invGUARD

Система защиты от сетевых атак

ИНОВЕНТИКА
ТЕХНОЛОДЖЕС

СОДЕРЖАНИЕ

Что такое invGUARD? 2
Функциональность 2
Архитектура системы 3
Технологии 3
Производительность 3
invGUARD AS – Анализатор 4
invGUARD AS – блокировка атак на маршрутизаторах 5
Инструмент для принятия решений 6
Безопасность 7
Спецификация invGUARD AS (на устройство) 8
invGUARD CS – Очиститель 8
invGUARD CS – подавление атак 9
Спецификация invGUARD CS (на устройство) 9
Преимущества invGUARD 10
Применение invGUARD 11
Техническая спецификация 15
Отчёты 18
Программный интерфейс invGUARD API 19
invGUARD + inoSphere 19
Интеграция invGUARD с внешними системами мониторинга по протоколу SNMP 19
invGUARD Cloud Signaling 20
Дорожная карта invGUARD 21
Техническая поддержка и сопровождение 21
Внедрение 21

invGUARD

Система защиты от сетевых атак

ЧТО ТАКОЕ invGUARD?

invGUARD производит мониторинг потока сетевого трафика в реальном времени для задач детектирования DDoS-атак и подавления атак для уменьшения вредоносного воздействия на сеть, центры обработки данных, клиентов или услуги.

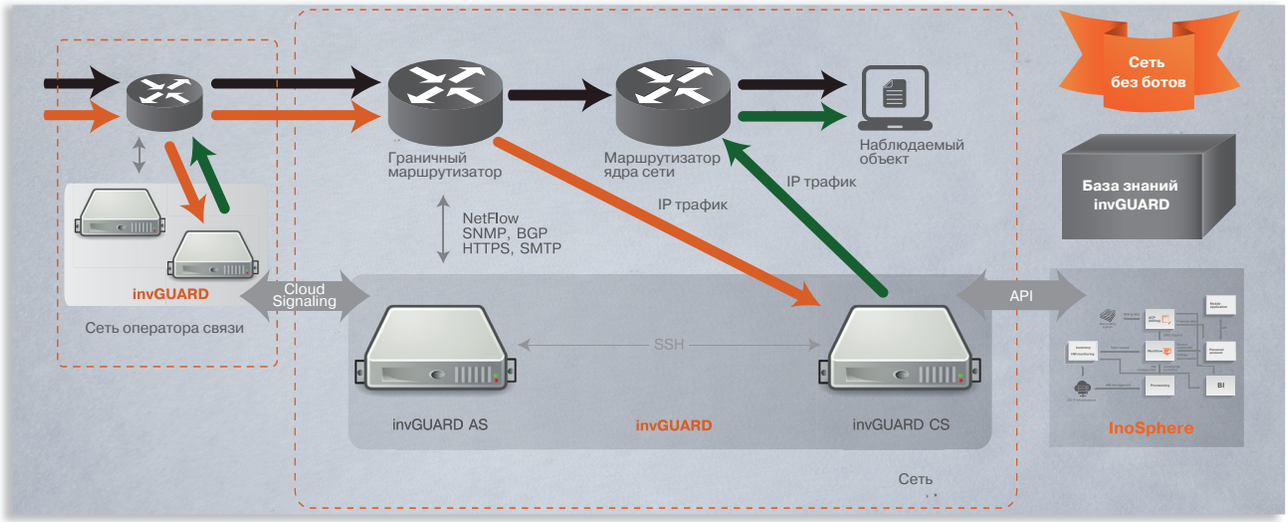
invGUARD предоставляет:

- Анализ трафика до 5 Тбит/с в сети из десятков и сотен маршрутизаторов
- Детектирование и подавление сетевых атак в реальном времени
- Высокоскоростную очистку и фильтрацию трафика до 200 Гбит/с
- Контроль качества потоков трафика к ресурсам, клиентам и провайдерам
- Возможность оказания услуг защиты от сетевых атак для заказчиков
- Низкую стоимость владения

ФУНКЦИОНАЛЬНОСТЬ

- Собирает и агрегирует NetFlow и SNMP данные, обновления BGP
- Предоставляет отчеты по различным срезам стека протоколов TCP/IP и маршрутной BGP информации
- Детектирует аномальную активность объектов и воздействия, не имеющих четко выраженных сигнатур
- Детектирует DDoS-атаки – ICMP flood, TCP SYN flood, TCP Connection flood, UDP flood и более 100 других типов атак
- Формирует более чем 250 различных отчетов
- Подавляет атаки с помощью BGP анонсов: Blackhole и FlowSpec
- Производит очистку трафика от сетевых червей, зомби, бот-сетей и других типов вредоносных воздействий
- Применяет различные контрмеры для фильтрации трафика для предотвращения вредоносных воздействий: TCP-аутентификация, количество запросов и соединений, объемы передаваемых данных и др.
- Интегрируется в системы мониторинга с помощью протокола SNMP
- Поддерживает маршрутизаторы различных производителей: Juniper, Cisco, Huawei, HPE, H3C, Extreme и других
- Многоязычный интерфейс

АРХИТЕКТУРА СИСТЕМЫ



ТЕХНОЛОГИИ

- Анализ потоков трафика: NetFlow v5, v9 и IPFIX, NetStream v5 и v9, sFlow
- Опрос маршрутизаторов: SNMP v2c и v3
- Таблица маршрутизации и управление маршрутизацией: BGP v4
- Операционная система: Linux (Red Hat, CentOS или подобная)
- Поддерживается архитектура x86
- Поддержка виртуальных машин KVM для системы invGUARD AS
- Система управления базами данных MySQL Database
- Сервер веб-публикаций Apache
- Высокоскоростная очистка трафика обеспечивается специальными или intel DPDK-совместимыми сетевыми платами

ПРОИЗВОДИТЕЛЬНОСТЬ

- Анализ трафика до 5 Тбит/с для защиты от кибератак
- 100+ маршрутизаторов в одном интерфейсе
- 20000+ наблюдаемых объектов
- Поддержка гетерогенной инфраструктуры: Juniper, HPE, H3C, Cisco, Huawei, Alcatel, Exterme и других
- 250+ различных отчетов по трафику и объектам
- 100+ типов детектируемых кибератак
- 10000+ детектируемых событий в день
- 80- часов на развертывание системы

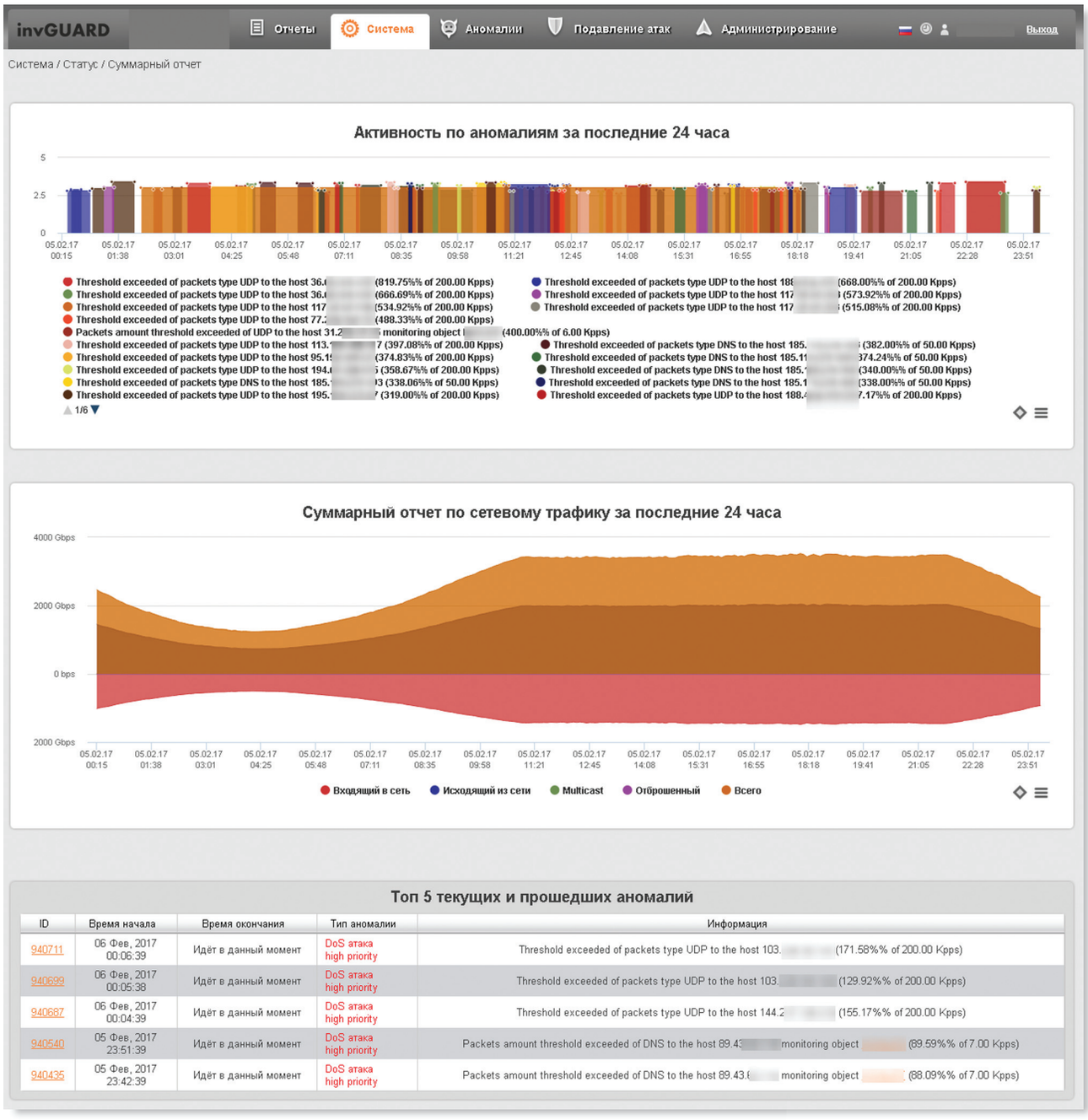
invGUARD

Система защиты от сетевых атак

invGUARD AS – АНАЛИЗАТОР

invGUARD AS – основной компонент системы invGUARD:

