«УТВЕРЖДАЮ»

Член правления — Заместитель генерального директора — Технический директор ПАО МГТС

_____ А.В.Трохин

«____» _____ 2016 г.

Система мониторинга и защиты от DoS/DDoS-атак

Требования технические

Версия 2.1

Москва

2016

Содержание

1 Общие сведения

Документ представляет собой технические требования к аппаратно-программному комплексу (АПК) анализа трафика магистральной сети с целью детектирования DoS/DDoS-атак на

телекоммуникационное оборудование и другие объекты защиты (сервисы, клиенты) и защиты (очистки трафика) от DoS/DDoS-атак на сервисы.

АПК предназначен для использования в реализации проекта «Защита коммутационного оборудования ПАО МГТС от внешних DoS/DDoS-атак».

2 Обязательства Участника

2.1 Требования по составу рабочей группы

2.1.1 В составе Рабочей группы Участника должны быть предусмотрены исполнители ролевых функций (должность, ФИО, контактная информация) согласно требованиям Проекта, коммерческое предложение должно содержать описание ролевых функций и трудозатраты по каждой роли.

2.1.2 Участник должен предоставить детализированный План-график реализации Проекта.

2.2 Требования к взаимодействию

2.2.1 Взаимодействие между специалистами ПАО «МГТС» и Компании-Участника должно документироваться Участником и должно организовываться:

- По телефону;
- По электронной почте;
- В рамках рабочих встреч.

2.2.2 Взаимодействие между специалистами ПАО «МГТС» и Компании-Участника должно быть организовано на русском языке.

2.3 Требования к этапности работ

2.3.1 Заключение Договора поставки оборудования АПК между ПАО «МГТС» и Участником конкурсной процедуры.

2.3.2 Разработка и утверждение Технического решения по внедрению АПК на сети ПАО «МГТС».

2.3.3 Поставка оборудования АПК на склад Поставщика в Москве, его последующая доставка и установка на сеть ПАО «МГТС», выполнение ПНР.

2.3.4 Стендовые испытания на соответствие функциональным и техническим требованиям.

2.3.5 Ввод в коммерческую эксплуатацию.

3 Требования к АПК

3.1 Цели создания Системы

3.1.1 Обнаружение и локализация DoS/DDoS-атак на коммутационное оборудование и объекты защиты ПАО «МГТС».

3.1.2 Уменьшения ущерба, наносимого DoS/DDoS-атаками ресурсам сети IP/MPLS и объектам защиты ПАО «МГТС».

3.1.3 Предоставления сервиса предупреждения DoS/DDoS.

3.1.4 Предоставление информации об актуальной маршрутизации магистральной сети и распределении трафика.

3.2 Назначение Системы:

3.2.1 Сбор статистической информации с маршрутизаторов МСПД (Магистральная сеть передачи данных), обнаружение DoS/DDoS-атак в наблюдаемом трафике, автоматическое оповещение об обнаруженных атаках в подсистему управления инцидентами, а также ответственным подразделениям по доступным каналам связи (электронная почта, СМС оповещения).

3.2.2 Изменение настроек маршрутизаторов в автоматическом/полуавтоматическом режиме, с целью предотвращения атак.

3.2.3 Предоставление пользователям системы собранной информации об обнаруженных DoS/DDoS-атаках в виде спектра отчетов.

3.2.4 Очистка трафика в автоматическом/полуавтоматическом режиме.

3.2.5 Снятие дампов трафика с фильтрацией по заданным критериям для последующей обработки.

3.2.6 Предоставление пользователям системы собранной информации об обнаруженных DoS/DDoS-атаках в виде спектра отчетов.

3.2.7 Система решает следующие задачи:

- Многофункциональное решение по мониторингу и выявлению атак типа «отказ в обслуживании» (DoS), включая «распределенные» (DDoS) на коммутационное оборудование и сервисы связи.
- Формирование правил по настройке маршрутизаторов магистральной сети и применение их в автоматическом/полуавтоматическом режиме.
- Очистка трафика в автоматическом/полуавтоматическом режиме
- Предоставление отчетов по сетевому трафику, включая отчеты по взаимодействию с вышестоящими операторами, отчеты по атрибутам BGP, отчеты по клиентам и абонентам, отчеты по приложениям и типам трафикам, отчеты по использованию вредоносного кода и угроз в сети.

3.3 Состав системы

3.3.1 Состав проектируемой Системы

3.3.2 Проектируемая Система должна включать в себя:

- подсистему сбора данных для статистического анализа распределения трафика на сети и обнаружения атак типа «отказ в обслуживании», включая распределенные атаки такого типа, выполненную в виде программно-аппаратной платформы.
- подсистему управления и принятия решений.
- подсистему очистки трафика.
- подсистему резервного копирования, предназначенную для периодического сохранения информации, собранной системой статистического анализа распределения трафика.

3.4 Структура Системы

3.4.1 Система должна содержать следующие элементы:

- **Обнаружение DoS/DDoS-атак**. Подсистема предназначена для обнаружения атак типа «отказ в обслуживании», в том числе распределенных;
- **Очистка трафика**. Подсистема предназначена для очистки подозрительного трафика
- **Управление и отчетность**, в состав которой входит GUI интерфейс. Подсистема предназначена для осуществления управления Системой;
- **Резервное копирование** – хранение резервных копий данных.

