Compare TACACS + and RADIUS

Contents

Introduction

This document describes and compares the two prominent security protocols used to control access into networks, Cisco TACACS+ and Cisco RADIUS.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to Cisco Technical Tips and Format.

Background Information

The RADIUS specification is described in RFC 2865 , which obsoletes RFC 2138 . Cisco supports both protocols. It is not the intention of Cisco to compete with RADIUS or influence users to use TACACS+. You must choose the solution that best meets your needs. This document discusses the differences between TACACS+ and RADIUS, so that you can make an informed choice.

Cisco has supported the RADIUS protocol since Cisco IOS® Software Release 11.1 in February 1996. Cisco continues support RADIUS and to enhance it with new features and capabilities.

Cisco seriously evaluated RADIUS as a security protocol before it developed TACACS+. Many features were included in the TACACS+ protocol to meet new security market demands. The protocol was designed to scale as networks grow, and to adapt to new security technology as the market matures. The underlying architecture of the TACACS+ protocol complements the independent authentication, authorization, and accounting (AAA) architecture.

RADIUS Background

RADIUS is an access server that uses AAA protocol. It is a system of distributed security that secures remote access to networks and network services against unauthorized access. RADIUS comprises three components:

- A protocol with a frame format that utilizes User Datagram Protocol (UDP)/IP.
- A server.
- A client.

The server runs on a central computer typically at the client site, while the clients reside in the dial-up access servers and can be distributed throughout the network. Cisco has incorporated the RADIUS Client into Cisco IOS Software Release 11.1 and later and other device software.

Client/Server Model

A network access server (NAS) operates as a client of RADIUS. The client passes user information to designated RADIUS servers, and then acts on the response that is returned. RADIUS servers receive user connection requests, authenticate the user, and returns all configuration information necessary for the client to deliver service to the user. The RADIUS servers can act as proxy clients to other kinds of authentication servers.

Network Security

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent

encrypted between the client and RADIUS server. This eliminates the possibility that someone snooping on an unsecured network could determine a user password.

Flexible Authentication Mechanisms

The RADIUS server supports a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, Password Authentication Protocol (PAP), or Challenge Handshake Authentication Protocol (CHAP), UNIX login, and other authentication mechanisms.

Server Code Availability

There are a number of distributions of server code commercially and freely available. Cisco servers include Cisco Secure ACS for Windows, Cisco Secure ACS for UNIX, and Cisco Access Registrar.

Compare TACACS+ and RADIUS

These sections compare several features of TACACS+ and RADIUS.

UDP and TCP

RADIUS uses UDP while TACACS+ uses TCP. TCP offers several advantages over UDP. TCP offers a connection-oriented transport, while UDP offers best-effort delivery. RADIUS requires additional programmable variables such as re-transmit attempts and time-outs to compensate for best-effort transport, but it lacks the level of built-in support that a TCP transport offers:

- TCP usage provides a separate acknowledgment that a request has been received, within (approximately) a network round-trip time (RTT), regardless of how loaded and slow the backend authentication mechanism (a TCP acknowledgment) is.
- TCP provides immediate indication of a crashed, or a stopped, server by a reset (RST). You can determine when a server crashes and returns to service if you use long-lived TCP connections. UDP cannot tell the difference between a server that is down, a slow server, and a non-existent server.
- With TCP keepalives, server crashes can be detected out-of-band with actual requests. Connections to multiple servers can be maintained simultaneously, and you only need to send messages to the ones that are known to be up and that run.
- TCP is more scalable and adapts to networks that increase in size as well as increased congestion.

Packet Encryption

RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party.

TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the

body of the packet is fully encrypted for more secure communications.

Authentication and Authorization

RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.

TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without a need for re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.

During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while the authentication mechanism is disassociated.

Multiprotocol Support

RADIUS does not support these protocols:

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

TACACS+ offers multiprotocol support.

Router Management

RADIUS does not allow users to control which commands can be executed on a router and which cannot. Therefore, RADIUS is not as useful for router management or as flexible for terminal services.

TACACS+ provides two methods to control the authorization of router commands on a per-user or per-group basis. The first method is to assign privilege levels to commands and have the router verify with the TACACS+ server whether or not the user is authorized at the specified privilege level. The second method is to explicitly specify in the TACACS+ server, on a per-user or per-group basis, the commands that are allowed.

Interoperability

Due to various interpretations of the RADIUS Request for Comments (RFCs), compliance with the RADIUS RFCs does not guarantee interoperability. Even though several vendors implement RADIUS clients, this does not mean they are interoperable. Cisco implements most RADIUS attributes and consistently adds more. If clients use only the standard RADIUS attributes in their servers, they can interoperate between several vendors as long as these vendors implement the

same attributes. However, many vendors implement extensions that are proprietary attributes. If a client uses one of these vendor-specific extended attributes, interoperability is not possible.

Traffic

Due to the previously cited differences between TACACS+ and RADIUS, the amount of traffic generated between the client and server differs. These examples illustrate the traffic between the client and server for TACACS+ and RADIUS when used for router management with authentication, exec authorization, command authorization (which RADIUS cannot do), exec accounting, and command accounting (which RADIUS cannot do).

TACACS+ Traffic Example

This example assumes login authentication, exec authorization, command authorization, start-stop exec accounting, and command accounting is implemented with TACACS+ when a user Telnets to a router, performs a command, and exits the router:

RADIUS Traffic Example

This example assumes login authentication, exec authorization, and start-stop exec accounting is implemented with RADIUS when a user Telnets to a router, performs a command, and exits the router (other management services are not available).

Device Support

This table lists TACACS+ and RADIUS AAA support by device type for selected platforms. This includes the software version in which the support was added. Check product release notes for further information if your product is not in this list.

Cisco Device	TACACS+ authentication	TACACS+ authorization	TACACS+ accounting	RADIUS authentication	RADIUS authorization	RADIUS accounting
Cisco Aironet[1]	12.2(4)JA	12.2(4)JA	12.2(4)JA	all Access-points	all Access-points	all 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]	--
Cisco Catalyst switches	2.2	5.4.1	5.4.1	5.1	5.4.1[4]	5.4.1[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 1900/2820 switches	8.x enterprise[9]	--	--	--	--	--
Cisco Catalyst	11.2.(8)SA6[10]	11.2.(8)SA6[10]	11.2.(8)SA6	12.0(5)WC5[11]	12.0(5)WC5[1]	12.0(5)WC5[1]

2900XL/3500XL switches			10		1, 4	1, 5
Cisco VPN 3000 Concentrator[6]	3.0	3.0	--	2.0[12]	2.0	2.0[12]
Cisco VPN 5000 Concentrator	--	--	--	5.2X[12]	5.2X[12]	5.2X[12]

Table Notes

1. Termination of wireless clients only, not management traffic in versions other than Cisco IOS Software Release 12.2(4)JA or later. In Cisco IOS Software Release 12.2.(4)JA or later, authentication for both termination of wireless clients and management traffic is possible.
2. Check the Software Advisor for platform support within Cisco IOS software.
3. Command accounting is not implemented until Cisco IOS Software Release 11.1.6.3.
4. No command authorization.
5. No command accounting.
6. URL blocking only, not administrative traffic.
7. Authorization for non-VPN traffic through the PIX.**Note**: Release 5.2 - Access-list support for Access Control List (ACL) RADIUS Vendor-Specific Attribute (VSA) or TACACS+ authorization for VPN traffic terminated on PIX Release 6.1 - support for ACL RADIUS attribute 11 authorization for VPN traffic terminated on PIX Release 6.2.2 - support for downloadable ACLs with RADIUS authorization for VPN traffic terminated on PIX Release 6.2 - support for authorization for PIX management traffic through TACACS+.<
8. Accounting for non-VPN traffic through the PIX only, not management traffic.**Note**: Release 5.2 - Support for accounting for VPN Client TCP packets through the PIX.
9. Enterprise software only.
10. Needs 8M Flash for image.
11. VPN termination only.

Note: Only registered Cisco users can access internal Cisco tools and information.

Related Information

- **RADIUS Support**
- **TACACS/TACACS+ Support / Authentication Protocols**
- **Requests for Comments (RFCs)**
- **Cisco Technical Support & Downloads**