

# Poor or Intermittent FTP/HTTP Performance Through a PIX

Document ID: 13810

## Contents

### Introduction

#### Prerequisites

- Requirements

- Components Used

- Conventions

#### Symptoms

#### Troubleshooting

#### Fixing the Problem

#### Verify

#### Related Information

## Introduction

When trying to download files with FTP or access external sites on the worldwide web from behind the PIX Firewall, network users may experience poor or intermittent performance. This can occur because host IP addresses in the global pool (or internal host IP addresses, if you are using Network Address Translation [NAT] 0) are not properly registered in the Domain Name System (DNS).

## Prerequisites

### Requirements

There are no specific prerequisites for this document.

### Components Used

This document is not restricted to specific software and hardware versions.

### Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

## Symptoms

Some symptoms of poor performance include the following.

- A user can connect to an FTP site, but cannot execute any commands (such as **LS**, **PUT**, or **GET**).
- FTP performance is extremely slow.
- File transfers being performed using FTP will reach only n%, at which point the transfer will halt without being completed.
- A user may not be able to access certain web sites.

**Note:** These symptoms may also be caused by the IDENT protocol.

# Troubleshooting

Use **nslookup** to resolve a random number from your global pool. If you are using NAT 0, try to resolve your actual host IP addresses. The error message `No host/domain` usually indicates a lack of reverse DNS entries. If you do successfully resolve to a name, please refer to [PIX Performance Issues Caused by IDENT Protocol \(Port 113\)](#).

In PIX software versions earlier than 4.2.x, syslog at 20.7 may show deny messages, even though the hosts in question are not being blocked by access lists, authentication, license count, and so on. In PIX software versions 4.2.x or later, the **logging facility 20** and **logging trap debugging** commands may show similar deny messages.

## Fixing the Problem

In the primary DNS for the domain, make sure there is a Pointer (PTR) record for each IP address, either those in a global pool or the ones that pass through via NAT 0. (These records are also known as **in-addr.arpa** entries.)

## Verify

Once PTR records have been entered, an **nslookup** run on an IP address should resolve to a name.

---

## Related Information

- [Understanding the Domain Name System](#)
- [DNS Resource Records](#)
- [PIX Support Page](#)
- [Documentation for PIX Firewall](#)
- [PIX Command References](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support – 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: Jan 17, 2005

Document ID: 13810

---