Приложение

Передовые операционные практики и рекомендации

> В настоящее время у IETF нет механизма или средств для публикации соответствующей технической информации, одобренной IETF. Этот документ создает новую подсерию RFC под названием Best Current Practices (BCP).
>
> *RFC 1818[1], август 1995 г.*

Разработка новых протоколов, решений и технологий является необходимым условием полноценного развития Интернета. Однако их ценность и эффект появляются только в процессе внедрения и использования. И не просто использования, а использования их значительной частью операторов связи и услуг.

Существенным фактором, усложняющим процесс внедрения новых протоколов и технологий, является децентрализованный характер Интернета. Ведь для успешного внедрения необходимо, чтобы все участники, обеспечивающие передачу данных, добровольно согласились применить нововведение. Особенно остро эта проблема стоит перед протоколами и технологиями инфраструктуры в области адресации, системы имен DNS, маршрутизации. Проблема отягощается не только числом участников, которые должны договориться, но и отсутствием «бизнес-кейса» или его слабостью: преимущества от внедрения технологии на начальном этапе незначительной группой участников не соответствуют уровню затрат и рискам, связанным с внедрением. Например, какая польза от протокола IPv6, если по этому протоколу доступно только незначительное число ресурсов,

[1] RFC 1818: Best Current Practices, URL: https://www.rfc-editor.org/rfc/rfc1818

а при этом оператору, по сути, необходимо параллельно управлять двумя сетями (IPv4 и IPv6)?

В этом плане значительную ценность представляют так называемые передовые практики. Они позволяют существенно снизить затраты и избежать ошибок при внедрении и эксплуатации новых технологий.

DNS

В этом разделе мы кратко остановимся на практиках и рекомендациях по внедрению и эксплуатации системы DNS.

Руководство по развертыванию защищенной системы доменных имен (DNS), специальная публикация NIST 800-81-2[2]

Это руководство, разработанное Национальным институтом стандартов и технологий США, содержит рекомендации по защите DNS на предприятии. В документе представлены подробные рекомендации по поддержанию целостности данных и аутентификации источника, которые необходимы для обеспечения подлинности информации о доменных именах и поддержания целостности информации о доменных именах при передаче. Также в документе представлены рекомендации по настройке DNS для предотвращения атак типа «отказ в обслуживании» (Denial of Service, DoS), использующих уязвимости в различных компонентах DNS. Это наиболее часто используемый тип атак, направленный на нарушение доступа к ресурсам, доменные имена которых обрабатываются атакованными компонентами DNS.

Рекомендации по противодействию DDoS-атакам с использованием инфраструктуры DNS, SSAC065[3]

Эти рекомендации, разработанные консультативным комитетом ICANN по безопасности и стабильности (Security and Stability Advisory Committee, SSAC), предлагают комплексный подход к противодействию распределенным рефлекторным атакам отказа в обслуживании с усилением (reflection-amplification DDoS attacks). Поскольку создание таких атак использует уязвимые места многих систем, обслуживаемых различными операторами, эффективное решение требует коллективных действий. Так, например, для успешного запуска атаки используются сети, в которых отсутствует защита от спуфинга адресов источника, DNS-резолверы с открытым доступом, а также авторитетные DNS-серверы. Документ предлагает список конкретных действий, адресованный операторам этих компонентов общей системы.

---

2 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf

3 https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-065-en.pdf

Предотвращение использования рекурсивных резолверов для рефлекторных атак, RFC 5358[4]

Рекурсивные резолверы являются привлекательным объектом для запуска рефлекторных DDoS-атак с усилением. Действительно, резолверы используют протокол DNS, основанный на UDP, не требующем создания канала, а размеры ответов могут в десятки раз превышать размеры запросов. Документ содержит рекомендации для предотвращения такого использования. Общая рекомендация операторам серверов имен — использовать средства, поддерживаемые выбранной реализацией, для предоставления услуги рекурсивного поиска имен только предполагаемым клиентам. Другими словами, серверы имен не должны предлагать рекурсивное обслуживание внешних сетей. Для серверов имен, выполняющих роль авторитетных серверов, функции рекурсивного резолвера должны быть отключены.

Рекомендации для операторов DNS со службой конфиденциальности, RFC 8932[5]

Этот документ предлагает рекомендации для операторов DNS-резолверов, предоставляющих услуги конфиденциальности. Под услугами конфиденциальности подразумевается шифрование трафика между клиентом и резолвером с использованием протоколов DoT [RFC7858], «DNS over DTLS» [RFC8094] и DoH. Документ содержит рекомендации по хранению и обработке данных для операторов служб конфиденциальности DNS. Также в документе рассматривается ситуация, когда оператор такого резолвера, особенно в случаях, когда используется резолвер, внешний по отношению к сети пользователя, имеет доступ ко всей информации, которую защищают протоколы шифрования. Усугубляется это тем фактом, что в ряде случаев пользователь продолжает использовать этот же резолвер при перемещении в другую сеть, тем самым предоставляя возможность трассировки.

Для увеличения прозрачности и ответственности операторов таких услуг документ предлагает шаблон «заявления о конфиденциальности рекурсивного оператора (Recursive operator Privacy Statement, RPS)». RPS — это документ, который должен опубликовать оператор. В документе описываются методы работы оператора и обязательства в отношении конфиденциальности, что дает клиентам возможность оценить как измеримые, так и заявленные свойства конфиденциальности конкретной службы конфиденциальности DNS.

---

4 RFC 5358: Preventing Use of Recursive Nameservers in Reflector Attacks, URL: https://www.rfc-editor.org/rfc/rfc5358

5 RFC 8932: Recommendations for DNS Privacy Service Operators, URL: https://www.rfc-editor.org/rfc/rfc8932

Сетевая инфраструктура

В этом разделе мы кратко остановимся на практиках и рекомендациях по эксплуатации сетевой инфраструктуры и ее адресации. Особое внимание уделено практикам по развертыванию протокола IPv6.

Рекомендации по развертыванию протокола IPv6 в корпоративных сетях, RFC 7381[6]

Этот документ предлагает архитекторам и администраторам корпоративных сетей возможные стратегии и рекомендации по развертыванию протокола IPv6. Общая задача внедрения заключается в том, чтобы обеспечить услуги доступа в Интернет через IPv6 и поддержку этого протокола внутри корпоративной IT-сети, продолжая при этом поддерживать IPv4. В результате общего перехода большинство сетей перейдут из среды IPv4 в сетевую среду с двойным стеком и, в конечном итоге, в режим работы исключительно с IPv6. Документ рассматривает различные фазы развертывания и останавливается на таких аспектах, как адресация, маршрутизация, безопасность и мониторинг.

Рекомендации по предотвращению IP-спуфинга

Решение проблемы IP-спуфинга, когда IP-адреса отправителя пакетов подменяются на адрес вне сети отправителя (в случае намеренной рефлекторной атаки – обычно на адрес жертвы), было впервые предложено еще в 1998 году в RFC2267, который через два года был обновлен и получил категорию передовой практики BCP38[7]. Суть решения заключается в установке на граничных маршрутизаторах, к которым подключаются клиенты, «входных фильтров» (ingress filters). Эти фильтры разрешают только трафик, отправленный с исходных адресов блока клиента, и запрещают злоумышленнику использовать «недействительные» исходные адреса, находящиеся за пределами этого диапазона префиксов. Документ не содержит конкретных примеров конфигурации. Этот вопрос более детально рассматривается в документе «Входная фильтрация для сетей, использующих несколько провайдеров», RFC3704[8], также известном как передовая практика BCP84. В документе изложены пять различных способов реализации входных фильтров, начиная от статических листов доступа и заканчивая вариантами технологии переадресации обратного пути (точнее – Unicast Reverse Path Forwarding, uRPF). Применение технологий uRPF включает риски, связанные с возможной асимметрией трафика, например, когда клиент отправляет трафик через одного

---

6 RFC 7318: Enterprise IPv6 Deployment Guidelines,
URL: https://www.rfc-editor.org/rfc/rfc7318

7 BCP 38: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,
URL: https://www.rfc-editor.org/info/bcp38

8 RFC 3704: Ingress Filtering for Multihomed Networks,
URL: https://www.rfc-editor.org/rfc/rfc3704

провайдера, а предпочитает получать трафик через другого. BCP84 содержит рекомендации по применению конкретного варианта uRPF в зависимости от сетевой топологии. Примечательно, что фильтрация на основе статических листов доступа до сих пор считается наиболее надежной. Ее основным недостатком является плохая масштабируемость и необходимость дополнительной автоматизации построения фильтров.

Конкретные примеры использования описанных подходов в конфигурациях для различного сетевого оборудования приведены в «Практическом руководстве рабочей группы по борьбе со спуфингом», RIPE-431[9].

Более широкий спектр оборудования и соответствующие примеры конфигурации можно также найти в описании каждого участника программы MANRS для производителей сетевого оборудования[10].

Конфигурация префикса IPv6 для конечных пользователей, RIPE-690[11]

Этот документ описывает передовую практику при присвоении IPv6-префикса конечным пользователям. Под конечными пользователями подразумеваются как домашние сети, так и корпоративные. Как отмечается в документе, неправильный выбор при проектировании сети IPv6 рано или поздно приведет к негативным последствиям для развертывания и потребует дальнейших усилий, таких как изменение нумерации, когда сеть уже работает. В этом плане IPv6 существенно отличается от IPv4 и требует другого подхода при проектировании адресного плана. Документ, в частности, рекомендует минимальный размер префикса /48, позволяя /56 для домашних сетей.

Вопросы эксплуатационной безопасности сетей IPv6, RFC 9099[12]

В этом документе анализируются проблемы эксплуатационной безопасности, связанные с несколькими типами IPv6-сетей, и предлагаются технические и процедурные методы их решения. Как отмечается в документе, знания и опыт безопасной эксплуатации сетей IPv4 доступны независимо от того, является ли оператор интернет-провайдером (ISP) или внутренней сетью предприятия. Однако IPv6 создает некоторые новые проблемы безопасности. Данный документ рассчитан на сетевых администраторов, предлагая необходимые практические рекомендации, ориентированные на эксплуатацию,

---

9 RIPE Anti-Spoofing Task Force HOW-TO, https://www.ripe.net/publications/docs/ripe-43

10 https://www.manrs.org/equipment-vendors/participants/

11 Best Current Operational Practice for Operators: IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose, https://www.ripe.net/publications/docs/ripe-690

12 RFC 9099: Operational Security Considerations for IPv6 Networks, URL: https://www.rfc-editor.org/rfc/rfc9099

и анализируя преимущества и недостатки определенных вариантов решений. Документ охватывает широкий спектр вопросов – от адресации и маршрутизации, до использования переходных технологий, мониторинга и защищенности устройств. Отдельно выделены соображения безопасности для корпоративных и домашних сетей и сетей сервис-провайдера.

Требования по поддержке IPv6 в ИКТ-оборудовании, RIPE-772[13]

Для обеспечения плавного и экономически эффективного внедрения IPv6 в компьютерных сетях важно, чтобы крупные коммерческие, государственные или исследовательские и образовательные предприятия при составлении тендеров на оборудование и поддержку информационных и коммуникационных технологий (ИКТ) правильно формулировали требования к поддержке протокола IPv6. Основная проблема заключается в том, что функциональность IPv6 определена во множестве стандартов и технических спецификаций. Кроме того, для различных типов устройств определенная функциональность может быть как обязательной, так и дополнительной. Таким образом, точная формулировка требований требует знания конкретных стандартов/спецификаций и их применимости к конкретному типу оборудования.

Этот документ предлагает передовую практику для поддержки организаций в таких тендерных процессах. Документ также содержит рекомендации для разработчиков программного обеспечения и системных интеграторов.

Маршрутизация

В этом разделе мы кратко остановимся на практиках и рекомендациях по внедрению и эксплуатации системы междоменной маршрутизации с особым фокусом на безопасность.

Управление и безопасность BGP, BCP 194[14]

Этот документ является всесторонним обзором мер по защите BGP. В нем описаны меры по защите сеансов BGP, такие как время жизни (TTL), опция аутентификации TCP (TCP-AO) и фильтрация в плоскости управления. В нем также описываются меры по более строгому контролю маршрутной информации с использованием префиксной фильтрации и автоматизации префиксных фильтров (как с помощью IRR, так и системы RPKI), фильтрации по максимальным префиксам, фильтрации путей автономной системы (AS), подавления колебаний маршрутов и очистки сообществ BGP.

---

13 Requirements For IPv6 in ICT Equipment, https://www.ripe.net/publications/docs/ripe-772

14 BCP 194: BGP Operations and Security, URL: https://www.rfc-editor.org/info/bcp194

Требования к доверяющим сторонам инфраструктуры открытых ключей ресурсов (RPKI), RFC 8897[15]

Документ суммирует все требования к программному обеспечению пользователей, использующих инфраструктуру открытых ключей ресурсов (RPKI) для проверки аутентичности хранящейся в ней информации, т.н. доверяющие стороны. В документе приводятся требования, которые присутствуют в более чем десяти RFC, что облегчает разработчикам ознакомление с этими требованиями.

Требования разбиты на четыре группы:

- Извлечение и кеширование объектов репозитория RPKI.
- Обработка сертификатов и списков отзыва сертификатов (CRL).
- Обработка подписанных объектов репозитория RPKI.
- Распространение проверенного кеша данных RPKI.

Предполагается, что документ будет обновляться с учетом новых или измененных требований по мере обновления этих RFC или написания дополнительных RFC.

Требования к эксплуатационной безопасности для инфраструктуры IP-сети крупного интернет-провайдера (ISP), RFC 3871[16]

Этот документ определяет список эксплуатационных требований безопасности для инфраструктуры IP-сетей крупных интернет-провайдеров (ISP) - маршрутизаторов и коммутаторов. В документе используется подход, позволяющий определять «профили», которые представляют собой набор требований, применимых к определенным контекстам топологии сети (вся сеть, только ядро, только периферия...). Цель состоит в том, чтобы предоставить сетевым операторам четкий и краткий способ донести свои требования безопасности до поставщиков оборудования.

Практическое использование языка спецификации политик маршрутизации (RPSL), RFC 2650[17]

RPSL используется для описания политики маршрутизации интернет-провайдера и создания соответствующих объектов в реестре маршрутизации Интернета (IRR). Данный документ представляет собой руководство по использованию языка RPSL. В нем изложено, как указывать различные политики и конфигурации

---

15 RFC 8897: Requirements for Resource Public Key Infrastructure (RPKI) Relying Parties,
URL: https://www.rfc-editor.org/rfc/rfc8897

16 RFC 3871: Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure,
URL: https://www.rfc-editor.org/rfc/rfc3871

17 RFC 2650: Using RPSL in Practice,
URL: https://www.rfc-editor.org/rfc/rfc2650

маршрутизации с помощью RPSL, как регистрировать эти политики в IRR и как анализировать их с помощью инструментов анализа политик маршрутизации, например, для создания конфигураций маршрутизатора для конкретного типа оборудования.

Взаимосогласованные нормы безопасности маршрутизации, MANRS[18]

MANRS является глобальной инициативой, запущенной в 2014 году сетевыми операторами при поддержке Internet Society. Начавшись с программы для интернет-провайдеров, на сегодняшний день MANRS поддерживает отдельные программы для операторов точек обмена трафиком, операторов CDN и облачных услуг, а также производителей сетевого оборудования. По состоянию на конец 2023 года более тысячи операторов различных типов являлись участниками инициативы.

Для каждой категории операторов MANRS определяет набор требований (Actions), которым оператор должен удовлетворять для участия в инициативе. Так, например, сетевые операторы должны продемонстрировать выполнение следующих требований:

- Предотвращение передачи ложных анонсов. Интернет-провайдер должен обеспечить фильтрацию анонсов от своих клиентов и собственных сетей для избежания атак захвата или утечки маршрута.
- Противодействие IP-спуфингу. Системы провайдера должны использовать соответствующие фильтры, блокирующие трафик клиентов с подменой адреса отправителя.
- Поддержка коммуникации и координации в глобальном масштабе. Поскольку реакция на атаки и операционная координация являются необходимыми факторами эффективного противодействия, данное требование устанавливает публичную доступность контактной информации оператора.
- Поддержка маршрутной информации в глобальном масштабе. Это требование предусматривает поддержку актуальной информации о маршрутах провайдера в соответствующих регистратурах – IRR и RPKI.

Необходимо отметить, что инициатива MANRS не определяет новых требований или практик. Она базируется на существующих подходах решения проблем и фокусируется на конечном результате.

[18] Mutually Agreed Norms for Routing Security (MANRS), https://www.manrs.org