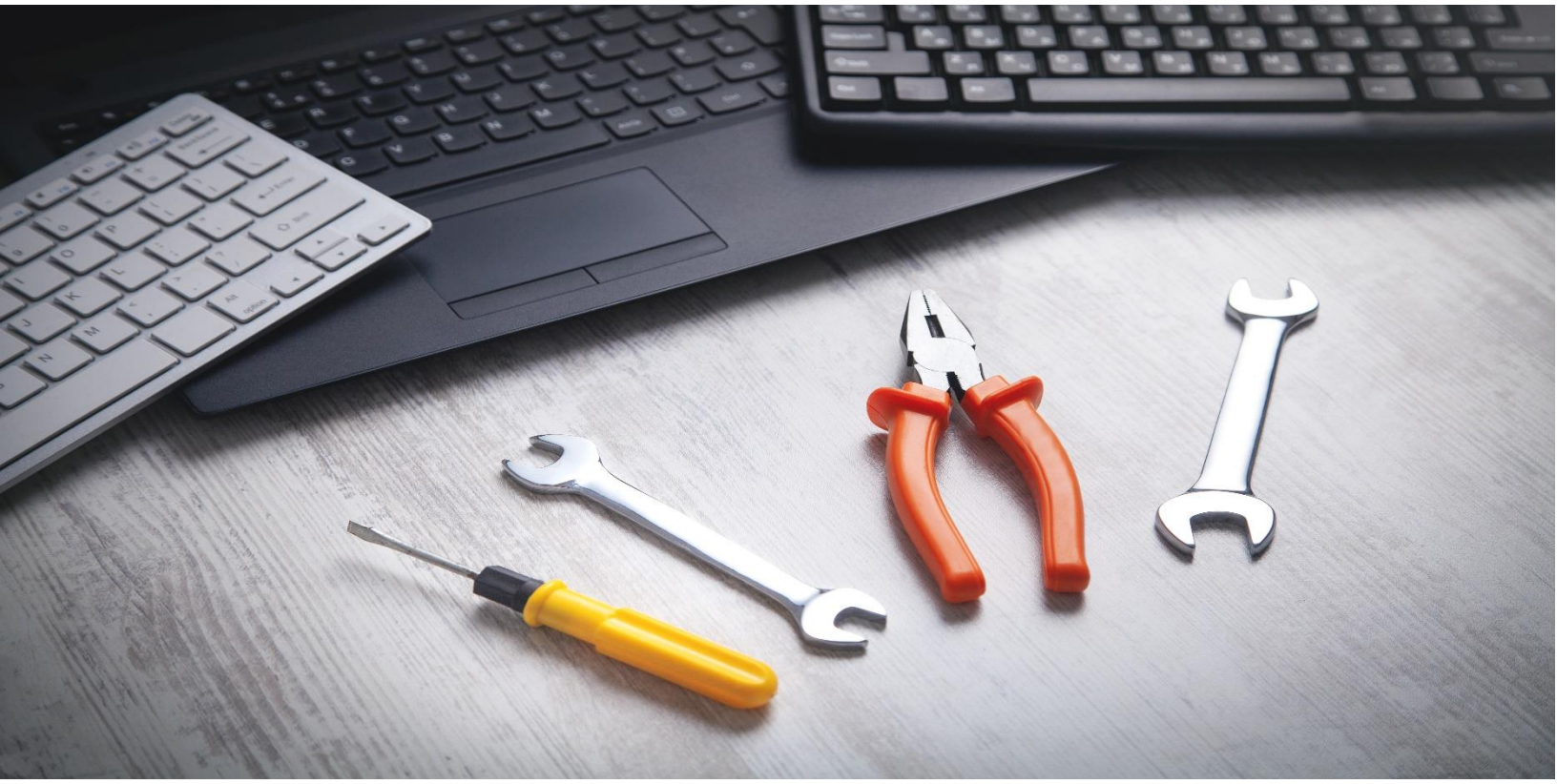
GESTIÓN Y SOPORTE DE SEGURIDAD EN HARDWARE Y SOFTWARE



