TACACS.net™

The Advantages of TACACS+ for Administrator Authentication

Centrally manage and secure your network devices with one easy to deploy solution.

IT departments are responsible for managing many routers, switches, firewalls, and access points throughout a network. They need to be able to implement policies to determine who can log in to manage each device, what operations they can run, and log all actions taken. Managing these policies separately on each device can become unmanageable and lead to security incidents or errors that result in loss of service and network downtime. Most compliance requirements and security standards require using standardized tools to centralize authentication for administrative management. Some vendors offer proprietary management systems, but those only work on that vendor's devices, and can be very expensive. Many IT departments choose to use AAA (Authentication, Authorization and Accounting) protocols RADIUS or TACACS+ to address these issues. These protocols enable you to have all network devices managed by a single platform, and the protocols are already built in to most devices.

Protocol Differences

RADIUS was designed to authenticate and log dial-up remote users to a network, and TACACS+ is used most commonly for administrator access to network devices like routers and switches. This is indicated in the names of the protocols. RADIUS stands for Remote Access Dial-In User Service, and TACACS+ stands for Terminal Access Controller Access Control Service Plus.

The primary functional difference between RADIUS and TACACS+ is that TACACS+ separates out the Authorization functionality, where RADIUS combines both Authentication and Authorization. Though this may seem like a small detail, it makes a world of difference when implementing administrator AAA in a network environment.

RADIUS doesn't log the commands used by the administrator. It will only log the start, stop, and interim records of that session. This means that if there are two or more administrators logged at any one time, there is no way of telling which administrator entered which commands.

RADIUS can include privilege information in the authentication reply; however, it can only provide the privilege level, which means different things to different vendors. Because there is no standard between vendor implementations of RADIUS authorization, each vendor's attributes often conflict, resulting in inconsistent results. Even if this information were consistent, the administrator would still need to manage the privilege level for commands on each device. This will quickly become unmanageable.

RADIUS doesn't log the commands used by the administrator. It will only log the start, stop, and interim records of that session. This means that if there are two or more administrators logged at any one time, there is no way to tell from the RADIUS logs which administrator entered which commands.

The TACACS+ protocol was developed to resolve these issues. TACACS+ is a standard protocol developed by the U.S. Department of Defense, and later enhanced by Cisco Systems. TACACS+ separates out the authorization functionality, so it enables additional flexibility and granular access controls on who can run which commands on specified devices. Each command entered by a user is sent back to the central TACACS+ server for authorization, which then checks the command against an authorized list of commands for each user or group. TACACS+ can define policies based on user, device type, location, or time of day. The TACACS+ service can use locally configured users or users and groups defined in Active Directory or LDAP to control access to devices in your network. This enables Single Sign-On (SSO), which increases security, simplifies management, and makes it easier for users.

RADIUS was designed for subscriber AAA, and TACACS+ is designed for administrator AAA. RADIUS can still be used for small network administrator AAA, but only if authorization is not required, or if it is a homogeneous network (all one vendor). In any scenario where there is a heterogeneous environment or authorization policies are required for network devices, TACACS+ is the best option.

RADIUS was designed for subscriber AAA, and TACACS+ was designed for administrator AAA.

