



## Introduction

The *Cisco IOS Security Command Reference* contains commands that are used to configure Cisco IOS security features for your Cisco networking devices; specifically, it contains commands used to perform the following functions:

- Configure authentication, authorization, and accounting (AAA).
- Configure security server protocols such as RADIUS, TACACS+, and Kerberos.



### Note

TACACS and Extended TACACS commands are included in Cisco IOS Release 12.2 software for backward compatibility with earlier Cisco IOS releases; however, these commands are no longer supported and are not documented for this release.

Cisco recommends using only the TACACS+ security protocol with Release 12.1 and later of Cisco IOS software.

[Table 1](#) identifies Cisco IOS software commands available to the different versions of TACACS. Although TACACS+ is enabled through AAA and uses commands specific to AAA, there are some commands that are common to TACACS, Extended TACACS, and TACACS+. TACACS and Extended TACACS commands that are not common to TACACS+ are not documented in this release.

**Table 1** TACACS Command Comparison

| Cisco IOS Command                 | TACACS | Extended TACACS | TACACS+ |
|-----------------------------------|--------|-----------------|---------|
| aaa accounting                    | —      | —               | yes     |
| aaa authentication arap           | —      | —               | yes     |
| aaa authentication enable default | —      | —               | yes     |
| aaa authentication login          | —      | —               | yes     |
| aaa authentication ppp            | —      | —               | yes     |
| aaa authorization                 | —      | —               | yes     |
| aaa group server tacacs+          | —      | —               | yes     |
| aaa new-model                     | —      | —               | yes     |
| arap authentication               | —      | —               | yes     |
| arap use-tacacs                   | yes    | yes             | —       |
| enable last-resort                | yes    | yes             | —       |

**Table 1** TACACS Command Comparison (continued)

| <b>Cisco IOS Command</b>              | <b>TACACS</b> | <b>Extended TACACS</b> | <b>TACACS+</b> |
|---------------------------------------|---------------|------------------------|----------------|
| <b>enable use-tacacs</b>              | yes           | yes                    | —              |
| <b>ip tacacs source-interface</b>     | yes           | yes                    | yes            |
| <b>login authentication</b>           | —             | —                      | yes            |
| <b>login tacacs</b>                   | yes           | yes                    | —              |
| <b>ppp authentication</b>             | yes           | yes                    | yes            |
| <b>ppp use-tacacs</b>                 | yes           | yes                    | no             |
| <b>server</b>                         | —             | —                      | yes            |
| <b>tacacs-server administration</b>   | —             | —                      | yes            |
| <b>tacacs-server directed-request</b> | yes           | yes                    | yes            |
| <b>tacacs-server dns-alias-lookup</b> | —             | —                      | yes            |
| <b>tacacs-server host</b>             | yes           | yes                    | yes            |
| <b>tacacs-server key</b>              | —             | —                      | yes            |
| <b>tacacs-server packet</b>           | —             | —                      | yes            |
| <b>tacacs-server timeout</b>          | yes           | yes                    | yes            |

- Configure the following traffic filtering and firewall features:
  - Context-Based Access Control (CBAC)
  - Intrusion Detection System (IDS)
  - Port to application mapping (PAM)
  - Reflexive access lists
  - TCP Intercept
- Configure IP Security (IPSec) and encryption features such as public key infrastructure (PKI) and Internet Key Exchange (IKE).
- Configure additional security features such as passwords and privileges, IP Security Options (IPSO), Unicast Reverse Path Forwarding (uRPF), secure shell (SSH), and AutoSecure.

For information on how to configure Cisco IOS security features and configuration examples using the commands in this book, refer to the *Cisco IOS Security Configuration Guide*.