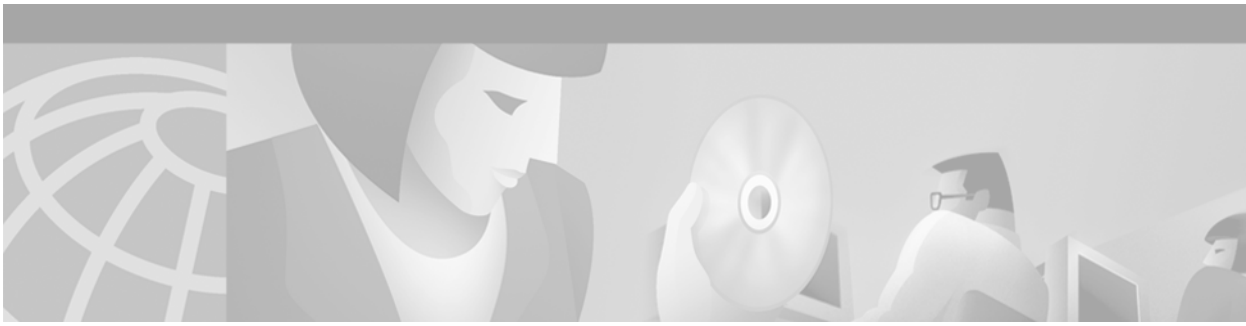

Preface

This case study describes various Cisco-based security and accounting capabilities for monitoring and managing access within a large-scale dial environment.

Purpose

This Internetworking Solutions Guide (ISG) case study provides examples intended to be models for building an effective, Cisco AAA-based security environment for dial-based and router environments. In following the procedures and recommendations provided in this document, readers should be able to:

- Understand the working relationship among various Cisco AAA components, including NASs, AAA servers, and the AAA database.
- Configure and verify operation for these AAA components.
- Troubleshoot typical problems found in AAA environments.

Audience

The audience for this document consists of network engineers supporting large-scale dial networks. The audience is expected to have a basic understanding of Cisco IOS software, and a working knowledge of both the UNIX operating system and CiscoSecure for UNIX user interface.

Scope

This case study provides:

- Complete network device configurations and specific fragments to support implementation task descriptions.
- Example diagnostic output showing verification of correct configuration.
- Troubleshooting output supporting problem scenarios show problem configurations and other AAA environment failures.
- A foundation from which effective AAA-based security solutions can be tailored to specific network requirements.

The information provided here does not include advanced tuning tips—nor does it provide a primer for the uninitiated novice. In addition, site planning and preparation are beyond the scope of this case study.

Related Documentation and Sites

The following URLs provide the essentials for preparing to install Cisco Secure for UNIX and NT:

- CiscoSecure ACS for UNIX

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx

- CiscoSecure ACS for NT

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/csnt23

- Oracle database implementation

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/csinstl.htm

Software Used in This Case Study

The features and capabilities described in this case require these software versions:

- Cisco IOS 12.0(7)T
- OS Solaris 2.5(1)
- CiscoSecure for UNIX 2.3(3)
- Oracle DB Server 7.3(4)
- Oracle DB Client 7.3(4)
- SQL*Plus: Release 3.3.4.0.1

To identify other software versions that might apply, please contact your Cisco customer service representative.

Hardware Used in This Case Study

This case is built on a production environment consisting of a single authentication, authorization, and accounting (AAA) server, an Oracle-based AAA database, a Cisco network access server (NAS), and a router. The diagnostic captures and system configurations provided in this case study were derived from the following systems:

- Cisco AS5300 or Cisco AS5800 network access server (NAS)
- Cisco 7206 VXR router
- Sun Microsystems server (UltraSPARC Enterprise 2 Model)
  - Two 200 MHz processors
  - One GB RAM
  - One internal 4.2 GB disk drive
  - CD-ROM drive

The system used as a platform for CiscoSecure ACS for UNIX 2.3 must meet with the minimum system specifications described in the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/instl23.htm

Document Conventions

Convention	Description
italic	File names, paths to files, user names, and groups names used in descriptions. Example: */var/log/csuslog*
< >	Angle brackets show nonprinting characters, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)
[ ]	Square brackets show default responses to system prompts.

Command Syntax Conventions

Convention	Description
bold	Command or keyword that you must enter. This format is used for commands, paths to files, and file names when used within an example illustrating required input.
italic	Argument for which you supply a value.
[x]	Optional keyword or argument that you enter.
{x | y | z}	Required keyword or argument that you must enter.
[x {y | z}]	Optional keyword or argument that you enter with a required keyword or argument.
string	Set of characters that you enter. Do not use quotation marks around the character string, or the string will include the quotation marks.
`screen`	Information that appears on the screen.
→	Important line of text in an example.
^ or Ctrl	Control key—for example, ^D means press the Control and the D keys simultaneously.
< >	Nonprinting characters, such as passwords.
!	Comment line at the beginning of a line of code.

Cisco Connection Online

Cisco Connection Online (CCO) is the primary, real-time support channel for Cisco Systems. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to customers and business partners of Cisco Systems. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- http://www.cisco.com
- http://www-europe.cisco.com
- http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of the CCO Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

If you are a network administrator and need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact the Cisco Technical Assistance Center (TAC). Information for contacting TAC can be found at:

http://www.cisco.com/web/about/ac49/ac162/about_cisco_customer_service_contacts.html

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly; therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Providing Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can also submit feedback on Cisco documentation as follows:

- Mail in the Cisco Reader Comment Card located at the front of this book
- Send an e-mail to bug-doc@cisco.com

- Send a fax to 408 527-8089

We appreciate your comments.

Acknowledgements

This ISG case study was created as a collaborative effort. The following team members participated in the creation of this document: Joellen Amato, Dave Anderson, Robert “Bob” Brown, Alan Dowling, Dianne Dunlap, Paul Hafeman, Anthony Hall, Kim Lew, Robert Lewis, Dave Leyland, Brian Murphy, Dang Nguyen, Nilesh Panicker, Anjali Puri, Robert Sargent, David Sims, Tim Stevenson, Kris Thompson, Craig Tobias, and Syed Atif Ullah.