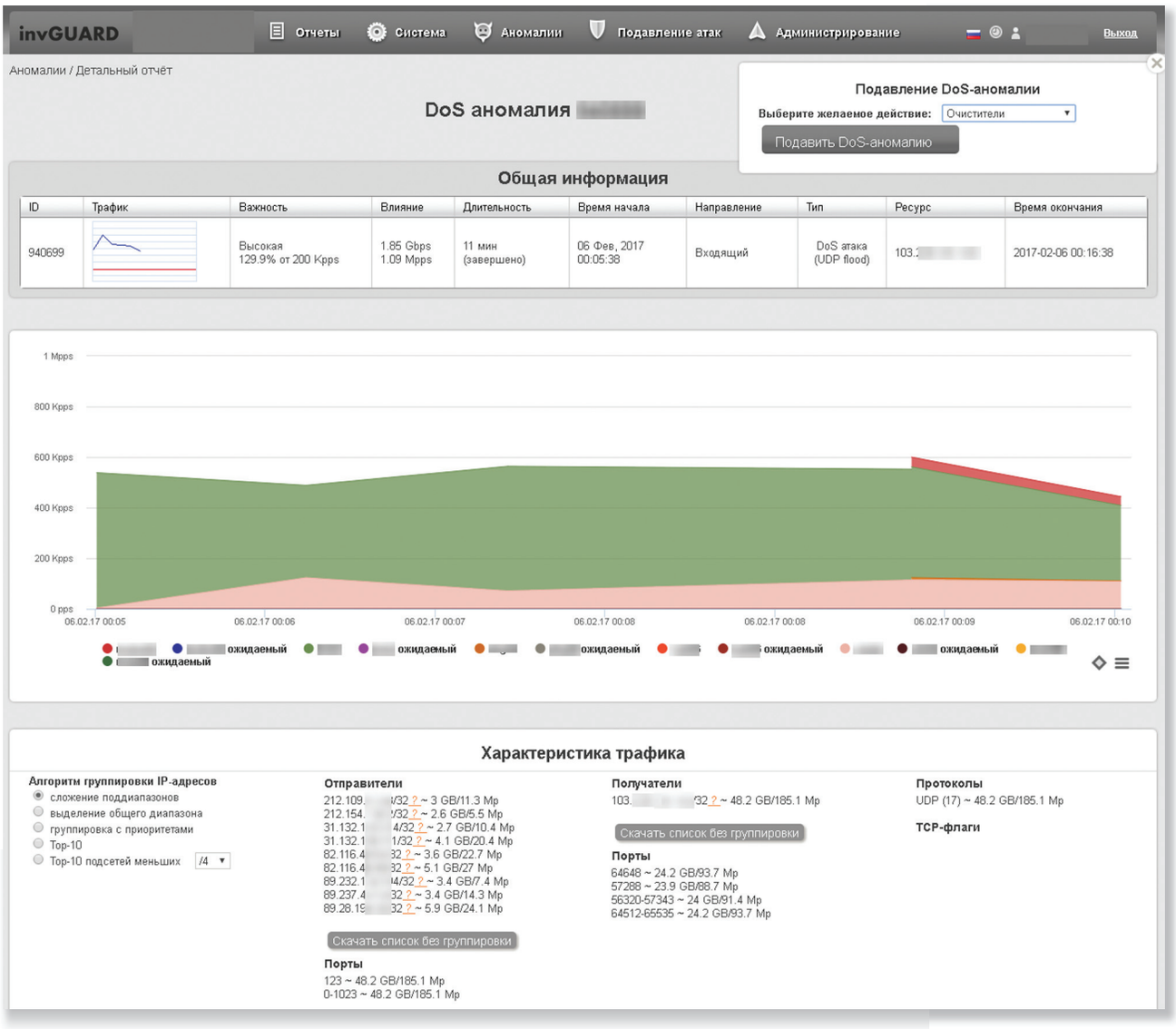
- Собирает, агрегирует, анализирует и сохраняет данные о сетевом трафике с маршрутизаторов по протоколам NetFlow, SNMP и BGP;
- Детектирует аномалии в сетевом трафике, DDoS-атаки и другие типы сетевых атак;
- Формирует детальные отчеты по сетевому трафику.



Суммарный отчет по системе

invGUARD AS – БЛОКИРОВКА АТАК НА МАРШРУТИЗАТОРАХ

- Блокировка трафика: BGP Blackhole
- Динамическая фильтрация на маршрутизаторах (BGP FlowSpec): IP-адреса источника и получателя трафика, протоколы, порты, флаги, размеры пакетов, фрагментация
- Фильтрация с помощью ACL: IP-адреса источника и получателя, порты, флаги, протоколы
- Шейпинг трафика с помощью BGP FlowSpec



Детектирование аномалий (атак)

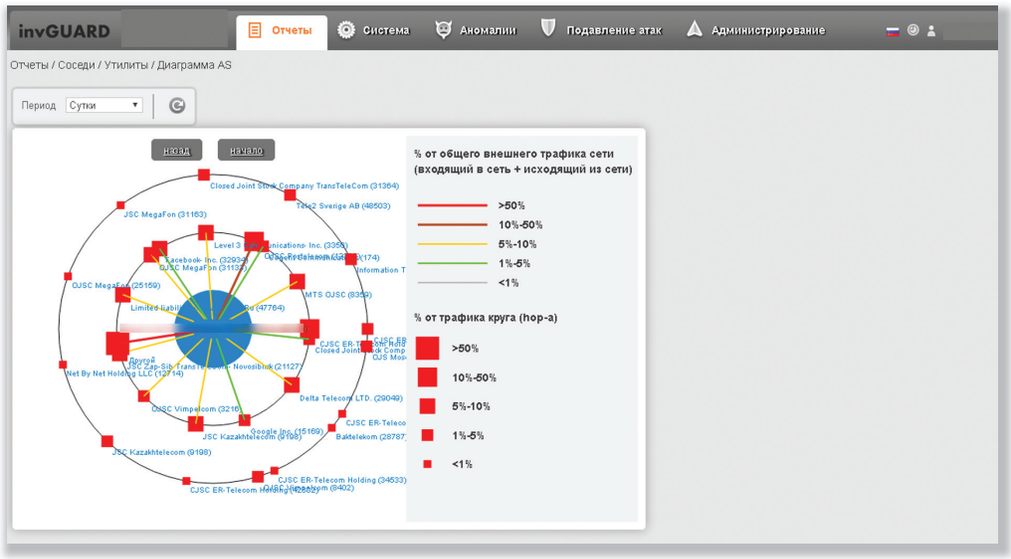
invGUARD

Система защиты от сетевых атак

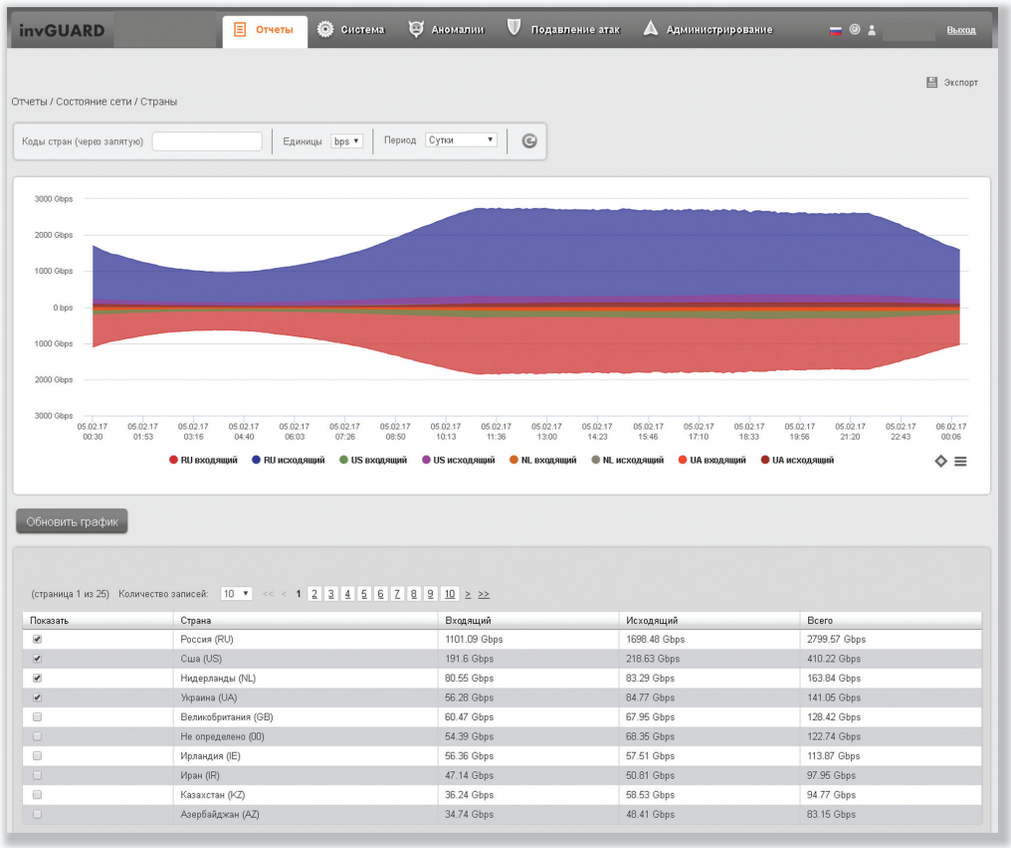
ИНСТРУМЕНТ ДЛЯ ПРИНЯТИЯ РЕШЕНИЯ

invGUARD AS – инструмент, который позволяет получить ответы на вопросы:

- Какой трафик поступает в сеть и отправляется из сети;
- Какой маршрут проходит трафик;
- Какие интерфейсы и маршрутизаторы задействованы и как они загружены;
- Какие адреса формируют больше всего трафика.



Соседи и провайдеры

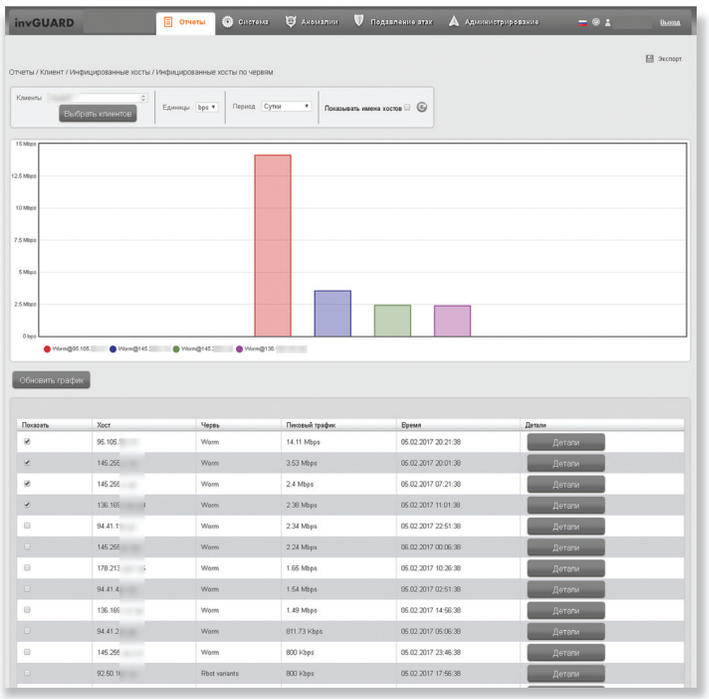


Отчеты по странам

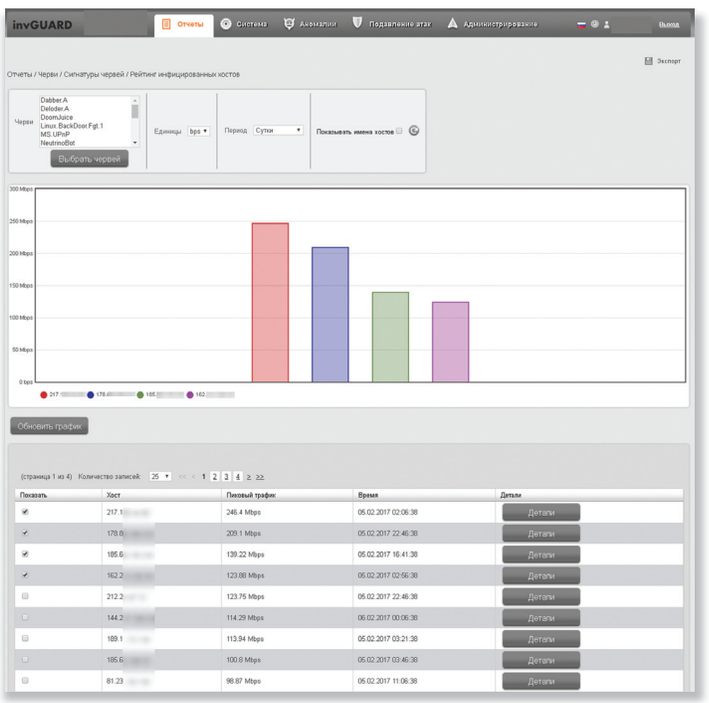
БЕЗОПАСНОСТЬ

invGUARD AS детектирует:

- Превышение динамически вычисляемого профиля трафика;
- DDoS-атаки: различные типы flood, некорректное использование протоколов;
- Зараженные объекты в сети («черви»);
- Объекты, которые возможно будут целями атак;
- Боты в сети и их общение с центрами управления.



Зараженные объекты



Боты в сети

invGUARD

Система защиты от сетевых атак

СПЕЦИФИКАЦИЯ invGUARD AS (НА УСТРОЙСТВО):

- Анализ трафика до 5 Тбит/с;
- Поток NetFlow до 100000 пакетов в секунду;
- BGP: до 100 маршрутизаторов ;
- BGP: до 6 000 000 записей в таблице маршрутизации;
- API для управления наблюдаемыми объектами, параметрами детектирования и подавления атак и для получения отчетов;
- Уведомления: сообщения по SMTP, SNMP-трэпы и syslog;
- Веб-интерфейс для управления (администраторы, инженеры по безопасности);
- Веб-интерфейс для клиентов (личный кабинет).

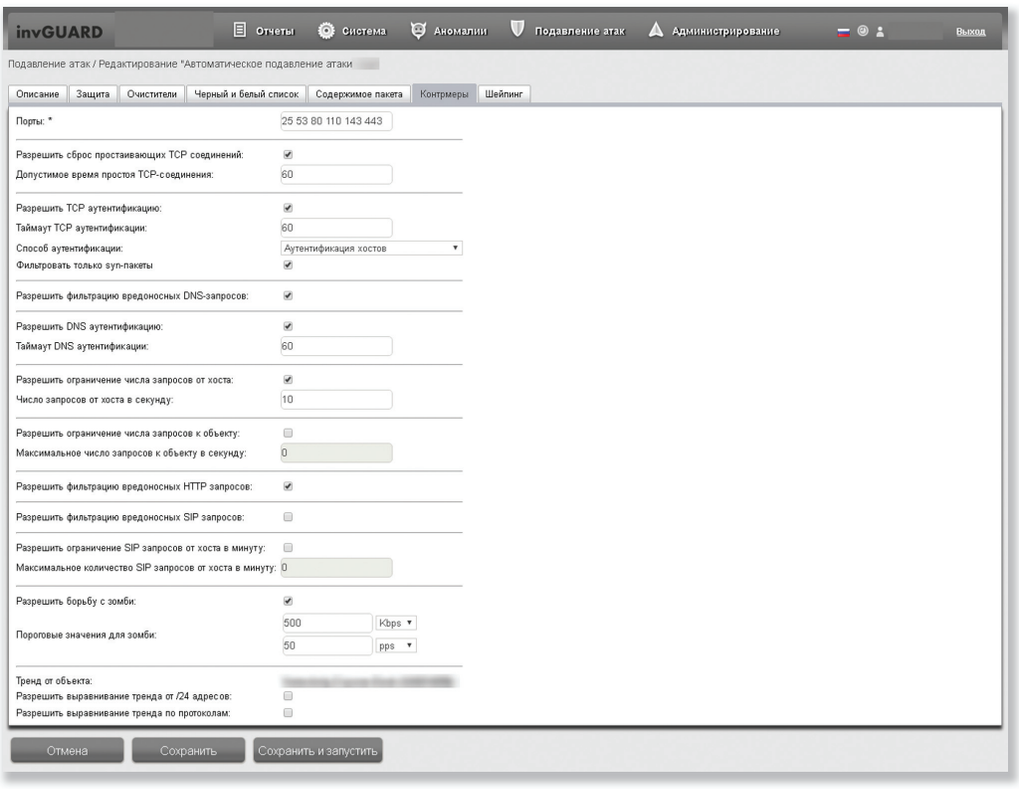
invGUARD CS – ОЧИСТИТЕЛЬ

invGUARD CS тщательно и деликатно производит очистку трафика

Аномальный трафик выделяется системой invGUARD AS из обычного потока с помощью анонса BGP nexthop и перенаправляется на систему очистки трафика invGUARD CS, где аномальный трафик проходит детальный разбор до прикладного уровня (7-й уровень по OSI) – нелегитимные пакеты трафика атаки отбрасываются, а легитимные направляются к объекту.

invGUARD CS позволяет:

- Собирать сессии трафика для выявления и устранения вредоносных воздействий;
- Использовать настройки контрмеры для маркировки пакетов трафика как нелегитимные внутри системы;
- Сбрасывать нелегитимные пакеты (не пропускает трафик атаки к защищаемому объекту)
- Пропускать очищенный трафик к защищаемому объекту.



