TACACS+- und RADIUS-Vergleich

Inhalt

Einführung

Cisco TACACS+ und RADIUS sind zwei herausragende Sicherheitsprotokolle, die zur Kontrolle des Zugriffs auf Netzwerke verwendet werden. Die RADIUS-Spezifikation wird in RFC 2865 beschrieben, der RFC 2138 ersetzt. Cisco unterstützt beide Protokolle mit erstklassigen Angeboten. Cisco möchte weder mit RADIUS konkurrieren noch die Benutzer zur Verwendung von TACACS+ bewegen. Sie sollten die Lösung auswählen, die Ihren Anforderungen am besten gerecht wird. In diesem Dokument werden die Unterschiede zwischen TACACS+ und RADIUS erläutert, sodass Sie eine fundierte Entscheidung treffen können.

Seit Version 11.1 der Cisco IOS® Software im Februar 1996 unterstützt Cisco das RADIUS-Protokoll. Cisco verbessert den RADIUS-Client auch weiterhin durch neue Funktionen und Funktionen und unterstützt RADIUS als Standard.

Cisco hat RADIUS vor der Entwicklung von TACACS+ als Sicherheitsprotokoll ernsthaft evaluiert. Um den Anforderungen des wachsenden Sicherheitsmarktes gerecht zu werden, wurden zahlreiche Funktionen in das TACACS+-Protokoll aufgenommen. Das Protokoll wurde entwickelt, um skalierbar zu sein, wenn Netzwerke wachsen, und um sich an neue Sicherheitstechnologien anzupassen, wenn der Markt wächst. Die zugrunde liegende Architektur des TACACS+-Protokolls

ergänzt die unabhängige AAA-Architektur (Authentication, Authorization, Accounting).

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

RADIUS-Hintergrund

RADIUS ist ein Zugriffsserver, der das AAA-Protokoll verwendet. Es handelt sich um ein System mit verteilter Sicherheit, das den Remote-Zugriff auf Netzwerke und Netzwerkservices gegen unbefugten Zugriff schützt. RADIUS besteht aus drei Komponenten:

- Ein Protokoll mit einem Frame-Format, das User Datagram Protocol (UDP)/IP verwendet.
- Ein Server.
- Ein Client.

Der Server wird in der Regel auf einem zentralen Computer am Kundenstandort ausgeführt, während sich die Clients in den DFÜ-Zugriffsservern befinden und über das Netzwerk verteilt werden können. Cisco hat den RADIUS-Client in die Cisco IOS-Softwareversion 11.1 und höher sowie in andere Gerätesoftware integriert.

Client/Server-Modell

Ein Netzwerkzugriffsserver (NAS) fungiert als Client von RADIUS. Der Client ist dafür verantwortlich, Benutzerinformationen an bestimmte RADIUS-Server zu übergeben und dann auf die zurückgegebene Antwort zu reagieren. RADIUS-Server sind dafür verantwortlich, Benutzeranbindungsanfragen zu empfangen, den Benutzer zu authentifizieren und alle Konfigurationsdaten zurückzugeben, die der Client für die Bereitstellung des Dienstes an den Benutzer benötigt. Die RADIUS-Server können als Proxy-Clients für andere Arten von Authentifizierungsservern fungieren.

Netzwerksicherheit

Transaktionen zwischen dem Client und dem RADIUS-Server werden mithilfe eines gemeinsam genutzten geheimen Codes authentifiziert, der niemals über das Netzwerk gesendet wird. Darüber hinaus werden alle Benutzerpasswörter zwischen dem Client und dem RADIUS-Server verschlüsselt gesendet. Dadurch ist es nicht mehr möglich, dass jemand, der in einem ungesicherten Netzwerk schnüffelt, das Kennwort eines Benutzers festlegt.

Flexible Authentifizierungsmechanismen

Der RADIUS-Server unterstützt eine Vielzahl von Methoden zur Authentifizierung eines Benutzers. Wenn der Benutzername und das ursprüngliche Kennwort vom Benutzer angegeben werden, können PPP, Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), UNIX-Anmeldung und andere Authentifizierungsmechanismen unterstützt werden.

Servercodeverfügbarkeit

Es gibt eine Reihe von Distributionen von Servercode kommerziell und frei verfügbar. Zu den Cisco Servern gehören Cisco Secure ACS für Windows, Cisco Secure ACS für UNIX und Cisco Access Registrar.

