



★ 4.74

Оценка

1783.06

Рейтинг

Selectel

IT-инфраструктура для бизнеса

[Подписаться](#)

is113 29 июн 2023 в 16:24

Snort и Suricata — простой путь к использованию IDPS: от установки на сервер до грамотной настройки



14 мин



18K

Блог компании Selectel, Информационная безопасность*, Системное администрирование*, Сетевые технологии*, Сетевое оборудование



Межсетевые экраны — один из первых эшелонов защиты интернет-сервисов с довольно широким функционалом по безопасности. В их состав обычно входит класс решений IDPS, который позволяет с высокой точностью определять нелегитимные запросы и блокировать их.

В этом материале рассказываю, что такое системы IDPS и какие они бывают. А также показываю, как их разворачивать на виртуальных серверах и настраивать сигнатуры для блокирования



+35



52



12 +12



Знакомство с IDPS

Intrusion Detection and Prevention System, IDPS — это системы обнаружения и предотвращения вторжения. По сути, IDPS мониторит транзитный и локальный трафик на попытки сканирования и атак, соотнося их с имеющимися сигнатурами. Если трафик «зловредный» — он блокируется.

Классификация IDPS и популярные решения

IDPS можно разделить на два класса — NIDS (Network Intrusion Detection System) и HIDS (Host-based Intrusion Detection). Первые — мониторят сетевой трафик, в то время как вторые — анализируют события хоста, в том числе приходящий и уходящий трафик внутри систем.

Как видно из названия, NIDS необходимо ставить на хосты, управляющие трафиком, а HIDS больше подходят для endpoint-хостов с локальными сервисами. Более подробно о классификации и особенностях IDPS-систем можно почитать в Академии Selectel.

В рамках статьи покажем, как начать работать с двумя представителями систем IDPS:


- Suricata (как инстанс в Ubuntu 20.04) — это высокопроизводительный софт для анализа трафика и поиска угроз;
- Snort (как пакет в pfSense 2.6.0) — это один из самых популярных IDPS с открытым исходным кодом.

Между этими решениями есть одно важное отличие. Snort работает только в однопоточном режиме, в то время как Suricata может запускаться в многопоточных сценариях и позволяет обрабатывать больше трафика одновременно.

Реклама. enid: 2VtzqeCsGc. ООО Селектел

Selectel

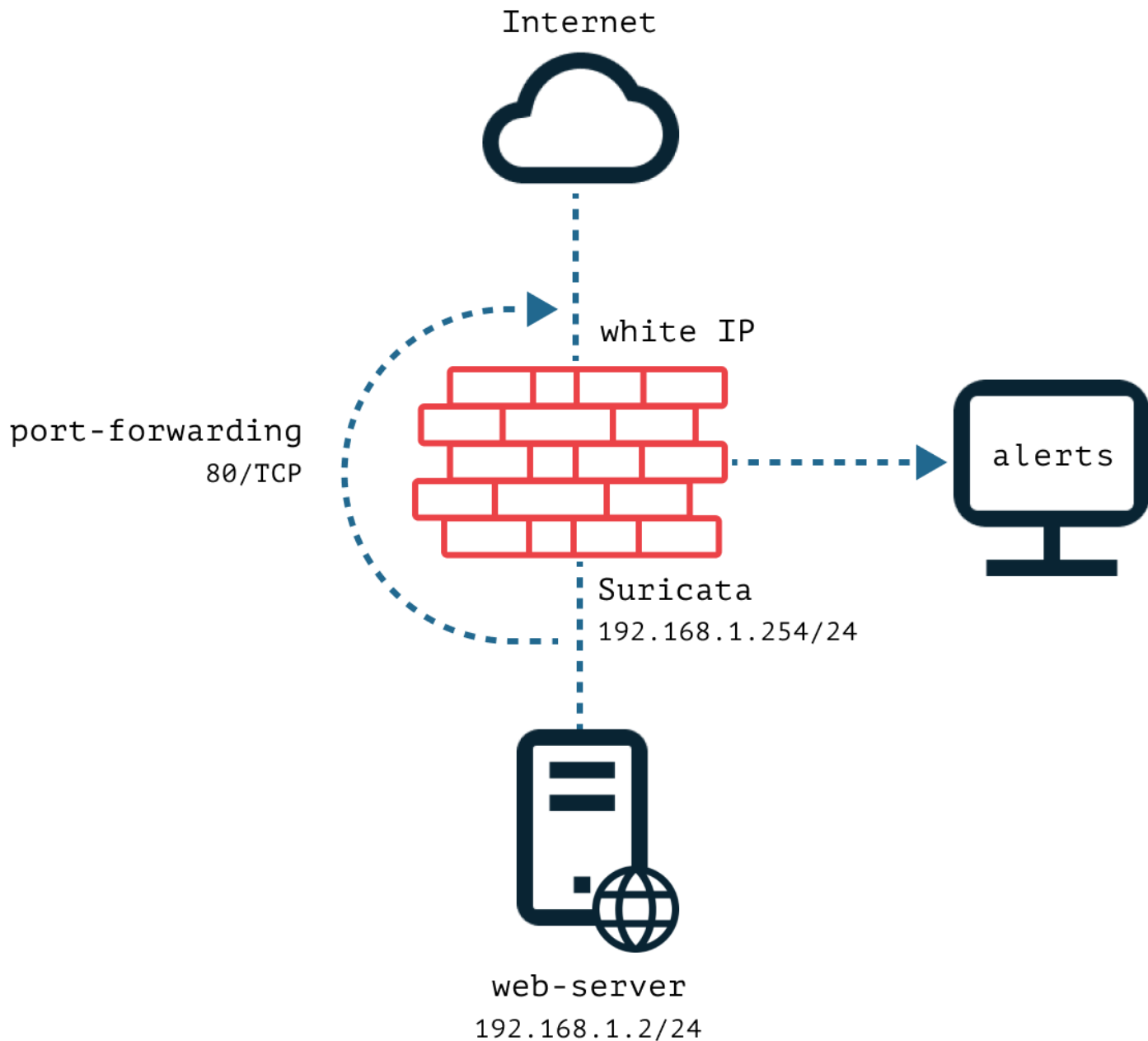
Переносите, храните
и обрабатывайте данные по 152-ФЗ



Сетевая схема на базе Suricata

В рамках статьи рассмотрим схемы включения IDPS в «разрыв».





Сетевая схема на базе Suricata

В данной схеме между целевым веб-сервером и интернетом установлена IDPS. То есть маршрутизацию и проброс портов обеспечивает именно хост с IDPS. Таким образом, правильно настроив систему, можно блокировать трафик при срабатывании сигнатур.

Настройка хоста

Для начала развернем виртуальный сервер с Ubuntu — хост для IDPS. Это можно сделать за несколько кликов: регистрируемся и входим в панель управления, переходим в раздел **Облачная платформа**, выбираем **Серверы** и настраиваем конфигурации.



Новый сервер

Имя и расположение

Имя Регион Пул

Источник

☒ Ubuntu 20.04 LTS 64-bit 512 МБ RAM, 5 Гб Диск

Конфигурация

☒ Фиксированные конфигурации
выбор из готовых наборов ресурсов

☐ Произвольная конфигурация
настройка каждого ресурса отдельно

☐ Локальный SSD NVMe диск Загрузочный диск без сетевых задержек. Чтение **12800** IOPS / Запись **6400** IOPS.

vCPU от 1 до 32 ядер RAM от 512 МБ до 256 Гб

Процессоры 2,2–2,4 ГГц.

Произвольные конфигурации с GPU доступны только в Москве (ru-7a).

Если вы не нашли подходящую конфигурацию, напишите в [службу поддержки](#) и мы подберем решение.

Сетевые диски

Тип диска Размер диска

Сеть

Подсеть

Выведем доступные сетевые интерфейсы. Один из них будет вести в интернет, а второй — в локальную сеть, ему необходимо назначить свободный адрес.

```
eth1: inet 192.168.1.254/24 brd 192.168.1.255 scope global eth1
```

Теперь настроим для локальной сети выход в интернет и заранее «опубликуем» веб-сервер наружу:

```
$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward
$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

```
$ sudo iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 80 -j DNAT --to-destination 192.1
$ sudo iptables -A FORWARD -p tcp -d 192.168.1.2 --dport 80 -m state --state NEW,ESTABLISHED,
```



```
$ sudo iptables-save > /etc/iptables/rules.v4
```

Вторым этапом развернем хост для веб-сервера, на который поставим Nginx и проверим доступность снаружи:

```
$ sudo apt install nginx -y
$ curl http://45.145.64.243
```

► [Что должен вернуть cURL запрос к Nginx ↓](#)

Отлично — страница отвечает, в логах Nginx можно увидеть подобные обращения:

```
$ tail -f /var/log/nginx/access.log
- - [25/Jun/2023:10:05:15 +0000] "PROPFIND / HTTP/1.1" 400 166 "-" "-"
- - [25/Jun/2023:10:05:15 +0000] "TRACE / HTTP/1.0" 405 166 "-" "Mozilla/5.00 (Nikto/2.1.5) ("
- - [25/Jun/2023:10:05:15 +0000] "TRACE / HTTP/1.0" 405 166 "-" "Mozilla/5.00 (Nikto/2.1.5) ("
- - [25/Jun/2023:10:05:15 +0000] "TRACK / HTTP/1.0" 405 166 "-" "Mozilla/5.00 (Nikto/2.1.5) ("
- - [25/Jun/2023:10:05:15 +0000] "TRACK / HTTP/1.0" 405 166 "-" "Mozilla/5.00 (Nikto/2.1.5) ("
- - [25/Jun/2023:10:05:15 +0000] "GET /TiVoConnect?Command=QueryServer HTTP/1.1" 404 162 "-"
- - [25/Jun/2023:10:05:15 +0000] "GET /TiVoConnect?Command=QueryContainer&Container=/&Recurse
- - [25/Jun/2023:10:05:15 +0000] "GET /cfappman/index.cfm HTTP/1.1" 404 162 "-" "Mozilla/5.00
- - [25/Jun/2023:10:05:15 +0000] "GET /cfdocs/examples/cvbeans/beaninfo.cfm HTTP/1.1" 404 162
- - [25/Jun/2023:10:05:15 +0000] "GET /cfdocs/examples/parks/detail.cfm HTTP/1.1" 404 162 "-"
```

Сервер начали сканировать — надо поспешить настроить IDPS. Система позволит отслеживать и блокировать обращения, которые будут совпадать с сигнатурами атак. Давайте поставим решение Suricata на хост.

Установка Suricata

Для начала скачаем необходимые зависимости.

```
$ sudo apt install libpcap3 libpcap3-dbg libpcap3-dev build-essential libpcap-dev libnet1-dev
```

Теперь у нас есть два способа, как установить систему Suricata на хост:

1. Сборка из исходников

Первый способ довольно простой: достаточно просто скачать архив и распаковать из него



Suricata.

```
$ wget https://www.openinfosecfoundation.org/download/suricata-6.0.13.tar.gz
$ ls
suricata-6.0.13.tar.gz
$ tar xzvf suricata-6.0.13.tar.gz
$ cd suricata-6.0.13
$ sudo ./configure --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/
$ sudo make
$ sudo make install
```

2. Установка из PPA

Второй способ — установить Suricata из Personal Package Archive, PPA. Это специальный репозиторий с open source-проектами разных компаний, в том числе разработчиков Suricata (OSIF).

```
$ sudo add-apt-repository ppa:oisf/suricata-stable
$ sudo apt-get update
$ sudo apt-get install suricata
```

Супер! Suricata установлена на хосте. Это можно проверить, введя `suricata -V` — специальную команду, которая возвращает версию установленной системы.

Обновление

После установки Suricata важно обновить правила (сигнатуры) и их источники:

```
root@suricata:~/suricata-6.0.12# suricata-update
</source lang="bash">
<spoiler title="Результат корректного обновления правил ↓">
<source lang="bash">
25/6/2023 -- 11:54:49 - <Info> -- Using data-directory /var/lib/suricata.
25/6/2023 -- 11:54:49 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
25/6/2023 -- 11:54:49 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules
25/6/2023 -- 11:54:49 - <Info> -- Found Suricata version 6.0.13 at /usr/bin/suricata.
25/6/2023 -- 11:54:49 - <Info> -- Loading /etc/suricata/suricata.yaml
25/6/2023 -- 11:54:49 - <Info> -- Disabling rules for protocol http2
25/6/2023 -- 11:54:49 - <Info> -- Disabling rules for protocol modbus
25/6/2023 -- 11:54:49 - <Info> -- Disabling rules for protocol dnp3
25/6/2023 -- 11:54:49 - <Info> -- Disabling rules for protocol enip
25/6/2023 -- 11:54:49 - <Info> -- No sources configured, will use Emerging Threats Open
25/6/2023 -- 11:54:49 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-6
100% - 3949155/3949155
25/6/2023 -- 11:54:50 - <Info> -- Done.
```



```

25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ap
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/de
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dh
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dn
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dn
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/fi
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ht
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ip
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ke
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/mo
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/nf
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/nt
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/sm
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/sm
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/st
25/6/2023 -- 11:54:50 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/tl
25/6/2023 -- 11:54:51 - <Info> -- Ignoring file rules/emerging-deleted.rules
25/6/2023 -- 11:54:53 - <Info> -- Loaded 43346 rules.
25/6/2023 -- 11:54:53 - <Info> -- Disabled 14 rules.
25/6/2023 -- 11:54:53 - <Info> -- Enabled 0 rules.
25/6/2023 -- 11:54:53 - <Info> -- Modified 0 rules.
25/6/2023 -- 11:54:53 - <Info> -- Dropped 0 rules.
25/6/2023 -- 11:54:54 - <Info> -- Enabled 131 rules for flowbit dependencies.
25/6/2023 -- 11:54:54 - <Info> -- Backing up current rules.
25/6/2023 -- 11:54:57 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: to
25/6/2023 -- 11:54:57 - <Info> -- Writing /var/lib/suricata/rules/classification.config
25/6/2023 -- 11:54:57 - <Info> -- Testing with suricata -T.
25/6/2023 -- 11:55:23 - <Info> -- Done.
root@suricata:~/suricata-6.0.12# suricata-update update-sources
25/6/2023 -- 11:56:27 - <Info> -- Using data-directory /var/lib/suricata.
25/6/2023 -- 11:56:27 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
25/6/2023 -- 11:56:27 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules
25/6/2023 -- 11:56:27 - <Info> -- Found Suricata version 6.0.13 at /usr/bin/suricata.
25/6/2023 -- 11:56:27 - <Info> -- Downloading https://www.openinfosecfoundation.org/rules/ind
25/6/2023 -- 11:56:28 - <Info> -- Adding all sources
25/6/2023 -- 11:56:28 - <Info> -- Saved /var/lib/suricata/update/cache/index.yaml

```

Далее в файле `/etc/default/suricata` сверим значение параметра `IFACE` с именем внешнего интерфейса хоста:

```

$ cat /etc/default/suricata | grep IFACE
IFACE=eth0
$ ip a
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
    link/ether fa:16:3e:29:e3:e3 brd ff:ff:ff:ff:ff:ff
    inet 45.145.64.243/29 brd 45.145.64.247 scope global eth0
        valid_lft forever preferred_lft forever

```




```
inet6 fe80::f816:3eff:fe29:e3e3/64 scope link
    valid_lft forever preferred_lft forever
```

Обратите внимание на строку `IFACE=eth0` и 2: `eth0`:
<`BROADCAST,MULTICAST,UP,LOWER_UP`>.

Названия интерфейсов совпадают, идем дальше. Проверим, чтобы это же значение стояло в файле `/etc/suricata/suricata.yaml` в блоках `pcap`, `pfring` и `af-packet`. По умолчанию там установлено `eth0` — совпадает с именем внешнего интерфейса.

Конфигурирование

Основным конфигурационным файлом `suricata` является `/etc/suricata/suricata.yaml` — откроем его и поправим настройки. В блоке `outputs` включим вывод данных:

```
outputs:
  # a line based alerts log similar to Snort's fast.log
  - fast:
    enabled: yes
    filename: fast.log
    append: yes
  - eve-log:
    enabled: yes
    filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
    filename: eve.json
    types:
      - alert:
        payload: yes          # enable dumping payload in Base64
        # payload-buffer-size: 4kb # max size of payload buffer to output in eve-log
        # payload-printable: yes   # enable dumping payload in printable (lossy) format
        # packet: yes             # enable dumping of packet (without stream segments)
        # metadata: no            # enable inclusion of app layer metadata with alert. D
        http-body: yes          # Requires metadata; enable dumping of HTTP body in Base
  - http-log:
    enabled: yes
    filename: http.log
    append: yes
```

Проверить валидность файла конфигураций можно с помощью команды `suricata -T -c /etc/suricata/suricata.yaml -v`.

► [Результат проверки конфигурации ↓](#)



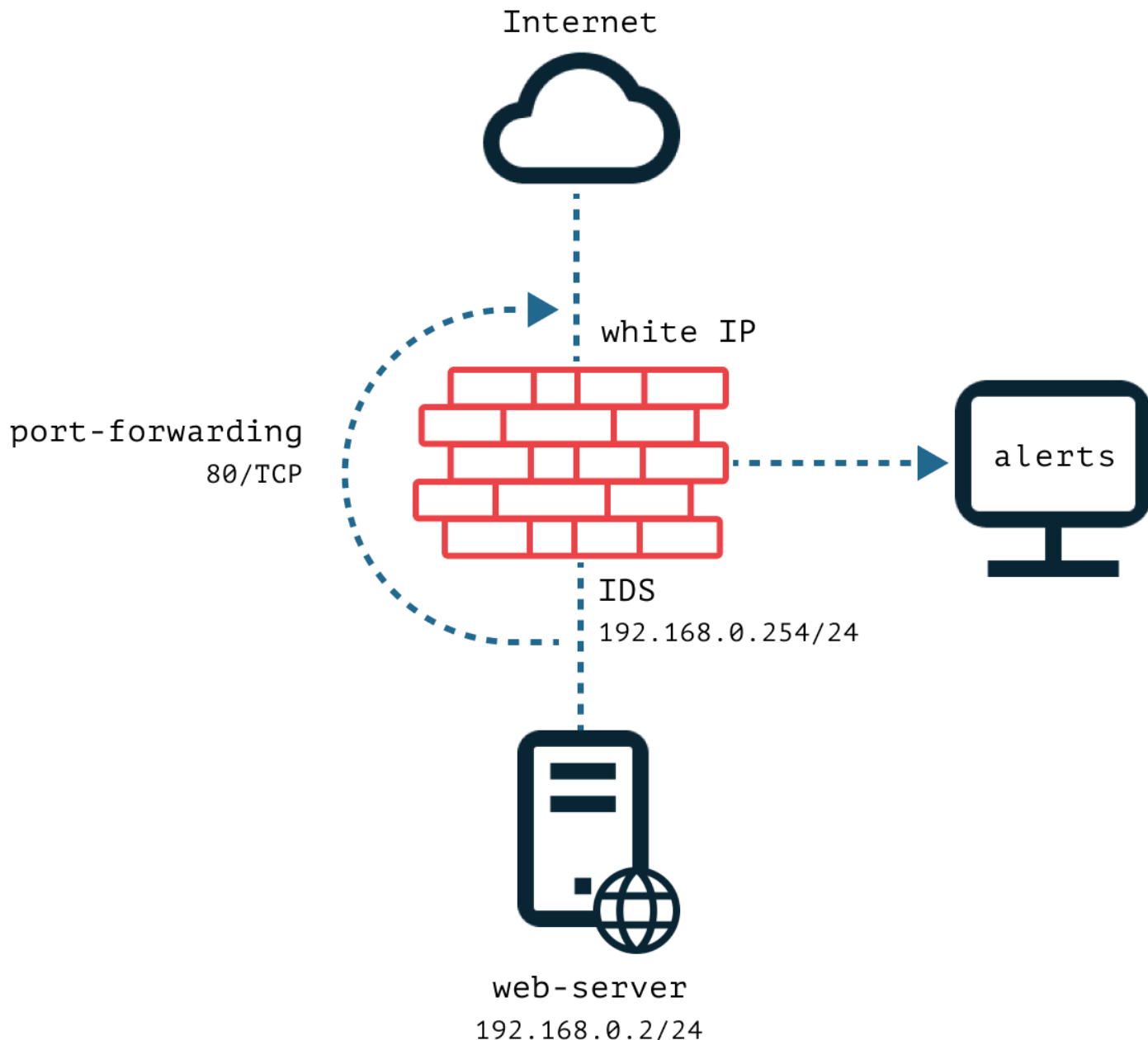
Если открыть лог-файлы, вы увидите обращения к веб-серверу, которые фиксирует Suricata. Это связано с тем, что в большинстве правил этой IDPS-системы указано действие `alert`. Чтобы Suricata не просто логировала подозрительный трафик, но и блокировала его, нужно добавить действие `drop` в сигнатурах, которые находятся по адресу `/var/lib/suricata/rules`. В этом же каталоге можно создавать файлы со своими правилами.

```
$ tail -f /var/log/suricata/http.log
06/25/2023-12:33:15.638309 45.145.64.243[**]/[**]Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (
06/25/2023-12:33:15.763447 45.145.64.243[**]/[**]Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (
06/25/2023-12:33:15.799758 45.145.64.243[**]/[**]Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (
06/25/2023-12:33:15.836635 45.145.64.243[**]/dpyyI9SK.link[**]Mozilla/5.00 (Nikto/2.1.5) (Eva
06/25/2023-12:33:15.873426 45.145.64.243[**]/dpyyI9SK.de[**]Mozilla/5.00 (Nikto/2.1.5) (Evasi
06/25/2023-12:33:15.909272 45.145.64.243[**]/dpyyI9SK.nlm[**]Mozilla/5.00 (Nikto/2.1.5) (Evas
06/25/2023-12:33:15.945103 45.145.64.243[**]/dpyyI9SK.var[**]Mozilla/5.00 (Nikto/2.1.5) (Evas
06/25/2023-12:33:15.980823 45.145.64.243[**]/dpyyI9SK.pm[**]Mozilla/5.00 (Nikto/2.1.5) (Evasi
06/25/2023-12:33:16.016680 45.145.64.243[**]/dpyyI9SK.config[**]Mozilla/5.00 (Nikto/2.1.5) (E
06/25/2023-12:33:16.053655 45.145.64.243[**]/dpyyI9SK.jsp[**]Mozilla/5.00 (Nikto/2.1.5) (Evas
06/25/2023-12:33:16.089380 45.145.64.243[**]/dpyyI9SK.pwd[**]Mozilla/5.00 (Nikto/2.1.5) (Evas
```

Логи подозрительных обращений к веб-серверу, которые записала Suricata.

Сетевая схема на базе Snort





Сетевая схема с промежуточным маршрутизатором

В данной схеме, как и в первой, есть промежуточный маршрутизатор pfSense, на котором настроен NAT для выхода веб-сервера в интернет. А также port-forwarding для доступа к службе веб-сервера снаружи.

Внутри репозитория pfSense есть пакет snort, который мы установим и настроим в режиме мониторинга. Таким образом, мы сможем наблюдать срабатывания IDS, но трафик до сервера блокироваться не будет.

В качестве IDS для второй схемы рассмотрим Snort — вероятно, самый популярный open source-IDPS. Давайте соберем целевую схему и посмотрим, как работать с этой системой.

Запуск хоста с веб-сервером

Разворачиваем хост для IDPS. Создаем сервер и настраиваем произвольную конфигурацию. Оптимальный вариант — 2 ядра vCPU, 4 ГБ ОЗУ, универсальный SSD-диск и Ubuntu в качестве операционной системы.



Новый сервер

Имя и расположение

Имя

ubuntu

Регион

Санкт-Петербург

Пул

ru-3a

Источник

Ubuntu 20.04 LTS 64-bit512 МБ RAM, 5 Гб Диск

Выбрать другой источник

Конфигурация

Фиксированные конфигурации
выбор из готовых наборов ресурсов

Произвольная конфигурация
настройка каждого ресурса отдельно

☐ Локальный SSD NVMe диск
Загрузочный диск без сетевых задержек. Чтение **12800** IOPS / Запись **6400** IOPS.

vCPU
от 1 до 32 ядер

—2+

RAM
от 512 МБ до 256 ГБ

—4+

МБГБ

Процессоры 2,2–2,4 ГГц.

Произвольные конфигурации с GPU доступны только в Москве ([ru-7a](#)).

Если вы не нашли подходящую конфигурацию, напишите [в службу поддержки](#) и мы подберем решение.

Сетевые диски

Тип диска

Размер диска

Универсальный SSD диск

—30+

ГБТБ

Добавить сетевой диск

Сеть

Подсеть

192.168.0.0/24 • (new_net)

Далее подключаемся к виртуальной машине из консоли панели управления и меняем адрес шлюза по умолчанию на 192.168.0.254. Это будущий LAN-адрес хоста с Short.

```
# ip route replace default via 192.168.0.254 dev eth0
```

После переключения трафика сервера на pfSense обновим локальную копию списка пакетов в репозиториях и поставим Nginx. А после — проверим доступность веб-сервера снаружи с помощью cURL-запроса.

```
# apt update && apt install nginx -y
$ curl http://45.145.64.242/
```

Запуск второго хоста

Теперь развернем второй хост, но уже с системой Short. В качестве него может выступить,



например, Linux-сервер, виртуальная машина с pfSense или межсетевой экран Selectel.

В рамках теста развернем виртуальную машину с pfSense 2.6 — ее также можно создать через панель управления. Сначала скачаем образ pfsense с официального сайта, а после — загрузим в хранилище образов.

Хранилище образов

Создать образ

Искать по имени, UUID

Санкт-Петербург

ru-3

По дате создания

pfSense-CE-2.6.0-RELEASE-amd64Linux

UUID: 6b84f87a-a9c0-4304-aa61-ab09764649b3

Санкт-Петербург / ru-3

Размер: 732 МБ

Статус: active

MD5: 5ca6d4cb89977022d2e76c9158eeeb67

Формат: iso

Создан: 25.06.2023, 12:00:00

Во время настройки конфигурации нужно выбрать загруженный образ в разделе **Источник**. Далее все стандартно: для сервера с pfSense будет достаточно 4 ядер vCPU, 8 ГБ ОЗУ и универсального SSD на 50 ГБ.

Серверы /

пfsense

ACTIVE

Power On

Refresh

More

Санкт-Петербург / ru-3a

e8d9127d-546b-4a5f-879e-aa8cce9c66be

Конфигурация

Сетевые диски

Порты

Статистика

Syslog

Консоль

Тип конфигурации

Произвольная

vCPU

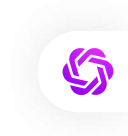
4 ядра

Память

8 ГБ

Изменить конфигурацию

После включения хоста назначаем адресацию, как указано на целевой схеме выше.





Порты

[Добавить порт](#)

Подсеть	IP-адрес	Публичный IP ⓘ	MAC
new_net	192.168.0.254	Подключить	fa:16:3e:e4:0a:ef
45.145.64.240/29	45.145.64.244		fa:16:3e:70:c1:83

Настройка портов

Применять изменения ⓘ

Вручную в файле конфигурации сети на сервере

Изменения в панели управления необходимо вручную дублировать в файл конфигурации сети на сервере.

[Редактировать](#)

```
8) Shell
Enter an option:

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
KVM Guest - Netgate Device ID: 88b8f2d604dce22f2355
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4: 45.145.64.242/29
LAN (lan)      -> vtnet1      -> v4: 192.168.0.254/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password
4) Reset to factory defaults  12) PHP shell + pfSense tools
5) Reboot system              13) Update from console
6) Halt system                 14) Enable Secure Shell (sshd)
7) Ping host                   15) Restore recent configuration
8) Shell                       16) Restart PHP-FPM

Enter an option: █
```

Супер! Теперь нужно провести первичную инициализацию pfSense, изменить пароль администратора — и pfSense готов к работе:



pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@95.213.254.17 (Local Database)
System	KVM Guest Netgate Device ID: 88b8f2d604dce22f2355
BIOS	Vendor: SeaBIOS Version: 1.10.2-1ubuntu1 Release Date: Tue Apr 1 2014
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE The system is on the latest version. Version information updated at Sun Jun 25 6:28:21 -03 2023
CPU Type	Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz 4 CPUs: 4 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

Netgate Services And Support

Interfaces

WAN	↑	10Gbase-T <full-duplex>	45.145.64.242
LAN	↑	10Gbase-T <full-duplex>	192.168.0.254

Snort Alerts

Interface/Time	Src/Dst Address	Description
----------------	-----------------	-------------

Наиболее подробно мы рассказали о настройке pfSense в отдельной статье.

Настроим проброс порта 80/TCP с Nginx в интернет. Это можно сделать в разделе Port Forward внутри панели pfSense.

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPT

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.0.2	80 (HTTP)		

Add Add Delete Save Separator

Установка и настройка Snort

Хост подготовлен к установке Snort. Это можно сделать через менеджер пакетов в pfSense. На данный момент, в репозиториях доступна версия Snort 2.9.20.



pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term

snort

Both ▾

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
snort	4.1.6	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.	+ Install
Package Dependencies: snort-2.9.20			

System / Package Manager / Package Installer

pfSense-pkg-snort installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

Please note that, by default, snort will truncate packets larger than the default snaplen of 15158 bytes. Additionally, LRO may cause issues with Stream5 target-based reassembly. It is recommended to disable LRO, if your card supports it.

This can be done by appending '-lro' to your ifconfig_ line in rc.conf.
====
Message from pfSense-pkg-snort-4.1.6:

--
Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured rulesets.
>>> Cleaning up cache... done.
Success



pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Package Manager / Installed Packages


Installed Packages Available Packages


Installed Packages

Name	Category	Version	Description	Actions
✓ snort	security	4.1.6	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.	 
Package Dependencies: snort-2.9.20				

Отлично! Теперь идем в раздел конфигурирования Snort и настраиваем обновления сигнатур в разделе Global Settings:



pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ 

Services / **Snort** / Global Settings 

Snort Interfaces **Global Settings** Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Snort Subscriber Rules

Enable Snort VRT ☐ Click to enable download of Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

Snort GPLv2 Community Rules

Enable Snort GPLv2 ☒ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open ☒ Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro ☐ Click to enable download of Emerging Threats Pro rules

[Sign Up for an ETPro Account](#)
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Sourcefire OpenAppID Detectors

Enable OpenAppID ☒ Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.

OpenAppID Version N/A (Not Downloaded)

Enable AppID Open Text Rules ☐ Click to enable download of the AppID Open Text Rules

Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is https://files.netgate.com/openappid/appid_rules.tar.gz.

FEODO Tracker Botnet C2 IP Rules

Enable FEODO Tracker Botnet C2 IP Rules ☒ Click to enable download of FEODO Tracker Botnet C2 IP rules

Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals to commit ebanking fraud. Since 2010, various malware families evolved from Feodo, such as Cridex, Dridex, Geodo, Heodo and Emotet.

В Snort есть несколько категорий сигнатур — community, registered и subscription. Подробнее о каждой можно узнать на официальном сайте.

Все архивы с сигнатурами Snort подтягивает из следующих репозиториев:
 SNORT_ENFORCING_RULES, ET_BASE_DNLD_URL, SNORT_GPLV2_DNLD,
 SNORT_OPENAPPID_DNLD_URL, SNORT_OPENAPPID_RULES,
 SNORT_ENFORCING_RULES, FEODOTRACKER.

Сигнатуры Snort можно использовать в качестве правил для Suricata. Также их можно конвертировать в сигнатуры для других IDPS-систем — например, с помощью fortios-ips-snort ретранслировать правила из Snort для Fortigate.

Далее необходимо установить параметры детектирования трафика в разделе Snort Interface.



- Pattern Match — алгоритм обнаружения подозрительных запросов.
- Blocking Mode — способ блокирования. По умолчанию можно установить на DISABLED.







pfSense
COMMUNITY EDITION



System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Snort / Interfaces

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (vtnet0)	  	AC-BNFA	DISABLED	WAN	  

 Add  Delete

В логах Snort (раздел Alerts) будет информация о выявленном вредоносном трафике, приходящим на наш опубликованный веб-сервер:



System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

Services / Snort / Alerts

Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync

Alert Log View Settings

Interface to Inspect

WAN (vtnet0)

Choose interface..

☐ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download
Clear

Alert Log View Filter

13 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-06-25 07:22:39	⚠	3	TCP	Unknown Traffic	109.207.173.75	34680	45.145.64.242	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2023-06-25 07:22:38	⚠	3	TCP	Unknown Traffic	109.207.173.75	34676	45.145.64.242	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2023-06-25 07:22:38	⚠	3	TCP	Unknown Traffic	109.207.173.75	34668	45.145.64.242	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2023-06-25 07:22:38	⚠	3	TCP	Unknown Traffic	109.207.173.75	34660	45.145.64.242	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2023-06-25 07:22:38	⚠	3	TCP	Unknown Traffic	109.207.173.75	34650	45.145.64.242	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2023-06-25 07:22:37	⚠	3	TCP	Not Suspicious Traffic	109.207.173.75	34650	45.145.64.242	80	119:2	(http_inspect) DOUBLE DECODING ATTACK
2023-06-25 07:22:37	⚠	3	TCP	Unknown Traffic	109.207.173.75	34648	45.145.64.242	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2023-06-25 07:22:37	⚠	3	TCP	Not Suspicious Traffic	109.207.173.75	34648	45.145.64.242	80	119:2	(http_inspect) DOUBLE DECODING ATTACK
2023-06-25 07:22:37	⚠	3	TCP	Unknown Traffic	109.207.173.75	34632	45.145.64.242	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2023-06-25 07:22:35	⚠	3	TCP	Unknown Traffic	109.207.173.75	44224	45.145.64.242	80	119:31	(http_inspect) UNKNOWN METHOD
2023-06-25 07:22:22	⚠	3	TCP	Unknown Traffic	109.207.173.75	54150	45.145.64.242	80	119:31	(http_inspect) UNKNOWN METHOD
2023-06-25 07:22:14	⚠	3	TCP	Not Suspicious Traffic	81.209.147.7	39316	45.145.64.242	80	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2023-06-25 07:22:14	⚠	3	TCP	Unknown Traffic	45.145.64.242	80	81.209.147.7	39316	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request

В описании алертов можно найти краткую информацию о найденных атаках. Также на сайте Snort есть более подробное описание — например, WEBROOT DIRECTORY TRAVERSAL и UNESCAPED SPACE IN HTTP URI.

Snort, как и Suricata, умеет блокировать IP-адрес источника атаки — это можно настроить в разделе Snort Interfaces/Block Settings:



Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States

☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block

BOTH

Select which IP extracted from the packet you wish to block. Default is BOTH.

А что насчет отправки логов, например, в собственную SIEM? Тут схема такая: Snort умеет отправлять данные в System Log, а pfSense — пересылать логи на удаленный syslog-сервер. Настраивается это довольно просто.

1. Настраиваем логирование в Snort:

pfSense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

Services / Snort / WAN - Interface Settings

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

WAN Settings

WAN Categories

WAN Rules

WAN Variables

WAN Preprocs

WAN IP Rep

WAN Logs

General Settings

Enable

☒ Enable interface

Interface

WAN (vtnet0)

Choose the interface where this Snort instance will inspect traffic.

Description

WAN

Enter a meaningful description here for your reference.

Snap Length

1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log

☒ Snort will send Alerts to the firewall's system log. Default is Not Checked.

2. Включаем отправку логов на внешний syslog-сервер:

Remote Logging Options

Enable Remote Logging

☒ Send log messages to remote syslog server

Source Address

LAN

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol

IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers

192.168.100.15:514

IP[:port]

IP[:port]

Remote Syslog Contents

☐ Everything

☐ System Events

☒ Firewall Events

☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)

☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)

☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)

☐ General Authentication Events

☐ Captive Portal Events

☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)

☐ Gateway Monitor Events

☐ Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)

☐ Network Time Protocol Events (NTP Daemon, NTP Client)

☐ Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

Настройка IDPS и применение сигнатур — не самая сложная задача, но крайне полезная, если вы заботитесь о безопасности своих сервисов. Важно понимать, что это не панацея от взлома, но важный элемент эшелонированной защиты инфраструктуры.

В следующей части разберем, как работает IDPS на отечественных NGFW. Интересно? Тогда следите за обновлениями на Хабре и в Академии Selectel. Увидимся!

Возможно, эти тексты тоже вас заинтересуют:

- Open source, собственные серверы и экспертиза: доступный межсетевой экран для инфраструктуры в Selectel
- Укрепление Nginx с помощью Fail2ban: тестируем и оцениваем «профит»
- Проблемы безопасности SNMP на практике: имитация атак и меры профилактики

Теги: selectel, idps, ips, suricata, snort, межсетевые экраны, информационная безопасность, pfsense, linux

Хабы: Блог компании Selectel, Информационная безопасность, Системное администрирование, Сетевые технологии, Сетевое оборудование

Редакторский дайджест

Присылаем лучшие статьи раз в месяц





Selectel

IT-инфраструктура для бизнеса

[ВКонтакте](#) [Telegram](#) [Сайт](#)



26

Карма

27

Рейтинг

@is113

Инженер ИБ

Подписаться



Комментарии 12

Публикации

ЛУЧШИЕ ЗА СУТКИ

ПОХОЖИЕ



ntsaplin 22 часа назад

Десантируем арктический ЦОД и орбитального сисадмина на дрейфующую льдину

6 мин

4.4K

+57

24

29 +29



DRoman0v 21 час назад

Самые неприятные поломки ноутбуков в моей практике. Чинить или не чинить — тот еще вопрос

4 мин

8.7K

+55

22

8 +8



Lex98 11 часов назад

Rust — это не «memory safe C»

Средний

25 мин

10K

Из песочницы



 +51  77  61 +61



timyrik20 23 часа назад

Об одной изящной задаче

 Простой  4 мин  7.8K

 +30  45  35 +35



andrey_nado 22 часа назад

Нет у меня никакого первого имени

 Простой  4 мин  7.9K

Мнение

 +28  38  76 +76



leonik 22 часа назад

Выращиваем тимлидов в домашних условиях

 Простой  8 мин  3.4K

Мнение

 +21  35  4 +4



roman-gorb 22 часа назад

Ускорение инференса LLM

 Средний  13 мин  2.2K

 +20  34  1 +1



Parker0 23 часа назад

Структура объекта в JavaScript движках

 20 мин  2.3K

 +20  52  0



markshevchenko вчера в 10:09

1. Почему вам стоит попробовать Nix (Nix в пилюлях)

 Средний  6 мин  5.4K

Тutorial

Перевод





Kilor 19 часов назад

Курс «PostgreSQL для начинающих»: #4 — Анализ запросов (ч.1 — как и зачем читать планы)



Средний



16 мин



5.5K

Тutorial



+17



140



0

Показать еще

ВАКАНСИИ КОМПАНИИ «SELECTEL»

Golang-разработчик в команду PaaS-продуктов

Selectel · Можно удаленно

Python Tech Lead в команду разработки Выделенных серверов и оборудования

Selectel · Можно удаленно

Python/Go-разработчик в команду Клиентских сервисов

Selectel · Санкт-Петербург

QA Fullstack Engineer в команду разработки Выделенных серверов

Selectel · Можно удаленно

Больше вакансий на Хабр Карьере

ИНФОРМАЦИЯ

Сайт	selectel.ru
Дата регистрации	16 марта 2010
Дата основания	11 сентября 2008
Численность	501–1 000 человек
Местоположение	Россия
Представитель	Влад Ефименко

ССЫЛКИ



Выделенный сервер от 26 рублей в день

selectel.ru

Сервер для 3D-моделирования и рендеринга

selectel.ru

Физический сервер от 800 рублей в месяц

selectel.ru

Облачные серверы от 280 рублей в месяц

selectel.ru

FAQ

slc.tl

Реферальная программа

slc.tl

Telegram-канал о технологиях

t.me

Telegram-канал про карьеру в IT

t.me

Вакансии

slc.tl

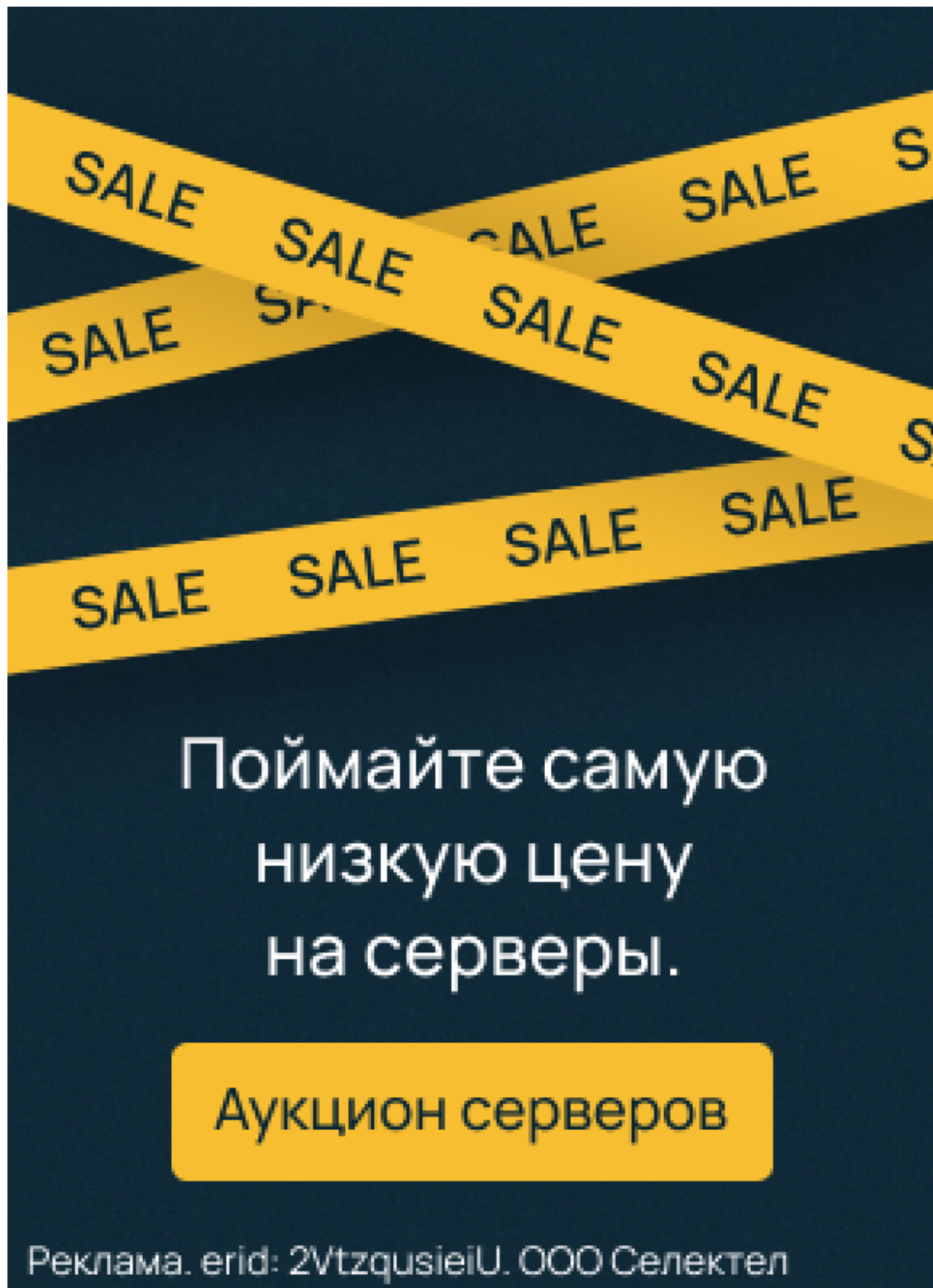
Академия Selectel

slc.tl

В КОНТАКТЕ

ВИДЖЕТ





БЛОГ НА ХАБРЕ

21 час назад

Самые неприятные поломки ноутбуков в моей практике. Чинить или не чинить — тот еще вопрос

 8.7K  8 

1 апр в 15:54

Как развернуть Minecraft на сервере и сделать бэкап мира

 2.4K  19 



31 мар в 16:25

Китайская компания Intellifusion представила 14-нм ИИ-процессор. Что это за чип и для чего он нужен?

 3.6K  4 +4

31 мар в 13:17

Бэкапы для самых маленьких и матерых

 9.7K  10 +10

30 мар в 13:19

Нидерланды сделают все, чтобы оставить ASML в стране: миллиардные инвестиции и всесторонняя помощь

 31K  65 +65

Ваш аккаунт

- Войти
- Регистрация

Разделы

- Статьи
- Новости
- Хабы
- Компании
- Авторы
- Песочница

Информация

- Устройство сайта
- Для авторов
- Для компаний
- Документы
- Соглашение
- Конфиденциальность

Услуги

- Корпоративный блог
- Медийная реклама
- Нативные проекты
- Образовательные программы
- Стартапам



Настройка языка

Техническая поддержка

