Content Security FAQ: How do you access the CLI on a Content Security appliance?

Document ID: 117914

Contributed by Chris Haag, Cisco TAC Engineer.
Jul 11, 2014

Contents

Introduction
Prerequisites
Requirements
Components Used
How do you access the CLI on a Content Security appliance?

Introduction

This document describes how to access the CLI through a Telnet or Secure Shell (SSH) client on a Cisco Content Security appliance.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Email Security Appliance (ESA)
- Cisco Web Security Appliance (WSA)
- Cisco Security Management Appliance (SMA)
- AsyncOS

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ESA AsyncOS, all Versions
- Cisco WSA AsyncOS, all Versions
- Cisco SMA Versions AsyncOS, all Versions

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Note: This document references software that is not maintained or supported by Cisco. The information is provided as a courtesy for your convenience. For further assistance, please contact the software vendor.

How do you access the CLI on a Content Security appliance?

You can access the CLI of your appliance with a Telnet client or an SSH client. However, the Telnet protocol is unencrypted, so when you log into your appliance through Telnet, your credentials can more easily be stolen.

Cisco recommends that all production machines use an SSH client. Additionally, the standard Microsoft Windows Telnet client is difficult to use. By factory default, Telnet is configured on the Management port.

Complete these steps in order to disable Telnet:

1. Log into the web GUI.

2. Navigate to ***Network > IP Interfaces***.

3. Click the name of the interface that you want to edit.

4. Uncheck the ***Telnet*** check box in the Services field.

Complete these steps in order to access your appliance through SSH (port 22):

1. Install an SSH client in Microsoft Windows, such as PuTTY.

2. Launch the SSH client:

   A. Add the host information for your appliance (such as ***c650.example.com***).

   B. Click ***Load***.

   C. Enter your user name.

   D. Enter your password.

3. Open a command prompt with ****nix***.

4. Enter the ***$ ssh exampleC650.com*** command.

5. If you need to specify a different user, enter the ***$ ssh <user>@exampleC650.com*** command. If the user name is ***admin***, enter the ***$ ssh admin@C650.example.com*** command.

Complete these steps in order to access your appliance through Telnet:

Note: Cisco recommends that you use an SSH client for access; the use of Telnet is not recommended.

1. Open a command prompt.

2. Enter the ***telnet c650.example.com*** command.

3. Enter your user name.

4. Enter your password.

Updated: Jul 11, 2014 Document ID: 117914