TACACS+ und RADIUS vergleichen

In diesen Abschnitten werden mehrere Funktionen von TACACS+ und RADIUS verglichen.

UDP und TCP

RADIUS verwendet UDP, TACACS+ hingegen TCP. TCP bietet mehrere Vorteile gegenüber UDP. TCP bietet eine verbindungsorientierte Übertragung, während UDP eine bestmögliche Bereitstellung ermöglicht. RADIUS erfordert zusätzliche programmierbare Variablen, z. B. Sendeversuche und -zeitüberschreitungen, um den bestmöglichen Transport auszugleichen. Es fehlt jedoch die integrierte Unterstützung, die ein TCP-Transport bietet:

- Die TCP-Nutzung stellt eine separate Bestätigung bereit, dass innerhalb (ungefähr) einer Netzwerk-Round-Trip-Zeit (RTT) eine Anfrage empfangen wurde, unabhängig davon, wie geladen und verlangsamt der Backend-Authentifizierungsmechanismus (eine TCP-Bestätigung) sein könnte.
- TCP zeigt einen abgestürzten oder nicht ausgeführten Server durch Rücksetzen (RST) an. Wenn Sie langlebige TCP-Verbindungen verwenden, können Sie bestimmen, wann ein Server abstürzt und zum Dienst zurückkehrt. UDP kann den Unterschied zwischen einem Server, der ausgefallen ist, einem langsamen Server und einem nicht vorhandenen Server nicht erkennen.
- Mithilfe von TCP-Keepalives können Serverabstürze außerhalb des Band mit tatsächlichen Anfragen erkannt werden. Verbindungen zu mehreren Servern können gleichzeitig verwaltet werden, und Sie müssen nur Nachrichten an die Server senden, von denen bekannt ist, dass sie betriebsbereit sind.
- TCP ist skalierbarer und passt sich an wachsende und überlastete Netzwerke an.

Paketverschlüsselung

RADIUS verschlüsselt nur das Kennwort im Access-Request-Paket vom Client zum Server. Der Rest des Pakets ist unverschlüsselt. Andere Informationen wie Benutzername, autorisierte Services und Buchhaltung können von Dritten erfasst werden.

TACACS+ verschlüsselt den gesamten Text des Pakets, hinterlässt jedoch einen standardmäßigen TACACS+-Header. Innerhalb des Headers ist ein Feld, das angibt, ob der Text

verschlüsselt ist oder nicht. Für Debugzwecke ist es nützlich, den Hauptteil der Pakete unverschlüsselt zu haben. Während des normalen Betriebs wird der Paketkörper jedoch vollständig verschlüsselt, um eine sicherere Kommunikation zu gewährleisten.

Authentifizierung und Autorisierung

RADIUS kombiniert Authentifizierung und Autorisierung. Die vom RADIUS-Server an den Client gesendeten Access-Accept-Pakete enthalten Autorisierungsinformationen. Dies erschwert die Entkopplung von Authentifizierung und Autorisierung.

TACACS+ verwendet die AAA-Architektur, die AAA trennt. Dies ermöglicht separate Authentifizierungslösungen, die noch TACACS+ für Autorisierung und Abrechnung verwenden können. Mit TACACS+ ist es beispielsweise möglich, die Kerberos-Authentifizierung sowie die TACACS+-Autorisierung und -Abrechnung zu verwenden. Nachdem sich ein NAS-Gerät auf einem Kerberos-Server authentifiziert hat, werden Autorisierungsinformationen von einem TACACS+-Server angefordert, ohne dass eine erneute Authentifizierung erforderlich ist. Das NAS-Gerät informiert den TACACS+-Server, dass er sich erfolgreich auf einem Kerberos-Server authentifiziert hat, und der Server stellt dann Autorisierungsinformationen bereit.

Wenn während einer Sitzung eine zusätzliche Autorisierungsüberprüfung erforderlich ist, überprüft der Zugriffsserver mit einem TACACS+-Server, ob dem Benutzer die Berechtigung zur Verwendung eines bestimmten Befehls erteilt wurde. Dies bietet eine bessere Kontrolle über die Befehle, die auf dem Zugriffsserver ausgeführt werden können, während sie vom Authentifizierungsmechanismus entkoppelt werden.

Unterstützung mehrerer Protokolle

RADIUS unterstützt diese Protokolle nicht:

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

TACACS+ bietet Unterstützung für mehrere Protokolle.

