TACACS+ 및 RADIUS 비교

목차

소개

네트워크에 대한 액세스를 제어하는 데 사용되는 두 가지 주요 보안 프로토콜은 Cisco TACACS+와 RADIUS입니다.RADIUS 사양은 RFC 2138 을 사용하지 않는 RFC 2865에 설명되어 있습니다 .Cisco는 동급 최고의 제품과 함께 두 프로토콜을 모두 지원하기 위해 최선을 다하고 있습니다 .Cisco가 RADIUS와 경쟁하거나 사용자가 TACACS+를 사용하도록 영향력을 행사하려는 의도는 아닙니다.필요에 가장 적합한 솔루션을 선택해야 합니다.이 문서에서는 TACACS+와 RADIUS의 차이점에 대해 설명하며, 이를 통해 정보를 기반으로 선택할 수 있습니다.

Cisco는 1996년 2월 Cisco IOS® Software 릴리스 11.1부터 RADIUS 프로토콜을 지원합니다 .Cisco는 RADIUS를 표준으로 지원하면서 새로운 기능 및 기능으로 RADIUS 클라이언트를 지속적으로 개선합니다.

Cisco는 TACACS+를 개발하기 전에 RADIUS를 보안 프로토콜로 진지하게 평가했습니다.증가하는 보안 시장의 요구 사항을 충족하기 위해 많은 기능이 TACACS+ 프로토콜에 포함되어 있었습니다 .이 프로토콜은 네트워크가 확장됨에 따라 확장되고 시장이 성숙함에 따라 새로운 보안 기술에 적응하도록 설계되었습니다.TACACS+ 프로토콜의 기본 아키텍처는 AAA(Independent Authentication, Authorization, and Accounting) 아키텍처를 보완합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

RADIUS 배경

RADIUS는 AAA 프로토콜을 사용하는 액세스 서버입니다.네트워크 및 네트워크 서비스에 대한 원격 액세스를 무단 액세스로부터 보호하는 분산 보안 시스템입니다.RADIUS는 세 가지 구성 요소로 구성됩니다.

- UDP(User Datagram Protocol)/IP를 사용하는 프레임 형식의 프로토콜.
- 서버.
- 클라이언트.

서버는 일반적으로 고객 사이트에서 중앙 컴퓨터에서 실행되며 클라이언트는 전화 접속 액세스 서버에 상주하며 네트워크 전체에 분산될 수 있습니다.Cisco는 RADIUS 클라이언트를 Cisco IOS Software 릴리스 11.1 이상 및 기타 장치 소프트웨어에 통합했습니다.

클라이언트/서버 모델

NAS(Network Access Server)는 RADIUS의 클라이언트로 작동합니다.클라이언트는 지정된 RADIUS 서버에 사용자 정보를 전달한 다음 반환되는 응답에 대해 작업을 수행합니다.RADIUS 서버는 사용자 연결 요청을 수신하고 사용자를 인증하며 클라이언트가 사용자에게 서비스를 제공하는 데 필요한 모든 구성 정보를 반환하는 역할을 합니다.RADIUS 서버는 다른 종류의 인증 서버에 대한 프록시 클라이언트 역할을 할 수 있습니다.

네트워크 보안

클라이언트와 RADIUS 서버 간의 트랜잭션은 네트워크를 통해 전송되지 않는 공유 암호를 사용하여 인증됩니다.또한 모든 사용자 비밀번호는 클라이언트와 RADIUS 서버 간에 암호화됩니다.이렇게 하면 안전하지 않은 네트워크에서 사용자가 사용자의 암호를 확인할 수 있는 가능성이 사라집니다.

유연한 인증 메커니즘

RADIUS 서버는 사용자를 인증하는 다양한 방법을 지원합니다.사용자가 제공한 사용자 이름 및 원래 비밀번호와 함께 제공된 경우 PPP, PAP(Password Authentication Protocol) 또는 CHAP(Challenge Handshake Authentication Protocol), UNIX 로그인 및 기타 인증 메커니즘을 지원할 수 있습니다.

서버 코드 가용성

상업적이고 자유롭게 사용할 수 있는 서버 코드 분배가 많습니다.Cisco 서버에는 Windows용 Cisco Secure ACS, UNIX용 Cisco Secure ACS 및 Cisco Access Registrar가 포함됩니다.

