

Установка и настройка CSF



Введение

Брандмауэр Config Server Firewall (или CSF) - это бесплатный и продвинутый брандмауэр для большинства дистрибутивов Linux и VPS на базе Linux. В дополнение к базовой функциональности брандмауэра – фильтрации пакетов – CSF включает в себя другие функции безопасности, такие как обнаружение входа в систему/ вторжений/наводнений. CSF включает интеграцию пользовательского интерфейса для cPanel, DirectAdmin и Webmin, но в этом руководстве рассматривается только использование командной строки. CSF способен распознавать множество атак, таких как сканирование портов, синхронизирующие потоки и атаки методом перебора при входе во многие сервисы. Он настроен на временную блокировку клиентов, которые, как было обнаружено, атакуют облачный сервер.

С полным списком поддерживаемых операционных систем и функций можно ознакомиться на веб-сайте [Config Server](http://configserver.com).

Для начала, пожалуйста, обратите внимание, что Perl и libwww являются обязательными условиями для установки CSF в любом из поддерживаемых дистрибутивов (RHEL и CentOS, openSUSE, Debian и Ubuntu). Поскольку он должен быть доступен по умолчанию, с вашей

стороны не требуется никаких действий, если только один из следующих шагов не вернет фатальную ошибку (в этом случае используйте систему управления пакетами для установки отсутствующих зависимостей).

```
yum install perl-libwww-perl #CentOS/Fedora  
apt install libwww-perl #Debian/Ubuntu
```

Если Вы хотите установить CSF на Debian 11 и выше, то Вам потребуется установить пакет **iptables**. Сделать это можно командой: `apt install iptables`

Шаг 1 – Загрузка CSF

Перейдем в папку `/usr/src` и скачаем CSF:

```
cd /usr/src  
wget https://download.configserver.com/csf.tgz
```

Шаг 2 – Распакуем архив с CSF

Распаковываем архив с файлами и переходим в папку `csf`:

```
tar xzf csf.tgz  
cd csf
```

Шаг 3 – Запускаем скрипт установки

Скрипт проверит, установлены ли все зависимости, создаст необходимые структуры каталогов и файлы для веб-интерфейса, обнаружит открытые в данный момент порты и напомнит вам перезапустить демонов `csf` и `lfd` после завершения начальной настройки.

```
sh install.sh
```

Ваш IP-адрес был добавлен в белый список, если это возможно. Кроме того, SSH-порт был открыт автоматически, даже если он использует пользовательский порт. Брандмауэр также был настроен на включение режима тестирования, что означает, что правила `iptables` будут автоматически удалены через пять минут после запуска

CSF. Это следует отключить, как только вы убедитесь, что ваша конфигурация работает, и вы не будете заблокированы.

Теперь запустим стандартный тест для проверки наличия всех модулей для корректной работы CSF:

```
perl /usr/local/csf/bin/csftest.pl
```

Вы должны получить такой вывод:

```
Testing ip_tables/iptables_filter...OK
Testing ipt_LOG...OK
Testing ipt_multiport/xt_multiport...OK
Testing ipt_REJECT...OK
Testing ipt_state/xt_state...OK
Testing ipt_limit/xt_limit...OK
Testing ipt_recent...OK
Testing xt_connlimit...OK
Testing ipt_owner/xt_owner...OK
Testing iptable_nat/iptables_REDIRECT...OK
Testing iptable_nat/iptables_DNAT...OK

RESULT: csf should function on this server
```

Если получаете ошибку, то проверьте наличие пакета **iptables** на своем сервере.

Шаг 4 – Отключение FirewallD

Отключите брандмауэр, если он запущен, и настройте CSF:

```
systemctl stop firewalld
systemctl disable firewalld
```

Шаг 5 – Базовая настройка CSF

CSF можно настроить, отредактировав его файл конфигурации **csf.conf** в `/etc/csf/`:

```
nano /etc/csf/csf.conf
```

Настройка портов

Чем меньше доступ к вашему VPS, тем безопаснее ваш сервер. Однако не все порты могут быть закрыты, так как клиенты должны иметь возможность пользоваться вашими услугами.

По умолчанию открыты следующие порты:

```
TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995"
```

```
TCP_OUT = "20,21,22,25,53,80,110,113,443"
```

```
UDP_IN = "20,21,53"
```

```
UDP_OUT = "20,21,53,113,123"
```

Тут Вы сможете найти подробное описание каждого порта и если считаете, что он ненужен, то можете удалить из файла CSF.

Приведем парочку примеров конфигурации портов, которые нужны для успешного запуска той или иной службы.

На любом сервере:

```
TCP_IN: 22,53 TCP_OUT: 22,53,80,113,443 UDP_IN: 53 UDP_OUT: 53,113,123
```

Apache:

```
TCP_IN: 80,443
```

FTP-сервер:

```
TCP_IN: 20,21 TCP_OUT: 20,21 UDP_IN: 20,21 UDP_OUT:20,21
```

Почтовый сервер:

```
TCP_IN: 25,110,143,587,993,995 TCP_OUT: 25,110
```

Сервер MySQL (если требуется удаленный доступ)

```
TCP_IN: 3306 TCP_OUT: 3306
```

Если вы используете IPv6 для своих служб, вам также следует настроить **TCP6_IN**, **TCP6_OUT**, **UDP6_IN** и **UDP6_OUT** аналогично настройке портов IPv4 ранее.

Дополнительные настройки

CSF предлагает огромное количество различных опций в своих конфигурационных файлах. Некоторые из наиболее часто используемых настроек описаны ниже.

ICMP_IN Установка ICMP_IN в 1 разрешает пинговать ваш сервер, а 0 отклоняет такие запросы. Если вы размещаете какие-либо общедоступные службы, рекомендуется разрешать запросы ICMP, поскольку их можно использовать для определения доступности вашей службы.

ICMP_IN_LIMIT Устанавливает количество запросов ICMP (ping), разрешенных с одного IP-адреса в течение заданного промежутка времени. Обычно нет необходимости изменять значение по умолчанию (1/с)

DENY_IP_LIMIT Устанавливает количество заблокированных IP-адресов, которые CSF отслеживает. Рекомендуется ограничить количество запрещенных IP-адресов, так как слишком большое количество блоков может снизить производительность сервера.

DENY_TEMP_IP_LIMIT То же, что и выше, но для временных блоков IP-адресов.

PACKET_FILTER Фильтровать недопустимые, нежелательные и незаконные пакеты.

SYNFLOOD, SUNFLOOD_RATE и SYN Flood BURST Обеспечивает защиту от SYN-флуд-атак. Это замедляет инициализацию каждого соединения, поэтому вам следует включать это, только если вы знаете, что ваш сервер подвергается атаке.

CONNLIMIT Ограничивает количество одновременных активных подключений к порту.

Пример:

```
22;tcp;5;250
```

Это заблокирует IP-адрес, если на порту 22 будет установлено более 5 подключений с использованием протокола TCP в течение 250 секунд. Блокировка снимается по прошествии 250 секунд после отправки последнего пакета клиентом на этот порт. Вы можете добавить больше портов, разделив их запятыми, как описано ниже.

```
порт1;протокол1;количество_соединений1;время1,порт2;протокол2;количество_соединений2;время2
```

Больше настроек

CSF предлагает широкий спектр настроек, которые мы не рассматривали в этом руководстве. Значения по умолчанию, как правило, хороши и могут использоваться практически на любом сервере. Настройки по умолчанию настроены на предотвращение большинства флуд-атак, сканирования портов и попыток несанкционированного доступа.

Однако если вы хотите настроить конфигурацию более подробно, прочтите комментарии в файле `/etc/csf/csf.conf` и отредактируйте их по своему усмотрению.

Без установки Вы можете ознакомиться с описанием каждой функции [Тут](#).

Шаг 6 – Применение изменений

Всякий раз, когда вы изменяете настройки в `csf.conf`, вы должны сохранить файлы и перезапустить CSF, чтобы изменения вступили в силу.

Когда Вы закончите редактировать файл **conf.csf**, закройте файл, нажав **Ctrl + X**. Когда вас спросят, сохранять изменения или нет, нажмите **Y**, чтобы сохранить изменения.

После этого следует применить изменения, перезапустив CSF командой:

```
csf -r
```

Если все прошло по плану, и вы все еще можете получить доступ к серверу, откройте файл конфигурации еще раз:

```
nano /etc/csf/csf.conf
```

и измените параметр `TESTING` в начале файла конфигурации на `0`, как показано ниже:

```
TESTING = "0"
```

Сохраните файл и примените изменения с помощью команды:

```
csf -r
```

Шаг 7 – Активация CSF

Пришло запустить CSF с нашими правилами в работу:

```
systemctl restart {csf,lfd}  
systemctl enable {csf,lfd}  
systemctl is-active {csf,lfd}  
csf -v
```

На этом базовая настройка CSF завершена.

Шаг 8 – Работа с CLI CSF

Скоро...

Версия #3

Artem создал 18 августа 2023 01:28:33

Artem обновил 21 августа 2023 06:58:28