Router-Management

Mit RADIUS können Benutzer nicht steuern, welche Befehle auf einem Router ausgeführt werden können und welche nicht. Daher ist RADIUS nicht so nützlich für die Router-Verwaltung oder so flexibel für Terminaldienste.

TACACS+ bietet zwei Methoden, um die Autorisierung von Routerbefehlen auf Benutzer- oder Gruppenbasis zu steuern. Die erste Methode besteht darin, Befehlen Berechtigungsebenen zuzuweisen und den Router mit dem TACACS+-Server überprüfen zu lassen, ob der Benutzer auf der angegebenen Berechtigungsebene autorisiert ist. Die zweite Methode besteht darin, im TACACS+-Server für jeden Benutzer oder für jede Gruppe explizit die zulässigen Befehle anzugeben.

Interoperabilität

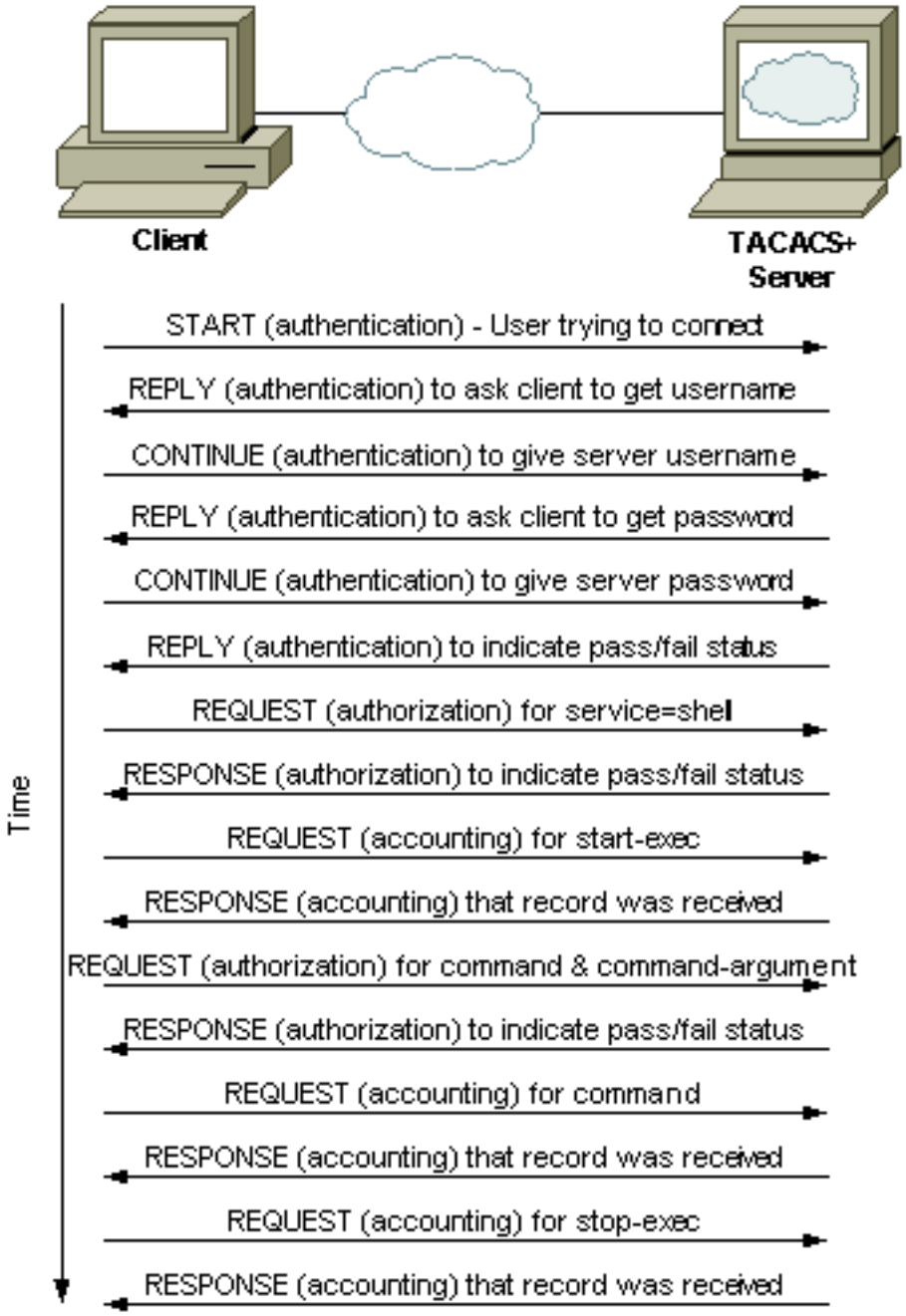
Aufgrund verschiedener Interpretationen der RADIUS Request for Comments (RFCs) kann die Interoperabilität nicht durch die Einhaltung der RADIUS RFCs gewährleistet werden. Obwohl mehrere Anbieter RADIUS-Clients implementieren, bedeutet dies nicht, dass sie interoperabel sind. Cisco implementiert die meisten RADIUS-Attribute und fügt konsistent mehr hinzu. Wenn Kunden nur die RADIUS-Standardattribute in ihren Servern verwenden, können sie mit mehreren Anbietern zusammenarbeiten, sofern diese Anbieter dieselben Attribute implementieren. Viele Anbieter implementieren jedoch Erweiterungen, die proprietäre Attribute darstellen. Wenn ein Kunde eines dieser anbieterspezifischen erweiterten Attribute verwendet, ist Interoperabilität nicht möglich.

Datenverkehr

Aufgrund der zuvor genannten Unterschiede zwischen TACACS+ und RADIUS ist die zwischen Client und Server generierte Datenverkehrsmenge unterschiedlich. In diesen Beispielen wird der Datenverkehr zwischen Client und Server für TACACS+ und RADIUS veranschaulicht, wenn dieser für die Router-Verwaltung mit Authentifizierung, Exec-Autorisierung, Befehlsautorisierung (was RADIUS nicht kann), exec Accounting und Befehlsabrechnung (was RADIUS nicht kann) verwendet wird.

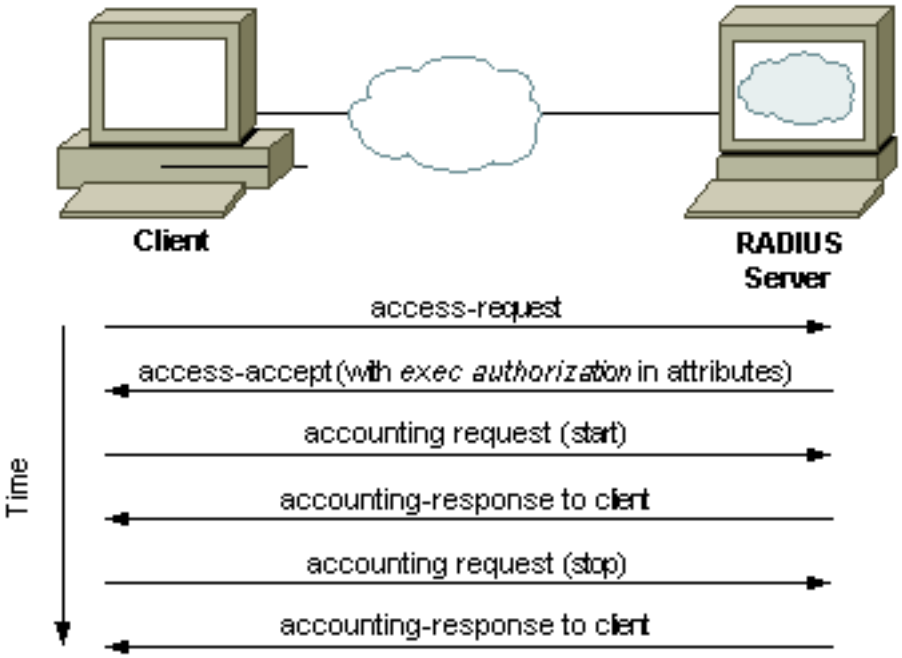
Beispiel für TACACS+-Datenverkehr

In diesem Beispiel wird davon ausgegangen, dass Anmeldenauthentifizierung, Exec-Autorisierung, Befehlsautorisierung, Start-Stopp-exec-Accounting und Befehlsabrechnung mit TACACS+ implementiert sind, wenn ein Benutzer Telnet zu einem Router führt, einen Befehl ausführt und den Router verlässt:



Beispiel für RADIUS-Datenverkehr

In diesem Beispiel wird davon ausgegangen, dass die Anmeldeauthentifizierung, die exec-Autorisierung und die Start-Stopp-exec-Accounting mit RADIUS implementiert werden, wenn ein Benutzer Telnet zu einem Router führt, einen Befehl ausführt und den Router verlässt (andere Management-Services sind nicht verfügbar):



Geräteunterstützung

In dieser Tabelle sind die Unterstützung von TACACS+ und RADIUS AAA nach Gerätetyp für ausgewählte Plattformen aufgeführt. Dazu gehört auch die Softwareversion, in der die Unterstützung hinzugefügt wurde. Weitere Informationen finden Sie in den Versionshinweisen für Produkte, wenn Ihr Produkt nicht in dieser Liste aufgeführt ist.

