Отчесь флуд !

Описание: Поомгите разобраться

Поиск в теме | **Версия для печати**

Justbox

Newbie

Покинул форум
Сообщений всего: **10**
Дата рег-ции: **Апр. 2011**

Отправлено: 30 Апреля, 2011 - 13:54:39

Провайдер понизил скорость с 100мб до 10мб заявим что микротик шлет много флуд пакетов этим самым глушит его шлюзы , отключив от микротика две сети пользователей флуд прекратился . Помогите настроить микротик чтобы он мог пресекать флудирастов до выхода в инет и кидал их например в группу flud_users .
Вот настройки firewall

E-Mail

alexnov66

Super Member

Покинул форум
Сообщений всего: **1030**
Дата рег-ции: **Февр. 2010**
Откуда: Новокузнецк

Отправлено: 01 Мая, 2011 - 02:15:02

Цитата:

> Провайдер понизил скорость с 100мб до 10мб заявим что микротик шлет много флуд пакетов этим самым глушит его шлюзы , отключив от микротика две сети пользователей флуд прекратился . Помогите настроить микротик чтобы он мог пресекать флудирастов до выхода в инет и кидал их например в группу flud_users .
> Вот настройки firewall

Какой флуд имеется ввиду ?
Может у пользователя вирус завелся.

CODE:

```
<<<<< Начало: Блокируем спамеров >>>>>
/ip firewall filter
add chain=forward protocol=tcp dst-port=25 src-
address-list=spammer action=drop comment="Drop
spamers an viruses"
add chain=forward protocol=tcp dst-port=25
connection-limit=30,32 limit=50,5 src-address-
list=!spammer action=add-src-to-address-list
address-list=spammer address-list-timeout=1d
<<<<< Конец: Блокируем спамеров >>>>>
```

CODE:

```
<<<<< Начало: Ограничиваем не более 30 одновременных
подключений с одного IP адреса >>>>>
/ip firewall filter
add chain=forward protocol=tcp tcp-flags=syn
connection-limit=30,32 action=drop comment="Drop 30
connection"
<<<<< Конец: Ограничиваем не более 30 одновременных
подключений с одного IP адреса >>>>>
```

(Добавление)
Зачем стоко разрешающих правил на подключения к микротику ?
На подключение достаточно разрешить несколько портов TCP и UDP
Для работы FTP достаточно проброс порта 21
Что за правило на адрес 127.0.0.1 ?

Вообще попробуйте ввести выше всех правил запрет на локальные адреса прова, почему у вас их нет, хотя нужно знать само подключение какое к провайдеру, надеюсь что у вас и у провайдера диапазоны адресов не пересекаются.

CODE:

```
<<<<< Начало: Блокируем пакеты с локальных адресов
провайдера >>>>>
/ip firewall filter
add chain=input src-address=10.0.0.0/8 in-
interface="pppoe_out1" action=drop comment="Drop all
fake" disabled=no
add chain=input src-address=172.16.0.0/12 in-
interface="pppoe_out1" action=drop disabled=no
add chain=input src-address=192.168.0.0/13 in-
interface="pppoe_out1" action=drop disabled=no
<<<<< Конец: Блокируем пакеты с локальных адресов
провайдера >>>>>
```

(Отредактировано автором: 01 Мая, 2011 - 04:56:10)

Если плохо работает микротик, значит его надо правильно настроить...
Настройка микротиков.

Justbox

Newbie

Покинул форум
Сообщений всего: **10**
Дата рег-ции: **Апр. 2011**

Отправлено: 01 Мая, 2011 - 13:01:07

Я сделал вот так :

Цитата:

```
add action=accept chain=input comment="accept established connection packets"
connection-state=established disabled=no
add action=accept chain=input comment="accept related connection packets"
connection-state=related disabled=no
add action=drop chain=input comment="drop invalid packets" connection-
state=invalid disabled=no
add action=accept chain=input comment="Allow access to router from known
```

network" disabled=no src-address-list=safe
add action=drop chain=input comment="detect and drop port scan connections" disabled=no protocol=tcp psd=21,3s,3,1
add action=tarpit chain=input comment="suppress DoS attack" connection-limit=3,32 disabled=no protocol=tcp src-address-list=black_list
add action=add-src-to-address-list address-list=black_list address-list-timeout=1d chain=input comment="detect DoS attack" connection-limit=10,32 disabled=no protocol=\
tcp
add action=jump chain=input comment="jump to chain ICMP" disabled=no jump-target=ICMP protocol=icmp
add action=jump chain=input comment="jump to chain services" disabled=no jump-target=services
add action=accept chain=input comment="Allow Broadcast Traffic" disabled=no dst-address-type=broadcast
add action=log chain=input comment="" disabled=no log-prefix=Filter:
add action=drop chain=input comment="drop everything else" disabled=no
add action=accept chain=ICMP comment="0:0 and limit for 5pac/s" disabled=no icmp-options=0:0-255 limit=5,5 protocol=icmp
add action=accept chain=ICMP comment="3:3 and limit for 5pac/s" disabled=no icmp-options=3:3 limit=5,5 protocol=icmp
add action=accept chain=ICMP comment="3:4 and limit for 5pac/s" disabled=no icmp-options=3:4 limit=5,5 protocol=icmp
add action=accept chain=ICMP comment="8:0 and limit for 5pac/s" disabled=no icmp-options=8:0-255 limit=5,5 protocol=icmp
add action=accept chain=ICMP comment="11:0 and limit for 5pac/s" disabled=no icmp-options=11:0-255 limit=5,5 protocol=icmp
add action=drop chain=ICMP comment="Drop everything else" disabled=no protocol=icmp
add action=accept chain=services comment="accept localhost" disabled=no dst-address=127.0.0.1 src-address=127.0.0.1 src-address-list=""
add action=accept chain=services comment="allow MACwinbox " disabled=yes dst-port=20561 protocol=udp
add action=accept chain=services comment="Bandwidth server" disabled=yes dst-port=2000 protocol=tcp
add action=accept chain=services comment=" MT Discovery Protocol" disabled=yes dst-port=5678 protocol=udp
add action=accept chain=services comment="allow SNMP" disabled=yes dst-port=161 protocol=tcp
add action=accept chain=services comment="Allow BGP" disabled=yes dst-port=179 protocol=tcp
add action=accept chain=services comment="allow BGP" disabled=yes dst-port=5000-5100 protocol=udp
add action=accept chain=services comment="Allow NTP" disabled=yes dst-port=123 protocol=udp
add action=accept chain=services comment="Allow PPTP" disabled=no dst-port=1723 protocol=tcp
add action=accept chain=services comment="allow PPTP and EoIP" disabled=no protocol=gre
add action=accept chain=services comment="allow DNS request" disabled=yes dst-port=53 protocol=tcp
add action=accept chain=services comment="Allow DNS request" disabled=yes dst-port=53 protocol=udp
add action=accept chain=services comment=UPnP disabled=yes dst-port=1900 protocol=udp

```
add action=accept chain=services comment=UPnP disabled=yes dst-port=2828
protocol=tcp
add action=accept chain=services comment="allow DHCP" disabled=yes dst-
port=67-68 protocol=udp
add action=accept chain=services comment="allow Web Proxy" disabled=yes dst-
port=8080 protocol=tcp
add action=accept chain=services comment="allow IPIP" disabled=yes
protocol=ipencap
add action=accept chain=services comment="allow https for Hotspot"
disabled=yes dst-port=443 protocol=tcp
add action=accept chain=services comment="allow Socks for Hotspot"
disabled=yes dst-port=1080 protocol=tcp
add action=accept chain=services comment="Allow IPSec-esp" disabled=yes
protocol=ipsec-esp
add action=accept chain=services comment="Allow IPSec-ah" disabled=yes
protocol=ipsec-ah
add action=accept chain=services comment="Allow IKE" disabled=yes dst-
port=500 protocol=udp
add action=accept chain=services comment="Allow IPSec-esp" disabled=yes
protocol=ipsec-esp
add action=accept chain=services comment="Allow IPSec-ah" disabled=yes
protocol=ipsec-ah
add action=accept chain=services comment="allow RIP" disabled=yes dst-
port=520-521 protocol=udp
add action=accept chain=services comment="allow OSPF" disabled=yes
protocol=ospf
add action=return chain=services comment="" disabled=no
add action=accept chain=forward comment="" disabled=no dst-
address=10.8.0.0/16 src-address=192.168.1.0/24
add action=accept chain=forward comment="" disabled=no dst-
address=192.168.1.0/24 src-address=10.8.0.0/16
add action=accept chain=forward comment="" disabled=no dst-
address=0.0.0.0/0 src-address=10.8.0.0/16
add action=accept chain=forward comment="" disabled=no dst-
address=10.8.0.0/16 src-address=0.0.0.0/0
add action=accept chain=forward comment="" disabled=no dst-
address=192.168.1.0/24 src-address=0.0.0.0/0
add action=accept chain=forward comment="" disabled=no dst-
address=0.0.0.0/0 src-address=192.168.1.0/24
add action=drop chain=forward comment="Drop 30 connection" connection-
limit=30,32 disabled=no protocol=tcp tcp-flags=syn
add action=drop chain=forward comment="" disabled=no
```

Пров сказал что от меня идет много фпакетов что гасит его шлюзи =(

Сеть прова 89.31.18.XXX/24
Сеть офиса 1 10.8.0.0/16
Сеть офиса 2 192.168.1.0/24

Я правильно поставил цепочку на блокировку подключений ?

(Отредактировано автором: 01 Мая, 2011 - 13:04:20)

alexnov66

Отправлено: 01 Мая, 2011 - 13:17:54

Super Member

Покинул форум
Сообщений всего: **1030**
Дата рег-ции: **Февр. 2010**
Откуда: Новокузнецк

Правила читаются с верху в низ, то что вы их добавили в самый низ ни какого эфекта непринесет.
Правила должны быть в самом верху это первое, второе я разве дал выше настройки на форвард, инпут должен быть, третье ни один даже самый мощный компьютер не потянет столько пользователей сколько у вас указано в маске сети, желательно увеличить до возможного предела.

pppoe_out1 имя подключения к провайдеру, в данном примере pppoe подключение к прову

<<<<< Начало: Блокируем пакеты с локальных адресов провайдера >>>>>
/ip firewall filter
add chain=input src-address=10.0.0.0/8 in-interface="pppoe_out1" action=drop comment="Drop all fake" disabled=no
add chain=input src-address=172.16.0.0/12 in-interface="pppoe_out1" action=drop disabled=no
add chain=input src-address=192.168.0.0/13 in-interface="pppoe_out1" action=drop disabled=no
<<<<< Конец: Блокируем пакеты с локальных адресов провайдера >>>>>

ps: Странно пытался ввести весь ваш код в сообщение выдало что размер сообщения не может быть больше 6 килобайт

(Отредактировано автором: 01 Мая, 2011 - 13:27:14)

Если плохо работает микротик, значит его надо правильно настроить...
Настройка микротиков.

E-Mail AIM

Justbox

Отправлено: 01 Мая, 2011 - 20:59:15

Newbie

Покинул форум
Сообщений всего: **10**
Дата рег-ции: **Апр. 2011**

В верх всех правил добавляю:

CODE:

```
/ip firewall filter
add chain=input src-address=10.0.0.0/8 in-
interface="ether1-wan" action=drop comment="Drop all
fake" disabled=no
add chain=input src-address=172.16.0.0/12 in-
interface="ether1-wan" action=drop disabled=no
add chain=input src-address=192.168.0.0/13 in-
interface="ether1-wan" action=drop disabled=no
add chain=input src-address=10.0.0.0/8 in-
interface="ether4-wan" action=drop comment="Drop all
fake" disabled=no
add chain=input src-address=172.16.0.0/12 in-
interface="ether4-wan" action=drop disabled=no
add chain=input src-address=192.168.0.0/13 in-
interface="ether4-wan" action=drop disabled=no
add chain=forward protocol=tcp dst-port=25 src-
address-list=spammer action=drop comment="Drop
spamers an viruses"
add chain=forward protocol=tcp dst-port=25
connection-limit=30,32 limit=50,5 src-address-
```

```
list=!spammer action=add-src-to-address-list
address-list=spammer address-list-timeout=1d
add chain=forward protocol=tcp tcp-flags=syn
connection-limit=30,32 action=drop comment="Drop 30
connection"
```

Повторюсь у меня две сети:
1-я 10.8.0.0/16
2-я 192.168.1.0/24

Я не потеряю контроль над тиком ?

E-Mail

alexnov66

Отправлено: 02 Мая, 2011 - 06:13:06

Id

Super Member

Покинул форум
Сообщений всего: **1030**
Дата рег-ции: **Февр. 2010**
Откуда: Новокузнецк

А контроль над микротиком нужен с внешней стороны или с локальной ?
В настройке указывается внешний интерфейс, на котором получается внешний реальный адрес, еще раз повторюсь нужно знать какое подключение к провайдеру, вы этого не озвучили, в принципе блокировка должна стоять у провайдера, если админы нормальные, введите пока эти настройки, на самый верх.

CODE:

```
<<<<< Начало: Ограничиваем не более 30 одновременных
подключений с одного IP адреса >>>>>
/ip firewall filter
add chain=forward protocol=tcp tcp-flags=syn
connection-limit=30,32 action=drop comment="Drop 30
connection"
<<<<< Конец: Ограничиваем не более 30 одновременных
подключений с одного IP адреса >>>>>
```

CODE:

```
<<<<< Начало: Блокируем спамеров >>>>>
/ip firewall filter
add chain=forward protocol=tcp dst-port=25 src-
address-list=spammer action=drop comment="Drop
spamers an viruses"
add chain=forward protocol=tcp dst-port=25
connection-limit=30,32 limit=50,5 src-address-
list=!spammer action=add-src-to-address-list
address-list=spammer address-list-timeout=1d
<<<<< Конец: Блокируем спамеров >>>>>
```

Если плохо работает микротик, значит его надо правильно настроить...
Настройка микротиков.

E-Mail AIM

Justbox

Отправлено: 02 Мая, 2011 - 19:37:06

Id

1 Подлючение статика .

Newbie

Покинул форум
Сообщений всего: **10**
Дата рег-ции: **Апр. 2011**

2 поробую

E-Mail

sergey85

Отправлено: 03 Мая, 2011 - 10:45:14

Junior Member

Покинул форум
Сообщений всего: **71**
Дата рег-ции: **Март 2010**

Цитата:

> 1 Подлючение статика .

замечательный ответ можно сказать что вы ничего не ответили....

E-Mail

warez

Отправлено: 03 Мая, 2011 - 13:36:58

Advanced Member

Покинул форум
Сообщений всего: **299**
Дата рег-ции: **Март 2010**
Откуда: Vladimir

Почему же - статический тип подключения по IP протоколу.
Провайдер дает ему белый статический IP адрес

(Отредактировано автором: 03 Мая, 2011 - 13:37:36)

E-Mail

Justbox

Отправлено: 03 Мая, 2011 - 15:26:15

Newbie

Покинул форум
Сообщений всего: **10**
Дата рег-ции: **Апр. 2011**

У меня два офиса один ЦО второй БО соединил эти офисы по ЕоИП .Провайдер сказал что приходит от офиса Бо фрагментированные пакеты поэтому его шлюз глохнит =(что делать ?

E-Mail

Поиск в теме | **Версия для печати**

Страниц (2): [1] 2 »

« RouterOS »

Переход по форумам

Все гости форума могут просматривать этот раздел.
Только зарегистрированные пользователи могут создавать новые темы в этом разделе.
Только зарегистрированные пользователи могут отвечать на сообщения в этом разделе.

Ответить
НоваяТема

Powered by ExBB

ExBB FM 1.0 Beta by TvoyWeb.ru
InvisionExBB Style converted by Markus®
[Script Execution time: 0.0542] [Gzip Disabled]