Автор:
13.12.11 15:08 - Последнее обновление 07.02.12 12:25

Лимитирование ОБЪЕМА трафика в Pfsense 2.0.

Обзоров данной системы управления передачи сетевых пакетов множество, действительно данная система заслуживает большого внимания, ведь в этом крохотном дистре собрана мощнейшая система блокировки, шейпинга, контентного фильтра, антивируса, прокси, сервер и клиент VPN, по разным протоколам, балансировка провайдеров, и многое другое, и все это из коробки под ключ. Пользование данной системы 1 год, за это время сборка показала отличную стабильность.
Но вскоре была поставлена задача, лимитировать объем трафика, потребляемого обычными пользователями, и отрезать доступ по окончании лимита, но доступ скайпа, аськи и почты, через outlook, оставить! Очень не хотелось переезжать на другую систему после столь длительного времени существования. По этому ушёл в поиск, прямых статей, по организации лимита на Pfsense не нашел, но зато опираясь, на статьи раскрывающие лимитирование при помощи стандартного Squid.
Итак, за основу была взята статья : http://www.opennet.ru/tips/info/1797.shtml
Автору огромное спасибо, за столь простой и действующий способ!

Изложу кратко: Допускаем что у нас уже имеется установленная система Pfsense, Squid, LightSquid
Squid из пакетов Pfsense. Пишем скрипт в файлике traf_limit.pl

```
#!/usr/bin/perl
#
# Довесок на LightSquid Project (c) 2004-2005 Sergey Erokhin aka ESL
#
# Скрипт создает файлик user_deny для ограничения сети по трафику
# Автор: Иван Лонин loninia@apksouz.ru  2008 год.
use File::Basename;

# коряво конечно напрямую писать путь к конфигу, но лениво было sh файлик для крона делать

require "/usr/local/etc/squid/traf_limit/config";
#($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst)=localtime(time);

@dat=localtime(time);
$year =1900+$dat[5];
$month=1 + $dat[4];
```

```
if ($month<10){
$month="0".$month
}
$filter="$year$month";

#print "$log_path/$filter*n";
@daylist=glob("$log_path/$filter*");

foreach $daypath (sort @daylist) {
open FF,"<$daypath/.total";

$totaluser=<FF>;chomp $totaluser;$totaluser=~s/^user: //;
$totalsize=<FF>;chomp $totalsize;$totalsize=~s/^size: //;

while (<FF>) {
($user,$size,$hit)=split;
$h{$user}{size}+=$size;
$h{$user}{hit}+=$hit;
}
close FF;
}
#
$cummulative=0;
open RES,">$res_file";
#print RES "# файл содержит юзеров превысивших квоту.n# автоматически
переписывается скриптом
#traf_limit.plndolzhen_bit_odin_usern";
foreach $user (sort {$h{$b}{size}<=>$h{$a}{size}} keys  %h) {

$all4user=$h{$user}{size}/1024/1024;
if ($vip_user{$user}{size} > 0) {
$limit=$vip_user{$user}{size};
}else{
$limit=$all_limit;
}

if ($all4user >= $limit) {
print RES "$usern";
# print "$h{$user}{size}n";
};

}
__END__
```

Конфиг к нему под названием config

```
#!/usr/bin/perl
# конфигурационный файл для скрипта traf_limit.pl
#
# путь к логам lightsquid
$log_path="/var/lightsquid/report";

# файл в который пушутся пользователи превысившие лимит
$res_file="/var/squid/acl/banned_hosts.acl";

# лимит инета в мегабайтах
$all_limit=600;

# привилегированные пользователи с повышенным или пониженным лимитом
# для каждого пользователя строка формата:
#$vip_user{<имя_юзера>}{size}=<лимит_в_мегабайтах>;
$vip_user{user1}{size}=5;
$vip_user{qwe}{size}=50;
```

Выше указанные 2 файла, поселяем в папку /usr/local/etc/squid/traf_limit, они будут обрабатывать логи LightSquid, отбирать тех кто уже превысил 600 мб в этом месяце, и писать их айпишники в файлик /var/squid/acl/banned_hosts.acl, пути до логов у вас могут быть другие!
На нем остановимся подробнее, дело в том, что система Pfsense, каждый раз при загрузке, перезаписывает конфигурационные файлы в частности - squid.conf, опираясь на данные в веб конфигураторе, из-за этого вносить изменения вручную не вариант, пользоваться custom options, в веб конфигураторе тоже нет смысла, эта секция располагается ниже ACL в squid.conf.
Идем на маленькую хитрость, в веб конфигураторе squid, есть секция Access Control, banned host addresses. Если Вы ей пользовались, то ищите компромисс либо в SquidGuard, либо блочте в фаерволле. Т.к. Эта секция нам нужна, пишем в ней 1 ip адрес не занятый в нашей сети и в будущем не нужный, просто чтоб /var/squid/acl/banned_hosts.acl существовал.
Данная секция(banned host addresses) в веб конфигураторе пишет в файлик /var/squid/acl/banned_hosts.acl, тех кого мы хотим заблочить, а в Squid.conf данный файлик указан в сеции как раз ACL:

```
acl banned_hosts src "/var/squid/acl/banned_hosts.acl"
```

Этим мы и воспользуемся... Наш скрипт будет перезаписывать этот файлик раз в час, и затем тут же нам необходимо чтобы Squid перечитал свою конфигурацию, но не перезагружать! А то данные в файле /var/squid/acl/banned_hosts.acl, опять заменятся на данные в веб конфигураторе, т.е. на тот 1 ip который мы указали
Итак создаем файлик squidr.sh поселяем его в /usr/local/etc/squid/traf_limit, содержимое файлика :

```
#!/bin/sh
```

/usr/local/sbin/squid -k reconfigure >> /dev/null 2>&1

Ставим пакет Cron из Pfsense. Добавляем задания:
5 * * * * /usr/local/etc/squid/traf_limit/traf_limit.pl
7 * * * * /usr/local/etc/squid/traf_limit/squidr.sh
Все, теперь кто превысил лимит, будут блочиться, и им будет выдаваться сообщение из файла /usr/local/etc/squid/errors/Russian-1251/ ERR_ACCESS_DENIED , его мы можем изменить на свой вкус,
С сообщением типа закончился лимит.

Теперь задача, оградить от правила лимита, главу организации, их iP мы можем прописать в секции обхода прокси или попробывать в секции Access control, - Unrestricted IPs.

2011г Аксёнов Алексей

оригинал: http://forum.pfsense.org/index.php?topic=43926.0

ссылка на статью: http://thin.kiev.ua/index.php?option=com_content&view=article&id=478:pfsense-20&catid=50:pfsense&Itemid=81

доп материал: http://thin.kiev.ua/index.php?option=com_content&view=article&id=287:traffik&catid=39:linux&Itemid=63

http://www.opennet.ru/base/net/traf_gate.txt.html

{jcomments on}

Автор:
13.12.11 15:08 - Последнее обновление 07.02.12 12:25