Vergelijking van TACACS+ en RADIUS

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Conventies
RADIUS-achtergrond
Clientmodel/servermodel
Netwerkbeveiliging
Flexibele verificatiemechanismen
Beschikbaarheid servercode
Vergelijk TACACS+ en RADIUS
UDP en TCP
Packet-encryptie
Verificatie en autorisatie
Ondersteuning van Multiprotocol
Routerbeheer
Interoperabiliteit
verkeer
Apparaatondersteuning
Gerelateerde informatie

Inleiding

Twee prominente veiligheidsprotocollen die gebruikt worden om de toegang tot netwerken te controleren zijn Cisco TACACS+ en RADIUS. De RADIUS-specificatie wordt beschreven in RFC 2865 , die RFC 2138 vervalt . Cisco is gecommitteerd aan het ondersteunen van beide protocollen met het beste van klasse aanbiedingen. Het is niet de bedoeling van Cisco om met RADIUS te concurreren of gebruikers te beïnvloeden om TACACS+ te gebruiken. U dient de oplossing te kiezen die het best aan uw behoeften voldoet. In dit document worden de verschillen tussen TACACS+ en RADIUS besproken, zodat u een gefundeerde keuze kunt maken.

Cisco heeft het RADIUS-protocol ondersteund sinds Cisco IOS®-softwarerelease 11.1 in februari 1996. Cisco blijft de RADIUS-client verbeteren met nieuwe functies en functies, waarbij RADIUS als standaard wordt ondersteund.

Cisco heeft RADIUS ernstig geëvalueerd als een beveiligingsprotocol voordat het TACACS+ ontwikkelde. In het TACACS+-protocol zijn veel elementen opgenomen om te voorzien in de behoeften van de groeiende veiligheidsmarkt. Het protocol was ontworpen om te schalen terwijl netwerken groeien en om zich aan nieuwe security technologie aan te passen naarmate de markt zich ontwikkelt. De onderliggende architectuur van het TACACS+-protocol vult de onafhankelijke

authenticatie-, autorisatie- en boekhoudarchitectuur (AAA) aan.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

RADIUS-achtergrond

RADIUS is een toegangsserver die AAA-protocol gebruikt. Het is een systeem van gedistribueerde veiligheid dat de toegang op afstand tot netwerken en netwerkdiensten waarborgt tegen toegang door onbevoegden. RADIUS bestaat uit drie componenten:

- Een protocol met een frame-indeling dat User Datagram Protocol (UDP)/IP gebruikt.
- Een server.
- Een cliënt.

De server draait op een centrale computer, gewoonlijk op de plaats van de klant, terwijl de klanten in de inbeltoegangsservers wonen en door het netwerk kunnen worden verdeeld. Cisco heeft de RADIUS-client opgenomen in Cisco IOS-softwarerelease 11.1 en hoger en andere apparaatsoftware.

Clientmodel/servermodel

Een Network Access Server (NAS) werkt als een client voor RADIUS. De klant is verantwoordelijk voor het doorgeven van gebruikersinformatie aan aangewezen RADIUS-servers en handelt vervolgens op de respons die wordt teruggegeven. RADIUS-servers zijn verantwoordelijk voor het ontvangen van gebruikersverbindingsverzoeken, het voor zich houden van de gebruiker en het retourneren van alle configuratieinformatie die nodig is voor de client om de service aan de gebruiker te leveren. De RADIUS-servers kunnen als proxy-clients fungeren voor andere soorten authenticatieservers.

Netwerkbeveiliging

De transacties tussen de client en de RADIUS-server worden geauthentiseerd door het gebruik van een gedeeld geheim dat nooit via het netwerk wordt verstuurd. Bovendien worden alle wachtwoorden van de gebruiker versleuteld tussen de client en de RADIUS-server. Dit heft de mogelijkheid op dat iemand die rondkijkt op een onbeveiligd netwerk het wachtwoord van een gebruiker kan bepalen.

Flexibele verificatiemechanismen

De RADIUS-server ondersteunt een verscheidenheid aan methoden om een gebruiker te authentiseren. Wanneer de gebruikersnaam en het oorspronkelijke wachtwoord door de gebruiker zijn opgegeven, kan deze ondersteuning bieden voor PPP, Password Authentication Protocol (PAP) of Challenge Handshake Authentication Protocol (CHAP), UNIX-inloggen en andere verificatiemechanismen.

Beschikbaarheid servercode

Er is een aantal distributies van servercodes die commercieel en vrij beschikbaar zijn. Cisco-servers omvatten Cisco Secure ACS voor Windows, Cisco Secure ACS voor UNIX en Cisco Access Registrar.

Vergelijk TACACS+ en RADIUS

Deze secties vergelijken verschillende eigenschappen van TACACS+ en RADIUS.

UDP en TCP

RADIUS gebruikt UDP terwijl TACACS+ TCP gebruikt. TCP biedt verschillende voordelen ten opzichte van UDP. TCP biedt een op verbinding gericht transport aan, terwijl UDP de best-inspanning levert. RADIUS vereist extra programmeerbare variabelen zoals het opnieuw verzenden van pogingen en time-outs om het best-inspanningstransport te compenseren, maar het ontbreekt het niveau van ingebouwde ondersteuning dat een TCP-transport biedt:

- TCP-gebruik biedt een afzonderlijke erkenning dat een verzoek is ontvangen, binnen (ongeveer) een netwerk round-trip tijd (RTT), ongeacht hoe geladen en vertragen het backend-authenticatiemechanisme (een TCP-erkenning) zou kunnen zijn.
- TCP biedt onmiddellijke indicatie van een crashed, of geen actieve server door een reset (RST). U kunt bepalen wanneer een server crasht en terugkeert naar service als u langlevende TCP verbindingen gebruikt. UDP kan het verschil niet zien tussen een lagere server, een vertraagde server en een niet-bestaande server.
- Met TCP-overlevingskansen kunnen servercrashes worden gedetecteerd in out-of-band met werkelijke verzoeken. Aansluitingen op meerdere servers kunnen tegelijkertijd worden onderhouden en u hoeft alleen berichten naar de servers te sturen waarvan bekend is dat ze actief zijn.
- TCP is schaalbaarder en past zich aan aan groeiende, zowel als verstopte netwerken.

Packet-encryptie

RADIUS versleutelt alleen het wachtwoord in het toegangspakket, van de client tot de server. De rest van het pakket is niet versleuteld. Andere informatie, zoals gebruikersnaam, geautoriseerde services en accounting, kan door een derde partij worden opgenomen.

TACACS+ versleutelt de gehele inhoud van het pakket maar geeft een standaard TACACS+ kop. Binnen de header is een veld dat aangeeft of het lichaam versleuteld is of niet. Voor het debuggen is het handig om de inhoud van de pakketten niet versleuteld te hebben. Tijdens normaal gebruik wordt de inhoud van het pakket echter volledig versleuteld voor beveiligde communicatie.

Verificatie en autorisatie

RADIUS combineert authenticatie en autorisatie. De toegang-accepteer pakketten die door de RADIUS-server naar de client worden verzonden informatie over de vergunning bevatten. Dit maakt het moeilijk om authenticatie en autorisatie los te koppelen.

TACACS+ gebruikt de AAA-architectuur, die AAA scheidt. Dit maakt afzonderlijke authenticatieoplossingen mogelijk die TACACS+ nog kunnen gebruiken voor autorisatie en boekhouding. Met TACACS+ kan bijvoorbeeld gebruik worden gemaakt van Kerberos-authenticatie en TACACS+-toestemming en accounting. Nadat NAS op een Kerberos-server authentiek verklaarde, verzoekt het om vergunninginformatie van een TACACS+ server zonder opnieuw te hoeven authentiseren. NAS informeert de TACACS+ server dat het met succes op een Kerberos server geauthentiseerd is en de server dan verstrekt machtigingsinformatie.

Tijdens een sessie, als extra autorisatie controle nodig is, controleert de toegangsserver met een TACACS+ server om te bepalen of de gebruiker toestemming wordt verleend om een bepaalde opdracht te gebruiken. Dit zorgt voor een grotere controle over de opdrachten die op de toegangsserver kunnen worden uitgevoerd terwijl de verbinding met het verificatiemechanisme wordt losgemaakt.

Ondersteuning van Multiprotocol

RADIUS ondersteunt deze protocollen niet:

- AppleTalk Remote Access-protocol (ARA)
- NetVOS Frame Protocol-beheerprotocol
- Novell Asynchronous Services Interface (NASI)
- X.25-PAD-verbinding

TACACS+ biedt ondersteuning voor meerdere protocollen.

Routerbeheer

RADIUS laat gebruikers niet toe om te controleren welke opdrachten op een router kunnen worden uitgevoerd en welke niet. Daarom is RADIUS niet zo nuttig voor routerbeheer of zo flexibel voor terminalservices.

TACACS+ biedt twee methoden om de autorisatie van routeropdrachten op een per-gebruiker- of per-groep-basis te controleren. De eerste methode is om prioriteitsniveaus aan opdrachten toe te wijzen en de router te laten controleren met de TACACS+ server of de gebruiker al dan niet is geautoriseerd op het gespecificeerde voorkeursniveau. De tweede methode is om expliciet, op een per-gebruiker of per-groep-basis, in de TACACS+ server de toegestane opdrachten te specificeren.

Interoperabiliteit

Wegens verschillende interpretaties van het RADIUS-verzoek om opmerkingen (RFC's) biedt de naleving van de RADIUS-RFC's geen garantie voor interoperabiliteit. Hoewel meerdere verkopers RADIUS-klanten implementeren, betekent dit niet dat ze interoperabel zijn. Cisco implementeert de meeste RADIUS-kenmerken en voegt consequent meer toe. Als klanten alleen de standaard RADIUS eigenschappen in hun servers gebruiken, kunnen ze tussen meerdere verkopers

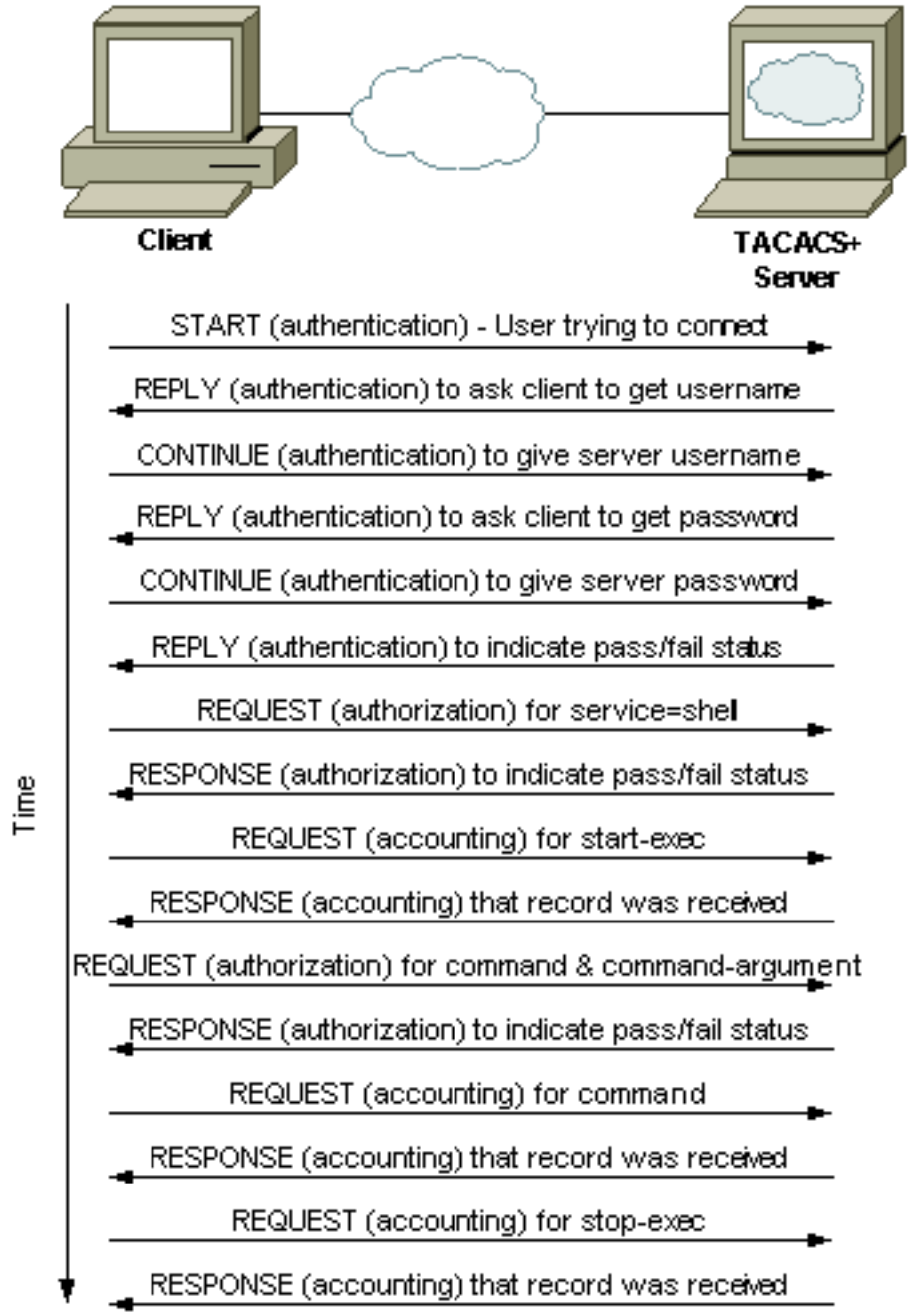
samenwerken zolang deze verkopers dezelfde eigenschappen implementeren. Veel verkopers passen echter uitbreidingen toe die eigen kenmerken zijn. Als een klant een van deze leverancierspecifieke uitgebreide eigenschappen gebruikt, is interoperabiliteit niet mogelijk.

verkeer

Vanwege de eerder genoemde verschillen tussen TACACS+ en RADIUS verschilt de hoeveelheid verkeer die tussen de client en de server wordt gegenereerd. Deze voorbeelden illustreren het verkeer tussen de client en de server voor TACACS+ en RADIUS wanneer gebruikt voor routerbeheer met verificatie, exec autorisatie, commandoautorisatie (wat RADIUS niet kan doen), exec accounting en commando accounting (wat RADIUS niet kan doen).

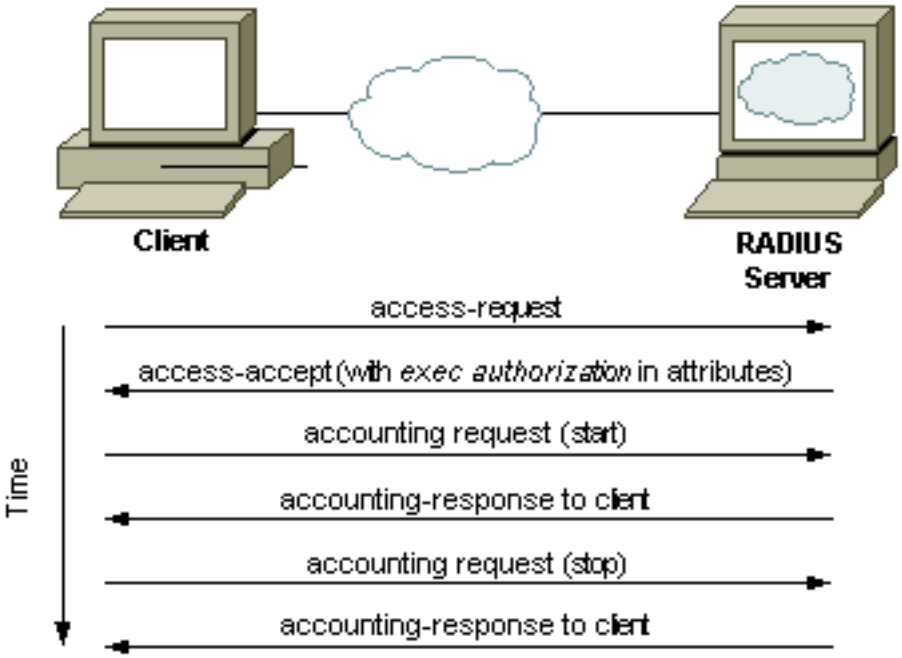
Voorbeeld TACACS+ verkeer

Dit voorbeeld veronderstelt inlogverificatie, exec autorisatie, opdracht autorisatie, start-stop exec accounting en commandoaccounting wordt geïmplementeerd met TACACS+ wanneer een gebruiker Telnet naar een router, een opdracht uitvoert en de router verlaat:



RADIUS-verkeersvoorbeeld

Dit voorbeeld gaat uit van inlogverificatie, exec-autorisatie en start-stop-exec accounting wordt uitgevoerd met RADIUS wanneer een gebruiker Telnetten aan een router uitvoert, een opdracht uitvoert en de router (andere beheerservices zijn niet beschikbaar) verlaat:



Apparaatondersteuning

Deze tabel toont ondersteuning van TACACS+ en RADIUS AAA per apparaattype voor geselecteerde platforms. Hieronder valt de softwareversie waarin de ondersteuning is toegevoegd. Als uw product niet in deze lijst staat, raadpleegt u de opmerkingen bij de productrelease voor meer informatie.

Cisco-apparaat	Verificatie TACACS+	Toestemming voor TACACS+	Boekhouding TACACS+	RADIUS-verificatie	RADIUS-vergunning	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 release[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 9300 switches	2.2	5.4.1	5.4.1	5.1	5.4.14	5.4.15
Cisco CSS 1000	5.03	5.03	5.03	5.0	5.04	—

content services Switch						
Cisco CSS 1500 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 ondernemingen[9]	—	—	—	—	—
Cisco Catalyst 2900XL/3500XL switches	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]
Cisco VPN 3000 Concentrator [6]	3.0	3.0	—	2.012	2.0	2.012
Cisco VPN 5000 Concentrator	—	—	—	5,2 x[12]	5,2 x[12]	5,2 x[12]

Tabelopmerkingen

1. Beëindiging van uitsluitend draadloze klanten, geen beheerverkeer in versies anders dan Cisco IOS-softwarerelease 12.2(4)JA of hoger. In Cisco IOS-softwarerelease 12.2(4)JA of hoger is verificatie voor zowel beëindiging van draadloze klanten als beheerverkeer mogelijk.
2. Controleer functiesnavigator (nu verouderd door Softwareadviseur (alleen geregistreerde klanten) op platform ondersteuning binnen Cisco IOS-software.
3. Opdracht accounting wordt niet uitgevoerd tot Cisco IOS-softwarerelease 11.1.6.3.
4. Geen commando toestemming.
5. Geen opdrachtaccounting.
6. Alleen URL-blokkering, geen beheerverkeer.
7. Toestemming voor niet-VPN-verkeer door de PIX.**Opmerking:** release 5.2 - Ondersteuning voor toegangslijst voor toegangscontrolelijst (ACL) RADIUS-leverancierspecifieke kenmerk (VSA) of TACACS+ vergunning voor VPN-verkeer die eindigt op PIX release 6.1 -

ondersteuning voor ACL RADIUS-kenmerk 11 autorisatie voor VPN-verkeer die eindigt op PIX release 6.2.2 - ondersteuning voor RADIUS-toegangsvergunning voor VPN-verkeer die eindigt op PIX release 6.2 steun voor toestemming voor het verkeer van PIX-beheer door middel van TACACS+.

8. accounting voor niet-VPN verkeer door alleen PIX, niet beheerverkeer.**Opmerking:** release 5.2 - ondersteuning voor accounting voor VPN-client-TCP-pakketten via de PIX.
9. Alleen ondernemingssoftware
10. Heeft 8M Flash nodig voor beeld.
11. Alleen VPN-beëindiging.

Gerelateerde informatie

- RADIUS-ondersteuningspagina
- TACACS+ in IOS-documentatie
- Ondersteuningspagina voor TACACS/TACACS+
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems