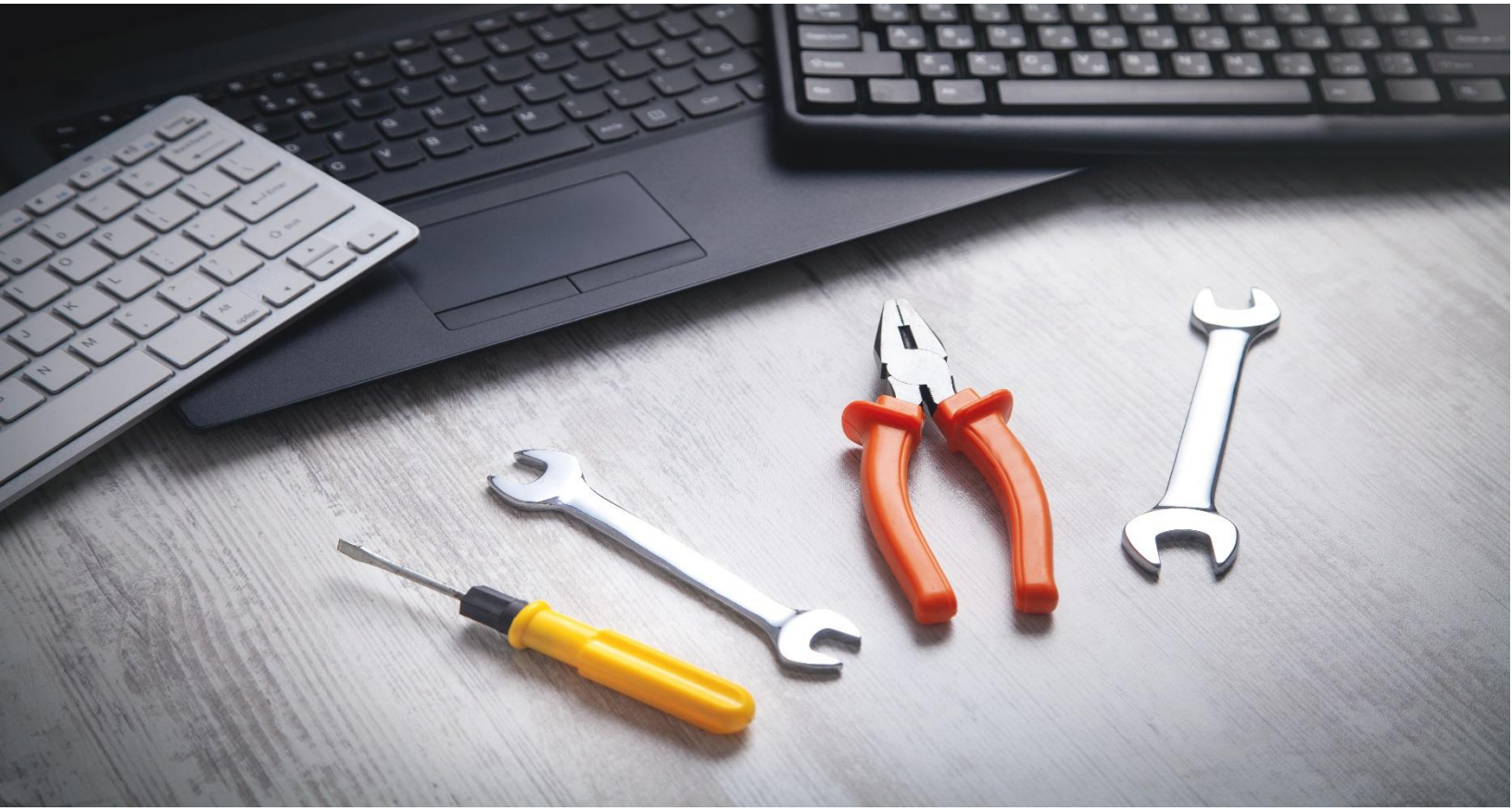
GESTIÓN Y SOPORTE DE SEGURIDAD EN HARDWARE Y SOFTWARE



Controles de acceso

Unidad 1

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yañez

ELABORACIÓN

Experto disciplinar: Felipe Reyes Cáceres

Diseñador instruccional: Antonio Colmenares Prieto

Editora instruccional: María José Fonseca Palacios

VALIDACIÓN

Experto disciplinar:

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

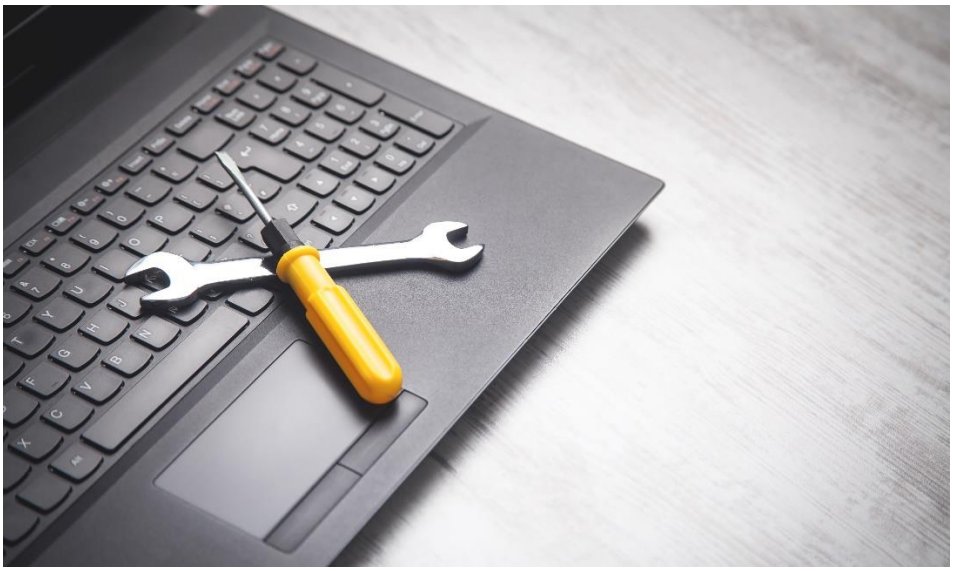
AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Configuran servicios de seguridad y control de acceso, considerando estandarización y normativa legal vigente.



Introducción

Durante esta primera semana abordaremos conceptos relacionados con la implementación de soluciones de seguridad, a través de controles de acceso tomando en consideración la normativa legal vigente y protocolos estándares de la industria

Así podrán revisar los siguientes aspectos:

- Los propósitos del protocolo AAA.
- La Autenticación Local de AAA.
- La Autorización del protocolo.
- Los Servicios de seguridad basados en AAA.
- La Configuración de AAA basado en Servidor.

1. Componentes de control de acceso AAA

La sigla AAA tiene el significado de Autenticación, Autorización y Registro.

Al observar la definición de AAA, se deprende que la misma tiene similitud a la utilización de una tarjeta de crédito, como se demuestra en siguiente figura, la tarjeta de crédito puede identificar quién las usa y cuánto pueden gastar en ella, manteniendo además un registro de qué cantidad de servicios o elementos adquirió el usuario.

"AAA" o "triple A", son servicios que entregan el marco principal para poder realizar el ajuste en el control de acceso en los dispositivos de redes. AAA se define como una manera de controlar quienes tienen permitidos el acceso a una red (autenticación), poder regular y controlar lo que la persona pueden hacer mientras este allí (autorización) y qué acción puede realizar mientras accede a la red (registro).