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

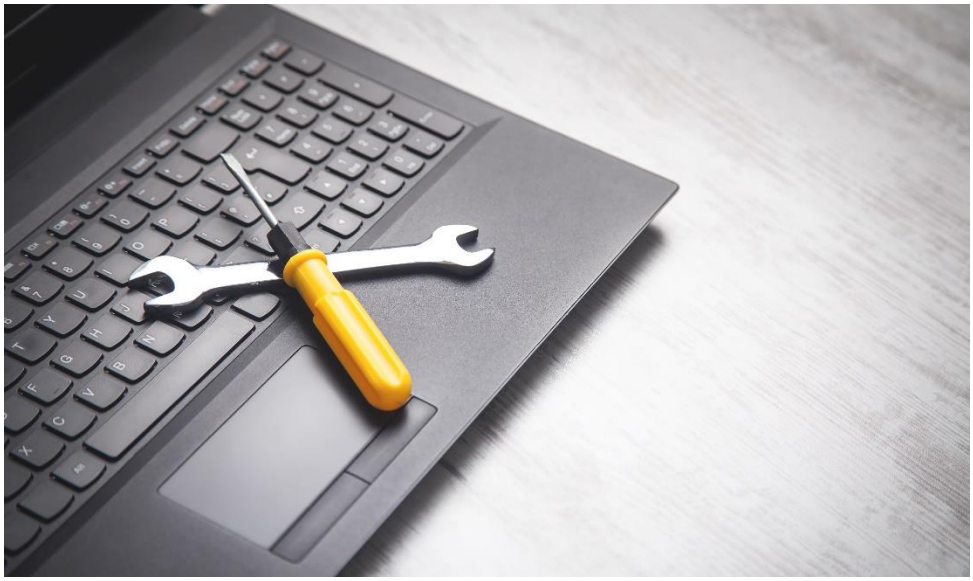
AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Configuran servicios de seguridad y control de acceso Radius y Tacacs, según estandarizaciones y normativas.



Introducción

En esta ocasión abordaremos el protocolo estándar y las leyes legales cuando discutimos formas de implementar sistemas de seguridad.

Los temas a ser revisados son los siguientes:

- Los servidores Tacacs y Radius.
- Configuración del radio del servidor que modifica y cómo se configura el acceso dependiente.
- Utilización de la configuración de acceso del Tacacs Server.
- Los estándares se refieren a IEEE y RCF 2138, así como a IEEE y RCF 1492.

1. Los protocolos TACACS+ y RADIUS

Los protocolos adicionales admiten la conexión de servicios que no están incluidos en el conjunto básico: TACACS+ y RADIUS.

Los diferentes protocolos de autenticación admiten diferentes funciones y capacidades, como se indica en la tabla.

	TACACS+	RADIO
Funcionalidad	Separa AAA de acuerdo con la arquitectura AAA, lo que permite la modularidad de la implementación del servidor de seguridad.	Combina autenticación y autorización pero separa la contabilidad, lo que permite menos flexibilidad en la implementación que TACACS+
Estándar	Principalmente compatible con Cisco	Estándar abierto/RFC
Protocolo de transporte	TCP	UDP
CAP	Desafío y respuesta bidireccionales como se usa en el Protocolo de autenticación por desafío mutuo (CHAP)	Desafío y respuesta unidireccionales del servidor de seguridad RADIUS al cliente RADIUS
Confidencialidad	Todo el paquete encriptado	Contraseña encriptada
personalización	Proporciona autorización de los comandos del enrutador por usuario o por grupo	No tiene opción para autorizar los comandos del enrutador por usuario o por grupo

Figura 1. Protocolos TACACS+ y RADIUS

Fuente. Cisco networking academy (2022)

1.1 Autenticación TACACS+

Para acceder al sistema, los usuarios deben proporcionar autenticación TACACS+.

El protocolo TACACS se mejoró con la adición de TACACS+ de Cisco.

TACACS+ brinda múltiples servicios AAA. Se puede utilizar junto con otros métodos de autenticación, como la biometría, para contabilidad y

autorización. También se puede utilizar por separado para cada propósito.

El uso de un ícono más correlaciona la autenticación con TACACS+

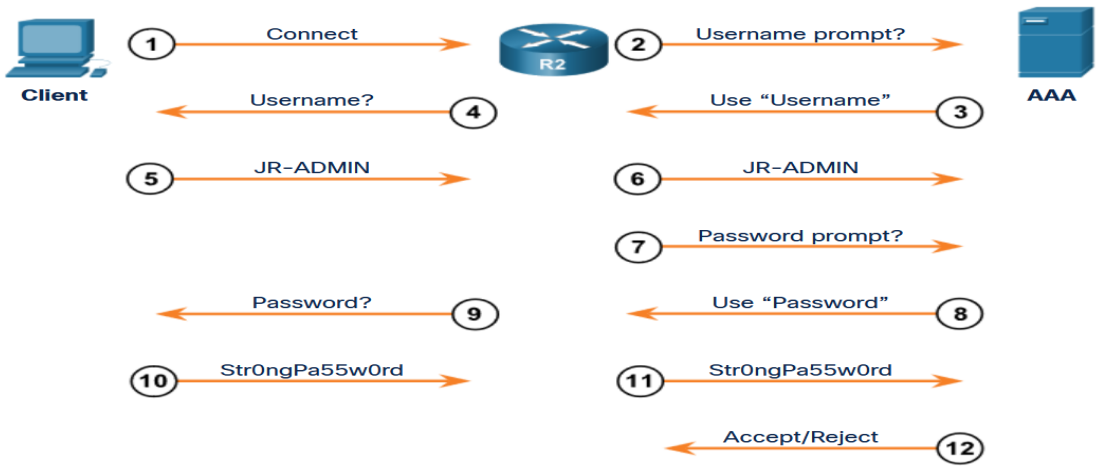


Figura 2. Autenticación TACACS+

Fuente: Cisco networking academy (2022)

1.2 Autenticación RADIUS

La autenticación de RADIUS requiere comprender el radio del esquema de autenticación.

El protocolo AAA de IETF, RADIUS, es un estándar abierto que se usa comúnmente para mover direcciones IP entre ubicaciones. Se puede usar mientras está en movimiento o en una configuración de red de área local.

Cuando se utiliza el protocolo RADIUS, los datos se ocultan mediante la función de hashing MD5 con una contraseña compartida y el protocolo

de autenticación de contraseña PAP. En ausencia de PAP, las contraseñas se transmiten en texto claro.

Radius combina autenticación y autorización en un solo paso.

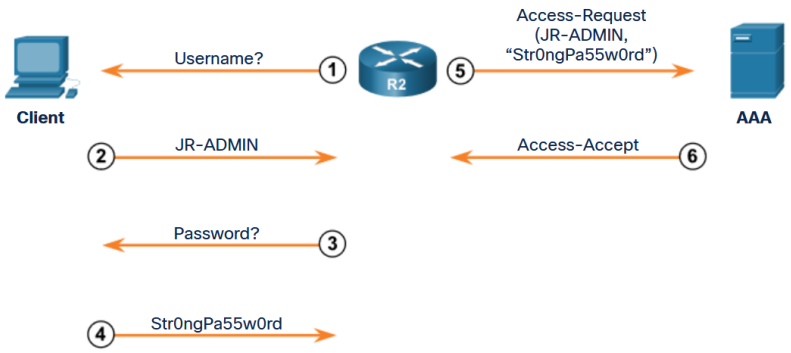


Figura 3. Autenticación RADIUS

Fuente. Cisco networking academy (2022)

2. Configurar la autenticación basada en servidor

Para ellos debemos al menú para ajustar las opciones de autenticación en el lado del servidor.

Para probar la identidad de un usuario, es necesario un proceso de cuatro pasos secuenciales.

Paso 1. Habilitar AAA globalmente es esencial al ejecutar cualquier comando AAA. Esto se debe a que permite el uso de todos los elementos AAA.

Paso 2. Elija un servidor radius o tacacs si necesita usar las funciones avanzadas del enrutador.

Paso 3. Las transferencias de datos entre un dispositivo de red y los servidores AAA se pueden cifrar configurando la clave de cifrado.

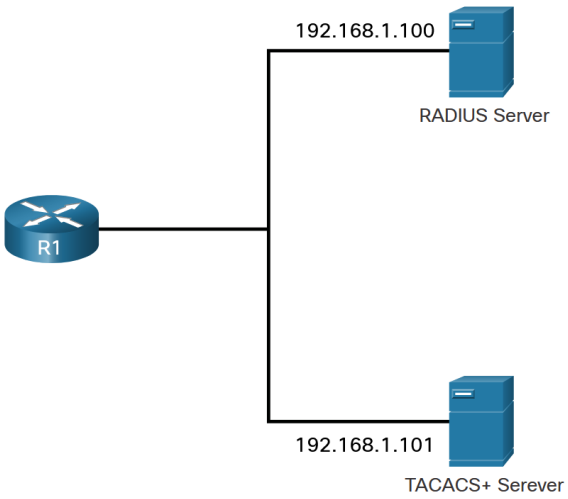
Paso 4. Es posible configurar varios métodos de autenticación AAA al configurar la redundancia. Hacerlo requiere elegir TACACS+ o RADIUS como la primera opción en la lista de métodos al configurar la redundancia.

2.1 Configurar servidores TACACS+

La configuración de un servidor TACACS+ requiere acceder a su modo de configuración a través de su panel de configuración. Desde aquí, cambie la dirección IPv4 debajo del encabezado ipv4 para configurar el servidor TACS+. También puede cambiar el puerto utilizado para autenticación y contabilidad.

Los servidores TACACS+ adicionales deben tener sus direcciones IP ingresadas usando el formato apropiado.

El servidor y el enrutador TACACS+ deben usar claves secretas compartidas configuradas a través del comando KEY.




```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs server Server-T
R1(config-server-tacacs)# address ipv4 192.168.1.101
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key TACACS-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)#
```

Figura 4. Configurar TACACS+

Fuente. Cisco networking academy (2022)

2.2 Configurar servidores RADIUS

Para ello debemos cambiar la configuración del servidor RADIUS haciendo referencia a su nombre de dominio.

Al ingresar el nombre de cada servidor RADIUS en el programa, se pueden descubrir servidores adicionales.

En la página de configuración del servidor RADIUS, establezca la dirección IPv4 del servidor que se configurará desde esa página.

La clave compartida se debe utilizar para cifrar la contraseña.

```
R1(config)# aaa new-model
R1(config)#
R1(config)# radius server SERVER-R
R1(config-radius-server)# address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
R1(config-radius-server)# key RADIUS-Pa55w0rd
R1(config-radius-server)# exit R1(config)#
```

Figura 5. Configurar RADIUS

Fuente. Cisco networking academy (2022)

3. Autenticarse en los comandos de configuración del servidor AAA

Los servidores necesitan reglas de firewall AAA para asociarse con ellos cuando se descubren. Los servidores AAA se enumeran en la categoría tacacs+ radius para su servidor AAA compartido.

```
R1(config)# aaa authentication login default ?
  cache          Use Cached-group
  enable         Use enable password for authentication.
  group          Use Server-group
  krb5           Use Kerberos 5 authentication.
  krb5-telnet    Allow logins only if already authenticated via Kerberos V
                 Telnet.
  line           Use line password for authentication.
  local          Use local username authentication.
  local-case     Use case-sensitive local username authentication.
  none           NO authentication.
  passwd-expiry  enable the login list to provide password aging support

R1(config)# aaa authentication login default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
```

