

Блокируем клиентов P2P сетей при помощи Cisco PIX Firewall.

Вступление

В данной статье рассмотрены методы блокирования распространённых peer-to-peer (P2P) клиентов (программ) при помощи Cisco PIX Firewall. Если приложение не возможно заблокировать посредством Cisco PIX Firewall, то можно воспользоваться технологией Cisco IOS® Network-Based Application Recognition (NBAR), конфигурация которой может применяться на маршрутизаторах Cisco между клиентами локальной подсети и интернет.

Важное примечание: Из-за особенностей содержания данного документа, описывающего методы блокирования определённого трафика, оборудование Cisco не может блокировать индивидуальные серверные адреса. Взамен этого, Cisco рекомендует блокировать пул адресов, для более надёжного контроля над требуемыми программами.

Используемые компоненты

Конфигурация в данной статье тестировалась с использованием следующего оборудования и ПО:

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

Конфигурация тестировалась на следующих клиентах P2P:

- 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

Информация в данном документе была собрана посредством лабораторных работ в тестовой среде. Все устройства были с заводскими установками. Прежде чем использовать данные из этой статьи в рабочей сети убедитесь в том, что Вы осознаёте все действия.

Конфигурация PIX

```
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
```

Конфигурация Blubster/Piolet

Клиентское ПО Blubster и Piolet использует протокол Multipoint P2P (MP2P). Он инициирует соединения с центральными серверами в сети для получения списка клиентских хостов. Доступ к данному списку мы можем заблокировать, используя списки доступа (access list), тем самым блокируя доступ клиентскому ПО. Соединения P2P обычно используют 80 TCP порт. В связи с этим, если инициирующее соединение было заблокировано, то список клиентских хостов не будет загружен клиентом.

Примените следующую конфигурацию к Вашему Cisco PIX для блокирования данных программ (Blubster и Piolet):

```
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
```

Альтернативно, Вы можете заблокировать более расширенный диапазон адресов:

```
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
```

Конфигурация eDonkey

eDonkey использует два порта - один для поиска файлов другой для трансфера (переноса) файлов. Для поиска файлов используется случайно выбранный исходный UDP порт к случайно выбранному UDP порту назначения. Для переноса файлов используется TCP порт назначения с номером 4662. Блокирование данного порта предотвратит загрузку файлов. В тоже время, пользователи могут искать файлы, и поиск не может быть заблокирован посредством списков доступа.

Стандартный порт TCP/4662 может быть изменён пользователем посредством опции в программе, но это не будет распространяться на порт хоста предоставляющего доступ к загрузке файлов. Данный порт используется для предоставления доступа к загрузке файлов для других пользователей. Если большое количество других пользователей P2P изменили этот порт в настройках, что сомнительно, загрузка файлов прекратится из-за того, что был заблокирован исходящий 4662 TCP порт.

Примените следующую конфигурацию к Вашему Cisco PIX для блокирования данной программы (eDonkey):

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

Конфигурация FastTrack - Kazaa/KazaaLite/Grokster/iMesh

FastTrack на сегодняшний день самая распространённая P2P сеть. Клиенты P2P предоставления общего доступа к файлам, такие как Kazaa, KazaaLite, Grokster и iMesh все используют сетевые подключения для поиска и передачи файлов любой свободный TCP/UDP порт. Это означает, что использование списков доступа для блокирования данных клиентов невозможно.

Примечание: Данные клиенты не могут фильтроваться на Cisco PIX Firewall.

Для эффективной фильтрации данных приложений необходимо использовать технологию NBAR на внешнем маршрутизаторе (или любой другой маршрутизатор через который клиенты локальной подсети получают доступ в интернет). NBAR может определять соединения сетей FastTrack и блокировать их либо ограничивать доступ к данным сетям на основе времени (к примеру только в нерабочее время).

Рассмотрим пример конфигурации маршрутизатора с IOS и технологией NBAR предотвращающей (блокирующей) пакеты FastTrack:

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

policy-map block-p2p
  class p2p
    drop

!--- Команда drop появилась с выходом
!--- Cisco IOS Software Release 12.2(13)T.

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

если маршрутизатор работает под управление Cisco IOS Software ниже чем Cisco IOS Software Release 12.2(13)T, то команда **drop** в policy-map недоступна. Для блокирования данного трафика совместно с policy-map выставите значение bit для DSCP в соответствии с пакетами поступающими на Ваш маршрутизатор. Затем создайте список доступа, который будет блокировать все пакеты с выставленным битом (bit). Бит DSCP используется для определения «паразитного» трафика.

Рассмотрим пример:

```
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
```

Конфигурация Gnutella - BearShare/Limewire/Morpheus/ToadNode

Gnutella это протокол с открытым исходным кодом, который в данный момент используют более 50 приложений, для различных операционных систем. Его используют такие популярные P2P приложения как BearShare, Limewire, Morpheus и ToadNode. Они используют любой открытый TCP/UDP порт для соединения с другими P2P хостами, поэтому использование списков доступа для блокирования данных клиентов невозможно.

Примечание: Данные клиенты не могут фильтроваться на Cisco PIX Firewall.

Для эффективной фильтрации данных приложений необходимо использовать технологию NBAR на внешнем маршрутизаторе (или любой другой маршрутизатор через который клиенты локальной подсети получают доступ в интернет)..

Метод блокирования данных клиентов схож с методом блокирования FastTrack . Для блокирования клиентов сетей Gnutella используйте следующую настройку:

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

Более подробна настройка блокирования P2P приложений рассмотрена на сайте производителя по [следующей ссылке](#)

Если у Вас появились вопросы, можете задать их в форуме.