3.4.2 Работы по проектированию должны выполнялись с учетом требований, действующих государственных и международных стандартов, включая:

- ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;
- ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;
- ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы;
- РД 50-34.698-90. Автоматизированные системы. Требования к содержанию документов;
- РД 50-682-89. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения;
- ГОСТ 27.001-95. Надежность в технике. Основные положения;
- ГОСТ 27.002-89. Надежность в технике. Термины и определения;
- ГОСТ 27.003-90. Надежность в технике. Состав и общие правила задания требований по надежности;
- RFC 4364. BGP/MPLS IP Virtual Private Networks (VPNs);
- RFC 3330. Special-Use IPv4 Addresses;
- RFC 2328. OSPF Version 2;
- RFC 4271. A Border Gateway Protocol 4 (BGP-4);
- RFC 5575. Dissemination of Flow Specification Rules
- ГОСТ 12.1.004. Пожарная безопасность. Общие требования;
- ГОСТ 12.1.010. Взрывобезопасность. Общие требования;
- ГОСТ Р 50571.1. Электроустановки зданий. Основные положения;
- ГОСТ Р 50571.3. Электроустановки зданий. Часть 4. Требования по обеспечению безопасности. Защита от поражения электрическим током;
- ГОСТ Р 50571.10 (МЭК 364-1-72, МЭК 364-2-70). Электроустановки зданий. Заземляющие устройства и защитные проводники;
- ГОСТ 12.1.030. Электробезопасность. Защитное заземление, зануление.

3.5 Общие требования к системе

3.5.1 При разработке решения должен использоваться модульный/кластерный принцип, обеспечивающий последующее масштабирование Системы.

3.5.2 Управление всей системой, мониторинг трафика, выявление DoS/DDoS и применение правил очистки должны осуществляться из одного Web-интерфейса.

3.5.3 При масштабировании система должна позволять управлять не менее 150 собственными элементами, согласно описанию структуры (п.3.4), используя единый Web-интерфейс.

3.5.4 Система должна осуществлять сбор статистики с маршрутизаторов с помощью протоколов xFlow, SNMP, собирать информацию о маршрутизации по протоколу BGP и при необходимости, получать копию трафика для анализа.

3.5.5 Система должна управлять маршрутизацией трафика при обнаружении атак.

3.5.6 Система должна осуществлять очистку подозрительного трафика.

3.5.7 Система должна поддерживать полное и инкрементное резервное копирование, и восстановление с удалённого SFTP сервера.

3.5.8 Система должна поддерживать управление аутентификацией пользователей через локальную базу данных, RADIUS или TACACS+.

3.6 Функциональные требования к системе

3.6.1 Система должна иметь возможность сбора данных по протоколам Netflow версий 1, 3, 5, 7 or 9; Cflow версий 5, 9; Sflow версий 2, 4, 5; Netstream и IPFIX. Необходима поддержка Netflow sampling, конфигурируемый как в ручном режиме, так и с автоматическим распознаванием. Система должна иметь механизмы учёта и борьбы с дублированием собираемых данных, возникающих вследствие прохождения трафика через несколько находящихся под наблюдением системы интерфейсов.

3.6.2 Система должна иметь возможность сбора информации о маршрутизации с помощью BGP. Должна быть предусмотрена возможность получения не менее 1.000.000 BGP маршрутов с каждого маршрутизатора.

3.6.3 Система должна поддерживать 4-byte BGP ASN.

3.6.4 Подсистема должна иметь возможность отправления маршрутной информации с заданными администратором атрибутами Next-hop и Community по протоколу BGP для переключения трафика в BlackHole, подсистему очистки и прочие варианты дополнительной обработки и анализа. Должна быть возможность установить таймаут информации, после которой информация будет отозвана. Все указанные возможности должны поддерживаться в равной мере для IPv4 и IPv6.

3.6.5 Должна быть предусмотрена возможность перенаправления трафика в подсистему очистки с указанием целевого VRF (virtual routing and forwarding instance) с помощью BGP FlowSpec redirect community 0x8008 в процессе обнаружения атаки.

3.6.6 В подсистеме должен быть реализован механизм генерации и автоматического/полуавтоматического провижнинга (например, BGP flow-spec) настроечных команд на маршрутизаторы с целью управления ACL для пресечения нелегитимного трафика и ограничения/перенаправления аномального трафика.

3.6.7 Система должна иметь функционал автоматизированного сбора информации с маршрутизаторов, а также получения информации о всех интерфейсах маршрутизаторов по протоколу SNMP.

3.6.8 Необходимо наличие функционала автоматической конфигурации интерфейсов для снижения человеческих затрат на запуск системы.

3.6.9 Система должна иметь возможность создания до 2000 объектов мониторинга.

3.6.10 Должна существовать поддержка IPv6 объектов мониторинга.

3.6.11 Система должна иметь возможность получения сигнатур зловредного трафика от производителя и использования этих сигнатур для детектирования аномального трафика.

3.6.12 Система должна иметь возможность генерации собственных сигнатур и отправки данных сигнатур другим оператором связи для блокирования трафика в вышестоящих сетях.

3.6.13 Система должна осуществлять корреляцию полученных по BGP и Flow данных с целью предоставления отчетов о транзитном трафике в разрезе стран, сетевых элементов (в частности, номеров AS), приложений, объектов мониторинга, интерфейсов, сигнатур, протоколов, полей L3 и L4 заголовков.

3.6.14 Система должна предоставлять следующие возможности по анализу IPv6 трафика: отчеты о IP/TCP/UDP-трафике, отчеты о приложениях, отчеты по 6to4 (IP протокол 41) и teredo - туннелировании, отчеты по аппроксимации IPv6-трафика на будущие периоды времени.

3.6.15 Подсистема должна анализировать стабильность BGP-информации в сети с помощью анализа частоты изменения маршрутной информации.

3.6.16 Подсистема должна предоставлять отчеты по использованию “темного” (нелегитимного) IP-адресного пространства в заголовках анализируемого трафика.

3.6.17 Подсистема должна предоставлять возможность генерации пользовательских отчетов и их выгрузки в форматах CSV, XML, PDF, Excel.

3.6.18 Подсистема должна предоставлять доступ к базе данных Flow записей.

3.6.19 Система должна позволять обеспечить копирование Flow информации, получаемой от маршрутизаторов, на другие Flow-коллектора с целью уменьшения нагрузки на маршрутизаторы за счет снижения количества flow коллекторов, которым требуется отправка flow информации.

3.6.20 Подсистема очистки должна иметь возможность осуществлять эффективную очистку IPv6 трафика.

3.7 Требования к подсистеме очистки трафика

3.7.1 Подсистема очистки должна поддерживать по крайней мере 50 настраиваемых пользователем политик защиты. Пользователи должны иметь возможность изменять настройки защиты и включать/выключать защиту без прерывания трафика.

3.7.2 Подсистема очистки должна блокировать некорректные пакеты (включая проверку корректности заголовков, полноценности фрагмента, корректности контрольной суммы IP, дубликата фрагмента, длины фрагмента, длины пакета TCP/UDP/ICMP), корректности контрольной суммы TCP/UDP, корректности TCP-флагов, корректности ACK-номера) и обеспечивать статистику для отброшенных пакетов.

3.7.3 Подсистема очистки должна поддерживать сбрасывание неактивных TCP-сессий, если клиент не посылает заданный объём данных за заданный период времени.

3.7.4 Подсистема очистки должна ограничивать количество одновременных TCP-соединений по каждому хосту.

3.7.5 Подсистема очистки должна блокировать незавершённые в течение заданного промежутка времени HTTP и SSL/TLS-запросы.

3.7.6 Подсистема очистки должна поддерживать блокировку некорректных DNS, HTTP, SIP, SSL/TLS-запросов.

3.7.7 Подсистема очистки должна иметь возможность ограничивать количество DNS, HTTP и SIP-запросов в секунду с каждого источника в соответствии с настроенным порогом.

3.7.8 Подсистема очистки должна обеспечивать возможность конфигурировать по крайней мере 5 регулярных выражений для отбрасывания определённого DNS или HTTP-трафика с заголовками, соответствующими настроенным выражениям.

3.7.9 Подсистема очистки должна иметь возможность осуществлять ограничение (rate limiting) трафика по его географическим свойствам, т.е. на базе страны происхождения трафика.

3.7.10 Подсистема очистки должна иметь возможность выявлять хосты, превышающие заданный порог по пакетам или битам в секунду в рамках одной TCP/UDP-сессии, и ограничивать или блокировать трафик данной сессии.

3.7.11 Подсистема очистки должна выявлять ботов, не имеющих возможность распознавать и следовать командам HTTP 302 redirect.

3.7.12 Подсистема очистки должна выявлять ботов, не имеющих возможность распознавать и следовать redirect-командам, закодированным в JavaScript.

3.7.13 Подсистема очистки должна иметь возможность регулярно активировать новые защитные техники посредством регулярного обновления сигнатур атак, обеспечиваемые исследовательской командой производителя оборудования, которая осуществляет мониторинг Интернета 24x7, идентифицируя самую существенную и недавнюю активность ботнетов и стратегии нападения. Подсистема анализа ботнетов и текущих атак должна осуществлять глобальный мониторинг Интернет-трафика в крупнейших мировых Интернет-провайдерах.

3.7.14 Подсистема должна позволять создание профилей трафика для определенных администратором приложений.

3.7.15 Подсистема очистки должна позволять изменять параметры защиты во время её работы. Такие изменения не должны вызывать прерывания трафика.

3.7.16 Подсистема должна иметь возможность доставить уведомление о системных событиях посредством SMTP, SNMPtrap и SYSLOG.

3.7.17 Подсистема очистки должна иметь встроенный пакетный анализатор и декодер, который должен быть способен захватить по крайней мере 5000 пакетов соответствующих сконфигурированному пользователем фильтру, обеспечивая декодирование для заголовков протоколов IP, TCP, UDP, ICMP, HTTP, SSL/TLS, SIP и DNS. Пользователь должен иметь возможность скачать PCAP файл для его дальнейшего анализа.

3.7.18 Подсистема очистки должна поддерживать размещение в режиме SPAN или tap для дополнительного мониторинга трафика с целью предоставления следующих отчетов: Top DNS запросов, Top HTTP-запросов. Параметры качества обслуживания выбранного сервиса, основные типы HTTP-запросов, основные типы DNS-запросов.

3.8 Категории пользователей Системы

3.8.1 Должна быть реализована ролевая модель управления доступом.

3.8.2 В системе должны быть заложены следующие роли:

- **Операторы подсистемы мониторинга и выявления DoS/DDoS-атак.** Операторы подсистемы мониторинга и выявления DoS/DDoS-атакам используют систему для обнаружения DoS/DDoS-атак и противодействия им.

- **Администраторы Системы.** Администраторы системы обеспечивают работоспособность всех ее компонентов, ее подстройку под нужны операторов, а также управление пользователями.
- **Операторы подсистемы мониторинга трафика.** Операторы подсистемы мониторинга имеют возможность доступа к отчетам по трафику, но не имеют информации о DoS/DDoS-атаках.
- **Клиенты системы.** Клиенты системы имеют доступ к сформированным для них отчетам, информации об аномалиях в клиентских сетях, а также к методам очистки трафика в соответствии с установленным уровнем привилегий. Система должна позволять гибкую настройку пользовательского меню для указания возможностей индивидуального пользователя в системе.

3.9 Общие требования к масштабируемости и архитектуре

3.9.1 Система мониторинга и выявления DoS/DDoS-атак представляет собой программно-аппаратный комплекс, выполняющий сбор и анализ информации с маршрутизаторов магистральной сети. Целевая логическая схема системы представлена на Рис. 1.

3.9.2 Система должна являться законченным программно-аппаратным полнофункциональным решением по детектированию и устранению разнообразных сетевых атак отказа в обслуживании (DoS/DDoS).

3.9.3 Система должна быть реализована таким образом, чтобы не вносить дополнительную точку отказа в Сеть передачи данных и понижать ее отказоустойчивость.

3.9.4 Базы данных, используемые в системе, должны основываться на кластерном решении во избежание единой точки отказа.

3.9.5 При работе в режиме кластера, Система должна предоставлять возможность работы его компонент в следующих режимах:

3.9.6 - Active – Active;

3.9.7 - Active – Passive.

3.9.8 Система должна работать в режиме реального времени, обеспечивая обнаружение атак по поведенческим критериям, в том числе для обеспечения эффективного отражения ZeroDay-атак, для которых не существует соответствующих сигнатур.

3.9.9 Система должна быть наращиваемой, с возможностью масштабирования для обработки больших объемов трафика от разных источников по разным алгоритмам.

3.9.10 Наращивание мощности Системы должно производиться не посредством замены устройств, а путем масштабирования решения (компонентов Системы).

3.9.11 Уровень доступности (работоспособности) Системы должен быть не ниже 99,95%. Поставщик обеспечивает наличие компонентов Системы на складе ПАО МГТС, либо Поставщика для восстановления работоспособности Системы в течение 1-2 рабочих дней с даты открытия карточки неисправности.

3.9.12 Для исключения рисков при фатальном сбое в программно-аппаратном комплексе должно быть предусмотрено восстановление утраченных данных. Все важные данные (например, конфигурационные файлы Системы, персональные настройки Абонентов, база данных и т.п.) должны сохраняться на внешнем устройстве не реже одного раза в сутки.

3.9.13 Система должна иметь возможность создания выделенных зарезервированных в режиме hot standby подсистем управления.

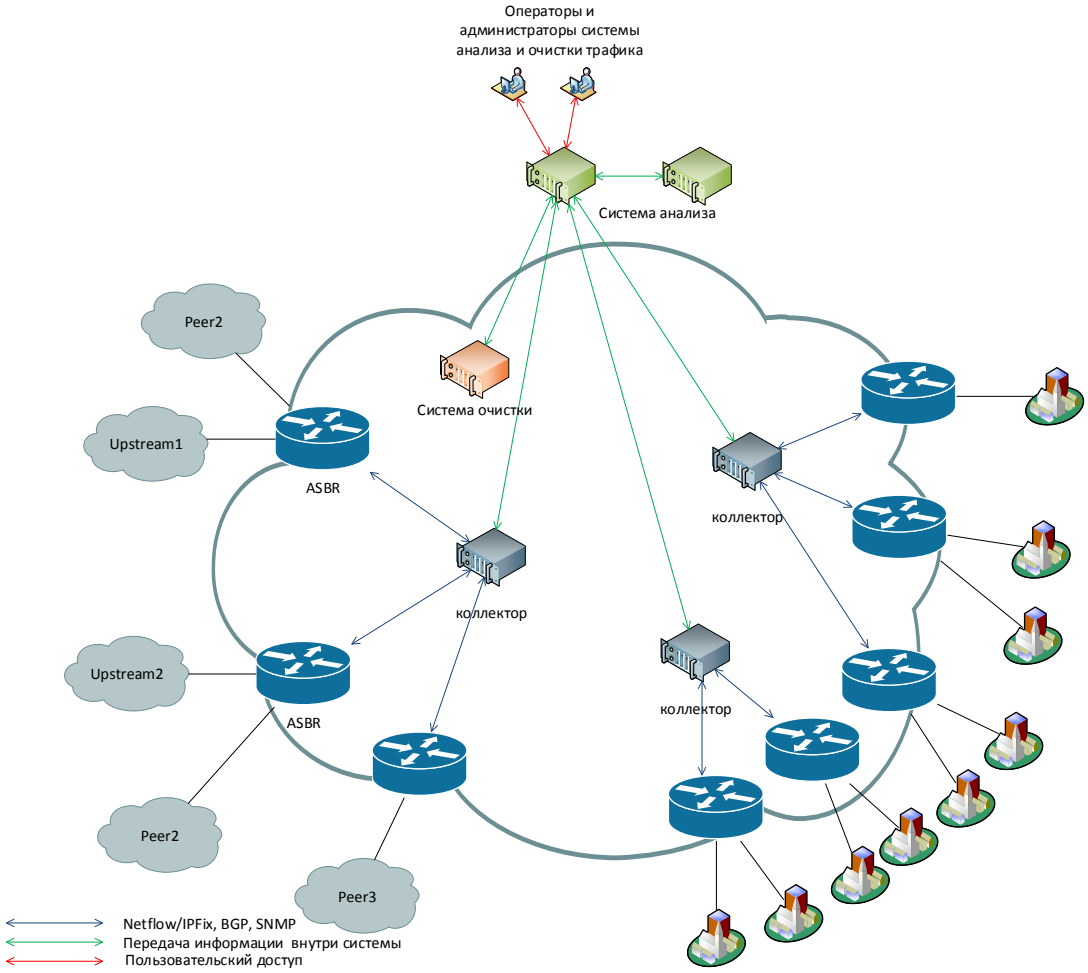

Рис. 1 — Логическая схема интеграции системы мониторинга и выявления DDoS-атак

Окончательная схема будет утверждена между МГТС и победителем закупочной процедуры

3.10 Требования к сетевым интерфейсам к масштабу и производительности Системы

3.10.1 Система размещается на географически распределенных площадках.

3.10.2 Время обнаружения атаки не должно превышать 300 секунд.

3.10.3 Решение должно предоставлять возможность одновременного анализа с помощью получения Flow не менее чем для 6 маршрутизаторов.

3.10.4 Решение должно иметь возможность последующего расширения до не менее 1000 маршрутизаторов.

3.10.5 Подсистема сбора данных должна обеспечивать производительность не менее 900 Gbps обрабатываемого (грязного) трафика с возможностью последующего расширения. Аппаратная платформа подсистемы должна поддерживать обработку не менее 300 Gbps трафика на шасси. Расширение должно осуществляться без замены используемой аппаратной платформы. Подсистема должна быть оснащена интерфейсами 10 или 100 Гбит Ethernet.

3.10.6 Подсистема очистки трафика должна обеспечивать производительность не менее 60 Gbps обрабатываемого (грязного) трафика при доле легитимного трафика от 0 до 100% с возможностью последующего расширения. Расширение должно осуществляться без замены используемой аппаратной платформы. Подсистема должна быть оснащена интерфейсами 100 Гбит Ethernet.

