

PIX Performance Issues Caused by IDENT Protocol

Document ID: 6370

Contents

Introduction

Prerequisites

Requirements

Components Used

Conventions

IDENT Protocol

Symptoms

Troubleshoot

Fix the Problem

Related Information

Introduction

If you go through a PIX Firewall in order to use Telnet, FTP, HTTP, or POP, you might occasionally notice that it takes a long time to connect to a server, or you might not be able to access the server you want at all.

The two probable causes for this are lack of reverse Domain Name Service (DNS) entries (refer to Poor or Intermittent FTP/HTTP Performance Through a PIX) or issues related to the use of the IDENT protocol, which are discussed in this document.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- PIX Firewall Software Releases through 6.3

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.

IDENT Protocol

The IDENT protocol is sometimes used by Telnet, POP mail, FTP, and HTTP servers to identify incoming users.

When a user requests a service, the server tries to initiate an IDENT connection back toward the client behind the firewall to identify the username of the process that initiates the connection. The PIX intercepts this IDENT connection and silently drops it. Therefore, the server never receives its expected response and it might not allow the user to connect.

Most users consider the IDENT protocol a security violation because it can allow an outsider to gain confidential knowledge of your secured network.

Symptoms

These symptoms can indicate that the IDENT protocol causes problems:

- Inability to establish a connection to a particular server, usually Telnet, FTP, HTTP or POP.
- Long waits to connect to a particular Telnet, FTP, HTTP, or POP server. Once connected, response times are normal.
- Poor performance once a connection is established.

Troubleshoot

Complete these steps to troubleshoot.

1. Set your logging to debugging level with the **logging trap debugging** command (for PIX Software versions 4.2 and later).
2. If you have configured a host for syslog, use the **logging host [in_if_name] ip_address** command to send syslog output to that host.
3. Read through the syslog output. Look for "deny TCP inbound" messages where the destination port to one of the internal (affected) machines is 113, which is IDENT. A sample of the TCP log is shown below.

```
%PIX-2-106001: Inbound TCP connection denied from 10.64.10.2/35969
to1132f1ag#18Y79/
```

4. If you do not see any "deny" messages as described, try this step. From the outside of the firewall, use **nslookup** to see if you can resolve addresses in your global pool. If you cannot, your host IP addresses might not be registered in the DNS. Refer to Poor or Intermittent FTP/HTTP Performance Through a PIX for more information.

Fix the Problem

- Contact the administrator of the server your users are trying to reach and see if that person can turn the IDENT facility off.

Or,

- Configure the PIX with the **service resetinbound** command, available in PIX Software versions 4.2 and later. Normally, the PIX silently drops inbound connection attempts that are not permitted. When the PIX is configured with the **service resetinbound** command, the PIX sends an RST to unpermitted connection attempts. When the IDENT service receives an RST, it is notified that the IDENT service is unavailable for that client, and continues to process the original traffic that spawned the IDENT request. This significantly decreases the delay for IDENT processing.

Or,

- Use the **established** command with the **permitto tcp 113** options. (Read the caution first!)



Caution: It can be considered a security risk if you allow port 113 traffic. Consult the security policy of your site before you implement the **established** command or add static/conduit or static/access list pairs.

Related Information

- [PIX Command Reference](#)
 - [PIX 500 Series Security Appliances Product Support Page](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

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

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 26, 2008

Document ID: 6370