Figura 6. Autenticacion

Fuente: Cisco networking academy (2022)

```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs server Server-T
R1(config-server-tacacs)# address ipv4 192.168.1.100
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key TACACS-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)#
R1(config)# radius server SERVER-R
R1(config-radius-server)# address ipv4 192.168.1.101 auth-port 1812 acct-port 1813
R1(config-radius-server)# key RADIUS-Pa55w0rd
R1(config-radius-server)# exit
R1(config)#
R1(config)# aaa authentication login default group tacacs+ group radius local-case
```

Figura 7. Autenticación

Fuente. Cisco networking academy (2022)

4. IEEE 802.1x

El estándar IEEE 802.1X define un control de acceso y un protocolo de autenticación basados en puertos. Este protocolo evita que las estaciones de trabajo no autorizadas se conecten a una LAN a través de puertos de switch de acceso público. El servidor de autenticación autentica cada estación de trabajo, que está conectada a un puerto del switch, antes de habilitar cualquier servicio ofrecido por el switch o la LAN.

Con la autenticación 802.1X basada en puertos, los dispositivos de la red cumplen roles específicos, como se muestra en la figura:

Figura 10 IEEE 802.1X

Fuente. Cisco networking academy (2022)

Cliente (suplicante): este es un dispositivo ejecutando software de cliente 802.1X, el cual está disponible para dispositivos conectados por cable o inalámbricos.

Switch (Autenticador): el switch funciona como actúa intermediario (proxy) entre el cliente y el servidor de autenticación. Solicita la identificación de la información del cliente, verifica dicha información al servidor de autenticación y transmite una respuesta al cliente. Otro dispositivo que puede actuar como autenticador es un punto de acceso inalámbrico.

Servidor de autenticación: el servidor valida la identidad del cliente y notifica al switch o al punto de acceso inalámbrico si el cliente esta o no autorizado para acceder a la LAN y a los servicios del Switch.

Cierre

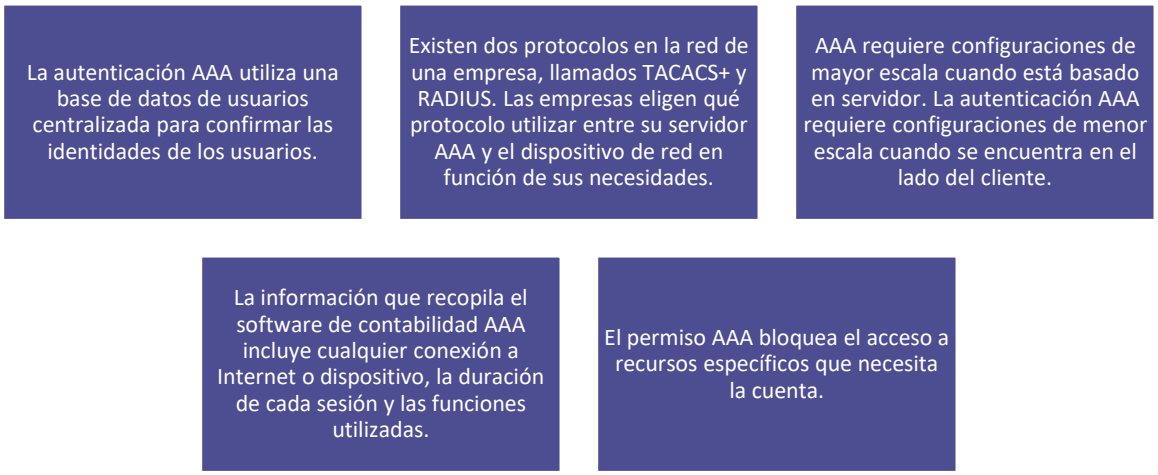


Figura 8. Ideas claves, semana 2

Fuente: Cisco networking academy (2022)

Referencias bibliográficas

Cisco networking academy. (2022). SEGURIDAD EN ACCESO

Redzone. Para qué sirve un servidor RADIUS y su funcionamiento https://www.redeszone.net/tutoriales/servidores/que-es-servidor-radius-funcionamiento/

Cisco.com. configuración TACACS+, RADIUS https://www.cisco.com/c/es_mx/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/13847-72.pdf