Comparación de TACACS+ y RADIUS

Contenido

Introducción

Dos protocolos de seguridad destacados utilizados para controlar el acceso a las redes son Cisco TACACS+ y RADIUS. La especificación RADIUS se describe en RFC 2865 , que deja obsoleto RFC 2138 . Cisco se ha comprometido en soportar ambos protocolos con las mejores ofertas de la clase. Cisco no pretende competir con RADIUS ni influir en los usuarios para que usen TACACS+. Debería elegir la solución que mejor satisfaga sus necesidades. Este documento detalla las diferencias entre TACACS+ y RADIUS a fin de poder realizar una elección informada.

Cisco ha soportado el protocolo RADIUS desde la Versión de Software 11.1 de febrero de 1996 de Cisco IOS®. Cisco continúa mejorando RADIUS Client con las nuevas funciones y capacidades, al soportar RADIUS como el estándar.

Cisco evaluó seriamente RADIUS como un security protocol antes de que desarrollara TACACS+. Muchas funciones fueron incluidas en el protocolo TACACS+ para que cumplan con las necesidades del mercado de seguridad en continuo crecimiento. El protocolo fue diseñado para que se incremente a medida que aumentan las redes y para que se adapte a la nueva tecnología de seguridad según la evolución del mercado. La arquitectura subyacente del protocolo TACACS+ complementa la arquitectura independiente de autenticación, autorización y

contabilidad (AAA).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Segundo plano de RADIUS

RADIUS un servidor de acceso que utiliza el protocolo AAA. Es un sistema de seguridad distribuida que protege el acceso remoto a las redes y a los servicios de red contra el acceso no autorizado. RADIUS comprende tres elementos:

- Un protocolo con un formato de trama que utiliza el User Datagram Protocol (UDP) /IP.
- Un servidor.
- Un cliente.

El servidor se ejecuta en un equipo central típicamente en el sitio de cliente, mientras que los clientes residen en los servidores de acceso por marcado y pueden ser distribuidos en la red. Cisco ha incorporado al RADIUS Client en el software de Cisco IOS Software Release 11.1 y posterior y del otro dispositivo.

Modelo de cliente/servidor

Un servidor de acceso a la red (NAS) actúa como cliente de RADIUS. El cliente es responsable de traspasar información del usuario a servidores RADIUS designados y de actuar según la repuesta recibida. Los servidores RADIUS son responsables de recibir las solicitudes de conexión del usuario, autenticar al usuario y devolver la información de configuración necesaria para que el cliente pueda brindarle el servicio al usuario. Los servidores RADIUS pueden actuar como clientes de servidor alterno respecto de otros servidores de autenticación.

Seguridad de redes:

Las transacciones entre el cliente y el servidor RADIUS son autenticadas mediante el uso de un secreto compartido, que nunca se envía por la red. Además, cualquier contraseña de usuario se envía cifrada entre el cliente y el servidor RADIUS. Esto elimina la posibilidad de que una persona que hace snooping en una red no segura pueda determinar la contraseña de un usuario.

Mecanismo de autenticación flexible

El servidor RADIUS soporta una variedad de métodos para autenticar un usuario. Cuando se proporciona con el nombre de usuario y la contraseña original otorgados por el usuario, puede soportar el PPP, el Password Authentication Protocol (PAP), o el Challenge Handshake Authentication Protocol (CHAP), UNIX login, y otros mecanismos de autenticación.

Disponibilidad del código del servidor

Hay una serie de distribuciones de código de servidor disponibles comercialmente y en forma gratuita. Los servidores de Cisco incluyen Cisco Secure ACS para Windows, Cisco Secure ACS para UNIX, y Access Registrar de Cisco.

Compare TACACS+ y RADIUS

Estas secciones comparan varias características del TACACS+ y RADIUS.

