TACACS Device Access Control with Cisco Active Network Abstraction

Executive Summary

Cisco[®] Active Network Abstraction (ANA) is an extensible and scalable product suite that resides between the network elements and OSS management applications, providing unified end-to-end service-level management for service provider and large enterprise networks. Terminal Access Controller Access Control System Plus (TACACS+) is a widely used protocol for device authentication, authorization, and accounting (AAA) control. Cisco Secure Access Control Server (ACS) is a high-performance access control server that operates as a centralized TACACS+ or RADIUS server.

This white paper describes the recommended device AAA configuration in an environment where Cisco ANA manages devices that are configured for AAA with TACACS+. It maintains complete AAA for both Cisco ANA and the managed devices without incurring significant additional load to the TACACS+ server.

Cisco Active Network Abstraction

Cisco Active Network Abstraction (ANA) is an extensible and scalable product suite enabling a unified management system that delivers true, end-to-end, service-level management of service provider and large enterprise networks. It is a virtualized management layer that resides between the network elements and OSS management applications, mediating communications among them. Managing the network through this virtualized network model enables tighter integration of subscriber-generated services for greater automation and control. The Cisco ANA approach scales directly alongside the real network, allowing operators to view and manage the complexities of multiple services and millions of customers in a multi-technology, multi-vendor network. Cisco ANA is part of the next-generation management system for the Cisco IP NGN architecture.

## TACACS+ and Cisco Secure Access Control Server

Terminal Access Controller Access Control System Plus (TACACS+) is a widely used protocol that provides access control for routers, network access servers and other networked computing devices. Cisco Secure Access Control Server (ACS) is a high-performance access control server that operates as a centralized TACACS+ or RADIUS server. It extends access security by combining authentication, user access, and administrator access with policy control within a centralized identity networking solution. It enforces a uniform security policy for all users regardless of how they access the network. Cisco Secure ACS centralizes the control of all user privileges and distributes them to the managed devices throughout the network. It also provides detailed reporting and monitoring capabilities of network users' behavior and keeps a record of every access connection and device configuration change across the entire network.

Cisco ANA Managing Devices Configured For TACACS+

TACACS+ server, as part of Cisco Secure ACS, provides powerful authentication, authorization, and accounting capabilities to network administrators. It provides initial authentication when users log in to the network devices, authorization at the granularity of the command-line interface (CLI) level, and detailed logging capabilities that facilitate accounting for network devices. TACACS+ can handle multiple users accessing the devices simultaneously.

Cisco ANA manages thousands of devices by design. Figure 1 shows a network of devices, managed by Cisco ANA, with Cisco Secure ACS providing the AAA functionality using TACACS+. Cisco ANA actively monitors the network devices and maintains a fully correlated object model of the network. The benefit of this approach is that individual management applications do not need to access network devices separately but can rely on the Cisco ANA object model for the latest status. Cisco ANA uses both Simple Network Management Protocol (SNMP) and Telnet to perform fault management. SNMP is used mainly while Telnet is used when the management data required by Cisco ANA is unavailable through SNMP, due to device software and hardware limitations. These Telnet connections can incur additional load on the TACACS+ server. The rest of this white paper discusses the recommended TACACS+ configuration for network devices when they are managed by high-performance management platforms, such as Cisco ANA, in order to maintain complete AAA functionality without creating significant additional load to the TACACS+ server.

Figure 1.   Cisco ANA Managing Devices Configured for AAA Using TACACS+
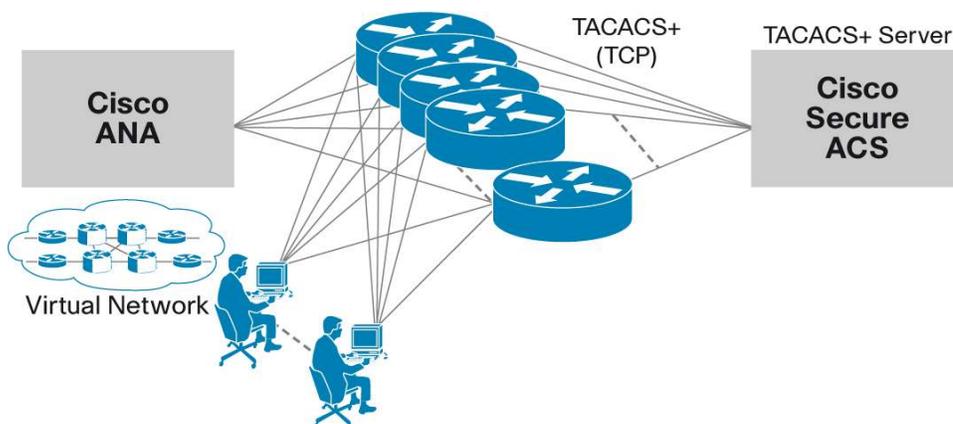
Recommended Device Configuration for TACACS+ in IP NGN

Cisco ANA implements role-based access control. Users are authenticated and authorized at a level of authorization associated with their roles at Cisco ANA. All user activities are also logged by Cisco ANA. Since Cisco ANA is already enforcing security policies on network administrators, we can simplify the authorization and accounting requirements on the managed network devices. Cisco ANA requires a user account on the device in order to access it. This user account is a server-to-device specific account, and we shall refer to it as device user account Cisco ANA hereafter. Because security policies are enforced in Cisco ANA, user account Cisco ANA can be considered as a "trusted source", and thus does not require TACACS+ authorization and accounting for every command.

Figure 2 describes the recommended device AAA configuration for TACACS+ when the device is managed by Cisco ANA (or other high-performance management platforms) It can be summarized as follows:

- Differentiate the user Cisco ANA from other users on the device by assigning dedicated VTY line(s)
- Use Network Access Restriction (NAR) to restrict user Cisco ANA access from only the specified IP address(es)
- Use local authorization at the device for the user Cisco ANA
- Configure for no accounting for user Cisco ANA at the device

This configuration uses TACACS+ for authentication and authorizes user Cisco ANA locally at the device for CLI commands. Local authorization will significantly reduce the load on the TACACS+ server from the large amount of automated transactions generated by user Cisco ANA. Note that this authentication approach should not affect other users accessing a router over Telnet or Shared Shell (SSH) Protocol. User Cisco ANA should be authenticated through TACACS+, although it can be authenticated locally on the managed device. If account information of user

Cisco ANA is to be stored locally in the device configuration, additional measures should be taken to minimize security risks associated. By assigning dedicated VTY lines and using NAR, it is ensured that device access by user Cisco ANA is allowed only from Cisco ANA, not by Telnet from anywhere else.

Figure 2.   Recommended Device AAA Configuration for TACACS+
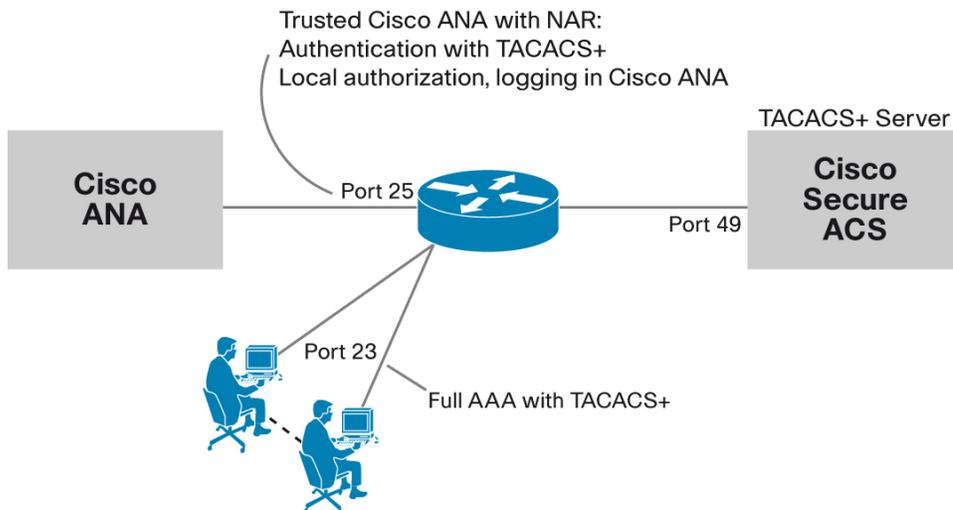
The following two sections describe the detailed recommended configuration at the device and TACACS+ server (Cisco Secure ACS).

Device Configuration

1. Assign one VTY line dedicated to management software transactions.

    a. This example configuration uses the capability of Cisco IOS® Software to change the inbound Telnet port for a particular VTY line.

```
Example:
    Line VTY 5
    Rotary 25
```

This command will change the port for the inbound Telnet session from 23 to 3025.

    b. To achieve a similar result for SSH, the solution uses the global configuration command:

```
ip ssh port 2025 rotary 25
```

This command changes the inbound SSH port (for line VTY 5 only) from 22 to 2025.

2. Now a separate VTY line that could be used by Cisco ANA user is constructed. Since it is aseparate line, we can apply different authentication methods.

    a. This is an example configuration of a Cisco IOS Software system that uses TACACS+ for all AAA:

```
aaa new-model
aaa authentication login default tacacs+ local
aaa authorization exec default tacacs+ if-authenticated
aaa authorization commands 0 default tacacs+ if-authenticated
aaa authorization commands 1 default tacacs+ if-authenticated
aaa authorization commands 15 default tacacs+ if-authenticated
aaa accounting exec default start-stop tacacs+
aaa accounting commands 0 default start-stop tacacs+
aaa accounting commands 1 default start-stop tacacs+
```

```
aaa accounting commands 15 default start-stop tacacs+
```

b. Configure separate authentication and authorization methods that will be used only for the management software user account.

```
aaa authentication login mgmt local
aaa authorization exec mgmt local
aaa authorization commands 0 mgmt local
aaa authorization commands 1 mgmt local
aaa authorization commands 15 mgmt local
```

When applied to line VTY 5, it will force anyone to get authenticated by using the "mgmt" method, which is defined as local.

```
line VTY 5
    login authentication mgmt
    authorization exec mgmt
    authorization commands 0 mgmt
    authorization commands 1 mgmt
```

If the CiscoANA user account is to be stored locally the following security hardening measures are recommended:

a. Configure the CiscoANA user using MD5 one-way so instead of using:

```
username devrec password cisco
```

Use

```
username devrec secret cisco
```

This will create an MD5 hash password.

b. Assign an inbound access list to line 5, so only Cisco ANA can initiate inbound Telnet or SSH sessions.

```
ip access-list standard mgmt-servers
    permit {management server IP address}
line vty 5
    transport input telnet ssh
    access-class mgmt-servers inbound
```

The following configuration includes all the aspects discussed above:

```
username devrec secret cisco

aaa authentication login mgmt local
aaa authorization exec mgmt local
aaa authorization commands 0 mgmt local
aaa authorization commands 1 mgmt local
aaa authorization commands 15 mgmt local

ip ssh port 2025 rotary 25
ip access-list standard mgmt-servers
permit {management server IP address}

line VTY 5
rotary 25
    login authentication mgmt
    authorization exec mgmt
    authorization commands 0 mgmt
```

```
        authorization commands 1 mgmt
        authorization commands 15 mgmt
        transport input telnet ssh
        access-class mgmt-servers inbound
```

Cisco Secure ACS Configuration

Cisco Secure ACS can be configured to force the management platform to be authenticated from one to several specified IP addresses only using NAR.

The following example shows an NAR configuration that restricts access to a router (Cisco 1721 is used in this example) to a given source IP address and a specified port. In the context of this discussion, the source IP address is that of Cisco ANA, and the port is the VTY for the new rotary number on the network device. The Cisco 1721 in this example runs on Cisco IOS Software Version 12.3(1a). Rotary 25 was configured on VTY 5 only. The line-to-TTY port mapping for the device is as follows:

```
tty0 = line con 0
tty6 = line vty 0
tty7 = line vty 1
...
tty11 = line vty 5
```

Note that this mapping may vary in different Cisco IOS Software releases, and each port may have a different nomenclature. Figure 3 shows the Cisco Secure ACS for Windows NAR configuration, which limits access to VTY 5 for a specific IP address, in this case 171.69.75.197.

Figure 3.   Network Access Restriction to Limit Port to a Given Source IP AddressNetwork Access Restriction to Limit a Port to a Given Source IP Address

This NAR, if applied to the CiscoANA username, will allow authentication to the device 1721_1 on TTY 11 from only 171.69.75.197. Multiple devices may be entered as necessary. If the TTY numbers match, network device groups may be used.

Conclusion

This white paper describes the recommended device AAA configuration in an environment where Cisco ANA manages devices that are configured for AAA with TACACS+. It maintains complete AAA functionality for Cisco ANA and the managed devices without incurring significant additional load to the TACACS+ server.

For More Information

For more information about Cisco ANA, please visit http://www.cisco.com/en/US/products/ps6776/index.html, contact your local account representative, or send an e-mail to the Cisco ANA product management team at ask-ana@cisco.com.

For more information about Cisco Secure ACS products, please visit http://www.cisco.com/go/acs.

For questions about product ordering, availability, and support contract information, please contact your local account representatives.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-392419-02   09/10