

Servidor de autenticación AAA mediante protocolo de autenticación TACACS

Trabajo Terminal No. 2020 _A052

Alumnos: Ortiz Gudiño Esmeralda

Hernandez Martinez Jorge Luis

Directores: Benjamín Cruz Torres

Turno para la presentación del TT: VESPERTINO

e-mail: esmeralda.ortizg96@gmail.com

jorsh.hernandez.fs@gmail.com

Resumen – Servidor de autenticación basado en el modelo AAA para equipos de Red (routers) que permita un acceso controlado mediante la validación de usuario y contraseña que conforme al perfilamiento previamente configurado en este servidor le sea otorgado un nivel de privilegio conforme al caso.

Palabras clave – Modelo AAA, TACACS, Seguridad , Administración de Red.

1. Introducción

Si bien, la gestión de los equipos de red nos provee de muchas características que hay que considerar a nivel configuración para que nuestros equipos puedan operar correctamente y podamos tener una gestión básica que satisfaga con los requerimientos mínimos para una administración de red mediana o pequeña . Sin embargo en temas de seguridad lo más básico como lo es el acceso a nuestros equipos se vuelve un punto clave y un pilar muy sólido para asegurar la disponibilidad de nuestra red y de la operación de los servicios que se encuentran en esta red.

Hoy en día existen los protocolos de autenticación de los cuales podemos partir para considerarlos dentro de nuestra arquitectura.

El servicio AAA (Authentication, Authorization and Accounting) es una infraestructura que, como su nombre lo indica, se utiliza principalmente para autenticar usuarios, autorizar la utilización de recursos y llevar un registro de la actividad de los usuarios, los recursos de red y diferentes tipos de eventos.

Autenticación

La autenticación es el proceso por el que una entidad demuestra que es quien dice ser, probando así su identidad frente a un sistema u otra entidad. En general, una entidad es un cliente, y la otra es un servidor ante el cual se requiere autenticación.

Autorización

Autorización es un proceso que ocurre normalmente luego de la autenticación. En este proceso se contempla el requerimiento de utilización de algún recurso por parte del usuario. El servidor autorizará el requerimiento dependiendo de los parámetros del mismo.

Accounting

Accounting es el proceso mediante el cual el servidor registra cualquier actividad que se considere importante sobre la utilización de recursos, pedidos de autenticación y autorización, estadísticas, etc.[1]

Pasando el proceso de autenticación es importante establecer el nivel de privilegios que puede tener este usuario. De forma predeterminada, hay 3 niveles de comando en un router.

Nivel de privilegio 0: incluye los comandos disable, enable, exit, help y logout.

Nivel de privilegio 1: es el nivel normal en Telnet e incluye todos los comandos de nivel de usuario en la petición de entrada **router>**.

Nivel de privilegio 15: incluye todos los comandos de nivel de habilitación en la petición de entrada **router#**. Se recomienda que únicamente los administradores de la red cuenten con un nivel de privilegio 15. [2]

TACACS (Terminal Access Controller Access-Control System)

¿Cómo funciona TACACS?

El servidor TACACS es consultado por el cliente y el servidor responde si el usuario pasó o falló la autenticación. Es bueno mencionar aquí que cuando hablamos de cliente, no necesariamente es la máquina desde donde se está intentando autenticar el usuario, si no, el dispositivo al que se quiere acceder, por ejemplo, el switch o router.

Cuando el usuario hace una conexión exitosa al dispositivo, este le pedirá sus credenciales, el dispositivo de red luego toma estas credenciales y las valida con el servidor TACACS. Este servidor luego responde indicando si el usuario tiene acceso o no al dispositivo. [3]

Tomando en cuenta los conceptos anteriores. La Tabla 1 muestra los sistemas similares que se han desarrollado son.

SOFTWARE	DESCRIPCIÓN	AAA	Protocolo de autenticación	Compatibilidad con equipos
Cisco Identity Services Engine	ISE es una solución de control de políticas centralizada que por medio de la autenticación vía radius de los usuarios y de la integración con directorios de usuarios tipo LDAP [4].	Si	Radius	Exclusivo de Cisco
Active Directory	Es un servicio de directorio desarrollado por Microsoft para redes de dominio de Windows . Se incluye en la mayoría de los sistemas operativos Windows Server como un conjunto de procesos y servicios [5] .	No	Kerberos	Aplica para redes de dominio de Windows
Extreme Control	Administrador de accesos y de políticas exclusivo de Extreme[6].	Si	Radius, TACACS	Exclusivo de Extreme
Solución Propuesta	Servidor de Autenticación AAA mediante protocolo TACACS	Si	Si	Si

Tabla 1. Resumen de productos similares.

2. Objetivo

Desarrollar una solución para la autenticación y perfilamiento en los equipos de Red que permita un acceso controlado mediante el servidor de autenticación que de acuerdo al perfil establecido por el servidor se le otorgará un nivel de privilegio al usuario. Garantizando la seguridad en el acceso a los equipos de red.

3. Objetivos específicos

- Garantizar la seguridad en la red a nivel acceso
- Permitir una mejor gestión de los privilegios de los usuarios.
- Control de accesos mediante servidor de autenticación
- Uso de protocolo de autenticación TACACS

4. Justificación

La gestión de equipos de red va más allá de la implementación de una arquitectura que satisfaga las necesidades de una empresa. Hoy en día la implementación de medidas de seguridad se volvió un pilar en la operación de los equipos de red.

Las grandes empresas cuentan con múltiples mecanismos que les permiten hacer frente a las diversas amenazas que atentan contra la información y la privacidad de los datos que se manejan en la red. Sin embargo, las soluciones de seguridad que nos ofrecen las grandes empresas no contemplan los mercados con arquitecturas o servidores locales los cuales se limitan a manejar las configuraciones básicas y estandarizadas para operar con normalidad, haciendo de este sector, uno de los más vulnerables.

La atención en cuanto al entorno de seguridad prioriza la atención a ataques de malware o de virus que se encargan del robo de información. Los peligros latentes a los cuales estamos expuestos una vez que nuestra red es atacada son [7]:

- Robo de información
- Robo de identidad
- Pérdida/manipulación de datos
- Interrupción del servicio

Sin embargo, en primera instancia el acceso a nuestros equipos de red que son los que operan la red deben de estar controlados. Ya que no cualquiera debería ser capaz de modificar configuraciones o de visualizar información dentro de estos equipos. Citando lo anterior, las soluciones que empresas como CISCO o Extreme nos venden nos pueden garantizar un acceso controlado mediante el perfilamiento de usuarios, sin embargo esta solución contempla los aspectos más importantes de un servidor de autenticación y los parámetros más generales para que pueda ser implementado dentro de una red local o mediana.

Para el desarrollo de esta solución se hará uso de tecnologías de desarrollo, así como el uso de protocolos y estándares de red.

5. Productos o Resultados esperados

Se contará con un servidor el cual mediante el protocolo de autenticación TACACS conectará con los equipos de red, y de acuerdo al perfil establecido a través del navegador web se contarán con permisos de acuerdo al perfilamiento.

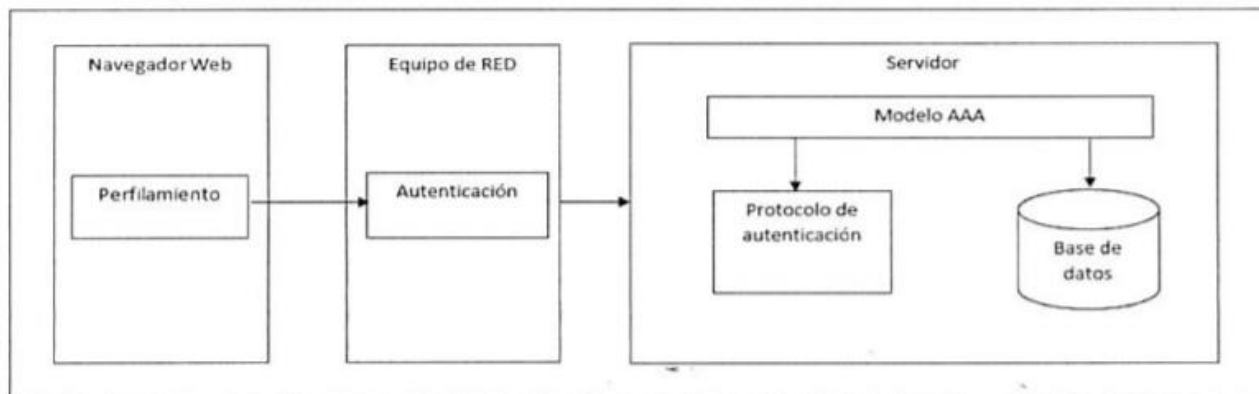


Figura 1. Arquitectura del sistema.

La solución propuesta contempla los elementos necesarios a nivel configuración en un equipo de red. En cuanto al desarrollo de la aplicación WEB la solución está contemplada para pequeñas y medianas empresas que cuenten con equipos de red que actualmente están administrados de manera local con credenciales genéricas para el acceso.

Al no ser una solución propia de CISCO o Extreme, que son dos empresas líderes en soluciones de IT, esta opción se vuelve viable para aquellas empresas o instituciones que no cuenten con un fuerte recurso económico para solventar una red grande que requiere soluciones más costosas y específicas.

Los productos que se esperan al término del trabajo son:

1. Código fuente
2. Manual Técnico.
3. Manual de usuario.
4. Aplicación WEB

6. Metodología

La necesidad de una metodología que sea ágil, flexible y que nos proporcione los mejores resultados en un corto periodo de tiempo, nos ha encaminado a hacer uso de Scrum. Para poder aplicarla a nuestro proyecto se establecerán metas en el desarrollo solución cada mes, mismas que tendrán una retroalimentación con los sinodales comprobando que se cumplen las metas propuestas.

Siendo nuestro cliente general los sinodales asignados, los cuales nos proporcionarán a lo largo del proyecto requerimientos específicos, cambios, etc. Gracias a ellos obtendremos una retroalimentación valiosa para poder seguir tomando decisiones en torno al desarrollo, evolución y dirección de nuestro proyecto.

Será de mucha utilidad esta metodología de desarrollo, debido a que podemos implementar otro tipo de soluciones que no se habían planteado desde el inicio. Adicional que al ser una metodología ágil nos permite ser flexibles en los cambios que se pudieran presentar en el futuro.

Dentro de las muchas ventajas que nos trae el uso de una metodología ágil, una de las ventajas que nos ayudarán en el desarrollo del proyecto es la gestión sistemática de riesgos, ya que los problemas que aparecen durante los procesos de gestión que pueden afectar a un proyecto son gestionados en el mismo momento de su aparición. Esto es posible debido a que la intervención de los equipos de trabajo puede ser inmediata.

Gracias a que esta metodología permite una retroalimentación del equipo, podemos visualizar las fallas y aciertos que tuvimos en el mes de desarrollo, tratando de solucionar los inconvenientes presentados. Cada etapa del proceso arroja una serie de resultados. No es necesario, por tanto, que el cliente espere hasta el final para ver el resultado. Finalizando con mejoras en los tiempos de presentación del proyecto.[8]

7. Cronograma

Nombre del alumno(a): Ortiz Gudiño Esmeralda

TT No.:

Título del TT: Servidor de autenticación AAA mediante protocolo de autenticación TACACS

Actividad	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	ENE
Investigación Documental.											
Revisión del hardware y software requerido.											
Prototipos del Diseño del servidor											
Pruebas preliminares											
Evaluación TT I.											
Diseño de la interfaz gráfica											
Corrección de errores.											
Pruebas finales											
Documentación.											

Creación de manuales (usuario y técnico).												
Evaluación TT II.												

Nombre del alumno(a): Hernandez Martinez Jorge Luis

TT No.:

Título del TT: Servidor de autenticación AAA mediante protocolo de autenticación TACACS

Actividad	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	ENE
Investigación Documental.											
Revisión del hardware y software requerido.											
Prototipos del Diseño del servidor											
Pruebas preliminares											
Evaluación TT I.											
Diseño de la interfaz gráfica											
Corrección de errores.											
Pruebas finales											
Documentación.											
Creación de manuales (usuario y técnico).											
Evaluación TT II.											

7. Referencias

- [1] R. Provoste, «SEC GRUUP,» Septiembre 2014. [En línea]. Available: <https://sites.google.com/site/secgruttp/Dispositivos-de-seguridadiservidoresaaa>. [Último acceso: Marzo 2020].
- [2] CISCO, «Privilegios TACACS,» CISCO, 26 Febrero 2008. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/scsecurity-vpn/remote-authentication-dial-uscr-service-radius/13860-PRIV.html. [Último acceso: Marzo 2020].
- [3] GIT BOOK, «GITBOOK,» Jsitech, Marzo 2016. [En línea]. Available: <https://legacy.gitbook.com/book/jsitech/servidor-tacacs-en-linux/details>. [Último acceso: Marzo 2020].
- [4] CISCO, «Cisco Identity Services Engine,» CISCO, [En línea]. Available: <https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html>—case-studies. [Último acceso: Marzo 2020].
- [5] Microsoft, «Introducción a Active Directory,» Microsoft, 18 Octubre 2000. [En línea]. Available: <https://support.microsoft.com/es-mx/help/196464>. [Último acceso: Marzo 2020].
- [6] Extreme, «Extreme Control,» Extreme, [En línea]. Available: <https://www.extremenetworks.com/product/extremecontrol/>. [Último acceso: Marzo 2020].
- [7] Networld, «Seguridad en la RED,» 2018. [En línea]. Available: <https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red>. [Último acceso: Marzo 2020].
- [8] Agile.org, «Beneficios de SCRUM,» 2017. [En línea]. Available: <https://proyectosagiles.org/beneficios-de-scrum/>. [Último acceso: Marzo 2020].

8. Alumnos y Directores

Ortiz Gudiño Esmeralda.- Alumna de la carrera de Ing. en Sistemas Computacionales en ESCOM, Boleta: 2015630356, email: esmeralda.ortizg96@gmail.com.

Firma: _____

Hernandez Martinez Jorge Luis.- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Boleta: 2016630461, email: jorsh.hernandez.fs@gmail.com

Firma: _____

Benjamín Cruz Torres.- Profesor de la carrera de Ing. en Sistemas Computacionales en ESCOM, email: benji.slayer@gmail.com

Firma: _____

CARÁCTER: Confidencial
FUNDAMENTO LEGAL: Art. 3, fracc. II, Art. 18, fracc. II y Art. 21, lineamiento 32, fracc. XVII de la L.F.T.A.I.P.G.
PARTES CONFIDENCIALES: No. de boleta y Teléfono.

Profesor Torres Cruz Benjamin

**Benji Cruz** Anteayer
para mí ▾

Buen día.

Estoy de acuerdo con la reactivación del protocolo.
Estoy de acuerdo con el alta.

Saludos.

**Instituto Politécnico Nacional**
Escuela Superior de Cómputo

DR. BENJAMÍN CRUZ TORRES
DOCENTE

Unidad Profesional Adolfo López Mateos,
Av. Juan de Dios Batiz s/n Colonia Lindavilla,
Demarcación Territorial Gustavo A. Madero, C. P. 07738
Tel. 5729 4000, ext. 52032
Cel. 044 55 16 49 32 27
benji_slay@hotmail.com

[Mostrar texto citado](#)

Profesora López Ruiz Gabriela de Jesús

**Esmeralda Ortiz** 10:17 a. m.
Muchas gracias. Profesora Gabriela. De su amable apoyo lo antes posible con el VoBo de


**TTs Escom** 2:51 p. m.
para mí ▾

Gracias por informarme, de acuerdo con su solicitud, confirmo de enterada y recibida la petición


Atte.
Maestra Gabriela de Jesús López Ruiz

[Mostrar texto citado](#)


Profesores Moreno Cervantes Axel Ernesto y Cortes Duarte Nidia Asunción

- **Esmeralda Ortiz**


3 mar. 2021 21:46 (hace 2 días) ☆

Buenas noches estimados. Les compartimos la nueva versión del protocolo en donde se incluye el nombre de mi compañero Hernandez Martinez Jorge Luis...
- **Axel Ernesto**

3 mar. 2021 23:23 (hace 2 días) ☆

Acuso de recibo y doy visto bueno
- **Esmeralda Ortiz**


4 mar. 2021 21:30 (hace 19 horas) ☆

Buenas noches. Profesora Nidia, Gabriela De su apoyo por favor con su vobo. Saludos
- **Nidia A. Cortez**


00:50 (hace 16 horas) ☆

Acuso de recibido y doy visto bueno.

Alumno Hernández Martínez Jorge Luis

- **Esmeralda Ortiz**

10:17 (hace 9 horas) ☆

Muchas gracias. Profesora Gabriela. De su amable apoyo lo antes posible con el VoBo de acuerdo a las modificaciones solicitadas para poder enviar la solici...
- **Josh Hdz** <jorsh.hernandez.fs@gmail.com>

19:53 (hace 4 minutos) ☆ ↩ ⋮

para Esmeralda ▾

Enterado y doy visto bueno