UDP y TCP

RADIUS utiliza UDP mientras que TACACS+ utiliza TCP. El TCP ofrece varias ventajas en comparación con el UDP. TCP ofrece un transporte orientado por conexión, mientras que UDP ofrece el mejor esfuerzo para entregar. RADIUS necesita variables programables adicionales tales como los intentos de retransmisión y tiempos de espera para compensar el transporte de producto de un esfuerzo razonable, pero carece del nivel de soporte incluido que ofrece un transporte TCP:

- El uso del TCP proporciona un reconocimiento independiente acerca de que se ha recibido una solicitud, dentro (aproximadamente) del trayecto de ida y vuelta (RTT), independientemente de la carga que soporte el mecanismo de autenticación de segundo plano y de su velocidad (un reconocimiento de TCP).
- TCP proporciona una indicación inmediata de un servidor caído o que no funciona a través de un reinicio (RST). Puede determinar cuando un servidor falla y vuelve a estar en servicio si utiliza las conexiones TCP de larga duración. UDP no puede indicar la diferencia entre un servidor desactivado, uno lento y uno inexistente.
- Mediante las señales de mantenimiento de TCP, las caídas del servidor pueden ser detectadas fuera de banda con peticiones actuales. Se pueden mantener conexiones a servidores múltiples simultáneamente, y sólo debe enviar mensajes a los que están activos y en funcionamiento.
- TCP permite mayor ampliación y se adapta a las redes en crecimiento y congestionadas.

Cifrado de Paquetes

RADIUS sólo cifra la contraseña en el paquete de solicitud de acceso, del cliente al servidor. El resto del paquete no está cifrado. Otra información, tal como el nombre de usuario, los servicios autorizados, y la cuenta, pueden capturarse a través de una tercera parte.

TACACS+ cifra todo el cuerpo del paquete pero deja un encabezado estándar de TACACS+. Dentro del encabezado se encuentra un campo que indica si el cuerpo se ha cifrado o no. Para facilitar el debugging, resulta útil que el cuerpo de los paquetes no esté cifrado. Sin embargo,

durante el funcionamiento normal, el cuerpo del paquete se cifra completamente para lograr comunicaciones más seguras.

Autenticación y autorización

RADIUS combina autenticación y autorización. Los paquetes access-accept enviados por el servidor de RADIUS al cliente contienen la información de autorización. Esto dificulta la tarea de desacoplar la autenticación y autorización.

TACACS+ usa la arquitectura AAA, la que separa a AAA. Esto permite soluciones de autenticación separada que pueden todavía usar TACACS+ para autorización y conteo. Por ejemplo, con TACACS+, es posible utilizar la autenticación de Kerberos y la autorización TACACS+ y el conteo. Después de que un NAS se autentique en un servidor de Kerberos, solicita la información de autorización de un servidor TACACS+ sin tener que volver a autenticarse. El NAS le informa al servidor TACACS+ que se ha autenticado de manera exitosa en un servidor Kerberos y luego el servidor le proporciona información de autorización.

Durante una sesión, si se requiere una verificación de autorización adicional, el servidor de acceso verifica con un servidor TACACS+ para determinar si el usuario tiene permiso para utilizar un comando determinado. Esto permite un mayor control de los comandos que pueden ejecutarse en el servidor de acceso mientras se desconecta del mecanismo de autenticación.

Soporte multiprotocolo

RADIUS no admite estos protocolos:

- Protocolo AppleTalk Remote Access (ARA)
- Protocolo NetBIOS Frame Protocol Control
- Novell Asynchronous Services Interface (NASI)
- Conexión X.25 PAD

TACACS+ ofrece soporte multiprotocolo.

Administración del router

RADIUS no permite a los usuarios controlar qué comandos pueden y no pueden ejecutarse en un router. Por lo tanto, RADIUS no es tan útil como para la administración del router ni tan flexible para los servicios de terminal.