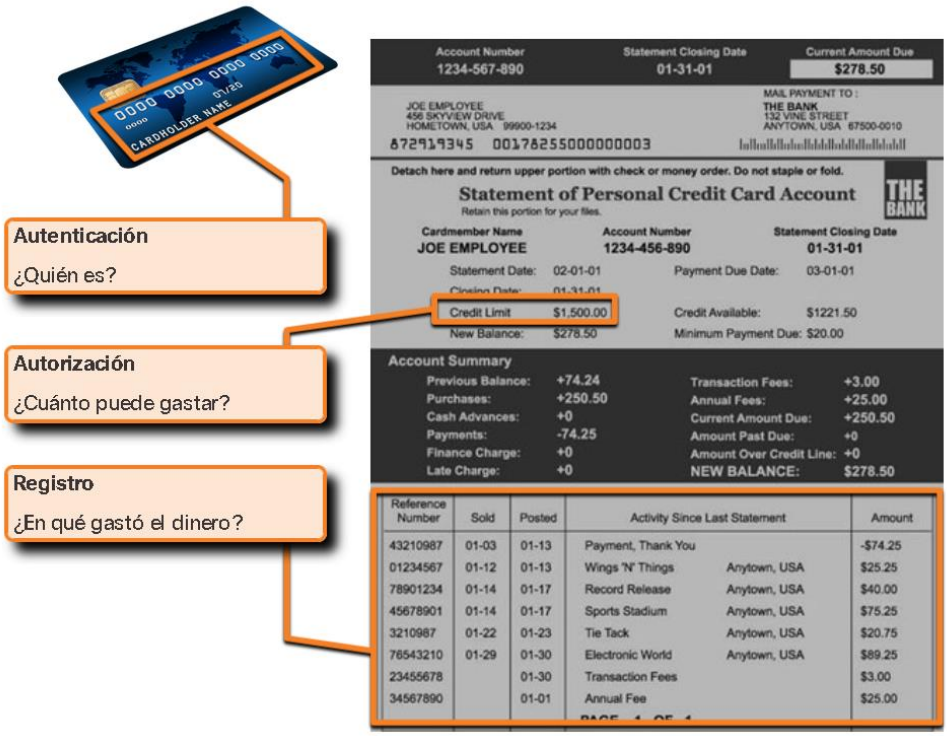


Figura 1. Tipos de archivos SQL Server

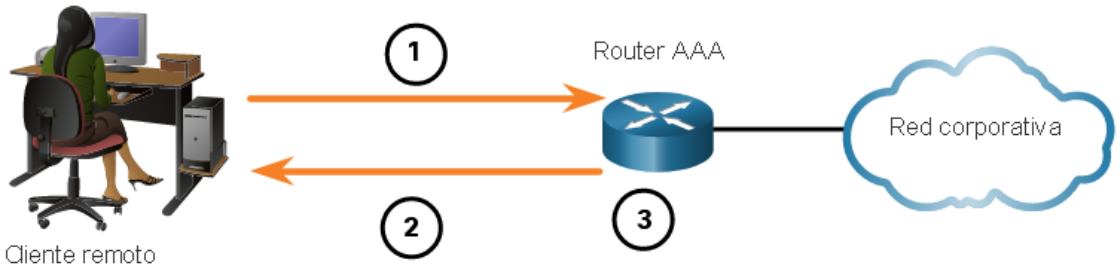
Fuente: Credit bank (2022)

2. Autenticación

Existen 2 métodos para implementar la autenticación AAA y estas son "Local" y "basado en servidor".

2.1 Autenticación AAA local

El AAA local, guarda el nombre de usuario y las contraseñas de forma local en los dispositivos de redes como el router Cisco. El usuario se autentica contra las bases de datos locales, como se observa en la figura. AAA local, la cual es ideal para un red pequeña.



1. El cliente establece una conexión con el router.
2. El router AAA solicita al usuario un nombre de usuario y una contraseña.
3. El router autentica el nombre de usuario y la contraseña mediante la base de datos local y el usuario obtiene acceso a la red en función de la información de esta base de datos.

Figura 2 Autenticación AAA local

Fuente: Cisco networking academy (2022)

2.2 Autenticación AAA basada en el servidor

Con los métodos basados en el servidor, el router da acceso a algún servidor central de AAA, como se puede observar en siguiente figura, el servidor AAA posee las contraseñas y nombres de usuario de los usuarios.

El router AAA, generalmente aplica el protocolo de Sistema de Control de Acceso del Controlador de Acceso Terminal Mejorado (TACACS+) o denominado protocolo de Servicio de Autenticación Remota de Usuario de Discado (RADIUS) para por tener comunicación con el servidor de AAA. Cuando existen múltiples switches y enrutadores, los métodos basados en el servidor son más apropiados.

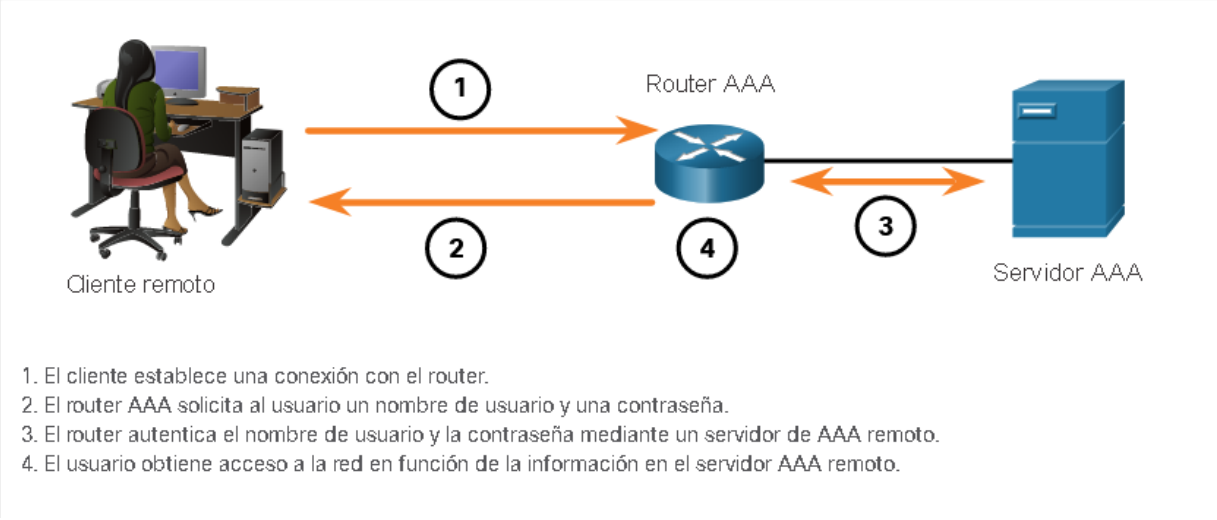


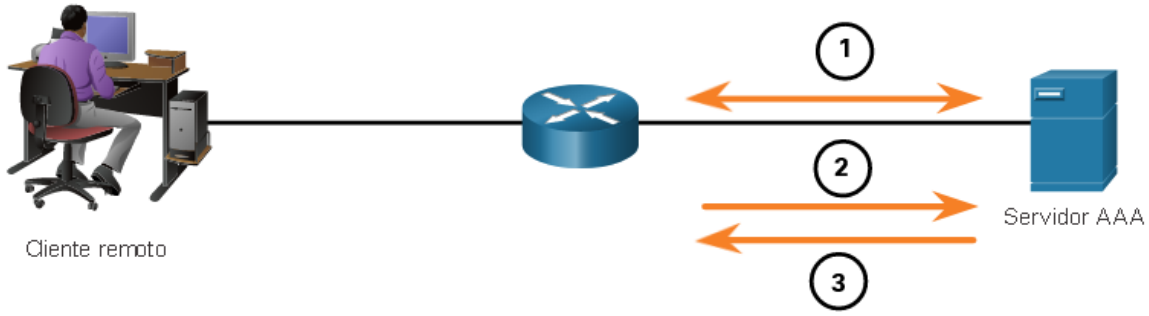
Figura 3. Autenticación AAA basada en servidor

Fuente: Cisco networking academy (2022)

3. Autorización

La autorización es automática y no requiere que los usuarios tomen medidas adicionales después de la autenticación. La autorización controla lo que el usuario puede hacer o no en la red después de una autenticación satisfactoria:

La autorización utiliza un conjunto de atributos que describe el acceso del usuario a la red. Estos atributos son usados por el servidor AAA para determinar privilegios y restricciones para ese usuario, como se muestra en la figura.



1. Cuando un usuario ha sido autenticado, una sesión es establecida entre el router y el servidor AAA.
2. El router pide autorización al servidor AAA para la solicitud de servicio del cliente.
3. El servidor AAA responde con un PASS/FAIL a la solicitud.

Figura 3. Autorización

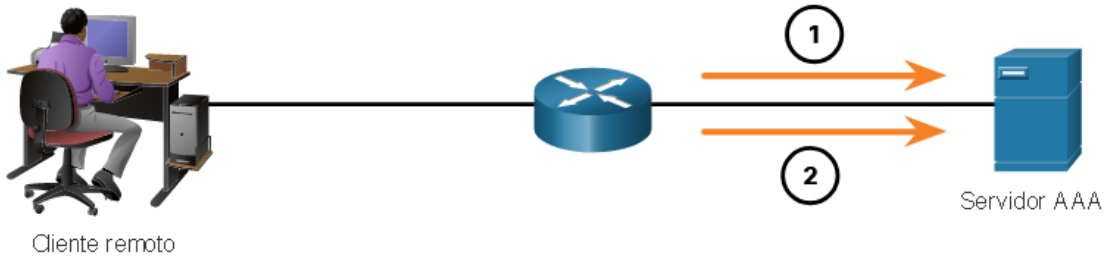
Fuente. Cisco networking academy (2022)

4. Registro

El registro de AAA recopila y reporta datos de uso. La organización puede utilizar estos datos para fines como auditorías o facturación. Los datos recopilados pueden incluir la hora de inicio y finalización de la conexión, los comandos ejecutados, la cantidad de paquetes y el número de bytes.

Un uso muy implementado debe registro consiste en combinarlo con la autenticación AAA. Los servidores AAA mantienen un registro detallado de lo que el usuario autenticado hace exactamente en el dispositivo, como se muestra en la imagen Esto incluye todos los comandos EXEC y de configuración que emite el usuario. El registro contiene varios campos de datos, incluidos el nombre de usuario, la fecha y hora, y el comando real que introdujo el usuario. Esta información resulta útil para solucionar

problemas de dispositivos. Además proporciona evidencia contra individuos que realizan actividades maliciosas.



1. Cuando se autentica a un usuario, el proceso de registro AAA genera un mensaje para comenzar el proceso de contabilidad.
2. Cuando el usuario termina, se registra un mensaje de finalización y se da por terminado el proceso de contabilidad.

Figura 4. Registro

Fuente: Cisco networking academy (2022)

5. Autenticación sin AAA

La autenticación de un usuario se puede completar sin AAA.

La autenticación de acceso se puede configurar viendo la figura que a continuación se muestra. Esto incluye especificar puertos auxiliares, inicio de sesión de consola y líneas vty.

Cualquier persona con la contraseña puede acceder y cambiar la configuración del dispositivo sin ninguna repercusión legal.

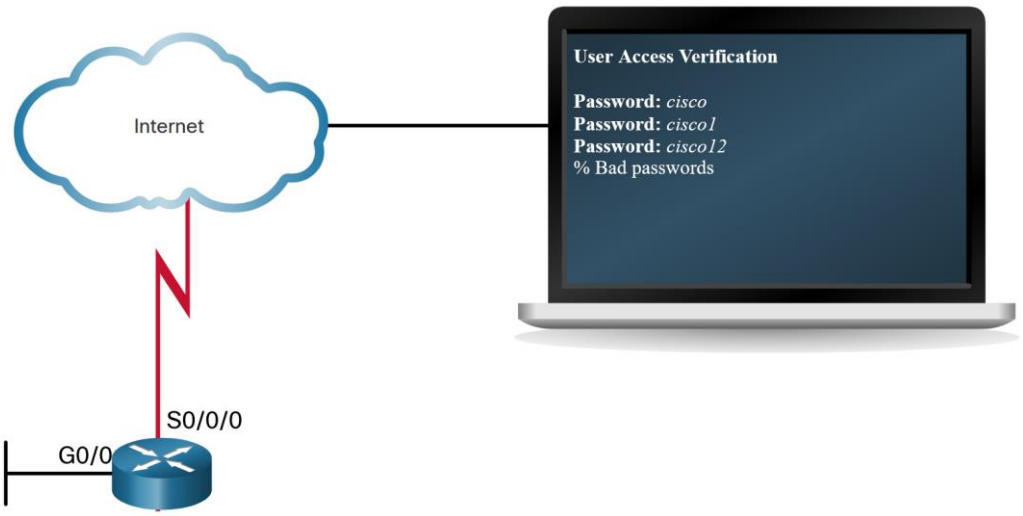


Figura 5. Autenticación sin AAA

Fuente. Credit bank (2022)

La seguridad AAA presenta tres secciones, cada una de las cuales trata un aspecto específico de la seguridad:

Autenticación: Estas secciones incluyen AAA administrativa y de red, las cuales mitigan los peligros para los usuarios. La prueba de identidad en una red se puede lograr a través de una combinación de nombre de usuario y contraseña, una tarjeta con un chip de seguridad o un conjunto de preguntas de desafío/respuesta. Algunos ejemplos de métodos para probar la identidad incluyen proporcionar la contraseña como prueba de que alguien es un usuario "estudiante".

Autorización: Los servicios controlan qué acciones puede realizar un usuario después de autenticarse. Por ejemplo, los estudiantes solo pueden acceder al servidor host XYZ a través de SSH después de la autenticación.

Contabilidad y auditoría: El registro preciso del tiempo y los recursos utilizados se logra mediante el registro de todo lo que hace un usuario. Este método registra que un estudiante usó 15 minutos de la conexión SSH compartida para alojar un servidor llamado XYZ.