3.10.7 Все компоненты подсистем должны обеспечивать возможность агрегации интерфейсов Ethernet с использованием стандартных протоколов LAG.

3.10.8 Система должна иметь возможность одновременного доступа минимум 10 администраторов с возможностью увеличения до 50.

3.10.9 В процессе обнаружения атаки должна быть предусмотрена возможность одновременного запуска 1 000 заданий защиты от DDoS (blackholing, BGP FlowSpec, использования центра очистки).

3.10.10 Система должна отслеживать не менее 300 инцидентов.

3.10.11 Система должна хранить информацию о не менее 100 000 инцидентов.

3.10.12 Система не должна иметь единой точки отказа, приводящей к неспособности управления системой, анализа трафика или запуска задания на очистку.

3.10.13 После принудительной/неконтролируемой перезагрузки сетевых элементов системы восстановление полного функционирования комплекса должно происходить автоматически.

3.10.14 Система должна поддерживать механизмы удаленного восстановления после сбоев.

3.10.15 Система должна обеспечивать защиту от атак на всех уровнях модели OSI.

3.10.16 Система должна обеспечивать защиту от относительно низкоскоростных атак на уязвимости на уровне приложений (например, CC, SockStress, Connection Flood, HTTPS flood, SSL DDoS и т.п.)

3.10.17 В режиме размещения out of path (не в пути трафика) система должна обладать возможностью использовать расширение FlowSpec протокола BGP (в том числе в VRF) для высылки маршрутной информации для переключения трафика на установленный пользователем next-hop. Должна быть возможность установить таймаут информации, после которой информация будет отозвана. Должна быть возможность указать, какой именно трафик необходимо перенаправить с указанием IP источника и назначения, протокола, TCP/UDP портов, размеров пакета.

3.10.18 Система должна иметь возможность установки GRE-туннелей для возврата очищенного трафика.

3.10.19 Подавление атак должно включать в себя, как минимум, следующие варианты: управляемое из системы с помощью BGP перенаправление трафика на подсистему очистки, генерация FlowSpec маршрутной информации для блокирования определенного трафика на маршрутизаторах, генерация Source Remotely Triggered Black Hole (S/RTBH) маршрутной информации.

3.11 Требования к интерфейсам управления и внешним программным интерфейсам

3.11.1 Система должна обеспечивать мониторинг состояния компонентов из единого интерфейса управления.

3.11.2 Система должна иметь графический интерфейс (GUI) на базе Web, совместимого со стандартными браузерами типа Internet Explorer (не ниже 8 версии), Firefox/Mozilla, Safari, Google Chrome и т.д. (т.е. со всеми популярными браузерами, используемыми в России).

3.11.3 Web-интерфейс системы не должен требовать установки дополнительного ПО на клиентской стороне (например, JVM, ActiveX и т.п.)

3.11.4 Web-интерфейс должен обеспечивать работу в удаленном режиме для случаев экстренного подключения администраторов системы с мобильных устройств (iPhone/iPad/Android/Windows).

3.11.5 Система должна иметь интерфейс командной строки с доступом на основе стандартного протокола SSH v.2 (с ключом не короче 1024 bit). Интерфейс командной строки должен поддерживать весь набор функций, который доступен через графический интерфейс.

3.11.6 Система должна обеспечивать генерацию и отсылку по электронной почте сообщений, касающихся системных событий, возникновения инцидентов или других событий, связанных с предметной областью используемого решения.

3.11.7 Система должна обеспечивать генерацию уведомлений SNMP trap version 3 и сообщений syslog внешней системе мониторинга, касающихся системных событий, возникновения инцидентов или других событий, связанных с предметной областью.

3.11.8 Система должна обеспечивать мониторинг состояния агентов на основе xflow и SNMP для каждого устройства – источника соответствующей информации.

3.11.9 Система должна обладать возможностью генерации уведомлений SNMP при сбое и последующем восстановлении информационного потока xflow от маршрутизатора.

3.11.10 Система должна вести аудит всех изменений в конфигурации.

3.11.11 Система должна поддерживать транзакционную модель изменения конфигурации с возможностью записать комментарии для каждой транзакции, просмотреть изменения конфигурации в рамках каждой транзакции, а также произвести переход на нужную версию конфигурации. Должно поддерживаться не менее 1000 версий конфигурации.

3.11.12 Система должна поддерживать стандарты IPv4 и IPv6 как минимум для следующих задач:

- Для управления системой;
- Для сбора статистки по трафику;
- Для обнаружения DoS/DDoS-атак;
- Для отсылки маршрутной информации BGP;
- Для формирования задач по очистке трафика от DoS/DDoS-атак.

3.11.13 Система должна содержать контекстную документацию на английском и/или русском языках.

3.12 Требования к пользовательскому интерфейсу и интерфейсу создания отчетов

3.12.1 Система должна обеспечивать генерацию в реальном времени или в виде отчетов информацию об атаках, инцидентах и активности сетевого трафика.

3.12.2 Система должна иметь возможность настройки пользовательских групп для их привязки к объектам мониторинга. Пользователи группы не должны иметь доступ к информации и отчетами другой группы.

3.12.3 Администраторы пользовательской группы должны иметь возможность создавать аккаунты других пользователей в рамках выбранной группы.

3.12.4 Система должна обеспечивать возможность экспорта данных в форматах CSV, XML, PDF, Excel-XML;

3.12.5 Наличие API для организации взаимодействия и выгрузки отчетов во внешние системы (АСР, ЛК и др.).

3.12.6 API должен быть основан на стандартном протоколе (например, SOAP, HTTP или аналог), производитель должен предоставить полную документацию по API-вызовам.

3.12.7 API должен обеспечивать возможность создания новых пользователей системы с указанием их ролей.

3.12.8 API должен обеспечивать возможность создания новых объектов в системе с указанием специфичных параметров этих объектов (профили защиты от DDoS, входящие в объект IP-префиксы, BGP ASN, BGP community, интерфейсы).

3.12.9 API должен позволять осуществлять полное управление процессом выявления и противодействия DDoS-атакам, аналогичное пользовательскому интерфейсу: запуск Blackhole маршрутов, запуск правил фильтрации BGP FlowSpec, включение системы противодействия DDoS-атаке и настройка всех ее правил фильтрации.

3.12.10 API должен обеспечивать получение информации по работе системы, выполнению заданий по выявлению и противодействию DDoS-атакам и отчетам по трафику.

3.12.11 Система должна обеспечивать возможность пользователям системы просматривать весь происходящий в настоящий момент и предыдущий профиль трафика в рамках их областей и объектов управления.

3.12.12 Система должна иметь возможность настройки стартового экрана для каждого пользователя с вынесением на этот экран наиболее важной информации: отчетов по трафику, аварий, системных событий, атак и т.д. Содержимое данного экрана должно быть настраиваемым.

3.12.13 Система должна позволять создание пользовательских отчетов по трафику, системным событиям и аномалиям. Необходима возможность высылки данных отчетов по расписанию на указанные адреса по протоколу SMTP.

3.12.14 Система должна позволять организацию личных кабинетов (персональных порталов) для пользователей в целях возможности запуск услуг по анализу трафика и защиты от DDoS.

3.13 Требования к личному кабинету для пользователей

3.13.1 Система должна поддерживать не менее 1000 личных кабинетов.

3.13.2 Система должна позволять выбрать отчеты, доступные пользователю в его личном кабинете.

3.13.3 Система должна позволять выбирать методы очистки трафика, доступные пользователю в его личном кабинете.

3.13.4 Для методов выявления и противодействия DDoS-атакам, связанных с анонсом маршрутной информации пользователем, система должна позволять указать префиксы, принимаемые для анонса.

3.13.5 Система должна позволять настройку администраторов и пользователей личных кабинетов в рамках одного объекта.

3.13.6 Авторизация пользователей при доступе к личному кабинету должна проводиться с использованием внешней AAA-системы (RADIUS, TACACS+, LDAP).

3.13.7 Подсистема очистки должна обеспечивать детализированную статистику и графики для суммарного пропущенного/заблокированного трафика, количество заблокированных хостов, статистику по каждой контрмере, географическую информацию, распределение протоколов и топ заблокированных хостов.

3.13.8 Система должна поддерживать создание отчётов в форматах pdf и e-mail.

3.13.9 Подсистема должна поддерживать CLI-доступ через RS-232 консольный порт, SSH или telnet.

3.14 Требования к безопасности системы

3.14.1 Система должна обеспечивать контроль доступа пользователей на базе токенов пользователей или групп пользователей для обеспечения требуемых полномочий;

3.14.2 Система должна соответствовать требованиям информационной безопасности, изложенным в стандарте СТ-МГТС-027-3 «Требования информационной безопасности для новых информационных систем и приложений». Участник должен заполнить и предоставить «Опросный лист для контроля обеспечения ИБ при разработке и внедрении ИС» Приложение 5. СТ-МГТС-027-3.

3.15 Требования к принципам мониторинга трафика, обнаружения и классификации атак

3.15.1 Система должна обладать возможностью обнаружения отклонений в «нормальных»[1] профилях трафика, протоколов и на пакетном уровне от/к объектам контроля системы. «Нормальный» профиль трафика должен формироваться автоматически в процессе.

3.15.2 Система должна позволять определять объекты мониторинга в виде блоков адресов, параметров IP L4, включая номера протоколов, номера портов TCP/UDP, регулярных выражений, номеров AS, BGP community, интерфейсов маршрутизаторов.

3.15.3 Для каждого объекта мониторинга, а также для всей сети система должна автоматически генерировать отчеты по трафику в разрезе приложений, протоколов, стран-источников трафика, BGP-атрибутов, длин пакетов, ToS/DSCP-битов.

3.15.4 Система должна обеспечивать возможность анализа трафика хостов, генерирующих самое большое количество трафика в рамках данного объекта.

3.15.5 Система должна строить отчеты по матрице трафика с указанием объектов мониторинга.

3.15.6 Система должна строить отчеты по трафику BGP L3VPN, включая, но не ограничиваясь отчетами по приложениям и клиентским площадкам.

3.15.7 Система должна обладать возможностью классификации атак по уровню их влияния на сетевую инфраструктуру.

3.15.8 Система должна обладать возможностью установки уровней определения атак для объектов управления на основе характеристик трафика, протоколов и на пакетном уровне в диапазонах от высокой чувствительности до низкой чувствительности.

---

[1] **«Нормальный» профиль трафика** – характеристика загрузки оборудования/каналов доступа в/из сети Интернет в штатном режиме работы, определяемая посредством сбора согласованных статистических данных.

3.15.9 Система должна обеспечивать обнаружение известных в настоящее время способов и типов DoS/DDoS-атак, связанных с глобальной сетью Интернет путем отслеживания и выдачи сигналов предупреждения по критерию превышения «нормального» профиля трафика к определенным объектам мониторинга. Система должна обладать возможностью отображения степени влияния атаки в рамках интерфейсов объектов управления в терминах битовой и пакетной скорости.

3.15.10 При значительном отклонении трафика от нормы система должна производить информирование оператора не более чем за 30 секунд от начала отклонения.

3.15.11 Система должна отображать основные характеристики атаки в части доминирующих компонент. Характеристики должны включать IP адресный блок, IP протокол /порт, флаги TCP, IP адреса источника и получателя, BGP ASN, страны-источники трафика.

3.15.12 Система должна автоматически коррелировать между собой различные векторы атак на один ресурс.

3.15.13 Система должна обладать возможностью отображения подробностей об атаке в любой момент ее существования.

3.15.14 Система должна позволять оператору оставить комментарий по каждому инциденту, а также проклассифицировать его вручную.

3.15.15 Система должна обеспечивать возможность идентификации IP адресов посредством использования обратного разрешения DNS или WHOIS.

3.16 Требования к возможности предоставления сервиса на базе системы

3.16.1 Система должна позволять организовать дополнительные сервисы для клиентов.

4 Требования к гарантийной и послегарантийной поддержке оборудования

4.1.1 Для обеспечения необходимого уровня сервиса, Система должна быть обеспечена поддержкой производителя на обновления ПО сроком не менее 3 лет, включая русскоязычную первую линию технической поддержки, оказываемую производителем, либо его авторизированными партнером на территории Российской Федерации. Стоимость гарантийной технической поддержки входит в стоимость оборудования.

4.1.2 Участник должен иметь в штате не менее 2-х инженеров, сертифицированных по данному оборудованию.

4.1.3 Участник обеспечивает за свой счет необходимый ремонт оборудования на протяжении гарантийного срока.

4.1.4 Участник самостоятельно выполняет управление запасными частями к поставленному оборудованию.

4.1.5 Запросы, поступающие в техническую поддержку классифицируются по уровням в соответствии со следующими критериями:

- **Уровень Критичный** – какой-либо компонент Системы недоступен для управления или неработоспособен. Имеет место существенная деградация сервиса (затронуто более 500 абонентов), в т.ч. по причине DoS/DDoS-атаки.
- **Уровень Высокий** – снижение производительности какого-либо компонента Системы, ложное срабатывание системы мониторинга и/или системы очистки, снижение

эффективности защиты. Имеет место деградация сервиса (затронуто менее 500 абонентов), в т.ч. по причине DoS/DDoS-атаки.

- **Уровень Средний** – критичное обновление ПО Системы, внеплановое изменение конфигурации Системы, политик безопасности.
- **Уровень Низкий** – плановое обновление ПО Системы, плановые изменения конфигурации Системы.

4.1.6 Для запросов разного уровня должны обеспечиваться следующие требования по обслуживанию:

4.1.7 **Уровень Критичный** – время принятия инцидента в работу инженером службы технической поддержки 30 минут, в течение 6 часов с момента обращения должно быть предложено решение, позволяющее восстановить работоспособность системы. При необходимости, в течение не более 4 часов должно быть обеспечено присутствие инженера службы технической поддержки на территории Заказчика.

4.1.8 Замена вышедшего из строя оборудования должна производиться в течение одного рабочего дня.

4.1.9 Прием и регистрация запросов, обеспечение реакции на инциденты для данного уровня выполняются в режиме 24x7 (24 часа в день, 7 дней в неделю).

4.1.10 **Уровень Высокий –** время принятия инцидента в работу инженером службы технической поддержки 1 час, в течение суток с момента обращения должно быть предложено решение, позволяющее повысить эффективность защиты, исключить ложное срабатывание защитных механизмов и обеспечить доступность компонентов Системы с центральной консоли управления.

4.1.11 Замена вышедшего из строя оборудования должна производиться в течение двух рабочих дней.

4.1.12 Прием и регистрация запросов, обеспечение реакции на инциденты для данного уровня выполняются в режиме 24x7 (24 часа в день, 7 дней в неделю).

4.1.13 **Уровень Средний –** время принятия инцидента в работу инженером службы технической поддержки 2 часа, в течение суток с момента обращения должно быть предложено решение по формированию настроек обеспечивающих выполнение требования Заказчика, или при отсутствии технической возможности реализации, предложено альтернативное решение.

4.1.14 При необходимости обновления программного обеспечения, изменения конфигурации Системы, проводятся дополнительные испытания на лабораторном стенде авторизированного партнера, дублирующем конфигурацию Системы Заказчика.

4.1.15 Прием и регистрация запросов, обеспечение реакции на инциденты для данного уровня выполняются в режиме 8x5 (8 часов в день, 5 дней в неделю).

4.1.16 **Уровень Низкий –** время принятия инцидента в работу инженером службы технической поддержки 2 часа, в течение 2 суток с момента обращения должно быть предложено решение по формированию настроек, обеспечивающих выполнение требования заказчика. При необходимости изменения конфигурации Системы, проводятся необходимые испытания на лабораторном стенде авторизированного партнера, дублирующем конфигурацию Системы Заказчика.

4.1.17 Прием и регистрация запросов, обеспечение реакции на инциденты для данного уровня выполняются в режиме 8x5 (8 часов в день, 5 дней в неделю).

5 Общие требования к подготовке Предложения

5.1.1 Поставщик должен предоставить детальное описание аппаратно-программного комплекса.

5.1.2 Поставщик должен предоставить информацию о требованиях к электрическому питанию программно-аппаратного комплекса, площади размещения и системе кондиционирования.

5.1.3 Предложение должно содержать стоимость Решения и механизм ценообразования в зависимости от производительности.

5.1.4 Наличие ЗИП (spare устройств для оперативной замены вышедшего из строя оборудования) в поставке и их перечень.

5.1.5 Поставщик должен учесть в предложении возможность формирования статистики по различным параметрам и возможности выгрузки ее на внешнюю платформу.

5.1.6 Поставщик должен предоставить Roadmap развития всего оборудования и программного обеспечения на 5 лет.

5.1.7 Поставщик должен указать стоимость продления технической поддержки в течении последующих 3-х лет после окончания периода действующей технической поддержки.

5.1.8 Поставщик должен продолжать сопровождение и поддержку Решения, обеспечивая поставку оборудования для расширения, замены вышедшего из строя оборудования, версий программного обеспечения, расширения функциональности и технического сопровождения во время всего периода действующей технической поддержки.

5.1.9 Необходимо предоставить подтверждение, что предлагаемое решение внедрено и успешно эксплуатируется более года на сети связи хотя бы одного российского оператора связи на масштабах более 100 маршрутизаторов с использованием более 100 объектов мониторинга, поддержкой BGP FlowSpec и одновременным доступом не менее 10 пользователей.

