



Cisco Secure Telnet

This chapter provides information about Cisco Secure Telnet and contains the following topics:

- [System Design, page 16-2](#)
- [Remote Access Methodology, page 16-2](#)
- [Firewall Protection, page 16-2](#)
- [Cisco Secure Telnet Design, page 16-2](#)
- [Cisco Secure Telnet Structure, page 16-3](#)
- [Cisco Secure Telnet Configuration Checklist, page 16-4](#)
- [Where to Find More Information, page 16-5](#)

Cisco Secure Telnet offers Cisco Service Engineers (CSE) transparent firewall access to Cisco CallManager servers on your site.

Cisco Secure Telnet works by enabling a Telnet client inside the Cisco Systems firewall to connect to a Telnet daemon behind your firewall. This secure connection allows remote monitoring and maintenance of your Cisco CallManager servers without requiring firewall modifications.



Note

Cisco accesses your network only with your permission. You must provide a network administrator at your site to help initiate the process.

System Design

The Cisco Secure Telnet system design provides the basis for communication with any Cisco CallManager installations on your site.

These paragraphs describe each component and application, along with a scenario outlining how you can use them.

Remote Access Methodology

CSEs can use techniques other than Cisco Secure Telnet to provide remote connectivity to a customer site, but using other methods may impose unacceptable conditions.

Dial-in access requires installation of a dedicated phone line and modem at your site, so dial-in access may be impractical. Using Telnet directly can establish a TCP/IP connection, but it requires opening your firewall, which can compromise security and cause delays in service.

Firewall Protection

Virtually all internal networks use firewall applications to restrict outside access to internal host systems. These applications protect your network by restricting IP connections between the network and the public internet.

Firewalls work by automatically blocking TCP/IP connections that are initiated from the outside, unless the software is reconfigured to allow such access.

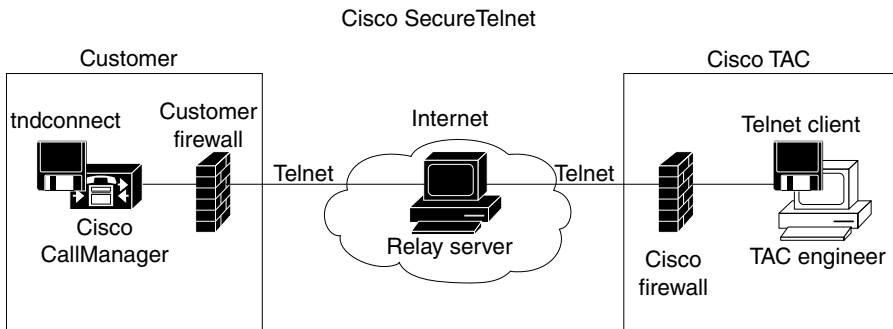
Corporate networks normally permit communication with the public Internet but only if connections directed to outside hosts originate from inside the firewall.

Cisco Secure Telnet Design

Cisco Secure Telnet takes advantage of the fact that Telnet connections can easily be initiated from behind a firewall. Using an external proxy machine, the system relays TCP/IP communications from behind your firewall to a host behind another firewall at the Cisco Technical Assistance Center (TAC).

Using this relay server maintains the integrity of both firewalls while supporting secure communication between the shielded remote systems. (See [Figure 16-1](#).)

Figure 16-1 Cisco Secure Telnet System



34433

Cisco Secure Telnet Structure

The external relay server establishes the connection between your network and Cisco Systems by building a Telnet tunnel. This enables you to transmit the IP address and password identifier of your Cisco CallManager server to your CSE.



Note

The password comprises a text string upon which your administrator and the CSE mutually agree.

Your administrator starts the process by initiating the Telnet tunnel, which establishes a TCP connection from inside your firewall out to the relay server on the public Internet. The Telnet tunnel then establishes another connection to your local Telnet server, creating a two-way link between the entities.



Note

The Telnet client at the Cisco TAC runs in compliance with systems running on Windows NT and Windows 2000 or with UNIX operating systems.

After the Cisco CallManager at your site accepts the password, the Telnet client that is running at the Cisco TAC connects to the Telnet daemon that is running behind your firewall. The resulting transparent connection allows the same access as if the machine were being used locally.

After the Telnet connection is stable, the CSE can implement all remote serviceability functionality to perform maintenance, diagnostic, and troubleshooting tasks on your Cisco CallManager server.

You can view the commands sent by the CSE and the responses issued by your Cisco CallManager server, but the commands and responses may not always be completely formatted.

Cisco Secure Telnet Configuration Checklist

Table 16-1 provides an overview of the steps for configuring Cisco Secure Telnet.

Table 16-1 Cisco Secure Telnet Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Obtain the Cisco Secure Telnet components.	Cisco Secure Telnet Components , <i>Cisco CallManager Serviceability Administration Guide</i>
Step 2	Obtain the Cisco Secure Telnet applications.	Cisco Secure Telnet Applications , <i>Cisco CallManager Serviceability Administration Guide</i>
Step 3	Invoke the <code>tnconnect</code> program.	Cisco Secure Telnet Executables , <i>Cisco CallManager Serviceability Administration Guide</i>
Step 4	Use the <code>tnconnect</code> commands to access the Cisco CallManager servers.	Command Line Syntax for <code>tnconnect</code> , <i>Cisco CallManager Serviceability Administration Guide</i>

Where to Find More Information

Related Topic

- [Chapter 29, “Cisco Secure Telnet Configuration,”](#) *Cisco CallManager Serviceability Administration Guide*

Additional Cisco Documentation

- *Troubleshooting Guide for Cisco CallManager*

■ Where to Find More Information