Компания Treatface

Передовые инфокоммуникационные решения

Современные технические средства защиты от инсайдеров российской разработки

treatface

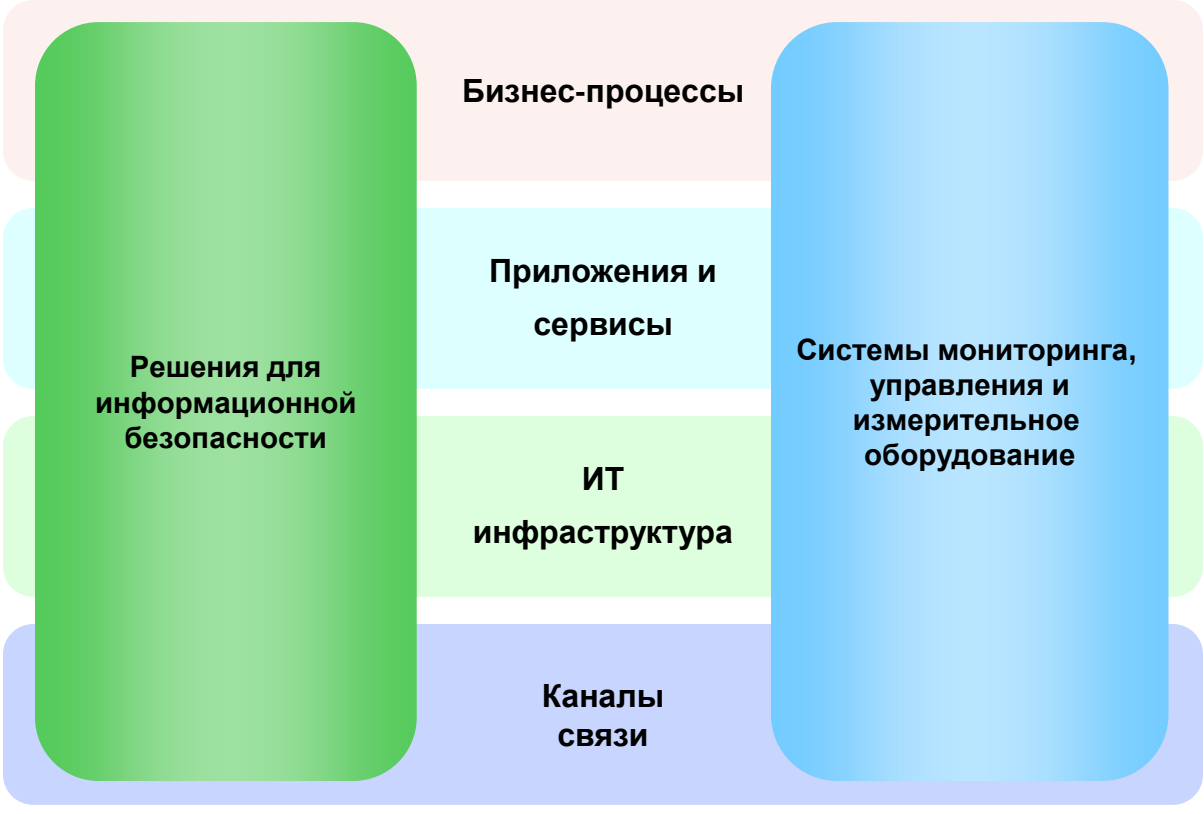
treatface

о компании

Основные факты

- Компания “Тритфейс” создана в 2010 году при поддержке крупных государственных заказчиков для разработки инфокоммуникационных решений с возможностью глубокого анализа пакетов (DPI) для закрытых государственных организаций.
- В 2011 году выпущена первая версия платформы DPI и внедрена на сети ОАО «ВымпелКом».
- В 2013 году разработана вторая версия платформы DPI, которая является одним из лучших решений на рынке средств глубокого анализа и обработки трафика.
- В начале 2014 года в деятельности компании “Тритфейс” появились новые направления, благодаря приходу в нее команд высококвалифицированных специалистов по мониторингу и тестированию сетей и приложений.
- В 2014 году внедрено решение для контроля трафика на базе платформы DPI в ОАО «Ростелеком»

Направления работы



Решения для защиты от инсайдеров

Системы съема копии трафика

IXIA Netoptics

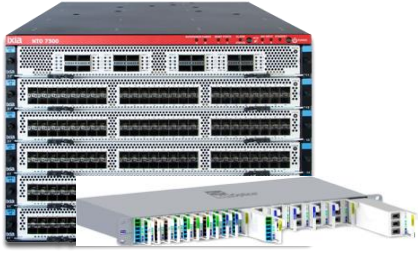
Системы интеллектуальной обработки трафика

ПАК «СОФИТ»

Инфраструктура тонкого клиента

ПАК «Стрелка»
ПАК «Стрелка-С»

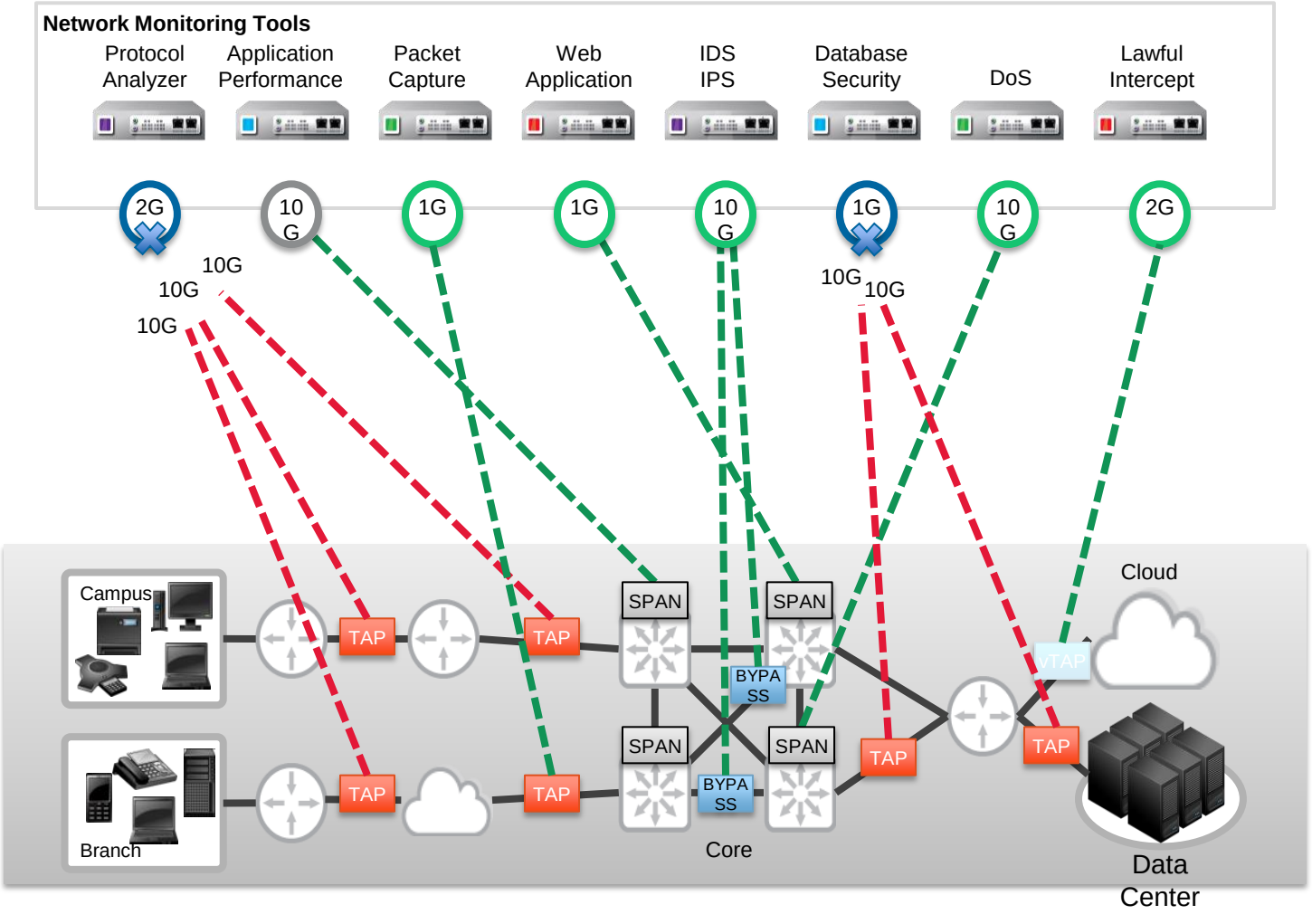
Treatface - дистрибьютор Ixia



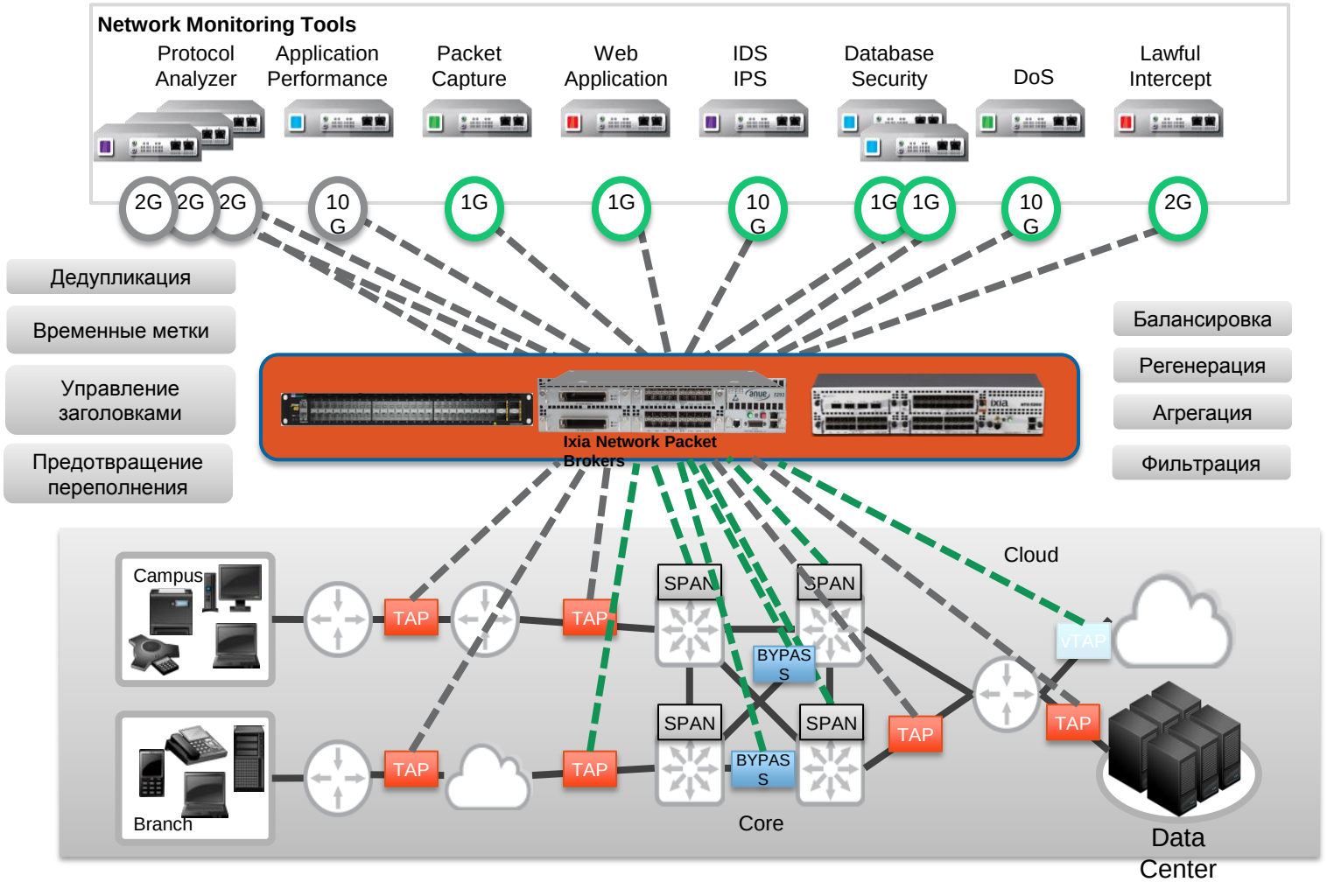
ixia
Deliver On

Управление трафиком	Тестирование L2-L7	Тестирование безопасности
•Ответвители •Байпас устройства •Спан-коммутаторы и балансировщики	•Коммутация и маршрутизация •MPLS •BGP •Данные, видео, голос •СХД •Устройства stateful обработки •Оценка QoE •Работа