Cisco Gerät	TACACS+-Authentifizierung	TACACS+-Autorisierung	TACACS+ Accounting	RADIUS-Authentifizierung	RADIUS-Autorisierung	RADIUS Accounting
Cisco Aironet[1]	12.2(4)JA	12.2(4)JA	12.2(4)JA	alle Access Points	alle Access Points	alle Access Points
Cisco IOS-Software[2]	10,33	10,33	10,33[3]	11.1.1	11.1.1[4]	11.1.1[5]
Cisco Cache-Engine	—	—	—	1,5	1,5[6]	—
Cisc	2,2	5,4/1	5,4/	5,1	5,4,1[4]	5,4,

o Catalyst Switches			1			1[5]
Cisco CSS 11000 Content Services-Switch	5,03	5,03	5,03	5,0	5,0[4]	—
Cisco CSS 11500 Content Services-Switch	5,20	5,20	5,20	5,20	5,20[4]	—
Cisco PIX-Firewall	4,0	4,0[7]	4,2[8,5]	4,0	5,2[7]	4,2[8,5]
Cisco Catalyst Switches der Serien 1900/2820	8.x Enterprise[9]	—	—	—	—	—
Cisco Catalyst Switches der Serie	11.2.(8)SA6[10]	11.2.(8)SA6[10]	11.2.(8)SA6[10]	12.0(5)WC5[11]	12.0(5)WC5[11, 4]	12.0(5)WC5[11, 5]

2900 XL/3500XL						
Cisco VPN 3000 Concentrator [6]	3,0	3,0	—	2,0[12]	2,0	2,0[12]
Cisco VPN 5000 Concentrator	—	—	—	5,2 X[12]	5,2 X[12]	5,2 X[12]

Tabelle Hinweise

1. Terminierung nur von Wireless-Clients, nicht von Management-Datenverkehr in anderen Versionen als der Cisco IOS Software, Version 12.2(4)JA oder höher. In der Cisco IOS-Softwareversion 12.2.(4)JA oder höher ist die Authentifizierung sowohl für die Terminierung von Wireless-Clients als auch für den Verwaltungsdatenverkehr möglich.
2. Plattformunterstützung innerhalb der Cisco IOS-Software finden Sie im Feature Navigator (jetzt durch Software Advisor veraltet (nur registrierte Kunden).
3. Die Befehlsabrechnung wird erst in Version 11.1.6.3 der Cisco IOS-Software implementiert.
4. Keine Befehlsautorisierung.
5. Keine Befehlsabrechnung.
6. Nur URL-Blockierung, nicht administrativer Datenverkehr.
7. Autorisierung für Nicht-VPN-Datenverkehr über den PIX.**Hinweis:** Version 5.2 - Zugriffslistenunterstützung für Access Control List (ACL) RADIUS Vendor-Specific Attribute (VSA) oder TACACS+-Autorisierung für VPN-Datenverkehr mit PIX Version 6.1 - Unterstützung für ACL RADIUS-Attribut 11-Autorisierung für VPN-Datenverkehr mit PIX Version 6.2.2 - Unterstützung für herunterladbare ACLs mit RADIUS-Autorisierung für VPN-Datenverkehr PIX Version 6.2 - Unterstützung für die Autorisierung von PIX-Management-Datenverkehr über TACACS+.
8. Abrechnung für Nicht-VPN-Datenverkehr nur über den PIX, nicht für Management-Datenverkehr**Hinweis:** Version 5.2 - Unterstützung für die Abrechnung von VPN-Client-TCP-Paketen über PIX.
9. Nur Unternehmenssoftware.
10. 8 Mio Flash für Image erforderlich.
11. Nur VPN-Terminierung.

Zugehörige Informationen

- RADIUS-Support-Seite

- TACACS+ in der IOS-Dokumentation
- Support-Seite für TACACS/TACACS+
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems