Ушаков И. А.
Беккель Л. С.
Красов А. В.

Построение защищенных компьютерных сетей в мультивендорной инфраструктуре

Учебное пособие

СПб ГУТ)))

Министерство цифрового развития, связи и массовых коммуникаций
Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования «Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М. А. Бонч-Бруевича»
(СПбГУТ)

И. А. Ушаков, Л. С. Беккель, А. В. Красов

ПОСТРОЕНИЕ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ В МУЛЬТИВЕНДОРНОЙ ИНФРАСТРУКТУРЕ

Учебное пособие

Электронное издание
локального распространения

Санкт-Петербург
Наукоемкие технологии
2026

© Ушаков И. А., Беккель Л. С., Красов А. В., 2026
© Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2026
ISBN 978-5-00271-170-3

УДК 004.056.5(075.8)
ББК 16.8я73
У93

Рецензенты:
А. А. Миняев, кандидат технических наук, руководитель
ЦИБ ООО «ДИДЖИТАЛ ДИЗАЙН ИТ»;
В. Е. Сокол, руководитель структурного подразделения,
ООО "Предприятие "ЭЛТЕКС", руководитель учебного центра,
ООО "Ин-софт", преподаватель ФГБОУ ВО «Новосибирский государственный технический университет» (НГТУ)

У93 **Ушаков, И. А.**
Построение защищенных компьютерных сетей в мультивендорной инфраструктуре [Электронный ресурс]: учебное пособие / И. А. Ушаков, Л. С. Беккель, А. В. Красов; СПбГУТ. – Электрон, текстовые дан. (3,4 Мб). – СПб.: Наукоемкие технологии, 2026. – 91 с. – 1 электрон., опт. диск (CD-ROM).

ISBN 978-5-00271-170-3

В данном учебном пособии рассматриваются принципы построения защищенных компьютерных сетей на примере отечественного оборудования ООО «Предприятие «ЭЛТЕКС». В частности, в пособии рассматриваются вопросы противодействия компьютерным атакам, приводятся примеры настройки оборудования.

Предназначено для подготовки бакалавров по направлению подготовки 10.03.01 «Информационная безопасность», специалистов по специальностям 10.05.02 «Информационная безопасность телекоммуникационных систем» и 10.05.07 «Противодействие техническим разведкам», магистров по направлению: 11.04.02 «Инфокоммуникационные технологии и системы связи», профиль «Защищенные системы и сети связи».

Текстовое электронное издание

Минимальные системные требования:

- процессор: Intel x86, x64, AMD x86, x64 не менее 1 ГГц;
- оперативная память RAM ОЗУ: не менее 512 МБайт;
- свободное место на жестком диске (HDD): не менее 120 МБайт;
- операционная система: Windows XP и выше;
- Adobe Acrobat Reader;
- дисковод CD-ROM;
- мышь.

УДК 004.056.5(075.8)
ББК 16.8я73

© Ушаков И. А., Беккель Л. С., Красов А. В., 2026
© Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2026

ISBN 978-5-00271-170-3

Учебное издание

Ушаков Игорь Александрович
Беккель Людмила Сергеевна
Красов Андрей Владимирович

Построение защищенных компьютерных сетей в мультивендорной инфраструктуре

Учебное пособие

Электронное издание
локального распространения

Издается в авторской редакции
Публикуется из оригинал-макета, подготовленного авторами

Издательство «Наукоемкие технологии»
ООО «Корпорация «Интел Групп»
https://publishing.intelgr.com
E-mail: publishing@intelgr.com
Тел.: +7 (812) 945-50-63
Интернет-магазин издательства
https://shop.intelgr.com/

Подписано к использованию 19.08.2026 г.
Объем издания – 3,4 Мб.
Комплектация издания – 1 CD.
Тираж 100 CD.

ISBN 978-5-00271-170-3



ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 6

1. ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ 8

1.1. Текущее состояние информационной безопасности (ИБ) в России 8

1.2. Основные категории инцидентов безопасности компьютерных сетей 9

1.3. DoS/DDoS-атаки 10

1.3.1. Основная идея DoS/DDoS-атак 10

1.3.2. Разновидности DoS/DDoS-атак и способы противодействия им 11

1.4. Сканирование сети: реализация и механизмы противодействия 19

1.4.1. Общая характеристика сетевого сканирования 19

1.4.2. Поиск активных устройств 19

1.4.3. Сканирование портов 19

1.4.4. Определение операционных систем 21

1.5. Атаки в локальной сети 22

1.5.1. ARP-poisoning 22

1.5.2. DHCP-spoofing и DHCP-starvation 24

2. МЕТОДЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИБ В КОМПЬЮТЕРНЫХ СЕТЯХ: БЕЗОПАСНОСТЬ КОММУТАТОРОВ 28

2.1. Сущность сетевой безопасности коммутаторов 28

2.2. Механизмы защиты от атак в локальных сетях 28

2.2.1. Port Security 28

2.2.2. DHCP Snooping 30

2.2.3. ARP Inspection 32

2.2.4. IP Source Guard 33

2.2.5. Защита от петель 33

2.2.6. Защита от шторма 34

2.2.7 Защита от атак с использованием VLAN 35

3. ПРОТОКОЛЫ AAA 39

3.1. Принципы AAA 39

3.2. Протокол RADIUS 41

3.3. Протокол TACACS+ 44

3.4. Аутентификация по стандарту IEEE 802.1x 47

3.5. MAC Authentication Bypass 50

4. МЕЖСЕТЕВОЙ ЭКРАН НА ОСНОВЕ ЗОН 53
4.1. Межсетевые экраны 53
4.1.1 Принципы работы Firewall 53
4.1.2. Поколения и типы МСЭ 54
4.2. Способы применения межсетевых экранов в архитектуре сети 57
5. ПРОТОКОЛ IPSEC И ПОСТРОЕНИЕ VPN ТУННЕЛЕЙ 61
5.1. Способы организации изолированных каналов связи 61
5.2. Стек протоколов IPsec 62
5.2.1. Структура стека протоколов IPsec 62
5.2.2. Режимы работы IPsec. IPsec VPN 66
6. ТЕХНОЛОГИЯ DMVPN 70
6.1 Предпосылки к появлению DMVPN 70
6.2. Принципы работы DMVPN и его составляющих 71
6.3. Отказоустойчивые топологии в DMVPN 76
7. СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ IPS 81
7.1 Атаки нулевого дня 81
7.2. Intrusion Prevention Systems (IPS) 81
7.2.1. Технология и формы ее реализации 81
7.2.2. Принципы функционирования и варианты применения в топологии сети 83
7.2.3. Сигнатуры 85
7.3. NGFW 86
ЗАКЛЮЧЕНИЕ 90
СПИСОК ЛИТЕРАТУРЫ 91

ВВЕДЕНИЕ

Целью данного пособия является подготовка специалистов в области безопасности компьютерных сетей на базе отечественного оборудования ООО «Предприятие «ЭЛТЕКС».

Современный мир невозможно представить без компьютерных сетей, которые играют ключевую роль в обеспечении передачи данных, организации коммуникаций и автоматизации процессов во всех сферах человеческой деятельности. Однако, наряду с ростом значимости сетевых технологий, увеличиваются и риски, связанные с их безопасностью. Кибератаки, утечки конфиденциальной информации, несанкционированный доступ и иные угрозы безопасности становятся серьезной проблемой для компаний и государственных учреждений. Реализация злонамеренной деятельности злоумышленников приводит к возникновению экономических проблем у хозяйственных предприятий страны. Утечки конфиденциальных данных приводят к репутационным потерям компаний и государственных организаций. Потеря секретной информации учреждений Министерства обороны может привести к потере обороноспособности страны. В связи с этим вопросы обеспечения безопасности компьютерных сетей приобретают первостепенное значение.

Важность данной отрасли обуславливается ее влиянием на экономическую, социальную и национальную безопасность. Успешное противодействие угрозам невозможно без подготовки квалифицированных специалистов, обладающих глубокими знаниями и навыками в области безопасности сетей, способных выявлять и предотвращать угрозы. Однако, подготовка таких специалистов требует наличия эффективных методик обучения и современных средств для проведения практических занятий, что особенно актуально в условиях стремительной информатизации общества.

Актуальность данного пособия подтверждается внутриполитическим курсом Российской Федерации на импортозамещение в области информационных технологий, в том числе необходимость разработки вызвана потребностью отказа от использования иностранных решений в области сетевых технологий, таких как продукция компании Cisco Systems Inc. Эта компания на протяжении многих лет является признанным мировым лидером в разработке сетевого оборудования и образовательных программ, включая курсы CCNAS (Cisco Certified Network Associate Security) и CyberOps (Cybersecurity Operations). С 3 марта 2022 года Cisco отключила доступ к своей сетевой академии для студентов и инструкторов из РФ, а 4 марта приостановила все бизнес-операции в России. В текущих условиях образовательные учреждения и предприятия сталкиваются с отсутствием широко распространенных российских программных и виртуальных решений, аналогичных по функциональности и доступности. Это создает серьезные

вызовы для подготовки специалистов в области безопасности компьютерных сетей.

Данное учебное пособие, разработанное на основе отечественного виртуального оборудования и свободно распространяемых дистрибутивов UNIX-систем, предназначено способствовать укреплению образовательной и технологической независимости страны, а также повышению квалификации выпускающихся специалистов в области информационной безопасности.

1. ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

1.1. Текущее состояние информационной безопасности (ИБ) в России

Настоящее время характеризуется стремительным ростом информатизации, которая охватывает все сферы жизни общества. В России этот процесс особенно заметен: цифровые технологии активно внедряются в государственное управление, экономику, здравоохранение, образование и повседневную жизнь граждан. Повсеместная интеграция цифровых решений влияет на множество различных процессов, таких как: финансовые операции, повышение эффективности телекоммуникаций и связи, рост качества и быстроту оказываемых услуг – от покупок в интернет-магазинах до получения справок в онлайн-сервисах государственных услуг. Тем не менее, вместе с этим растут и риски, связанные с использованием информационных технологий в незаконных корыстных целях. Злоумышленники, используя уязвимости в информационных системах, получают возможность похищать конфиденциальные данные, нарушать работу критически важных объектов и влиять на общественные процессы. Также стоит отметить рост мошенничества, где информационные системы и сети передачи данных являются средством распространения фишинговых сообщений, нацеленных на неосведомленное в области информационной безопасности население. В условиях обостренной внешнеполитической ситуации кибератаки используются как инструмент в руках спецслужб недружественных стран и хакерских группировок.

В период с 2022 года по настоящее время количество высококвалифицированных атак кратно увеличилось. На рис. 1 представлено распределение успешных кибератак на российские организации в 2020-2024 годах, составленное аналитиками Positive Technologies.

Так, целью группировки Core Werewolf являются российские организации военно-промышленного комплекса, объекты критической информационной инфраструктуры. Злоумышленники рассылают фишинговые письма с вредоносными вложениями, маскирующимися под различные документы: приказы, резюме, методические указания, даже под официальные документы регуляторов. К примеру, в конце 2023 года во время расследования инцидента команда экспертного центра безопасности Positive Technologies обнаружила письмо с фишингового домена fstec[.]support якобы от имени ФСТЭК России. В качестве вложения к письмам прилагался самораспаковывающийся архив с клиентом ПО для удаленного доступа.

