Your Short Cut to Knowledge

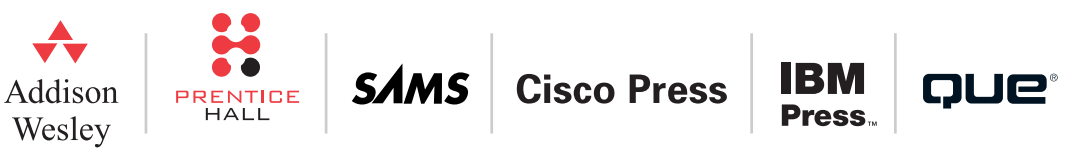
The following is an excerpt from a Short Cut published by one of the Pearson Education imprints.

Short Cuts are short, concise, PDF documents designed specifically for busy technical professionals like you.

We've provided this excerpt to help you review the product before you purchase. Please note, the hyperlinks contained within this excerpt have been deactivated.

Tap into learning—NOW!

Visit **www.informit.com/shortcuts** for a complete list of Short Cuts.



Chapter 4

AAA Configurations

AAA Overview

You should familiarize yourself with a few different configurations that involve user authentication of traffic through the security appliance but also administrative access to the security appliance. These configurations are accomplished using authentication, authorization, and accounting (AAA).

The basics of AAA are simple. The first step in AAA is authentication. When you authenticate users, you are just verifying that they are who they say they are. After a user has been authenticated, you then can optionally authorize what that user does. As this is happening, you might also want to track these happenings. This is the accounting process. The following sections detail each.

Authentication

Authentication is the process of verifying the identity of users who are requesting access to either a network resource using a protocol such as TACACS+ to communicate information to a remote authentication server or by using a local database of usernames stored in the configuration of the security appliance. You can authenticate for the following:

- Access to the security appliance
- Access through the security appliance using cut-through proxy
- IPsec and Secure Sockets Layer virtual private networking tunnel access

 Please see page 139 for more details.

Authorization

Once authenticated, users can be authorized for more-specific services; for example, a user may be authenticated as a valid network user but only authorized for web surfing and not other protocols such as FTP or Telnet. You can authorize for the following:

- **Console access**: This method specifies whether command execution is subject to authorization.
- **Cut-through proxy**: This method specifies what "through" services are subject to authorization.
- **Tunnel access**: This method specifies which "tunnel" services are authorized.

Accounting

The accounting process simply relates the activity that has occurred to a database that can later be referenced. You can account for the following:

- Security appliance console access
- Access through the security appliance using cut-through proxy
- IPsec and Secure Sockets Layer virtual private networking tunnel connections

Local AAA

Local AAA means that you are performing AAA without the use of an external database. When performing local AAA, you can authenticate with a username and password that is part of the configuration of the security appliance. It's common to perform local authentication for security appliance console access methods, such as the following:

- Telnet console access
- Serial console access
- SSH console access

- Enable mode access
- HTTP access for ASDM

You can also perform local authentication for cut-through proxy operations. The types of cut-through proxy user authentications include the following:

- Telnet traffic
- FTP traffic
- HTTP traffic
- HTTPS traffic

This means you can authenticate a user when he passes Telnet, FTP, HTTP, or HTTPS traffic through the security appliance. You may run into situations in which a user needs to pass other types of traffic through the firewall while performing cut-through proxy authentication. In these cases, you can either have the user telnet, FTP, HTTP, or HTTPS first, or you can set up a virtual Telnet address. With Virtual Telnet, the user needs to first telnet to the Virtual Telnet IP address and authenticate. Once authenticated, the user can then pass other types of traffic without needing to authenticate again.

Configuring local users

To begin a local authentication configuration, you need to create the local database. To do so, use the **username** command. The syntax is as follows:

```
username username {nopassword ¦ password password [mschap ¦ encrypted ¦ nt-encrypted]} [privilege level]
```

You can see from the syntax that much of it is optional. To create a simple user bcarroll with the password cisco123, enter the following:

```
MyAsa(config)# username bcarroll password cisco123
```

 Please see page 139 for more details.

Telnet authentication

To enable authentication for users who telnet into the security appliance, enter the following:

```
MyASA(config)# aaa authentication telnet console LOCAL
```

This command instructs the security appliance to authenticate Telnet connections to the LOCAL database. If you don't use this AAA configuration for Telnet authentication and Telnet is enabled, the password is configured using the **passwd** command. When you do it this way, you are not prompted for a username.

SSH auth

To enable authentication for users that Secure Shell into the security appliance, enter the following:

```
MyASA(config)# aaa authentication ssh console LOCAL
```

This command instructs the security appliance to authenticate Secure Shell (SSH) connections to the LOCAL database.

HTTP auth

To enable authentication for users who use ASDM to manage the security appliance, enter the following:

```
MyASA(config)# aaa authentication http console LOCAL
```

This command instructs the security appliance to authenticate HTTP connections to the LOCAL database. Although the command uses the keyword **http** to access the security appliance with ASDM, you initially make an HTTPS connection.

 Please see page 139 for more details.

Enable auth

After you have connected to the security appliance via the console port, SSH, or Telnet, you need to access the enable mode. With the default configuration, you are prompted for a password but none is set. You can configure an enable password and use it, essentially using a "local" entry; if you truly want to use the LOCAL database, however, you will use the command as follows:

```
MyASA(config)# aaa authentication enable console LOCAL
```

This command instructs the security appliance to authenticate users to the LOCAL database. Instead of being prompted for just a password you are prompted for both a username and a password.

Verifying the LOCAL database

To verify the configuration of the LOCAL database, use the **show aaa-server LOCAL** command:

```
MyAsa# show aaa-server LOCAL
Server Group:  LOCAL
Server Protocol: Local database
Server Address: None
Server port:   None
Server status:  ACTIVE, Last transaction at 15:38:37 UTC Wed Dec 1 2005
Number of pending requests       0
Average round trip time         0ms
Number of authentication requests    1
Number of authorization requests    0
Number of accounting requests      0
Number of retransmissions        0
Number of accepts             1
```

 Please see page 139 for more details.