invGuard CS настройки контрмер

invGUARD CS – ПОДАВЛЕНИЕ АТАК

- SYN авторизация: авторизация TCP сессий, авторизация соединений, авторизация хостов
- DNS авторизация: блокировка пакетов с поддельными адресами
- Черный и белый списки
- Глобальные настройки фильтрации (для всех задач подавления атак)
- Выявление зомби: фильтрация по количеству соединений, запросов и объему трафика
- Предотвращение «висящих» TCP сессий
- Сборка TCP сессий: правильный порядок TCP фрагментов от источника к получателю
- Автоподавление атак: активация фильтрации по данным от invGUARD AS
- Шейпинг: уменьшение трафика до определенного уровня
- Сбор детальной статистики
- Сбор сырого трафика может быть активирован пользователем в рамках задания

СПЕЦИФИКАЦИЯ invGUARD CS (НА УСТРОЙСТВО):

- Очистка и фильтрация трафика до 20 Гбит/с (invGUARD CS)
- Очистка и фильтрация трафика до 1 Гбит/с (invGUARD CS-01)
- Подавление атак на уровне приложений (HTTP, DNS, SIP,…)
- Автоматическое, полуавтоматическое и ручное подавление атак
- Поддержка тонких настроек фильтрации

ПРЕИМУЩЕСТВА invGUARD

1. Решение, эффективное по затратам, для детектирования и предотвращения кибератак (DoS/DDoS-атак и воздействий, не имеющих четко выраженных сигнатур)

invGUARD сохраняет инвестиции – не требуется обновление сетевого оборудования, т.к. система использует открытые форматы статистики трафика: SNMP и NetFlow.

Наилучшая практика для защиты от атак – использование BGP протокола для управления потокам и трафика: Blackhole, FlowSpec и Next Hop перенаправление трафика – все эти механизмы поддерживает invGUARD.

invGUARD детектирует аномалии и воздействия как поведение трафика наблюдаемых (защищаемых) объектов. Для полнофункциональной работы системы не требуется регулярного обновления баз данных сигнатур.

2. Снижение рисков от воздействий атак на отказ в обслуживании наблюдаемых (защищаемых) объектов, таких как веб-сайты, интернет-магазины, медиа-порталы и других

invGUARD детектирует аномалии трафика, DoS/DDoS атаки и вредоносные воздействия, не имеющих четко выраженных сигнатур, информирует сотрудников в режиме реального времени для минимизации влияния атак на защищаемые объекты, а также помогает объектам всегда быть доступными.

invGUARD очищает трафик по черным/белым спискам, некорректному использованию протоколам и вредоносным воздействиям для предотвращения DoS/DDoS атак на наблюдаемые (защищаемые) объекты.

3. Удобный инструмент для анализа трафика и оптимизации сетевой инфраструктуры

invGUARD предоставляет возможность анализа трафика в сетях с объемом трафика до 5 Тбит/с, состоящей из сотен маршрутизаторов: более 250 настраиваемых отчетов по протоколам, приложениям, BGP атрибутам, наблюдаемым объектам, интерфейсам, QoS-параметрам, маршрутной информации и странам.

invGUARD помогает принимать обоснованные решения по оптимизации потоков сетевого трафика, маршрутам и сетевой инфраструктуры.

4. Простая интеграция с существующими системами мониторинга и платформами управления сетями по протоколу SNMP (HPE OV, IBM Tivoli, Zabbix, Nagios и другие)

invGUARD просто интегрируется с системами мониторинга и платформами управления сетями по протоколу SNMP. Система направляет SNMP-трэпы при обнаружении аномалий и сетевых атак с использованием зарегистрированного идентификатора enterprise.44937.1.1 OID.

Дополнительно, invGUARD использует механизм SYSLOG для импорта и экспорта событий безопасности во внешние системы.

5. Эшелонированная защита от сетевых атак для повышенного уровня безопасности (Cloud Signaling)

invGUARD помогает выстроить эшелонированную защиту информационных ресурсов и сетей с помощью функционала Cloud Signaling для высокоскоростных и объемных DoS/DDoS-атак на уровнях сетей провайдеров для защищаемой сети.

invGUARD является инструментом для эффективной многоуровневой защиты и различных уровней безопасности.

6. Мониторинг исполнения SLA по доступу к информационным ресурсам

invGUARD формирует более 250 различных отчетов, которые позволяют выстроить механизмы контроля и мониторинга SLA по доступу к наблюдаемым объектам (информационным ресурсам, сегментам сети и т.д.) и направляет уведомления при нарушениях SLA. Отчеты содержат информацию о профилях трафика, порогах детектирования, периодах отсутствия доступа и наличия сервисов.

7. Эффективный инструмент для управления затратами на услуги связи

invGUARD формирует отчеты по провайдерам/соседям и предоставляет возможность определить наиболее опасные (источники атак) и наиболее безопасные (без источников атак) подключения к внешним сетям. Предоставляет инструменты для контроля использования и утилизации ресурсов сетевого оборудования.

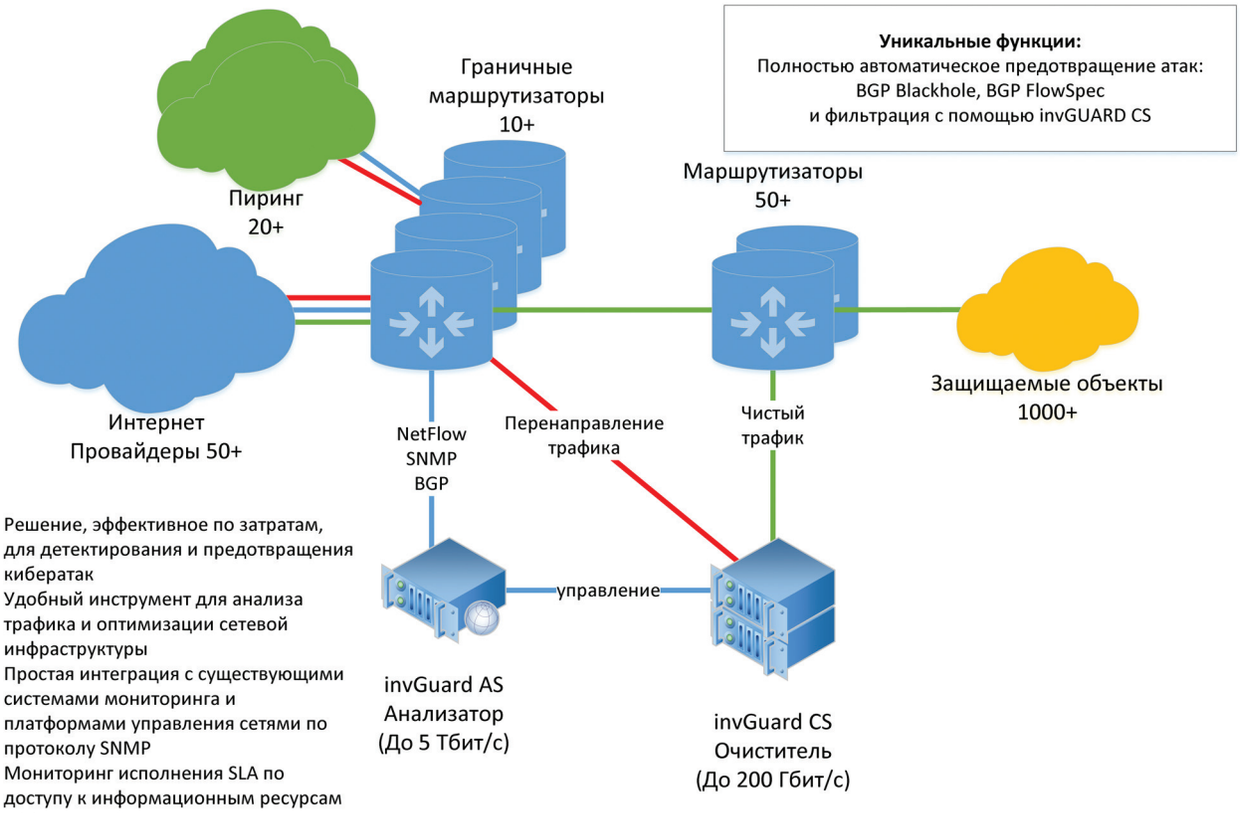
8. Дополнительный источник выручки по услугам защиты от DoS/DDoS-атак для B2B/B2C клиентов (простая интеграция с платформой управления облачными услугами InoSphere)

invGUARD обладает открытым API для интеграции с внешними системами управления и поставляется с предварительно настроенной конфигурацией для оказания услуг защиты от DoS/DDoS-атак, что позволяет заказчикам invGUARD организовать предоставление услуг в кратчайшие сроки и получать дополнительный доход.

InoSphere – платформа для предоставления облачных услуг для B2B/B2C клиентов в автоматическом режиме. InoSphere поставляется с встроенной поддержкой подключения к invGUARD и готова для предоставления услуг защиты от DoS/DDoS-атак с возможностью оказания платных услуг.

ПРИМЕНЕНИЕ invGUARD

Операторы связи



- Решение, эффективное по затратам, для детектирования и предотвращения кибератак
- Удобный инструмент для анализа трафика и оптимизации сетевой инфраструктуры
- Простая интеграция с существующими системами мониторинга и платформами управления сетями по протоколу SNMP
- Мониторинг исполнения SLA по доступу к информационным ресурсам
- Эффективный инструмент для управления затратами на услуги связи

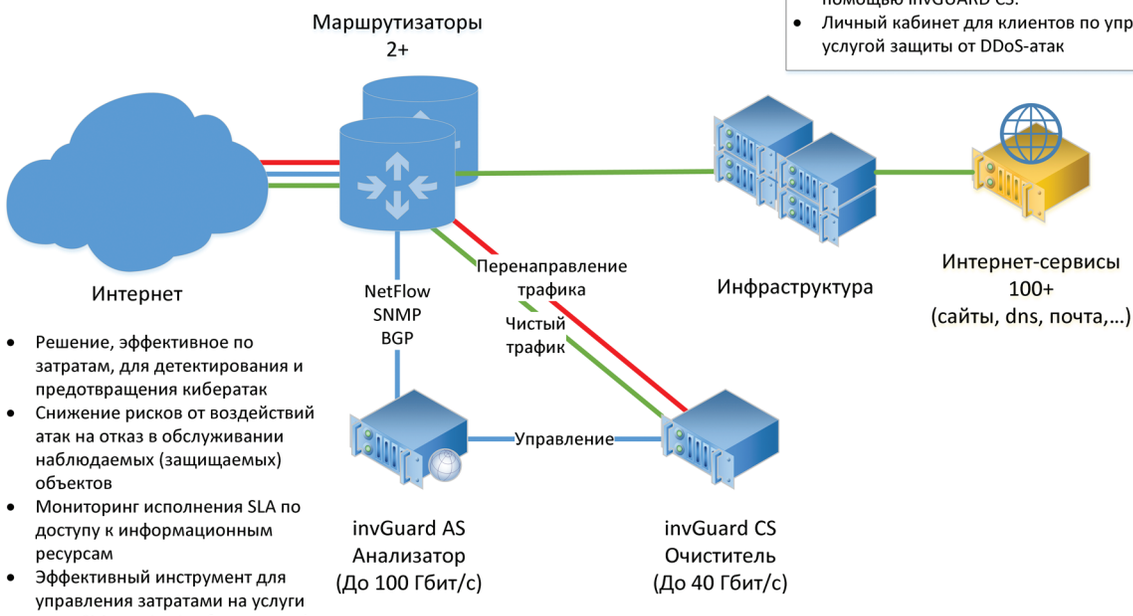
invGUARD

Система защиты от сетевых атак

Провайдеры интернет сервисов

Уникальные функции:

- Полностью автоматическое предотвращение атак: BGP Blackhole, BGP FlowSpec и фильтрация с помощью invGUARD CS.
- Личный кабинет для клиентов по управлению услугой защиты от DDoS-атак

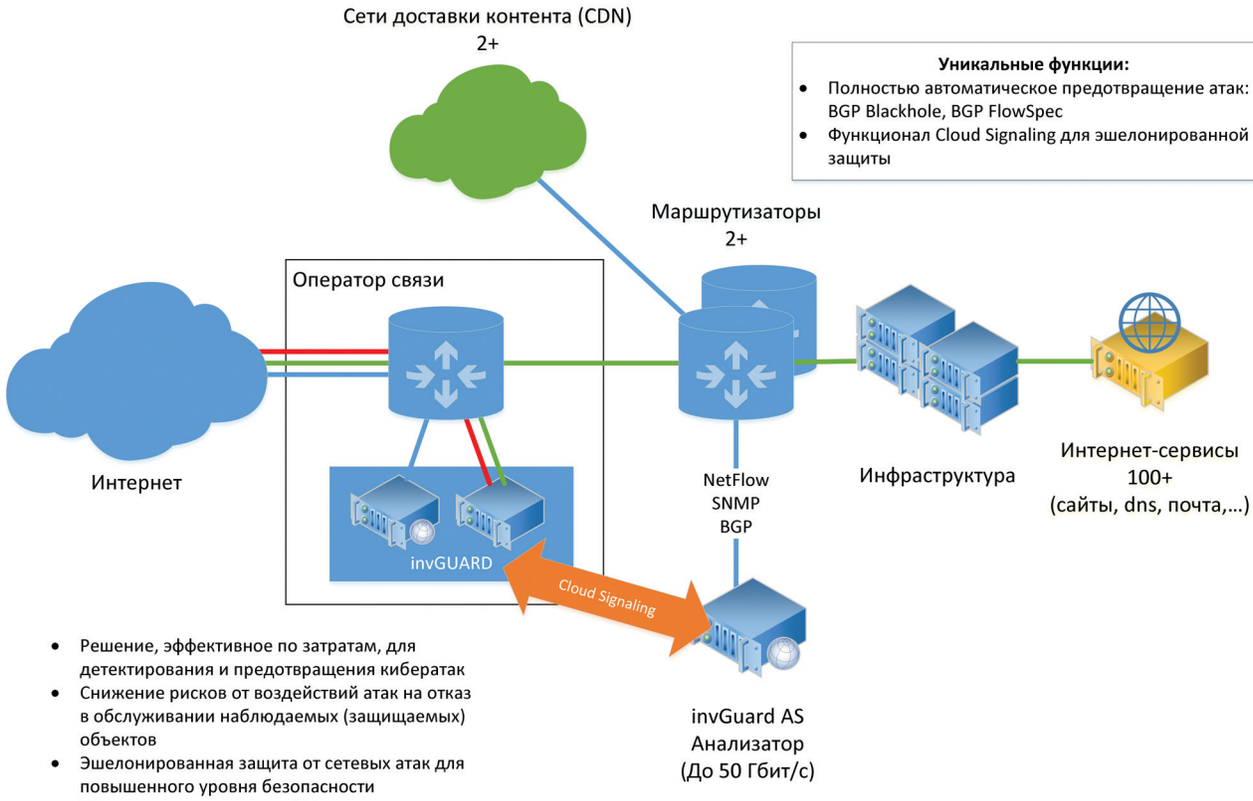


- Решение, эффективное по затратам, для детектирования и предотвращения кибератак
- Снижение рисков от воздействий атак на отказ в обслуживании наблюдаемых (защищаемых) объектов
- Мониторинг исполнения SLA по доступу к информационным ресурсам
- Эффективный инструмент для управления затратами на услуги связиSLA monitoring for managed objects access
- Effective tool for manage of telco services expenses

Операторы центров обработки данных

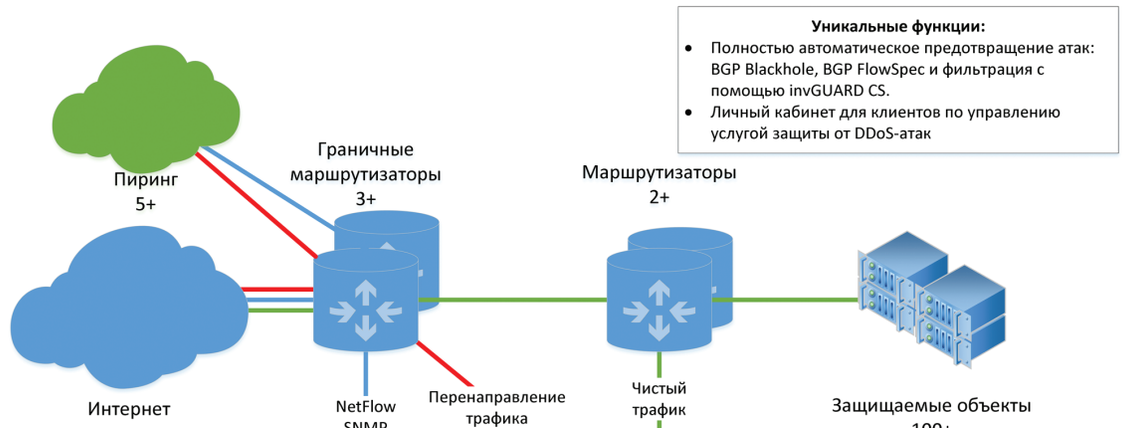
Уникальные функции:

- Полностью автоматическое предотвращение атак: BGP Blackhole, BGP FlowSpec
- Функционал Cloud Signaling для эшелонированной защиты



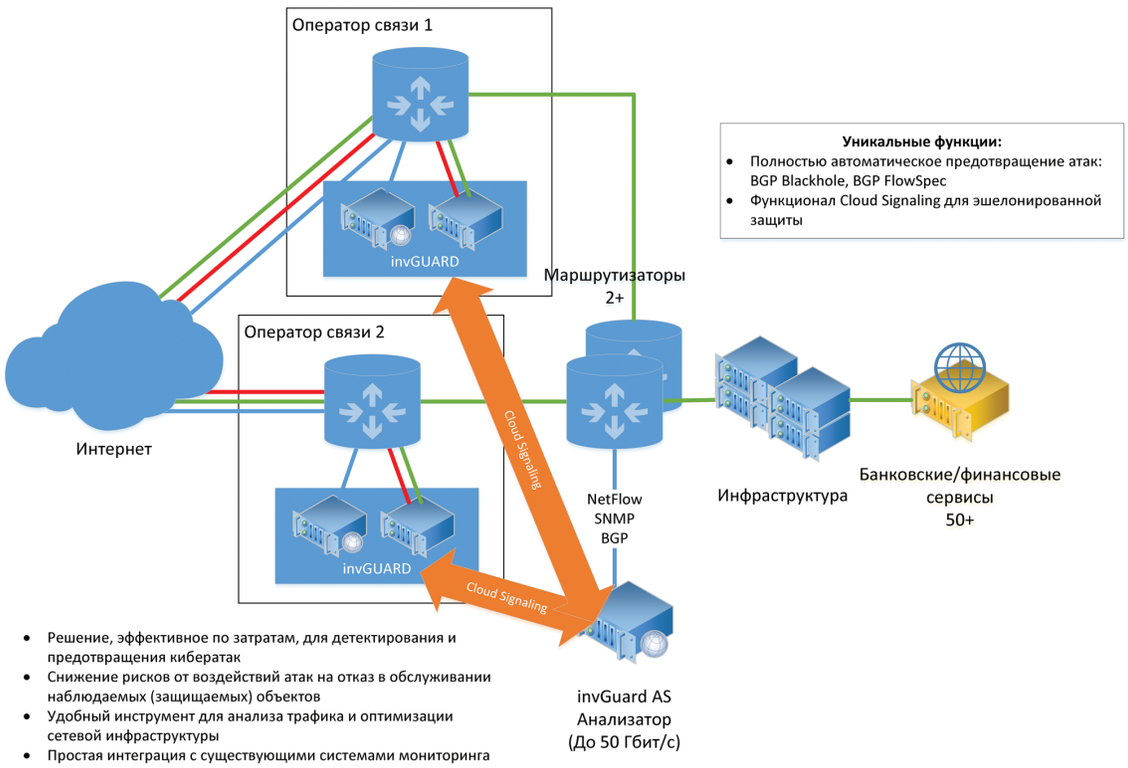
- Решение, эффективное по затратам, для детектирования и предотвращения кибератак
- Снижение рисков от воздействий атак на отказ в обслуживании наблюдаемых (защищаемых) объектов
- Эшелонированная защита от сетевых атак для повышенного уровня безопасности
- Мониторинг исполнения SLA по доступу к информационным ресурсам
- Эффективный инструмент для управления затратами на услуги связи

Компании медиа-сферы



- Решение, эффективное по затратам, для детектирования и предотвращения кибератак
- Удобный инструмент для анализа трафика и оптимизации сетевой инфраструктуры
- Простая интеграция с существующими системами мониторинга и платформами управления сетями по протоколу SNMP
- Мониторинг исполнения SLA по доступу к информационным ресурсам
- Эффективный инструмент для управления затратами на услуги связи

Банки и финансовые институты



- Решение, эффективное по затратам, для детектирования и предотвращения кибератак
- Снижение рисков от воздействий атак на отказ в обслуживании наблюдаемых (защищаемых) объектов
- Удобный инструмент для анализа трафика и оптимизации сетевой инфраструктуры
- Простая интеграция с существующими системами мониторинга и платформами управления сетями по протоколу SNMP
- Эшелонированная защита от сетевых атак для повышенного уровня безопасности
- Мониторинг исполнения SLA по доступу к информационным ресурсам
- Эффективный инструмент для управления затратами на услуги связи

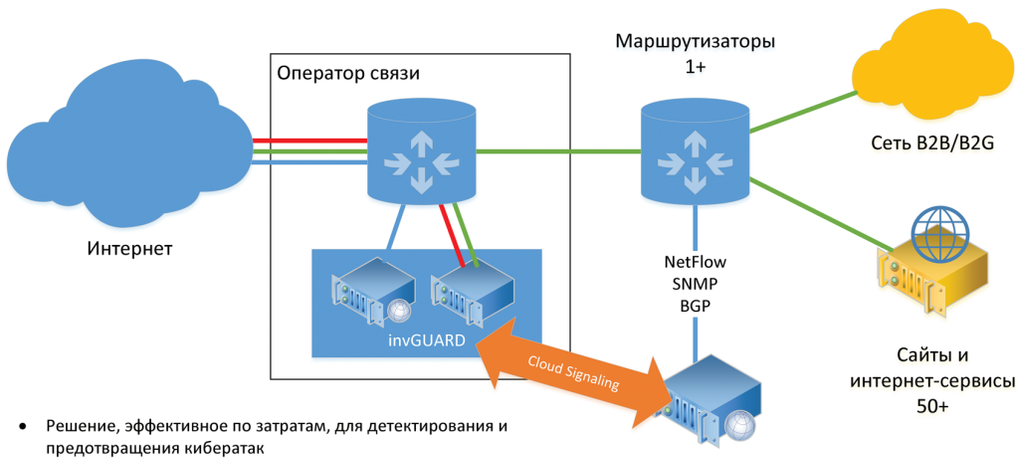
invGUARD

Система защиты от сетевых атак

B2B и B2G с собственной ИТ-инфраструктурой

Уникальные функции:

- Полностью автоматическое предотвращение атак: BGP Blackhole, BGP FlowSpec
- Функционал Cloud Signaling для эшелонированной защиты

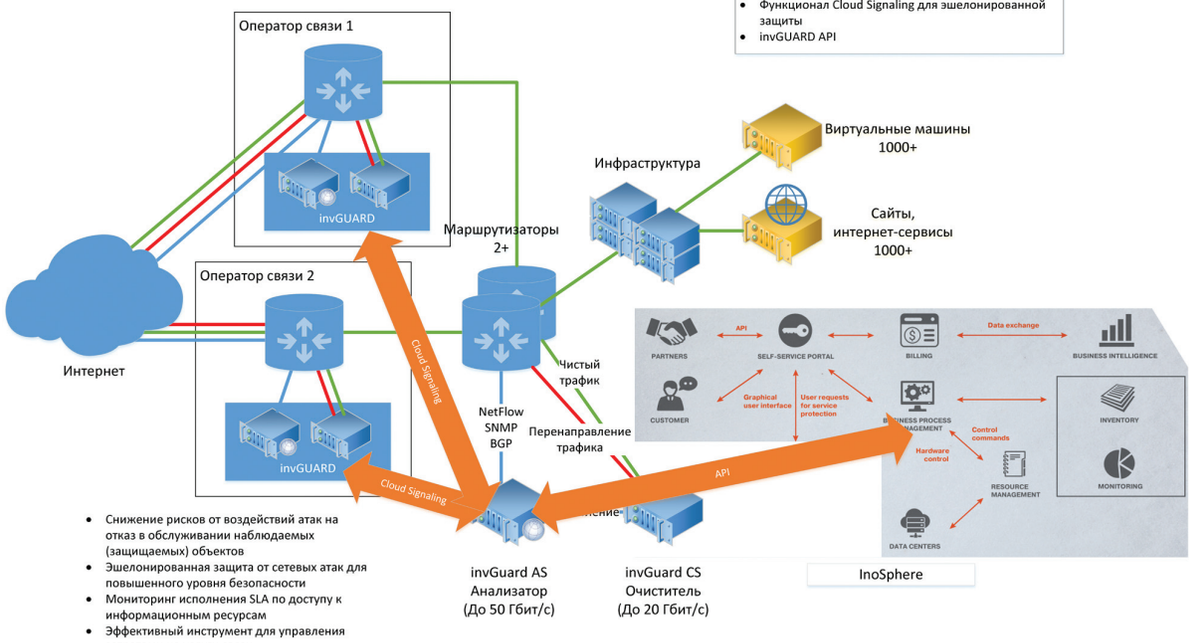


- Решение, эффективное по затратам, для детектирования и предотвращения кибератак
- Снижение рисков от воздействий атак на отказ в обслуживании наблюдаемых (защищаемых) объектов
- Простая интеграция с существующими системами мониторинга и платформами управления сетями по протоколу SNMP
- Эшелонированная защита от сетевых атак для повышенного уровня безопасности
- Мониторинг исполнения SLA по доступу к информационным ресурсам
- Эффективный инструмент для управления затратами на услуги связи

Защита от атак для провайдеров массовых облачных услуг и услуг хостинга

Уникальные функции:

- Полностью автоматическое предотвращение атак: BGP Blackhole, BGP FlowSpec и фильтрация с помощью invGUARD CS.
- Функционал Cloud Signaling для эшелонированной защиты
- invGUARD API



- Снижение рисков от воздействий атак на отказ в обслуживании наблюдаемых (защищаемых) объектов
- Эшелонированная защита от сетевых атак для повышенного уровня безопасности
- Мониторинг исполнения SLA по доступу к информационным ресурсам
- Эффективный инструмент для управления затратами на услуги связи
- Дополнительный источник выручки по услугам защиты от DoS/DDoS-атак для B2B/B2C клиентов (простая интеграция с платформой управления облачными услугами InoSphere)

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

СБОР NETFLOW

invGUARD собирает статистику трафика по протоколам:

- NetFlow v5
- NetFlow v9
- NetFlow v10
- NetStream v5 и v9 для маршрутизаторов Huawei с таблицей SNMP преобразования интерфейсов
- IPFIX
- sFlow

NetFlow параметры: IP-адрес источника, порт, уровень семплирования

ВЗАИМОДЕЙСТВИЕ ПО ПРОТОКОЛУ SNMP

invGUARD собирает информацию по интерфейсам с использованием протокола SNMP:

- интерфейсы маршрутизаторов: ifIndex, описание, скорость, IP-адреса
- статистика по трафику (счетчики)
- загрузка процессора маршрутизатора
- использование оперативной памяти маршрутизатора

SNMP-трэпы для внешних систем мониторинга и платформ управления сетями:

- invGUARD спроектирован для интеграции с внешними системами мониторинга для направления событий детектирования сетевых атак с помощью SNMP-трэп.
- Внешние системы мониторинга могут опрашивать invGUARD для получения детальной информации об атаках по протоколу SNMP v2c с определенным enterprise.44937.1.1 OID.
- invGUARD успешно интегрируется с такими системами мониторинга как: Zabbix, Nagios и другими.

SNMP параметры: версия, IP-адрес, community (для v2/v2c), логин/пароль (для v3)

МАРШРУТИЗАЦИЯ ТРАФИКА

- Обновления BGP для изменения маршрутов трафика:
  - Blackhole
  - NextHop
  - FlowSpec
- Динамическая маршрутизация с использованием GRE-туннелей в системе invGUARD CS

BGP параметры: IP-адрес маршрутизатора, ID маршрутизатора, локальный и удаленный номера автономных систем, ключ md5

BGP-PEERING

- iBGP
- iBGP с маршрутизаторами-рефлекторами маршрутов
- iBGP с сервером маршрутизации
- использование BGP таблиц маршрутизации других маршрутизаторов
- eBGP

ДЕТЕКТИРОВАНИЕ АНОМАЛИЙ

- BGP ловушки
- BGP нестабильность
- Подделка BGP
- Потеря BGP
- Пропуск NetFlow
- Отсутствие SNMP
- DoS- и DDoS-атаки
- Пороги по объему трафика
- Пороги по загрузке интерфейсов
- Пороги по трафику наблюдаемых объектов
- Трафик «темных» IP-адресов

ДЕТЕКТИРОВАНИЕ БОТОВ

- Детектирование активности ботов
- Пороги по трафику активности ботов

ДЕТЕКТИРОВАНИЕ СЕТЕВЫХ АТАК

- TCP SYN Flood
- TCP RST Flood
- TCP Flood
- HTTP Flood
- DNS Request Flood
- DNS Amplification
- NTP Amplification
- SSDP Amplification
- FTP Flood
- Некорректный SIP-трафик
- UDP Flood (Сервисы на базе UDP протокола: SNMP, Radius, NTP, IPSec поверх UDP и другие)
- ICMP Echo Request/Reply Flood

ФИНГЕРПРИНТЫ

invGUARD обладает настраиваемыми фингерпринтами сетевых атак, которые могут быть внесены пользователем или получены из центрального репозитория:

- Пользователи могут создавать и изменять фингерпринты через интерфейс invGUARD
- Фингерпринты могут обновляться из центральной базы данных базы данных базы данных «Иновентики Технолоджес»

КОНФИГУРАЦИЯ ИНТЕРФЕЙСОВ

- Список интерфейсов на маршрутизаторах (индекс, название, описание и скорость)
- Управление классификацией интерфейсов
- Пороги трафика по интерфейсам

АВТОМАТИЧЕСКАЯ КОНФИГУРАЦИЯ ИНТЕРФЕЙСОВ

- Управление правилами автоматической конфигурации интерфейсов: каждое изменение интерфейса на маршрутизаторе детектируется системой и invGUARD запускает определение типа интерфейса по заданным правилам.
- Правила определяются регулярным выражением (regexp) по описанию интерфейса для определения типа интерфейса.
- Правила устанавливают тип интерфейса (внутренний, внешний, игнорируемые и т.д.)

НАБЛЮДАЕМЫЕ ОБЪЕКТЫ

- Типы: клиент, профиль, сосед, червь
- Определение трафика наблюдаемого объекта:
  - Бинарное выражение
  - Регулярное выражение AS Path regexp
  - CIDR блоки
  - CIDR группы
  - BGP community
  - Интерфейсы
  - Соседние ASN
  - Локальная ASN или SubAS
- Порог по трафику объекта по детекторам или поведению трафика
- Параметры детектирования и уведомления
- Параметры подавления атак: автоматическое/ручное, шаблоны заданий на подавление атак, способ подавления атак

СОБСТВЕННАЯ БЕЗОПАСНОСТЬ

- Защищенные подключения между компонентами invGUARD
- Контроль доступа и логирование
- Управление идентификацией и авторизацией пользователей
- Исторические отчеты по доступу к системе и использованию функций
- Детектирование фишинга NetFlow

ОТЧЕТЫ

Каждый представленный в invGUARD отчет может быть настроен для просмотра необходимого периода (день, неделя, месяц, год или другой) и для экспорта отчетов в форматы: текст, XML, PDF (просто вызвав пункт «Экспорт» в отчете).

1. **Суммарный отчет по трафику**
2. **Суммарный отчет с активными аномалиями**
3. **Текущие и предыдущие аномалии с настраиваемым фильтром (важность, наблюдаемый объект, маршрутизатор, пороги и др.)**
4. **Статус системы invGUARD**
5. **Суммарный отчет по маршрутизаторам**
6. **Панель мониторинга маршрутизатора**
7. **Суммарный отчет по интерфейсам**
8. **Суммарный и детальный отчет по BGP (таблица маршрутизации, обновления)**
9. **NetFlow/SNMP comparing**
10. **Отчеты по наблюдаемым объектам:**
    - a. Суммарный
    - b. По протоколам: ICMP, TCP, UDP
    - c. По BGP атрибутам: все ASN, Origin ASN, Peer ASN, AS path, ASxAS, communities, Next hop, префиксы
    - d. По маршрутизаторам
    - e. По интерфейсам
    - f. По другим наблюдаемым объектам (клиент, сосед, профиль)
    - g. Мультикаст-трафик
    - h. QoS
        - i. ToS
        - ii. DTRM
        - iii. IP Precedence
    - i. По размерам пакетов
    - j. По странам
11. **Отчеты по червям и ботам:**
    - a. Активность по объектам или IP-адресам
    - b. Зараженные хосты (ресурсы) внутри или вне сети
12. **Отчеты по invGUARD CS**
    - a. Фильтрация трафика
    - b. Статистика:
    - i. По протоколам
    - ii. По HTTP: списки URL
    - iii. По DNS: домены
    - iv. По SIP: номера абонентов
13. **Отчеты по аномалиям:**
    - a. Текущие (активные) аномалии
    - b. Детализация по аномалиям:
    - i. Влияние
    - ii. Детальные IP-адреса: отправители и получатели
    - iii. Порты
    - iv. Страны
    - v. Номера автономных систем
    - vi. Размеры пакетов
    - vii. Маршрутизаторы и интерфейсы
    - c. Прошедшие (завершенные) аномалии

ПРОГРАММНЫЙ ИНТЕРФЕЙС invGUARD API

Программный интерфейс **invGUARD API** может быть использован через HTTPS протокол с поддержкой формата JSON, упакованного с помощью механизма MessagePack.

Программный интерфейс **invGUARD API** может использоваться для автоматизации задач управления системой invGUARD из внешних систем:

- Создание, изменение и просмотр наблюдаемых объектов
- Управление параметрами детектирования сетевых атак
- Получение перечня детектированных сетевых атак по текущим и историческим событиям
- Управление параметрами подавления атак
- Получение перечня заданий подавления атак
- Получение отчетных данных по трафику наблюдаемых объектов

invGUARD + InoSphere

invGUARD подготовлен для быстрой и простой интеграции с платформой управления облачными услугами InoSphere для предоставления услуг по защите от сетевых атак для пользователей (клиентов) услуг InoSphere.

Пользователи InoSphere получают бесплатный доступ к статистике трафика для каждого IP-адреса заказанной через InoSphere услуги.

Услуги по защите от сетевых атак включают детектирование и подавление (предотвращение) сетевых атак. InoSphere управляет системой invGUARD через программный интерфейс invGUARD API для настройки параметров наблюдаемых объектов, параметров детектирования и способов подавления атак.

InoSphere поддерживает возможность тарификации и биллинга услуг защиты от сетевых атак: ежемесячно по различным тарифам и по часам.

Пользователи InoSphere могут простым способом управлять услугами защиты от сетевых атак, представленных системой invGUARD и выбирать необходимый тариф через личный кабинет InoSphere.

ИНТЕГРАЦИЯ invGUARD С ВНЕШНИМИ СИСТЕМАМИ МОНИТОРИНГА ПО ПРОТОКОЛУ SNMP

invGUARD спроектирован для интеграции с внешними системами мониторинга для направления событий детектирования сетевых атак с помощью SNMP-трэп.

Внешние системы мониторинга могут опрашивать invGUARD для получения детальной информации об атаках по протоколу SNMP v2c с определенным enterprise.44937.1.1 OID.

invGUARD успешно интегрируется с такими системами мониторинга как: Zabbix, Nagios и другими.

invGUARD CLOUD SIGNALLING

invGUARD Cloud Signaling предоставляет функционал для «облачной» очистки трафика от сетевых атак, фильтрации по черных/белых спискам, шейпинга и некорректного использования протоколов.

invGUARD Cloud Signaling может быть использован в системе invGUARD AS для подключения к «облаку», предоставляемому операторами связи с помощью системы invGUARD и активным функционалом invGUARD Cloud Signaling. В случае отсутствия системы очистки invGUARD CS у заказчика, подключение к «облачной» очистке трафика от провайдера с функционалом invGUARD Cloud Signaling позволит заказчику производить фильтрацию и очистку трафика у провайдера.

Системы invGUARD используют стандартный протокол invGUARD Cloud Signalling для обмена заданиями подавления атак и обмена статистикой без сохранения любой коммерческой информации на системах провайдеров.

invGUARD Cloud Signaling с ролью «Клиент» может быть назначена любой системе invGUARD AS для предоставления дополнительных возможностей для подавления атак с функционалом фильтрации трафика в системах с ролью «Провайдер» без необходимости установки системы invGUARD CS.

invGUARD Cloud Signaling с ролью «Провайдер» может быть назначена для систем invGUARD в составе системы анализа трафика invGUARD AS и системы очистки трафика invGUARD CS (как

- Фильтрации по черным/белым спискам
- TCP авторизации
- Управления TCP соединения и ограничения количество соединений
- Проверки протоколов HTTP, DNS, SIP на соответствие стандартам (RFC)
- Ограничения одновременных запросов к/от объекту или хоступ
- Проверки содержимого пакетов трафика по регулярным выражениям
- Контроля тренда трафика
- Детектирования и подавления активности зомби
- Шейпинга трафика

ДОРОЖНАЯ КАРТА invGUARD

2 полугодие 2016	1 полугодие 2017	2 полугодие 2017
• invGUARD Cloud Signaling • invGUARD API • Поддержка оборудования: Huawei, Alcatel, Extreme • Улучшения интерфейсов: личный кабинет для клиентов, новый механизм отображения отчетов и графики	• Инструменты анализа по детектированию и предотвращению сетевых атак • IPv6: анализ NetFlow • IPv6: детектирование атак • Новые источники данных по атакам: IDS, IPS, firewall • Фильтрация трафика до 10 Гбит/с на базе сетевых плат с чипом intel	• IPv6: фильтрация и очистка трафика • Партнерство с антивирусными компаниями

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА И СОПРОВОЖДЕНИЕ

- Бесплатные обновления по Глобальной Программе Обновлений клиентов
- Техническая поддержка 24/7 или 8/5
- Разработка новых отчетов по требованиям клиента – от 2-х недель
- Интеграция с системами мониторинга – от 1 дня

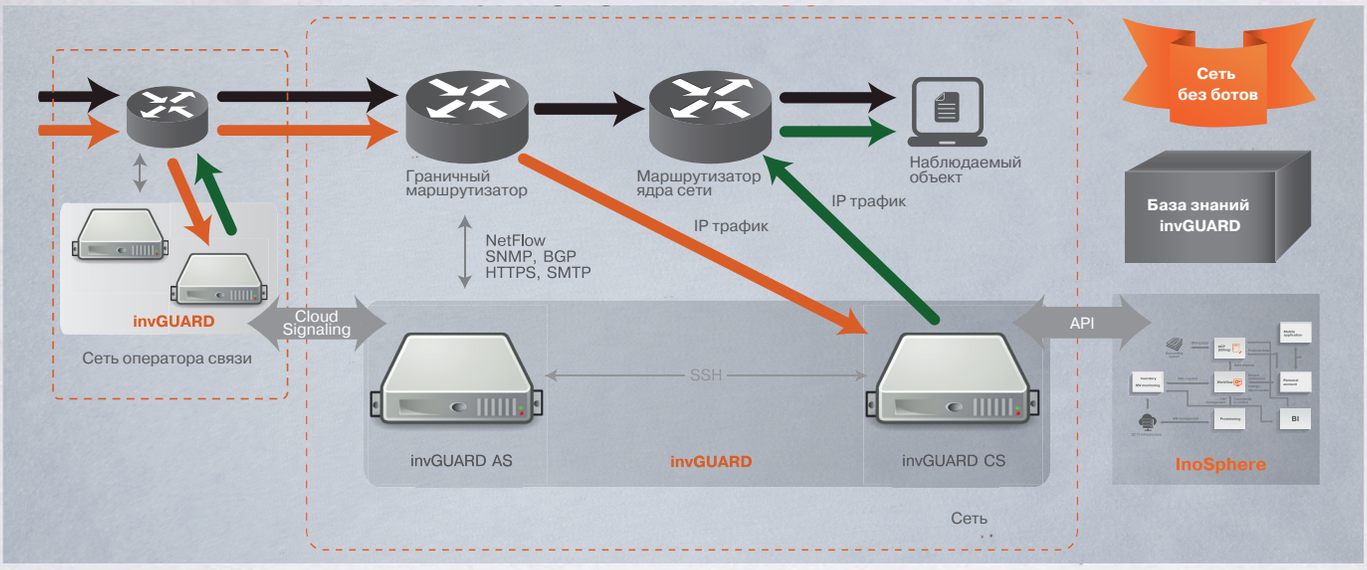
ВНЕДРЕНИЕ

Для типовой сети внедрение занимает 2 недели: 3-5 маршрутизаторов, до 100 Гбит/с трафика в сети.

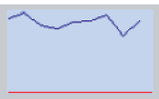
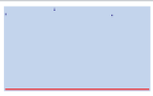
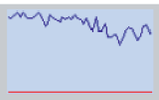
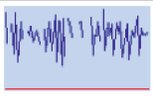
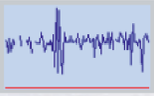
Внедрение удаленное или на площадке заказчика

Обучение специалистов заказчика экспертами invGUARD

АРХИТЕКТУРА СИСТЕМЫ invGUARD

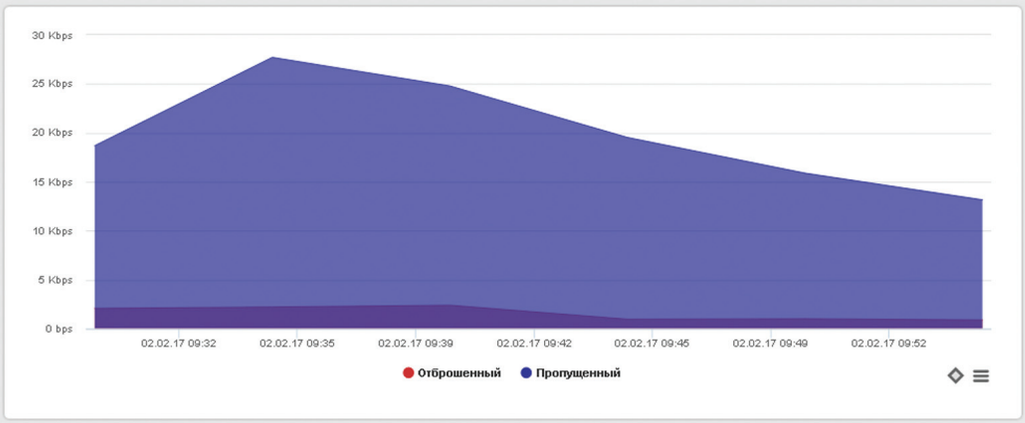


ОБНАРУЖЕНИЕ DOS-АТАК И АНОМАЛИЙ

508840		Высокая 244.0% от 4 Kpps	5.03 Kbps 2 pps	8 мин (продолжается)	02 Фев, 2017 09:57:26	Входящий	DoS атака (TCP RST)
508839		Средняя 71.5% от 6 Kpps	109.15 Mbps 9.66 Kpps	8 мин (продолжается)	02 Фев, 2017 09:57:26	Входящий	DoS атака (Превышение трафика для профиля)
508838		Средняя 12.1% от 100 Mbps	26.67 Mbps 2.7 Kpps	14 мин (продолжается)	02 Фев, 2017 09:51:26	Входящий	DoS атака (Превышение трафика для профиля)
508816		Высокая 244.0% от 4 Kpps	11.44 Mbps 26.53 Kpps	47 мин (продолжается)	02 Фев, 2017 09:18:26	Входящий	DoS атака (TCP RST)
508795		Средняя 10.4% от 100 Mbps	29.85 Mbps 2.65 Kpps	1 ч 23 мин (продолжается)	02 Фев, 2017 08:42:26	Входящий	DoS атака (Количество трафика, бит в секунду)
508780		Средняя 10.3% от 100 Mbps	36.31 Mbps 3.34 Kpps	1 ч 38 мин (продолжается)	02 Фев, 2017 08:27:26	Входящий	DoS атака (Количество трафика, бит в секунду)

ОЧИСТКА ТРАФИКА

Наименование	Автоматическое подавление атаки
ID задания	1245
ID исходного оповещения	895466
Очиститель	Cleaner 2
Наблюдаемый объект	
Префиксы	185.9.[redacted]/32
Время начала	02 Фев, 2017 09:32:23
Длительность	30 мин
Статус	Остановлено



Трафик

Период	Входящий	Пропущенный	Отброшенный	% Пропущенный
Последняя минута	0 bps/0 pps	0 bps/0 pps	0 bps/0 pps	0%
Всё время	17.92 Kbps/19.68 pps	16.59 Kbps/17.32 pps	1.33 Kbps/1.64 pps	93%

inoventica-tech.ru

facebook.com/inoventica vk.com/inoventica twitter.com/inoventica instagram.com/inoventica