kaspersky

Kaspersky DDoS Protection for Networks, Filtering Nodes

Руководство по эксплуатации

Версия программы: 7

kaspersky

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 29.01.2021

https://www.kaspersky.ru
https://help.kaspersky.com/ru
https://support.kaspersky.ru

О "Лаборатории Касперского": https://www.kaspersky.ru/about/company

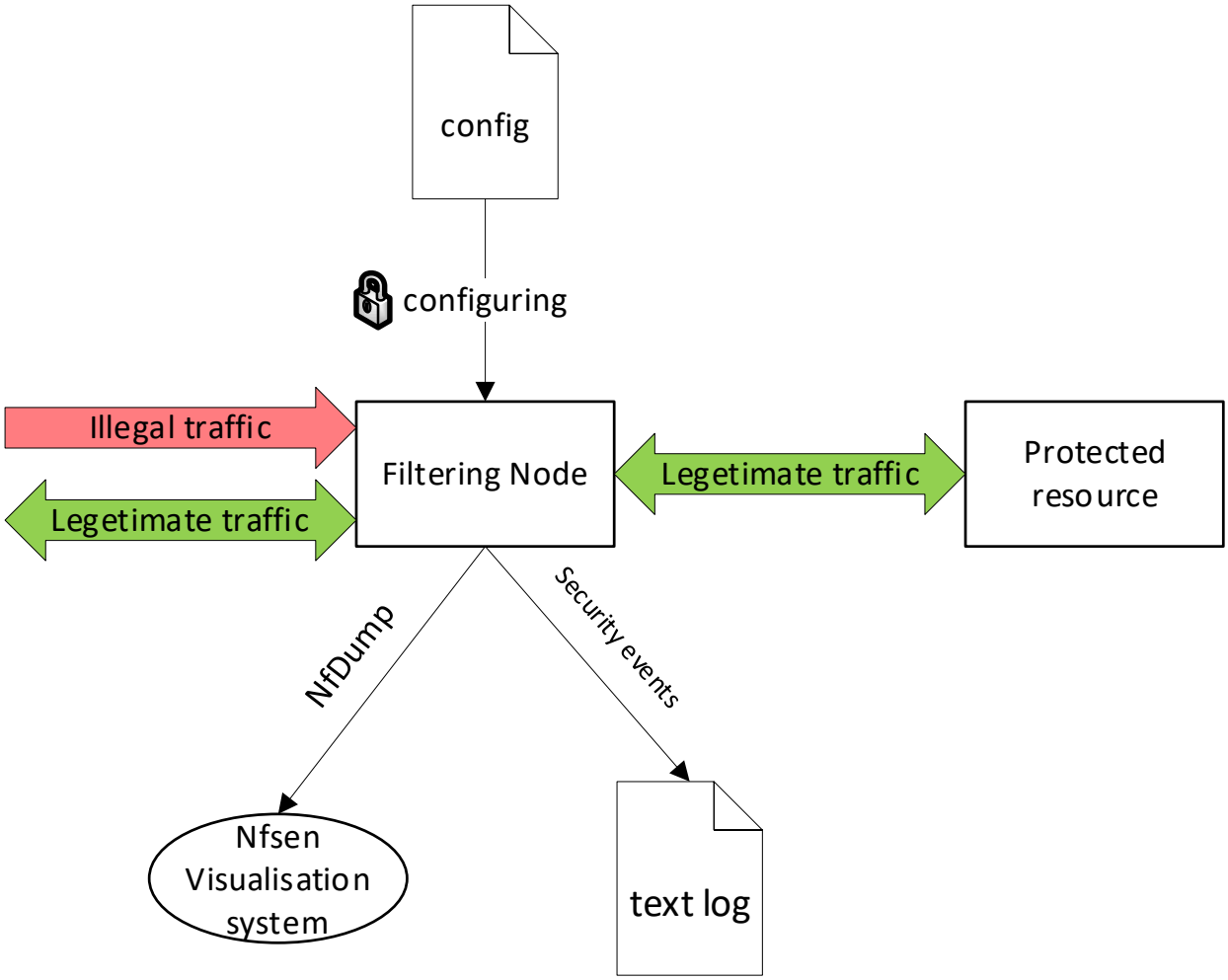
Оглавление

1.1. Описание подсистемы фильтрации KDP.

Подсистема фильтрации Kaspersky DDoS Protection представляет собой компонент Filtering Node, который в сочетании с некоторыми дополнительными программными средствами обеспечивает следующие возможности:

- Защита от DDoS атак уровня L3/L4 (фильтрация нелегитимного трафика)
- Формирование и выдача статистики до и после фильтрации
- Логирование блокировок
- Конфигурирование

Принципиальная схема компонентов необходимых для реализации возможностей Filtering Node:



Filtering Node (далее FN) разворачивается на отдельном сервере, там же разворачивает NFsen как средство визуализации поступающих с FN данных. На втором сервере разворачивается объект защиты (Protected resource) и генератор трафика, имитирующий как легитимный, так и атакующий трафик (Traffic Generator).

Конфигурирование FN осуществляется через шифрованный интерфейс, что позволяет обеспечить соответствие требованиям по защите от несанкционированного раскрытия и (или) модификации критических параметров, контролю целостности конфигурации, контролю доступа к функциям управления и настройкам. В ходе конфигурирования вводится информация о защищаемом ресурсе, в частности, защищаемые порты и протоколы, а также определяется конфигурация защитных модулей.

Получение информации о результатах работы FN возможно с помощью передачи информации о трафике, фильтруемом и проходящем через FN, по протоколу NetFlow средству визуализации NFsen,. Кроме того, информация о заблокированных при фильтрации IP адресах записывается в текстовый лог.

Самотестирование выполняется отдельным скриптом в составе FN, который запускается автоматически с периодичностью 1 раз в час. Информация о результатах самотестирования записывается в текстовый лог.

Контроль сохранения работоспособности при обработке некорректных данных обеспечивается проведением fuzzing-тестирования. Такое тестирования проводится для ключевых программных компонентов FN как обязательный этап цикла разработки при выпуске новых версий этих компонентов и перед передачей этих версий в эксплуатацию.

1.2 Требования к аппаратной платформе

Для обеспечения корректной работы системы, Filtering Node должна быть развёрнута на узле, соответствующем или превышающим следующие аппаратные характеристики:

- CPU: 8-ми ядерный процессор Intel Xeon или аналогичный
- RAM: Не менее 32 GB
- HDD: Не менее 300GB

Кроме того, необходимо использовать одну из следующих сетевых карт:

- Intel Gigabit ET Dual Port Server Adapter (82576)
- Intel Gigabit VT Quad Port Server Adapter (82575)
- Intel Single, Dual and Quad Gigabit Ethernet Controller (82580)
- Intel i210 and i211 Gigabit Ethernet Controller
- Intel i350 and i354 Gigabit Ethernet Controller
- Intel PRO/1000 CT Network Connection (82547)
- Intel PRO/1000 F Server Adapter (82543)
- Intel PRO/1000 Gigabit Server Adapter (82542)
- Intel PRO/1000 GT Desktop Adapter (82541PI)
- Intel PRO/1000 MF Dual Port Server Adapter (82546)
- Intel PRO/1000 MF Server Adapter (82545)
- Intel PRO/1000 MF Server Adapter (LX) (82545)
- Intel PRO/1000 MT Desktop Adapter (82540)
- Intel PRO/1000 MT Desktop Adapter (82541)
- Intel PRO/1000 MT Dual Port Server Adapter (82546)
- Intel PRO/1000 MT Quad Port Server Adapter (82546EB)
- Intel PRO/1000 MT Server Adapter (82545)
- Intel PRO/1000 PF Dual Port Server Adapter (82571)
- Intel PRO/1000 PF Quad Port Server Adapter (82571)
- Intel PRO/1000 PF Server Adapter (82572)
- Intel PRO/1000 PT Desktop Adapter (82572)
- Intel PRO/1000 PT Dual Port Server Adapter (82571)
- Intel PRO/1000 PT Quad Port Server Adapter (82571)
- Intel PRO/1000 PT Server Adapter (82572)
- Intel PRO/1000 T Desktop Adapter (82544)
- Intel PRO/1000 T Server Adapter (82543)

- Intel PRO/1000 XF Server Adapter (82544)
- Intel PRO/1000 XT Server Adapter (82544)
- Intel Gigabit ET Dual Port Server Adapter (82576)
- Intel Gigabit VT Quad Port Server Adapter (82575)
- Intel Single, Dual and Quad Gigabit Ethernet Controller (82580)
- Intel i210 and i211 Gigabit Ethernet Controller
- Intel i350 and i354 Gigabit Ethernet Controller
- Intel(R) 10 Gigabit XF SR/AF Dual Port Server Adapter
- Intel(R) 10 Gigabit XF SR/LR Server Adapter
- Intel(R) 82598EB 10 Gigabit AF Network Connection
- Intel(R) 82598EB 10 Gigabit AT CX4 Network Connection
- Intel(R) 82599ES 10Gbit Dual Port Server Adapter

При выборе аппаратной платформы для размещения системы рекомендуется проконсультироваться со службой технической поддержки.

1.2 Требования к ОС

Для обеспечения корректной работы системы, Filtering Node должна быть развёрнута в окружении операционной системы FreeBSD 12.1-RELEASE.

2.1 Настройка FN для защиты Protected Resource

Параметры защиты Protected Resource и конфигурация Filtering Node задаются в файле настроек программного компонента disp, непосредственно осуществляющего обработку и фильтрацию трафика, далее по тексту этот файл будет называться target.json. Пример такого файла можно увидеть в приложении 1.

2.2. Передача конфигурационного файла через шифрованный интерфейс

Загрузка конфигурации Filtering Node и настройка программного компонента disp производится с помощью специальным образом сформированного HTTPS-запроса к интерфейсу управления disp на порт TCP/8443. Группа эксплуатации KDP рекомендует использовать для этого утилиту curl, выполняя её со следующими параметрами:

```
curl -v -k --data-binary @ФАЙЛ_КОНФИГУРАЦИИ  --cert
СЕРТИФИКАТ_ДЛЯ_ДОСТУПА_К_ИНТЕРФЕЙСУ_КОНФИГУРАЦИИ --key
КЛЮЧ_К_СЕРТИФИКАТУ_ДЛЯ_ДОСТУПА_К_ИНТЕРФЕЙСУ_КОНФИГУРАЦИИ --cacert
СЕРТИФИКАТ_УДОСТОВЕРЯЮЩЕГО_ЦЕНТРА https://АДРЕС_СЕРВЕРА:8443/targets
```

Где:

1. -v — выводить подробную информацию о выполнении
2. -k — режим работы с явно указанными файлами сертификатов, без обращения к системному хранилищу сертификатов
3. --data-binary — передавать данные из конфигурационного файла в бинарном виде, без преобразований
4. --cert — путь к файлу сертификата для доступа к интерфейсу конфигурации disp
5. --key — путь к файлу ключа сертификата для доступа к интерфейсу конфигурации disp
6. --cacert — путь к файлу сертификата удостоверяющего центра, выписавшего сертификат для доступа к интерфейсу конфигурации disp

Доступ к интерфейсам disp осуществляется по протоколу HTTPS с использованием протокола TLS 1.3. Любая работа с шифрованными данными выполняется с использованием библиотеки openssl, для соблюдения требований по защите от несанкционированного раскрытия и (или) модификации критических параметров необходимо поддерживать данную библиотеку в актуальном состоянии.

2.3. Правила обращения с конфигурационным файлом Filtering Node:

1. Для соблюдения требований по защите от несанкционированного раскрытия и (или) модификации критических параметров, файл конфигурации Filtering Node рекомендуется хранить на одном хосте с настраиваемым программным компонентом disp.
2. Допускается хранение файла конфигурации Filtering Node на хосте, отличном от хоста, на котором работает настраиваемый программный компонент disp. При этом необходимо, чтобы хост, хранящий файл конфигурации, и хост, на котором работает disp, находились в пределах одного защищённого сетевого контура.
3. Загрузка конфигурации Filtering Node производится с помощью специальным образом сформированного HTTPS-запроса к интерфейсу управления disp на порт TCP/8443. Между хостом, с которого производится загрузка конфигурации, и хостом, на котором работает disp, должна быть обеспечена сетевая связность по порту TCP/8443 без каких-либо ограничений на отправку и получения HTTPS-запросов и ответов в обе стороны.

2.4. Получение конфигурации Filtering Node через шифрованный интерфейс

Получение конфигурации Filtering Node производится с помощью специальным образом сформированного HTTPS-запроса к интерфейсу управления disp на порт TCP/8443. Группа эксплуатации KDP рекомендует использовать для этого утилиту curl, выполняя её со следующими параметрами:

```
curl -v -k --cert СЕРТИФИКАТ_ДЛЯ_ДОСТУПА_К_ИНТЕРФЕЙСУ_КОНФИГУРАЦИИ --
key КЛЮЧ_К_СЕРТИФИКАТУ_ДЛЯ_ДОСТУПА_К_ИНТЕРФЕЙСУ_КОНФИГУРАЦИИ --cacert
СЕРТИФИКАТ_УДОСТОВЕРЯЮЩЕГО_ЦЕНТРА https://АДРЕС_СЕРВЕРА:8443/targets
```

Ключи команды описаны в разделе «2.2. Передача конфигурационного файла через шифрованный интерфейс.»

2.5. Получение статистики по трафику с интерфейсов Filtering Node.

Просмотр данных возможен через веб интерфейс NFSEN, который доступен по HTTP на управляющем интерфейсе:

```
http://АДРЕС_СЕРВЕРА
```

2.6. Получение информации о результатах работы Filtering Node.

Для обработки и фильтрации трафика в составе Filtering Node используется программный компонент disp. Disp —компонент, демонизируемый с помощью supervisord — сервиса демонизации. Disp отдаёт сообщения с результатами своей работы в STDOUT, а сообщения об ошибках — в STDERR, за сохранение этих данных отвечает supervisord и расположение этих файлов зависит от его настроек. По умолчанию данные сохраняются в два файла:

1. /var/log/supervisor/disp.out.log — лог результатов работы disp

2. /var/log/supervisor/disp.err.log — лог ошибок disp

Файлы с результатами работы хранятся на том же хосте, где работает disp — Filtering Node. Права для доступа к этим файлам могут настраиваться стандартными средствами ОС FreeBSD. По умолчанию доступ к этим файлам имеют все пользователи, обладающими достаточными правами для логина и просмотра файлов и директорий в системном каталоге /var/log хоста Filtering Node. Описание этих файлов можно увидеть в приложении 2.

Также возможно получение сводных данных о результатах работы Filtering Node, через веб интерфейс, обратившись к HTTS-интерфейсу disp с правильно сформированным запросом:

```
curl -v -k --cert СЕРТИФИКАТ_ДЛЯ_ДОСТУПА_К_ИНТЕРФЕЙСУ_КОНФИГУРАЦИИ --
key КЛЮЧ_К_СЕРТИФИКАТУ_ДЛЯ_ДОСТУПА_К_ИНТЕРФЕЙСУ_КОНФИГУРАЦИИ --cacert
СЕРТИФИКАТ_УДОСТОВЕРЯЮЩЕГО_ЦЕНТРА https://АДРЕС_СЕРВЕРА:8443/targets
```

Ключи команды описаны в разделе «2.2. Передача конфигурационного файла через шифрованный интерфейс.»

2.7. Контроль целостности конфигурации disp

Контроль целостности основных компонентов Filtering Node производится с помощью утилиты kdpintegritychecker, она проверяет исполняемые файлы и файлы конфигурации, для которых необходим контроль целостности, и сообщает о несовпадении контрольных сумм файлов, в которые были внесены изменения.

Настройка утилиты производится через конфигурационный файл integritychecker.conf, пример файла в приложении 3.

Первичная настройка утилиты выполняется следующей командой:

```
kdpintegritychecker -c КОНФИГУРАЦИОННЫЙ_ФАЙЛ_УТИЛИТЫ -w РАБОЧИЙ ФАЙЛ
УТИЛИТЫ update
```

где:

1. 1. -c путь к конфигурационному файлу утилиты
2. 2. -w путь к рабочему файлу утилиты

При запуске в таком режиме утилита потребует ввод пароля, котрый будет использован для шифрования рабочего файла. Этот пароль потребуется при запуске утилиты в режиме проверки.

2.8. Самотестирование disp

Для выполнения самотестирования периодический запуск утилиты контроля целостности в режиме проверки осуществляется с помощью утилиты cron. По умолчанию сценарий запуска по cron сохранен в файле integritychecker-periodic, путь к файлу /etc/cron.d/integritychecker-periodic

В результате первичной настройки kdpintegritychecker мы получили: конфигурационный файл утилиты, рабочий файл утилиты и пароль. Эти данные необходимо внести в сценарий запуска утилиты по cron:

```
0       *       *       *       *  date >>
ПУТЬ_КУДА_БУДЕТ_ЗАПИСЫВАТЬСЯ_ЛОГ/integritychecker.log &&
kdpintegritychecker -c КОНФИГУРАЦИОННЫЙ_ФАЙЛ_УТИЛИТЫ -w
РАБОЧИЙ_ФАЙЛ_УТИЛИТЫ -p ПАРОЛЬ check >>
ПУТЬ_КУДА_БУДЕТ_ЗАПИСЫВАТЬСЯ_ЛОГ/integritychecker.log
```

Записи о каждом запуске утилиты и результаты ее работы сохраняются в файл `integritychecker.log`, пример файла в приложении 4.

2.9. Проверка версии установленного пакета disp

Программный компонент disp разворачивается как стандартный пакет FreeBSD с помощью стандартного пакетного менеджера pkgng. Для проверки установленной версии пакета достаточно выполнить команду pkg info disp. Например:

```
[gut@fn ~]$ pkg info disp
disp-7.8.2
Name           : disp
Version        : 7.8.2
Installed on   : Wed Feb  3 14:09:46 2021 MSK
Origin         : kdp/disp
Architecture   : FreeBSD:12:amd64
Prefix         : /usr/local
Categories     : kdp net kld
Licenses       : NONE
Maintainer     : kdp@kaspersky.com
WWW            : https://gitlab.kdp/developers/dispatcher
Comment        : Netmap-based traffic dispatcher
Shared Libs required:
            libczmq.so.4
            libpcre.so.1
            liburcu-qsbr.so.6
            libzmq.so.5
            liburcu-cds.so.6
            libGeoIP.so.1
            librdkafka.so.1
            libjansson.so.4
Annotations    :
            FreeBSD_version: 1201000
Flat size      : 1.31MiB
Description    :
Netmap-based traffic processor

WWW: https://gitlab.kdp/developers/dispatcher
```

Приложение 1

Пример конфигурационного файла disp


```
[
{
 "name": "test-3",
 "ip": [
  "192.168.7.2"
 ],
 "id": 15,
 "nb_id": [
  "31"
 ],
 "nb": [
  "192.168.7.0/24"
 ],
 "type": "PROTECTED",
 "generate?": false,
 "one-way?": false,
 "blacklist": [],
 "whitelist": [],
 "services": [
  {
   "module": "sflow",
   "proto": "ip",
   "m_id": 220003922,
   "destination-port": 6343,
   "sampling": 100,
   "destination-ip": "10.134.9.2"
  },
  {
   "module": "bwlist",
   "proto": "ip",
   "m_id": 200000015,
   "filter-upstream?": true
  },
  {
   "module": "blklist",
   "proto": "ip",
   "m_id": 150000015
  },
  {
   "module": "tcp",
   "proto": "tcp/80",
   "m_id": 142988,
   "enabled": 1,
   "profile_id": 5692,
   "dry-run?": false,
   "close-timeout": 10,
   "ecr-rst-fine": 0,
   "ecr-rst-life": 0,
   "ecr-syn-fine": 0,
   "ecr-syn-life": 0,
   "mss": 1436,
```

```
  "syn-timeout": 60,
  "backlog-timeout": 30,
  "buffer-data?": false,
  "max-backlog": -1,
  "max-buffers": 10,
  "max-bufmem": 100000000,
  "wait-for-data?": false,
  "active-timeout": -1,
  "inactive-timeout": 3600,
  "brl-burst": 90000,
  "brl-rate": -1,
  "brl-rate-fine": 0,
  "connections-pip": -1,
  "connections-pip-fine": 0,
  "connections-pip-th": 0,
  "crl-burst": 10,
  "crl-rate": -1,
  "crl-rate-fine": 0,
  "global-brl-burst": 1,
  "global-brl-rate": 0,
  "global-crl-burst": 1,
  "global-crl-rate": 0,
  "global-prl-burst": 1,
  "global-prl-rate": 0,
  "min-window": 0,
  "min-window-fine": 0,
  "prl-burst": 100,
  "prl-rate": 500,
  "prl-rate-fine": 1
 },
 {
  "module": "sflow",
  "proto": "ip",
  "m_id": 220003945,
  "destination-port": 6344,
  "sampling": 100,
  "destination-ip": "10.134.9.3"
 },
 {
  "module": "accept",
  "proto": "tcp/80",
  "m_id": 230003945
 },
 {
  "module": "backflow",
  "proto": "tcp/0",
  "m_id": 190002791,
  "hole-life": 180,
  "min-port": 32768
 },
 {
  "module": "backflow",
  "proto": "udp/0",
  "m_id": 180002791,
```

```
      "hole-life": 180,
      "min-port": 32768
    }
  ]
},
114]
```

Описание конфигурационного файла disp

Ресурс (цель)

- должен иметь ключ "ip": простой IPv4 или IP/длина_маски_подсети.

  Длина маски >= 24.

  Перекрытие IP-адресов ресурсов считается ошибкой.

  Допускается также список адресов тех же форматов.

- должен иметь ключ "services": массив объектов типа сервис.

- может иметь ключ "name": имя цели для отладки.

- может иметь ключ "id": число, служащее для идентификации цели (см. ниже).

- может иметь ключи "blacklist" и "whitelist" (см. ниже).

Сервис

- должен иметь ключ "module": название одного из защитных модулей.

- может иметь ключ "proto": название протокола (ip, icmp, tcp, udp), при наличии заголовков которого в пакете он будет передан модулю.

Через опциональный слеш может идти номер порта. В этом случае в пакете будет проверяться и номер порта-получателя.

- может иметь ключ "service": название сервиса из /etc/services. Оно будет преобразовано в пару {протокол, порт}.

- если "proto" и "service" опущены, модулю будут переданы все пакеты IP.

- может иметь ключ "dry-run?": умолчание false. Если true, то модуль не отбрасывает пакеты

(DROP заменяется на ACCEPT) и не штрафует, но пишет вердикт в лог.

- для защиты одного сервиса несколькими модулями придется описать сервис несколько раз.

Ключ с неизвестным именем игнорируется (можно использовать для комментариев).

Несколько ключей с одним именем считаются ошибкой (ограничение Json).

При обработке пакета диспетчер находит цель и просматривает её список сервисов строго по порядку

в поисках сервиса, подходящего по протоколу и порту.

Если ни одного подходящего сервиса не найдено, пакет может быть передан в ОС (-O).

Если же последний сервис вернул NEXT или ключ -O не указан, пакет отбрасывается.

Пример: пропускаем ssh и telnet. Пропускаем все UDP, кроме как на порт 137.

```
[
 {
  "ip": "10.16.19.0/24",
  "": "this is the first target",
  "name": "Kitchen Sink",
  "services": [
   {
    "service": "ssh",     "module": "accept"
   },
   {
    "service": "telnet", "module": "accept"
   },
   {
    "proto": "udp/137",          "module": "drop"
   },
   {
    "proto": "udp",              "module": "accept"
   }
  ]
 }
]
```

Описание опций конфигурационного файла disp (настройки Protected resource)

- name – имя Protected Resource.

- ip — IP адреса Protected Resource.

- id — идентификатор Protected Resource в системе. Служебная настройка, менять которую не рекомендуется.

- nb_id — идентификатор сетевого бока (подсети) в системе, в который входя адреса Protected Resource. Служебная настройка, менять которую не рекомендуется.

- nb — сетевой блок (подсеть), в который входя адреса Protected Resource.

- type — тип обслуживания Protected Resource.

- generate? — если установить в true, то при приходе первого пакета на целевой IP цель порождает из себя подцель и привязывает её на этот IP. Фактически опция контролирует, делить или нет собираемые статистические данные по отдельным адресам ресурса или собирать эти данные по ресурсу целиком.

- one-way? — опция показывает, как трафик Protected Resource проходит через FN: входящий и исходящий или только входящий.

- blacklist — чёрный список IP адресов, трафик которых при обращении к Protected Resource безусловно блокируется.

- whitelist — белый список IP адресов, трафик которых при обращении к Protected Resource безусловно пропускается.

- services – настройки модулей disp, используемых для обслуживания Protected Resource.

Описание опций конфигурационного файла disp (настройки модулей disp)

Модули sflow, bwlist, blklist, accept и backflow являются служебными модулями, настройки которых менять не рекомендуется. При необходимости изменения настроек этих модулей рекомендуется обратиться в службу технической поддержки.

Описание настроек модуля tcp:

- proto — протокол и порт, с трафиком которых будет работать модуль

- m_id — Уникальный в пределах узла номер модуля (32 бита). На всех узлах кластера нумерация должна совпадать!

- enabled — флаг включения или отключения модуля. Модули с флагом enabled = 0 не используются при обработке трафика.

- profile_id — идентификатор профиля фильтрации в системе, на котором работает экземпляр модуля. Служебная настройка, менять которую не рекомендуется.

- dry-run? — флаг, указывающий disp, что модуль работает в режиме проверки. В этом режиме трафик обрабатывается согласно настройкам модуля, однако пакеты, попавшие под правила блокировки, не отбрасываются. Настройка используется при тестировании и в обычном режиме всегда должна быть “false”.

- close-timeout — Секунд перед удалением соединения из таблицы. Отсчитывается от полного закрытия соединения.

- ecr-rst-fine — На сколько штрафовать за попытку подключения, если ресурс заблокирован за RST на SYN.

- ecr-rst-life — На сколько секунд блокировать попытки соединения с ресурсом после того, как этот ресурс вернул RST на SYN.

- ecr-syn-fine — На сколько штрафовать за попытку подключения, если ресурс заблокирован за syn-timeout.

- ecr-syn-life — На сколько секунд блокировать попытки соединения с ресурсом после того, как был обнаружен syn-timeout.

- mss — MSS _цели_, передаваемый клиенту в первом SYN+ACK. Когда SYN от цели содержит меньшее значение MSS, это значение замещает конфигурационное.

- syn-timeout — Сколько секунд пытаться установить соединение с целью. Пока от цели не получен SYN+ACK, ей повторно передается SYN с интервалами 2, 4, 8... секунд.

- backlog-timeout — Время хранения соединений, пока они не получили ACK от пользователя.

- buffer-data? — Включает режим буферизации запроса, пока не установлено соединение с целью.

- max-backlog — Маскимальное количество соединений, которые ожидаютустановления без использования SYN proxy. Эти соединения создаются при приходе SYN от пользователя, при этом SYN пропускается к цели без изменений. Когда max-backlog превышен, в ответ на SYN пользователю отсылается SYN cookie, а соединение не создается. Если max-backlog установлен в 0, проксирование всегдавключено. Если max-backlog установлен в -1, проксирование всегда ВЫключено, соединения создаются только по SYN+ACK от цели.

- max-buffers — Максимум буферов, накапливаемых для одного соединения.

- max-bufmem — Максимум памяти под буферизацию запросов.

- wait-for-data? — Включает режим, когда соединение создается только по ACK с данными. Пустые ACK без соединения игнорируются.

- active-timeout — Через сколько секунд сбрасывать любое установленное соединение. При значении -1 соединения не сбрасываются.

- inactive-timeout — Через сколько секунд после приема последнего пакета сбрасывать УСТАНОВЛЕННОЕ соединение.

- brl-rate — Ограничение на скорость передачи с одного адреса. При превышении темпа пакет игнорируется.

- brl-burst — Байт с одного адреса в кратковременном пике. (Параметр алгоритма Token Bucket).

- brl-rate-fine — Штрафы, добавляемые при превышении предела скорости передачи по байтам.

- connections-pip — Максимум допускаемых соединений с одного адреса. Не считает соединения, по которым прошёл хоть один FIN! Соединение сперва устанавливается с клиентом с применением SYN cookies, затем проверяется предел, и, если он превышен, соединение разрывается. Иначе же соединение добавляется в таблицу и доустанавливается с целью в течение syn-timeout.

- connections-pip-th — Количество соединений в таблице ресурса, начиная с которого обрабатывается ограничение connections-pip.

- connections-pip-fine — Штрафы, добавляемые при превышении предела соединений.

- crl-rate — Ограничение на усредненный темп установления соединений с одного адреса. Требует указания connections-pip. Допустимые значения *-rate от 1e-3 до 1e7 [соед./с]

- crl-burst — Соединений с одного адреса в кратковременном пике. (Параметр алгоритма Token Bucket). Допустимые значения *-burst от 1 до 1000000.

- crl-rate-fine — Штрафы, добавляемые при превышении предела скорости установки новых соединений.

- global-brl-burst — Порог включения фильтрации по байтам. Байт со всех адресов в кратковременном пике. (Параметр алгоритма Token Bucket).

- global-brl-rate — Ограничение на скорость передачи со всех адресов. При превышении темпа включается фильтрация по байтам.

- global-crl-burst — Порог включения фильтрации по соединениям. Соединений со всех адресов в кратковременном пике. (Параметр алгоритма Token Bucket).

- global-crl-rate — Ограничение на скорость установки соединений со всех адресов. При превышении темпа включается фильтрация по соединениям.

- global-prl-burst — Порог включения фильтрации по пакетам. Байт со всех адресов в кратковременном пике. (Параметр алгоритма Token Bucket).

- global-prl-rate — Ограничение на темп передачи пакетов со всех адресов. При превышении темпа включается фильтрация по пакетам.

- min-window — Если размер окна в ACK от клиента меньше этой величины, сбросить соединение и оштрафовать.

- min-window-fine — Штрафы, добавляемые при получении ACK-пакета с размером окна меньше, чем min-window.

- prl-rate — Ограничение на темп передачи пакетов с одного адреса. При превышении темпа пакет игнорируется.

- prl-burst — Пакетов с одного адреса в кратковременном пике. (Параметр алгоритма Token Bucket).

- prl-rate-fine — Штрафы, добавляемые при превышении темпа передачи пакетов с одного адреса.

Приложение 2

Интерпретация данных лог файлов disp

Запуск компонента disp

При старте disp в лог будет записана информация подобная следующей:

```
210225 135402 main: disp-7.7.3 src=2fc59a77
210225 135402 readini: processed /usr/local/etc/disp.ini
210225 135402 announce: tid 100927 ~ target splitter
210225 135402 announce: tid 100928 ~ ctimer
210225 135402 announce: tid 100930 ~ atimer
210225 135402 init_tcpstat: 1146 services
210225 135402 init_kafka: rdkafka 0.11.6
(kafka2.linx.kdp:9093,kafka2.ost.kdp:9093,kafka2.kur.kdp:9093) node #0
210225 135402 announce: tid 101025 ~ kafka receiver
210225 135402 open_ifaces: 'span' 4 rings, 2048 slots, dirty
210225 135402 open_ifaces: 'span' 90:e2:ba:e5:82:71 ->
aa:aa:aa:aa:aa:00
210225 135402 open_ifaces: 'span' IP not assigned
210225 135402 kafka_recv: 15 partitions in fines_spanner
210225 135402 alloc_rings: |0000|
210225 135404 alloc_rings: (oooo)
210225 135404 announce: tid 101039 ~ worker
210225 135404 announce: tid 101058 ~ worker
210225 135404 make_workers: created 4 workers
210225 135404 announce: tid 101059 ~ worker
210225 135404 announce: tid 101062 ~ HTTP server
210225 135404 announce: tid 101061 ~ all-purpose timer
210225 135404 config_init: reloading /tmp/disp-0:8080.json
210225 135404 init_geoip: loaded /usr/local/share/GeoIP/GeoIP.dat
210225 135404 announce: tid 101041 ~ worker
```

Изменение состава защищаемых объектов

При измении состава защищаемых объектов в лог будет записана информация подобная следующей:

```
210225 135404 jadd: 'kdp.kaspersky.com 82.202.189.26 195.8.62.26'
```

Обращения к интерфейсам disp

При обращен в лог будет записана информация подобная следующей:

```
210225 132059 httpa: from 127.0.0.1
210225 132059 cb_hc: -<----->- GET /targets
210225 132059 cb_mc: replying...
210225 132059 http_status_line: 200 OK
```

```
210225 132059 http: closing...
210225 132059 httpa: from 127.0.0.1
210225 132059 cb_hc: -<----->- GET /version
210225 132059 cb_mc: replying...
210225 132059 http_status_line: 200 OK
210225 132059 http: closing...
```

Информация о блокировках посетителей защищаемых объектов

При блокировке посетителя, обращающегося к защищаемому объекту, в лог будет записана информация подобная следующей:

```
210225 132806 blklist_fine: IP:192.241.222.63,FIRST:2021-02-25
13:28:06,UNTIL:2021-02-25 13:38:33,BY:geofilter,INCR:50,NOW:50
```

Приложение 3

```
{
 "version": "1.0.1",
 "loglevel": "INFO",
 "sections":
  {
   "disp":
    {
     "files":
     [
      "/usr/local/etc/disp.ini",
      "/usr/local/etc/supervisord.conf.d/disp.conf",
      "/usr/local/bin/disp"
     ]
    }
  }
}
```

Приложение 4

```
Wed Feb  3 18:12:22 MSK 2021
Password OK
Checking integrity...
Checking section disp
Hashing files
2 hash OK
1 hash CHANGED
0 NEW files or tables
0 DELETED files or tables

Hash CHANGED
/usr/local/etc/disp.ini
Done
```

Приложение 5: сведения о передаваемых данных

1. Данные о трафике, собираемые и обрабатываемые системой при получении, оценке, фильтрации, маршрутизации и возврате трафика (другими словами, при любых действиях над трафиком) не передаются за приделы системы.
2. Для обновления ОС и стандартных пакетов системы используются официальные репозитории FreeBSD. При обновлении из официальных репозиториев за пределы системы могут передаваться данные об обновляемых пакетах.

Приложение 6: сведения о производительности системы.

В ходе проведения нагрузочных испытаний была подтверждена способность системы обрабатывать трафик и фильтровать DDoS атаки на скоростях не менее 10 Гбит/с.

Испытания проводились на следующей аппаратной платформе:

Lenovo/IBM x3550 M5
CPU: E5-2630 v4 10C 2.2GHz x 2
RAM: 16GB DDR4 x 8 = 128GB RAM
HDD: 300GB 10K 12Gb/s SAS 2.5" x 2
NIC1: Intel 82599ES dual port 10Gbit x 1