сервисов под нагрузкой •Емкость каналов связи на L4-7	•80 – 960 Гбит/с •NG firewall •WAF •IDS/IPS •Защита от DDoS •Родительский контроль •Антивирусы •СОРМ •Гос. реестр запрещенных ресурсов

С использованием устройств уровня доступа



Архитектура системы захвата траффика



Интеллектуальная обработка трафика (DPI)
ПАК «СОФИТ»

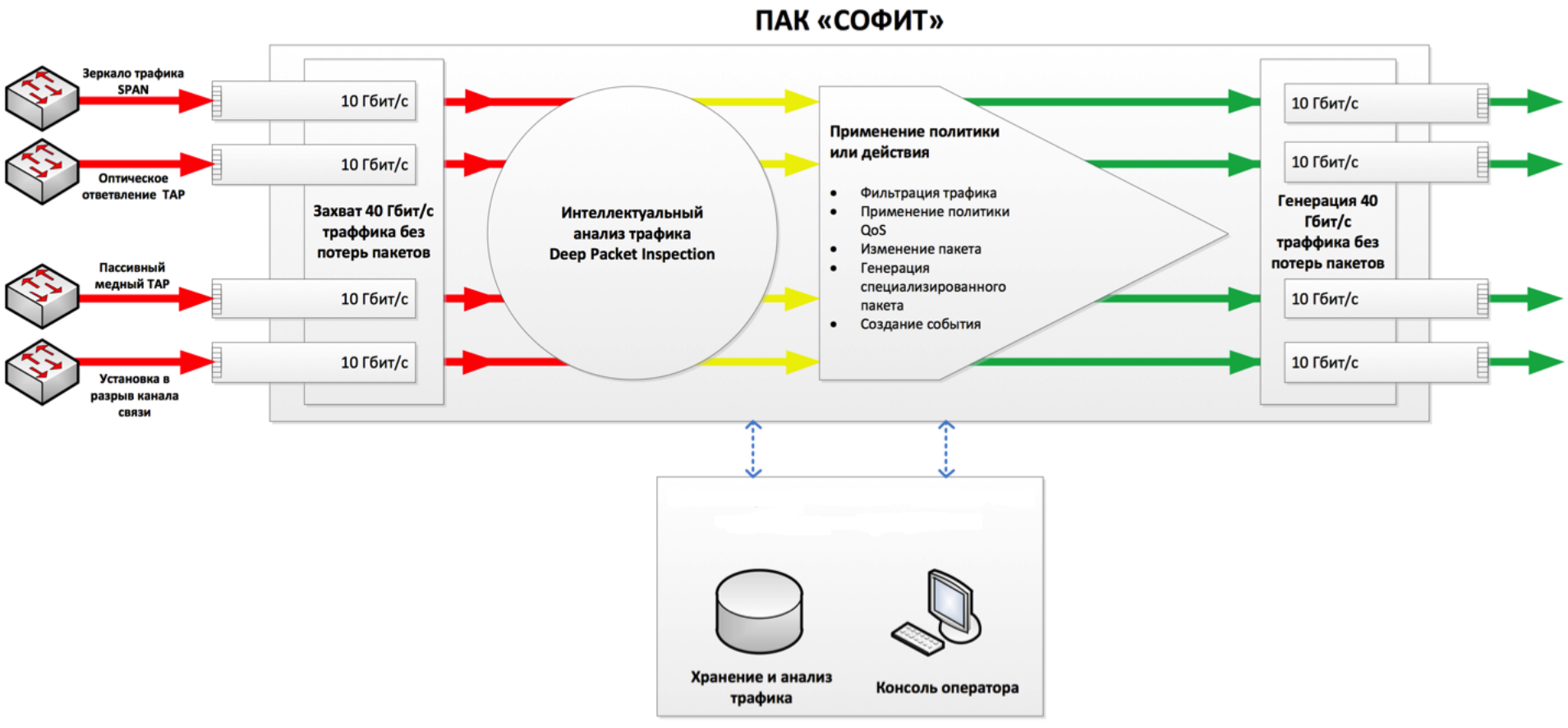
ПАК «СОФИТ»

ПАК «Софит» обрабатывает сетевой трафик на скоростях до **40 гигабит/секунду** «wirespeed» в реальном времени в форм-факторе 1U и позволяет решать следующие практические задачи:

- перехват, анализ, хранение и ретрансляция магистрального сетевого трафика;
- фильтрация интернета и сайтов;
- контроль трафика файлово-обменных сетей;
- поиск аномалий в прохождении трафика и/и его классификация для обеспечения разного уровня SLA и биллинга;
- противодействие сетевым атакам, в том числе DDoS атакам;
- префильтрация трафика.

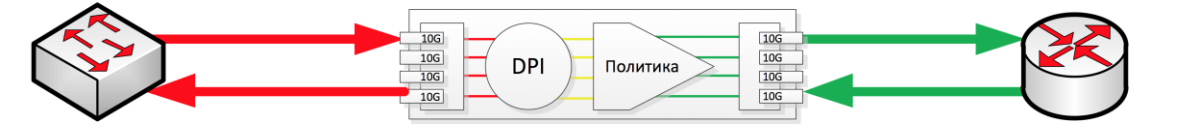
При разработке платформы не использовались редкие комплектующие, все используемые компоненты общедоступны.

ПАК «СОФИТ»


ПАК «СОФИТ»
Зеркало трафика SPAN
Оптическое ответвление TAP
Пассивный медный TAP
Установка в разрыв канала связи
10 Гбит/с
10 Гбит/с
10 Гбит/с
10 Гбит/с
Захват 40 Гбит/с траффика без потерь пакетов
Интеллектуальный анализ трафика Deep Packet Inspection
Применение политики или действия
Фильтрация трафика
Применение политики QoS
Изменение пакета
Генерация специализированного пакета
Создание события
10 Гбит/с
10 Гбит/с
Генерация 40 Гбит/с траффика без потерь пакетов
10 Гбит/с
10 Гбит/с
Хранение и анализ трафика
Консоль оператора

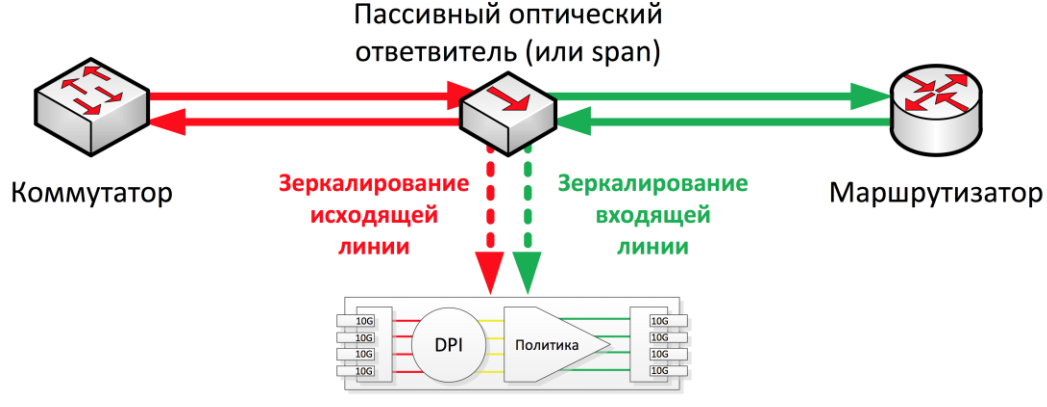
Схемы установки ПАК «СОФИТ»

Установка ПАК «Софит» в разрыв канала связи для защиты



Коммутатор Маршрутизатор

Установка ПАК «Софит» на копию сетевого трафика для анализа



Коммутатор Маршрутизатор

ПАК «СОФИТ» #1 СОРМ

Инсталляция ПАК «Софит» в крупнейшем федеральном операторе связи:

— оптимизация работы комплексов СОРМ;
— фильтрация трафика по L3 заголовкам, по имени пользователя, почтовому адресу, номеру ICQ;
— фильтрация трафика файлово-обменных сетей и видео-контента;
— прозрачная работа для сетевого оборудования и комплексов СОРМ (~DLP);
— ~250 инсталляций.

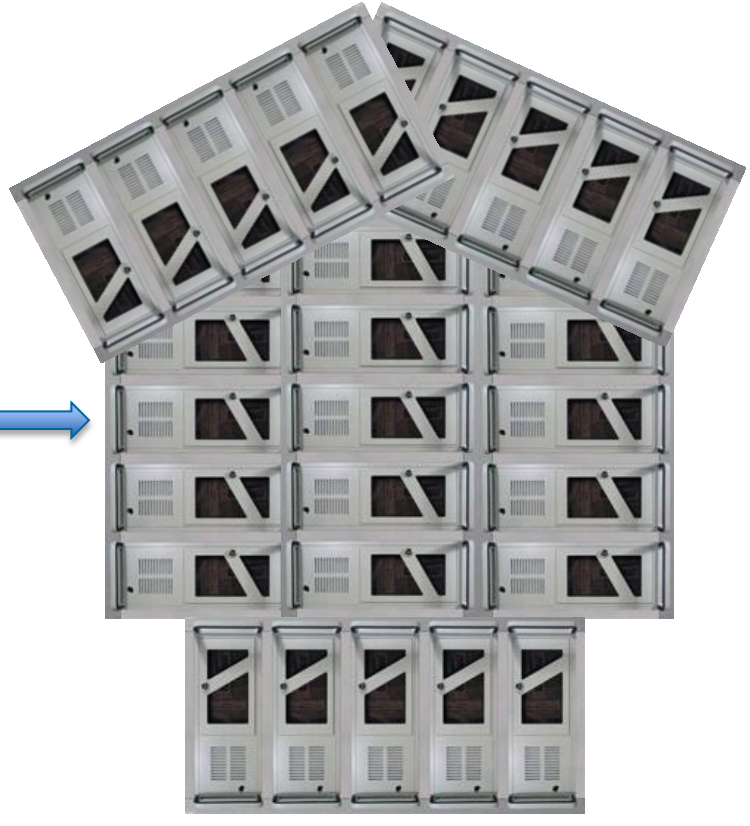
ПАК «СОФИТ» #1 СОРМ

200 Мбит/с

ПАК «СОФИТ» #1 СОРМ

ПАК «СОФИТ» #1 СОРМ

20 Гбит/с



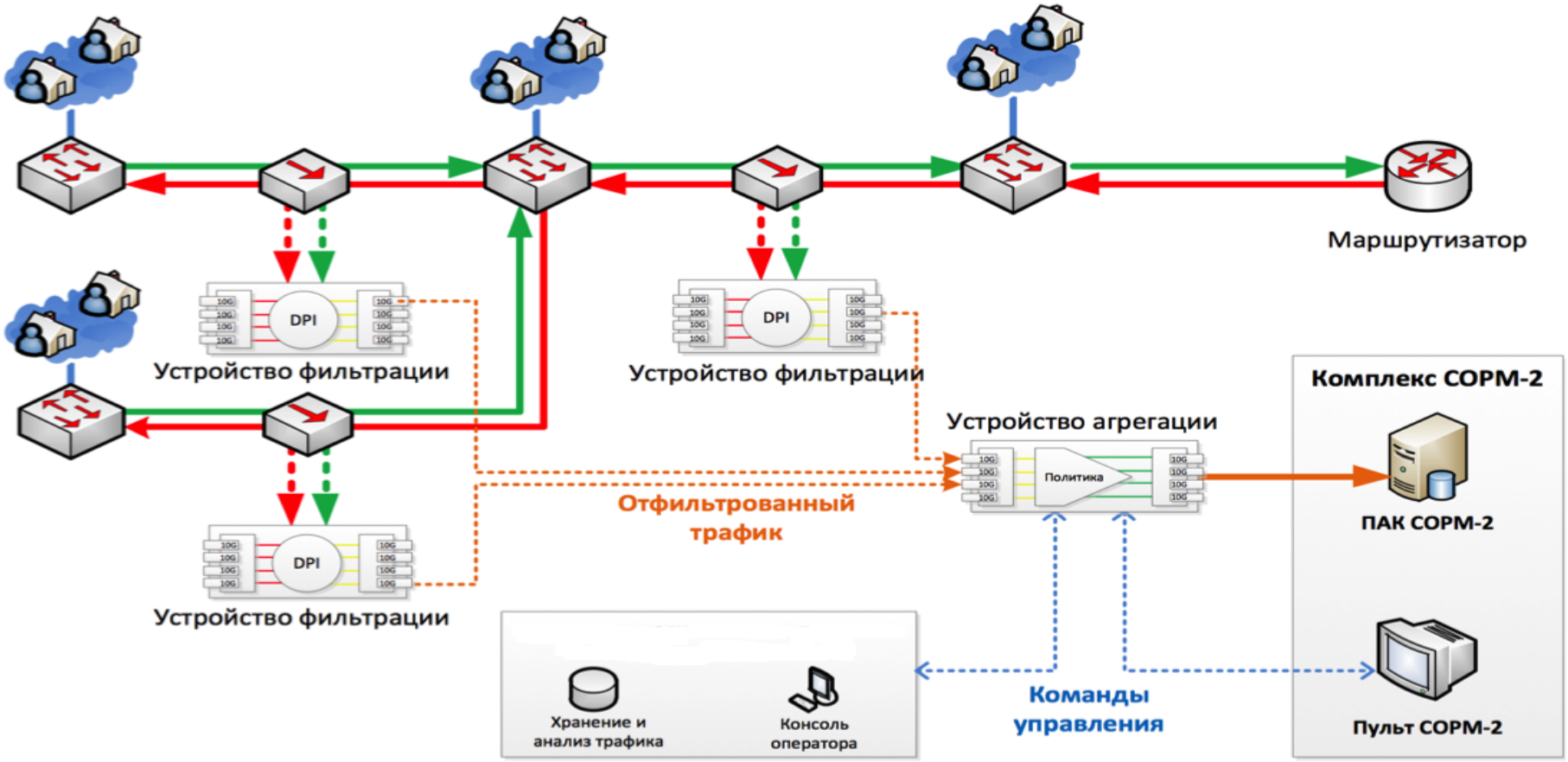
ПАК «СОФИТ» #1 СОРМ

20

200 Мбит/с

ПАК «СОФИТ» #1 СОРМ

Решение для масштабирования комплексов СОРМ-2 на базе ПАК «Софит»



ПАК «СОФИТ» #2 URL фильтрация

Инсталляция ПАК «Софит» в крупнейшем федеральном операторе связи:

— выполнение закона о «черных списках»;
— фильтрация по URL;
— фильтрация без необходимости внесения изменений в архитектуру сети;
— используется для фильтрации Москвы и некоторых регионов;
— 50 кратная экономия стоимости внедрения DPI, по сравнению с зарубежными решениями.

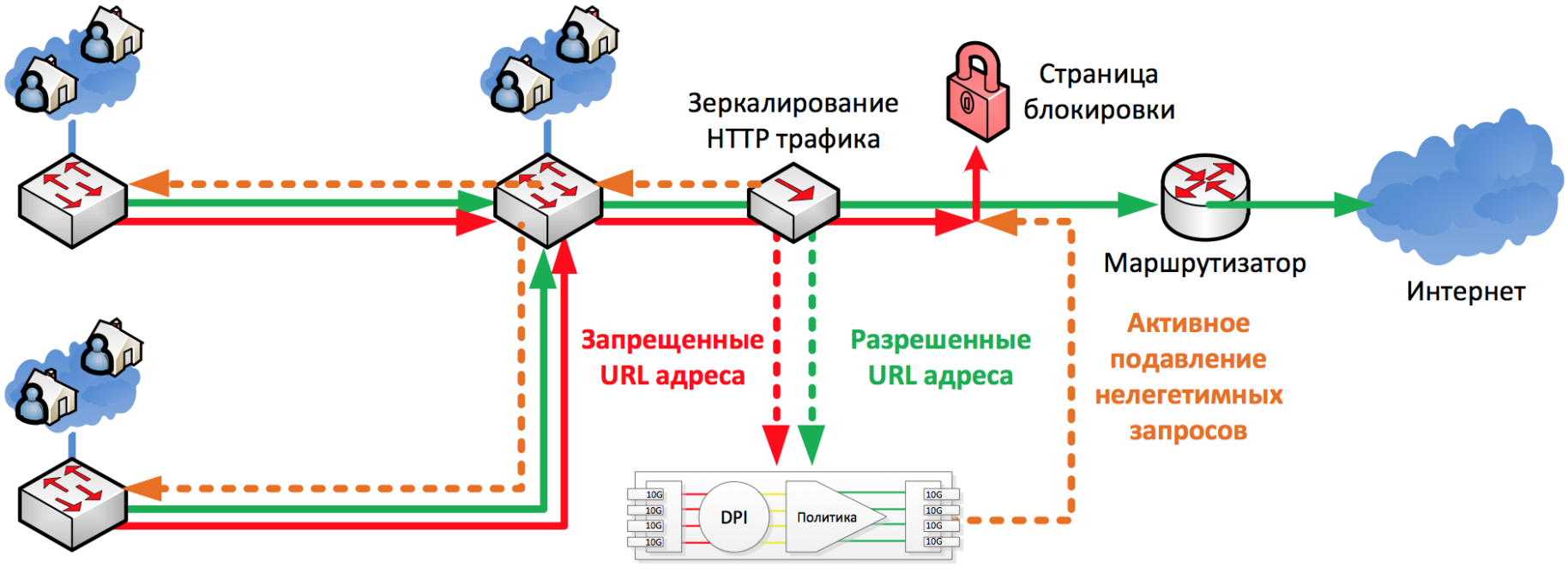
ВЕДОМОСТИ
THE WALL STREET JOURNAL | FINANCIAL TIMES

Практически у всех остальных операторов — кроме «Ростелекома» — уже стоят системы, позволяющие блокировать сайты по URL. С помощью DPI осуществляет фильтрацию «Вымпелком» и МТС, рассказывают их представители. Установку систем DPI на сетях фиксированного широкополосного доступа масштабов федерального игрока операторы «большой тройки», да и Роскомнадзор, оценивали в $40-50 млн.

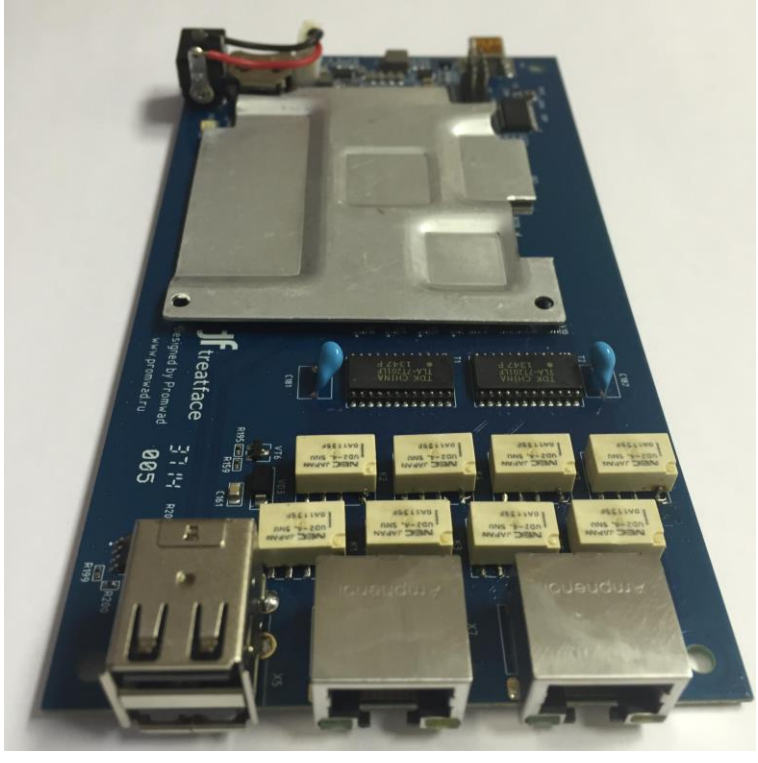
«Ростелекому» установка его решения обойдется гораздо дешевле. На разработку решения для фильтрации компания объявляла тендер, победительницей стала Inline Telecom Solutions. В конкурсной документации указана стоимость проекта — 36,9 млн руб., или чуть более $1 млн.

ПАК «СОФИТ» #2 URL фильтрация

Фильтрация интернета и поддержка единого реестра доменов и сайтов с запрещенной к распространению информацией



Перспективный автоматизированный шейпер «TOFSLAN» на базе ПАК «СОФИТ»

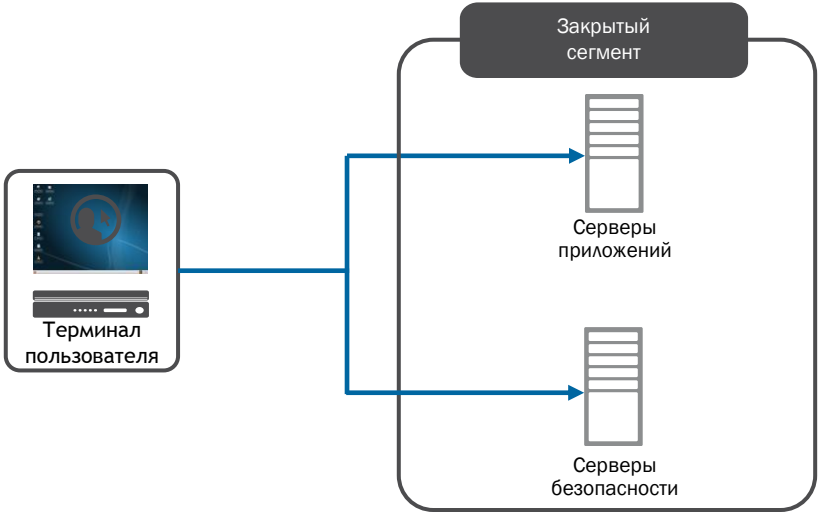


Отличительными особенностями TOFSLAN являются:

- Наличие встроенных датчиков для контроля климатических условий и физического воздействия.
- Возможность автономной работы за от встроенного аккумулятора.
- Поддержка стандартов RFC2544, RFC5357 (TWAMP), Y.1731 и IEEE 802.1ag для тестирования и мониторинга каналов связи.
- Мониторинг маршрутной информации для быстрого обнаружения проблем с маршрутизацией.
- Возможность управления полосой пропускания пользователей и приложений.
- Мониторинг состояния беспроводной среды.
- **Поддержка Netflow, DPI, записи трафика, bypass и т.п.**

Защищенный тонкий клиент ПАК «Стрелка»

Архитектура ПАК «Стрелка»



ПАК «Стрелка» состоит из нескольких компонентов:

- терминалы пользователей;
- сервер приложений;
- сервер безопасности.

Терминалы пользователей -- бюджетные бездисковые устройства, функционирующие под управлением доверенной операционной системы.

Сервер приложений обеспечивает публикацию, запуск и контроль пользовательских приложений (VDI).

Сервер безопасности предназначен для аутентификации и авторизации пользователей и компонентов системы, журналирования событий безопасности, а также для хранения пользовательских данных и профилей.

Гипервизоры (VDI)

Microsoft
vmware
CITRIX

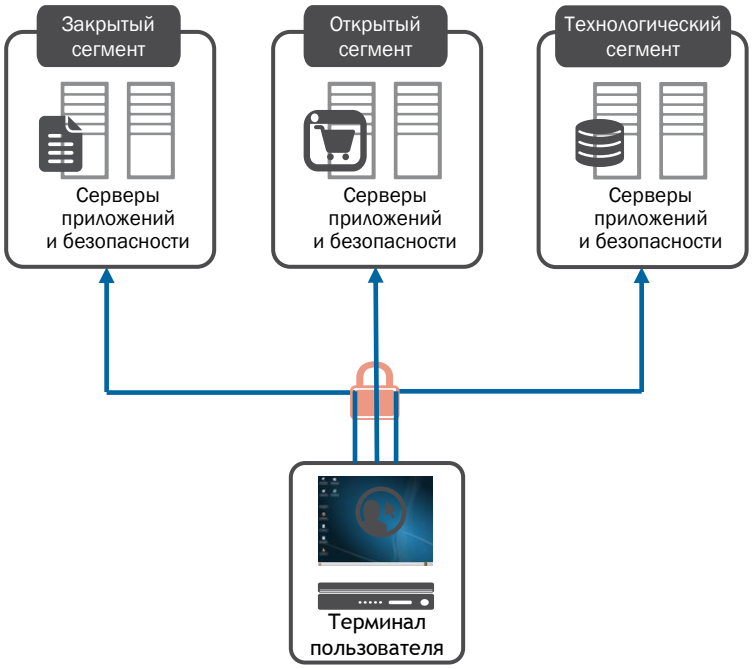
Приложения

1С SAP ORACLE

Периферийные устройства

- Матричные LTP-принтеры
- Смарт-карты
- Электронный ключ «таблетка»
- USB-токены
- POS-терминалы
- И другие COM- и USB-устройства

Возможности ПАК «Стрелка»

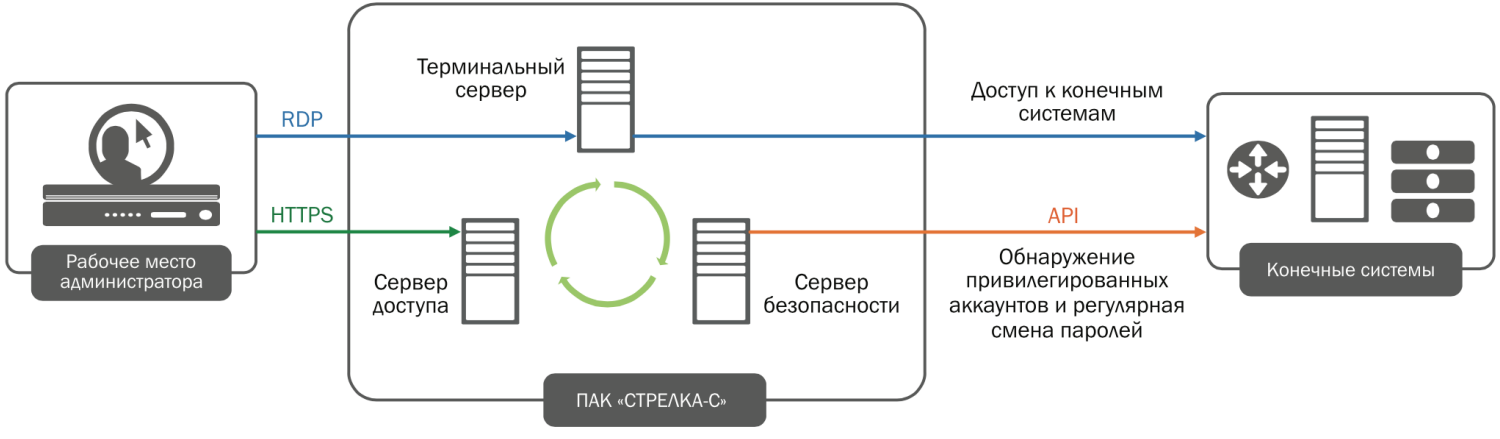


- Контроль политик безопасности путем централизованного исполнения ОС, прикладного ПО и контроля доступа пользователей;
- Защита от утечки или потери данных посредством централизованного хранения информации и использования бездисковых рабочих станций;
- Поддержка одновременной работы в нескольких контурах безопасности (защищенный, публичный и т.д.) с одной рабочей станции (изоляция, свой набор приложений);
- Простое переключение между контурами безопасности;
- Поддержка различных периферийных устройств;
- Снижение затрат на модернизацию и приобретение рабочих станций.

Перспективный ПАК «Стрелка-С»

ПАК «Стрелка-С» является специализированной версией **ПАК «Стрелка»** и представляет собой комплексное решение для контроля привилегированных учетных записей.

- Автоматический поиск привилегированных учетных записей в ИТ-инфраструктуре компании, обеспечение периодической процедуры смены паролей.
- Усиленная аутентификация привилегированных пользователей (поддерживается двухфакторная аутентификация, аутентификация по ключам eToken или одноразовым паролям).
- Высокий уровень контроля администраторов и упрощение расследование инцидентов за счет видеозаписи всех сессий работы привилегированных пользователей.
- Обеспечение оперативного реагирования на инциденты ИБ за счет интеграции с системами класса SIEM.




Спасибо!
treatface
115054, Москва, Б. Строченовский пер., 22/25, стр. 1, офис 503
Тел.: +7 (499) 403-14-09, факс: +7 (499) 346-84-70
info@treatface.ru · www.treatface.ru