Information About AAA

This chapter describes authentication, authorization, and accounting (AAA, pronounced “triple A”). AAA is a a set of services for controlling access to computer resources, enforcing policies, assessing usage, and providing the information necessary to bill for services. These processes are considered important for effective network management and security.

This chapter includes the following sections:

Authentication

Authentication provides a way to identify a user, typically by having the user enter a valid username and valid password before access is granted. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is permitted access to the network. If the credentials do not match, authentication fails and network access is denied.

You can configure the ASA to authenticate the following items:

- All administrative connections to the ASA, including the following sessions:
  - Telnet
  - SSH. For more information, see Chapter 43, “Management Access.”
  - Serial console
  - ASDM using HTTPS
  - VPN management access
- The **enable** command. For more information, see Chapter 43, “Management Access.”
- Network access. For more information, see Chapter 40, “Identity Firewall,” Chapter 41, “ASA and Cisco TrustSec,” of the firewall configuration guide.

- VPN access. For more information, see the VPN configuration guide.

Authorization

Authorization is the process of enforcing policies: determining what types of activities, resources, or services a user is permitted to access. After a user is authenticated, that user may be authorized for different types of access or activity.

You can configure the ASA to authorize the following items:

- Management commands. For more information, see Chapter 43, "Management Access."
- Network access. For more information, see legacy feature guide.
- VPN access. For more information, see the VPN configuration guide.

Accounting

Accounting measures the resources a user consumes during access, which may include the amount of system time or the amount of data that a user has sent or received during a session. Accounting is carried out through the logging of session statistics and usage information, which is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

Interaction Between Authentication, Authorization, and Accounting

You can use authentication alone or with authorization and accounting. Authorization always requires a user to be authenticated first. You can use accounting alone, or with authentication and authorization.

AAA Servers

The AAA server is a network server that is used for access control. Authentication identifies the user. Authorization implements policies that determine which resources and services an authenticated user may access. Accounting keeps track of time and data resources that are used for billing and analysis.

AAA Server Groups

If you want to use an external AAA server for authentication, authorization, or accounting, you must first create at least one AAA server group per AAA protocol and add one or more servers to each group. You identify AAA server groups by name. Each server group is specific to one type of server or service.

Local Database Support

The ASA maintains a local database that you can populate with user profiles. You can use a local database instead of AAA servers to provide user authentication, authorization, and accounting. For more information, see Chapter 35, "Local Database for AAA."

Summary of AAA Service Support

Table 34-1 provides cross-references to the configuration guide chapters that describe support for specific AAA service types.

Table 34-1 AAA Service Support

AAA Service	Configuration Guide Cross-Reference
Certificates	See Chapter 42, "Digital Certificates."
HTTP Form	See the VPN configuration guide.
Identity Firewall	See Chapter 40, "Identity Firewall."
Kerberos	See the VPN configuration guide.
LDAP	See Chapter 38, "LDAP Servers for AAA."
Local Database	See Chapter 35, "Local Database for AAA."
NT	See Chapter 39, "Windows NT Servers for AAA."
RADIUS	See Chapter 36, "RADIUS Servers for AAA."
RSA/SDI	See the VPN configuration guide.
TACACS+	See Chapter 37, "TACACS+ Servers for AAA."
TrustSec	See Chapter 41, "ASA and Cisco TrustSec."