

# Table of Contents

<b><u>Blocking Peer-to-Peer File Sharing Programs with the PIX Firewall</u></b> .....	1
<u>Introduction</u> .....	1
<u>Prerequisites</u> .....	1
<u>Requirements</u> .....	1
<u>Components Used</u> .....	1
<u>Conventions</u> .....	2
<u>PIX Configuration</u> .....	2
<u>Blubster/Piolet Configuration</u> .....	2
<u>eDonkey Configuration</u> .....	2
<u>FastTrack – Kazaa/KazaaLite/Grokster/iMesh Configuration</u> .....	3
<u>Gnutella – BearShare/Limewire/Morpheus/ToadNode Configuration</u> .....	3
<u>Related Information</u> .....	4

# Blocking Peer-to-Peer File Sharing Programs with the PIX Firewall

---

## Introduction

### Prerequisites

Requirements

Components Used

Conventions

### PIX Configuration

#### Blubster/Piolet Configuration

#### eDonkey Configuration

#### FastTrack – Kazaa/KazaaLite/Grokster/iMesh Configuration

#### Gnutella – BearShare/Limewire/Morpheus/ToadNode Configuration

### Related Information

---

## Introduction

This document demonstrates how to (attempt to) block the most common peer-to-peer (P2P) file sharing programs with the PIX firewall. If the application cannot effectively be blocked with the PIX, Cisco IOS® Network-Based Application Recognition (NBAR) configurations are included that can be configured on any Cisco router between the source host and the Internet.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The following configurations were tested using the following PIX software and hardware versions, although they should work on any hardware and software revision:

- Cisco PIX Firewall 501
- Cisco PIX Firewall Software version 6.3(3)

The following configurations were tested using the following P2P software versions:

- Blubster version 2.5
- eDonkey version 0.51
- iMesh version 4.2 build 137
- KazaaLite version 2.4.3
- LimeWire version 3.6.6
- Morpheus version 3.4

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

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

## PIX Configuration

```
interface ethernet0 10baset
interface ethernet1 10full
ip address outside dhcp setroute
ip address inside 192.168.1.1 255.255.255.0
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.129 inside
dhcpd auto_config
dhcpd enable inside
pdm logging informational
timeout xlate 0:05:00
```

## Blubster/Piolet Configuration

Blubster and Piolet use the Multipoint P2P (MP2P) protocol, which initially connects to the networks' central servers to gain the list of peer hosts, so this can be blocked effectively with an access list, therefore disabling the program. P2P connections are usually on TCP port 80, but if the initial connection is blocked this peer list cannot be downloaded.

Applying the following on your PIX should block this program:

```
access-list outbound deny tcp any 128.121.0.0 255.255.0.0 eq www
access-list outbound permit ip any any
access-group outbound in interface inside
```

Alternatively, if you want to be a little bit more selective, the following *should* also work:

```
access-list outbound deny tcp any 128.121.20.0 255.255.255.240 eq www
access-list outbound deny tcp any 128.121.4.0 255.255.255.0 eq www
access-list outbound permit ip any any
access-group outbound in interface inside
```

## eDonkey Configuration

eDonkey uses two ports, one for file searches and one for file transfers. File searches are done using a randomly picked UDP source port to a random destination port. File transfers however are done using a destination port of TCP/4662. Blocking this port stops file downloads, although users are still able to search for files as the UDP portion of this program cannot be blocked effectively with an access list.

The default port of TCP/4662 can be changed simply within the program options, but this does not affect the port that files are downloaded on. This port number option seems to be the port that other hosts would use to download files from your source host, so unless a large number of other P2P users have changed this port in their settings, which is doubtful, file downloads will be stopped (or at the very least severely impacted) just by blocking TCP/4662 outbound.

Applying the following on your PIX should block this program:

```
access-list outbound deny tcp any any eq 4662
access-list outbound permit ip any any
access-group outbound in interface inside
```

## FastTrack – Kazaa/KazaaLite/Grokster/iMesh Configuration

FastTrack is the most popular P2P network around today. P2P file sharing applications such as Kazaa, KazaaLite, Grokster and iMesh all use this network and connect to other hosts using any open TCP/UDP port to search and download files, making filtering them with an access list impossible.

**Note:** These applications cannot be filtered with a PIX firewall.

To effectively filter these applications, use NBAR on your outside router (or any router between the source host and the Internet connection). NBAR can match specifically on connections made to the FastTrack network and can either be dropped completely or rate-limited.

A sample IOS-router NBAR configuration to drop FastTrack packets appear as shown below:

```
class-map match-any p2p
  match protocol fasttrack file-transfer *

policy-map block-p2p
  class p2p
    drop

int FastEthernet0
  description PIX-facing interface
  service-policy input block-p2p
```

## Gnutella – BearShare/Limewire/Morpheus/ToadNode Configuration

Gnutella is an open source protocol and as such has over 50 applications using it on a wide variety of operating systems. Popular P2P applications include BearShare, Limewire, Morpheus and ToadNode. They use any open TCP/UDP port to communicate with another P2P host, and from there connect to many other hosts, making filtering these programs with an access-list impossible.

**Note:** These programs cannot be filtered with a PIX firewall.

To effectively filter these protocols, use NBAR on your outside router. NBAR can match specifically on connections made to the Gnutella network and can either be dropped completely or rate-limited.

A sample IOS-router NBAR configuration looks like the example in the FastTrack section above, and adding a Gnutella-matching line under the same class-map as follows:

```
class-map match-any p2p
  match protocol gnutella file-transfer *
```

---

## Related Information

- [Classification of Peer-to-Peer File-Sharing Applications](#)
  - [IPSec Support Page](#)
  - [PIX Support Page](#)
  - [Documentation for PIX Firewall](#)
  - [PIX Command References](#)
  - [Requests for Comments \(RFCs\)](#)
  - [Technical Support – Cisco Systems](#)
- 

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.