Руководство пользователя
iAdmin URL Filter
версия 1.4

Internet Administrator Company ltd. © 2024 http://www.iadmin.ru, e-mail: sales@iadmin.ru,
тел. +7 (495) 5147244

РАЗДЕЛ 1 – ВВЕДЕНИЕ 3
Раздел 1.1. – Краткое описание 3
Раздел 1.2. – Изменения версий 3
РАЗДЕЛ 2 – УСТАНОВКА И НАСТРОЙКА 5
Раздел 2.1. – Системные требования 5
Раздел 2.2. – Установка 5
Раздел 2.3. – Настройка внешнего клиента c-icap 6
Раздел 2.4. – Настройка доступа 7
ПРИЛОЖЕНИЕ А. 9

Internet Administrator Company ltd. © 2024 http://www.iadmin.ru, e-mail: sales@iadmin.ru,
тел. +7 (495) 5147244

РАЗДЕЛ 1 – ВВЕДЕНИЕ

Раздел 1.1. – Краткое описание

iAdmin URL Filter – это программное обеспечение, позволяющее блокировать доступ в Интернет по категориям веб-сайтов по базе iAdmin URL.

iAdmin URL Filter работает как сервер по протоколу ICAP для стороннего HTTP прокси-сервера или аппаратного устройства, через который осуществляется доступ в Интернет для других пользователей.

iAdmin URL Filter состоит из трех компонентов:
- c-icap (https://c-icap.sourceforge.net/) реализует непосредственно протокол ICAP и является открытым программным обеспечением по лицензии GPL.
- iadmin_filter, реализованный в виде библиотеки для c-icap, осуществляет фильтрацию по правилам доступа.
- iAdmin URL SDK реализует механизм определения категорий веб-сайтов, содержит в себе проприетарную базу веб-сайтов и механизм ее обновления.

Раздел 1.2. – Изменения версий

1. Версия 1.4

   - новый тип правила match добавляет в http request заголовок с номером категории для анализа на стороне squid. Squid обязательно должен быть собран с параметром “./configure --enable-http-violations” и удалить его перед отправкой на сайт.

2. Версия 1.3

   - добавлена возможность фильтрации по группам пользователей в Squid или по любому другому acl.

3. Версия 1.2

   - добавлена возможность фильтрации в правилах по IP, UserName и доменным именам.
   - страница блокировки отображает категории сайта, заблокированное правило и причину блока, но только по HTTP протоколу. Для установления причины блока по HTTPS можно убрать S из адреса и сделать новый запрос (если нет редиректа на сайте). Либо через icap клиента, см Раздел 2.2 пункт 6.
   - вывод версии iAdmin Filter можно получить, вызвав c-icap-client -s "iadmin_filter". Текущая работающая версия будет указана в заголовке Service.

4. Версия 1.1

   - добавлен отдельный демон iadmin_service, который обслуживает базу iAdmin URL в памяти и предоставляет интерфейс для определения категорий через механизм внутренних сокетов AF_UNIX.
   - сервер c-icap теперь не грузит базу в себя, а обращается за категориями в демон iadmin_service. Поэтому снимается ограничение на создание отдельных процессов c-icap.
   - механизм лицензирования контролирует не более 1000 запросов с одного хоста или имени пользователя в минуту. Если будет превышение – категории

Internet Administrator Company ltd. © 2024 http://www.iadmin.ru, e-mail: sales@iadmin.ru, тел. +7 (495) 5147244

определятся не будут. Для этого обязательно включайте передачу Client IP \ Client Username на своем прокси сервере.

5. Выпущена версия 1.0

Internet Administrator Company ltd. © 2024 http://www.iadmin.ru, e-mail: sales@iadmin.ru, тел. +7 (495) 5147244

РАЗДЕЛ 2 – УСТАНОВКА И НАСТРОЙКА

Раздел 2.1. – Системные требования

Операционные системы:
- Linux (Ubuntu 22.04), возможно создание компиляций под другие линуксы.

Зависимости:
- Openssl (libssl)
- libidn
- libcurl

Оперативная память сервера: быстрый SSD для режима кеширования с диска (по умолчанию), либо свободные 13 Гб для режима полной загрузки базы в оперативную память для максимального быстродействия.

Жесткий диск: 20 Гб свободного места.

Другое: Наличие подключения к сети Интернет для обновления базы категорий напрямую или через прокси сервер.

Раздел 2.2. – Установка

1. Установка iAdmin URL SDK (Смотрите его отдельную документацию в части установки и настройки).

Распакуйте архив с iAdmin URL SDK, пути в архиве прописаны относительно корня файловой системы. Файлы будут расположены в каталоге /opt/iadmin.

Необходимо прописать путь к библиотеке в /opt/iadmin/lib в /etc/ld.so.conf, для этого выполните, например:

```
echo "/opt/iadmin/lib" > /etc/ld.so.conf.d/iadmin.conf
ldconfig
```

Пропишите полученный лицензионный ключ в /opt/iadmin/etc/key и попробуйте выполнить обновление базы категорий /opt/iadmin/bin/iadminupdate. Для периодического получения обновлений пропишите запуск этой утилиты в планировщик Cron, например раз в сутки. Для этой утилиты **нужны права на запись в /opt/iadmin**

Проведите тест SDK, запустив /opt/iadmin/bin/iadmintest. Это тестовая утилита, где можно ввести имя сайта и проверить его категорию.

2. Установка c-icap (https://c-icap.sourceforge.net/)

Установите c-icap и настройте его как сервис. Если установка доступна из репозитория вашего линукса, используйте ее.
Если нет, то используйте наш архив с файлами, распакуйте его относительно корня файловой системы. Затем зарегистрируйте c-icap в качестве сервиса, скопируйте файл из нашего архива с c-icap по его пути /lib/systemd/system/c-icap.service и выполните
systemctl daemon-reload
.

3. Установите iAdmin filter, распаковав файлы из его архива.

Файл /usr/local/share/c_icap/templates/iadminurl/EN/DENY должен попасть в путь установки Вашего c-icap. Смотрите в c-icap.conf параметр TemplateDir.
Зарегистрируйте наш сервис: файл /lib/systemd/system/iadmin-service.service
из архива должен располагаться по его пути, при необходимости добавьте туда пользователя и выполните

Internet Administrator Company ltd. © 2024 http://www.iadmin.ru, e-mail: sales@iadmin.ru,
тел. +7 (495) 5147244

systemctl daemon-reload
.
Пользователю, под которым будет стартовать iadmin-service (по умолчанию root), если меняли, нужны права на запись в /opt/iadmin.
Сервис ведет свой лог файл по пути /opt/iadmin/etc/iadmin-service.log, а также пишет в syslog базовоую информацию (стартанул, остановился, не смог создать свой лог).

4. Запустите наш сервис

systemctl start iadmin-service
и протестируйте его работу с помощью
/opt/iadmin/bin/iadmin-client
. Это консольная утилита, в которую можно вводить имена сайтов, и она будет подключаться к iadmin-service и возвращать категории.
Подключите iAdmin filter к c-icap: в конфиге c-icap (/usr/local/etc/c-icap.conf или /etc/c-icap.conf) пропишите

Include /opt/iadmin/etc/iadmin_filter.conf

5. Теперь можно запускать c-icap. Либо как сервис через systemctl, либо как обычный процесс. Для отладочного вывода используйте запуск с ключами:
./c-icap -N -D -d 1

Последняя цифра означает уровень вывода отладочной информации. Iadmin_filter выводит свои сообщения с уровнем 1 и записывает их в лог c-icap, например при запуске базы, или при неудачной загрузке правила. Для максимального вывода всего c-icap используйте 10.

Для остановки используйте Ctrl-C, если запустили процесс без параметров, его можно остановить выполнив echo -n "stop" > /var/run/c-icap/c-icap.ctl (**параметр -n обязателен**).

6. Проверка работы протокола c-icap.

Для проверки связи и работы правил используйте c-icap-client -s "iadmin_filter" -req "https://www.iadmin.ru/" с разным значением сайтов.

Раздел 2.3. – Настройка внешнего клиента c-icap

Для подключения внешних прокси серверов или устройств, поддерживающих ICAP, обратитесь к их документации. iAdmin URL filter работает только в режиме reqmod, то есть анализирует только исходящие HTTP запросы для фильтрации URL, фильтрацию для respmod настраивать не надо.
Обязательно настроить клиента, чтобы он передавал IP адреса, либо Имена пользователей. Это необходимо для механизма лицензирования, который контролирует общее число пользователей (по IP или UserName), а также не более 1000 запросов с одного хоста или имени пользователя в минуту.

Настройка клиента на примере Squid proxy:

В конфигурационном файле Squid (/etc/squid/squid.conf) прописать:

```
icap_enable        on
icap_service  iadmin_filter reqmod_precache 0 icap://localhost:1344/iadmin_filter
adaptation_access iadmin_filter allow all
adaptation_send_client_ip on
adaptation_send_username on
icap_client_username_header X-Client-Username
```


Internet Administrator Company ltd. © 2024 http://www.iadmin.ru, e-mail: sales@iadmin.ru, тел. +7 (495) 5147244

#Также поддерживается заголовок X-Authenticated-User

#Для правил с группами (создание и настройка групп осуществляется заранее)
mark transactions from users in the "G 1" group
adaptation_meta X-Authenticated-Groups "G 1" authed_as_G1
#Подробнее https://www.squid-cache.org/Doc/config/adaptation_meta/

В squid можно настроить получение категории запроса в добавляемом заголовке X-Iadmin-Cat. И анализе его уже непосредственно правилами squid. Для этого осуществляется следующая конфигурация:
В squid.conf
acl bad_cat req_header X-Iadmin-Cat ^(19|21|8)$ #По хедеру определяет категории. Последний параметр – любое регулярное выражение
adapted_http_access deny bad_cat #Правило работающее после ICAP, сюда миксуете acl с категориями и с юзерами\группами
request_header_access X-Iadmin-Cat deny all #Удаление нашего хедера, его нельзя отдавать во вне. Ya.ru с ним не работает например.
В iadmin_filter.conf
iadmin_filter.AddRule match #Добавляет заголовок во все запросы.
Параметрами можно задавать условия как для правил pass и block.

Примечание. Прокси-сервер может кешировать запросы к ICAP серверу и\или сайту. Если на сайт был осуществлен разрешенный доступ, то прокси некоторое время может пускать на такой сайт, даже если он был впоследствии заблокирован. В том числе, если сайту недавно была присвоена запретная категория через обновления базы iAdmin URL. То же самое может произойти, если был перезапущен c-icap сервис – прокси сервер не сразу осуществит попытку переконнекта к нему для определения запретных сайтов.

Раздел 2.4. – Настройка доступа

Для ограничения доступа используйте правила в конфиг файле /opt/iadmin/etc/iadmin_filter.conf, смотрите комментарий там в разделе правил, как они создаются.
Для релоада правил после изменения без рестарта c-icap выполните
echo -n "reconfigure" > /var/run/c-icap/c-icap.ctl (**параметр -n обязателен**)
Правила работаю как на файрволе, сверху вниз, если произошло совпадение, то выполняется действие pass или block.
Объекты правил задаются в кавычках. Разные объекты допускается смешивать в одном правиле через пробел.
Объекты для использования:
Category: Номер категории сайта, определенный iAdmin URL SDK по имени сайта и полному URL. Описание категорий смотрите в приложении А.
Site: задает точные имена сайтов, при этом **наличие www имеет значение**.
Domain: поиск по произвольной строке в имени сайта.
ClientIP: правило сработает только на указанных IP адресах.
UserName: правило сработает только на указанных именах пользователей.
UserGroup: правило сработает только для указанных групп пользователей.
Time: правило сработает только в указанное время (1 – понедельник), с – по в формате Ч:М:С.

Internet Administrator Company ltd. © 2024 http://www.iadmin.ru, e-mail: sales@iadmin.ru, тел. +7 (495) 5147244

В случае блокировки доступа по https клиент сообщит, что невозможно установить соединение, например ERR_TUNNEL_CONNECTION_FAILED. Для http запроса, или в случае вскрытия https трафика, будет выдана страница с сообщением Access Denied.

Internet Administrator Company ltd. © 2024 http://www.iadmin.ru, e-mail: sales@iadmin.ru,
тел. +7 (495) 5147244

ПРИЛОЖЕНИЕ А.

Список категорий и их идентификаторов. Описание категорий смотрите на сайте http://www.iadmin.ru/products/?pid=7

Categories	
cat_id	cat_name
1	Спорт
2	Авто \ Мото \ Транспорт
3	Игры
4	Развлечения \ Образ жизни
5	Работа \ Поиск работы
6	Путешествия \ Туризм
7	Товары \ Услуги
8	Музыка \ Видео \ Изображения \ Торренты
9	Армия \ Оружие
10	Экономика \ Финансы
11	Наука \ Образование
12	Медицина \ Здоровье
13	Новости \ СМИ
14	Производство \ Промышленность
15	Компьютеры \ Интернет
16	Веб-почта
17	Бесплатный хостинг
18	Поисковые машины
19	Порнография \ Для взрослых
20	Преступники \ Криминал
21	Анонимные прокси \ TOR \ VPN-прокси
22	Непознанное \ Религия
23	Социальные сети \ Онлайн общение
24	Государство \ Политика и право
25	Дети \ Семья \ Школа
26	Культура \ Искусство \ Классика
27	Баннеры \ Реклама
28	Алкоголь \ Табакокурение
29	С плохой репутацией \ Аморальные \ Мат
30	Азартные игры
31	Насилие \ Расизм \ Ненависть
32	Наркотики
33	Форумы \ Блоги \ Персональные сайты
34	Справочная информация
35	Сексуальное образование
36	Архивы программ

Internet Administrator Company ltd. © 2024 http://www.iadmin.ru, e-mail: sales@iadmin.ru, тел. +7 (495) 5147244

Categories	
cat_id	cat_name
37	Заработок в Интернет
38	Веб порталы
39	Запаркованные домены
40	Биткоин
41	Благотворительность
42	Доски объявлений
43	Мода и красота
44	Вредоносное ПО \ Вирусы
45	Фишинговые сайты
46	Шпионское ПО
47	Литература \ Тексты произведений
48	Хакеры \ Взлом сетей и программ
49	Онлайн платежи
50	Нелегальное ПО
51	Образовательные игры
52	Нудизм
53	Онлайн аукционы
54	Запрещенные сайты
55	Домашние животные
56	Секты
57	Динамический IP адрес
58	Юмор
59	Хобби
60	Онлайн покупки
61	Эротика \ Обнажение
62	Кулинария \ Еда \ Напитки
63	Дом \ Дача \ Ремонт
64	Дизайн \ Архитектура
65	Страхование
66	Селебрити \ Популярные люди
67	Некоммерческие организации
68	Недвижимость
69	Фотография
70	Удаленное управление
71	Трекеры \ Счетчики
72	Веб телефон
73	Веб телевидение
74	Веб радио
75	Анимация

Internet Administrator Company ltd. © 2024 http://www.iadmin.ru, e-mail: sales@iadmin.ru,
тел. +7 (495) 5147244

Categories	
cat_id	cat_name
76	Онлайн игры
77	Этнос \ Национальность
78	Сельское \ Лесное хозяйство

Internet Administrator Company ltd. © 2024 http://www.iadmin.ru, e-mail: sales@iadmin.ru,
тел. +7 (495) 5147244