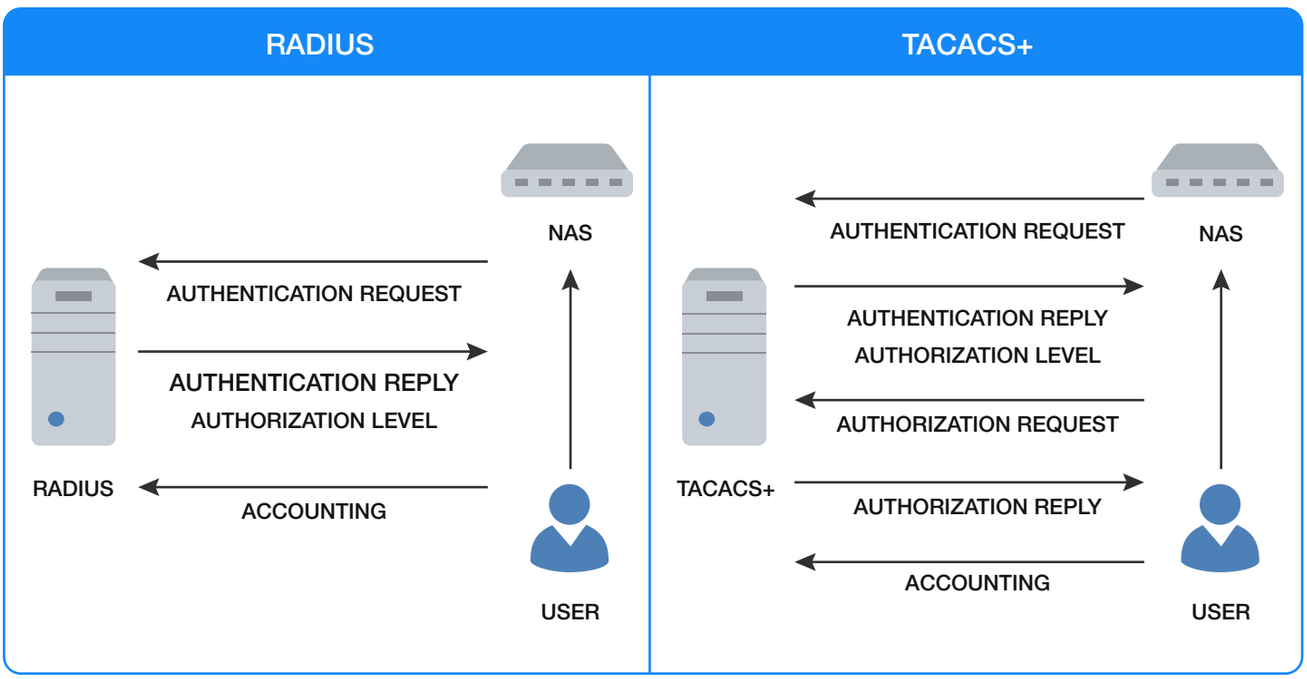

Figure 1: RADIUS vs. TACACS+

RADIUS	TACACS+
Combines authentication & authorization.	Separates all 3 elements of AAA, making it more flexible.
Less secure – only runs a hash on the password.	More secure - Encrypts the whole packet including username, password, and attributes.
Requires each network device to contain authorization configuration.	Central management for authorization configuration.
No command logging.	Full command logging.
Minimal vendor support for authorization.	Supported by most major vendors.
UDP- Connectionless UDP ports 1645/1646, 1812/1813	TCP- Connection oriented TCP port 49
Designed for subscriber AAA	Designed for administrator AAA

Table 1: RADIUS vs. TACACS+

Vendor Support

Most Enterprise or Carrier-class network device manufacturers support TACACS+ including Adtran, Alcatel/Lucent, Arbor, Aruba, Avocent/Cyclades, Blade Networks, BlueCat Networks, Blue Coat, Brocade/Foundry, Cisco/Linksys, Citrix, Dell, Edgewater, EMC, Enterasys, Ericsson/Redback, Extreme, Fortinet, Fujitsu, HP/3Com, Huawei, IBM, Juniper/Netscreen, Netgear, Nortel, Palo Alto Networks, Radware, Riverstone, Samsung, and many others.

Deployment Considerations

It is generally not a good idea to deploy RADIUS and TACACS+ services on the same server. There may be a perceived advantage to consolidating these services because they are both AAA protocols, however, they are deployed for different purposes, they use resources differently, and the licensing can be unnecessarily expensive. By combining these services, you may be increasing costs and reducing your network security. In an enterprise network, unprivileged remote users may be managed by a different operational group than privileged internal administrators. Combining these roles may violate the security principles of separation of duties and least privilege.

It is not a good idea to deploy RADIUS and TACACS+ on the same server. By combining these services, you may be increasing costs and reducing network security.

TACACS+ servers should be deployed in a fully trusted internal network. There should not be any direct access from untrusted or semi-trusted networks. RADIUS is typically deployed in a semi-trusted network, and TACACS+ uses internal administrative logins, so combining these services on the same server could potentially compromise your network security.

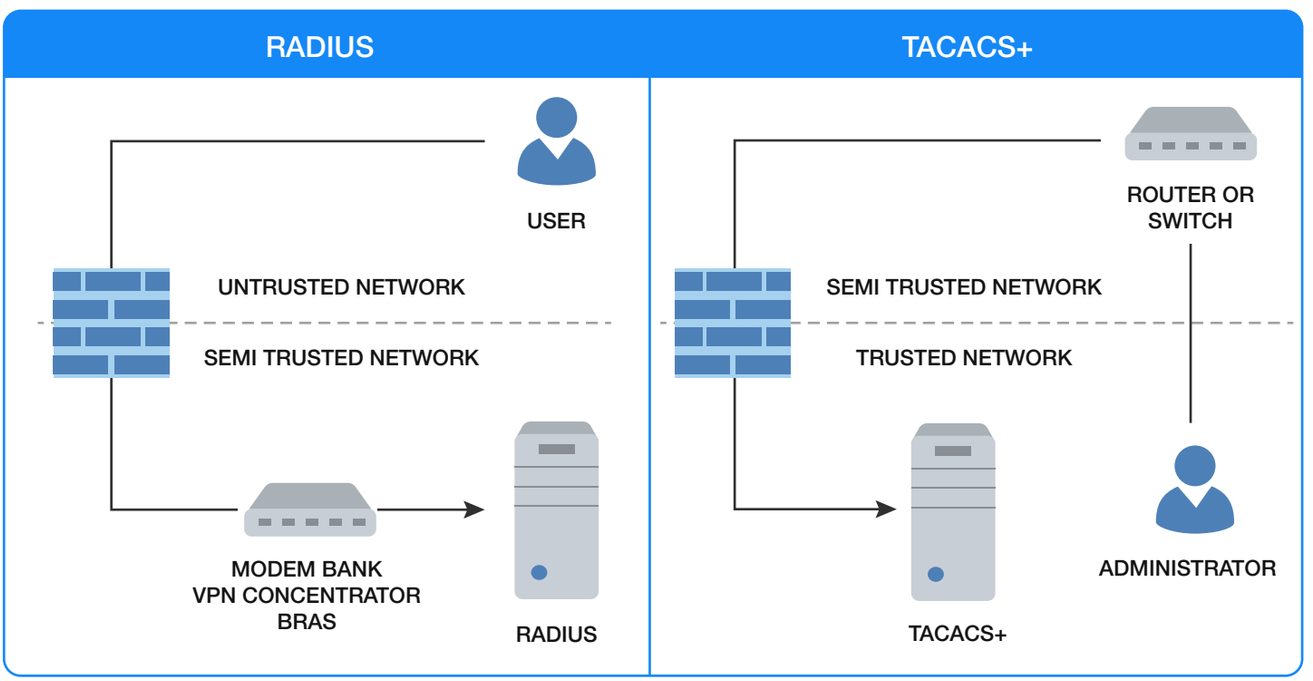

Figure 2: Differences between RADIUS and TACACS+ deployments

If you deploy your TACACS+ server in a semi-trusted network with a connection to your Windows Domain Controllers, you will have to open many ports for LDAP, SMB, Kerberos, etc. You may also need to open ports for DNS and NTP. If you keep your TACACS+ service within your trusted network, you only need to open one port, TCP 49. This is easier to manage and more secure.

The TACACS+ Service should be installed as close as possible to the user database, preferably on the same server.

The TACACS+ service should be installed as close as possible to the user database, preferably on the same server. If you intend to use Windows Active Directory as your user database, the best place to install your TACACS+ server is directly on your Windows Domain Controllers. TACACS+ needs to be closely synchronized with your Domain, and any network connection issues, DNS problems, or even time discrepancies can cause a critical service failure. Installing TACACS+ on the same server as the user database can also significantly improve performance.

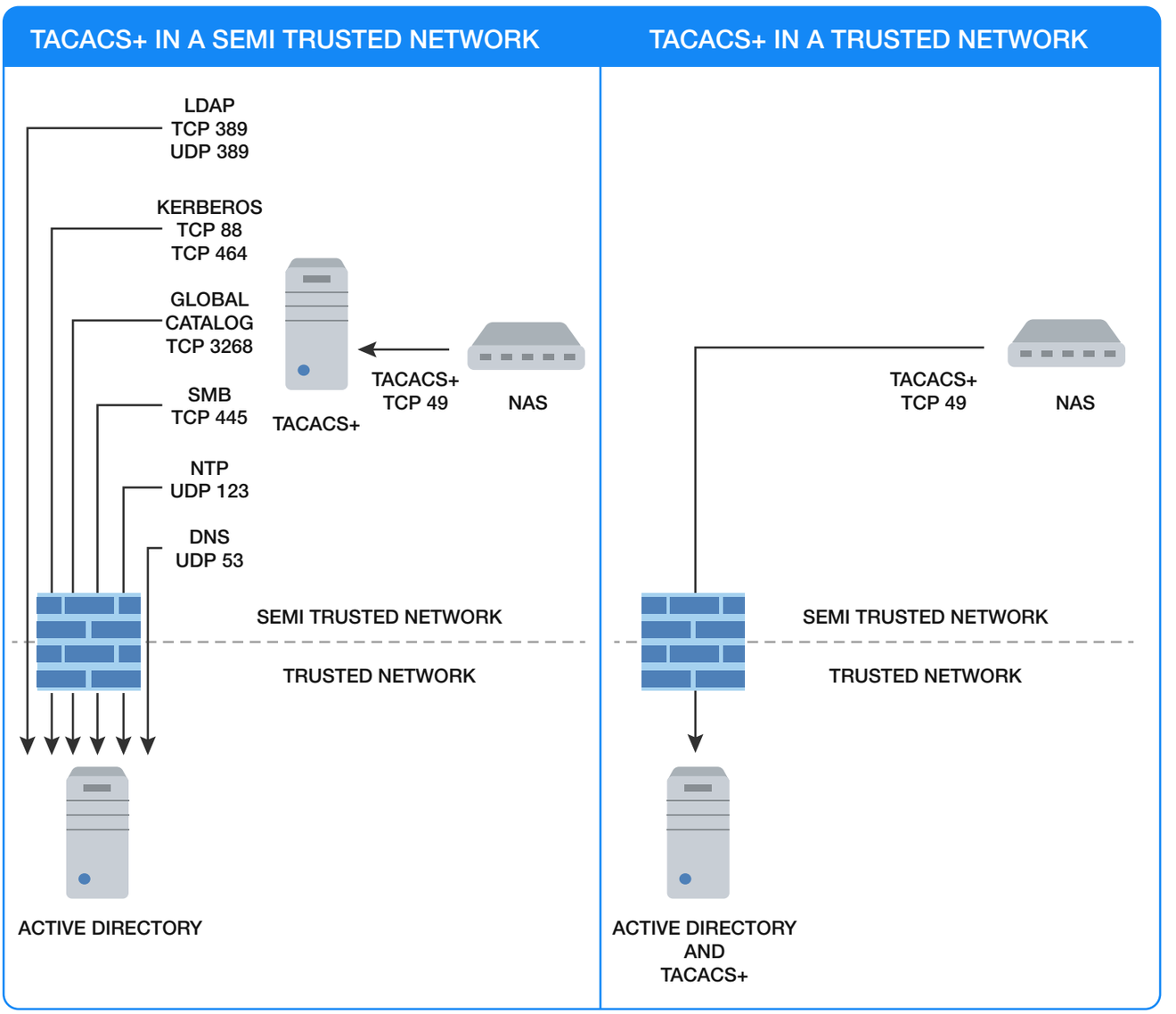

Figure 3: Deploying TACACS+ in a trusted network

Licensing Considerations

RADIUS is typically licensed differently than TACACS+. RADIUS servers are commonly licensed by users or modem connections, which can make the software prohibitively expensive. RADIUS is a more complex protocol than TACACS+. This is evidenced by the fact that there are more than 40 RFCs written on RADIUS, while TACACS+ only has one. The complexity in RADIUS does not offer any value for administrator access to network devices, so you may end up paying more for functionality that you don't use.

Summary

- RADIUS is designed for subscriber AAA, TACACS+ is designed for administrator AAA.
- TACACS+ includes per-command authorization and logging.
- TACACS+ enables you to set access policies by user, device, location, or time of day.
- The TACACS+ protocol is supported by most enterprise and carrier-grade devices.
- TACACS+ and RADIUS services should not be installed on the same server because it can reduce security and increase complexity and licensing costs.
- TACACS+ should be deployed in a fully-trusted, internal network to increase security and simplify management.
- TACACS+ should be installed as close to the user database as possible, preferably on the same server to minimize points of failure and increase performance.