TACACS+ 및 RADIUS 비교

이 섹션에서는 TACACS+ 및 RADIUS의 여러 기능을 비교합니다.

UDP 및 TCP

RADIUS는 UDP를 사용하는 반면 TACACS+는 TCP를 사용합니다.TCP는 UDP보다 몇 가지 이점을 제공합니다.TCP는 연결 지향 전송을 제공하는 반면 UDP는 최선의 노력을 제공합니다 .RADIUS는 BE(Re-transmit Attempts), 시간 초과 등 프로그래밍 가능한 추가 변수가 필요하므로 TCP 전송에서 제공하는 기본 제공 지원 수준이 부족합니다.

- TCP 사용법은 백엔드 인증 메커니즘(TCP 확인 응답)의 로드 및 속도 저하 여부와 상관없이 RTT(Network Round-Trip Time) 내에서 요청이 수신되었다는 별도의 승인을 제공합니다.
- TCP는 RST(Reset)에 의해 서버가 손상되었거나 실행되고 있지 않음을 즉시 나타냅니다. 오래 지속되는 TCP 연결을 사용하는 경우 서버가 crash하고 서비스로 반환되는 시간을 확인할 수 있습니다.UDP는 다운된 서버, 느린 서버 및 존재하지 않는 서버 간의 차이를 구별할 수 없습니다.
- TCP keepalive를 사용하면 실제 요청과 함께 서버 충돌을 대역 외로 탐지할 수 있습니다.여러 서버에 대한 연결은 동시에 유지 관리할 수 있으며, 실행 중인 것으로 알려진 서버로 메시지를 전송하기만 하면 됩니다.
- TCP는 확장성이 더 뛰어나고 증가하는 네트워크와 혼잡한 네트워크에 적응합니다.

패킷 암호화

RADIUS는 클라이언트에서 서버로 액세스 요청 패킷의 비밀번호만 암호화합니다.패킷의 나머지는 암호화되지 않습니다.사용자 이름, 공인 서비스, 회계 등의 기타 정보는 서드파티에서 캡처할 수 있습니다.

TACACS+는 패킷의 전체 본문을 암호화하지만 표준 TACACS+ 헤더는 남겨둡니다.헤더 안에는 본문이 암호화되었는지 여부를 나타내는 필드가 있습니다.디버깅을 위해 패킷의 본문을 암호화하지 않은 상태로 두는 것이 좋습니다.그러나 정상적인 작동 중에 패킷의 본문은 보다 안전한 통신을 위해 완전히 암호화됩니다.

인증 및 권한 부여

RADIUS는 인증 및 권한 부여를 결합합니다.RADIUS 서버가 클라이언트로 보낸 액세스 수락 패킷에는 권한 부여 정보가 포함됩니다.따라서 인증 및 권한 부여를 분리하기가 어렵습니다.

TACACS+는 AAA를 분리하는 AAA 아키텍처를 사용합니다.이렇게 하면 권한 부여 및 어카운팅에 TACACS+를 계속 사용할 수 있는 별도의 인증 솔루션이 허용됩니다.예를 들어, TACACS+에서는 Kerberos 인증 및 TACACS+ 권한 부여 및 계정 관리를 사용할 수 있습니다.NAS는 Kerberos 서버에서 인증한 후 다시 인증할 필요 없이 TACACS+ 서버에서 권한 부여 정보를 요청합니다.NAS는 TACACS+ 서버에 Kerberos 서버에서 성공적으로 인증되었음을 알리고 서버는 권한 부여 정보를 제공합니다.

세션 중에 추가 권한 확인이 필요한 경우 액세스 서버는 TACACS+ 서버와 함께 사용자에게 특정 명령을 사용할 수 있는 권한이 부여되었는지 확인합니다.이렇게 하면 인증 메커니즘과 분리되는 동안 액세스 서버에서 실행할 수 있는 명령을 더 효과적으로 제어할 수 있습니다.

다중 프로토콜 지원

RADIUS는 다음 프로토콜을 지원하지 않습니다.

- AppleTalk ARA(Remote Access) 프로토콜
- NetBIOS 프레임 프로토콜 제어 프로토콜
- Novell NASI(Asynchronous Services Interface)
- X.25 PAD 연결

TACACS+는 다중 프로토콜 지원을 제공합니다.

라우터 관리

RADIUS는 사용자가 어떤 명령을 라우터에서 실행할 수 있고 어떤 명령을 실행할 수 있는지를 제어할 수 없습니다.따라서 RADIUS는 라우터 관리에 유용하지 않거나 터미널 서비스에 유연하지 않습니다.

TACACS+는 사용자별 또는 그룹별로 라우터 명령의 권한 부여를 제어하는 두 가지 방법을 제공합니다.첫 번째 방법은 명령에 권한 수준을 할당하고 라우터가 TACACS+ 서버에서 사용자가 지정된 권한 레벨에서 권한이 부여되었는지 여부를 확인하는 것입니다.두 번째 방법은 TACACS+ 서버에서 사용자 또는 그룹별로 허용되는 명령을 명시적으로 지정하는 것입니다.

상호 운용성

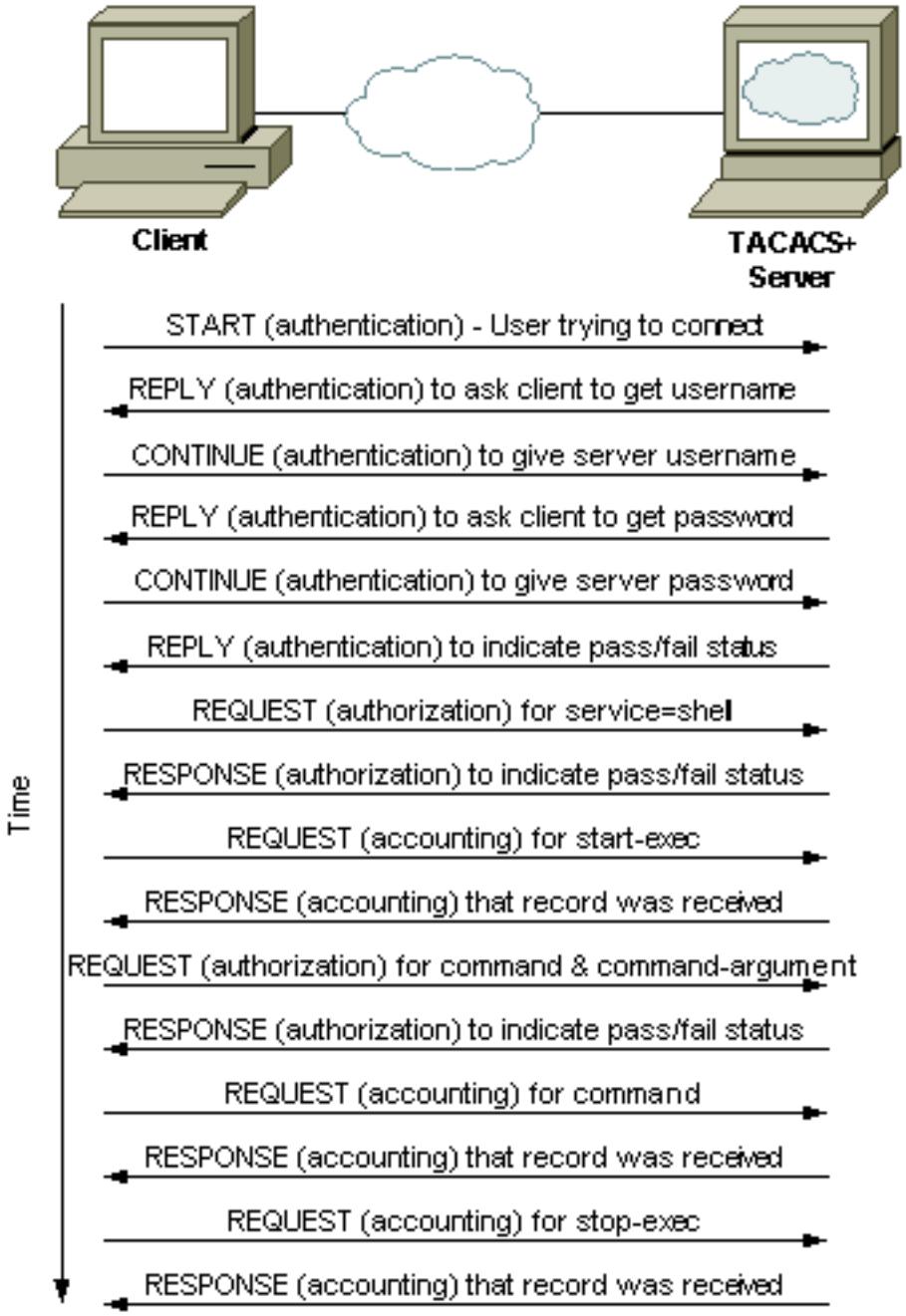
RADIUS RFC(Request for Comments)에 대한 다양한 해석으로 인해 RADIUS RFC를 준수하는 것은 상호운용성을 보장하지 않습니다.여러 공급업체가 RADIUS 클라이언트를 구현하더라도 상호 운용이 가능하다는 의미는 아닙니다.Cisco는 대부분의 RADIUS 특성을 구현하고 더 지속적으로 추가합니다.고객이 서버에서 표준 RADIUS 특성만 사용하는 경우, 이러한 공급업체가 동일한 특성을 구현하는 한 여러 벤더 간에 상호 작용할 수 있습니다.그러나 많은 공급업체가 독점적인 특성을 가진 확장을 구현하고 있습니다.고객이 공급업체별 확장 특성 중 하나를 사용하는 경우 상호 운용성이 불가능합니다.

트래픽

앞서 언급한 TACACS+ 및 RADIUS 간 차이 때문에 클라이언트와 서버 간에 생성된 트래픽의 양이 달라집니다.다음 예에서는 인증, exec authorization, 명령 권한 부여(RADIUS에서 할 수 없는 권한 부여), exec 계정 관리 및 명령 계정 관리(RADIUS에서 할 수 없는 명령 계정 관리)를 사용하는 라우터 관리에 사용되는 경우 TACACS+ 및 RADIUS용 클라이언트와 서버 간의 트래픽을 보여줍니다.

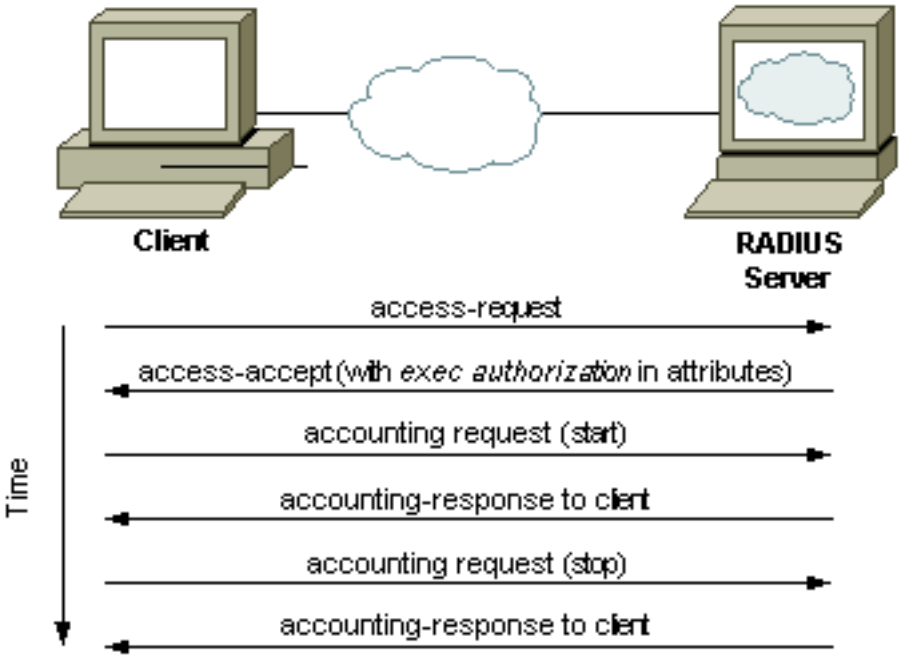
TACACS+ 트래픽 예

이 예에서는 사용자가 라우터에 텔넷하고, 명령을 수행하고, 라우터를 종료할 때 로그인 인증, exec 권한 부여, 명령 권한 부여, start-stop exec accounting 및 명령 어카운팅이 TACACS+로 구현된다고 가정합니다.



RADIUS 트래픽 예

이 예에서는 사용자가 라우터에 텔넷하고 명령을 수행하고 라우터를 종료할 때 로그인 인증, exec 권한 부여 및 start-stop exec 어카운팅이 RADIUS와 함께 구현된다고 가정합니다(다른 관리 서비스는 사용할 수 없음).



장치 지원

이 표에는 선택한 플랫폼에 대한 디바이스 유형별로 TACACS+ 및 RADIUS AAA 지원이 나열되어 있습니다.여기에는 지원이 추가된 소프트웨어 버전이 포함됩니다.제품이 이 목록에 없는 경우 제품 릴리스 정보를 참조하십시오.

Cisco 장치	TACACS+ 인증	TACACS+ 권한 부여	TACACS+ 계정 관리	RADIUS 인증	RADIUS 권한 부여	RADIUS 계정 관리
Cisco Aironet[1]	12.2(4)JA	12.2(4)JA	12.2(4)JA	모든 액세스 포인트	모든 액세스 포인트	모든 액세스 포인트
Cisco IOS Software[2]	10.33	10.33	10.333	11.1.1	11.1.14	11.1.15
Cisco 캐시 엔진	—	—	—	1.5	1.56	—
Cisco Catalyst 스위치	2.2	5.4.1	5.4.1	5.1	5.4.14	5.4.15
Cisco CSS 11000 Content Services Switch	5.03	5.03	5.03	5.0	5.04	—
Cisco CSS 11500 Content	5.20	5.20	5.20	5.20	5.204	—

Services Switch						
Cisco PIX 방화벽	4.0	4.07	4.28,5	4.0	5.27	4.28,5
Cisco Catalyst 1900/2820 스위치	8.x enterprise[9]	—	—	—	—	—
Cisco Catalyst 2900XL/3500XL 스위치	11.2.(8)SA6[10]	11.2.(8)SA6[10]	11.2.(8)SA6[10]	12.0(5)WC5[1,11]	12.0(5)WC5[1,4]	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	—	—	—	5.2X[12]	5.2X[12]	5.2X[12]

표 노트

1. Cisco IOS Software Release 12.2(4)JA 이상 버전에서는 관리 트래픽이 아니라 무선 클라이언트만 종료합니다.Cisco IOS Software 릴리스 12.2.(4)JA 이상에서는 무선 클라이언트 종료 및 관리 트래픽 모두에 대한 인증이 가능합니다.
2. Feature Navigator(이제 Software Advisor(등록된 고객만 해당)에서 Cisco IOS 소프트웨어 내의 플랫폼 지원을 확인합니다.
3. 명령 어카운팅은 Cisco IOS Software Release 11.1.6.3까지 구현되지 않습니다.
4. 명령 권한 부여가 없습니다.
5. 명령 어카운팅이 없습니다.
6. 관리 트래픽이 아닌 URL 차단만.
7. PIX를 통한 비 VPN 트래픽에 대한 권한 부여**참고:** 릴리스 5.2 - PIX 릴리스 6.1에서 종료되는 VPN 트래픽에 대한 ACL(Access Control List) RADIUS VSA(Vendor-Specific Attribute) 또는 TACACS+ 권한 부여에 대한 액세스 목록 지원 - PIX 릴리스 6.2.2에서 종료되는 VPN 트래픽에 대한 ACL 특성 11 지원 - PIX 릴리스에서 VPN 트래픽을 위한 RADIUS 권한 부여를 사용하는 ACL 지원 2.2 - TACACS+를 통한 PIX 관리 트래픽에 대한 권한 부여 지원
8. 관리 트래픽이 아니라 PIX를 통한 비 VPN 트래픽에 대한 어카운팅.**참고:** 릴리스 5.2 - PIX를 통한 VPN 클라이언트 TCP 패킷 어카운팅 지원.
9. 엔터프라이즈 소프트웨어만 해당됩니다.
10. 이미지에 8M 플래시가 필요합니다.
11. VPN 종료만.

관련 정보

- RADIUS 지원 페이지
- IOS 설명서의 TACACS+
- TACACS/TACACS+ 지원 페이지
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems