

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

Document ID: 42700

Contents

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 describes 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.

Important Note: Due to the nature of the content this document assists in blocking, Cisco is unable to block individual server addresses. Instead, Cisco recommends that you block address ranges in order to ensure you block all possible servers for each of the listed programs. The result of this can be that you block access to legitimate services. If this is the case, you need to add statements to the configuration that permit these individual services. Contact Cisco Technical Support if you have any difficulty.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

These configurations were tested with the use of these PIX software and hardware versions, although they are expected to work on any hardware and software revision:

- Cisco PIX Firewall 501
- Cisco PIX Firewall Software version 6.3(3)
- Cisco IOS Software Release 12.2(13)T

These configurations were tested with the use of these 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

Refer to the Cisco Technical Tips Conventions for more information on document 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. This initially connects to the central servers of the networks in order to gain the list of peer hosts and can be blocked effectively with an access list, therefore disabling the program. P2P connections are usually on TCP port 80. However, if the initial connection is blocked, you cannot download this peer list.

Applying these 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, this *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 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 use to download files from your source host. Unless a large number of other P2P users have changed this port in their settings, which is doubtful, file downloads are stopped (or at the very least severely impacted) just by blocking TCP/4662 outbound.

Applying these 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. This makes filtering them with an access list impossible.

Note: These applications cannot be filtered with a PIX Firewall.

In order 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 here:

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

policy-map block-p2p
  class p2p
    drop

!--- The drop command was introduced in
!--- Cisco IOS Software Release 12.2(13)T.

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

If the router runs a Cisco IOS Software earlier than Cisco IOS Software Release 12.2(13)T, then the **drop** command under the policy-map is not available. In order to drop this traffic, use a policy-map to set the DSCP bit in matching packets as they come into the router. Next, define an access list to drop all packets with this bit set as they exit the router. The DSCP bit is used as it is unlikely that any "normal" traffic uses this. A sample configuration for this is shown here:

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

policy-map block-p2p
  class p2p
    set ip dscp 1

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

```
int Serial0
  description Internet/Outside facing interface
  ip access-group 100 out

access-list 100 deny ip any any dscp 1
access-list 100 permit ip any any
```

Gnutella – BearShare/Limewire/Morpheus/ToadNode Configuration

Gnutella is an open source protocol and 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.

Use NBAR on your outside router to effectively filter these protocols. 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 of this document. The addition of a Gnutella-matching line under the same class-map is shown here:

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

Related Information

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

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

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 14, 2006

Document ID: 42700
