UNIVERSIDAD SANTO TOMÁS

MONOGRAFÍA PASANTÍA EMPRESARIAL
DESCA COLOMBIA S.A.

PRESENTADO POR:

GIOVANNI ANDRÉS PULIDO VELANDIA

DIRECTOR:

ING. MARIBEL ANAYA

FACULTAD DE INGENIERÍA ELECTRÓNICA

UNIVERSIDAD SANTO TOMÁS

BOGOTÁ D.C.

2015

HOJA DE ACEPTACIÓN

Firma del Estudiante

Firma del Tutor

Bogotá, Octubre de 2015

TABLA DE CONTENIDO

INTRODUCCIÓN

El siguiente documento contiene el desarrollo teórico y práctico que se llevó a cabo para la realización de un sistema de control de acceso para la administración y seguridad de equipos de red por medio de un servidor ACS (Access Control Server), evidenciando su elaboración ceñida a lo estipulado en la opción de grado de pasantía empresarial realizada en la empresa Desca Colombia S.A.

En conclusión, se establece la puesta en marcha de una red de comunicación constante del usuario y los equipos de red con la intermediación de un servidor con la debida configuración y protocolo de acceso, además de una descripción detallada de los pasos que se siguieron para la correcta ejecución del mismo. Se determina por medio de un estudio de factibilidad de implementación para clientes de la compañía con el objetivo de asegurar el ingreso a los equipos de red y general proteger la red de la compañía y la de sus clientes de cualquier posible ataque.

El contenido del documento, en primera parte cuenta la problemática que se pretende solucionar, mencionando el motivo por el cual es necesario para Desca Colombia S.A disminuir y optimizar la ejecución de labores. Además, se denotan algunos antecedentes basados en la implementación de protocolos de comunicación similares, así como el porqué de la realización del proyecto y sus objetivos a lograr. En segunda medida, se presenta el componente humanístico, resaltando las virtudes y el compromiso de responsabilidad social que el ingeniero tomasino posee; seguido de un marco teórico en donde se contextualizan conceptos necesarios para la elaboración del proyecto.

En tercera instancia, se acata el diseño metodológico, presentación de las herramientas y dispositivos a manejar durante el proceso de ejecución así como las técnicas de recolección de datos. Finalmente, se presentan las conclusiones relacionadas a la elaboración del proyecto junto con el material bibliográfico adicional citado y consultado que fue requerido para la elaboración del trabajo.

1. TITULO

SISTEMA DE CONTROL DE ACCESO PARA LA ADMINISTRACIÓN Y SEGURIDAD DE EQUIPOS DE RED.

2. PROBLEMA

El creciente desarrollo tecnológico ha generado que industrias de telecomunicaciones se expandan y desarrollen cada día más sus infraestructuras de TI (Tecnologías de Información), con el crecimiento surgen amenazas constantes que planean obtener provecho de la información privada que circula en la red de la compañía y sus clientes. La seguridad que proporciona el sistema de control de acceso es la más óptima, ya que ejecuta una completa administración de dispositivos con autenticación, autorización de comandos y registro de actividades de usuarios dentro de los equipos de red, para cubrir todas las brechas en la seguridad y obtener confianza en la red.

La dependencia de la red dentro de una compañía la cual lleva a cabo rutinas de trabajo diarias durante 24 horas los 7 días de la semana y el creciente número de métodos disponibles para acceder a las redes de hoy en día, las brechas de seguridad y el acceso de usuarios no controlado son preocupaciones de considerable prioridad en las empresas. De ahí la necesidad de buscar soluciones que apoyan las políticas de autenticación y autorización flexibles que están vinculados no sólo a la identidad de un usuario, sino también en el contexto de cómo se está accediendo a la red. Además, hay una necesidad fuerte de auditar eficazmente el uso de dispositivos de red, monitorear las actividades de los administradores de dispositivo para el cumplimiento corporativo, y proporcionar visibilidad y control más amplio sobre las políticas de acceso al dispositivo a través de la red.

Posterior a un análisis que se hizo al área del ROC (Regional Operation Center) dentro de la compañía Desca Colombia S.A. se encuentra una infraestructura de TI (Tecnologías de Información) compuesta por varios equipos a los cuales se puede ingresar ya sea para configurar o ejecutar determinadas tareas por medio de comandos, sin la implementación de una plataforma de control de acceso de la empresa basada en políticas y administración de dispositivos de red, omitiendo las reglas de acceso lo cual puede generar entorpecimiento de las comunicaciones con los clientes.

Después de contemplar los anteriores puntos junto con la necesidad de mejorar la seguridad de la infraestructura de telecomunicaciones, toda la problemática es desarrollada en torno a la implementación de una completa plataforma de control.

3. ANTECEDENTES

La década de los 80's fue marcada por el surgimiento de la primera computadora. Entre 1988 y 1993, NeXT fabricó una estación de trabajo de altos recursos para la época con un sistema operativo propio, contaba con un micro de la serie (68040) de Motorola capaz de trabajar a 25 MHz, una memoria de 8 MB ampliables a 64 MB. La máquina que se observa en la figura 1 de Anexos, recibió el nombre de NeXT Computer, aunque se le acabó conociendo como NeXTcube o, simplemente, "The Cube". La NeXT Computer ha pasado a formar parte importante de todo el desarrollo de la infraestructura de las comunicaciones por ser el ordenador, que se utilizó por primera vez como un Servidor Web.

Como resultado del crecimiento de la Internet, se produjo un cambio de gran importancia para la red y su gestión. Para facilitar el uso de Internet por sus usuarios se asignaron nombres a las computadoras conectadas a la red de forma que resultara innecesario recordar sus direcciones numéricas. Originalmente había un número muy limitado de máquinas, por lo que bastaba con una simple tabla con todos los ordenadores y sus direcciones asociadas.

El incremento del tamaño de la Internet resultó también un desafío para los routers. Originalmente había un sencillo algoritmo de enrutamiento que estaba implementado uniformemente en todos los routers de Internet. A medida que el número de redes en Internet se multiplicaba, el diseño inicial no era ya capaz de expandirse, por lo que fue sustituido por un modelo jerárquico de enrutamiento con un protocolo IGP (Interior Gateway Protocol) usado dentro de cada región de Internet y un protocolo EGP (Exterior Gateway Protocol) usado para mantener unidas las regiones.[1]

En un contexto general se puede decir que debido al constante crecimiento de la internet y las tecnologías a su alrededor como se ilustra en la figura 2 de Anexos, compañías como Cisco han aumentado su portafolio de servicios ofreciendo todas las herramientas para la gestión de la red conformada por los equipos que ellos mismos suministran, razón por la cual es importante utilizarlas y darles un uso correcto.

[1] *http://www.gitsinformatica.com/historia%20de%20internet.html*

JUSTIFICACIÓN

Con el desarrollo de este proyecto se complementa todo el proceso de pasantía empresarial ya que es la manera en la cual se entrega a la compañía Desca Colombia S.A. un resultado de los conocimientos adquiridos en el tiempo que se ejerce como practicante.

La pasantía empresarial es una experiencia que dentro del ambiente laboral forma al ingeniero electrónico para que este escoja el área de su preferencia y en la cual cree que pueda aportar todo su potencial, además son enriquecedoras las relaciones personales que se construyen ya que esto facilita no solo el desarrollo como persona sino como profesional. El proyecto es el reflejo de conocimientos adquiridos que entrega un beneficio a la compañía pero que además entrega al ingeniero un desarrollo que le aporta para su formación profesional.

Para la compañía el proyecto tiene un interés considerable porque se entrega una solución benéfica dentro del campo de la seguridad en la red de gran importancia en la actualidad por todos los riesgos latentes a los que es expuesta una red de cualquier compañía. Con la implementación del control de acceso se combatirá todo posible riesgo a través de una solución que entrega flexibilidad y control sobre las configuraciones planeadas para los equipos de red según las políticas de seguridad.

Durante la ejecución del proyecto se pondrán a prueba conocimientos vistos en el área de las comunicaciones y la programación con el objetivo de configurar un ACS (Access Control Server) bajo los parámetros de seguridad de la empresa, de esta manera evitar cualquier incidente en los equipos de red. Debido a la falta de conocimiento en algunos temas de redes es necesario consultar al tutor en la compañía para un soporte mayor al desarrollo del proyecto.

OBJETIVOS

3.1 Objetivo General

Implementar un sistema de control de acceso a través de un ACS (Access Control Server) para los equipos de red de la compañía Desca Colombia S.A., con el fin de aumentar la seguridad de la infraestructura de tecnologías de información.

3.2 Objetivos Específicos

- Realizar las investigaciones y pruebas con ayuda del tutor en la compañía, acerca de la configuración de un ACS (Access Control Server) para determinar los alcances de seguridad que se obtienen para los equipos de la red.

- Identificar los usuarios de la empresa que accedan a los equipos de red, para determinar con base a las políticas de seguridad las restricciones que van a tener al acceder al sistema.

- Analizar el funcionamiento de un ACS (Access Control Server) al ejecutar las restricciones configuradas logrando determinar un modo de operación óptimo y adecuado.

- Establecer las políticas de seguridad de la compañía para el acceso de usuario y la ejecución de comandos por este mismo con el fin de minimizar el riesgo al que son expuestos los equipos de red.

- Hacer un estudio de factibilidad de acuerdo a los resultados obtenidos con la implementación del sistema propuesto en otras áreas de la compañía.

4. FACTIBILIDAD

Esta clase de proyecto puede ser implementado en empresas con una infraestructura de tecnologías de información que necesiten proteger sus equipos de red, de usuarios no deseados obteniendo una alta probabilidad de mejorar la seguridad.

Para llevar a cabo exitosamente este proyecto se deben realizar consultas o investigaciones constantes además realizar diferentes pruebas del manejo de un ACS (Access Control Server) para hacer un buen uso de la herramienta con la que cuenta la compañía, verificar periódicamente el contenido de los temas a trabajar y hacer las respectivas modificaciones si se requiere, evaluar los resultados obtenidos con cada investigación o prueba que se realizarán antes y después de implementar el control de acceso, para ver si esté funciona adecuadamente y comprobar que el proceso que se está llevando a cabo esté por el camino adecuado de desarrollo, y sea la solución y complemento adecuado para la compañía y el ingeniero que lo está ejecutando. Estas investigaciones y pruebas se deben hacer con la guía del tutor en la compañía para no afectar intereses fuera de lo planeado, lo cual hace que la factibilidad se vea sujeta a la disponibilidad de tiempo por parte del tutor.

La implementación del control de acceso para la compañía Desca Colombia S.A. depende del manejo adecuado del tiempo y los recursos, como disponibilidad de equipos, tiempo de orientación por parte del tutor, acceso al espacio donde se encuentran los equipos de red para su configuración bajo estándares o políticas de seguridad, en beneficio de la compañía en especial el área del ROC donde se encuentran la mayoría de los ingenieros con acceso a los equipos y sientan que están seguros de cualquier amenaza. Por supuesto las ventajas que se obtienen posteriores a la implementación del proyecto empiezan teniendo en cuenta los resultados de la configuración establecida.

Al finalizar la implementación del control de acceso y las investigaciones correspondientes alrededor de la nueva barrera de seguridad establecida en los equipos de red, se realizarán revisiones de las configuraciones escogidas como medida de protección, posteriormente se va elaborar un análisis de resultados y de esta manera saber el alcance que se consiguió al culminar el proceso y así determinar su éxito.

5. FUNDAMENTO HUMANÍSTICO

Durante la elaboración del proyecto de grado siempre estuvieron de la mano la teoría y la práctica que rodea la ingeniería electrónica con el propósito de obtener un resultado satisfactorio, pero además que fuera visible la formación integral del ingeniero que formó la universidad no solo en el aspecto teórico y práctico si no también la formación humanista que refleja la universidad.

De este modo, en la realización del proyecto se evidencia la calidad de la formación profesional que busca la universidad a través de la facultad de ingeniería electrónica y como se destaca en cada uno de los aspectos propuestos la ética que siempre debe tener el profesional en su vida laboral, siendo objetivo con la responsabilidad que la universidad deposita en cada uno de los profesionales que frecuentemente se tienen que enfrentar a la sociedad.

También se observa la responsabilidad adquirida como ingeniero electrónico para ofrecer a la sociedad algo para beneficio de la misma por medio de los conocimientos depositados a lo largo de un proceso educativo, reflejando los aspectos distintivos de la universidad Santo Tomas que la hacen una gran institución de formación integral. Con el proyecto se evidencia el equilibrio tecnológico y ambiental haciendo uso correcto de la tecnología sin consecuencia alguna, por lo tanto la puesta en marcha del sistema de control acceso con servidor ACS no afecta el medio ambiente en ninguna de sus fases de ejecución y finalización.

A través de todo el proceso de elaboración del proyecto se busca proporcionar un registro por medio de un documento que ayude a manera de investigación a los ingenieros que van en búsqueda de respuestas a preguntas que ayuden a su crecimiento profesional. Entorno al documento se pretende que la solución propuesta pueda ser impartida en el ambiente educativo y empresarial ya que reúne conocimientos tecnológicos con una visión económica fomentando el interés intelectual y empresarial.

De igual manera la práctica empresarial fue fundamental en las relaciones personales en un ambiente laboral en donde las personas constantemente son sometidas a distintas problemáticas rutinarias en las cuales se ve reflejado la formación integral de cada uno en búsqueda de mantener un entorno agradable de trabajo.

Con respecto al crecimiento laboral son vitales las relaciones personales no solo con el área de trabajo diario si no también con las demás áreas de la compañía, además en cada actividad es fundamental el trabajo en equipo como principio de colaboración en búsqueda del mismo objetivo bajo las normas éticas y morales del profesional.

Por ultimo aspiro como Ingeniero Electrónico a enfrentar cada una de las adversidades que surjan en el ámbito laboral, ser siempre un profesional integro que aporte a la sociedad con conocimiento pero con los valores y ética que debe tener una persona formada en la Universidad Santo Tomas con aspiraciones a convertirse un excelente profesional.

6. MARCO TEÓRICO

A continuación se definirán algunos conceptos introductorios claves para la realización del proyecto, además se presenta de manera general una contextualización teórica y conceptual sobre el protocolo que se propone utilizar.

6.1 Servidor web

Un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al "servicio" de otras máquinas o personas llamadas clientes y que le suministran a estos, todo tipo de información.[2]

Ver figura 3 de Anexos.

6.2 Red de Telecomunicaciones

La red de telecomunicaciones, es el conjunto de equipos en constante comunicación, consiste en una infraestructura física a través de la cual se transporta la información desde la fuente hasta el destino, y con base en esa infraestructura se ofrecen a los usuarios que se conectan a ella los diversos servicios de telecomunicaciones, es por eso que muchas redes que hoy existen pueden ofrecer voz, datos e imágenes con la calidad de servicio deseada.[3]

Ver figura 4 de Anexos.

6.3 Router

Un router o encaminador es un dispositivo de red que equivale a un PC gestionando varias conexiones de red, lo cual permite que sea utilizado para redes de tamaño considerable disponiendo de gran cantidad de máquinas. Desde el

---

[2] *http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57:herramientas-informaticas&Itemid=179*

[3] *REDES y servicios de telecomunicaciones, 4 edición, José Manuel Huidobro Moya, editorial THOMSON PARANINFO*

punto de vista funcional, este dispositivo puede concebirse como una computadora de propósito específico, en contraposición a una computadora personal a la que suele caracterizarse como de “propósito general”. El Router permite el uso de varias clases de direcciones dentro de una misma red. De este modo permite la creación de subredes. [4]

Ver figura 5 de Anexos.

6.4 Switch

El Switch o conmutador es un equipo electrónico que distribuye los datos a cada máquina de destino, encargado de centralizar las comunicaciones y distribuir la información, esto quiere decir que es el encargado de interconectar dos o más segmentos de red.[5]

Ver figura 6 de Anexos.

6.5 La AAA (Authentication, Authorization and Accounting)

Es un sistema de seguridad que permite validar quién puede conectarse a los equipos de la red y además controlar cuáles comandos están autorizados a ejecutar en el sistema operativo de Cisco.

Authentication: proceso que permite verificar que un individuo es realmente quien dice ser. La validación de un usuario se puede realizar a través de varios métodos, siendo el usuario y contraseña la opción más utilizada.

Authorization: proceso que, luego de autenticar a un usuario, permite controlar a cuáles recursos un usuario tiene derecho a tener acceso. Por ejemplo, un usuario puede tener acceso para entrar a la interfaz del router y modificar su configuración, mientras otro usuario se le niega el acceso a este recurso.

Accounting: proceso mediante el cual el sistema registra cuándo y por cuánto tiempo un usuario tuvo acceso a los recursos del sistema. Esta información es

[4] *http://www.ort.edu.uy/fi/pdf/configuracionroutersciscomatturro.pdf*

[5] *http://www.mcgraw-hill.es/bcv/guide/capitulo/8448171683.pdf*

extremadamente útil para realizar auditorías de seguridad, principalmente después de ocurrido un ataque a la red.[6]

6.6 TACACS+ (Terminal Access Controller Access Control System)

Es un protocolo de seguridad y propiedad de Cisco que proporciona la validación de los usuarios que intentan tener acceso a un servidor de acceso o enrutador de red. Permitiendo a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red, este protocolo o aplicación tiene una estructura muy granular, lo que significa que permite definir permisos de acceso con un alto grado de precisión. Por esta razón TACACS+ es utilizado mayormente para controlar el acceso de los usuarios al sistema operativo de Cisco.[7]

Ver figura 7 de Anexos.

6.7 ACS (Access Control Server)

ACS es un servidor de seguridad basado en políticas que proporciona autenticación compatible con los estándares, autorización y servicios del protocolo (AAA) a la red. Además facilita la gestión administrativa de Cisco y demás dispositivos cuyas aplicaciones no sean propiedad de este. Como plataforma de control de acceso a la red de la empresa, ACS sirve como un punto de integración para el control de acceso a la red y gestión de identidades.

ACS 5.x proporciona un modelo de política basado en reglas que le permite controlar el acceso a la red basado en las condiciones y atributos dinámicos. La política basada en reglas está diseñada para satisfacer las necesidades más complejas de acceso.

Con la utilización del protocolo TACACS +, ACS facilita la gestión administrativa de Cisco y los dispositivos de red que no son Cisco, tales como switches, routers, y gateways, así como de los servicios y entidades tales como acceso telefónico, red privada virtual (VPN) y firewall.

---

[6] *http://blog.capacityacademy.com/2014/07/30/ccna-security-como-configurar-aaa-con-cisco-secure-acs-server/*

[7] *http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scftplus.html*

ACS es el punto de la red que identifica a los usuarios y dispositivos que intentan conectarse a la red. Este establecimiento de identidad puede ocurrir directamente utilizando el archivo de identidad interno ACS para la autenticación de usuario local; o bien, mediante el uso de archivos de identidad externos.[8]

Ver figura 8 de Anexos.

6.8 Hipótesis

Se espera realizar la configuración adecuada de un ACS (Access Control Server) para incrementar la seguridad de los equipos de red que conforman la infraestructura de tecnologías de información. Con esta implementación se quiere tener un control de acceso óptimo que proteja de posibles ataques la red de Desca Colombia S.A. Esto conduce a tener una barrera de seguridad y aumentar la confianza en los empleados de la empresa y tranquilidad en sus labores diarias.

El sistema contará con un ACS (Access Control Server) en constante comunicación con equipos de red (router, switch, AP, firewall, etc.) con la ventaja que estos utilizan la misma base de datos para verificar el acceso de los usuarios al sistema operativo de Cisco.

En el sistema de control de acceso se establecerán los permisos de ingreso para los equipos de red de acuerdo a las políticas de seguridad de la empresa, además se hará uso de restricciones para la ejecución de comandos por parte del usuario.

6.9 Desca Grupoamper Colombia S.A.

Desca hace parte de las múltiples compañías del Grupo Amper, encargada de ofrecer y desarrollar soluciones tecnológicas para facilitar la transformación que constantemente está sufriendo el mercado de las tecnologías. Con una experiencia de más de cincuenta años en el sector de las Tecnologías de la Información y de las Comunicaciones (TIC), ofrecen a sus clientes productos y servicios de vanguardia que permiten cubrir sus necesidades específicas.

Amper inició actividades en 1956. Empresa dedicada a la fabricación de porteros automáticos. En poco tiempo se situó en una posición envidiable en el ámbito de las telecomunicaciones convirtiéndose en uno de los principales proveedores de la

[8] *Guia de usuario acs.pdf, paginas 27-28*

Compañía Telefónica Nacional de España. A lo largo de su historia, y gracias al profundo conocimiento del sector, Amper ha ido adaptándose para dar respuesta a las necesidades y retos específicos de un mercado cada vez más competitivo, complejo y exigente. Esta capacidad de adaptación los ha llevado a especializarse en aquellos segmentos donde, gracias a su flexibilidad y capacidad innovadora, pueden ofrecer ventajas diferenciales.

Amper es hoy, una compañía multinacional española que cotiza en la Bolsa de Madrid. Actualmente, Amper se estructura en dos divisiones, en la primera se encuentra defensa y telecomunicaciones y en la segunda seguridad.
Amper afronta su presente y futuro sustentando su liderazgo en tres pilares básicos: Internacionalización, Eficiencia e Innovación. Su misión es facilitar la transformación del mercado hacia modelos de negocio, integrando soluciones sectoriales y tecnología de comunicaciones apostando por mercados de alto potencial de crecimiento.[9]

[9] *Tomado de la página web Desca-Grupo Amper: http://www.desca.com/latam/index.php/acerca*

7. DISEÑO METODOLÓGICO

En primera instancia se hará una investigación exhaustiva de varios conceptos relacionados con las telecomunicaciones, con especial énfasis en el servidor ACS (Access Control Server) el cual hace posible la configuración del control de acceso sobre cada uno de los equipos de red de la compañía, esta investigación se llevará a cabo con base a la documentación existente tanto en textos como en páginas de internet, además se contara con la constante guía del tutor.

En segunda instancia se determinarán las políticas de control de acceso dentro de los parámetros de la compañía a través de la recolección de datos, posteriormente se hará la configuración en el ACS con todas las políticas adquiriendo un dominio completo sobre toda la infraestructura de tecnologías de información por parte de los usuarios autorizados.

En tercera instancia ya con el sistema implementado se ejecutarán una serie de pruebas de seguridad tales como la incursión de usuario y contraseña, con la espera de una respuesta de autenticación válida o inválida. También se propone una prueba de digitación de comandos autorizados y no autorizados por parte del usuario que tuvo permiso para ingresar al equipo de red.

En cuarta y última instancia el tutor en la compañía hará una valoración concisa y detallada del control acceso en la infraestructura de tecnologías de información de la compañía, en la cual se observe claramente el cumplimiento de todos los objetivos propuestos y además llene las expectativas que desde un principio se esperaban con la formulación del proyecto. Posteriormente se sacarán las conclusiones que entregan el desarrollo y ejecución del proyecto desde mi posición como pasante de ingeniería electrónica y las expectativas que tenía la compañía con todo el proceso desarrollado a lo largo de la pasantía empresarial.

7.1 Especificaciones Técnicas de Cisco Secure ACS[10]

7.1.1 Eléctricas y físicas:

En las tablas 1 y 2 se encuentran todas las especificaciones eléctricas y físicas que posee un ACS (Access Control Server) importantes a tener en cuenta cuando se trabaja sobre cualquier equipo electrónico.

Ver tablas 1 y 2 de Anexos.

7.1.2 Entorno:

En la tabla 3 aparecen las especificaciones de entorno que debe tener el sitio donde se implementaría el ACS (Access Control Server) para su correcto funcionamiento en determinada zona de trabajo.

Ver tabla 3 de Anexos.

7.1.3 Funcionamiento:

En la tabla 4 se encuentran las especificaciones mínimas de funcionamiento para un ACS (Access Control Server) para estar en su punto óptimo de funcionamiento.

Ver tabla 4 de Anexos.

7.2 Conexión del equipo físico

Con base a la información de Cisco, la conexión más viable es la que se muestra en la figura 9 porque es la más eficiente y confiable opción de conectividad que brinda con los dispositivos de red. De esta manera se eligió el modelo de conexión a implementar entre el ACS (Access Control Server) y los dispositivos de red.

[10] *http://www.cisco.com/c/en/us/products/collateral/security/secure-access-control-system/data_sheet_c78-683481.html*

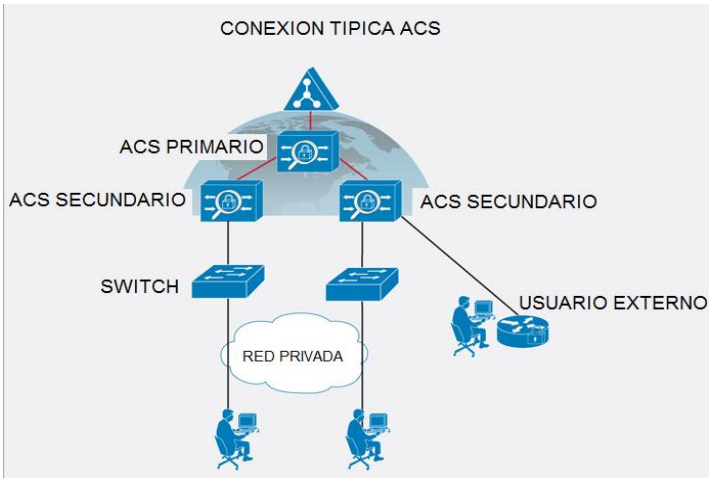

Fig. 9. Diagrama típico de conexión de un ACS.[11]

7.3 Técnicas De Recolección De Datos

La recolección de datos e información es de gran importancia para el establecimiento de las políticas de control de acceso a los equipos de red, es por eso que para obtener datos verídicos se utilizará la técnica de encuesta ya que proporciona mejores beneficios con respecto a la información con los nombres de los usuarios que tendrían acceso a los equipos y el dominio sobre cada uno. También se evidenció el buen estado en el que se encuentra la infraestructura de TI (Tecnologías de Información) de la compañía para el desarrollo del proyecto en condiciones adecuadas.

En este punto de trabajo se deben tener en cuenta las condiciones lumínicas y de espacio facilitan la configuración del ACS (Access Control Server), la toma de datos que es un componente fundamental a la hora de establecer las políticas de seguridad del control de acceso con los equipos de red. Finalmente se verificó la adecuada compatibilidad entre el dispositivo y el software al que estaba comunicado, realizando pruebas piloto de lectura**.**

7.4 Técnicas De Análisis

De los resultados que se obtengan a partir de las pruebas con los usuarios de la compañía que ingresen al sistema de control de acceso, se deben tener en cuenta

[11] *Imagen tomada de la página web: http://www.cisco.com/c/en/us/products/security/secure-access-control-system/index.html*

los siguientes aspectos como el cargo que desempeña dentro de la compañía Desca Colombia S.A. junto con los permisos que dispone sobre los equipos de red y además la auditoria posterior a todas las acciones que se hayan ejecutado dentro los equipos. También se tiene a consideración la cantidad de usuarios los permisos de cada uno y la información con la que se implementa el control de acceso.

7.5 Interfaz del Software

La interfaz web de Cisco Secure ACS está diseñada para ser vista usando Microsoft Internet Explorer 6.x, 7.x, 8.x, y Mozilla Firefox 3.x. La interfaz web no sólo hace que la visualización y administración de ACS sea posible, sino que también le permite monitorear e informar sobre cualquier evento en la red.

Estos reportes informan la actividad en la conexión, muestra qué usuarios se encuentran registrados en la actualidad, la lista de fallos en la autenticación, los intentos de autorización, y demás eventos detectados. [12]

Ver figura 10 de Anexos.

[12] *Guía de usuario acs.pdf, página 95*

8. EJECUCION DEL PROYECTO

8.1 Conexión PC-servidor (ACS)

Según el diagrama típico de conexión de un ACS se establece comunicación entre un PC de la compañía y el servidor, conectando los dos con un cable de red por el puerto Ethernet de tal manera que los dispositivos se reconozcan y se obtenga respuesta adecuada de ambas partes.

Una vez que se ha completado la conexión física y se verificó la comunicación, se procede en el PC a configurar en el centro de redes una red de comunicaciones asignándole una dirección IP dentro del rango de direcciones permitidas por el servidor. Posteriormente se ingresa al servidor a través de la dirección escogida por medio de un navegador ya que es compatible con las versiones de Microsoft Internet Explorer 6 y 7, y Firefox versión 3.x.

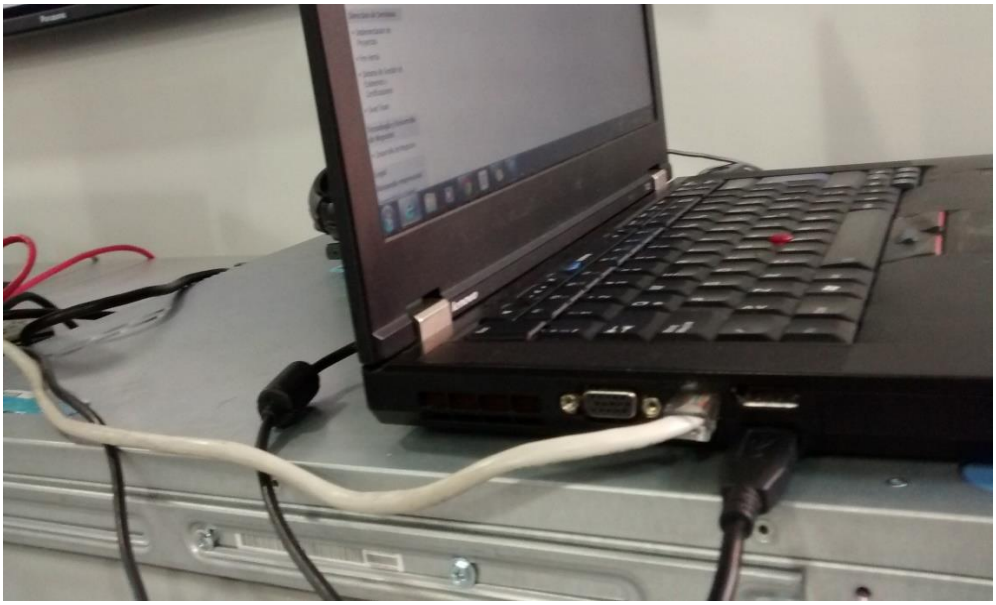

Fig. 11. Conexión física

Fig. 12. Conexión PC – Servidor por cable de red

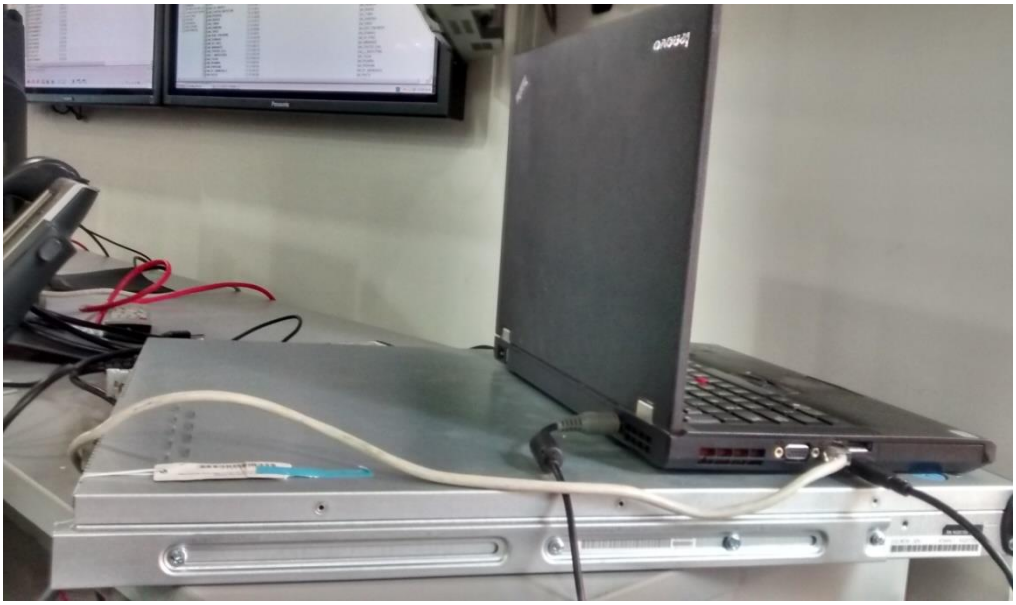

Fig. 13. Conexión PC – Servidor por cable de red al puerto Ethernet

8.2 Acceso a la interfaz Web de un ACS (Access Control Server)

La interfaz web de un ACS está diseñada para ser visualizada facilitando el control sobre el equipo entregando al usuario no solo una completa visualización y administración de recursos, sino que también le permite al usuario monitorear e informar sobre cualquier evento en la red. Estos informes hacen un seguimiento de la actividad de conexión, muestra los usuarios registrados actualmente y una lista de los intentos fallidos de autenticación y autorización.

El acceso a la interfaz web del servidor requiere el ingreso de una dirección en el navegador por ejemplo https: // <acs_host> / acsadmin, donde <acs_host> es la dirección IP, posteriormente aparece la página de inicio de sesión en la cual se introduce por defecto ACSAdmin en el campo nombre de usuario; teniendo en cuenta que el valor no distingue entre mayúsculas y minúsculas. Y por último aparecerá lleno por defecto el campo Contraseña; valor sin distinción entre mayúsculas y minúsculas.

Con el propósito de adquirir un dominio correcto del ACS a través de la interfaz gráfica es fundamental conocer cómo fue diseñada y donde se puede encontrar cada una de las herramientas para usar en cada uno de los cuatro bloques que la conforman. Por ejemplo un primer bloque de encabezado en el cual se observa el usuario actual o sea su nombre de usuario, acceso a la ayuda en línea, cerrar sesión y acceso a la información sobre la instalación y versión de la interfaz web.

El segundo bloque de navegación se compone de cajones con sub-secciones que permiten navegar en la interfaz y acceder a cada una de los ítems de configuración.

El tercero es el bloque de contenido en el cual se puede ver su ubicación actual dentro de la interfaz Web, la configuración de los diferentes servicios AAA debidamente organizados con filtros que facilitan la búsqueda en listas extensas bajo criterios específicos de búsqueda.

El cuarto y último bloque de ubicación actual el cual se encuentra más exactamente en la parte superior del área de contenido permite determinar en la interfaz la ubicación del cajón.

Ver figuras 14, 15, 16, 17.

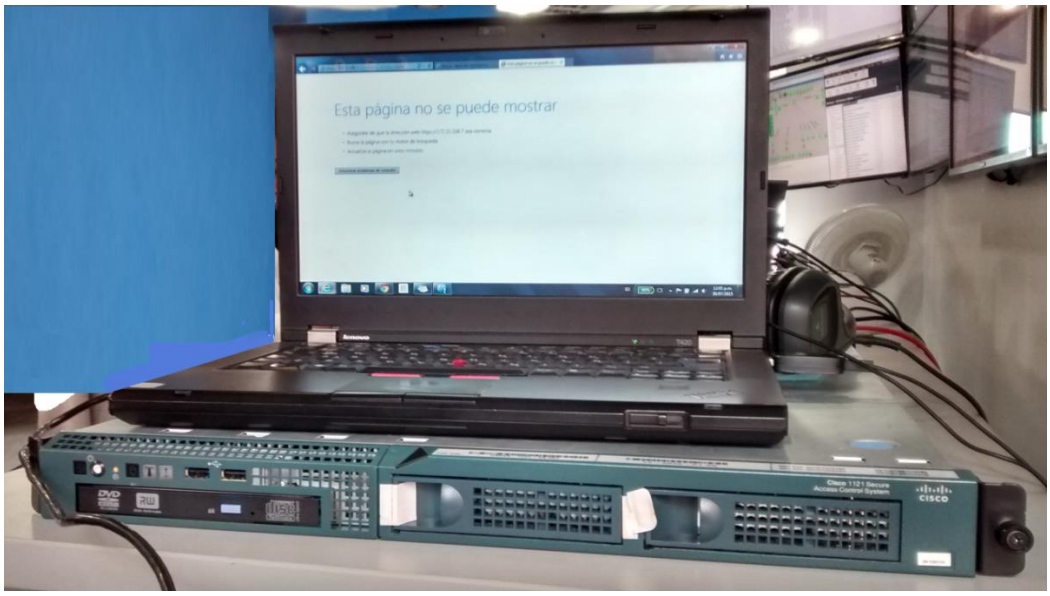

Fig. 14. Ingreso vía web al ACS

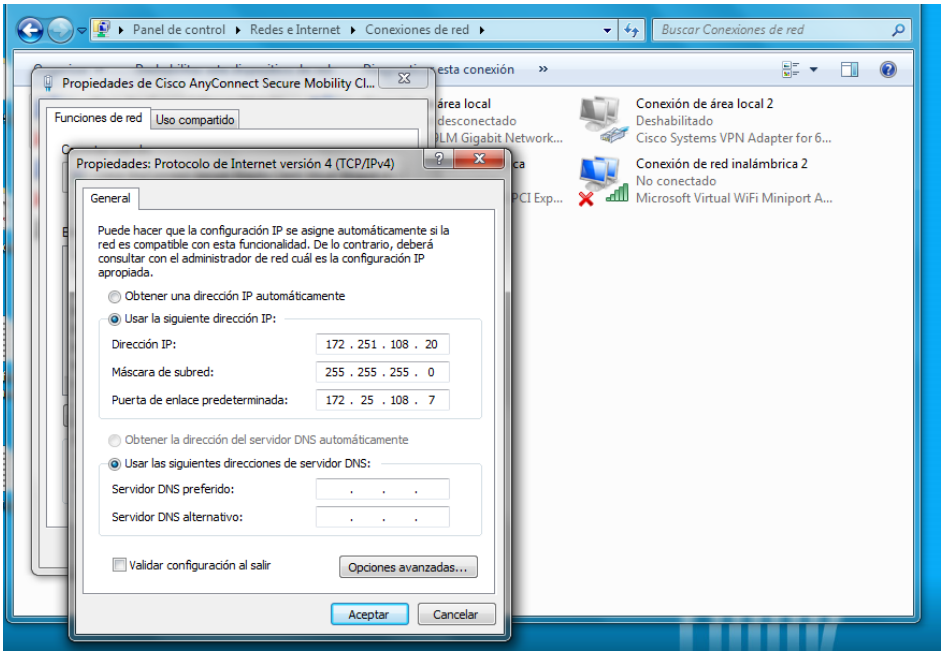

Fig. 15. Conexión a red del servidor ACS

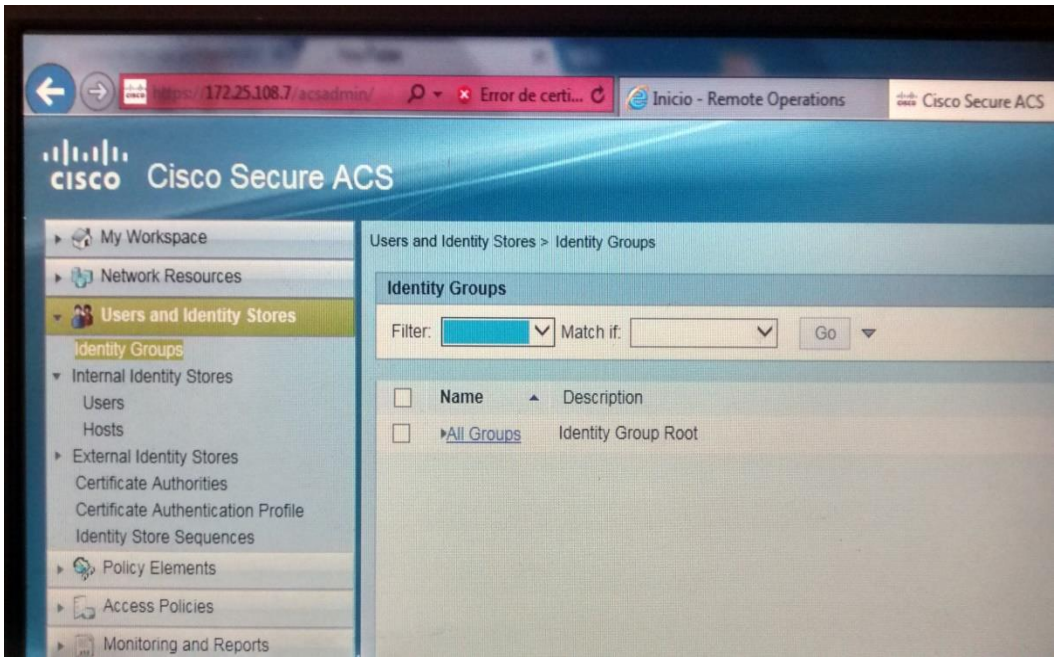

Fig. 16. Ingreso a interfaz web por Internet Explorer

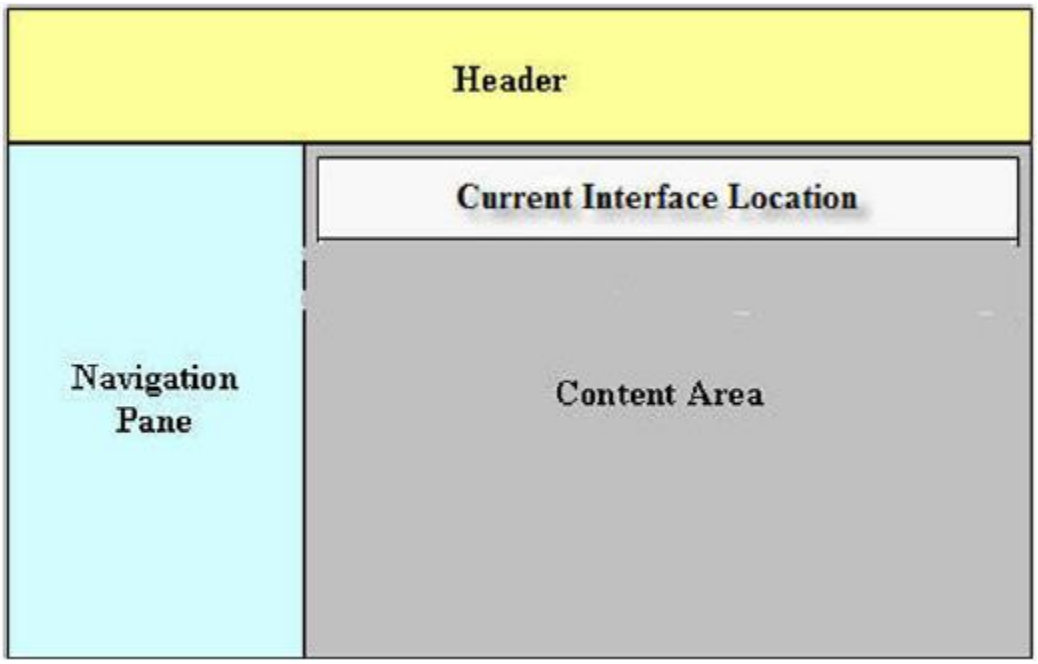

Fig. 17. Descripción de interfaz web

8.3 Estructura del sistema de control de acceso para la compañía Desca Colombia S.A.

El ROC (Regional Operation Center) área conformada por dos ingenieros nivel 3, seis nivel 2 y cuatro nivel 1 es donde se centran todas las operaciones de monitoreo y recepción de solicitudes de casos por parte de clientes en Colombia y otros países como ecuador, panamá, Costa Rica entre otros, es la base bajo la cual se estructura el sistema de control de acceso ya que ahí se deposita la totalidad de la población con permisos para acceder a los equipos de red.

Con base a la estructura de seguridad que propone Cisco, la cual se fragmenta en tres grupos, entre los que se encuentra Net Admin donde encontramos dos usuarios con perfiles de tipo Full Access para administrador. En segundo lugar está el grupo de Employee con permisos restringidos en el cual por diseño personal se ha dividido en dos partes asignándole a una parte cuatro usuarios con perfil Shell de privilegio 7 y a la otra cuatro de privilegio 10 con la única diferencia entre cada uno de los privilegios la lista de comandos que pueden ser usados al ingresar a los equipos de red. Por último se encuentra el tercer grupo de Guest con dos usuarios con perfil de tipo lectura para invitados el cual no posee ningún permiso para el uso de comandos, al ingresar a los equipos solamente está en capacidad de observar la configuración sin la menor posibilidad de afectar de alguna manera al equipo.

Ver figuras 19, 20, 21.

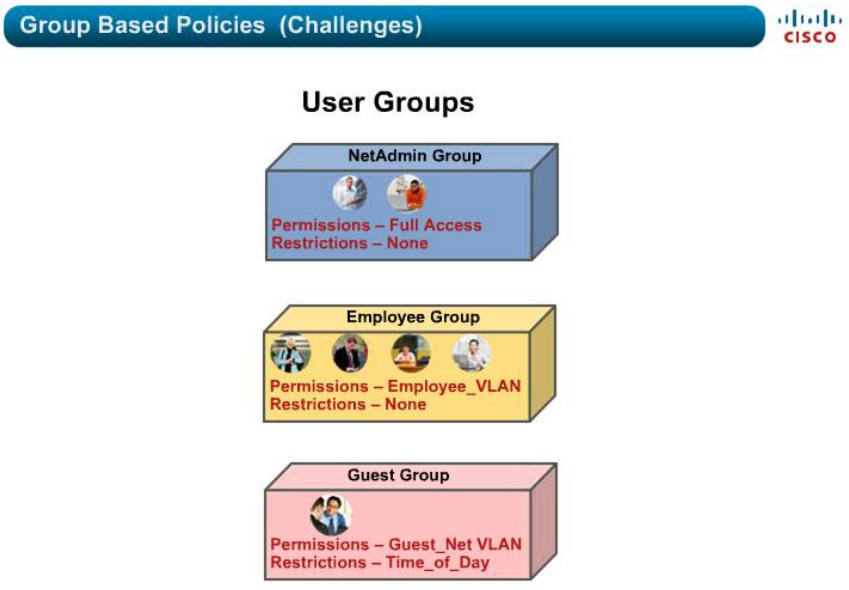

Fig. 19. Grupos base para la creación de políticas de acceso

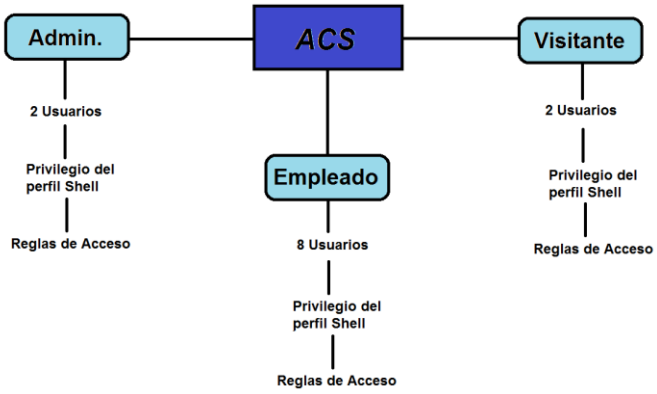

Fig. 20. Estructura del sistema de control de acceso para Desca Colombia S.A.

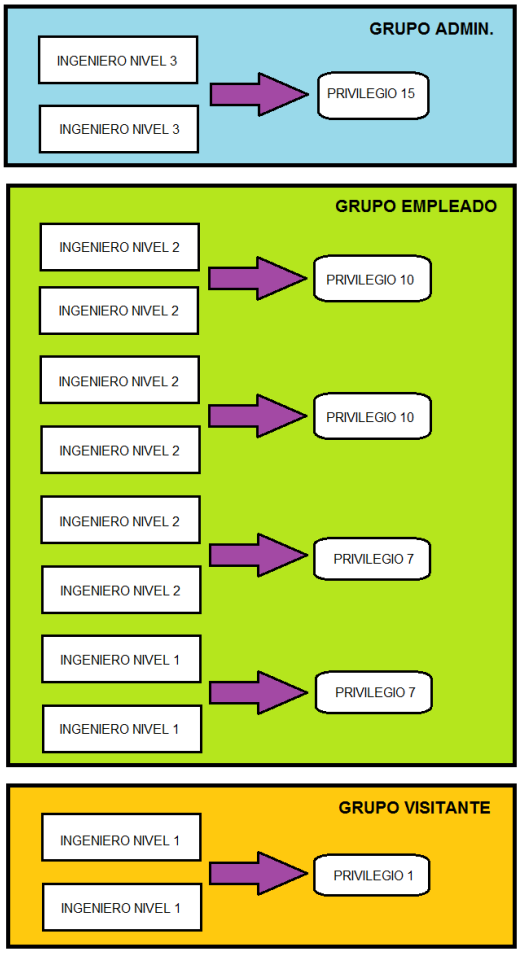

Fig. 21. Organización del sistema de control de acceso en el área del ROC.

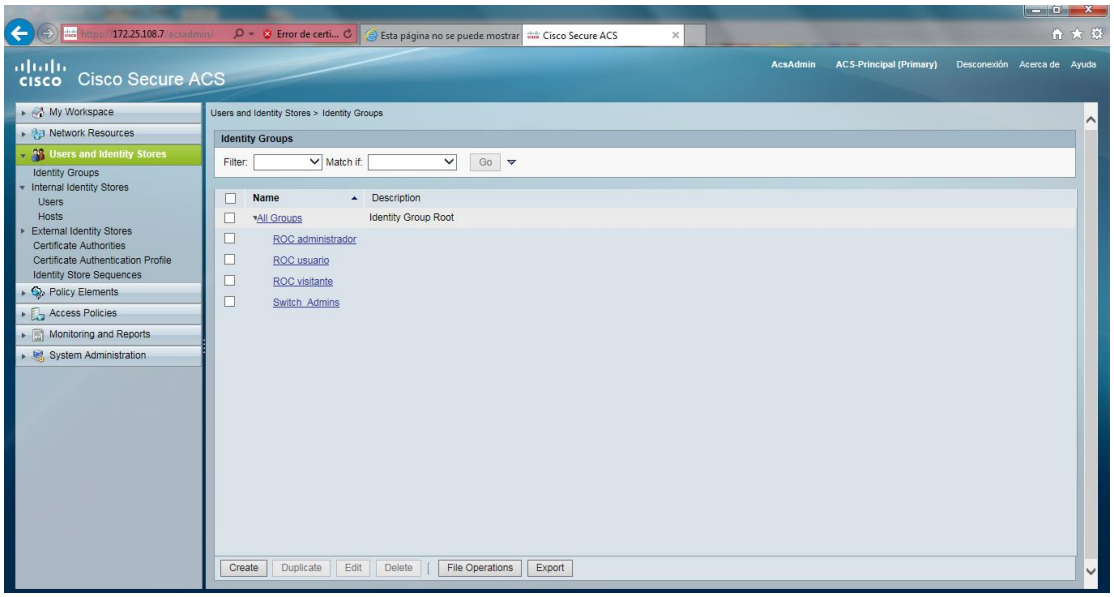

Fig. 22. Creación de grupos en ACS

8.4 Creación de perfiles de acceso Shell según privilegios Cisco

De acuerdo a la estructura de seguridad de Cisco y a las necesidades de la compañía se propone la creación de los diferentes perfiles dentro de cada uno de los grupos anteriormente mencionados. Por ende se decide crear los siguientes perfiles Shell y su respectivo privilegio dentro de lo establecido por Cisco:

GRUPO NET ADMIN

- Roc Admin1 (privilegio 15)
- Roc Admin2 (privilegio 15)

GRUPO EMPLOYEE

- Roc User1 (privilegio 7)
- Roc User2 (privilegio 7)
- Roc User3 (privilegio 7)
- Roc User4 (privilegio 7)
- Roc User5 (privilegio 10)
- Roc User6 (privilegio 10)
- Roc User7 (privilegio 10)
- Roc User8 (privilegio 10)

GRUPO GUEST

- Roc Visitante1 (privilegio 1)
- Roc Visitante2 (privilegio 1)

Ver figuras 23, 24, 25, 26, 27.

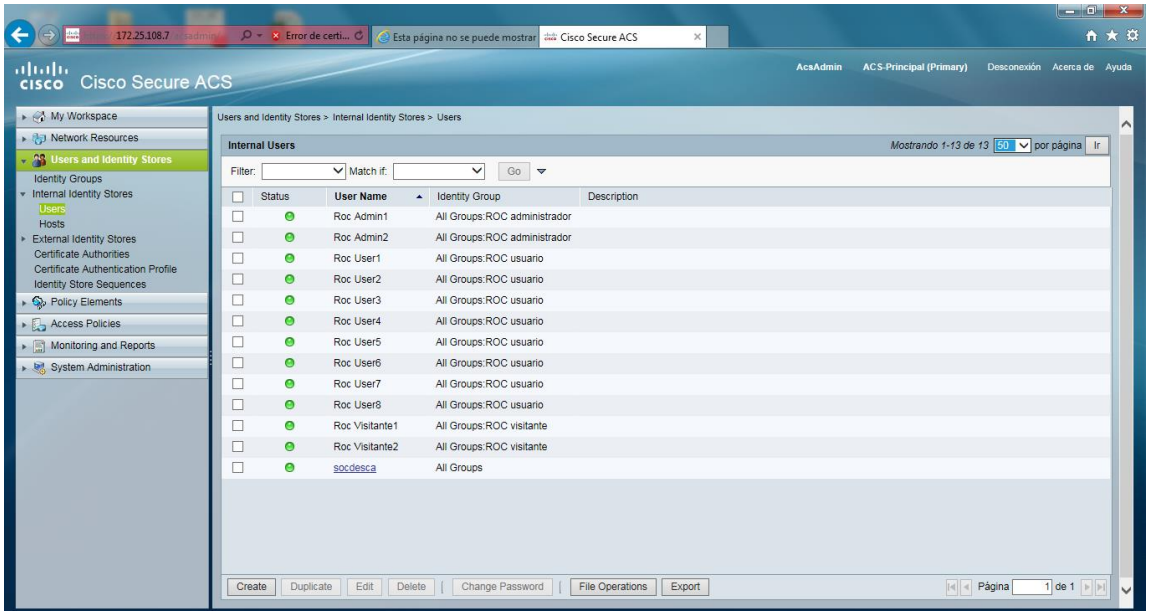

Fig. 23. Creación de usuarios en ACS

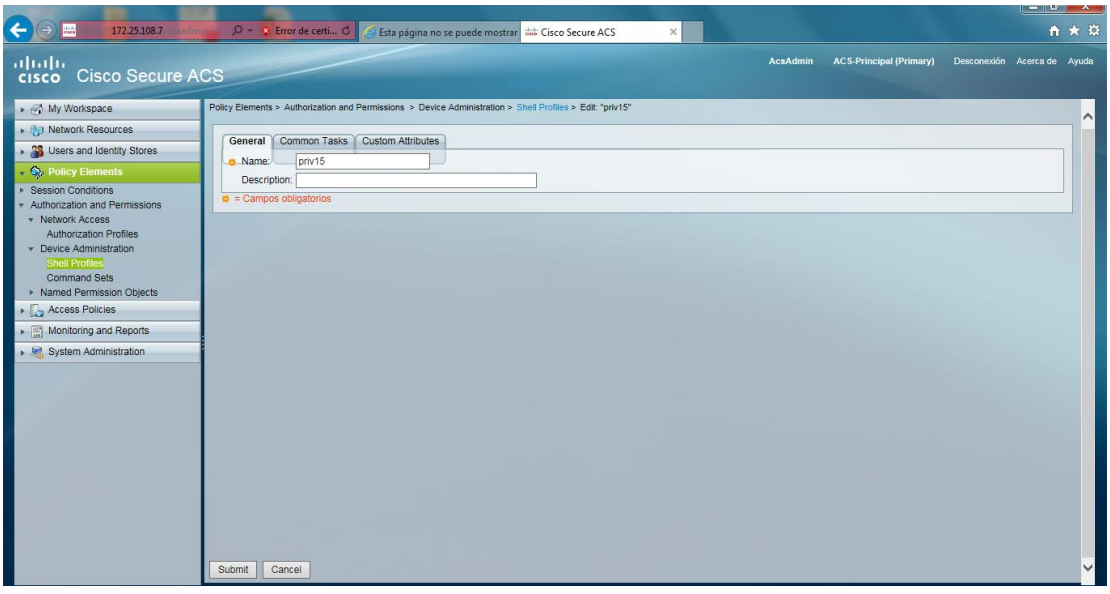

Fig. 24. Creación de privilegios en ACS

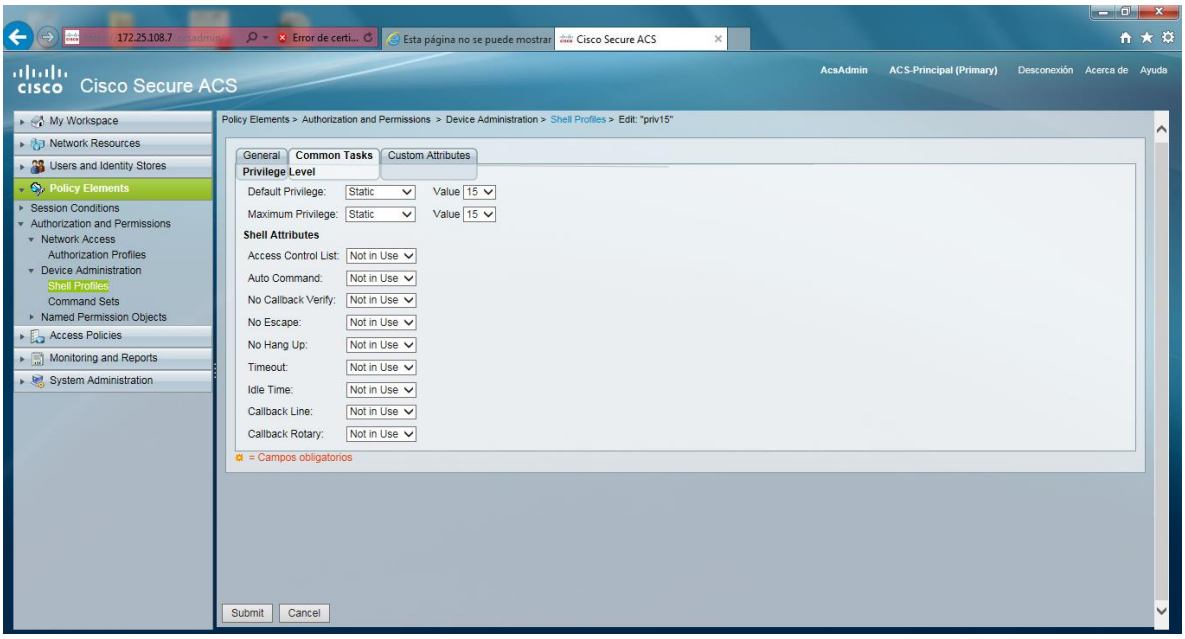

Fig. 25. Configuración de privilegios en ACS

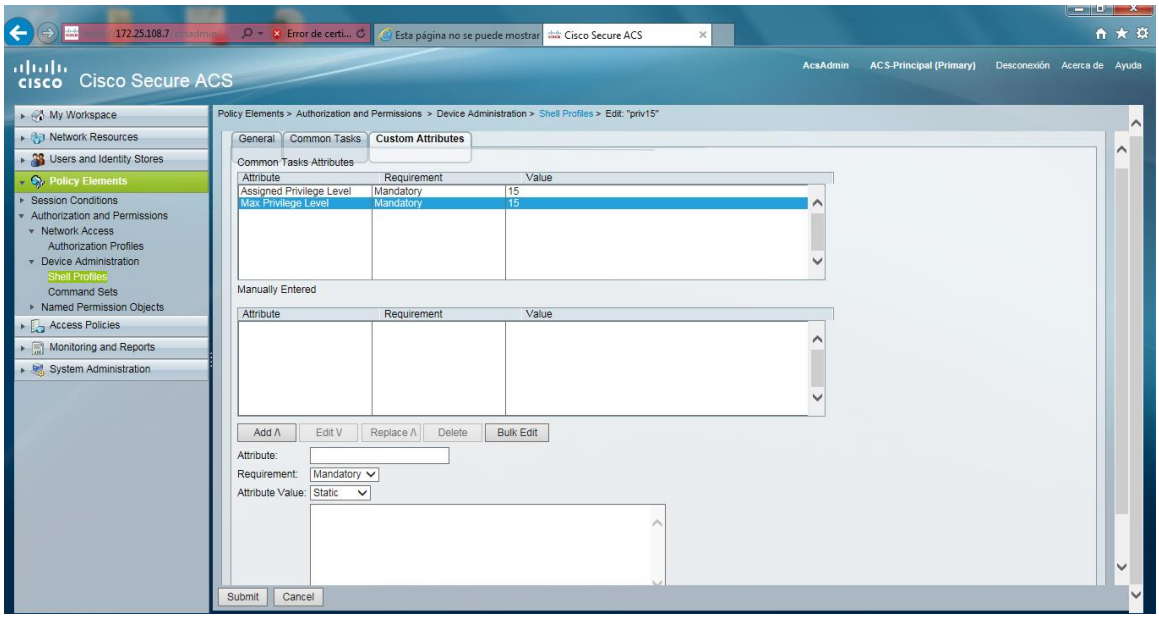

Fig. 26. Atributos de privilegios en ACS

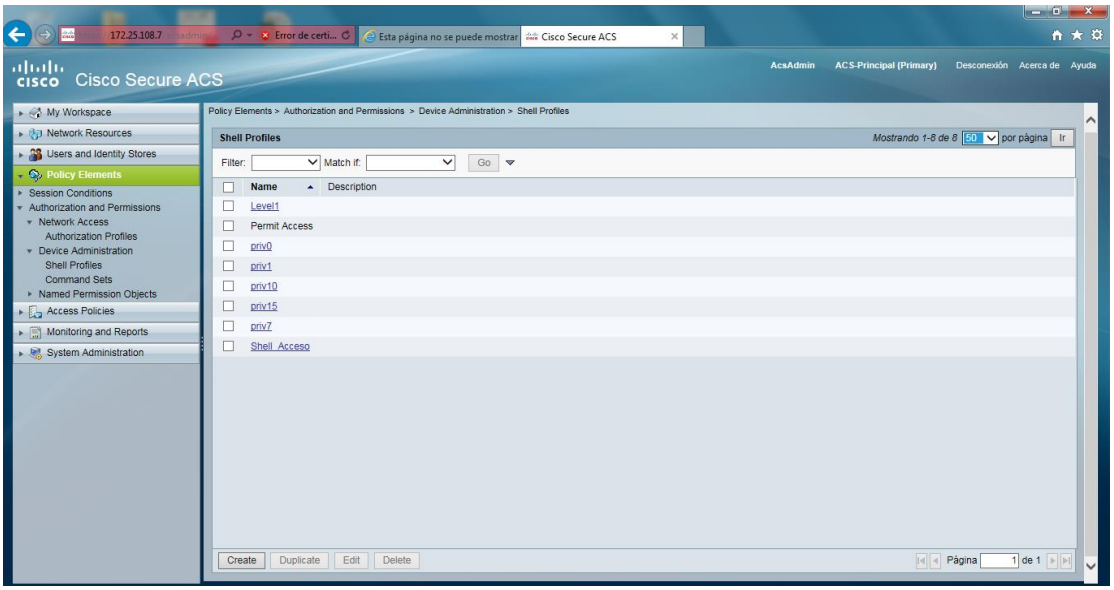

Fig. 27. Lista de privilegios en ACS para Desca Colombia S.A.

8.5 Modelos de políticas de acceso basados en la lógica estructural de Cisco

El modelo de política diseñado para la compañía Desca Colombia S.A. está basado en normas que proporcionan un control de acceso más poderoso y flexible que tiene la capacidad de enfoque por grupo con mayor privilegio.

En el modelo basado en el grupo de mayor privilegio, se entiende como un grupo principal que siempre es el administrador del sistema el cual define la política ya que contiene y une tres tipos de información:

• Información de Identidad: Esta información puede estar basada en la pertenencia a grupos de AD o LDAP o una asignación estática por usuarios internos de ACS.

•Otras restricciones o limitaciones condiciones de tiempo, restricciones de dispositivo, entre otras.

• Permisos-VLAN o niveles de privilegio Cisco.

El modelo de política en un ACS se basa en reglas de la forma:

If <condition> then <result>
La lógica anterior admite tres condiciones ID GROUP, POSTURE y LOCATION, con un solo resultado autorización de perfil.

Por ejemplo:
IF <identity-condition, restriction-condition> THEN <authorization-profile>

En un ACS, se definen las condiciones y resultados como objetos compartidos globales. Son definidos una vez y luego hace referencia a ellos al crear reglas. Además utiliza los elementos de política para estos objetos compartidos, y son los bloques de construcción para la creación de reglas.

Ver figuras 28, 29.

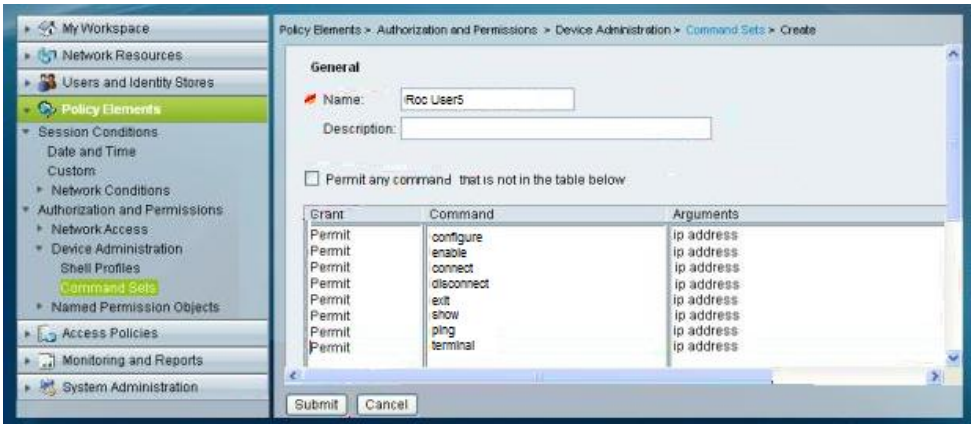

Fig. 28. Asignación de comandos en ACS

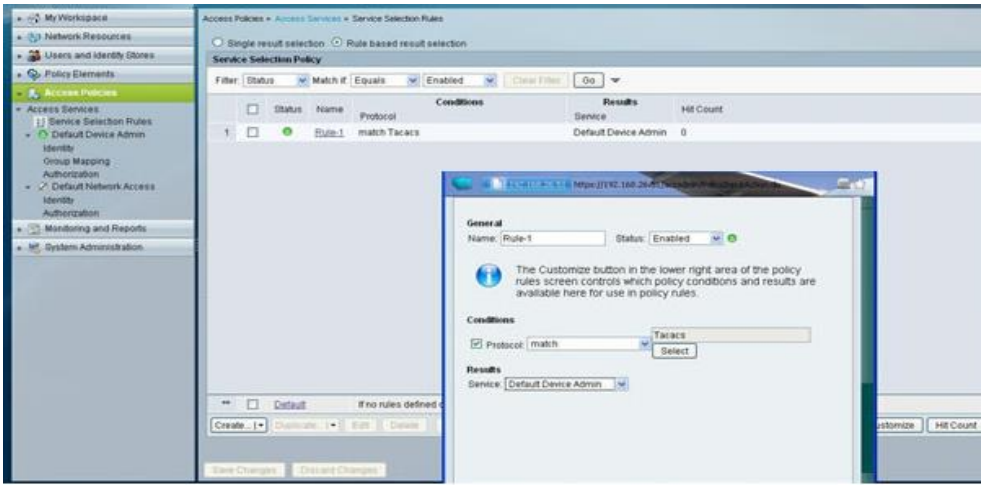

Fig. 29. Creación de reglas de acceso ACS

En las tablas 5, 6 y 7 se expone la lógica para la cual se determinan las reglas de autorización.

Ver tabla 5, 6 y 7 de Anexos.

8.6 Establecimiento de reglas de acceso por protocolo TACACS+

A continuación se expone cómo se puede utilizar los elementos de política para crear reglas acceso.

Para un ACS una compañía divide su red en dos regiones, Oriente y Occidente con los ingenieros de operaciones de red en cada sitio. Quienes buscan crear una política de acceso que le permitiría a los ingenieros:

• Acceso completo a los dispositivos de red de su región.

• Acceso de sólo lectura a los dispositivos fuera de su región.

Usted puede utilizar el modelo de política de un ACS para:

• Definir los grupos de dispositivos de red Este y Oeste.

• Definir los grupos de identidad y los usuarios al grupo apropiado.

• Definir el acceso pleno y Leer perfiles de autorización.

• Definir reglas que permiten a cada grupo de identidad acceso completo o acceso de sólo lectura, dependiendo de la ubicación del grupo de dispositivos de red.

El diseño propuesto a la compañía Desca Colombia S.A. plantea dos regiones dentro del área ROC, una la cual consta de equipos pertenecientes a la red local y otra región donde se encuentra la red de la compañía en comunicación con los equipos de algunos clientes. Estableciendo tres grupos de usuarios, ubicando cada uno de los ingenieros con los privilegios correspondientes para ingresar a cada región de acuerdo a los permisos según su nivel de acceso en la compañía.

La política que se utiliza con la selección de protocolo tacacs+ se selecciona como parte de la política de evaluación. En términos simples cuando se está utilizando el protocolo tacacs+ para autenticar la política de servicio seleccionado se denomina directiva predeterminada de política. Las reglas permiten determinar quién es el usuario y qué grupo no le pertenece y lo que se le permite hacer según el perfil configurado para la autorización.

Ver figura 30.

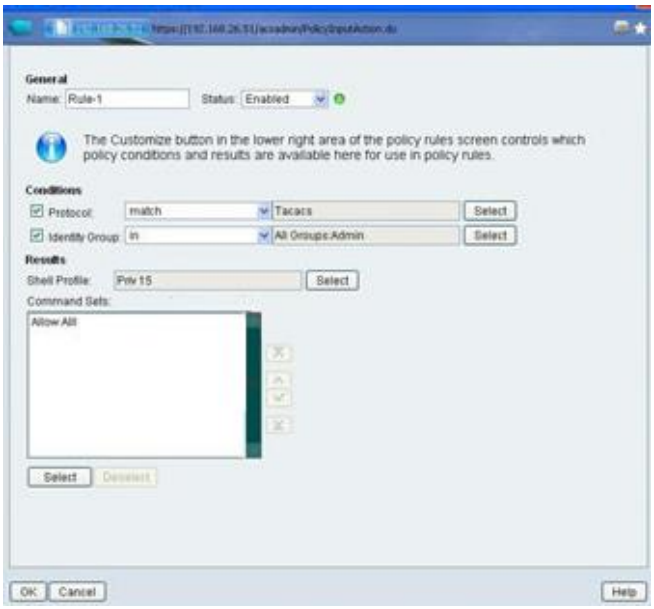

Fig. 30. Creación de regla para privilegio 15 de ACS

8.7 Asignación de comandos a los usuarios

Dentro de las políticas de acceso se realiza la asignación de comandos para que cada perfil y de este modo se define el privilegio que obtiene el usuario una vez es autorizado para ingresar al equipo a través de la ventana de comandos (CLI). En las tablas 8, 9 y 10 se define la lista de comandos para cada uno de los perfiles de acceso.

Ver tablas 8, 9 y 10 de Anexos.

8.8 Registro de operaciones y acceso a recursos en los equipos de red

El registro de auditoría se implementa usando una solución AAA basada en un servidor ACS con el propósito de obtener información detallada de las actividades que se desarrollan en los equipos de red.

Este servicio genera un reporte con parámetros al servidor ACS y por supuesto extraíbles para la administración de los equipos de red. Es un registro detallado de absolutamente todo lo que hace el usuario una vez autenticado en el dispositivo indicando fecha y hora de ingreso, al igual que todas las acciones ejecutadas como son la digitación de comandos.

Se evaluaron dos registros al ingresar a dos equipos de red exportando la información detallada de las actividades desarrolladas por los usuarios al ser autorizado para ingresar. Cabe resaltar que un ACS permite la generación de otros parámetros en los reportes para la administración de dispositivos además de los propuestos para la compañía Desca Colombia S.A.

El primer registro es extraído luego de que dos usuarios Roc User2 (privilegio 7) y Roc Visitante1 (privilegio 1) ingresaran a un switch y fueran autorizados exitosamente, y además ejecutaran varios comandos.

El segundo registro extraído contiene información de dos usuarios uno Roc Admin1 (privilegio 15) y otro Roc User7 (privilegio 10) que ingresan a un router y son autorizados exitosamente y ejecutan una serie de comandos.

Ver figura 31.

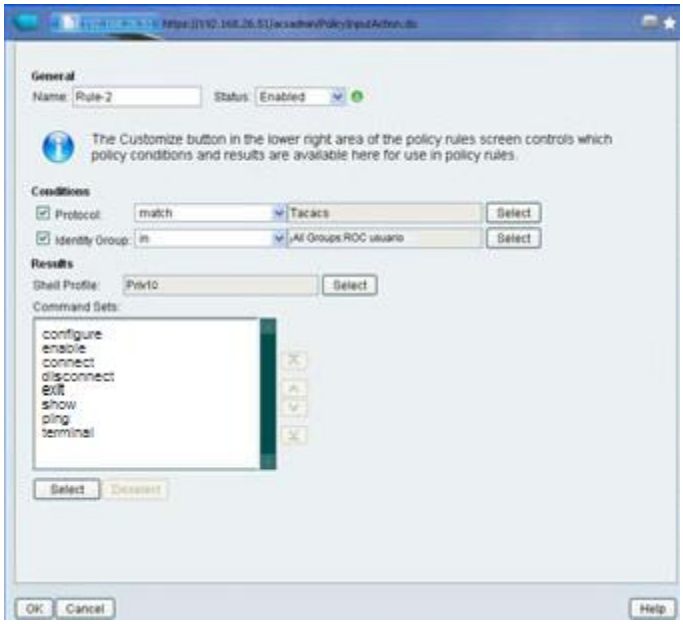

Fig. 31. Creación de regla para privilegio 10 de ACS

AAA Protocol > TACACS+ Accounting

Date : July 30, 2015

Generated on July 30, 2015 10:02:41 AM

Reload

=Click for details

Logged At	Details	ACS	User Name	Privilege Level	Command Set	Task ID	Network Device	Access Service
Jul 30,12 10:02:39.290 AM		OSI1500	Roc User2	priv7	[CmdAV=write memory]		KLM-test-SW	TACACS
Jul 30,12 10:02:38.340 AM		OSI1500	Roc User2	priv7	[CmdAV=end]		KLM-test-SW	TACACS
Jul 30,12 10:02:37.840 AM		OSI1500	Roc User2	priv7	[CmdAV=description this is a test of accounting]		KLM-test-SW	TACACS
Jul 30,12 10:02:30.710 AM		OSI1500	Roc User2	priv7	[CmdAV=interface]		KLM-test-SW	TACACS
Jul 30,12 10:02:28.413 AM		OSI1500	Roc User2	priv7	[CmdAV=configure terminal]		KLM-test-SW	TACACS
Jul 30,12 10:02:19.440 AM		OSI1500	Roc User2	priv7	[CmdAV=exit]		KLM-test-SW	TACACS
Jul 30,12 10:02:18.860 AM		OSI1500	Roc User2	priv7	[CmdAV=configure terminal]		KLM-test-SW	TACACS
Jul 30,12 10:02:17.750 AM		OSI1500	Roc User2	priv7	[CmdAV=enable]		KLM-test-SW	TACACS

Fig. 32. Registro de ingreso ACS de un usuario privilegio 7

AAA Protocol > TACACS+ Accounting

Date : July 31, 2015

Generated on July 31, 2015 11:41:20 AM

Reload

=Click for details

Logged At	Details	ACS	User Name	Privilege Level	Command Set	Task ID	Network Device	Access Service
Jul 31,12 11:42:39.290 AM		OSI1500	Roc Admin1	priv15	[CmdAV=write memory]		KLM-test-SW	TACACS
Jul 31,12 11:42:38.340 AM		OSI1500	Roc Admin1	priv15	[CmdAV=end]		KLM-test-SW	TACACS
Jul 31,12 11:42:37.840 AM		OSI1500	Roc Admin1	priv15	[CmdAV=configure memory]		KLM-test-SW	TACACS
Jul 31,12 11:42:30.710 AM		OSI1500	Roc Admin1	priv15	[CmdAV=show ip interface]		KLM-test-SW	TACACS
Jul 31,12 11:42:28.413 AM		OSI1500	Roc Admin1	priv15	[CmdAV=configure terminal]		KLM-test-SW	TACACS
Jul 31,12 11:42:19.440 AM		OSI1500	Roc Admin1	priv15	[CmdAV=exit]		KLM-test-SW	TACACS
Jul 31,12 11:42:18.860 AM		OSI1500	Roc Admin1	priv15	[CmdAV=description this is a test of accounting]		KLM-test-SW	TACACS
Jul 31,12 11:42:17.750 AM		OSI1500	Roc Admin1	priv15	[CmdAV=enable]		KLM-test-SW	TACACS

Fig. 33. Registro de ingreso ACS de un usuario privilegio 15

8.9 Factibilidad del sistema en clientes de la compañía

A través de un estudio que se elaboró para establecer la manera en la cual fuera posible implementar el sistema de control de acceso para clientes de la compañía se determinó que clientes como smurfit Kappa cuentan con un sistema ACS para algunas de sus sucursales en el país pero en otras no cuenta con la administración sobre los equipos de red ya que maneja una amplia cantidad de dispositivos como Switches, Routers, Firewalls, Access Points que

constantemente son monitoreados y a los que los ingenieros tiene acceso normalmente. Para lo que se hizo una propuesta en la que la cual se plantea un control de acceso basándose en las características de la infraestructura de TI del cliente.

De esta manera se elaboró una base de datos con los siguientes parámetros, con el fin de poder ser presentada a las áreas correspondientes para su futura puesta en marcha:

- *Equipos:* Es fundamental un listado en cual se especifique el tipo de equipo el cual se va gestionar, ya sea un Firewall (FW), Switch (SW), Router, Access Point (AP).

- *Ingenieros:* Un base de datos con la información correspondiente a los usuarios y los privilegios para ingresar a los equipos.

- *Modelo y serial:* Esta es la identificación del equipo que permite determinar si está bajo contrato de la compañía (cadena de caracteres de identificación).

- *Cliente:* En este caso particular Smurfit Kappa.

- *Ubicación:* Detalles exactos de la ciudad en la que se encuentran los equipos, además de los permisos de acceso a las instalaciones.

- *Estado del equipo:* Condiciones de funcionamiento del ACS. Se indica las condiciones óptimas para su uso.

9. CONCLUSIONES

Posterior a la realización del proyecto, se pueden deducir las siguientes conclusiones:

- ✓ Se observó que al establecer la estructura del sistema de control de acceso se abarcó toda la seguridad perimetral del área del ROC evitando un agujero por el cual fuera posible afectar la infraestructura de TI en la compañía.

- ✓ La flexibilidad y facilidad de escalamiento del sistema permite ejecutar cambios a cualquier nivel dentro de la estructura jerárquica de la compañía, sin afectar la seguridad manteniendo activos los tres estándares del protocolo AAA (Authentication, Authorization, and Accounting) en la administración de dispositivos.

- ✓ La implementación de un modelo de seguridad de red con servidor ACS y protocolo de comunicación Tacacs+ es la solución más completa para mantener a salvo los recursos específicos en la red, donde todo el intercambio de información es cifrado protegiendo la información de cualquier compañía con una estructura de TI (Tecnologías de Información).

- ✓ El modelo de seguridad de red con servidor ACS es uno de los modelos más utilizados en el ámbito empresarial, ya que ofrece una amplia variedad de soluciones para la administración de acceso de los usuarios y administradores de toda la red de la empresa.

- ✓ Durante todo el proceso de pasantía empresarial se adquirieron conceptos y experiencias laborales fundamentales para el desarrollo profesional y personal que son reflejadas en la elaboración del proyecto, el cual tuvo la supervisión del tutor en la compañía lo cual contribuyo a la formación como ingeniero electrónico.

BIBLIOGRAFÍA

Citada Texto:

1. Guía de usuario acs.pdf, página 95
2. Guía de usuario acs.pdf, paginas 27-28
3. Imagen tomada de: Guía de usuario acs.pdf, página 98
4. Imagen tomada del texto: REDES y servicios de telecomunicaciones, 4 edición, José Manuel Huidobro Moya, editorial THOMSON PARANINFO
5. REDES y servicios de telecomunicaciones, 4 edición, José Manuel Huidobro Moya, editorial THOMSON PARANINFO

Citada Pagina Web:

1. http://www.gitsinformatica.com/historia%20de%20internet.html
2. http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57:herramientas-informaticas&Itemid=179
3. http://www.ort.edu.uy/fi/pdf/configuracionroutersciscomatturro.pdf
4. http://www.mcgraw-hill.es/bcv/guide/capitulo/8448171683.pdf
5. http://blog.capacityacademy.com/2014/07/30/ccna-security-como-configurar-aaa-con-cisco-secure-acs-server/
6. http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scftplus.html
7. http://www.cisco.com/c/en/us/products/collateral/security/secure-access-control-system/data_sheet_c78-683481.html
8. Imagen tomada de: http://www.fcet.staffs.ac.uk/jdw1/sucfm/sucfmcomputers.htm
9. Imagen tomada de: http://irsweb.es/?q=node&page=8
10. Imagen tomada de la página web: http://www.codejobs.biz/es/blog/2014/11/05/que-es-el-modelo-cliente-servidor-networking#sthash.MNp5IAa6.dpbs
11. Imagen tomada de la página web: http://www.clker.com/clipart-233152.html
12. Imagen tomada de la página web: http://www.clker.com/clipart-switch- 9.html

13. Imagen tomada de la página web: http://www.ebrahma.com/2014/08/what-is-the-difference-between-tacacs-and-radius/

14. Imagen tomada de la página web: http://www.packetwisdom.com/CiscoSecureACSProduct.html

15. Imagen tomada de la página web: http://www.cisco.com/c/en/us/products/security/secure-access-control-system/index.html

16. Tomado de la página web Desca-Grupo Amper: http://www.desca.com/latam/index.php/acerca

Consultada:

1. Cisco Networking Academy Program CCNA 1 and 2, Version 3.1, Curriculum en formato pdf por staky.

2. Fundamentos de Seguridad en Redes Aplicaciones y Estándares WILLIAM STALLINGS, SEGUNDA EDICIÓN, 2004 por Pearson Educación de México, S.A. de C.V

3. Redes de computadoras, ANDREW S. TANENBAUM, CUARTA EDICIÓN, 2003 por Pearson Educación de México, S.A. de C.V.

4. Redes telemáticas, CARLOS VALDIVIA MIRANDA, PRIMERA EDICION, 2015 por paraninfo S.A.

5. Seguridad de la Informática Redes, informática y sistemas de información, JAVIER AREITIO, PRIMERA EDICIÓN, 2008 por Cengage Learning paraninfo S.A.

