

**ИНТЕЛЛЕКТУАЛЬНЫЙ СЕТЕВОЙ ЭКРАН ДЛЯ ЗАЩИТЫ
ВЕБ-ПРИЛОЖЕНИЙ SOLIDWALL**

Руководство по установке

Листов 8

2020 г.

СОДЕРЖАНИЕ

1	ВВЕДЕНИЕ	2
1.1	Область применения	2
1.2	Краткое описание возможностей	2
2	ПРОЦЕДУРЫ УСТАНОВКИ.....	3
2.1	Минимальные требования	3
2.2	Установка SolidWall WAF	3
2.2.1	Подготовка к установке ПО SolidWall WAF	3
2.2.2	Настройка sudo без запроса пароля для пользователя waf.....	4
2.2.3	Распаковка дистрибутива	5
2.2.4	Настройка интерфейса захвата трафика	5
2.2.5	Запуск установки.....	6
2.2.6	Окончание установки	7
2.3	Первоначальная настройка.....	7

1 ВВЕДЕНИЕ

1.1 Область применения

Область применения интеллектуального сетевого экрана SolidWall (далее – SolidWall WAF) мониторинг состояния защищённости веб-приложений.

1.2 Краткое описание возможностей

SolidWall WAF является интеллектуальным сетевым экраном прикладного уровня и предназначен для мониторинга трафика веб-приложений на наличие интернет-угроз.

SolidWall WAF выполняет следующие функции:

- мониторинг трафика;
- идентификацию и аутентификацию пользователей, являющихся работниками оператора;
- регистрацию событий безопасности (аудит);
- бесперебойное функционирование и восстановление;
- тестирование и контроль целостности;
- управление (администрирование);
- взаимодействие с другими средствами защиты информации.

2 ПРОЦЕДУРЫ УСТАНОВКИ

2.1 Минимальные требования

Компьютер, на котором запускается SolidWall WAF, должен соответствовать следующим минимальным требованиям, приведенным в таблице 1.

Таблица 1 – Минимальные требования к ЭВМ, на которых запускается SolidWall WAF SolidWall

Компонент	Минимальное требование
Объём оперативной памяти (RAM)	Не менее 8 ГБ.
Процессор (CPU)	4-ядерный и более с архитектурой x86-64, тактовая частота не ниже 2.2 ГГц
Объём жёсткого диска (HDD)	Не менее 500 ГБ
Сетевые интерфейсы	Один 1 ГБ Ethernet

В качестве системного программного обеспечения используются операционные системы Ubuntu 16.04 Server 64-bit или Astra Linux SE Smolensk (1.6).

2.2 Установка SolidWall WAF

2.2.1 Подготовка к установке ПО SolidWall WAF

Дистрибутив ПО SolidWall WAF необходимо скачать по предоставленной после подписания договора ссылке. Для скачивания дистрибутива необходимо авторизоваться с использованием предоставленной уникальной пары логин-пароль. Дистрибутив представляет собой архив «*.tgz», объемом порядка 1 ГБ. Перед началом установки необходимо создать пользователя операционной системы «waf» с правами администратора, а затем скопировать дистрибутив в домашний каталог пользователя waf, который был создан в процессе установки ОС (/home/waf).

В случае установки по сети это можно сделать при помощи команды `scp`, а в случае наличия физического доступа - с использованием установочного съемного носителя.

Далее необходимо повторно вставить загрузочный usb с операционной системой и вмонтировать его в /media/usb. Для этого нужно выполнить команду `sudo fdisk -l`.

Команда выведет на экран список устройств, из которого следует выбрать соответствующий загрузочный диск (Рисунок 1).

```

/dev/vda5          501760    52426751    25962496    8e    Linux LVM

Диск /dev/mapper/waf--vg-root: 18.3 Гб, 18333302784 байт
255 головок, 63 секторов/треков, 2228 цилиндров, всего 35807232 секторов
Units = секторы of 1 * 512 = 512 bytes
Размер сектора (логического/физического): 512 байт / 512 байт
I/O size (minimum/optimal): 512 bytes / 512 bytes
Идентификатор диска: 0x00000000

На диске /dev/mapper/waf--vg-root отсутствует верная таблица разделов

Диск /dev/mapper/waf--vg-swap_1: 8250 МБ, 8250195968 байт
255 головок, 63 секторов/треков, 1003 цилиндров, всего 16113664 секторов
Units = секторы of 1 * 512 = 512 bytes
Размер сектора (логического/физического): 512 байт / 512 байт
I/O size (minimum/optimal): 512 bytes / 512 bytes
Идентификатор диска: 0x00000000

На диске /dev/mapper/waf--vg-swap_1 отсутствует верная таблица разделов

ВНИМАНИЕ: На '/dev/sda' обнаружена GPT (GUID Partition Table)! Утилита fdisk не поддерживаетGPT. Используйте GNU Parted.

Диск /dev/sda: 16.0 Гб, 15997075456 байт
255 головок, 63 секторов/треков, 1944 цилиндров, всего 31244288 секторов
Units = секторы of 1 * 512 = 512 bytes
Размер сектора (логического/физического): 512 байт / 512 байт
I/O size (minimum/optimal): 512 bytes / 512 bytes
Идентификатор диска: 0x51226372

Устр-во Загр      Начало      Конец      Блоки  Id  Система
/dev/sda1 *        0          1185791    592896  0   Пустой
/dev/sda2          461172     465715     2272   ef   EFI (FAT-12/16/32)

ВНИМАНИЕ: На '/dev/sda1' обнаружена GPT (GUID Partition Table)! Утилита fdisk не поддерживаетGPT. Используйте GNU Parted.

Диск /dev/sda1: 607 МБ, 607125504 байт
255 головок, 63 секторов/треков, 73 цилиндры, всего 1185792 секторов
Units = секторы of 1 * 512 = 512 bytes
Размер сектора (логического/физического): 512 байт / 512 байт
I/O size (minimum/optimal): 512 bytes / 512 bytes
Идентификатор диска: 0x51226372

Устр-во Загр      Начало      Конец      Блоки  Id  Система
/dev/sda1p1 *      0          1185791    592896  0   Пустой
/dev/sda1p2       461172     465715     2272   ef   EFI (FAT-12/16/32)
waf@waf:~$

```

Рисунок 1

Затем необходимо произвести монтирование usb-устройства с помощью команды mount.

Для этого нужно выполнить следующую последовательность команд:

```
sudo mkdir /media/usb
```

`sudo mount /dev/sda /media/usb` (где /dev/sda – идентификатор Вашего устройства)

```
sudo apt-cdrom add -m -d /media/usb
```

```
sudo apt-get update
```

2.2.2 Настройка sudo без запроса пароля для пользователя waf

ВНИМАНИЕ! Установка SolidWall WAF должна производиться ТОЛЬКО от имени пользователя waf. Установка от имени пользователя root не допускается!

Для успешной установки в автоматическом режиме необходимо установить для пользователя waf режим sudo без пароля.

Для этого необходимо отредактировать файл /etc/sudoers при помощи команды `sudoedit /etc/sudoers.d/waf` и добавить в его конец строку `waf ALL=(ALL:ALL) NOPASSWD:ALL` как показано ниже (Рисунок 2).

```
GNU nano 2.2.6      Файл: /var/tmp/waf.XXXxg0k2      Изменён
waf ALL=(ALL:ALL) NOPASSWD:ALL
```

^G Помощь ^O Записать ^R ЧитФайл ^Y ПредСтр ^K Вырезать ^C ТекПозиц
^X Выход ^J Выровнять ^W Поиск ^V СледСтр ^U ОтмВырезк ^T Словарь

Рисунок 2

2.2.3 Распаковка дистрибутива

Перед установкой необходимо создать папку для распаковки дистрибутива и распаковать его, выполнив команду, представленную ниже:

```
$ tar xzf home/waf/latest.tgz -C /home/waf/
```

2.2.4 Настройка интерфейса захвата трафика

Примечание: все команды в данном разделе требуют привилегий суперпользователя (root).

Пусть ethX - это имя сетевого интерфейса, на котором должен происходить захват трафика, где X - порядковый номер интерфейса (например, eth0). Необходимо убедиться, что данный интерфейс сконфигурирован в файле /etc/network/interfaces, и если конфигурация данного интерфейса отсутствует, добавить следующие строки в конец файла, используя встроенный текстовый редактор vi:

```
auto ethX
iface ethX inet static
    address XXX.XXX.XXX.XXX
    netmask YYY.YYY.YYY.YYY
    network XXX.XXX.XXX.AAA
    broadcast XXX.XXX.XXX.255
    gateway XXX.XXX.XXX.BBB
    dns-nameservers ZZZ.ZZZ.ZZZ.ZZZ
```

Пример файла /etc/network/interfaces приведён ниже (Рисунок 3).

```
waf@waf:/$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 172.16.8.132
    netmask 255.255.255.0
    network 172.16.8.0
    broadcast 172.16.8.255
    gateway 172.16.8.1
    # dns-* options are implemented by the resolvconf package, if installed
    dns-nameservers 8.8.8.8
```

Рисунок 3

Затем при помощи команды `ifconfig ethX` необходимо проверить, что нужный интерфейс находится в активном состоянии.

В выводе команды должны присутствовать слова `UP` и `RUNNING` (Рисунок 4, Рисунок 5).

```
waf@waf:/$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:d8:fe:61
          inet addr:172.16.8.132 Bcast:172.16.8.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fed8:fe61/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:986546 errors:0 dropped:92585 overruns:0 frame:0
          TX packets:222701 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:188585678 (188.5 MB)  TX bytes:269264085 (269.2 MB)
```

Рисунок 4

```
waf@solidwall:~/distr$ sudo ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:22:b2:27
          inet6 addr: fe80::20c:29ff:fe22:b227/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:120 (120.0 B)  TX bytes:648 (648.0 B)
```

Рисунок 5

В случае если интерфейс не находится в активном состоянии, необходимо его активировать командой `ifup ethX`.

2.2.5 Запуск установки

Для запуска процесса установки необходимо запустить скрипт командой `./install_interactive.sh` из установочного каталога:

```
sudo /home/waf/install_interactive.sh
```

Далее последуют запросы от системы относительно настроек и паролей, описанных в п.п.

2.2.6.

2.2.6 Окончание установки

После ответа на оставшиеся вопросы системы, запустится процесс установки, который может занять 10-15 минут (Рисунок 69).

```
AptOfflineQtInstallBugList.pyc", "byte-compiling /usr/local/lib/python2.7/dist-p
ackages/apt_offline_core/AptOfflineLib.py to AptOfflineLib.pyc", "byte-compiling
/usr/local/lib/python2.7/dist-packages/apt_offline_core/AptOfflineCoreLib.py to
AptOfflineCoreLib.pyc", "byte-compiling /usr/local/lib/python2.7/dist-packages/
apt_offline_core/AptOffline_argparse.py to AptOffline_argparse.pyc", "byte-compi
ling /usr/local/lib/python2.7/dist-packages/apt_offline_core/__init__.py to __in
it__.pyc", "byte-compiling /usr/local/lib/python2.7/dist-packages/apt_offline_co
re/AptOfflineDebianBtsLib.py to AptOfflineDebianBtsLib.pyc", "byte-compiling /us
r/local/lib/python2.7/dist-packages/apt_offline_core/AptOfflineMagicLib.py to Ap
tOfflineMagicLib.pyc", "running install_scripts", "copying build/scripts-2.7/apt
-offline -> /usr/local/bin", "copying build/scripts-2.7/apt-offline-gui -> /usr/
local/bin", "changing mode of /usr/local/bin/apt-offline to 755", "changing mode
of /usr/local/bin/apt-offline-gui to 755", "running install_egg_info", "Writing
/usr/local/lib/python2.7/dist-packages/apt_offline-1.7.2.egg-info", "warnings'
: []
```

Рисунок 6

В процессе установки будет выведено большое количество диагностических сообщений, которые будут скопированы в файл /var/tmp/install.log.

В случае неуспешной установки необходимо передать этот файл инженерам SolidWall WAFO «СолидСофт» для анализа.

Успешность установки можно проверить в консоли при помощи следующей команды: `grep -A 1 RECAP /var/tmp/install.log`

Индикатором успешного завершения установки является появление сообщения `PLAY RECAP` с нулевым числом неуспешных (failed) шагов:

```
PLAY RECAP *****
localhost : ok=149 changed=106 unreachable=0 failed=0
```

Рисунок 7

2.3 Первоначальная настройка

Характерной особенностью работы интеллектуального сетевого экрана является то, что работоспособность и доступность защищаемых приложений не зависит от работоспособности SolidWall WAF. SolidWall WAF получает копию всего трафика с сетевого устройства (это может быть, например, коммутатор или устройство распределения нагрузки сети) через SPAN-порт.

Схема включения SolidWall WAF в инфраструктуру в режиме работы с копией трафика представлена на рисунке ниже.

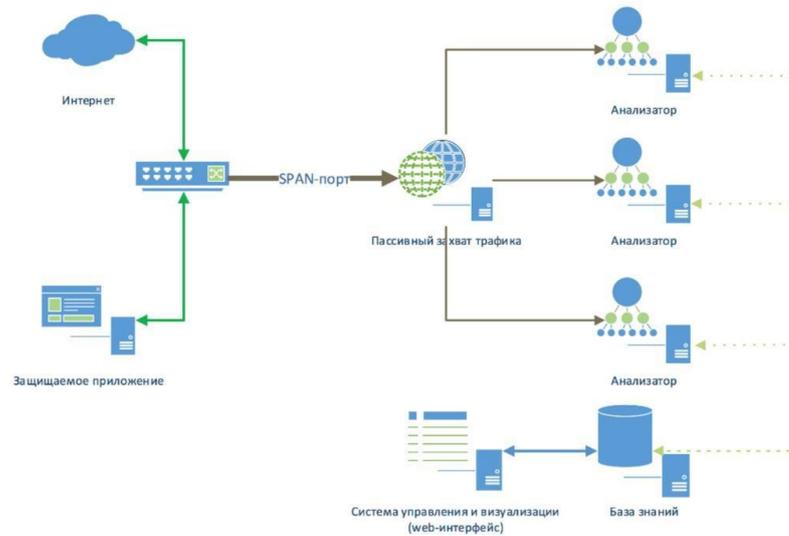


Рисунок 8 – Работа в режиме мониторинга

В режиме мониторинга проводится пассивный анализ трафика без возможности блокирования запросов. Для работы SolidWall WAF в режиме мониторинга необходимо до запуска процедуры установки, стандартными средствами ОС настроить сетевой интерфейс, на который отправляется копия трафика.

Примечание: все команды в данном разделе должны выполняться от имени суперпользователя (root).

Пусть ethX - это имя сетевого интерфейса, с которого должен происходить захват трафика. Необходимо убедиться, что конфигурация данного интерфейса описана в файле /etc/network/interfaces, и, в случае отсутствия, добавить следующие строки в конец файла:

```
auto ethX
iface ethX inet manual
```

Убедитесь, что нужный интерфейс находится в активном состоянии при помощи команды `ifconfig ethX`. В теле ответа команды должны присутствовать слова UP и RUNNING. В случае если интерфейс не находится в активном состоянии (DOWN), активируйте его командой `ifup ethX`.