TACACS+ proporciona dos métodos para controlar la autorización de los comandos del router por usuario o por grupo. El primer método es asignarle niveles de privilegio a los comandos y hacer que el router verifique con el servidor TACACS+ si el usuario está autorizado o no en ese nivel de privilegio específico. El segundo método es especificar explícitamente los comandos permitidos en el servidor TACACS+, por usuario o por grupo.

Interoperabilidad

Debido a las diversas interpretaciones de la Solicitud de Comentarios de RADIUS (RFC), el cumplimiento con RADIUS RFC no garantiza la interoperabilidad. Aunque varios vendedores implementan clientes RADIUS, esto no significa que sean interoperables. Cisco implementa la mayoría de los atributos de RADIUS y agrega constantemente más. Si los clientes utilizan

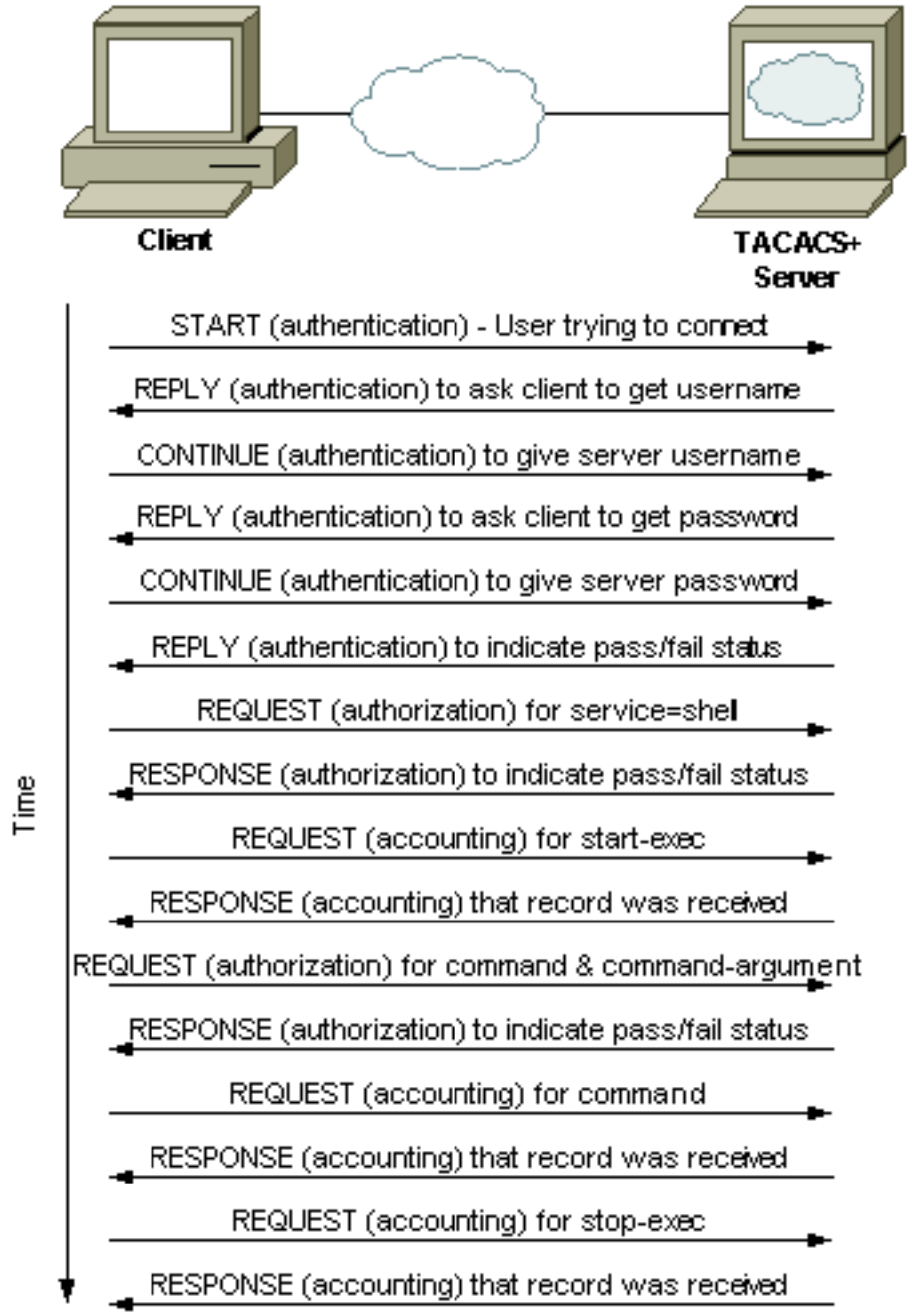
solamente los atributos de RADIUS estándar en sus servidores, pueden interoperar entre varios vendedores siempre que estos vendedores implementen los mismos atributos. Sin embargo, muchos proveedores implementan extensiones que son atributos de propietario. Si un cliente utiliza uno de estos atributos extendidos específicos del proveedor, la interoperabilidad no es posible.

Tráfico

Debido a las diferencias previamente mencionadas entre TACACS+ y RADIUS, la cantidad de tráfico generada entre el cliente y el servidor difiere. Estos ejemplos ilustran el tráfico entre el cliente y el servidor para TACACS+ y RADIUS cuando se usan para la administración del router con autenticación, autorización de exec, autorización de comandos (la cual RADIUS no puede llevar a cabo), contabilización de exec y contabilización de comandos (la cual RADIUS no puede llevar a cabo).

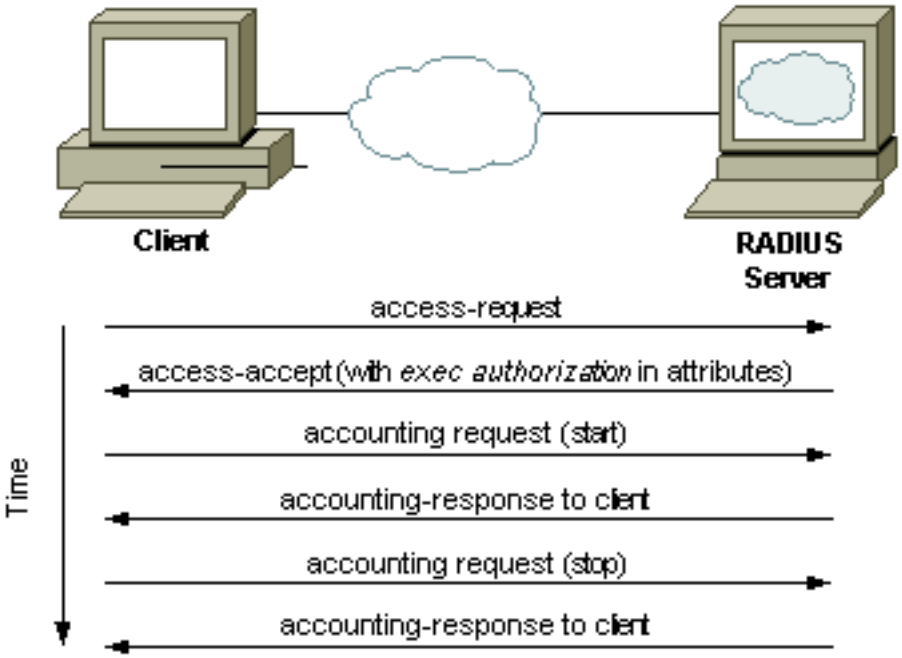
Ejemplo de tráfico de TACACS+

En este ejemplo se asume que la autenticación del inicio de sesión, la autorización exec, la autorización de comandos, el exec iniciar-detener y los comandos fueron implementados con TACACS cuando un usuario se conecta mediante Telnet a un router, ejecuta un comando y sale del router (no están disponibles otros servicios de administración):



Ejemplo deTráfico de RADIUS

En este ejemplo se asume que las cuentas de autenticación de usuario, la autorización exec y el exec iniciar-detener fueron implementadas con RADIUS cuando un usuario se conecta mediante Telnet a un router ejecuta un comando y sale del router (no están disponibles otros servicios de administración):



Soporte de dispositivo

Esta tabla detalla los soportes de TACACS+ y RADIUS AAA por tipo de dispositivo para las plataformas seleccionadas. Esto incluye la versión de software en la que se agregó el soporte. Verifique las notas de versión del producto para obtener más información, si su producto no se encuentra en esta lista.

