



Configuring AAA Servers and the Local Database

This chapter describes support for AAA (pronounced “triple A”) and how to configure AAA servers and the local database.

This chapter contains the following sections:

- [AAA Overview, page 14-1](#)
- [AAA Server and Local Database Support, page 14-3](#)
- [Configuring the Local Database, page 14-9](#)
- [Identifying AAA Server Groups and Servers, page 14-11](#)

AAA Overview

AAA enables the FWSM to determine who the user is (authentication), what the user can do (authorization), and what the user did (accounting).

AAA provides an extra level of protection and control for user access than using access lists alone. For example, you can create an access list allowing all outside users to access Telnet on a server on an inside interface. If you want only some users to access the server and you might not always know IP addresses of these users, you can enable AAA to allow only authenticated and/or authorized users to make it through the FWSM. (The Telnet server enforces authentication, too; the FWSM prevents unauthorized users from attempting to access the server.)

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.

If you use multiple security contexts, AAA settings are discrete per context, not shared between contexts. This provides you the opportunity to control access, authorize resources and commands, and perform accounting differently among contexts.

This section includes the following topics:

- [About Authentication, page 14-2](#)
- [About Authorization, page 14-2](#)
- [About Accounting, page 14-2](#)

About Authentication

Authentication controls access by requiring valid user credentials, which are typically a username and password. You can configure the FWSM to authenticate the following items:

- All administrative connections to the FWSM including the following sessions:
 - Telnet
 - SSH
 - Serial console
 - ASDM (using HTTPS)
 - VPN management access

The **enable**

About Authorization

per user

-
-
-



Note

The FWSM caches the first 16 authorization requests per user, so if the user accesses the same services during the current authentication session, the FWSM does not resend the request to the authorization server.

About Accounting

Accounting tracks traffic that passes through the FWSM, enabling you to have a record of user activity. If you enable authentication for that traffic, you can account for traffic per user. If you do not authenticate the traffic, you can account for traffic per IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the FWSM for the session, the service used, and the duration of each session.

AAA Server and Local Database Support

The FWSM supports a variety of AAA server types and a local database that is stored on the FWSM. This section describes support for each AAA server type and the local database.

This section contains the following topics:

- [Summary of Support, page 14-3](#)
- [RADIUS Server Support, page 14-4](#)
- [TACACS+ Server Support, page 14-5](#)
- [SDI Server Support, page 14-6](#)
- [NT Server Support, page 14-7](#)
- [Kerberos Server Support, page 14-7](#)
- [LDAP Server Support, page 14-7](#)
- [Local Database Support, page 14-8](#)

Summary of Support

[Table 14-1](#) summarizes the support for each AAA service by each AAA server type, including the local database. For more information about support for a specific AAA server type, see the topics following the table.

Table 14-1 Summary of AAA Support

AAA Service	Database Type						
	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP
Authentication of . . .							
VPN users ¹	Yes	Yes	Yes	Yes	Yes	Yes	No
Firewall sessions	Yes	Yes	Yes	No	No	No	No
Administrators	Yes	Yes	Yes	No	No	No	No
Authorization of . . .							
VPN users ¹	Yes	Yes	No	No	No	No	Yes
Firewall sessions	No	Yes ²	Yes	No	No	No	No
Administrators	Yes ³	No	Yes	No	No	No	No
Accounting of . . .							
VPN connections ¹	No	Yes	Yes	No	No	No	No
Firewall sessions	No	Yes	Yes	No	No	No	No
Administrators	No	No	Yes	No	No	No	No

1. VPN is available for management connections only.
2. For firewall sessions, RADIUS authorization is supported with user-specific access lists only, which are received or specified in a RADIUS authentication response.
3. Local command authorization is supported by privilege level only.

RADIUS Server Support

The FWSM supports RADIUS servers.

This section contains the following topics:

- [Authentication Methods, page 14-4](#)
- [Attribute Support, page 14-4](#)
- [RADIUS Functions, page 14-4](#)

Authentication Methods

The FWSM supports the following authentication methods with RADIUS:

- PAP
- CHAP
- MS-CHAPv1
- MS-CHAPv2 (including password aging), for IPSec users only

Attribute Support

The FWSM supports the following sets of RADIUS attributes:

- Authentication attributes defined in RFC 2138.
- Accounting attributes defined in RFC 2139.
- RADIUS attributes for tunneled protocol support, defined in RFC 2868.
- Cisco IOS VSAs, identified by RADIUS vendor ID 9.
- Cisco VPN-related VSAs, identified by RADIUS vendor ID 3076.
- Microsoft VSAs, defined in RFC 2548.

RADIUS Functions

The FWSM can use RADIUS servers for the functionality described in [Table 14-2](#).

Table 14-2 RADIUS Functions

Functions	Description
User authentication for CLI access	When a user attempts to access the FWSM with Telnet, SSH, HTTP, or a serial console connection and the traffic matches an authentication statement, the FWSM challenges the user for a username and password, sends these credentials to the RADIUS server, and grants or denies user CLI access based on the response from the server.
User authentication for the command	When a user attempts to access the <code>enable</code> command, the FWSM challenges the user for a password, sends to the RADIUS server the username and enable password, and grants or denies user access to enable mode based on the response from the server.

Table 14-2 RADIUS Functions (continued)

Functions	Description
User authentication for network access	When a user attempts to access networks through the FWSM and the traffic matches an authentication statement, the FWSM sends to the RADIUS server the user credentials (typically a username and password) and grants or denies user network access based on the response from the server.
User authorization for network access using dynamic access lists per user	To implement dynamic access lists, you must configure the RADIUS server to support it. When the user authenticates, the RADIUS server sends a downloadable access list to the FWSM. Access to a given service is either permitted or denied by the access list. The FWSM deletes the access list when the authentication session expires.
User authorization for network access using a downloaded access list name per user	To implement downloaded access list names, you must configure the RADIUS server to support it. When the user authenticates, the RADIUS server sends a name of an access list. If an access list with the name specified exists on the FWSM, access to a given service is either permitted or denied by the access list. You can specify the same access list for multiple users.
VPN authentication	When a user attempts to establish a management connection using VPN and the applicable tunnel-group record specifies a RADIUS authentication server group, the FWSM sends to the RADIUS server the username and password, and then grants or denies user access based on the response from the server.
VPN authorization	When user authentication for VPN access has succeeded and the applicable tunnel-group record specifies a RADIUS authorization server group, the FWSM sends a request to the RADIUS authorization server and applies to the VPN session the authorizations received.
VPN accounting	When user authentication for VPN access has succeeded and the applicable tunnel-group record specifies a RADIUS accounting server group, the FWSM sends the RADIUS server group accounting data about the VPN session.
Accounting for network access per user or IP address	You can configure the FWSM to send accounting information to a RADIUS server about any traffic that passes through the FWSM.

TACACS+ Server Support

The FWSM can use TACACS+ servers for the functionality described in [Table 14-3](#). The FWSM supports TACACS+ authentication with ASCII, PAP, CHAP, and MS-CHAPv1.

Table 14-3 TACACS+ Functions

Functions	Description
User authentication for CLI access	When a user attempts to access the FWSM with Telnet, SSH, HTTP, or a serial console connection and the traffic matches an authentication statement, the FWSM challenges the user for a username and password, sends these credentials to the TACACS+ server, and grants or denies user CLI access based on the response from the server.
User authentication for the command	When a user attempts to access the <code>enable</code> command, the FWSM challenges the user for a password, sends to the TACACS+ server the username and enable password, and grants or denies user access to enable mode based on the response from the server.

Table 14-3 TACACS+ Functions (continued)

Functions	Description
Accounting for CLI access	You can configure the FWSM to send accounting information to a TACACS+ server about administrative sessions.
User authentication for network access	When a user attempts to access networks through the FWSM and the traffic matches an authentication statement, the FWSM sends to the TACACS+ server the user credentials (typically a username and password) and grants or denies user network access based on the response from the server.
User authorization for network access	When a user matches an authorization statement on the FWSM after authenticating, the FWSM consults the TACACS+ server for user access privileges.
VPN authentication	When a user attempts to establish a management connection using VPN and the applicable tunnel-group record specifies a TACACS+ authentication server group, the FWSM sends to the TACACS+ server the username and password, and then grants or denies user access based on the response from the server.
VPN accounting	When user authentication for VPN access has succeeded and the applicable tunnel-group record specifies a TACACS+ accounting server group, the FWSM sends the TACACS+ server group accounting data about the VPN session.
User authorization for management commands.	On the TACACS+ server, configure the commands that a user can use after authenticating for CLI access. Each command that a user enters at the CLI is checked by the TACACS+ server.
Accounting for network access per user or IP address	You can configure the FWSM to send accounting information to the TACACS+ server about any traffic that passes through the FWSM.

SDI Server Support

The FWSM can use RSA SecureID servers for VPN authentication. These servers are also known as SDI servers. When a user attempts to establish VPN access and the applicable tunnel-group record specifies a SDI authentication server group, the FWSM sends to the SDI server the username and one-time password and grants or denies user access based on the response from the server.

This section contains the following topics:

- [SDI Version Support, page 14-6](#)
- [Two-step Authentication Process, page 14-7](#)
- [SDI Primary and Replica Servers, page 14-7](#)

SDI Version Support

The FWSM offers the following SDI version support:

- **Versions prior to Version 5.0**—SDI versions prior to 5.0 use the concept of an SDI master and an SDI slave server which share a single node secret file (SECURID).
- **Versions 5.0**—SDI Version 5.0 uses the concepts of an SDI primary and SDI replica servers. Each primary and its replicas share a single node secret file. The node secret file has its name based on the hexadecimal value of the ACE/Server IP address with .sdi appended.

A Version 5.0 SDI server that you configure on the FWSM can be either the primary or any one of the replicas. See the “[SDI Primary and Replica Servers](#)” section on page 14-7 for information about how the SDI agent selects servers to authenticate users.

Two-step Authentication Process

SDI Version 5.0 uses a two-step process to prevent an intruder from capturing information from an RSA SecurID authentication request and using it to authenticate to another server. The SDI agent first sends a lock request to the SecurID server before sending the user authentication request. The server locks the username, preventing another (replica) server from accepting it. This means that the same user cannot authenticate to two FWSMs using the same authentication servers simultaneously. After a successful username lock, the FWSM sends the passcode.

SDI Primary and Replica Servers

The FWSM obtains the server list when the first user authenticates to the configured server, which can be either a primary or a replica. The FWSM then assigns priorities to each of the servers on the list, and subsequent server selection derives at random from those assigned priorities. The highest priority servers have a higher likelihood of being selected.

NT Server Support

The FWSM supports authentication of VPN-based management connections with Microsoft Windows server operating systems that support NTLM Version 1, which we collectively refer to as NT servers. When a user attempts to establish VPN access and the applicable tunnel-group record specifies an NT authentication server group, the FWSM uses NTLM Version 1 to for user authentication with the Microsoft Windows domain server. The FWSM grants or denies user access based on the response from the domain server.

**Note**

NT servers have a maximum length of 14 characters for user passwords. Longer passwords are truncated. This is a limitation of NTLM Version 1.

Kerberos Server Support

The FWSM can use Kerberos servers for VPN-based management connections. When a user attempts to establish VPN access, and the traffic matches an authentication statement, the FWSM consults the Kerberos server for user authentication and grants or denies user access based on the response from the server.

The FWSM supports 3DES, DES, and RC4 encryption types.

**Note**

The FWSM does not support changing user passwords during tunnel negotiation. To avoid this situation happening inadvertently, disable password expiration on the Kerberos/Active Directory server for users connecting to the FWSM.

LDAP Server Support

The FWSM can use LDAP servers for authorization of VPN-based management connections. When user authentication for VPN access has succeeded and the applicable tunnel-group record specifies an LDAP authorization server group, the FWSM queries the LDAP server and applies to the VPN session the authorizations it receives.

Local Database Support

The FWSM maintains a local database that you can populate with user profiles.

This section contains the following topics:

- [User Profiles, page 14-8](#)
- [Local Database Functions, page 14-8](#)
- [Fallback Support, page 14-9](#)

User Profiles

User profiles contain, at a minimum, a username. Typically, a password is assigned to each username, although passwords are optional.

The **username attributes** command enables you to enter the username mode. In this mode, you can add other information to a specific user profile. The information you can add includes VPN-related attributes, such as a VPN session timeout value.

Local Database Functions

The FWSM can use local database for the functionality described in [Table 14-4](#).

Table 14-4 Local Database Functions

Functions	Description
User authentication for CLI access	When a user attempts to access the FWSM with Telnet, SSH, HTTP, or a serial console connection and the traffic matches an authentication statement, the FWSM challenges the user for a username and password, checks these credentials against the local database, and grants or denies user CLI access based on the result.
User authentication for the enable or login command	When a user attempts to access the enable command, the FWSM challenges the user for a password, checks the username and password against the local database, and grants or denies user access to enable mode based on the result.
User authorization for management commands.	When a user authenticates with the enable command (or logs in with the login command), the FWSM places that user in the privilege level defined by the local database. You can configure each command to belong to privilege level between 0 and 15 on the FWSM.
User authentication for network access	When a user attempts to access networks through the FWSM and the traffic matches an authentication statement, the FWSM challenges the user for a username and password, checks these credentials against the local database, and grants or denies user network access based on the result.
VPN authentication	When a user attempts to establish a management connection using VPN and the traffic matches an authentication statement, the FWSM checks the username and password received against the local user database, and grants or denies VPN access based on the result.
VPN authorization	When user authentication for VPN access has succeeded, the FWSM applies to the VPN session the attributes from the local database that are associated with the username and the applicable group policy.