10. ANEXOS

TABLA DE ANEXOS

COMPONENTE	ESPECIFICACIONES
CPU	Intel Xeon Q9400 2.66 GHz (Quad Core)
La memoria del sistema	4 GB DDR II ECC
Disco duro	2 x 250 GB 7.2K RPM 3.5-in. SATA
Almacenamiento óptico	DVD-ROM
Conectividad de red	4 10/100/1000, RJ-45 de interfaces
Puertos de E / S	1 puerto serie, 4 USB 2.0 (2 frontales, 2 traseros), vídeo SVGA
Montaje en bastidor	4 postes (kit incluido)
Dimensiones físicas (1 RU) (W x D x H)	● 44,0 x 55,9 x 4,45 cm ● 17,3 x 22,0 x 1,75 pulg.
Peso	24.25 (mínimo) a 28,0 libras (máximo); 11,0-12,7 kg

Tabla No.1 Especificaciones Físicas

ENERGIA	ESPECIFICACIONES
Número de fuentes de alimentación	1
Tamaño de la fuente de alimentación	351W universal, autoconmutación

Tabla No. 2 Especificaciones Eléctricas

AMBIENTAL	ESPECIFICACIONES
Rango de temperatura de funcionamiento	50 a 95 ° F; 10 a 35 ° C (hasta 3000 pies / 914,4 m)
Emitida Heat	341 (mínimo) a 1024 (máximo) BTUs; 100 a 300W
Altitud máxima	7000 pies; 2133 m

Tabla No. 3 Especificaciones de Entorno

ESPECIFICACION	REQUISITO MINIMO
Velocidad de procesador	Procesador Pentium IV 1,8 GHz o más rápido
Memoria	Mínimo 1GB de RAM
Memoria virtual	Mínimo 1GB
Disco Duro	Al menos 1GB de espacio libre en disco duro
Sistema Operativo	• Windows Server 2008, Enterprise Edition o Standard • Windows Server 2003 Service Pack, Enterprise Edition o Standard • Japonés Server 2003 Service Pack, Enterprise Edition o Standard • Windows Server 2003 R2 Estándar Edition • Windows Server 2003 Service Pack 2 • Windows Server 2003 R 2 Service Pack 2
Resolución	Un mínimo de 800 x 600 (256 colores)

Tabla No. 4 Especificaciones de Funcionamiento

	CONDITIONS						RESULT
IF	ID GROUP	AND	POSTURE	AND	LOCATION	THEN	Authorization PROFILE
IF	NET ADMIN	AND	Non-COMPLIANT	AND	Clientes	THEN	Roc Admin1
IF	NET ADMIN	AND	Non-COMPLIANT	AND	Clientes	THEN	Roc Admin2

Tabla No. 5 Lógica de autorización para Administradores

	CONDITIONS						RESULT
IF	ID GROUP	AND	POSTURE	AND	LOCATION	THEN	Authorization PROFILE
IF	EMPLOYEE	AND	COMPLIANT	AND	Local	THEN	Roc User1
IF	EMPLOYEE	AND	COMPLIANT	AND	Local	THEN	Roc User2
IF	EMPLOYEE	AND	COMPLIANT	AND	Local	THEN	Roc User3
IF	EMPLOYEE	AND	COMPLIANT	AND	Local	THEN	Roc User4
IF	EMPLOYEE	AND	COMPLIANT	AND	Clientes	THEN	Roc User5
IF	EMPLOYEE	AND	COMPLIANT	AND	Clientes	THEN	Roc User6
IF	EMPLOYEE	AND	COMPLIANT	AND	Clientes	THEN	Roc User7
IF	EMPLOYEE	AND	COMPLIANT	AND	Clientes	THEN	Roc User8

Tabla No. 6 Lógica de autorización para Empleados

	CONDITIONS						RESULT
IF	**ID GROUP**	**AND**	**POSTURE**	**AND**	**LOCATION**	**THEN**	**Authorization PROFILE**
IF	GUEST	AND	COMPLIANT	AND	Local	THEN	Roc Visitante1
IF	GUEST	AND	COMPLIANT	AND	Local	THEN	Roc Visitante2

Tabla No. 7 Lógica de autorización para Visitantes

USUARIO	COMANDOS DISPONIBLES
Roc Admin1 /Roc Admin2	clear cdp counters
	clear cdp table
	clear counters
	confugure memory
	configure terminal
	copy flash tftp
	copy running-config startup-config
	copy running-config tftp
	copy tftp flash
	copy tftp runnig-config
	debug cdp adjacency
	debug cdp eventes
	debug cdp ip
	debug cdp packets
	debug ip igrp events
	debug ip igrp transactions
	debug ip igrp rip
	debug ip rip [events]
	disable
	erase flash
	erase startup-config
	no debug all
	reload
	setup
	show access-lists
	show arp
	show cdp traffic
	show controllers serial
	show debugging
	show flash
	show ip interface
	show ip protocols

	show memory
	show processes
	show running-config
	show sessions

Tabla No. 8 Comandos asignados a los perfiles Roc Admin1, Roc Admin2

USUARIOS	COMANDOS DISPONIBLES
Roc User1 /Roc User2 /Roc User3 /Roc User4	write memory
	end
	description this is a test of accounting
	interface
	configure terminal
	exit
	enable
	show ip protocols
	show memory
	show processes
	disable
	erase flash
	clear cdp counters
	copy flash tftp
	interface
Roc User5 /Roc User6 / Roc User7 /Roc User8	write memory
	end
	description this is a test of accounting
	interface
	configure terminal
	exit
	enable
	show ip protocols
	show memory
	show processes
	disable
	no debug all
	reload
	setup
	show arp
	show flash
	disable

	erase flash
	show processes
	show running-config
	show sessions

Tabla No. 9 Comandos asignados a los perfiles Roc User1, Roc User2, Roc User3, Roc User4, Roc User5, Roc User6, Roc User7, Roc User8

USUARIOS	COMANDOS DISPONIBLES
Roc Visitante1 /Roc Visitante2	solo lectura

Tabla No. 10 Comandos asignados a los perfiles Roc Visitante1, Roc Visitante2

Fig. 1. Primer Servidor Web NeXTcube o "The Cube". [13]

[12] *Imagen tomada de: http://www.fcet.staffs.ac.uk/jdw1/sucfm/sucfmcomputers.htm*

[13] *Imagen tomada de: http://irsweb.es/?q=node&page=8*

Fig. 2. Diagrama construcción de la Internet. [14]

Fig. 3. Modo Cliente Servidor[15]

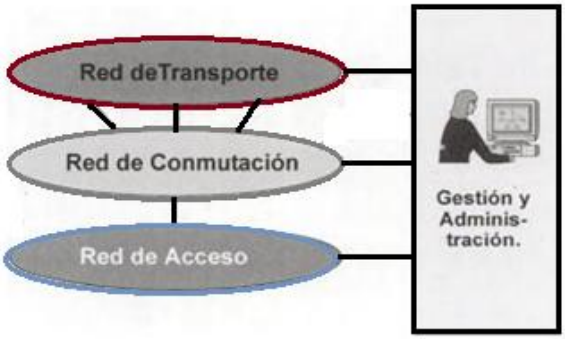

Fig. 4. Estructura típica de RED.[16]

[15] *Imagen tomada de la página web: http://www.codejobs.biz/es/blog/2014/11/05/que-es-el-modelo-cliente-servidor-networking#sthash.MNp5IAa6.dpbs*

[16] *Imagen tomada del texto: REDES y servicios de telecomunicaciones, 4 edición, José Manuel Huidobro Moya, editorial THOMSON PARANINFO*

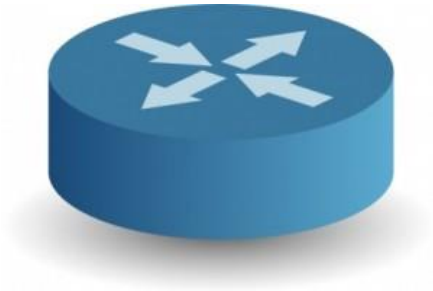

Fig. 5. Símbolo que representa un router.[17]

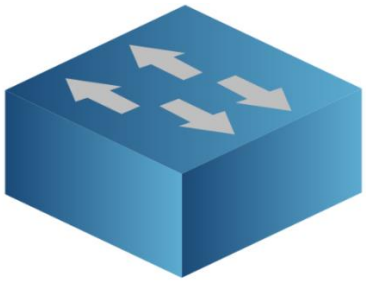

Fig. 6. Símbolo que representa un switch. [18]

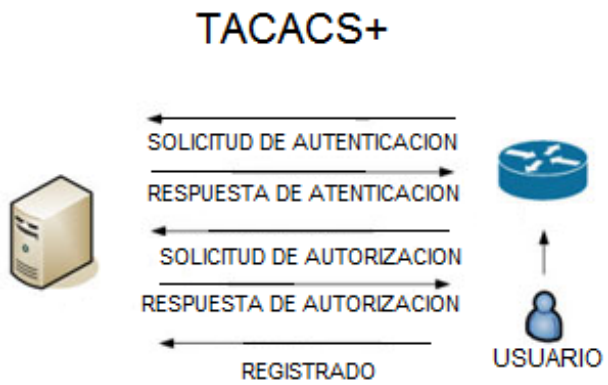

Fig. 7. Diagrama de comunicación del protocolo TACACS+.[19]

[17] *Imagen tomada de la página web: http://www.clker.com/clipart-233152.html*

[18] *Imagen tomada de la página web: http://www.clker.com/clipart-switch-9.html*

[19] *Imagen tomada de la página web: http://www.ebrahma.com/2014/08/what-is-the-difference-between-tacacs-and-radius/*

Fig. 8. Imagen de un ACS Cisco.[20]

Fig. 10. Interfaz del Software Cisco.[21]

[20] *Imagen tomada de la página web: http://www.packetwisdom.com/CiscoSecureACSProduct.html*

[21] *Imagen tomada de: Guía de usuario acs.pdf, página 98*

Fig. 18. Software ACS Cisco Versión 5.1

Estos son algunos de los equipos corporativos que Desca Colombia S.A tiene al servicio de sus empleados para establecer comunicación interna y además con los clientes de la compañía. Cada equipo cuenta con su respectivo manual y demás herramientas para su correcto uso.

- Imagen de un Servidor de control de acceso para la implementación.

Fig. 34. Imagen de Secure Access Control System

- Imagen de un Switch para la implementación.

Fig. 35. Imagen de Switch

- Imagen de Router para la implementación.

Fig. 36. Imagen de Router