6. Configurar la autenticación AAA local

En la pestaña Autenticación, seleccione la opción para configurar la autenticación AAA para configurar la autenticación AAA local.

Los métodos de autenticación AAA son equivalentes a iniciar sesión localmente.

Los usuarios de AAA pueden seleccionar entre varios métodos de autenticación de respaldo al crear una configuración.

Paso 1. Es necesario crear procedimientos básicos para la autenticación local de los administradores. La protección de contraseña en las funciones administrativas de un enrutador debe

ingresarse a través de la base de datos. Esto es necesario para acceder a los nombres de usuario y contraseñas.

Paso 2. Habilite AAA para que se puede habilitar en el enrutador a nivel mundial.

Paso 3. Resuelva cualquier problema AAA.

Paso 4. Verificando y resolviendo cualquier problema en la configuración.

```
Router(config)# aaa authentication login {default | list-name} method1…[ method4 ]
```

Dominio	Descripción
defecto	Utiliza los métodos de autenticación enumerados que siguen a esta palabra clave como la lista predeterminada de métodos cuando un usuario inicia sesión.
Lista de nombres	Cadena de caracteres utilizada para nombrar la lista de métodos de autenticación activados cuando un usuario inicia sesión.
método1...[método4]	Identifica la lista de métodos que el proceso de autenticación AAA consultará en la secuencia dada. Se debe especificar al menos un método. Se puede especificar un máximo de cuatro métodos.

Figura 6. Autenticación AAA local

Fuente. Cisco networking academy (2022)

Se pueden agregar métodos de autenticación secundarios a la configuración de una base de datos. Estas medidas adicionales se pueden utilizar incluso si fallan otros métodos de autenticación.

```
Router(config)# aaa authentication login {default | list-name} method1…[ method4 ]
```

Palabras clave de tipo de método	Descripción
habilitar	Utiliza la contraseña de activación para la autenticación.
local	Utiliza la base de datos de nombres de usuario local para la autenticación.
caso-local	Utiliza autenticación de nombre de usuario local que distingue entre mayúsculas y minúsculas.
ninguna	No utiliza autenticación.
radio de grupo	Utiliza la lista de todos los servidores RADIUS para la autenticación.
grupo tacacs+	Utiliza la lista de todos los servidores TACACS+ para la autenticación.
grupo nombre-grupo	Utiliza un subconjunto de servidores RADIUS o TACACS+ para la autenticación según lo define el comando aaa group server radius o aaa group server tacacs+.

Figura 7 método de autenticación AAA local

Fuente. Cisco networking academy (2022)

Las líneas e interfaces cuentan con múltiples métodos de autenticación gracias a una lista genérica.

Primero se debe elegir un título antes de que la lista sea de acceso público.

Agregar métodos de autenticación personalizados puede omitir las listas configuradas de forma predeterminada para cada interfaz.

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case enable
R1(config)# aaa authentication login SSH-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication SSH-LOGIN
```

Figura 8 método predeterminado de autenticación AAA I

Fuente. Cisco networking academy (2022)

Se agrega seguridad adicional a la línea al requerir frecuentes intentos de autenticación.

Este comando bloquea todas las cuentas con muchos intentos de inicio de sesión fallidos al bloquear todas las cuentas de usuario AAA.

```
Router(config)# aaa local authentication attempts max-fail [number-of-unsuccessful-attempts]
```

Dominio	Descripción
número de intentos fallidos	Número de intentos de autenticación fallidos antes de que se interrumpa la conexión y se bloquee la cuenta de usuario.

Figura 9 Cantidad de intentos de autenticación AAA

Fuente. Cisco networking academy (2022)

Cierre

Después de revisado el contenido de la semana, pueden establecer los siguientes conceptos clave:

Figura 11 Ideas claves, semana 1.

Fuente. Reyes, F. (2022)

Referencias bibliográficas

Cisco networking academy. (2022). SEGURIDAD EN ACCESO.

Perle System .Uso de seguridad AAA para la administración de Equipos de Conectividad https://www.perlesystems.es/supportfiles/aaa-security.shtml

Ciberseguridad .com ¿Qué es AAA en Ciberseguridad? Todo lo que debes saber. https://ciberseguridad.com/guias/prevencion-proteccion/aaa/