Fallback Support

With the exception of fallback for network access authentication, the local database can act as a fallback method for the functions in [Table 14-4](#). This behavior is designed to help you prevent accidental lockout from the FWSM.

For users who need fallback support, we recommend that their usernames and passwords in the local database match their usernames and passwords in the AAA servers. This provides transparent fallback support. Because the user cannot determine whether a AAA server or the local database is providing the service, using usernames and passwords on AAA servers that are different than the usernames and passwords in the local database means that the user cannot be certain which username and password should be given.

The local database supports the following fallback functions:

- **Console and enable password authentication**—When you use the **aaa authentication console** command, you can add the **LOCAL** keyword after the AAA server group tag. If the servers in the group all are unavailable, the FWSM uses the local database to authenticate administrative access. This can include enable password authentication, too.
- **Command authorization**—When you use the **aaa authorization command** command, you can add the **LOCAL** keyword after the AAA server group tag. If the TACACS+ servers in the group all are unavailable, the local database is used to authorize commands based on privilege levels.
- **VPN authentication and authorization**—VPN authentication and authorization are supported to enable remote access to the FWSM if AAA servers that normally support these VPN services are unavailable. The **authentication-server-group** command, available in tunnel-group general attributes mode, lets you specify the **LOCAL** keyword when you are configuring attributes of a tunnel group. When VPN client of an administrator specifies a tunnel group configured to fallback to the local database, the VPN tunnel can be established even if the AAA server group is unavailable, provided that the local database is configured with the necessary attributes.

Configuring the Local Database

This section describes how to manage users in the local database. You can use the local database for CLI access authentication, privileged mode authentication, command authorization, network access authentication, and VPN authentication and authorization. You cannot use the local database for network access authorization. The local database does not support accounting.

For multiple context mode, you can configure usernames in the system execution space to provide individual logins using the **login** command; however, you cannot configure any **aaa** commands in the system execution space.



Caution

If you add to the local database users who can gain access to the CLI but who should not be allowed to enter privileged mode, enable command authorization. (See the [“Configuring Local Command Authorization”](#) section on page 21-14.) Without command authorization, users can access privileged mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use RADIUS or TACACS+ authentication so that the user will not be able to use the **login** command, or you can set all local users to level 1 so you can control who can use the system enable password to access privileged mode.

To define a user account in the local database, perform the following steps:

Step 1 Create the user account. To do so, enter the following command:

```
hostname/contexta(config)# username username {nopassword | password password} [encrypted]
[privilege level]
```

username

password

encrypted

privilege *level*

nopassword

Step 2

a.

username **attributes**

username attributes

- **group-lock**
- **password-storage**
- **vpn-access-hours**
- **vpn-filter**
- **vpn-framed-ip-address**
- **vpn-group-policy**
- **vpn-idle-timeout**
- **vpn-session-timeout**
- **vpn-simultaneous-logins**
- **vpn-tunnel-protocol**

*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services
Module Command Reference*

b.

exit

```
username admin password passw0rd privilege 15
```

```
username bcham34 nopassword
```

```
username rwilliams password g0ge0us  
username rwilliams attributes
```

```
hostname/contexta(config-username)# vpn-tunnel-protocol IPsec
```

```
hostname/contexta(config-username)# vpn-simultaneous-logins 6  
hostname/contexta(config-username)# exit
```

Identifying AAA Server Groups and Servers

Step 1

a.

```
hostname/contexta(config)# aaa-server server_group protocol {kerberos | ldap | nt |  
radius | sdi | tacacs+}
```

b.

```
hostname/contexta(config-aaa-server-group)# max-failed-attempts number  
number
```

c.

Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference

Table 14-5 Host Mode Commands, Server Types, and Defaults (continued)

Command	Applicable AAA Server Types	Default Value

c.

```

hostname/contexta(config)# aaa-server AuthInbound protocol tacacs+
hostname/contexta(config-aaa-server-group)# max-failed-attempts 2
hostname/contexta(config-aaa-server-group)# reactivation-mode depletion deadtime 20
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server AuthInbound (inside) host 10.1.1.1
hostname/contexta(config-aaa-server-host)# key TACPlusUauthKey
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# aaa-server AuthInbound (inside) host 10.1.1.2
hostname/contexta(config-aaa-server-host)# key TACPlusUauthKey2
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# aaa-server AuthOutbound protocol radius
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
hostname/contexta(config-aaa-server-host)# key RadUauthKey
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# aaa-server NTAAuth protocol nt
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server NTAAuth (inside) host 10.1.1.4
hostname/contexta(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname/contexta(config-aaa-server-host)# exit

```

