Контроль над доступом в Интернет сотрудников предприятия

ООО «Солидекс»

Ровнов Павел

6 октября 2017 г.

Содержание

- **Какая постановка задачи?**
- **Поиск решения**
  - **Идентификаторы пользователей**
  - **Распознавание приложений**
  - **Противодействие методам уклонения**
- **Решение**

Общая постановка задачи

- **Доступ в Интернет**
- **Под вопросами:**
  - **Продуктивность**
    - **Кто и какие приложения запускается?**
  - **Безопасность**
    - **Не скачивается ли вредоносный контент?**
  - **Производительность**
    - **Интернет «тормозит»! Канал забит трафиком P2P?**
- **Ввести средства контроля:**
  - **Фильтрация**
  - **Отчёты**

Постановка задачи в деталях

Solidex

Я хочу увидеть **статистику** использования **приложений** для **пользователя** за месяц

500 событий, или 756 TCP-сессий и 35 МБ?

TCP/80, или HTTP, или Vkontakte, или Vkontakte_Video?

Что будет являться ID пользователя?

Задачка 1. «Медленный» Интернет

- **Пользователи сообщают, что все тормозит!**

- **Вопросы:**
  - **Кто больше всех использует Интернет?**
  - **Какой топ трафика?**
  - **Как повлиять на ситуацию?**

Задачка 2. Социальные сети (СС)

- **Доступ к СС запрещен для всех пользователей**
  - **В политике безопасности, но не в СЗИ**
- **Исключение в части доступа к СС для группы сотрудников**
  - **Поддержание в актуальном состоянии корпоративного аккаунта**
- **Предположительно:**
  - **В СС заходят все**
  - **В актуальном состоянии не только корпоративный аккаунт, но персональные страницы пользователей**

Опасные формулировки задач (1)

Я хочу знать топ-5 пользователей, которые «накачали» трафик через Torrent

- **В чем опасность?**
  - **Как воздействовать на ситуацию? Только административные меры**
  - **Анализ отчетов силами администратора?**
  - **Сбора данных вплоть до байтов -> увеличение объема логов**
- **Предлагаемый подход: блокировать сессии, которые принадлежат заведомо «вредным» приложениям**

Опасные формулировки задач (2)

Я хочу знать, кто написал комментарий X на публичном форуме Y! Я знаю, что это был наш сотрудник!

- **В чем опасность?**
  - **Требуется собирать и хранить все POST-запросы для всех сайтов, включая их содержимое -> увеличение объема хранилища**
  - **Как проанализировать большие объемы данных?**

- **Предлагаемые подходы:**
  - **Заранее блокировать все форумы;**
  - **Идентификация: сбор идентификаторов пользователей**

Содержание

- Какая постановка задачи?
- Поиск решения
  - Идентификаторы пользователей
  - Распознавание приложений
  - Противодействие методам уклонения
- Решение

Когда требуется ID пользователя?

- **Пользователи с различными полномочиями:**
  - **Группа 1: «Общий Интернет»,**
  - **Группа 2: «Интернет + Социальные сети»**

- **Анализ логов по доступу в Интернет:**
  - **По пользователю**
  - **По группе, в которую пользователь входит**

На какой ID пользователя сделать ставку?

- **IP @**
  - **Если динамический (DHCP)**
    - Какой пользователь скрывается за IP @ x.x.x.x?
    - Как посчитать трафик для пользователя за месяц, при условии что полмесяца у пользователя был IP @ X, полмесяца – IP @ Y?

не вариант

  - **Если статический (наши соболезнования :)**
    - Какой пользователь скрывается за IP @ x.x.x.x?
    - Какая группа пользователей «накачала» больше всех за месяц?

не вариант

На какой ID пользователя «сделать ставку»?

- **Имя АРМ**

  — Как управлять доступом в случае АРМ, за которым работают попеременно несколько пользователей?

  — Какая группа пользователей «накачала» больше всех за месяц?

не вариант

- **Локальные* учетные записи**

  — Требуется: Учетная запись запрашивается у пользователя

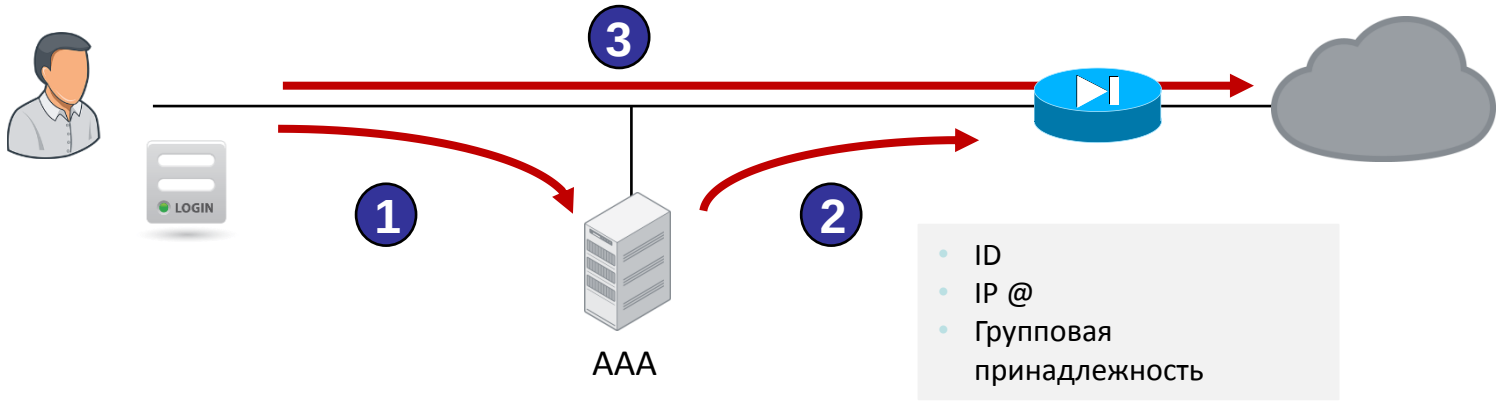
  — Минус: Изменение учетной записи (напр., смена пароля) требует подстройки СЗИ

как вариант

* Настроены на СЗИ

На какой ID пользователя «сделать ставку»?

- **Центральный каталог AAA (LDAP, Active Directory)**
  - **Плюсы:**
    - Один идентификатор: доступ в домен Windows, доступ в Интернет
    - Можно избежать повторного запроса учетной записи у пользователя (за счёт SSO)



Типы ID, не попавшие под рассмотрение

Solidex

- **Сетевые идентификаторы**
  - **MAC-адрес**
- **ID сторонних сервисов:**
  - **Google (OpenID)**
  - **Социальные сети**
  - **…**

Аномалии использования ID

- **1 пользователь, но 2 ID**
  - **Пример: «Обычный» пользователь + администратор**
  - **Интересный вопрос: Кто «скрывается» за сетевым ID?**
- **2 пользователя, но 1 ID**
  - **Пример: совместное использование одной учётной записи**
  - **Интересный вопрос: Какой сетевой ID?**

Какие требования серверу AAA?

Solidex

- **Должен быть :)**
  - **Настроены группы пользователей**
- **Протоколы доступа к AAA для получения информации об ID, принадлежности к группам:**
  - **LDAP**
  - **RADIUS**
- **В случае SSO:**
  - **На серверы AAA устанавливаются агенты**

Содержание

- Какая постановка задачи?
- Поиск решения
  - Идентификаторы пользователей
  - Распознавание приложений
  - Противодействие методам уклонения
- Решение

Как точно требуется контролировать?

Solidex

L3/L4c → L7/DPI → +SSL (TLS) инспекция

- Производительность

- Точность фильтрации
- Детальность отчётов
- Объем данных

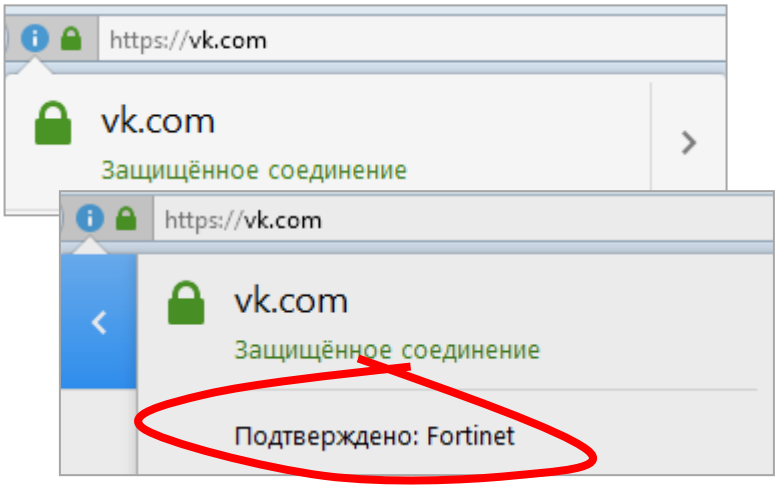
L3/L4	172.17.17.9	95.213.11.181 (vk.com)	HTTPS
L7/DPI	172.17.17.9	95.213.11.181	Vkontakte
SSL-i	172.17.17.9	95.213.11.150	Vkontakte_Login

SSL-, TLS-инспекция

Solidex

- **2 варианта**
  - **Расшифрование, просмотр контент (атака MiTM)**
    - **Назначение: AV, IPS проверки HTTPS, чтение содержимого HTTP для распознавания составные приложения сервисы как Google**
  - **Инспекция заголовков SSL-, TLS-пакета**
    - **Назначение: веб-фильтрация**

SSL-, TLS-инспекция (атака MiTM)

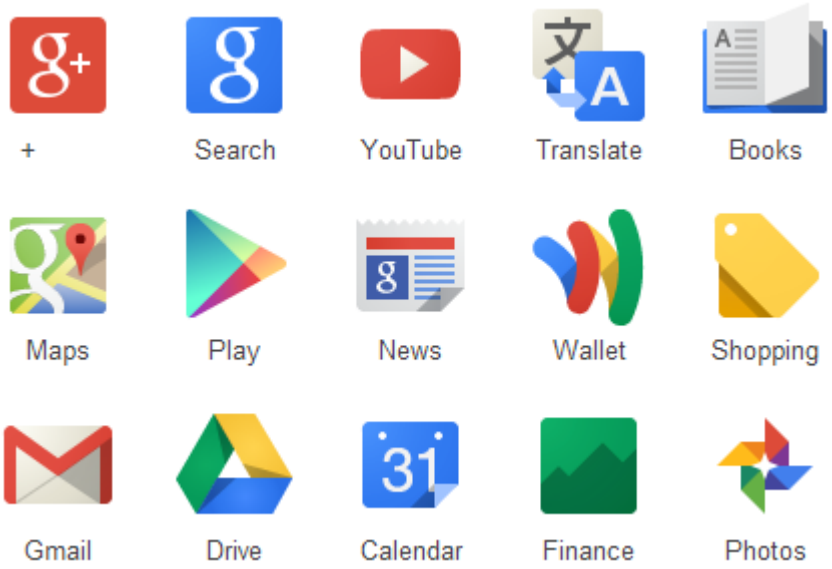


SSL-, TLS-инспекция. Ограничения

- **HPKP – HTTP Public Key Pinning**
  - **Ассоциация публичного ключа с конкретным сервером**
    - **Нацеленное противодействие SSL-, TLS-инспекции**
    - **Вариант обхода ограничения – исключение (для сайта инспекция не производится)**
- **HSTS – HTTP Strict Transport Security**
  - **Механизм для сайтов объявить о своей доступности только через SSL/TLS**
  - **Механизмы браузера отключают возможность перехода на сайт, если нет доверия цифровому сертификату**
- **Инфраструктурные**
  - **Нет возможности разместить на клиенте цифровой сертификат и СЗИ**

Распознавание веб-приложений

- **Единый протокол HTTP**
- **Разные приложения**
  - **По характеру трафика**
  - **Риски информационной безопасности**



- **Какие именно сервисы используются?**
- **Каким образом:**
  - **Кто? Какая учетная запись?**
  - **Какой контент?**

Демо!

- **Фильтрация идентификаторов социальных сетей**
- **Фильтрация сервисов социальных сетей**

Инструменты

- **Сигнатуры IPS/Application Control**
  - https://github.com/pavelrn/fortigate-custom-ips-sig.git

- **FortiGate FortiOS 5.4.5**
  - **IPS Engine 3.00311**

Какие функции применять?

Solidex

- **В зависимости:**
  - **От задачи**
  - **От того, как реализован сенсор**
    - **Как именно производитель назвал функции распознавания DPI**
- **Несколько идей:**
  - **App Control:**
    - **Всегда (если хотим знать, что пользователь делает)**
  - **Web Filter:**
    - **Когда требуется фильтрация веб-сайтов**
    - **(Супер)Детальная статистика по веб-приложениям**
  - **Content Filter (DLP):**
    - **Когда требуется фильтрация содержимого (напр. Можно ли скачивать *.exe)**

Содержание

- Какая постановка задачи?
- Поиск решения
  - Идентификаторы пользователей
  - Распознавание приложений
  - Противодействие методам уклонения
- Решение

Противодействие методам уклонения (1)

- **Метод «Карманный Интернет пользователя»**
  - **Пользователь: включает свой модем в сеть, «раздает» Интернет**
  - **Противодействие: мониторинг инфраструктуры, IPAM**

- **Протоколы, которые не возможно перлюстрировать**
  - **Пример: Google QUIC, передача фалов Skype**
  - **Противодействие: блокирование**

Противодействие методам уклонения (2)

Solidex

- **Метод «VPN, прокси-серверы, веб-прокси»**
  - **Противодействие:**
    - **Блокирование по протоколам (L7/DPI) – для VPN, прокси-серверов**
    - **Блокирование сайтов по категориям (веб-фильтрация) – для веб-прокси**

Содержание

- Какая постановка задачи?
- Поиск решения
  - Идентификаторы пользователей
  - Распознавание приложений
  - Противодействие методам уклонения
- Решение

Компоненты решения

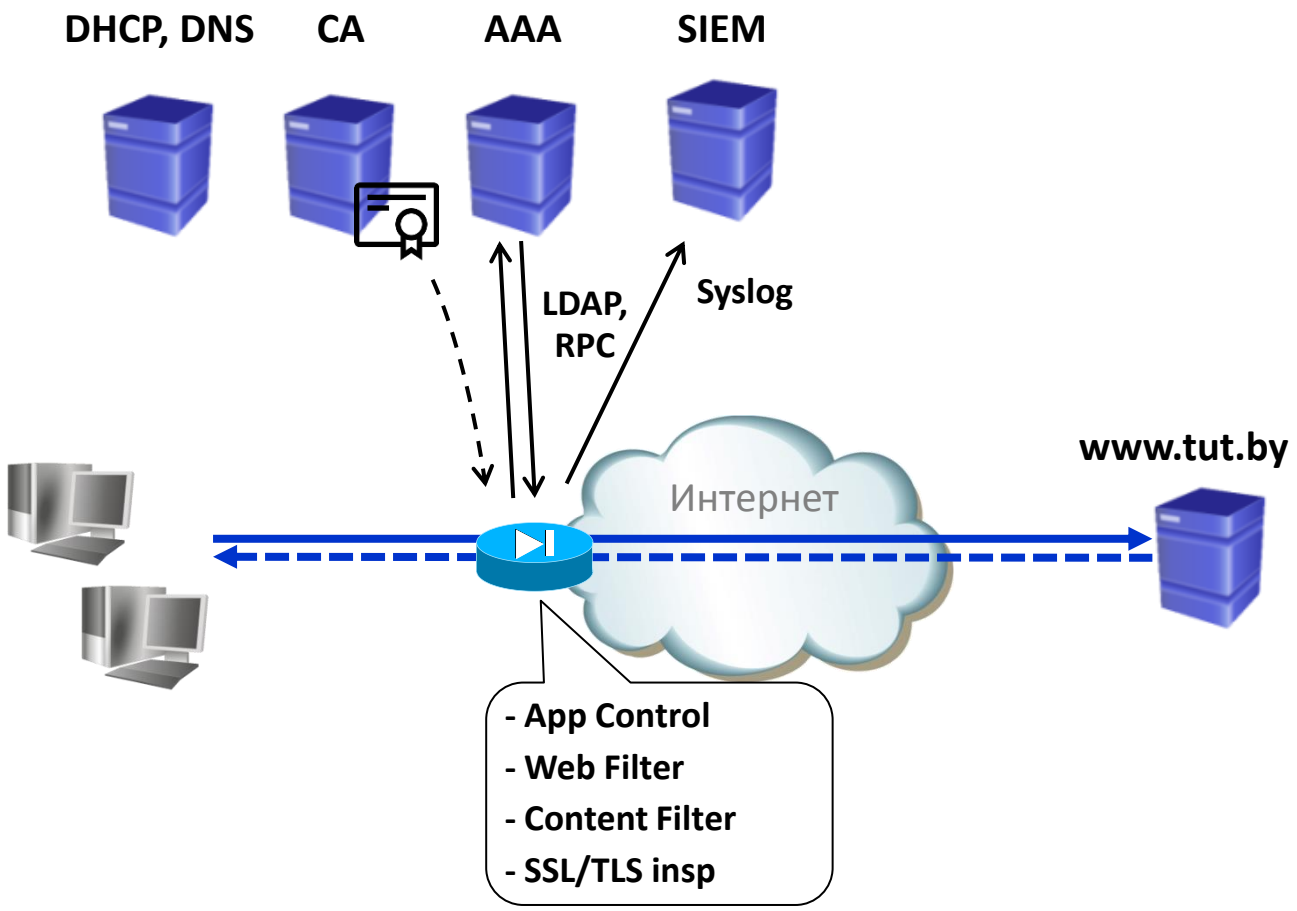
- **AAA, DHCP+DNS**
  - **Каталог пользователей и их полномочий**
  - **Сервис IP-2-ID**
- **Удостоверяющий центр**
  - **При условии SSL/TLS инспекции (MiTM)**

Компоненты решения

- **Сенсор**
  - **Распознавание информационных потоков**
    - **L7/DPI**
    - **SSL/TLS-инспекция**
  - **Фильтрация**
  - **Лог сообщения**

- **Система анализа сообщений**
  - **Формирование отчетов**

Функциональная схема решения



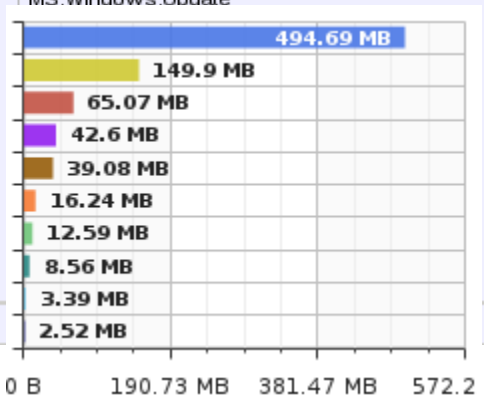
Что в результате?

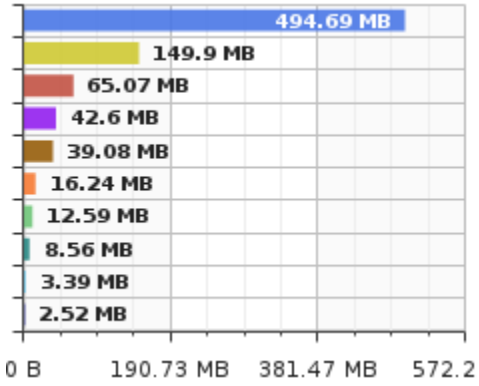
Solidex

- **Топ приложений по объему данных**

Июль

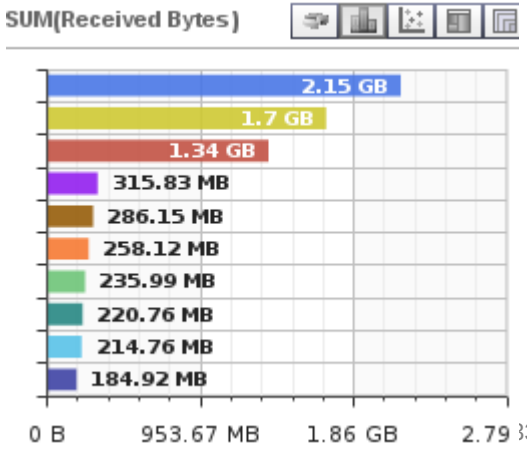
Chart	Application Group Name	Application Name
	Update	MS.Windows.Update
	Video/Audio	
	Video/Audio	
	Web.Others	
	General.Interest	
	Collaboration	
	Network.Service	
	Web.Others	





Октябрь

Chart	Application Group Name	Application Name
	General.Interest	Google.Services
	Email	POP3S
	Web.Others	HTTPS.BROWSER
	Collaboration	Microsoft.Portal
	Web.Others	HTTP.BROWSER
	General.Interest	Yandex
	Web.Others	HTTP.BROWSER_Chrome
	Email	IMAPS



Что в результате?

Solidex

- **Топ пользователей по объему данных**

Chart	Source IP	Source Host Name	SUM(Received Bytes)
	172.28.11.88	lsov-nout2	38.33 MB
	172.28.13.45	Upr-k24-3	18.75 MB
	172.28.11.42	lsov-k2-3	17.20 MB
	172.28.5.41	ilen-zav	15.65 MB
	172.28.17.53	iokt-k1085-N	11.17 MB
	172.28.9.48	iperv-k5-21	10.75 MB

Что в результате?

Solidex

- **Топ пользователей по объему данных, приложениям**

Chart	Source IP	Source Host Name	Application Name	SUM(Received Bytes)
	172.24.1.147		POP3S	1.70 GB
	172.24.47.35	Cherven-Nach	Google.Services	335.07 MB
	172.24.25.35	DESKTOP-EQB55LQ	Google.Services	294.99 MB
	172.24.37.42	DESKTOP-VNGEAJK	Google.Services	280.45 MB
	172.24.25.32	DESKTOP-EN4ITRE	Google.Services	280.42 MB
	172.24.33.35	DESKTOP-AB6UEES	Google.Services	267.03 MB

ID пользователя

Solidex

Ваши вопросы?