Dispositivo de Cisco	autenticación TACACS+	autorización TACACS+	Contabilidad de TACACS+	Autenticación RADIUS	Autorización RADIUS	Contabilización RADIUS
Cisco Aironet [1]	12.2(4)AY	12.2(4)AY	12.2(4)AY	todos los puntos de acceso	todos los puntos de acceso	todos los puntos de acceso
Software Cisco IOS [2]	10.33	10.33	10.333	11.1.1	11.1.14	11.1.15
Cisco Cache Engine	—	—	—	1.5	1.56	—
Cisco Catalyst Switches	2.2	5.4.1	5.4.1	5.1	5.4.14	5.4.15
Cisco CSS 11000	5.03	5.03	5.03	5.0	5.04	—

Content Services Switch						
Cisco CSS 11500 Content Services Switch	5.20	5.20	5.20	5.20	5.204	—
Cisco PIX Firewall	4.0	4.07	4.28,5	4.0	5.27	4.28,5
Cisco Catalyst 1900/2820 switches	8.x empresa[9]	—	—	—	—	—
Cisco Catalyst 2900XL/3500XL switches	11.2.(8)SA610	11.2.(8)SA610	11.2.(8)SA610	12.0(5)WC511	12.0(5)WC5[11, 4]	12.0(5)WC5[11, 5]
Concentrador Cisco VPN 3000 [6]	3.0	3.0	—	2.012	2.0	2.012
Concentrador Cisco VPN 5000	—	—	—	5.2X12	5.2X12	5.2X12

'Notas de la tabla'

1. Terminación sólo de clientes inalámbricos, no del tráfico de administración en otra versión que no sea la del software 12.2(4)JA l posteriores del IOS de Cisco. En la versión de Cisco IOS Software 12.2.(4)JA o posterior, autenticación para la terminación de clientes inalámbricos y el tráfico de administración es posible.
2. Verifique el Feature Navigator (ahora obsoleto por el Software Advisor (clientes registrados solamente)) para conocer el Soporte de la plataforma dentro de Cisco IOS Software.
3. La contabilidad del comando no se implementa hasta la Cisco IOS Software Release 11.1.6.3.

4. Ninguna autorización de comando.
5. Ninguna contabilidad del comando.
6. Bloqueo de URL solamente, sin tráfico administrativo.
7. Autorización para el tráfico no VPN con PIX.**Nota:** Versión 5.2 - Soporte de lista de acceso para Lista de control de acceso (ACL) Atributo específico del proveedor (VSA) RADIUS o autorización TACACS+ para tráfico VPN que termina en la versión 6.1 de PIX - soporte para autorización de atributo 11 de RADIUS de ACL para tráfico VPN que termina en la versión 6.2.2 de PIX - soporte para ACL descargables con autorización RADIUS para tráfico VPN que termina en la versión 6.2 de PIX tráfico de administración a través de TACACS+.
8. Contabilidad para el tráfico no VPN con el PIX solamente, sin tráfico de administración.**Nota:** Versión 5.2 - Soporte para la contabilización de los paquetes TCP del cliente VPN a través del PIX.
9. Enterprise software solamente.
10. Requiere memoria Flash de 8 M para las imágenes.
11. Sólo terminación VPN.

Información Relacionada

- Página de soporte de RADIUS
- TACACS+ en documentación de IOS
- Página de soporte de TACACS/TACACS+
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems