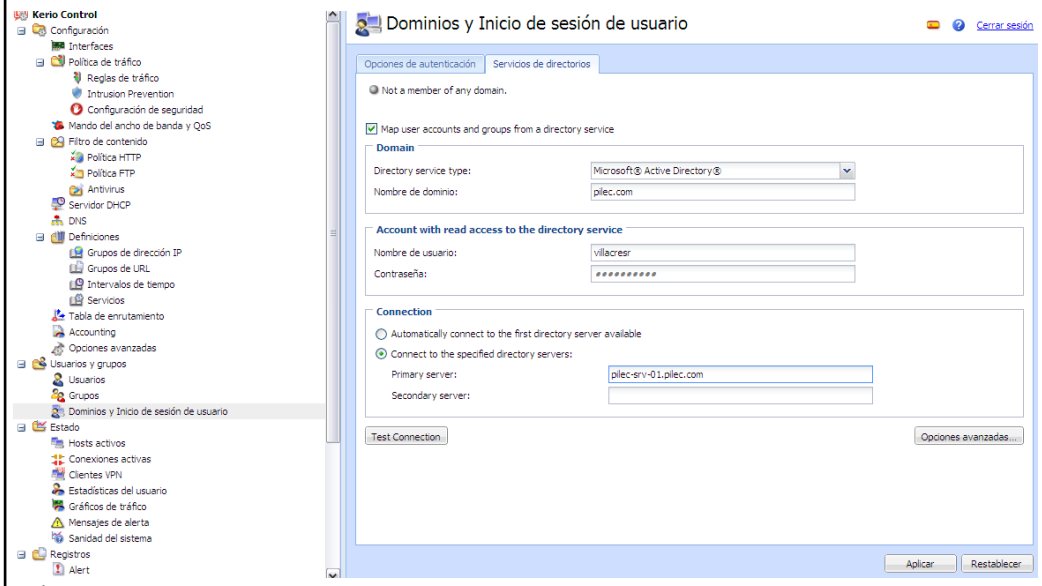


Figura 31.
Elaborado por: Andrés Valdivieso.

2.4.2.3 Usuario con acceso a servicios web

En la figura 32, se observa que para que un usuario tenga acceso a los servicios web, el servidor le presenta un portal cautivo en el cual, debe ingresar su username y password.

Portal cautivo para acceso a servicios web

Figura 32.
Elaborado por: Andrés Valdivieso.

Como se observa en la figura 33 si la autenticación fue positiva el usuario está registrado y puede acceder a los servicios web de la red.

Acceso de usuario a la web

Figura 33.
Elaborado por: Andrés Valdivieso.

Para resumir en el capítulo 2 se muestra que el sistema de autenticación y acceso seguro de la red corporativa de comunicaciones de Proyectos Integrales del Ecuador PIL S.A., disponía de una configuración de puertos estáticos asignados a determinadas VLAN en sus Switch de acceso, los cuales tenían conexión directa con el Directorio Activo para la autenticación de las credenciales de los usuarios de la red.

El anterior esquema de autenticación de puertos estáticos, en conjunto con la carencia de un servicio de acceso inalámbrico para la mayoría de sus usuarios de red, no permitía movilidad dentro de la misma, es decir que si un determinado usuario que aun ingresando correctamente sus credenciales, se conectaba en un punto de red el cual no estuviese asignado a una VLAN de datos, no podría establecer una conexión satisfactoria con esta red.

Adicionalmente bajo este mismo esquema de acceso seguro de red, si un usuario autenticado requería el servicio de internet, tenía que ingresar nuevamente sus credenciales en el portal cautivo presentado por el servidor UTM Kerio Control, el cual haría una comparativa de estos datos con la base de datos del directorio activo para permitirle o no acceso a este servicio respectivamente.

CAPÍTULO 3

REESTRUCTURACIÓN DE LA RED PIL S. A.

Debido al aumento de requerimientos de servicio de seguridad e infraestructura en PIL S.A., se ha llevado a cabo una reestructuración de la red de comunicaciones anterior, pensando en la mejora de servicios tales como: telefonía IP, sistema de seguridad perimetral, control de ancho de banda y control de acceso seguro de red basado en identidad.

3.1 Reestructuración de la red PIL S. A.

La reestructuración de la red de PIL S. A. se ilustra en la figura 34, se observa un modelo jerárquico que se compone de un núcleo, distribución y acceso. La capa núcleo y distribución lo realiza un único equipo que es el Switch de CORE CISCO modelo 4507.

Diagrama topológico actual de la red PIL S. A.

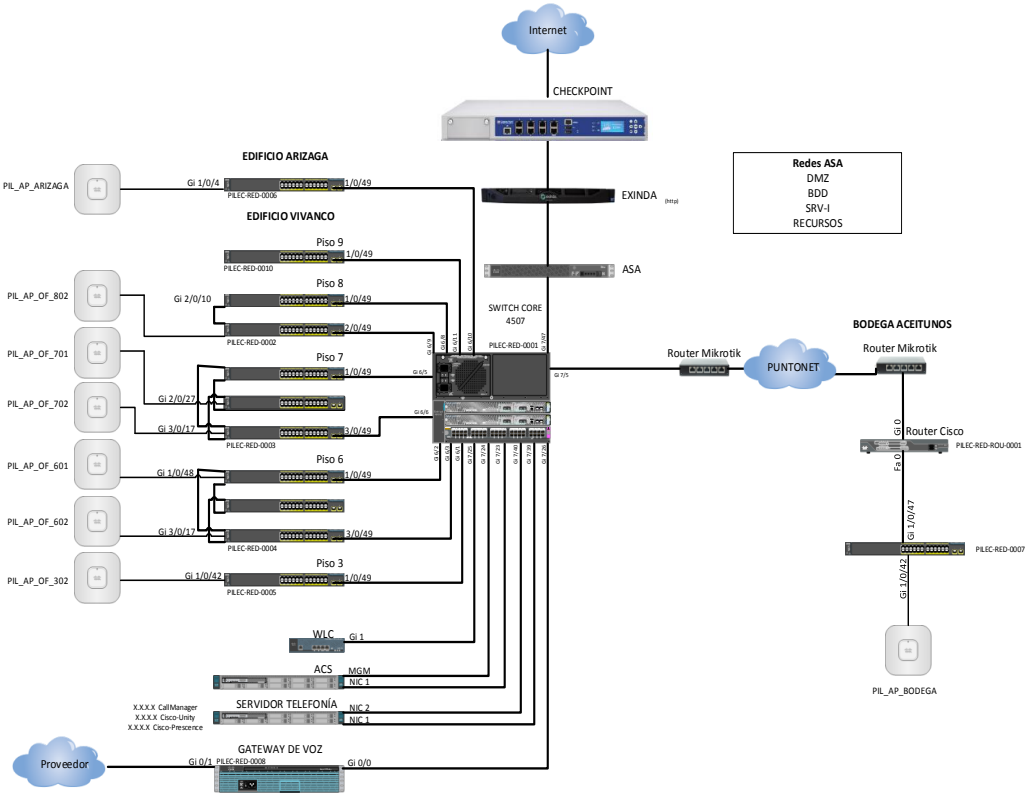


Figura 34.
Elaborado por: Andrés Valdivieso.

Para esta reestructuración de la red, se han reemplazado todos los equipos de marca 3com descritos en el capítulo 2, por equipos de la marca cisco, principalmente para mejorar la disponibilidad, rendimiento y seguridad, en relación con los equipos anteriores.

A continuación se detallan los nuevos equipos instalados en la infraestructura de la red de PIL S.A.

3.2 Topología física de la red

3.2.1 Data center

En el data center de la red corporativa de Proyectos Integrales del Ecuador PIL S.A. se instalaron dos nuevos racks, los que sumados a los existentes, se encuentran distribuidos de la siguiente manera:

- Rack de comunicaciones cerrado de 40UR (Rack core).
- Rack de comunicaciones cerrado de 40UR (Rack servidores - existente).
- Rack de comunicaciones abierto de 45UR (Rack ups).
- Rack de comunicaciones abierto de 45UR (Rack acceso piso - existente).

En las tablas 10 y 11 se describen los equipos nuevos instalados.

3.2.1.1 Rack de core

Tabla 10.
Distribución de rack de core

Item	Cantidad	Descripción	Número de Parte	Fabricante	Posición UR
1	1	Smart Event para rack de 1UR	CPAP-SM503-EVNT	CHECK POINT	32
2	1	Web Filtering para rack de 1UR	CPAP-SG4600-NGTP	CHECK POINT	31
3	1	Router de Gateway de Voz para rack de 2UR	CISCO2911-V/K9	CISCO	30 - 29
4	1	Firewall, IPS, DES/AES para rack de 1UR	ASA5515-IPS-K9	CISCO	23
5	1	Administrador de Ancho de Banda, para rack de 1UR	EX-4761-10	EXINDA	22
6	1	Controlador de Access Point para rack de 1UR	AIR CT2504-15-K9	CISCO	21
7	1	Switch de Core para Rack de 7UR	WS-C4507R+E	CISCO	19 - 13

Nota.
Elaborado por: Andrés Valdivieso.

3.2.1.2 Rack de servidores

Tabla 11.
Distribución de rack servidores

Item	Cantidad	Descripción	Número de Parte	Fabricante	Posición UR
1	1	Servidor Directorio Activo, para rack de 1UR (SRV-01).	POWER EDGE 310	DELL	19
2	1	Servidor Repositorio de Archivos, para rack de 2UR (SRV-04).	NAS N63001905-48	DELL	17 - 16
3	1	Servidor Repositorio de Archivos, para rack de 2UR (SRV-04).	NAS N63001905-48	DELL	14 - 13
4	1	Servidor Telefonía, para rack de 1UR.	BE6K-UCL-100USR	CISCO	11
5	1	Servidor de Autenticación, para rack de 1UR.	CSACS-3415-K9	CISCO	10

Nota.
Elaborado por: Andrés Valdivieso.

3.2.1.3 Rack de ups

Dentro de este Rack se encuentra instalado un UPS de 10KVA, para el sistema de alimentación de los equipos de comunicación del Data Center, además de los servidores existentes SRV-02 y SRV-03, descritos en la tabla 1 del capítulo dos.

3.2.1.4 Rack de acceso piso 8

Este es un Rack existente en el cual los switch de acceso descritos en tabla 2 del capítulo dos, fueron reemplazados, por equipos de marca Cisco modelo WS-C2960S-48LPS-L, ubicados en las mismas unidades de rack que los anteriores dispositivos de red ocupaban.

3.2.2 Cuartos de equipos de comunicaciones (Acceso de red)

Como se indicó en el capítulo dos, todas las localidades de PIL S.A. cuentan con sus respectivos cuartos de comunicaciones, a continuación se describen los equipos que conforman la parte del nuevo mecanismo de acceso de red.

3.2.2.1 Agencia principal

En la agencia principal de PIL S.A., los cuartos de equipos de comunicaciones que se encuentran ubicados en los pisos en los que la empresa cumple sus funciones, fueron reemplazados los switch de acceso descritos en las tablas del capítulo dos, por equipos de marca Cisco de modelo WS-C2960S-48LPS-L, a excepción del rack de acceso del piso siete, en donde se instalaron switchs de marca Cisco de modelo WS-C2960S-48FPS-L, todos los equipos nuevos instalados fueron ubicados en las mismas unidades de rack que los anteriores dispositivos de red ocupaban.

3.2.2.2 Sucursal

En la sucursal de PIL S.A., dentro del cuarto de equipos de comunicaciones ubicado en el tercer piso del edificio Jocay, fue reemplazado el switch de acceso descrito en la tabla 6 del capítulo dos, por un equipo de marca Cisco modelo WS-C2960S-48LPS-L, ubicado en la misma unidad de rack que el anterior dispositivo de red ocupaba.

3.2.2.3 Bodega de materiales

En el interior de la Bodega de materiales de PIL S.A., dentro del cuarto de equipos de comunicaciones ubicado en la primera planta, fue reemplazado el switch de acceso descrito en la tabla 7 del capítulo dos, por un equipo de marca Cisco modelo WS-C2960S-48LPS-L, ubicado en la misma unidad de rack que el anterior dispositivo de red ocupaba.

3.2.3 Diseño de la LAN

Como se indicó en el capítulo dos, el diseño de la red corporativa de PIL S.A., mantiene una topología de red tipo estrella, donde existe un MDF principal y SDF ubicados en las distintas localidades de la empresa.

3.2.4 Comunicación de los servicios de distribución

La conexión entre el MDF ubicado en el Datacenter y los SDF, distribuidos en los diferentes pisos de la agencia principal (Cableado Vertical), fue reemplazada por fibra óptica multimodo de seis hilos OM3, con una configuración etherchanel. Dentro de los racks de comunicaciones en donde exista dos o más switchs de acceso se realizó una conexión Stack entre los mismos para una mejor administración y redundancia como se muestra en la figura 35.

Comunicación de los servicios de distribucion

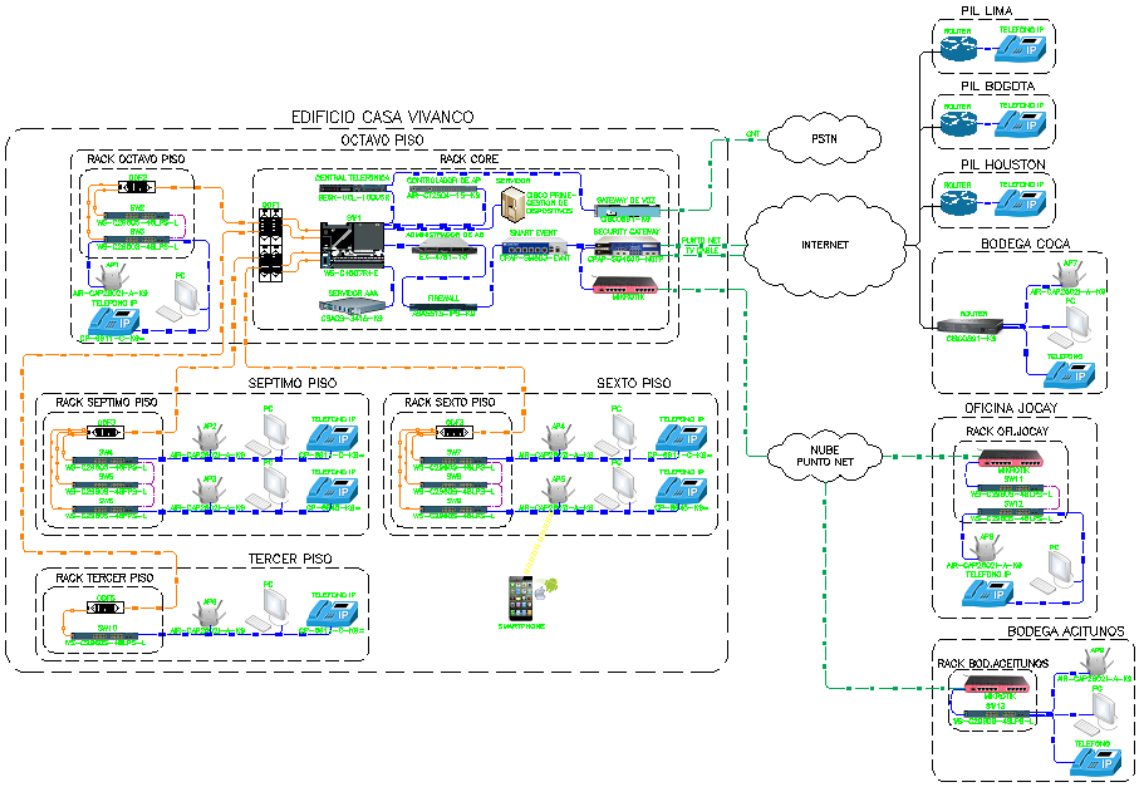


Figura 35.
Elaborado por: Andrés Valdivieso.

3.2.5 Dispositivos que conforman la WLAN

Para mejorar el servicio de la red WLAN se instalaron nuevos equipos distribuidos por todas las localidades de PIL S.A. Está conformada por la controladora de Access Points WLC especificada en la tabla 10, esta trabaja en conjunto con los Access Points lightweight y Cisco Wireless Control System (WCS) para proporcionar funciones de LAN inalámbrica en todo el sistema, permite la comunicación en

tiempo real entre los puntos de acceso inalámbricos y otros dispositivos para ofrecer políticas centralizadas de seguridad, el acceso de invitados, sistemas de prevención de intrusión inalámbrica (WIPS).

Además se ha implementado ocho Access Points los cuales están directamente conectados hacia los Switch de acceso correspondiente como muestra la figura 40. A continuación se detallan los equipos que brindan el servicio de red inalámbrica en PIL S.A.

- 1 Wireless LAN Controller, marca Cisco, modelo AIR-CT2504-K9.
- 8 Access Point, marca Cisco, modelo AIR-CAP2602I-A-K9.

3.3 Topología lógica de la red

3.3.1 Redes

Según las necesidades de la empresa Proyectos Integrales del Ecuador PIL S.A se crearon VLAN en el Switch de CORE y fueron propagadas mediante el protocolo VTP (VLAN Trunking Protocol), como se indica en la tabla 12.

Tabla 12.
VLAN creadas en el switch de core

VLAN id	Nombre de VLAN	Descripción
2	MNG- EQUIPOS	Administración de Equipos
3	IMPRESORAS	Impresoras de Red
4	CCTV	Sistema de Circuito Cerrado de Televisión por IP
6	PERIFERICOS	Equipos Biométricos
8	FALLO	ACS Falla
9	CRITICO	Autenticación por ACS denegada
10	GR_ADMINISTRATIVA	Vlans de Usuarios de Unidad de Negocio Administrativa
11	GR_COMERCIAL	Vlans de Usuarios de Unidad de Negocio Comercial
13	GR_DESARROLLO_ INTERNO	Vlans de Usuarios de Unidad de Negocio Desarrollo
14	GR_GERENCIAS	Vlans de Usuarios de Unidad de Negocio Gerencial
15	GR_SOPORTE_TI	Vlans de Usuarios de Unidad de Negocio Soporte

(continúa...)

(continuación...)

VLAN id	Nombre de VLAN	Descripción
16	GR_TEMPORALES	Vlans de Usuarios Temporales
17	GR_SA	Vlans de Usuarios de Unidad de Negocio SA
18	GR_OPERATIVA	Vlans de Usuarios de Unidad de Negocio Operativa
30	INVITADOS	Wireless Invitados
31	SRV-INT	Servidores Internos: DHCP, DNS, AD, SMB
32	VIP	Wireless VIP
33	INVITADOS-VIP	Wireless Invitados-VIP
100	TELEFONIA_CISCO	Vlans de Telefonía CISCO
102	TELEFONIA_ATA	Vlans de Telefonía ATA
200	SRV-DMZ	Servidores DMZ
220	SRV_RECURSOS	Servidores de recurso
230	SRV-BDD	Servidores Base de Datos
250	INSIDE_ASA	Firewall

Nota.
Elaborado por: Andrés Valdivieso.

VTP es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLAN en equipos Cisco. Permite centralizar y simplificar la administración en un domino de VLAN, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

3.4 Control de acceso basado en identidad

Para el control de acceso a la red basado en identidad se tiene un servidor AAA (Autenticación, Autorización y Accounting), en este caso el ACS de Cisco especificado en la tabla 11.

El ACS es un servidor de seguridad basado en políticas que provee Autenticación Autorización y Accounting (AAA).
Las principales funciones de esta plataforma son:

- Proveer administración de políticas de acceso para equipos en redes cableadas e inalámbricas.
- Soportar un repositorio de usuarios integrado, así con repositorios de identidad externos incluyendo Windows Active Directory y con LDAP.
- Soportar RADIUS Y TACACS+
- Administración y monitoreo centralizado mediante una interfaz web.

3.5 Instalación del CISCO Secure ACS

El CISCO Secure ACS se encuentra conectado a las interfaces GigabitEthernet del switch de Core, a través de dos puertos troncales mediante cables de cobre UTP Cat 6. En la figura 36 se ilustra la configuración realizada a los puertos del switch Core que se conectan con el ACS.

Configuración del switch de core para ACS

```
interface GigabitEthernet7/23
description ACS-NIC-1
switchport access vlan 2
switchport mode access
spanning-tree portfast
interface GigabitEthernet7/24
description ACS-NIC-2
switchport access vlan 2
switchport mode access
spanning-tree portfast
```

Figura 36.
Elaborado por: Andrés Valdivieso.

El modelo del CISCO Secure ACS es el CSACS-3415-K9 en el cual se encuentra instalado el IOS Cisco con la versión 5.4.0.46.0a como se ilustra en la figura 37.

Versión de software ACS

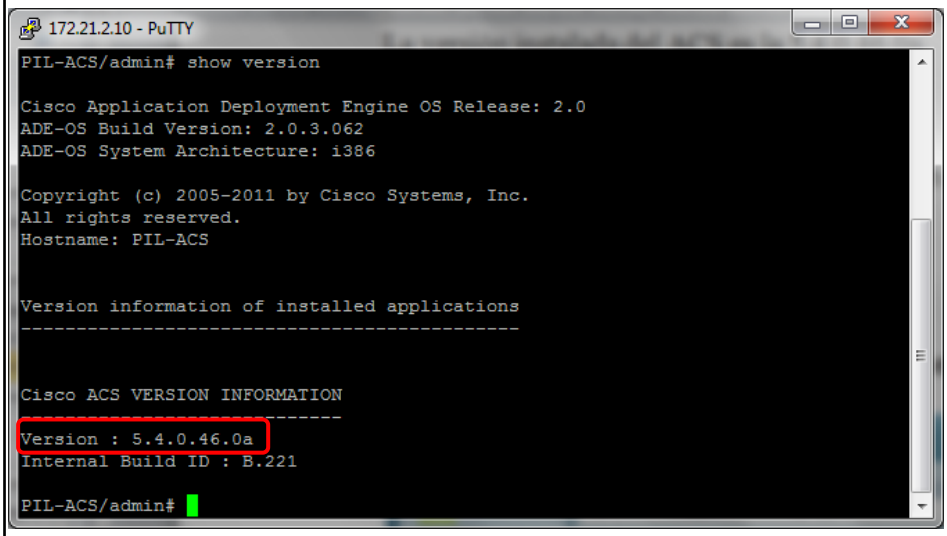


Figura 37.
Elaborado por: Andrés Valdivieso.

3.6 Configuración del CISCO Secure ACS

Para la configuración del servidor ACS se lo puede realizar de dos maneras, la una es por medio de la línea de comandos CLI y la otra por medio de su interfaz gráfica accediendo a través del acceso web.

En la tabla 13 se muestra la dirección IP, usuario y contraseña que vienen por defecto para acceder al servidor ACS por medio del CLI o su interfaz gráfica.

Tabla 13.
Credenciales de acceso a equipo ACS

MODELO	NOMBRE	DIRECCIÓN	USUARIO	CONTRASEÑA	ACCESO
CSACS-3415-K9	PIL-ACS	X.X.X.X	ACSAdmin	X.X.X.X	Web
CSACS-3415-K9	PIL-ACS	X.X.X.X	admin	X.X.X.X	CLI

Nota.
Elaborado por: Andrés Valdivieso.

La configuración del servidor ACS para proveer el servicio de control de acceso a la red de los usuarios de la empresa PIL S. A. se lo realizó mediante su interfaz gráfica tal como se ilustra en la figura 38. Primero se realizaron los cambios en la dirección IP del servidor y credenciales para acceder de manera segura al servidor.

Configuración de credenciales ACS

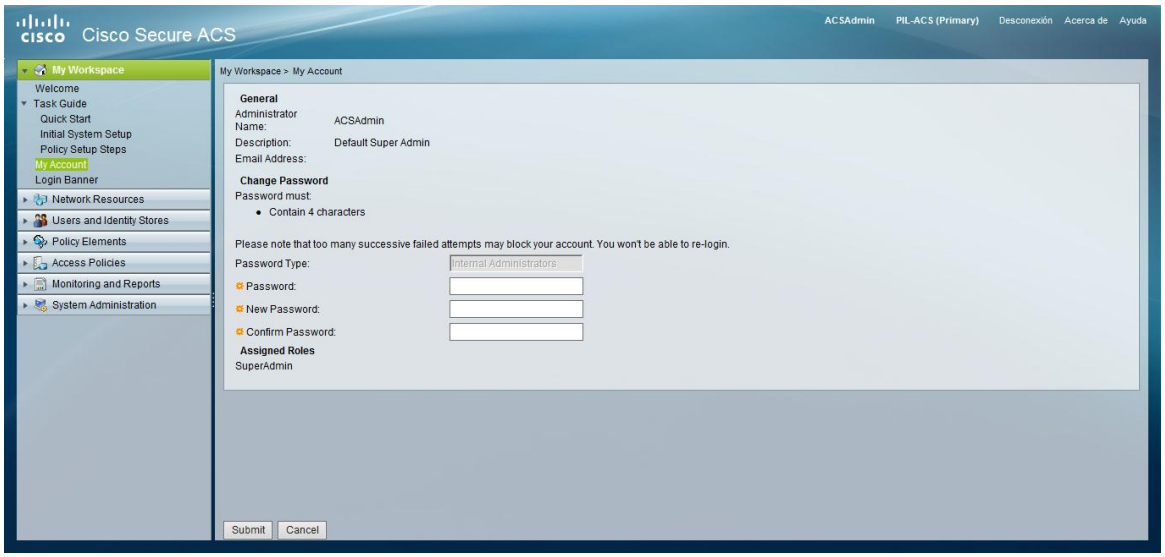


Figura 38.
Elaborado por: Andrés Valdivieso.

A continuación se muestran cada una de las configuraciones que se realizaron en el servidor ACS.

3.6.1 Recursos de red (Network resources)

3.6.1.1 Grupos de equipos de red (Network device groups)

En la pestaña **Network Device Groups**, se realizó la creación de los grupos de dispositivos de red para tener una mejor distribución y gestión en el procedimiento de autenticación. Como parámetros se necesita configurar la localización del grupo y el tipo de dispositivos que se encuentran instalados en la red. En el servidor ACS se crearon 6 grupos de dispositivos de red.

3.6.1.1.1 Locación (Location)

En la figura 39 se ilustran los cuatro diferentes grupos de dispositivos que fueron creados y asignados a las diferentes áreas de la empresa PIL S. A., tales como: sucursal Arizaga, bodega, campo y matriz principal.

Configuración de locations ACS

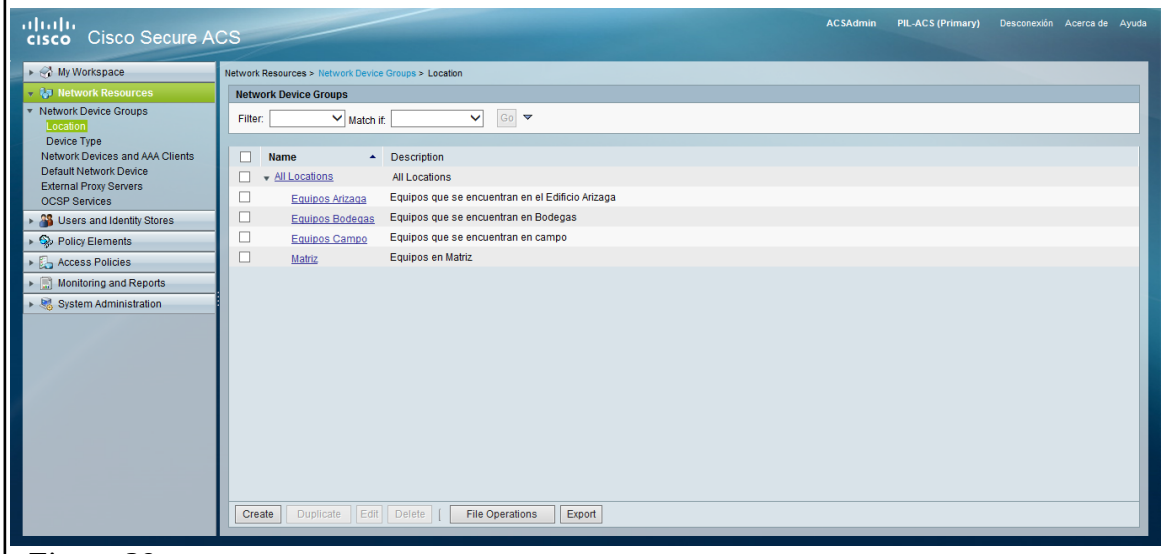


Figura 39.
Elaborado por: Andrés Valdivieso.

3.6.1.1.2 Tipo de dispositivo (Device type)

En la figura 40 se ilustran los seis grupos de equipos que se crearon, cada uno de los dispositivos que son implementados a la red van a estar asociados a un determinado grupo, dependiendo de la función que tengan y su respectivo servicio específico a prestar, dentro de los cuales están los equipos de seguridad, de Wireless, de acceso y de telefonía.

Configuración de tipos de dispositivos ACS

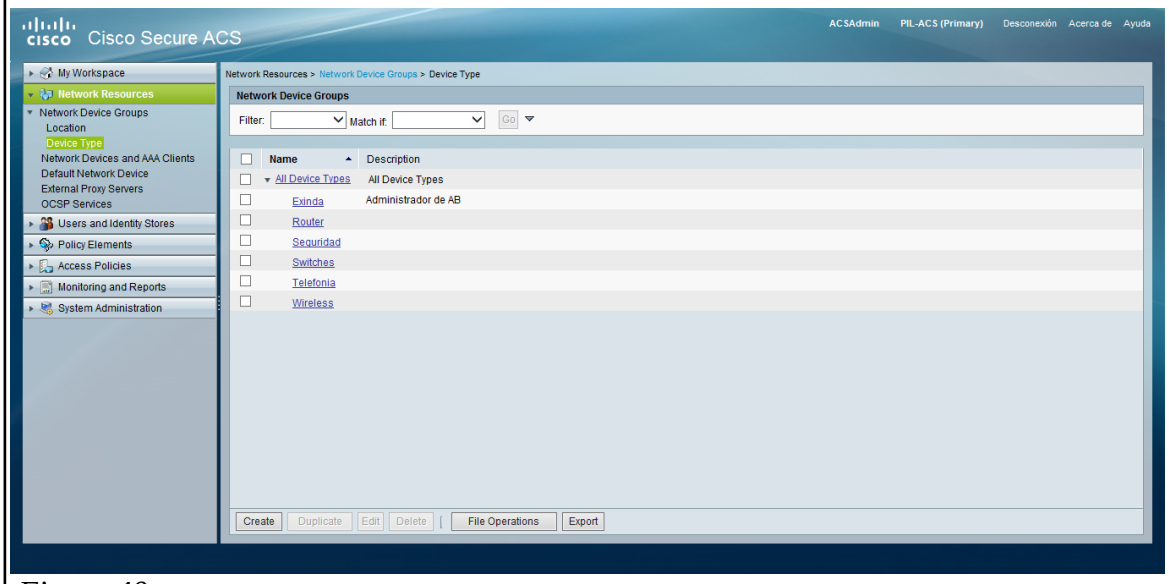


Figura 40.
Elaborado por: Andrés Valdivieso.

3.6.1.2 Equipos de red y clientes AAA (Network devices and AAA clients)

Para proveer el servicio de autenticación se registraron los equipos de la red en la base del servidor ACS, el registro se lo realizó mediante la configuración de su dirección IP de administración, en esta configuración también se decide si la autenticación va a ser realizada mediante el protocolo TACACS+ o RADIUS.

De esta manera cuando un cliente envía una solicitud de acceso a la red de PIL S. A. el servidor ACS verifica en su base si se encuentra registrado aquel cliente por medio de su dirección IP y compara las contraseñas para permitir o no el permiso de acceso a la red.

En la figura 41 se muestra el registro de los trece equipos de red con la configuración de sus respectivas direcciones IP y seguridades PSK (pre-shared Key), en la que incluyen a todos los switch de la red como son acceso y CORE, los routers, el ASA, el Exinda y el Wireless LAN Controller, como se muestra cada dispositivo está registrado con su dirección IP de administración y su PSK.

Configuración de network devices ACS

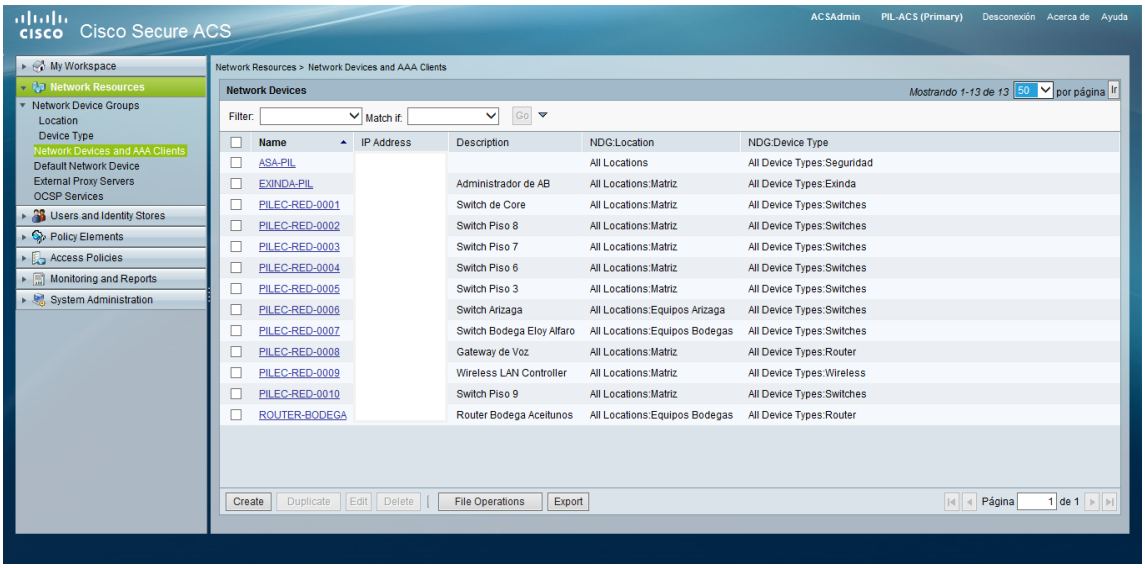


Figura 41.
Elaborado por: Andrés Valdivieso.

3.6.2 Usuarios y directorios de identidad (Users and identity stores)

3.6.2.1 Grupos de identidad (Identity groups)

Los grupos de identidad son creados para asociar las entidades a los diferentes servicios de red, dentro de los cuales se configuran las políticas que van a ser asignadas a los usuarios dependiendo del grupo de identidad al que pertenezcan. En la figura 42 se muestran los grupos de identidad que se encuentran configurados en el servidor ACS.

Configuración de identity groups

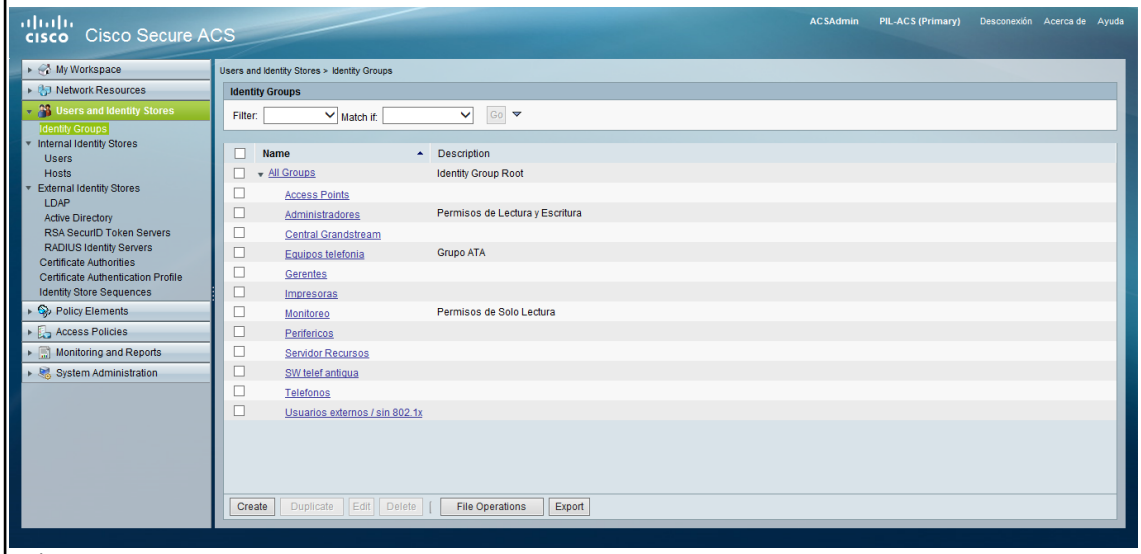


Figura 42.
Elaborado por: Andrés Valdivieso.

3.6.2.2 Directorio de identidad local (Internal identity stores)

3.6.2.2.1 Usuario (User)

En la pestaña **user** se crearon dos usuarios locales temporales como se muestra en la figura 43, que se almacenarán en la base local del servidor ACS para la configuración y administración de los equipos.

Configuración de usuarios internos ACS

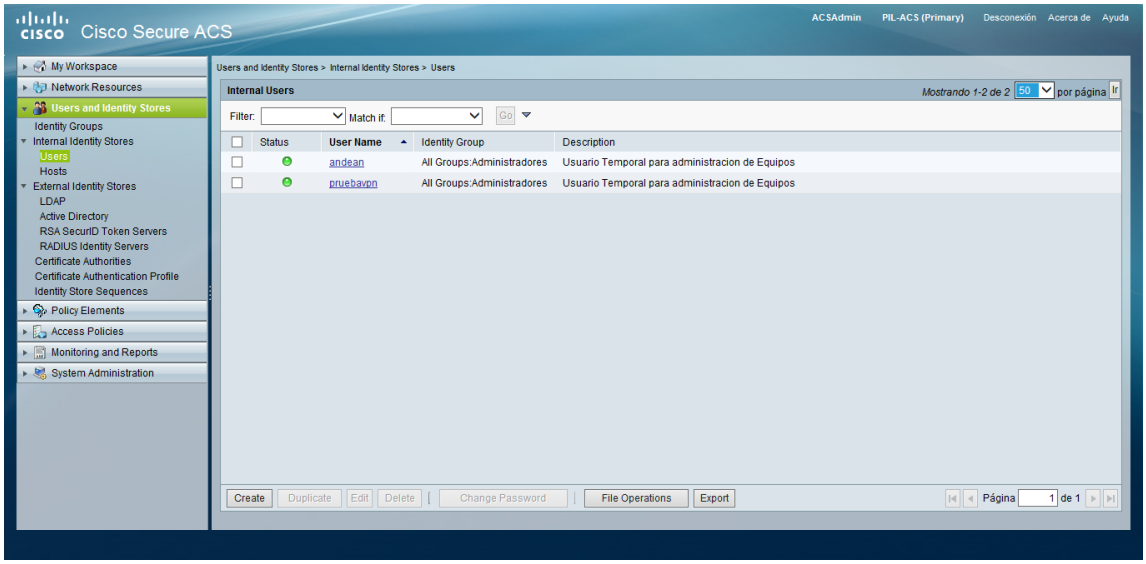


Figura 43.
Elaborado por: Andrés Valdivieso.

3.6.2.2.2 Equipos Periféricos (Host)

En la pestaña host se configuraron todos los equipos que van a ser autenticados por medio de su dirección MAC, como se muestra en la figura 44. Se configuraron un total de 152 dispositivos.

Configuración host internos ACS

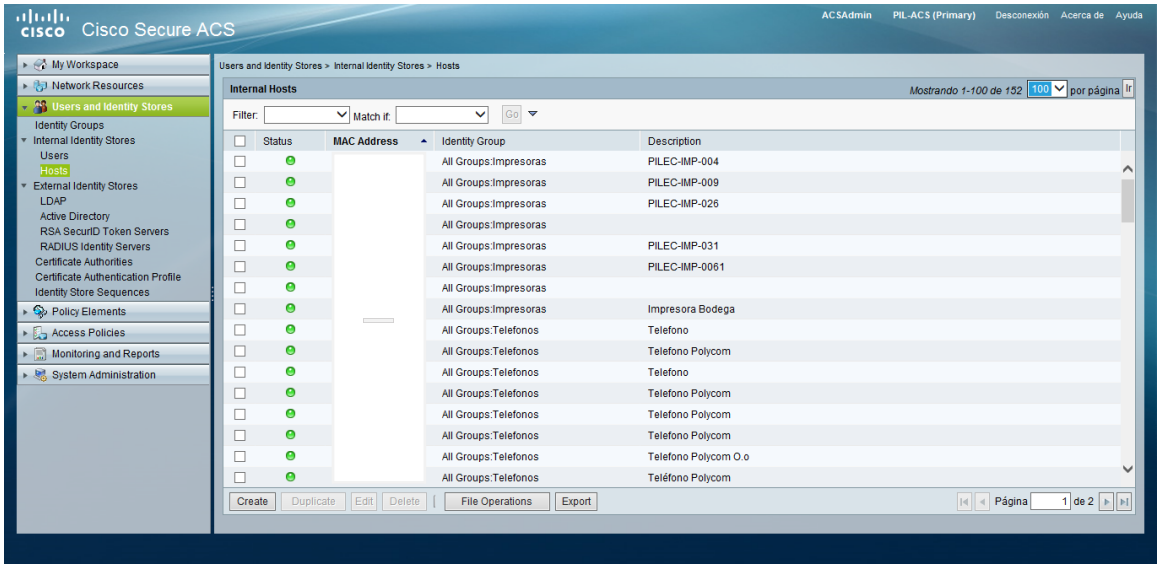


Figura 44.
Elaborado por: Andrés Valdivieso.

3.6.2.3 Directorio de identidad externo (External identity stores)

3.6.2.3.1 Directorio activo (Active directory)

A continuación se configura la integración entre el servidor ACS y el directorio activo, para permitir entregar perfiles de autorización, dependiendo de la unidad organizativa a la que pertenezca el usuario, esto se ilustra en la figura 45.

Configuración enlace AD – ACS

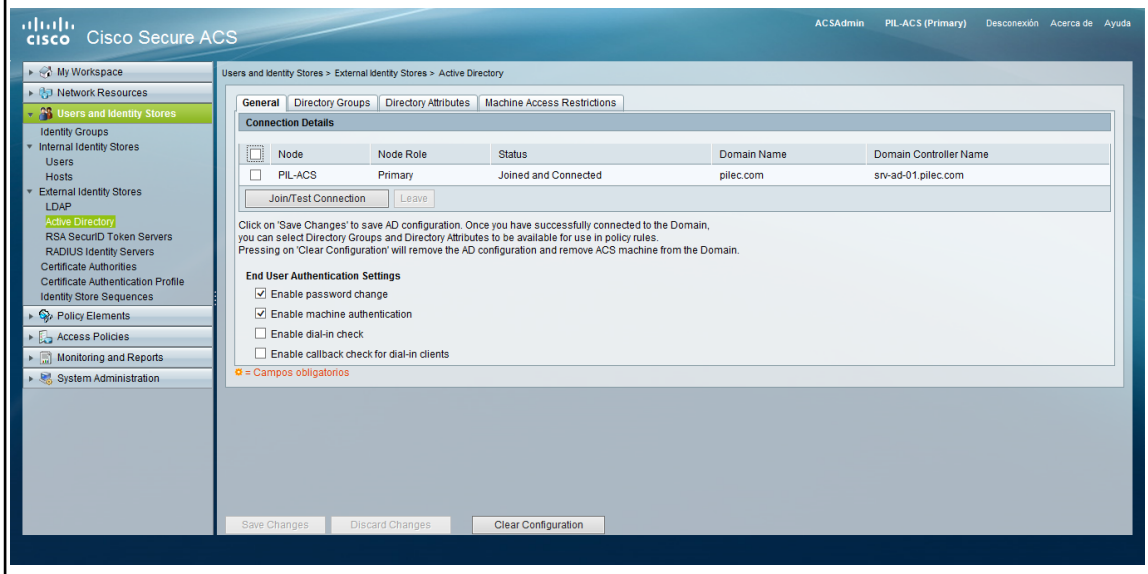


Figura 45.
Elaborado por: Andrés Valdivieso.

En las figuras 46 y 47 se muestran los 17 grupos añadidos del Active Directory para la configuración del ACS.

Grupos obtenidos del AD parte 1

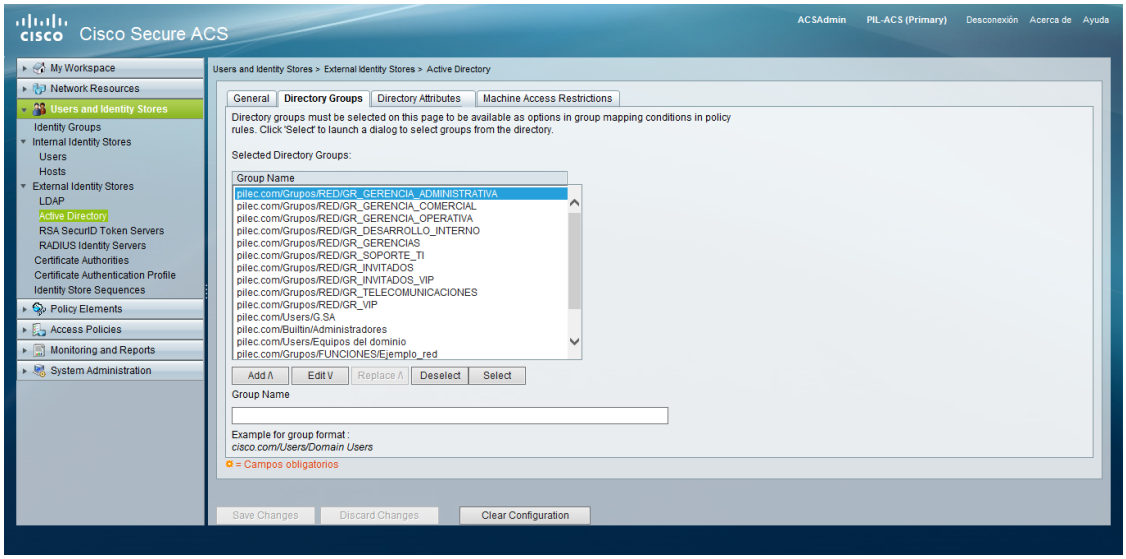


Figura 46.
Elaborado por: Andrés Valdivieso.

Grupos obtenidos del AD parte 2

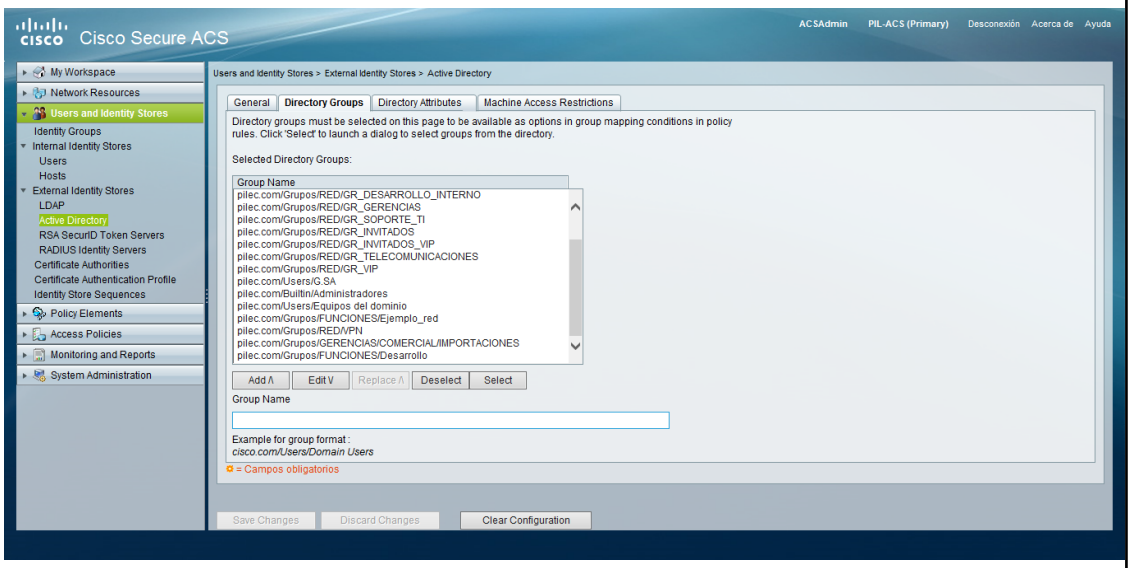


Figura 47.
Elaborado por: Andrés Valdivieso.

3.6.2.3.2 Secuencias de directorio de identidad (Identity store sequences)

En esta pestaña se configura una secuencia de autenticación como se muestran en las figuras 48 y 49, esto permite especificar el orden de los grupos en que serán autenticados los usuarios. Como pudiera ser que primero sean autenticados los usuarios del Active Directory, segundo los usuarios internos y por último los host internos.

Secuencia de autenticación ACS

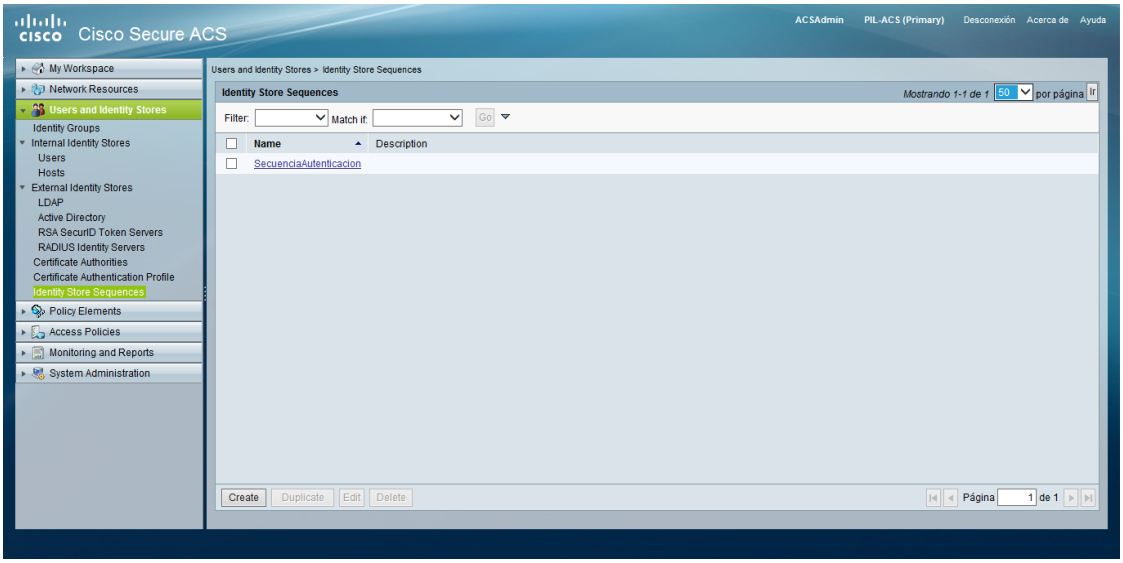


Figura 48.
Elaborado por: Andrés Valdivieso.

Secuencia de autenticación configurada ACS

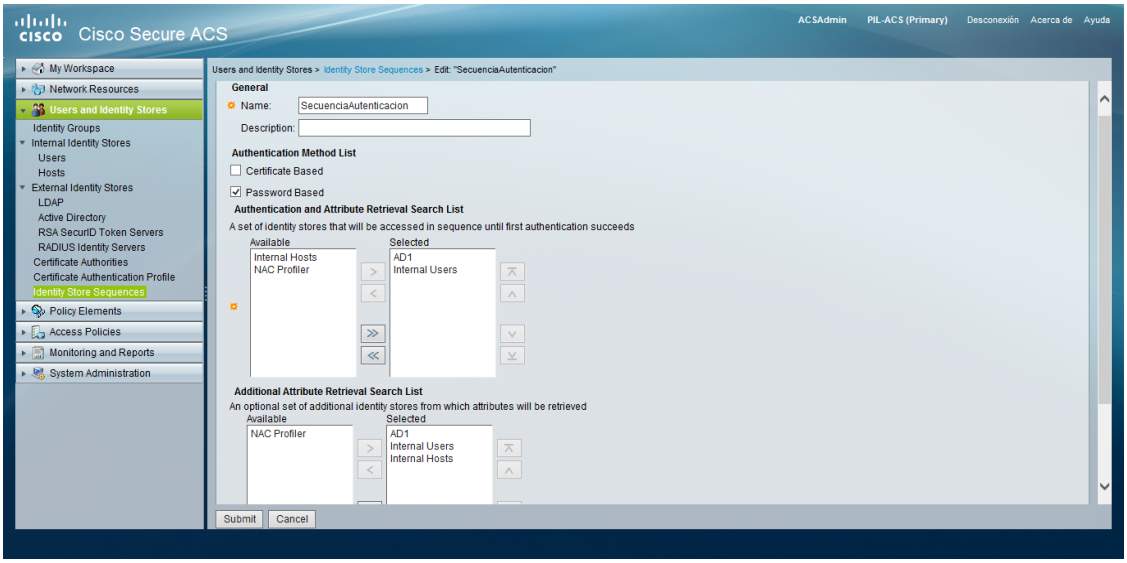


Figura 49.
Elaborado por: Andrés Valdivieso.

3.6.3 Elementos de directiva (Policy elements)

Las políticas de seguridad permiten definir, cómo se protege a una organización ante posibles ataques. Debe contar con una política general de seguridad.

El diseño de la política de seguridad se basa en:

- En la evaluación de riesgos.
- En la creación de planes acordes con el nivel de seguridad a implementar.

El empleo de una política de seguridad debe ser proporcional a la jerarquía de la información que va hacer protegida.

3.6.3.1 Autorización y permisos (Authorization and permissions)

3.6.3.1.1 Acceso de red (Network access)

Para el acceso a la red se configuraron ciertos parámetros, el primero es la configuración de los perfiles de autorización como se muestra en la Figura 50.

Authorization profiles ACS

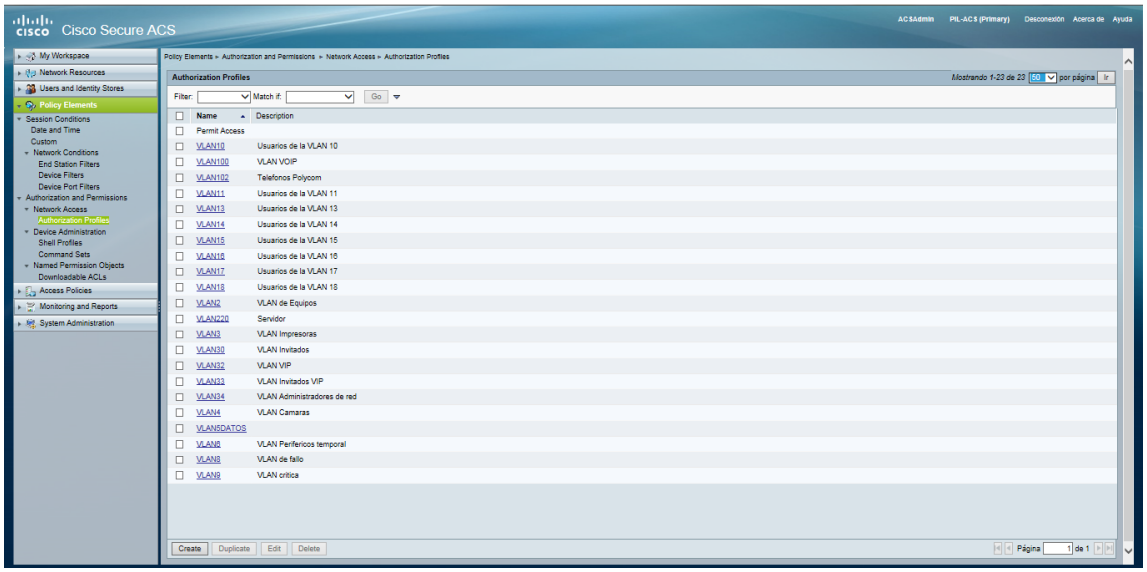


Figura 50.
Elaborado por: Andrés Valdivieso.

Como segundo paso, se configuró un perfil de autenticación basado en VLAN para datos, esto se ilustra en la figura 51.

Configuración de VLAN dentro de authorization profile

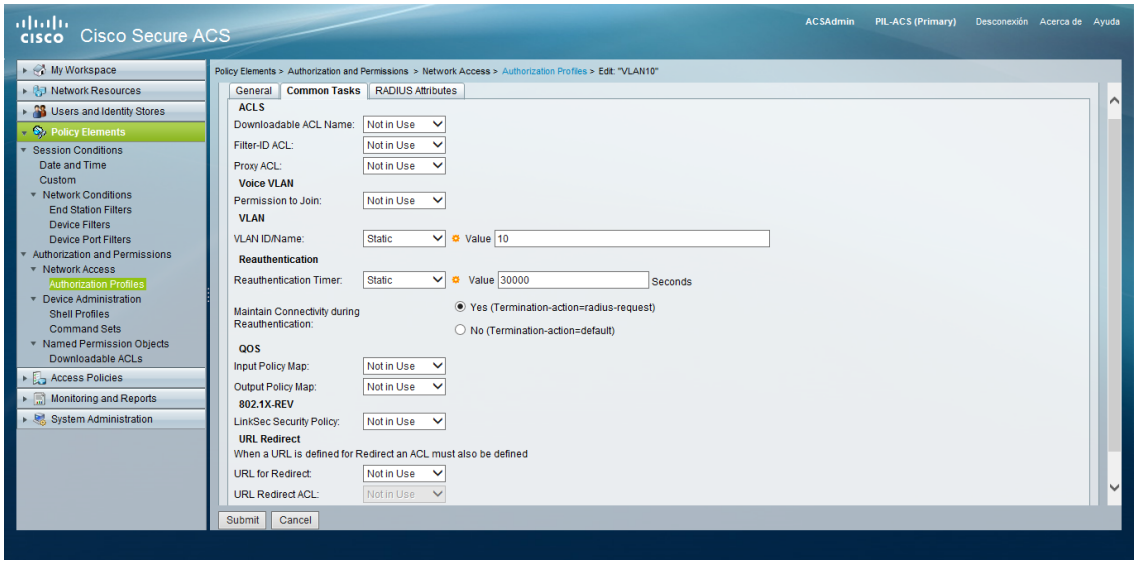


Figura 51.
Elaborado por: Andrés Valdivieso.

Como tercer paso, se configuró un perfil de autenticación basado en VLAN para voz, esto se ilustra en la figura 52.

Configuración de VLAN de voz authorization profile

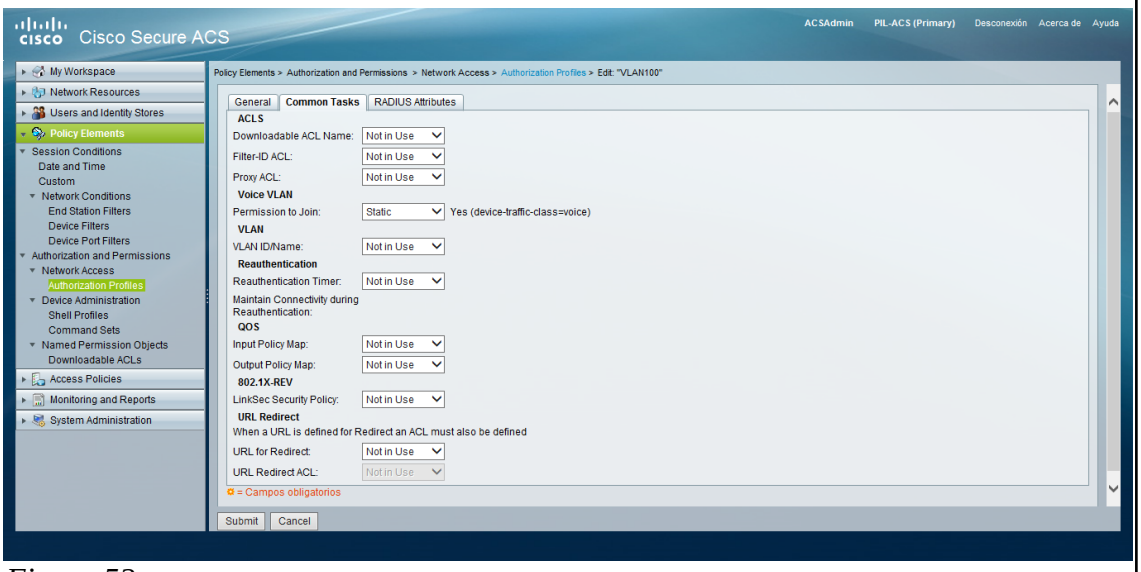


Figura 52.
Elaborado por: Andrés Valdivieso.

3.6.3.2 Administración de equipos (Device administration)

3.6.3.2.1 Perfiles de consola (Shell profiles)

En la figura 53 se muestran los perfiles Shell creados. En esta parte se configuran las políticas de permisos a los que el usuario está autorizado dentro de la red de PIL S.A.

Shell profile ACS

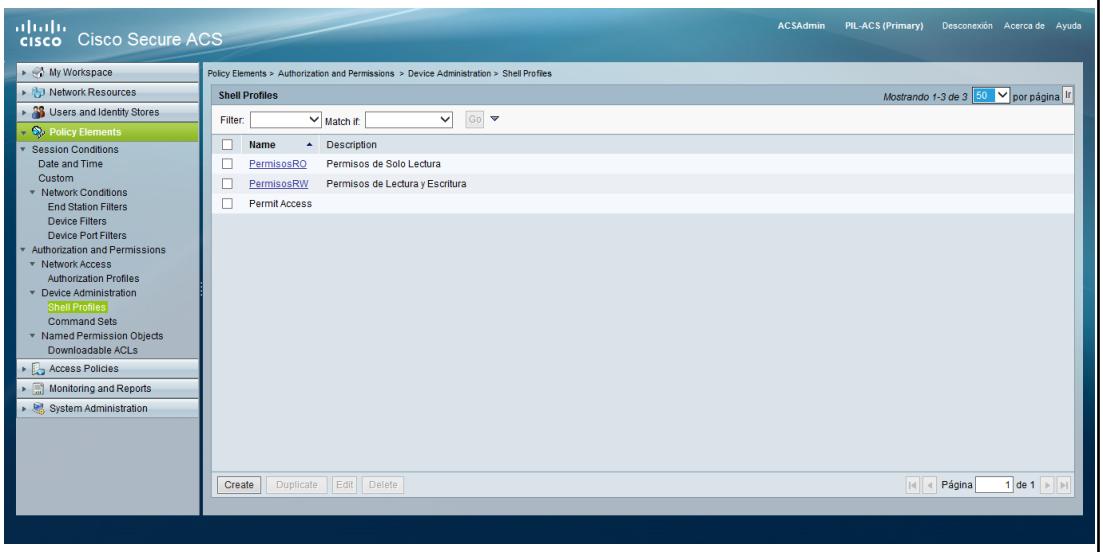


Figura 53.
Elaborado por: Andrés Valdivieso.

En las figuras 54 y 55 se muestran las configuraciones de los perfiles antes creados, para Read Only con privilegio 0 y Read Write con privilegio 15. En el Cisco IOS podemos crear y definir diferentes niveles de privilegio, a fin de delimitar el acceso que tienen los usuarios sobre la administración del equipo.

Existen 16 niveles de privilegio donde:

-Los niveles 0 y 1 poseen configuraciones y comandos predefinidos, solo permitiendo monitoreo del equipo.

-Los niveles entre el 2 y el 14 son completamente customizables, podrán ejecutar comandos configurados previamente en sus niveles de privilegio.

-El nivel 15 tiene configuraciones y comandos predefinidos, lo que le permite administración y monitoreo total dentro del equipo.

Es importante saber que por ejemplo si se tiene un usuario asociado a un nivel de privilegio 10, este va a tener acceso a los comandos definidos dentro de ese nivel, así como también a los comandos definidos en los niveles inferiores (0 hasta el 9).

Shell profile privilegio 0

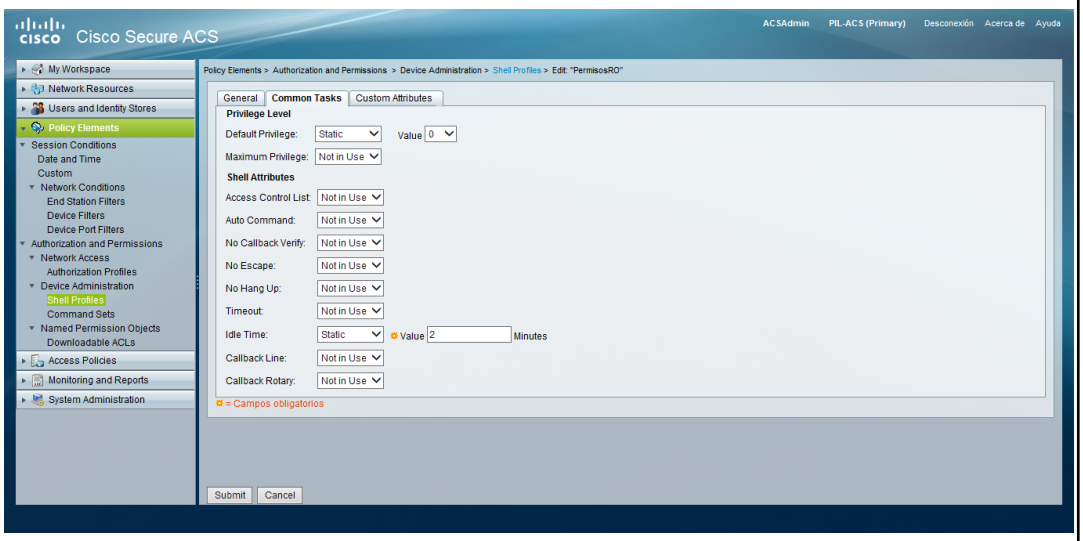


Figura 54.
Elaborado por: Andrés Valdivieso.

Shell profile privilegio 15

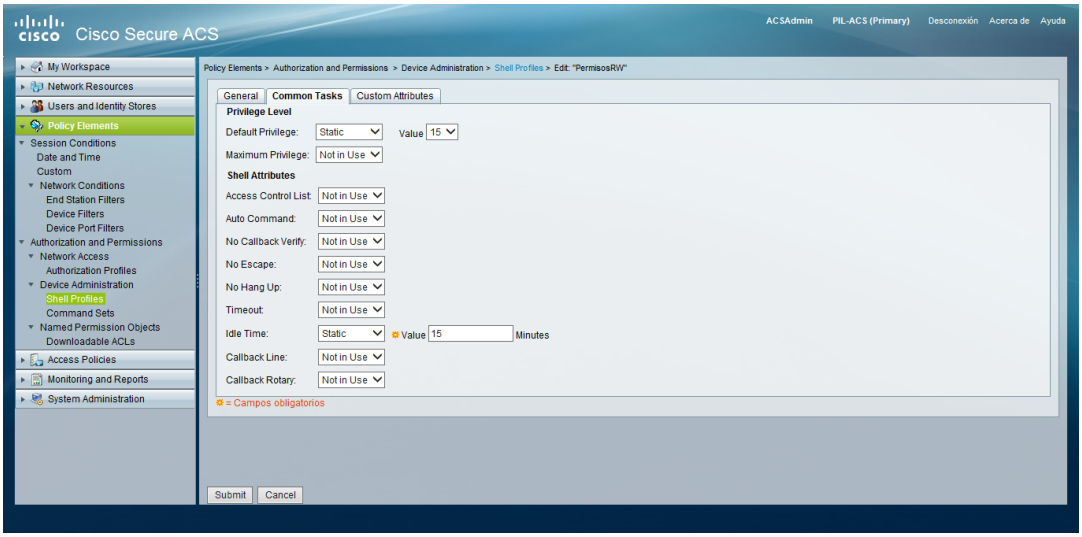


Figura 55.
Elaborado por: Andrés Valdivieso.

3.6.4 Políticas de acceso (Access policies)

Es la configuración más importante dentro del ACS, ya que es donde se establece la forma como se van a autenticar los usuarios, los Switch, los equipos que no se comunican con el IEEE 802.1x (MAB) y donde se integran todos los objetos creados anteriormente.

3.6.4.1 Servicios de acceso (Access services)

En la figura 56, se muestran los servicios de acceso creados, para la autenticación de los usuarios, estos son:

- MAB,
- RADIUS Y
- TACACS.

Access services ACS

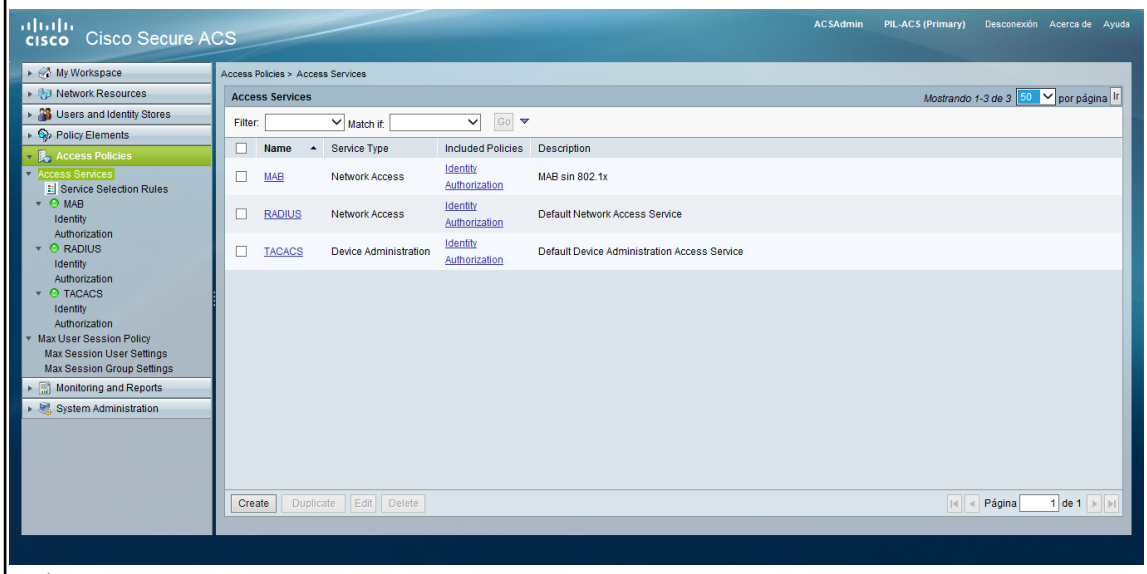


Figura 56.
Elaborado por: Andrés Valdivieso.

3.6.4.1.1 Reglas de selección de servicio (Service selection rules)

En la figura 57, se muestran las 4 reglas creadas para la selección de servicio:

-Regla 1, Autenticación de usuarios Radius

-Regla 2, Autenticación de ususarios TACACS

-Regla 3, Autenticación de usuarios MAB

-Regla 4, Autencicación de usuarios Radius a traves de VPN

Service selection rules ACS

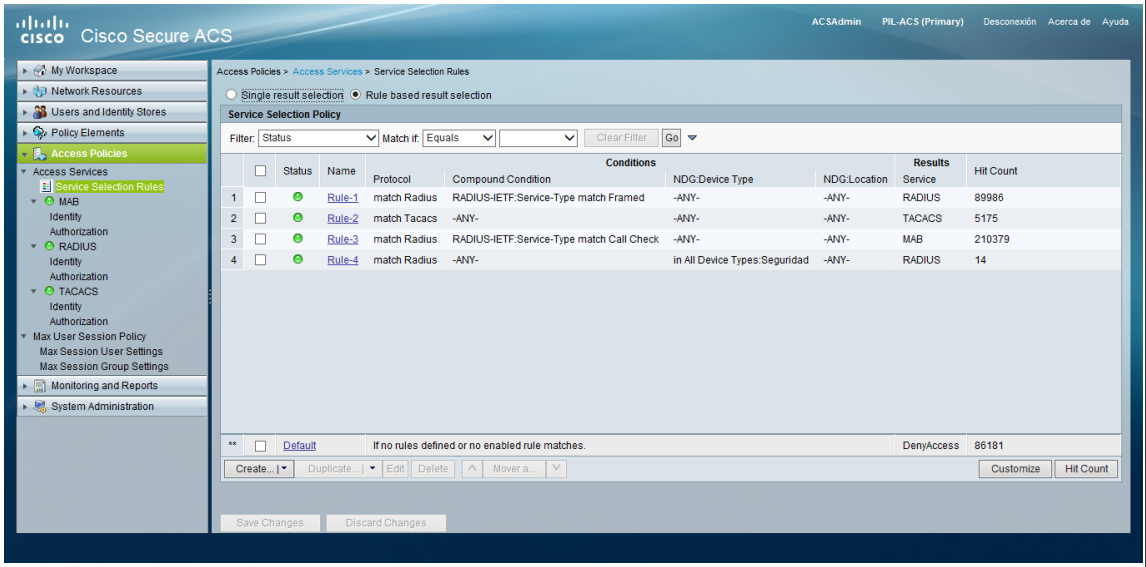


Figura 57.
Elaborado por: Andrés Valdivieso.

3.6.4.1.2 Configuración del método MAB

3.6.4.1.2.1 Identidad (Identity)

La identidad selecionada para el servicio de MAB es Internal Host, se muestra en la figura 58.

MAB selección de identidad

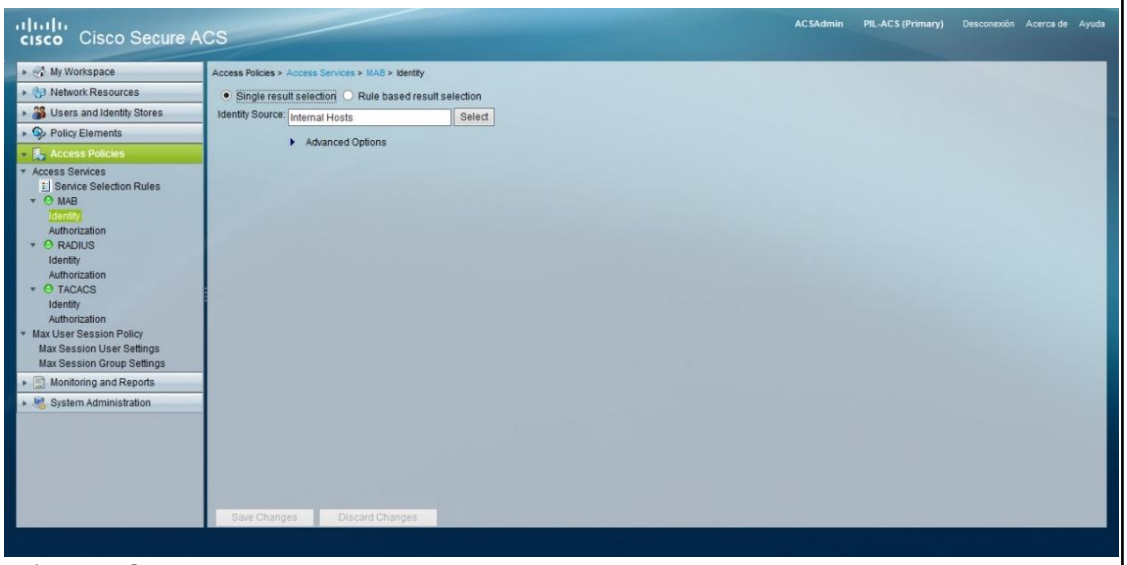


Figura 58.
Elaborado por: Andrés Valdivieso.

3.6.4.1.2.2 Autorización (Authorization)

En la figura 59, se muestra que se encuentran configuradas 10 reglas para la autenticación de equipos vía MAB.

Reglas de autorización vía MAB

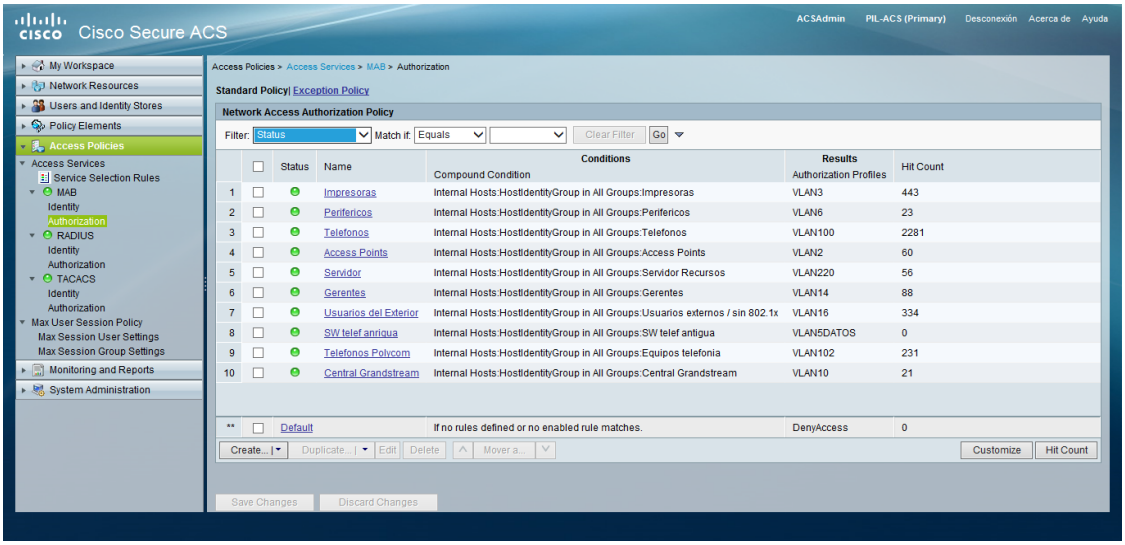


Figura 59.
Elaborado por: Andrés Valdivieso.

En la figura 60, se muestra un ejemplo de configuración para la autorización basada en un servicio vía MAB.

Autorización basada en condiciones MAB

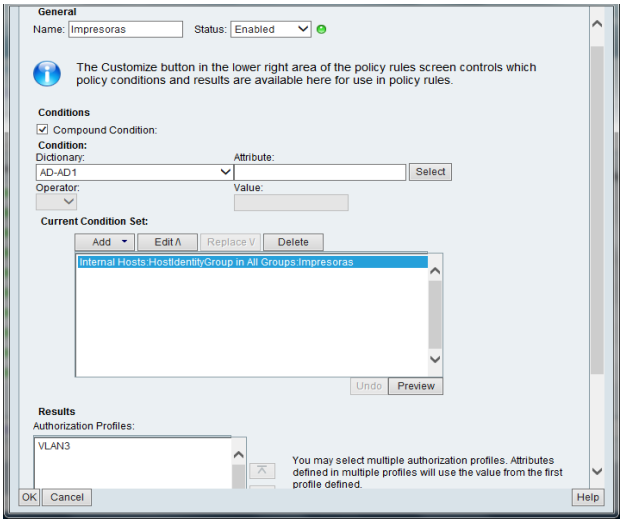


Figura 60.
Elaborado por: Andrés Valdivieso.

3.6.4.1.3 Configuración del protocolo RADIUS

3.6.4.1.3.1 Identidad (Identity)

Para la configuración del servicio RADIUS se utilizó la secuencia de autenticación configurada anteriormente en la pestaña **Identity Store Sequences,** esto se muestra en la figura 61.

Selección de identidad RADIUS

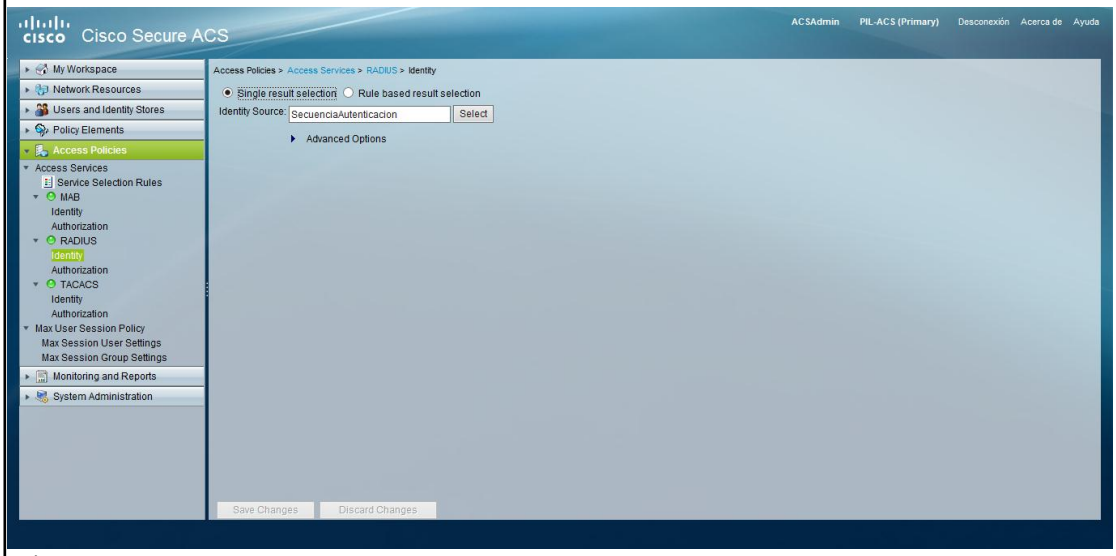


Figura 61.
Elaborado por: Andrés Valdivieso.

3.6.4.1.3.2 Autorización (Authorization)

Se ha realizado la configuración de autenticación mediante RADIUS para 11 grupos del Active Directory y una regla para la conexión vía VPN como se muestra en la figura 62.

Reglas de autorización vía RADIUS

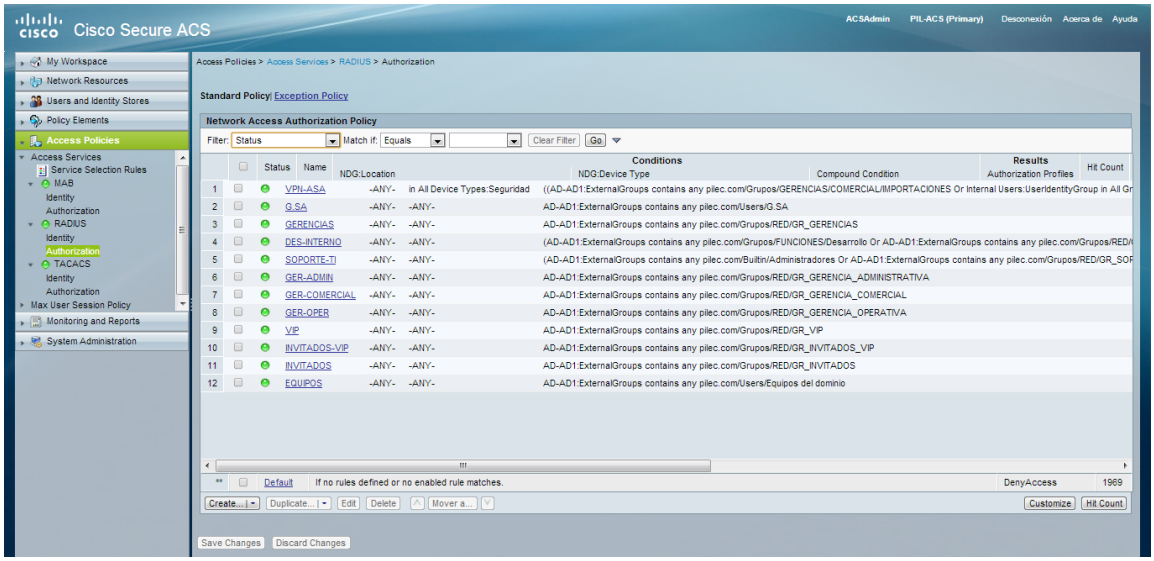


Figura 62.
Elaborado por: Andrés Valdivieso.

En la figura 63 se muestra un ejemplo de configuración para la autorización basada en un servicio RADIUS.

Autorización basada en condiciones RADIUS

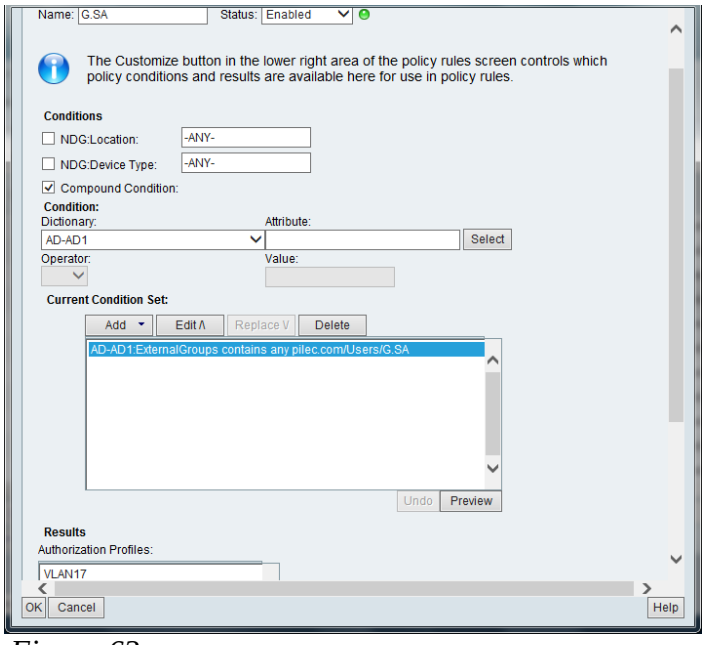


Figura 63.
Elaborado por: Andrés Valdivieso.

Para el caso de la conexión vía VPN es necesario aumentar los grupos que tengan este servicio. En la figura 64, se muestra se muestra la autorización para la conexión vía VPN.

Autorización para VPN

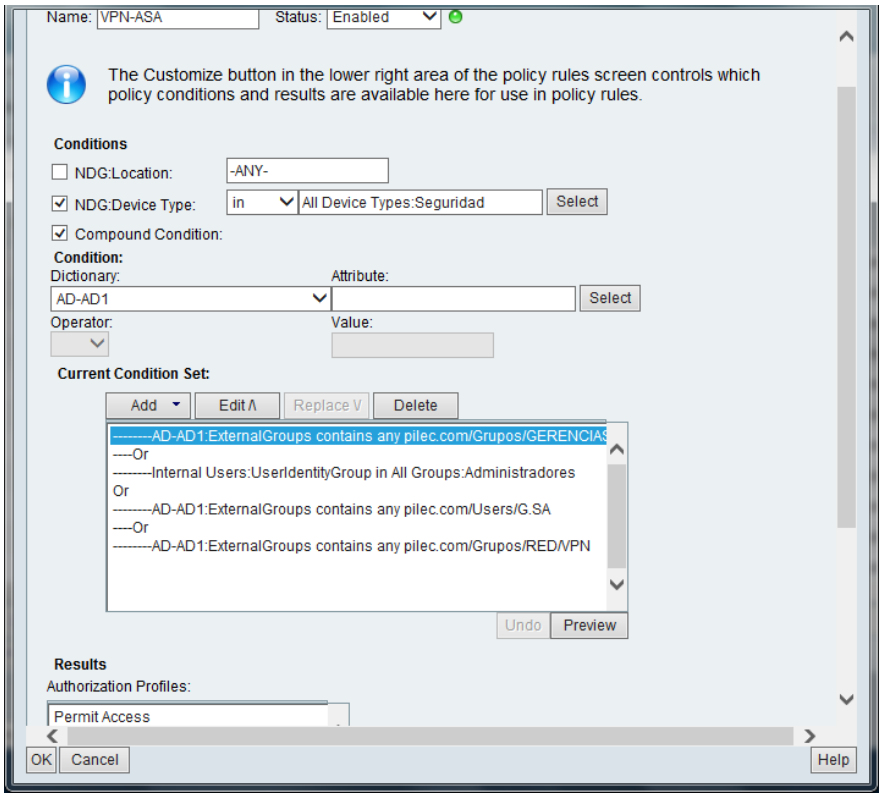


Figura 64.
Elaborado por: Andrés Valdivieso.

3.6.4.1.4 Configuración del protocolo TACACS+

3.6.4.1.4.1 Identidad (Identity)

Al igual que en la configuración del servicio RADIUS, para la configuración del servicio de TACACS+ también se utiliza la secuencia de autenticación configurada anteriormente en la pestaña **Identity Store Sequences,** como se muestra en la figura 65.

TACACS secuencia de autenticación

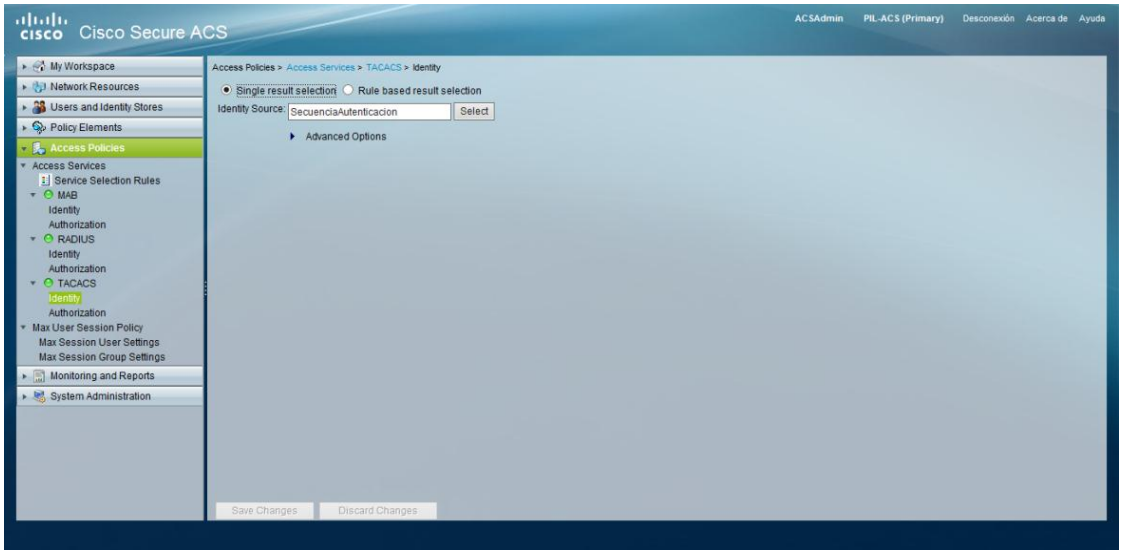


Figura 65.
Elaborado por: Andrés Valdivieso.

3.6.4.1.4.2 Autorización (Authorization)

Se han creado grupos de administración y monitoreo para los diferentes dispositivos de la red, esto se muestra en la figura 66.

Reglas de autorización vía TACACS

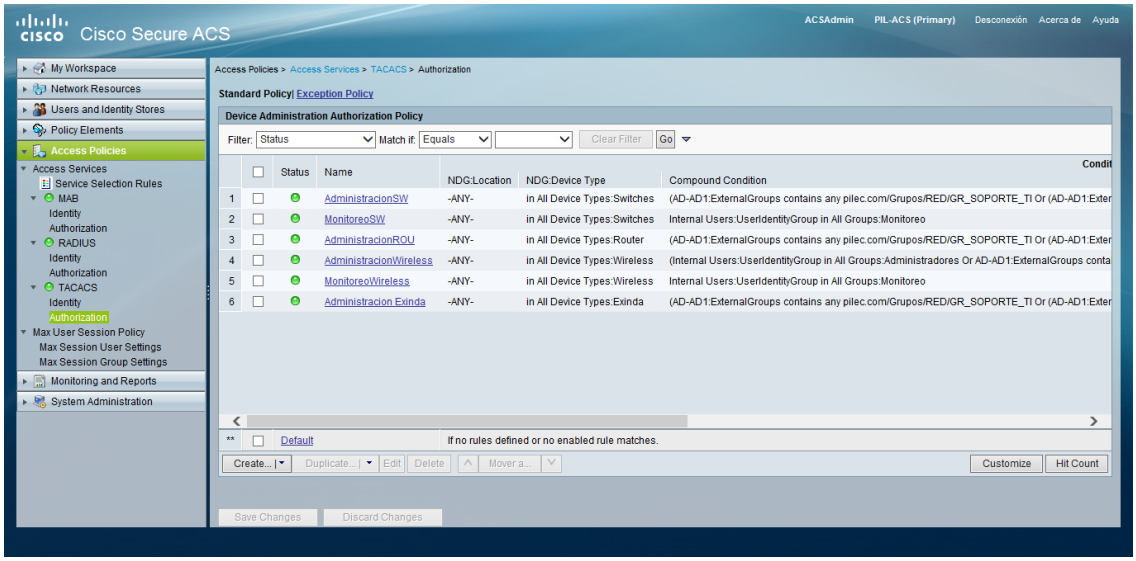


Figura 66.
Elaborado por: Andrés Valdivieso.

En la figura 67 se muestra un ejemplo de configuración de un grupo de Administración.

Autorización basada en condiciones vía TACACS RW

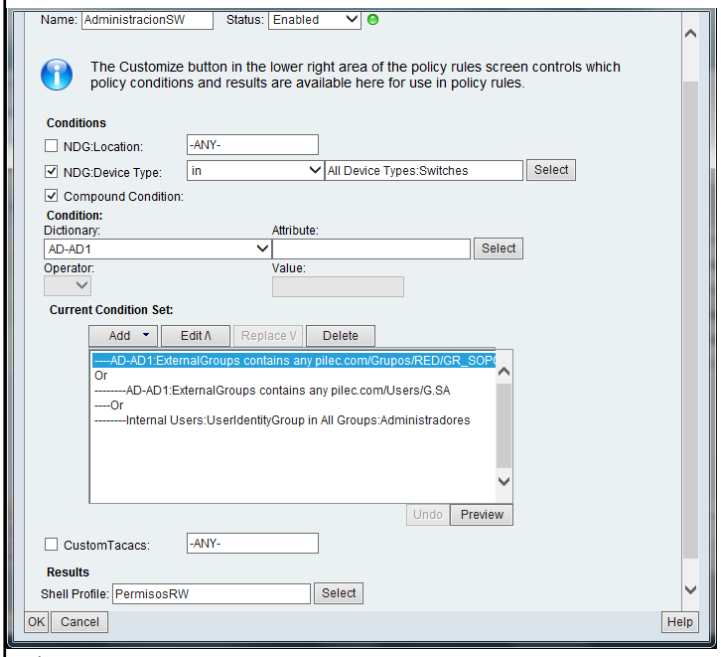


Figura 67.
Elaborado por: Andrés Valdivieso.

En la figura 68 se muestra un ejemplo de configuración de un grupo de Monitoreo.

Autorización basada en condiciones vía TACACS RO

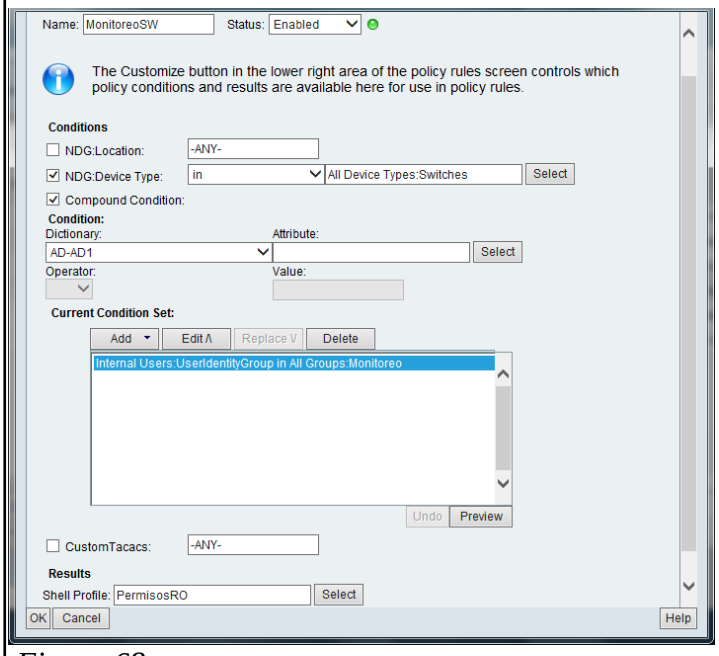


Figura 68.
Elaborado por: Andrés Valdivieso.

3.7 Sincronización del ACS con el servidor NTP

Como requisito para la autenticación de los usuarios, el servidor ACS necesita estar integrado con el servidor NTP, ya que los usuarios que van a ser autenticados para acceder a la red de PIL S. A., deben estar sincronizados con la hora y fecha del servidor.

3.8 Configuración en equipos externos

Además de las configuraciones realizadas en el servidor ACS para proveer la seguridad en el acceso a la red de PIL S. A., a través de la autenticación de los usuarios, se debe configurar la seguridad entre ciertos equipos, como los que se detallan a continuación.

3.8.1 Switch

3.8.1.1 Configuración global

En la figura 69, se muestra la configuración realizada en los switch para la autenticación, activando los protocolos RADIUS y TACACS+ a través de la línea de comandos (CLI).

Configuración global de RADIUS y TACACS+ en Switch

```
aaa new-model

aaa authentication login default group tacacs+ local

aaa authentication dot1x default group radius

aaa authorization exec default group tacacs+ local

aaa authorization network default group radius

aaa accounting exec default start-stop group tacacs+

aaa accounting network default start-stop group radius

dot1x system-auth-control

tacacs-server host X.X.X.X key Pilsen2k13

tacacs-server directed-request

radius-server host X.X.X.X auth-port 1645 acct-port 1646 key
Pilsen2k13

radius-server vsa send accounting

radius-server vsa send authentication
```

Figura 69.
Elaborado por: Andrés Valdivieso.

3.8.1.2 Configuración por puerto

En la figura 70, se muestra la configuración realizada en el switch para activar el procolo 802.1X para la autenticación por puerto.

Configuración por puerto de 802.1x en Switch

```
switchport mode access
switchport voice vlan 100
authentication event fail action authorize vlan 8
authentication event server dead action authorize vlan 1
authentication event no-response action authorize vlan 8
authentication event server alive action reinitialize
authentication host-mode multi-domain
authentication order mab dot1x
authentication priority dot1x mab
authentication port-control auto
authentication violation replace
mab
dot1x pae authenticator
spanning-tree portfast
```

Figura 70.
Elaborado por: Andrés Valdivieso.

3.8.2 Router

3.8.2.1 Configuración global

En la figura 71, se muestra la configuración del protocolo 802.1X en los router.

Configuración global de 802.1x en Router

```
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
tacacs-server host X.X.X.X key Pilsen2k13
tacacs-server directed-request
```

Figura 71.
Elaborado por: Andrés Valdivieso.

3.9 Configuración de TACACS+ en EXINDA

En la figura 72, se muestra la configuración en el EXINDA (Administrador de Ancho de Banda), para la autenticación mediante el protocolo TACACS+.

Configuración de TACACS en Exinda

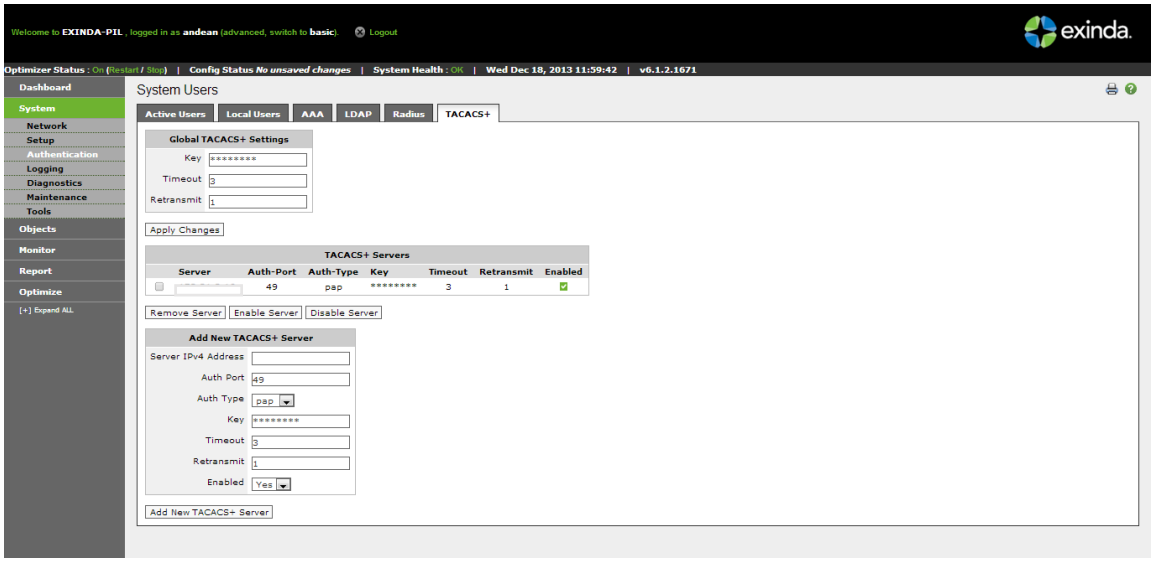


Figura 72.
Elaborado por: Andrés Valdivieso.

3.10 Configuración en el Wireless Lan Controller

El WLC instalado en la infraestructura de la red de PIL S. A., es el modelo 2504, este se encuentra configurado con los protocolos LWAPP (Protocolo Ligero para Puntos de Acceso) y CAPWAP (Control y Aprovisionamiento de los Puntos de Acceso Inalámbricos). En la red de PIL se encuentran configurados un total de cuatro SSID (Service Set Identifier), esto permitirá dar un servicio diferenciado dependiendo del tipo de usuario que se asocie a la red inalámbrica. Cada SSID se configuró con un nivel de seguridad acorde a los requerimientos de PIL S.A.

3.10.1 Ingreso al WLC

Se accedió a la interfaz gráfica del WLC a través del browser para realizar las configuraciones necesarias para la autenticación de los usuarios conectados a la red inalámbrica por medio del protocolo. En la figura 73 se muestra la interfaz gráfica del WLC.

Usuarios de administración de la WLC

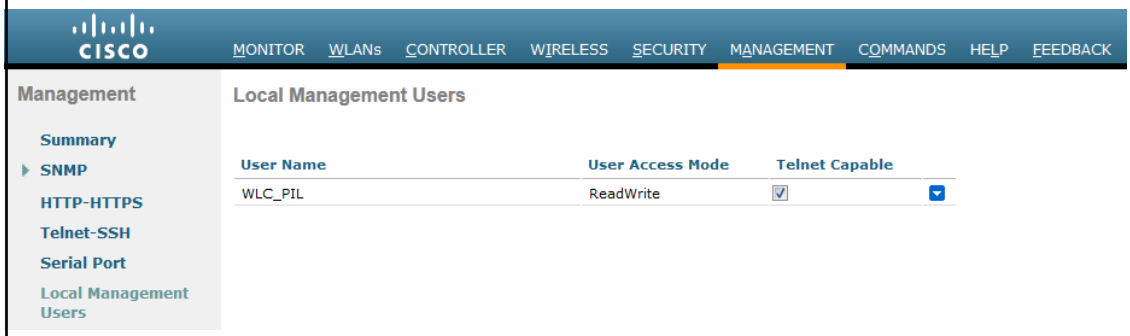


Figura 73.
Elaborado por: Andrés Valdivieso.

La versión instalada en el WLC es la 7.5.102.0 y se encuentra configurada para soportar hasta 25 puntos de acceso, de los cuales solo únicamente están conectados 8 puntos de acuerdo a las necesidades de PIL S. A.

Para el registro de los equipos inalámbricos, al WLC fueron actualizados a la última versión de Cisco IOS en el modo LIGHTWEIGHT. Los puntos de acceso fueron nombrados por medio de su ubicación en el piso donde fueron instalados. En la figura 74, se ilustran los puntos de acceso registrados.

Access Points registrados

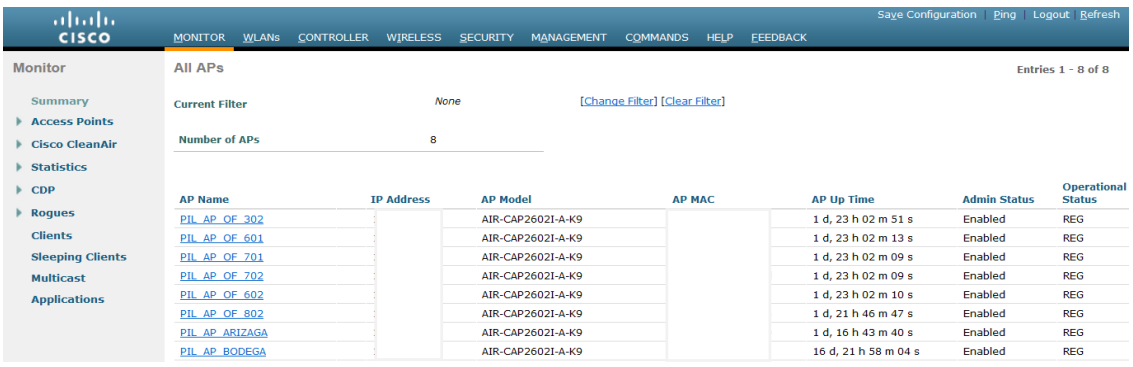


Figura 74.
Elaborado por: Andrés Valdivieso.

3.10.2 Configuración del NTP

En la figura 75, se muestra la sincronización del WLC con el Servidor NTP.

Sincronización con el servidor NTP

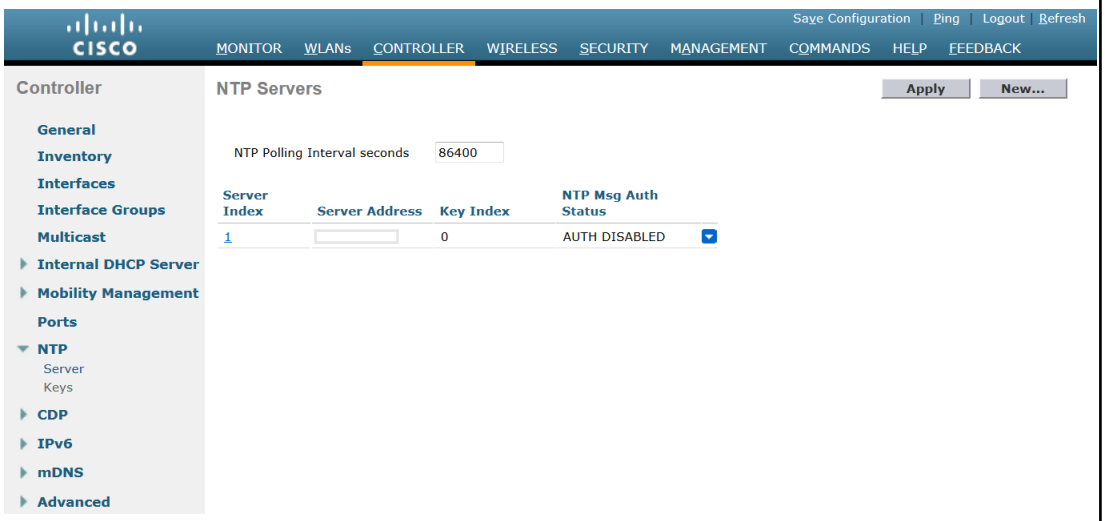


Figura 75.
Elaborado por: Andrés Valdivieso.

3.10.3 Configuración de RADIUS

Se configuró el protocolo RADIUS en el WLC para utilizar 802.1x en el SSID PIL, la IP del servidor de autenticación es la X.X.X.X que corresponde al ACS.

En las figuras 76 y 77 se muestra la configuración de los servicios de Authentication y Accounting en el WLC mediante el protocolo RADIUS.

Configuración de RADIUS para autenticación en WLC

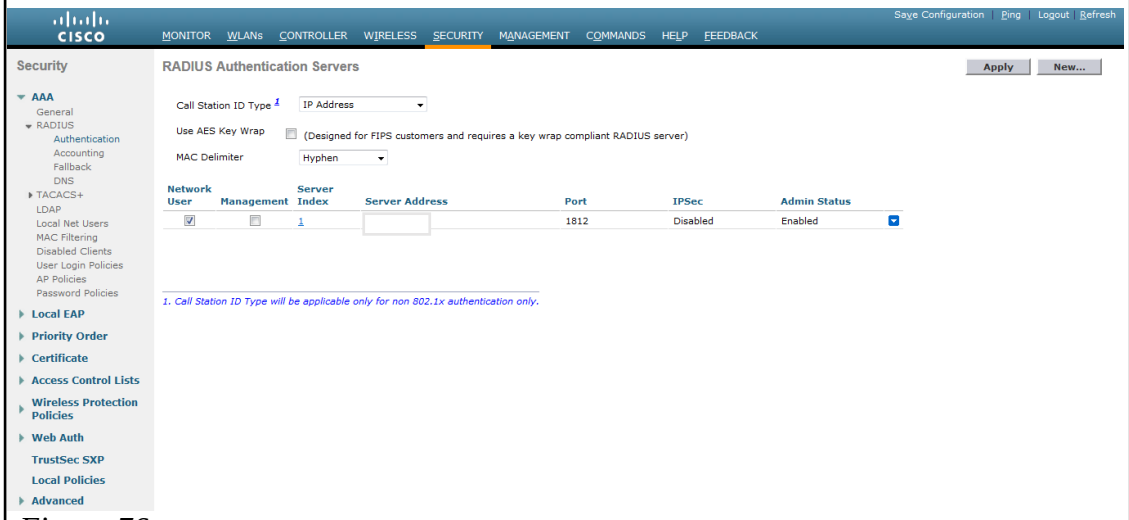


Figura 76.
Elaborado por: Andrés Valdivieso.

Configuración de RADIUS para registro en WLC

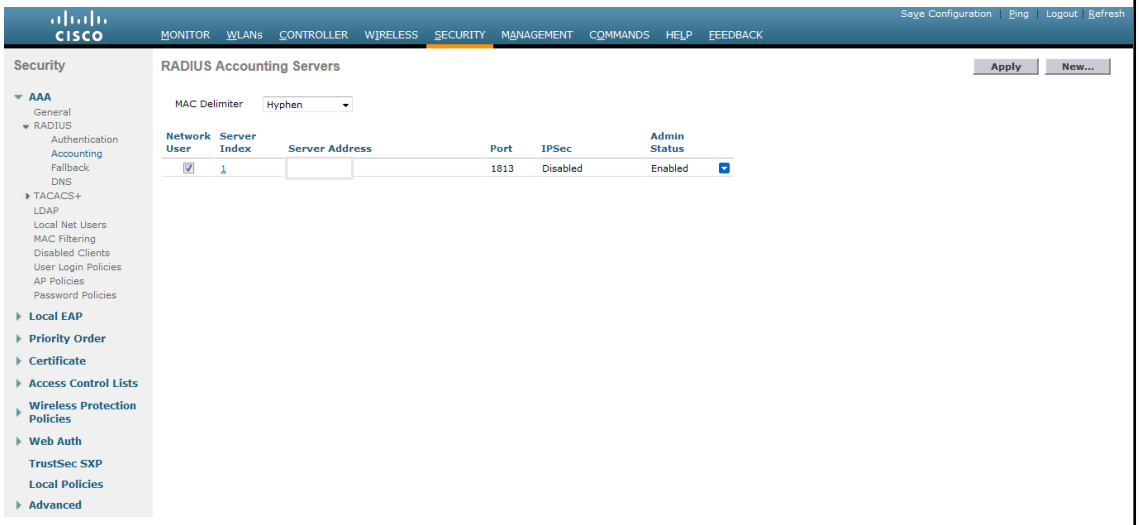


Figura 77.
Elaborado por: Andrés Valdivieso.

Actualmente la infraestructura de acceso y de core de la red corporativa de comunicaciones de Proyectos Integrales del Ecuador PIL S.A., trabaja con equipos de marca Cisco, por lo cual se diseñó un mecanismo de acceso seguro de red, que es compatible con estos dispositivos, mediante un servidor de seguridad de control de acceso CSACS-3415-K9 de la misma marca, con el que se aumentan los niveles de acceso seguro a la red, a través de los servicios de autenticación TACACS+, RADIUS y MAB, previamente implementados por el fabricante, facilitando el trabajo del administrador de red, el cual únicamente debe registrar usuarios y grupos, además de asignar políticas de seguridad de red.

Para implementar más equipos de conmutación Cisco a la red de PIL S.A., hay que asegurarse que el equipo este en modo transparente, se debe configurar el dominio, la contraseña y luego pasarlo a modo cliente, con esto se evitará que posiblemente las VLAN creadas sean borradas si el equipo es conectado directamente.

Para crear y configurar una nueva VLAN el administrador de la red deberá realizarlo en el Switch de Core para facilitar su trabajo, ya que mediante el protocolo VTP esta será propagada a los demás Switchs Cisco de la infraestructura.

Para la implementación de las políticas de acceso seguro de la red de PIL S.A., dentro del servidor de seguridad de control de acceso ACS, fueron creados perfiles de autorización, basados en los grupos añadidos desde la base de datos del directorio activo, en los cuales se especifica cómo se van a autenticar los usuarios.

El servicio de autenticación por Radius de la red de PIL S.A., configurado dentro del ACS está orientado a todos los usuarios registrados en la base de datos del directorio activo para brindarles acceso seguro y conectividad a la red, el servicio de autenticación MAB está orientado a usuarios no registrados en la base de datos del directorio activo, que necesitan hacer uso temporal de los recursos de la red, registrando la dirección MAC del host que desee acceso a la misma.

Para establecer conexión segura entre un dispositivo y el administrador de red de PIL S.A., se debe iniciar una sesión por medio del servicio de autenticación TACACS+, la cual brinda mayor seguridad en la comprobación de sus credenciales por la encriptación total de sus credenciales, el mismo que debe estar previamente registrado en el directorio activo y además tener todos los permisos necesarios de gestión red.

CAPÍTULO 4

PRUEBAS Y RESULTADOS

En este capítulo, se describen las pruebas realizadas de autenticación en el Secure ACS Cisco de los usuarios que necesiten ingresar a la red de PIL S.A.

4.1 Usuario registrado en el dominio

Todo usuario que necesite acceder a la red de la empresa, debe estar registrado en el dominio de PIL S.A. (pilec.com), este es configurado únicamente por el administrador de red del departamento de TI. En la figura 78 se ilustra el certificado de dominio que ha sido establecido en un equipo para un determinado usuario, tanto para acceder a través de la red inalámbrica o cableada.

Equipo registrado con el dominio de pilec.com

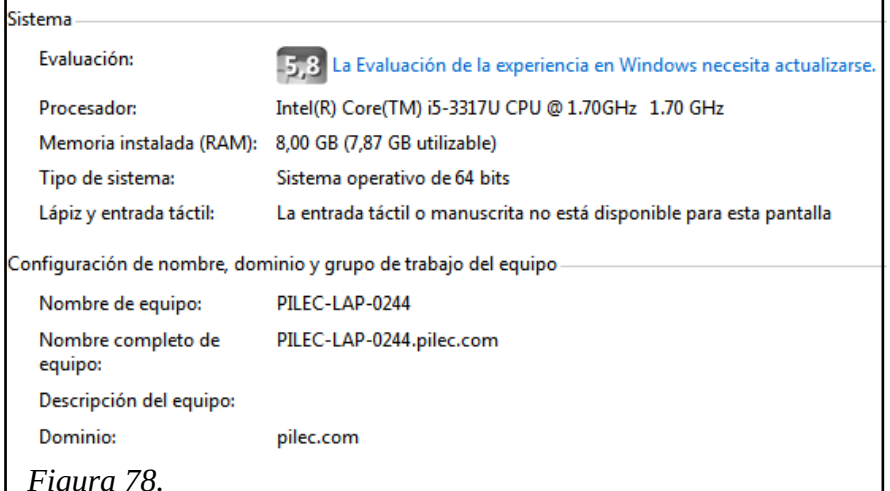


Figura 78.
Elaborado por: Andrés Valdivieso.

En la figura 79 se ilustran los certificados configurados dentro del equipo para establecer una conexión a través de la red inalámbrica, estos certificados son enviados a través de la red por un servidor GPO el cual describe políticas de seguridad y cifrado que no pueden ser modificadas por los usuarios.

Certificados configurados en cada equipo

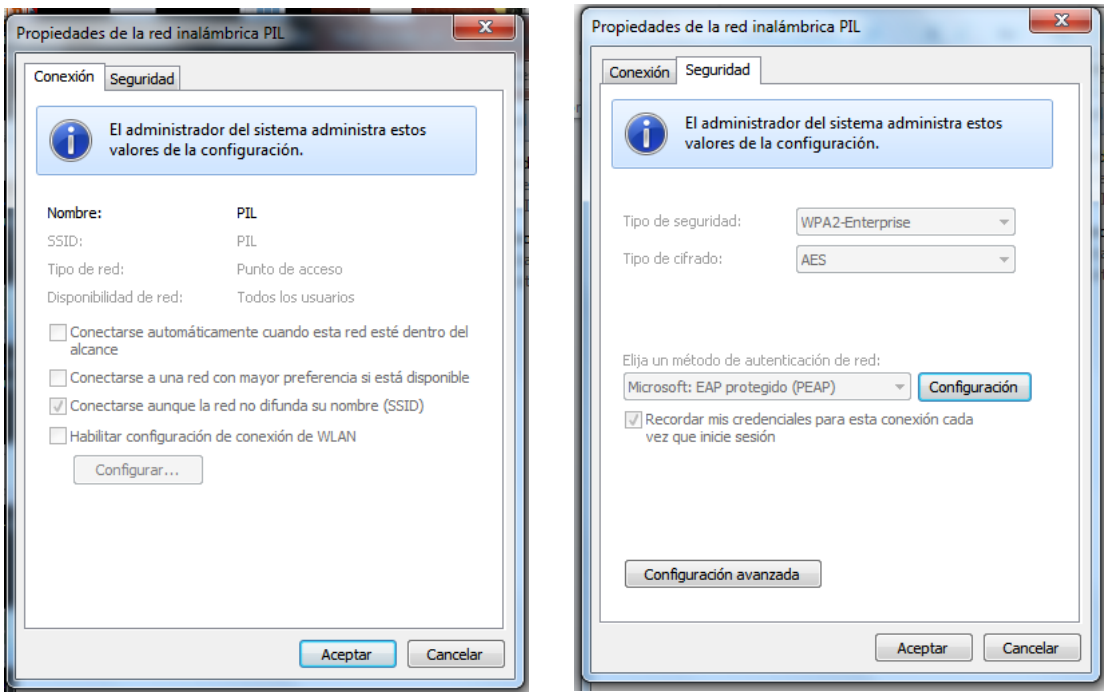


Figura 79.
Elaborado por: Andrés Valdivieso.

4.2 Autenticación RADIUS

La autenticación RADIUS está orientada a los usuarios registrados en el directorio activo de windows de PIL S.A., independientemente del medio físico para el acceso a la red, toda esta información está concentrada en el Secure ACS Cisco en la base de datos local.

A continuación se detallan los diferentes procesos para la autenticación de un determinado usuario.

4.2.1 Autenticación usuario red LAN

En la figura 80 se muestra, que para la autenticación de un usuario en la red, es necesario ingresar sus credenciales (username y password) para el primer inicio de sesión designadas previamente por el departamento de TI, estas están registradas dentro del directorio activo.

El usuario podrá cambiar su contraseña cuando este lo crea necesario, siempre y cuando cumpla con los parámetros (caracteres) designados por el departamento de TI.

Inicio de sesión

Figura 80.
Elaborado por: Andrés Valdivieso.

4.2.1.1 Registro de autenticación en ACS

En la figura 81 se muestra dentro del servidor ACS una lista de los usuarios que están ingresando a la red y que han sido o no autenticados exitosamente para disponer de los recursos de la red, según su perfil creado dentro del directorio activo.

Registro de autenticación RADIUS en el ACS por LAN

AAA Protocol > RADIUS Authentication

Authentication Status : Pass or Fail
Date : February 25, 2015 (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on February 25, 2015 12:43:37 PM ECT

Reload

✔=Pass ✖=Fail =Click for details =Mouse over item for additional information

ACS View Timestamp	ACS Timestamp	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method
Feb 25,15 12:43:17.686 PM	Feb 25,15 12:43:17.666 PM	✖			mantillag		RADIUS	PEAP (EAP-MSCHAPv2)
Feb 25,15 12:43:11.083 PM	Feb 25,15 12:43:11.070 PM	✖			acerca		RADIUS	PEAP (EAP-MSCHAPv2)
Feb 25,15 12:42:53.210 PM	Feb 25,15 12:42:53.196 PM	✔			PILEC\valdiviesca		RADIUS	PEAP (EAP-MSCHAPv2)
Feb 25,15 12:42:42.830 PM	Feb 25,15 12:42:42.826 PM	✔			PILEC\escobarn		RADIUS	PEAP (EAP-MSCHAPv2)

Figura 81.
Elaborado por: Andrés Valdivieso.

En la figura 82 se visualizan los parámetros que posee un usuario autenticado exitosamente a través de la red cableada, entre los que están: hora y fecha en la que se realizó la autenticación, dirección IP, dirección MAC, VLAN, Access Service, dispositivo de red y número de interfaz por el que se realizó la conexión.

Detalle de un usuario autenticado

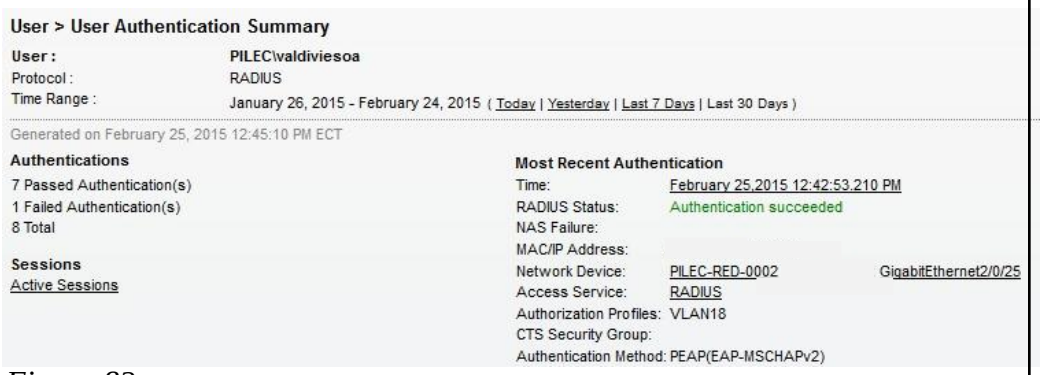


Figura 82.
Elaborado por: Andrés Valdivieso.

4.2.1.2 Propiedades de red de usuario

En la figura 83 se muestra que el usuario ha establecido una conexión exitosa hacia la red cableada de PIL S.A., se visualizan los parámetros tales como dominio, tipo de acceso, direccionamiento físico y lógico.

Recursos de red entregados al usuario autenticado por LAN

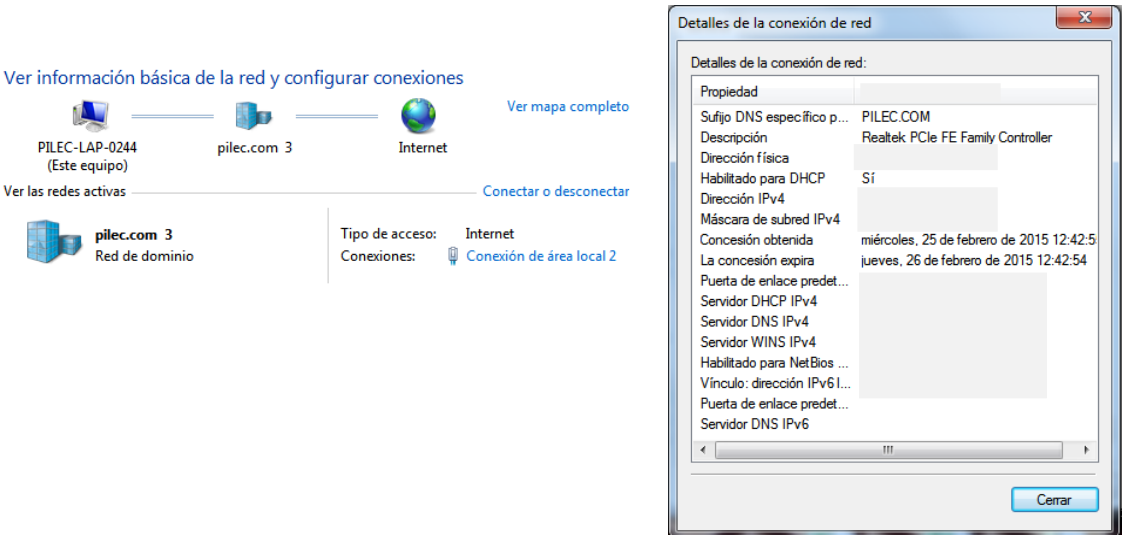


Figura 83.
Elaborado por: Andrés Valdivieso.

4.2.2 Autenticación usuario red WLAN

El proceso de autenticación de un usuario a la red inalámbrica, es el mismo que para una red cableada para su inicio de sesión.

4.2.2.1 Registro de autenticación en WLC

En la figura 84 se muestra un detalle del proceso de autenticación que se está llevando en el WLC de los usuarios que requieren acceder a través de la red inalámbrica.

Detalle del proceso de autenticación RADIUS en el WLC

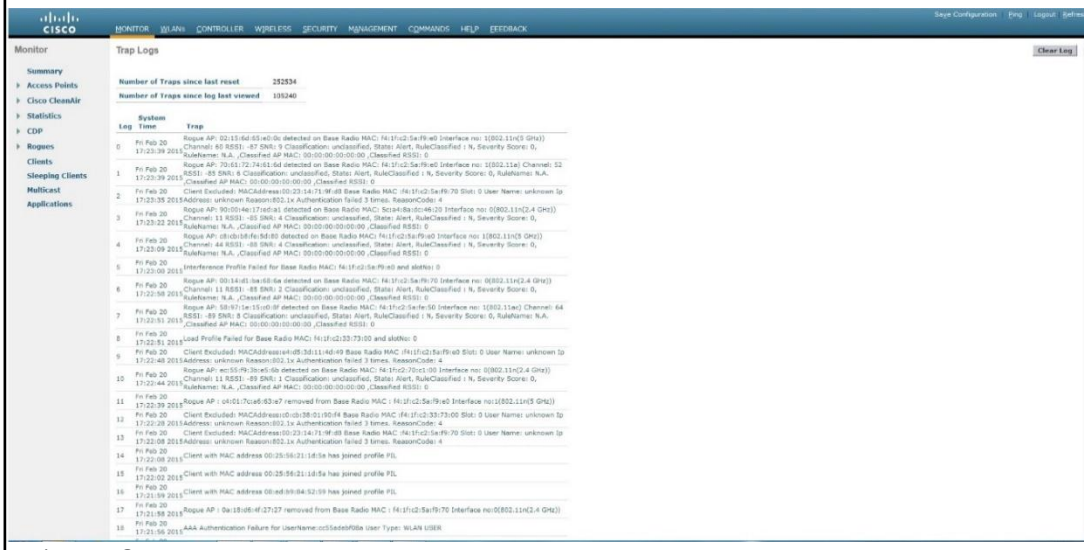


Figura 84.
Elaborado por: Andrés Valdivieso.

4.2.2.2 Registro de autenticación ACS

En la figura 85 se muestra dentro del servidor ACS una lista de los usuarios que están ingresando a la red a través de la infraestructura inalámbrica para disponer de los recursos de la red, según su perfil creado dentro del directorio activo.

Registro de autenticación RADIUS en el ACS por WLAN

Figura 85.
Elaborado por: Andrés Valdivieso.

En la figura 86 se visualizan los parámetros que posee un usuario autenticado exitosamente a través de la red inalámbrica, a diferencia de la conexión cableada no se muestra ninguna información acerca del número de la interfaz, mediante este parámetro se puede diferenciar entre una conexión cableada o inalámbrica.

Detalle de un usuario autenticado por WLAN

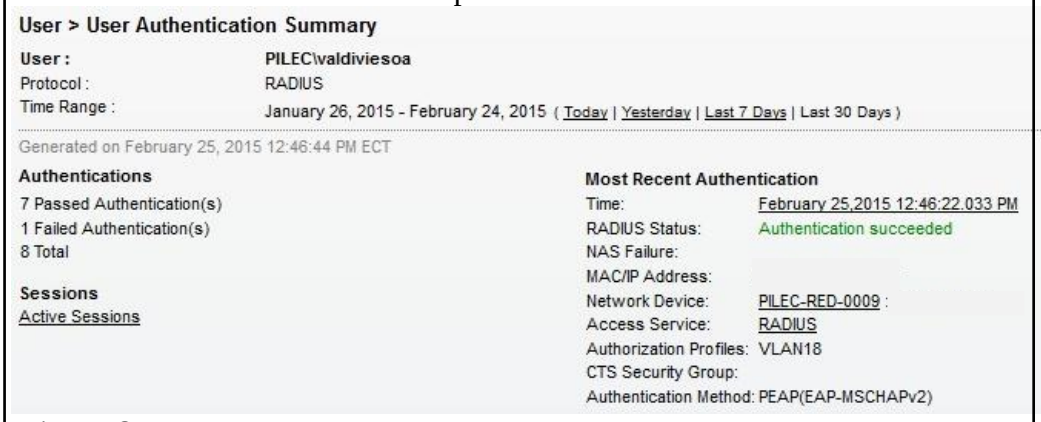


Figura 86.
Elaborado por: Andrés Valdivieso.

4.2.2.3 Propiedades de red de usuario

En la figuras 87 se observa que el usuario ha establecido una conexión exitosa hacia la red inalámbrica de PIL S.A., mostrando parámetros tales como dominio, tipo de acceso, direccionamiento físico y lógico.

Recursos de red entregados al usuario autenticado por WLAN

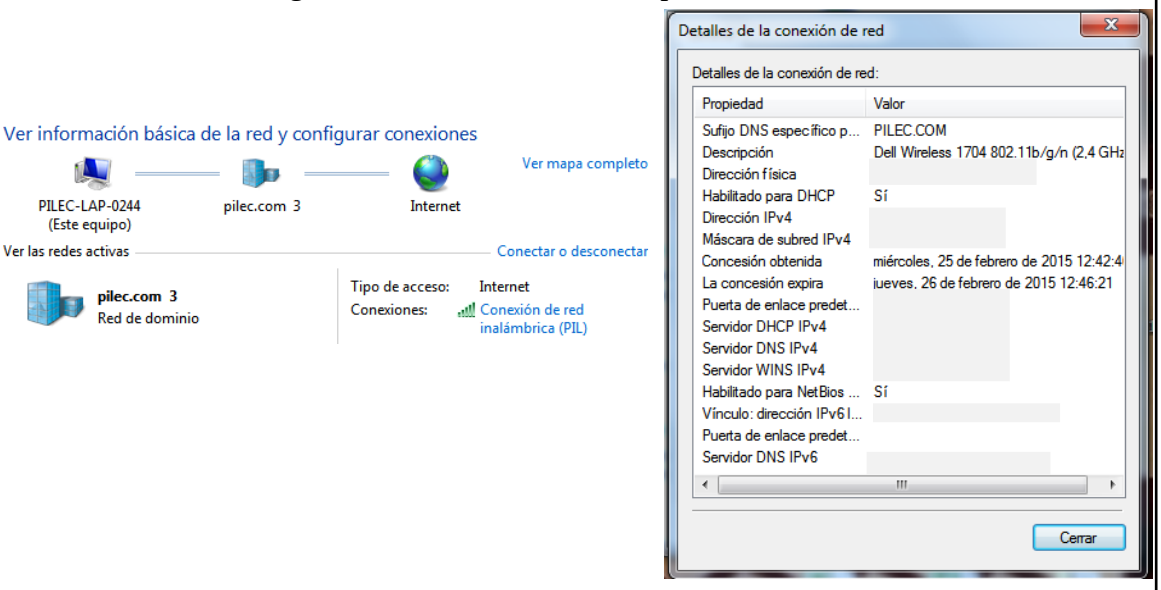


Figura 87.
Elaborado por: Andrés Valdivieso.

4.2.3 Autenticación usuario VPN

Para el proceso de autenticación de un usuario VPN, debe ingresar sus credenciales en el portal cautivo mostrado en la figura 88.

Portal cautivo para VPN

Figura 88.
Elaborado por: Andrés Valdivieso.

4.2.3.1 Registro de autenticación ASA

En la figura 89 se muestra el proceso de autenticación que realiza un usuario VPN a través del ASA.

Autenticación de usuario por VPN

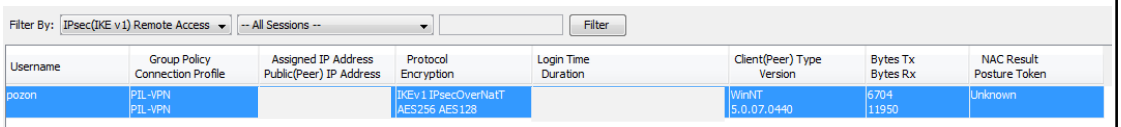


Figura 89.
Elaborado por: Andrés Valdivieso.

4.2.3.2 Registro de autenticación ACS

En la figura 90 se muestra dentro del servidor ACS una lista de los usuarios que están ingresando a la red por medio de VPN, para disponer de los recursos de la red, según su perfil creado dentro del directorio activo.

Registro de autenticación RADIUS en el ACS por VPN

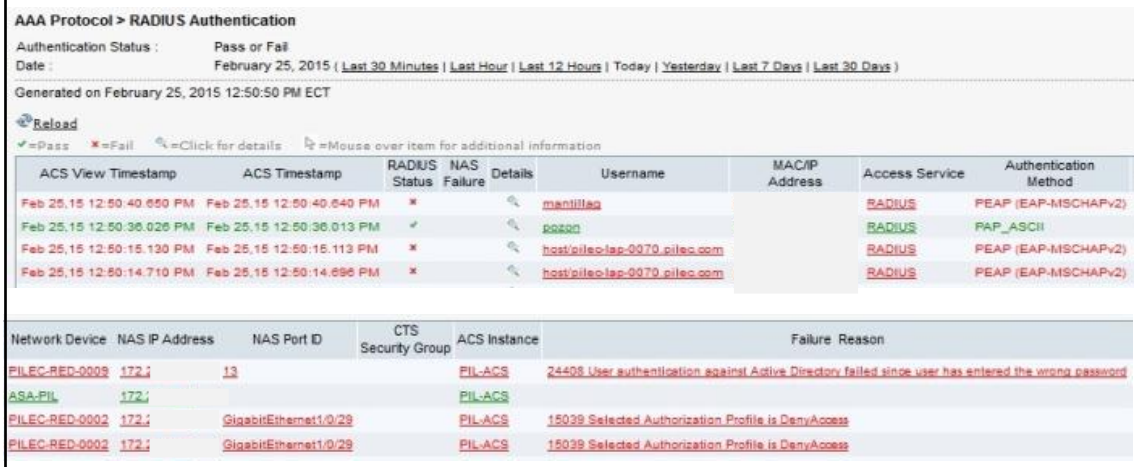


Figura 90.
Elaborado por: Andrés Valdivieso.

En la figura 91 se visualizan los parámetros que posee un usuario VPN autenticado exitosamente, a diferencia de los anteriores casos de autenticación se visualiza en el parámetro de dispositivo de red la conexión a través de túnel VPN hacia el ASA.

Detalle de un usuario autenticado por VPN

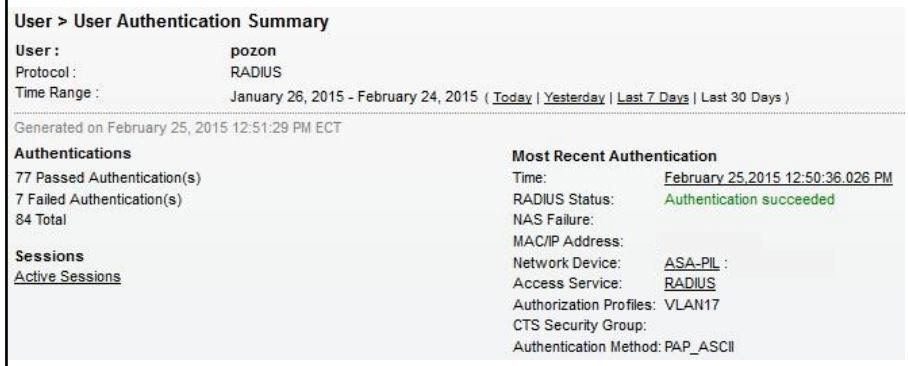


Figura 91.
Elaborado por: Andrés Valdivieso.

4.2.4 Autenticación MAB

La autenticación por MAB se lleva a cabo cuando un usuario quiere acceder a la red, pero no está registrado en el directorio activo de PIL S.A., para llevar este proceso a cabo el usuario debe proporcionar la información de la dirección MAC de su equipo al personal de TI para su respectivo registro en la base de datos local del ACS.

4.2.4.1 Registro de autenticación MAB

En la figura 92 se muestra dentro del servidor ACS una lista de los usuarios que están ingresando a la red mediante MAB para disponer de los recursos de la red. A diferencia de las anteriores autenticaciones con dispositivos pertenecientes al directorio activo, se puede visualizar que el username del equipo autenticado es su dirección MAC.

Registro de autenticación RADIUS en el ACS con MAB

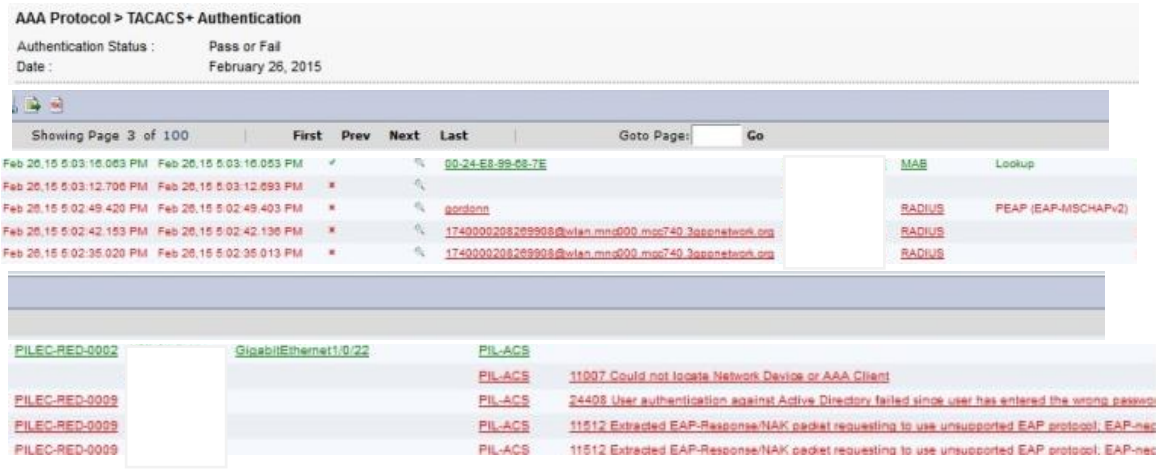
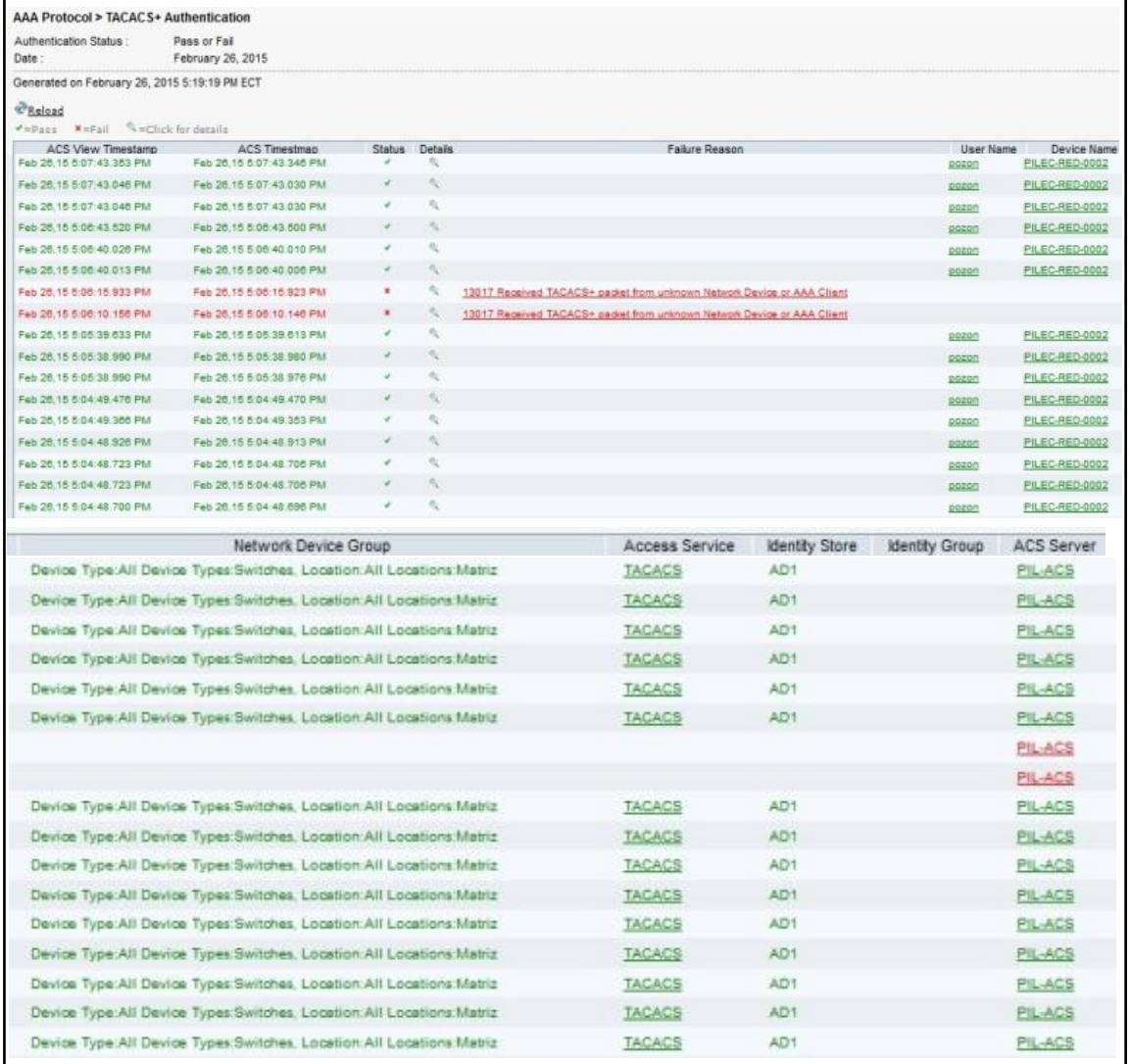


Figura 92.
Elaborado por: Andrés Valdivieso.

4.3 Autenticación TACACS+

En la figura 93 se muestra el registro de autenticación que se ve en el ACS realizado por el administrador de TI a través del protocolo TACACS+, esto se relaiza para acceder remotamente a los equipos de la red de PIL S.A., que están registrados en el directorio activo.

Registro de autenticación TACACS+ en el ACS



AAA Protocol > TACACS+ Authentication

Authentication Status : Pass or Fail
Date : February 26, 2015

Generated on February 26, 2015 5:19:19 PM ECT

Reload

✔=Pass ✖=Fail =Click for details

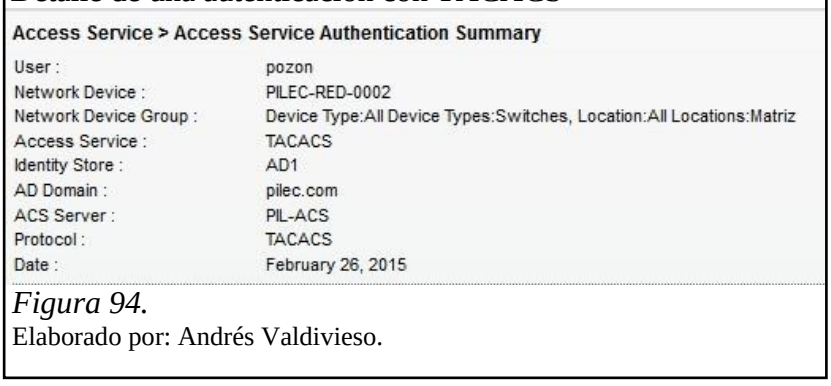
ACS View Timestamp	ACS Timestmap	Status	Details	Failure Reason	User Name	Device Name
Feb 26,15 5:07:43.353 PM	Feb 26,15 5:07:43.346 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:07:43.046 PM	Feb 26,15 5:07:43.030 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:07:43.046 PM	Feb 26,15 5:07:43.030 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:06:43.520 PM	Feb 26,15 5:06:43.500 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:06:40.026 PM	Feb 26,15 5:06:40.010 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:06:40.013 PM	Feb 26,15 5:06:40.006 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:06:15.933 PM	Feb 26,15 5:06:15.923 PM	✖		13017 Received TACACS+ packet from unknown Network Device or AAA Client		
Feb 26,15 5:06:10.156 PM	Feb 26,15 5:06:10.146 PM	✖		13017 Received TACACS+ packet from unknown Network Device or AAA Client		
Feb 26,15 5:05:39.633 PM	Feb 26,15 5:05:39.613 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:05:38.990 PM	Feb 26,15 5:05:38.980 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:05:38.990 PM	Feb 26,15 5:05:38.976 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:04:49.476 PM	Feb 26,15 5:04:49.470 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:04:49.366 PM	Feb 26,15 5:04:49.353 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:04:48.926 PM	Feb 26,15 5:04:48.913 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:04:48.723 PM	Feb 26,15 5:04:48.706 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:04:48.723 PM	Feb 26,15 5:04:48.706 PM	✔			pozon	PILEC-RED-0002
Feb 26,15 5:04:48.700 PM	Feb 26,15 5:04:48.696 PM	✔			pozon	PILEC-RED-0002

Network Device Group	Access Service	Identity Store	Identity Group	ACS Server
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
				PIL-ACS
				PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS
Device Type:All Device Types:Switches, Location:All Locations:Matriz	TACACS	AD1		PIL-ACS

Figura 93.
Elaborado por: Andrés Valdivieso.

En la figura 94 se muestra el detalle de la autenticación realizada por el protocolo TACACS+.

Detalle de una autenticación con TACACS+



Access Service > Access Service Authentication Summary

User :	pozon
Network Device :	PILEC-RED-0002
Network Device Group :	Device Type:All Device Types:Switches, Location:All Locations:Matriz
Access Service :	TACACS
Identity Store :	AD1
AD Domain :	pilec.com
ACS Server :	PIL-ACS
Protocol :	TACACS
Date :	February 26, 2015

Figura 94.
Elaborado por: Andrés Valdivieso.

4.4 Autenticación fallida

En la figura 95 se muestra la autenticación fallida, que un usuario realiza a través de un teléfono celular por tiempo agotado de sesión.

Registro de una autenticación RADIUS en el ACS fallida

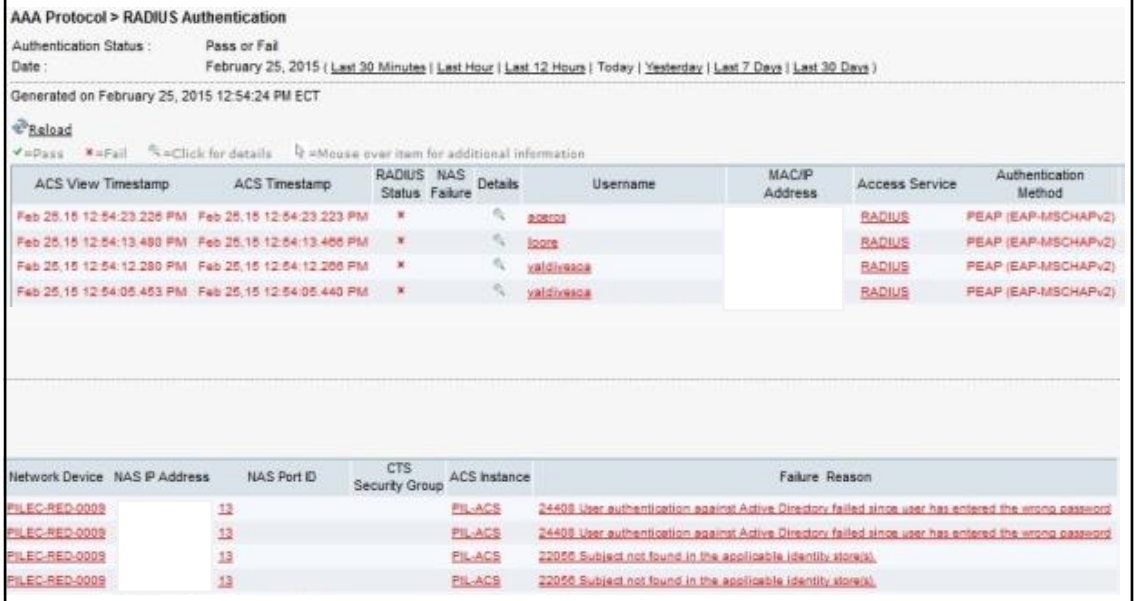


Figura 95.
Elaborado por: Andrés Valdivieso.

En la figura 96 se muestra el estado fallido de la autenticación realizada por un usuario.

Detalle de la autenticación fallida de un usuario

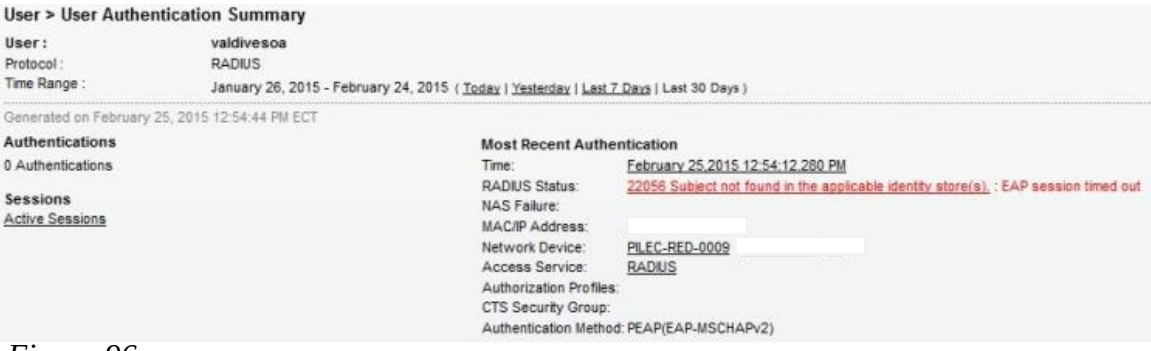


Figura 96.
Elaborado por: Andrés Valdivieso.

De esta manera en este capítulo, se han mostrado las autenticaciones realizadas utilizando el protocolo RADIUS y el protocolo TACACS+.

4.5 Políticas de seguridad

Las políticas de seguridad, fueron configuradas por el departamento de TI de PIL S.A. dentro del Directorio Activo, al que el servidor de Autenticación ACS realiza las consultas para determinar a que recursos de la red puede acceder un determinado usuario, dependiendo de los permisos asignados al mismo; cabe recalcar que otros equipos como el administrador de ancho de banda, el web filter y el firewall de la red, hacen las respectivas consultas con el directorio activo para corroborar los permisos y limitantes que tenga el usuario para con estos servicios.

4.5.1 Recursos de red

Después de que un usuario haya sido autenticado y autorizado en la red de comunicaciones de PIL S.A. podrá ingresar a los recursos de la red como se muestra en la figura 97.

Recursos de red

Figura 97.
Elaborado por: Andrés Valdivieso.

4.5.2 Acceso permitido

Para este ejemplo se utilizo un usuario del grupo operaciones VLAN 18, dentro de sus permisos esta poder acceder a todos los recursos de red que estén enfocados a la parte técnica, por lo que se intentara ingresar a la unidad organizativa (Documentos Ingenieros), como se muestra en la figura 98 el acceso fue permitido y se puede acceder a dicha información.

Acceso permitido

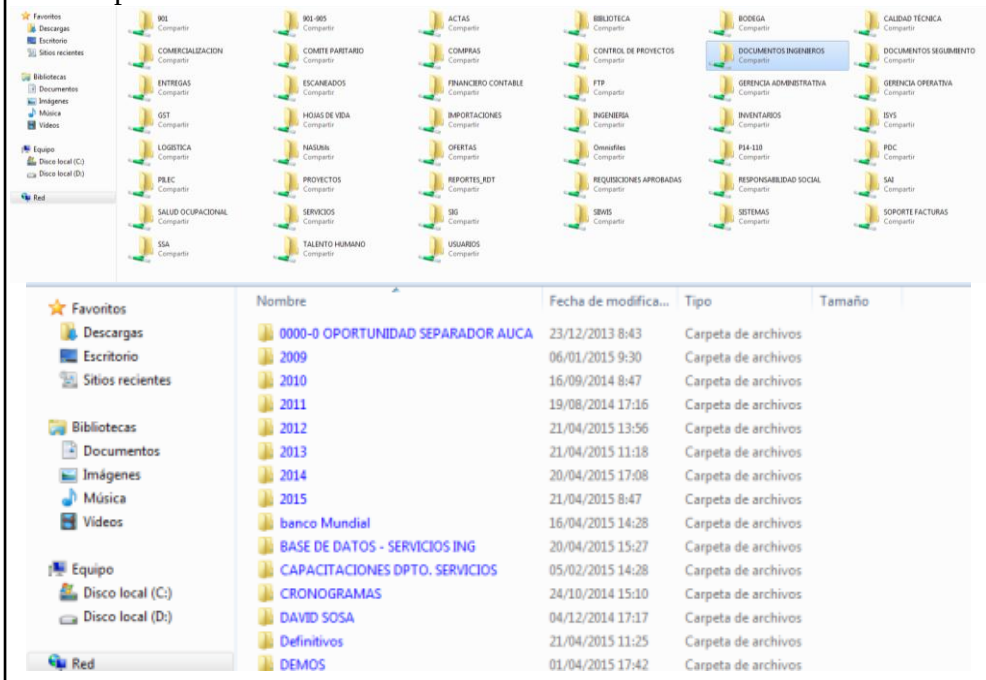


Figura 98.
Elaborado por: Andrés Valdivieso.

4.5.2 Acceso denegado

Para este ejemplo se utilizo un usuario del grupo operaciones VLAN 18, dentro de sus permisos esta poder acceder a todos los recursos de red que estén enfocados a la parte técnica, por lo que se intentará ingresar a la unidad organizativa (Gerencia Operativa), como se muestra en la figura 99 el acceso fue denegado y no se podrá acceder a esta información.

Acceso denegado

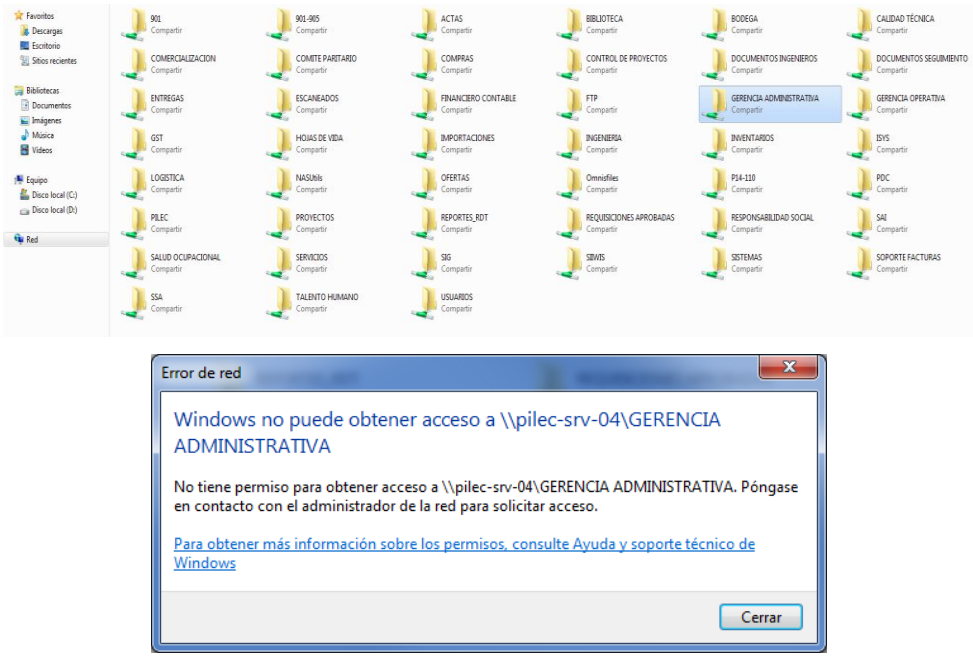


Figura 99.
Elaborado por: Andrés Valdivieso.

CONCLUSIONES

El diseño de una solución utilizando el servidor de autenticación CISCO ACS conjuntamente con dispositivos de acceso de red, de la misma marca compatibles con los servicios de autenticación propuestos por el servidor el cual tiene incorporados de fabrica los protocolos RADIUS, TACACS+ y MAB, facilitó la creación de usuarios, grupos y la asignación de políticas de seguridad para el administrador de red.

La implementación de un mecanismo de acceso seguro y conjuntamente con las políticas de seguridad Cisco ACS, y los dispositivos autenticadores de switching, VLAN dinámicas creadas y enviadas por el Switch de Core a todos los equipos de acceso de red mediante VTP, incremento la movilidad y dos niveles de seguridad al mecanismo de acceso seguro actual con respecto al esquema anterior a nivel LAN y WLAN.

Mediante el uso de los protocolos de autenticación RADIUS, TACACS+ y MAB, previamente levantados en el Servidor de Autenticación ACS, se pudo crear diferentes tipos de usuarios previamente registrados en el directorio activo, asociados a políticas de seguridad y autenticación. TACACS+ permite acceder remotamente a los equipos de red de una forma segura y confiable, MAB permite autenticación a los usuarios temporalmente registrados con la dirección MAC del equipo con el que accedieron a la red, además conjuntamente con el firewall ASA de CISCO se permitió la autenticación de usuarios a través de VPN con el protocolo RADIUS.

La implementación del Servidor ACS de Cisco permitió crear localmente registros para monitoreo del cumplimiento de las políticas de seguridad y acceso seguro de red lo que permitirá al personal de TI hacer un análisis del correcto funcionamiento de las políticas implementadas en la red de comunicaciones, llevando un registro de acceso de los usuarios a la red por parte del administrador de red, pudiéndose elaborar cuadros estadísticos que incluyen fecha, hora, tipo de autenticación que uso determinado usuario y recursos de red que ha utilizado mientras estuvo su sesión activa.

RECOMENDACIONES

Cuando se vayan a realizar los upgrades del sistema se recomienda analizar, si este cambio no afectaría a los servicios que están ejecutándose actualmente. Comprendiendo que update corresponde realizar una actualización de la versión del IOS/Sistema Operativo con el cual el equipo trabaja actualmente como por ejemplo el Update de IOS 16.3 a IOS 16.3.1 y que upgrade corresponde a realizar un cambio de la versión del sistema y que usualmente corresponde a nuevas funcionalidades y cambios mayores como por ejemplo: el upgrade el cambio de versión 8 a la 9.

Si se presentan problemas de incompatibilidad para ingresar a la interfaz gráfica de los diferentes equipos, es recomendable usar un navegador diferente si se tiene algún problema de visualización o funcionamiento.

Es recomendable crear y tener activo un usuario local de administración en la base de datos local del ACS, esto es en caso de pérdida de conexión con el directorio activo.

Se recomienda sincronizar a todas las PCs a un servidor GPO ya que este envía los certificados a todos los usuarios para que puedan ser autenticados.

Es recomendable en la parte de acceso a red inalámbrica realizar un filtrado por dirección MAC adicional a la autenticación implementada en el proyecto a fin de mejorar la seguridad en el acceso a la red.

LISTA DE REFERENCIAS

Cicenia Cárdenas, K. N., & Vásconez Núñez, V. A. (2011). *Análisis de la Tecnología IBNS como solución AAA (Authentication, Authorization, Accounting) para el Control de Acceso a Redes Corporativas.* Riobamba.

CISCO. (11 de 11 de 2008). *MAC Authentication Bypass Deployment Guide*. Obtenido de http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html

Internet society. (2012). *Seguridad informática SMR*. Obtenido de http://seguridadinformaticasmr.wikispaces.com/TEMA+3+-+SEGURIDAD+L%C3%93GICA

Lescano Rodríguez, M. D. (2009). *Análisis y Diseño de una solución de seguridad para el control de accesos enfocados en la IBNS sobre la infraestructura Tecnológica de una empresa Financiera y de Servicios.* Sangolquí.

Plasencia Bedón, L. C. (2012). *Servidor AAA para validación y control de acceso de usuarios hacia la infraestructura de networking de un ente del Ministerio de Defensa Nacional.* Ibarra.

Red Hat Enterprise Linux. (04 de 08 de 2012). *Manual de referencia*. Obtenido de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ldap.html

Red IRIS. (15 de 07 de 2002). *Seguridad física de los sistemas*. Obtenido de http://www.rediris.es/cert/doc/unixsec/node7.html

RedUSERS. (22 de 02 de 2013). *Seguridad en redes: Autenticación con servidores AAA*. Obtenido de http://www.redusers.com/noticias/seguridad-en-redes-autenticacion-con-servidores-aaa/

GLOSARIO

PIL S.A.: proyectos integrales del Ecuador

RADIUS: remote authentication dial-in user service, protocolo que permite los servicios de autenticación y autorización para aplicaciones de acceso a la red.

TACACS+: terminal access controller access control system, protocolo que permite el servicio de autenticación remota.

IEEE: the Institute of electrical and electronics engineers, es una asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, ingenieros en sistemas e ingenieros en telecomunicación dedicada a la estandarización, entre otras cosas.

802.1X: es la norma de la IEEE que permite el control de acceso a la red basada en puertos.

VPN: virtual private network, tecnología de la red para permitir un acceso seguro a la red local sobre una red pública.

MAB: mac authentication bypass, es una de las técnicas de control de acceso que Cisco ofrece de manera segura, MAB utiliza la dirección MAC de un dispositivo para proporcionar el acceso a la red.

LDAP: lightweight directory access protocol, es el protocolo a nivel de aplicación, este permite el acceso a un servicio de directorio ordenado y distribuido con el fin de buscar información en la red.

ACS: access control server, servidor que permite un acceso controlado mediante ciertos protocolos AAA.

AAA: authentication, authorization and accounting, esta sigla se refiere a una familia de protocolos que ofrecen los tres servicios antes mencionados.

UR: unidad de rack, es una unidad de medida usada para describir la altura de un equipo que va ser instalado en un rack equivale a 4,445 cm de alto.

PLATAFORMA: es un sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software, establecen los tipos de arquitectura, sistema operativo, lenguaje de programación o interfaz de usuario con los que es compatible.