5.1.10 Необходимо предоставить подтверждение, что подобная система внедрена и успешно эксплуатируется более года на сети связи двух зарубежных операторов связи на масштабах более 100 маршрутизаторов с использованием более 100 объектов мониторинга, поддержкой BGP FlowSpec и одновременным доступом не менее 10 пользователей.

5.1.11 Поставщик должен привести примеры успешных проектов по интеграции системы с сетевым оборудованием телекоммуникационных операторов. В сведениях необходимо указать вендора, название системы, версии HW и SW-систем, с которыми проводилась интеграция, а также указать дату проведения тестирования.

6 Требования к документации

6.1 Состав документации

6.1.1 Перечень оборудования и его производительность (спецификация Системы).

6.1.2 Техническое описание системы в составе:

- Общее описание системы;
- Техническая документация по эксплуатации платформы;
- Описание продукта с детальной документацией по устройству системы, её логическим модулям, подробное описание внутренних и внешних интерфейсов взаимодействия, правил настройки и администрирования модулей и интерфейсов;
- Документация по формированию и мониторингу аварийных/информационных сообщений;

- Описание методов сбора и анализа статистической информации;
- Схему интеграции оборудования в локальную/коммутационную сеть, схема комплекса технических средств (схема размещения оборудования);
- Схема взаимодействия внутренних компонентов системы (сетевая, электрическая, коммутационная и др.)

6.1.3 Методика расчета расширения Системы, включающая в себя:

- Описание принципов расширения и резервирования;
- Описание максимально возможной конфигурации Системы;
- Описание принципов увеличения производительности системы (программно и аппаратно);
- Описание максимально возможной аппаратной конфигурации предлагаемого оборудования с указанием производительности каждого модуля.

6.1.4 Описание конкурентных преимуществ Решения по отношению к аналогичным на рынке РФ.

6.1.5 Необходимо предоставить подтверждение опыта проведения сертификации оборудования по требованиям ФСТЭК и готовность в случае появления требований со стороны регулирующих органов организовать необходимую сертификацию.

6.1.6 Методики функционального и технического тестирования поставляемого Решения.

6.1.7 Во время приемки участники комиссии оставляют за собой право проводить любое дополнительное тестирование функциональности системы.

6.1.8 Программу проведения консультационного семинара по управлению и эксплуатации решения, а также его стоимость в зависимости от числа участников Семинар должен проводиться до момента начала приемочных испытаний.

6.1.9 Наличие программы и курсов для обучения и сертификации инженеров.

6.1.10 Описание решения должно быть предоставлено на русском языке.

6.1.11 Описание решение также должно подробно отображать:

- Логику предоставления сервисов (use-cases);
- Графический интерфейс администратора, пользователя услуги;
- Дополнительные возможности Решения, заявленные поставщиком/производителем.

6.1.12 Документы, подтверждающие права поставщика на поставляемое ПО.

6.1.13 Описание процесса оформление прав ПАО «МГТС» на передаваемое ПО.

7 Объем работ

7.1.1 Участник должен предоставить предложение по реализации системы «под ключ».

7.1.2 Участник разрабатывает и утверждает проект, включая низкоуровневый и высокоуровневый дизайн.

7.1.3 На этапе оценки и тестирования предлагаемого технического решения на соответствие ТТ, Участник инсталлирует компоненты Системы и предоставляет генератор трафика атак и легитимных приложений с производительностью и набором лицензий отвечающим ПМИ. Данная инсталляция может быть проведена как на площадке заказчика, так и на площадке Участника с обеспечением удаленного доступа к компонентам и тестовому оборудованию.

7.1.4 Проведение приемо-сдаточных испытаний (ПНР и ПМИ):

- на время проведения ПНР и ПМИ, а так же в рамках гарантийной поддержки для целей аудита и дополнительной настройки системы (при необходимости) требуется предоставление тестового генератора трафика атак и легитимных приложений;
- обучение персонала отдела управления оборудованием телематики и сетевой защиты новому оборудованию на базе учебного центра сертифицированными преподавателями. Место обучения – г.Москва.

7.1.5 На период начальной эксплуатации (12 месяцев со дня окончания ПНР) закрепить 1-го сервисного сотрудника от компании производителя оборудования для решения текущих вопросов и устранения неисправностей. Место размещения – Хачатуряна д.5. Время размещения – рабочие дни.

7.1.6 Предоставление гарантийной технической поддержки в режиме 24x7x365.

7.1.7 ПИР и СМР новых шкафов, включая ЭПУ и кондиционирование (при необходимости).

7.1.8 ПИР и СМР перекидных кабелей от существующих ОДФ (при необходимости).

7.1.9 Предоставить документы по совместимости с EMC Smarts. Предусмотреть работы по интеграции поставляемого оборудования с установленной системой EMC Smarts.

7.1.10 Оборудование должно иметь 19” форм фактор или поставляться со шкафами согласованного размера.

7.1.11 При поставке собственных шкафов, необходимо учитывать, что они:

- должны иметь возможность установки как на фальшпол, так и без него;
- должны иметь весовые характеристики с оборудованием до: 750 кг/кв.м. в помещениях без фальшпола, 1100 кг/кв.м. – в помещениях с фальшполом.

7.1.12 Установка дополнительных ЭПУ (при необходимости) проводится за счет и силами контрагента.

7.1.13 Закупка и установка всего дополнительного оборудования (линейные карты, SFP, etc) необходимого для подключения ПАК к оборудованию сети МГТС проводится за счет и силами контрагента. (В состав предложения должны быть включены модули интерфейсов для подключения к сети Заказчика, включая модули для установки в оборудование Заказчика в количестве, необходимом для обеспечения требуемой производительности).

7.1.14 В комплектацию ко всему оборудованию должны быть включены все необходимые для монтажа и организации связей комплектующие (в т.ч. винты/болты/гайки, направляющие, патчкорды, коммутационные панели, провода, автоматы, шины и пр).