Содержание

Общее описание 3
DPI для фильтрации по спискам PKH 4

Общее описание

Для выполнения требований Федеральных законов **139 и 114** оператору требуется осуществлять блокировку страниц интернет сайтов, содержащих противоправную информацию, по спискам, подготовленным **Роскомнадзором и Министерством Юстиции**.

Использование нашего решения позволит оператору сэкономить на разработке и поддержке собственного решения. Решение обладает рядом преимуществ по сравнению с использованием прокси и, заодно, оператор получает платформу, которая позволит ему экономить ресурсы и получать доход, предоставляя новые дополнительные услуги.

Требуемые компоненты:

1. Платформа глубокого анализа трафика (DPI)

Преимущества решения:
1) Удобство:

- применение правил находится в одном месте - на платформе DPI
- платформа сама загружает и применяет правила из списка

2) Производительность:

- размер списка составляет 4 млрд URL со сжатием в памяти до 10 раз (для сравнения в мире всего около 600 млн сайтов)
- обеспечивается фильтрация до 2 млн URL в секунду на 1 ядре процессора (для сравнения Google public DNS отрабатывает всего 800000 запросов в секунду)
- пропускная способность до 40 Гигабит в секунду на 1 CPU
- задержка в линии менее 30 микросекунд (сравните с proxy, и даже дорогими аппаратными вендорами)
- При построении схемы с ассиметричной маршрутизацией 1 процессора достаточно для фильтрации трафика всей России

3) Функциональность:

- из коробки поддерживается http и https, можно добавить другие протоколы,
- не зависит от номера порта (т.е. http://www.example.com и http://www.example.com:8080)
- не зависит от смены сайтом IP адреса
- вместо блокировки можно переадресовать абонента на заданную страничку

4) Надежность
Работает 24x7, поддерживается Bypass.
А как часто у вас падает squid или перестают отвечать сайты при повышении нагрузки ?
процесс закачки и применения списка автоматизирован, в отличие от решений "сделай сам" с непрогнозируемой надежностью

5) Дешевизна
По сравнению с современными платформами DPI (Procera/Allot стоят от $100 тыс) наше

решение значительно дешевле.
По сравнению со старыми (Cisco SCE) имеет больше возможностей и продолжает развиваться.
DPI работает на компьютере общего назначения, функциональность фильтрации предоставляется по минимальной цене (ENTRY лицензия), стоимость поддержки стремится к нулю, так как все автоматизировано:

- не нужно тратить время и деньги на разработку и поддержку собственного решения
- при соизмеримой производительности стоимость оборудования для прокси будет стоить во много раз дороже

(стоимость аппаратной платформы DPI получается менее 100 евро за Гигабит/с пропускной способности для платформы на 40G)

Кроме того DPI платформа имеет еще много других полезных применений в отличие от специализированного решения для фильтрации

DPI для фильтрации по спискам РКН

Доводим до Вашего сведения **информацию о смене IP адресов** ООО "ВАС Экспертс". Начиная с 2020 года IP адреса 5.200.43.10 и 5.101.74.130 станут недоступны.
Для корректного функционирования оборудования СКАТ после 31 декабря 2019 Вам следует настроить Ваши межсетевые экраны (МСЭ) / брандмауэры / firewall, отредактировать статические записи имен содержащихся в `/etc/hosts`, если используются, таким образом, чтобы обеспечить доступ к следующим доменным именам VAS Experts:

- vasexperts.ru
- data.vasexperts.ru
- data1.vasexperts.ru
- data2.vasexperts.ru
- cloud.vasexperts.ru
- catalog.vasexperts.ru
- ftp.vasexperts.ru

Сеть/IP адреса:

- 45.151.108.0/24
- 185.255.76.160

1. На 04.04.17 Роскомнадзор трактует нарушением наличие любого URL из списка прокуратуры в отчете, по остальным (негласно) накопление не более 1 процента за 5 дней, также обращаем внимание, как Роскомнадзор трактует аварию - отсутствие доступа абонентов в интернет для всех, включая ревизор (если случилась авария, то есть отсутствие доступа абонентов в сеть, то ревизор также не должен иметь доступа в сеть).
2. НЕ рекомендуется схема зеркало, так как в этой схеме при фильтрации идет борьба за скорость ответа абоненту, любые задержки на порту с зеркалом трафика, повторы,

потери и т.п. влияют на блокировку ресурса, и приводят к появлению в отчете не заблокированных ресурсов.

3. При покупке байпасс карты для обеспечения устойчивой работы сети в случае аварии оборудования и/или программного обеспечения DPI, необходимо понимать, что включение режима байпасс на карте приводит к отсутствию фильтрации, так как DPI исключается из схемы на уровне карты и это может привести к пропускам в ревизоре. При наличии такой карты (с байпасс), требуется в обязательном порядке наладить мониторинг, проверку состояния байпасс bpctl_util all get_bypass, проверять по alert логу событие включения в байпасс режим

```
grep bpm /var/log/dpi/fastdpi_alert.log
```

Когда включается байпасс - включение байпасс в процессе работы DPI (исключая действия администратора) это всегда аварийная ситуация, означает что WD (watchdog) карты не получил команду сброса от системы/процесса DPI и т.п., **основные причины**:

- забыли отключить диагностический режим (например трассировку пакетов trace_ip)
- неисправность оборудования
- блокировка процесса DPI в ОС, например, запуск ресурсоемкого стороннего процесса, синхронизация программного рейд после отказа
- значительное превышение параметров нагрузки DPI (например DDOS с превышением по сессиям в сек.)

Типовые случаи переключения в байпасс при действиях администратора, обращаем внимание, что в этом случае также происходит пропуск трафика без обработки:

- перезагрузка сервиса (при обновлениях, изменении холодных параметров конфигурации)
- останов сервиса
- отключение питания сервера
- перезагрузка ОС

В случае необходимости можно отключить режим байпасс на карте путем переключения карты в стандартный режим (соответственно режим байпасс включаться не будет)

```
bpctl_util all set_std_nic on
```

4. Рекомендуем при покупке DPI для фильтрации трафика в связи с возросшими требованиями Роскомнадзора обеспечивать резервирование за счет альтернативного канала с резервной системой фильтрации, без использования байпасс карт.
5. СКАТ осуществляет скачивание списков для автоматической блокировки из облака VAS Experts через управляющий интерфейс, через который осуществляется доступ по SSH. Для корректной работы необходимо обеспечить доступ с этого интерфейса к сайту vasexperts.ru и поддоменам.