

ACS Solution Engine Does Not Respond to Pings

Document ID: 71068

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Background Information

Problem

Solution

- Check TCP Port 2002

[NetPro Discussion Forums – Featured Conversations](#)

Related Information

Introduction

In the course of typical network administration, it is common to attempt to ping the Cisco Secure Access Control Server (ACS) Solution Engine in order to determine if the appliance is up and reachable. However, these pings fail due to enhanced security restrictions in place on the appliance.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Secure ACS Solution Engine.

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.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The Cisco Secure ACS Solution Engine, also known as the Cisco Secure ACS Appliance, is based on Microsoft Windows, and therefore is vulnerable to PMTUD attacks and to attacks based on ICMP "hard" error messages. Such attacks are detailed in the [Crafted ICMP Messages Can Cause Denial of Service](#) security advisory.

Recent versions of the Cisco Secure ACS Solution Engine ship with Cisco Security Agent (CSA), which is configured to block all incoming ICMP messages. Under this situation, the Cisco Secure ACS Solution Engine is not vulnerable to any of the attacks that this document describes.

Problem

The Cisco Secure ACS Solution Engine does not respond to pings like a normal, Windows-based Cisco Secure ACS server.

Solution

The failure of the Cisco Secure ACS Solution Engine to respond to pings is the result of the rule set applied to the CSA installed on the appliance.

In order to allow ping on your ACS Solution Engine, you need to disable the CSA. This can be done via the System Configuration > Appliance Configuration menu. There is an option to disable or enable the CSA. If you disable this agent, you can then ping the appliance.

Note: Disable CSA only if you want to verify the pings to work.

Check TCP Port 2002

Instead of monitoring the status of the appliance with the use of ICMP, you can verify it is up and reachable when you connect to the appliance on TCP port 2002. Telnet to the appliance on port 2002 and press **Enter**. You should see the error: **HTTP 500 Internal Server Error**

This is an example of this procedure performed at the Windows command line:

```
C:\>telnet 172.18.124.101 2002 <enter>
<enter>

HTTP/1.0 500 Internal Server Error

Connection to host lost.

C:\>
```

Additionally, you can download several free TCP ping-type utilities from the Internet that attempt to connect to a host on any TCP port and report back if the host responds.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Crafted ICMP Messages Can Cause Denial of Service](#)
 - [Cisco Secure Access Control Server Solution Engine](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 25, 2006

Document ID: 71068