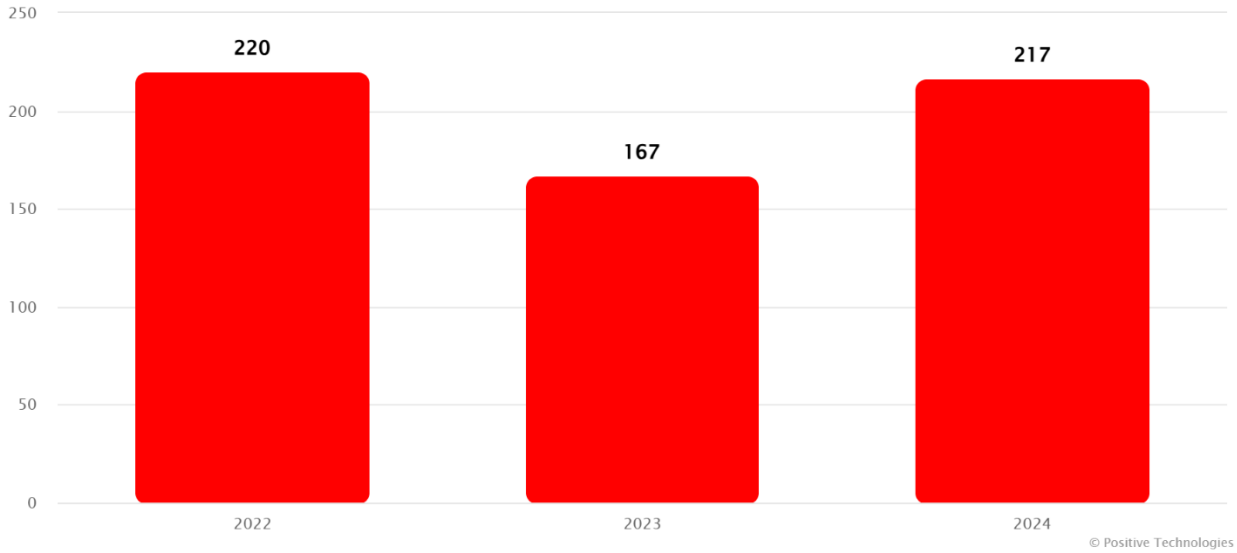


Рис. 1. Распределение успешных кибератак на российские организации (Positive Technologies, 2020-2024 гг.)

1.2. Основные категории инцидентов безопасности компьютерных сетей

Использование вредоносного программного обеспечения (майнеры криптовалют, шифровальщики, шпионское ПО, нелегитимные средства удаленного управления) на текущий момент является одним из основных методов компьютерных атак, но до целевой системы его нужно доставить. Безусловно, самым популярным способом доставки вирусного программного обеспечения являются сети передачи данных. Активность ВПО в сетевом трафике – это не единственная категория инцидентов в компьютерных сетях.

В отдельную категорию инцидентов в рамках сетевой безопасности можно выделить подозрительную активность – попытки несанкционированного доступа в виде подбора паролей (Brute Force атаки), подключение по нестандартным портам, сканирование сети, а также попытки запуска средств удаленного управления. Данный тип инцидентов нельзя однозначно интерпретировать как действия злоумышленника. К примеру, процесс сканирования сети может быть инициирован сканером уязвимостей, поэтому в случае возникновения событий безопасности данного типа следует тщательно рассматривать каждый случай.

Но угрозы не всегда исходят только со стороны внешних нарушителей. Очень часто действиям злоумышленника непреднамеренно содействуют сотрудники организации, нарушая регламенты информационной безопасности, в частности политики ИБ (как ключевой нормативный элемент защиты информации), содержащие регламентацию использования информационных ресурсов, протоколов, требования к аутентификации и другие организационные меры информационной безопасности. Наиболее распространенные инциденты этой категории связаны с использованием:

- незащищенных протоколов передачи данных (HTTP, LDAP, Telnet, FTP, протоколы электронной почты);
- бесконтрольным применением ПО для удаленного доступа (TeamViewer, AnyDesk);
- использованием слабых паролей и паролей по умолчанию, часто встречающихся в различных словарях, что упрощает выполнение атаки методом перебора пароля.

При таких ситуациях нападающий имеет большие шансы проникнуть в систему организации по сети.

В рамках обзора типичных инцидентов сетевой безопасности стоит отдельно упомянуть атаки типа «Отказ в обслуживании» (DoS/DDoS). Они направлены на перегрузку целевых сетей или сервисов для исчерпания критических ресурсов, поддерживающих работоспособность и доступность для легитимных пользователей (память, пропускная способность сети, процессорное время). Данный тип неправомерного воздействия имеет ряд преимуществ по сравнению с другими видами кибератак:

- простота реализации: провести такую атаку способен злоумышленник с низким уровнем возможностей без глубоких технических знаний благодаря готовым скриптам и инструментам;
- высокая эффективность: DoS-атаки способны быстро парализовать работу сети, сервера или веб-сайта при отсутствии должного уровня защищенности;
- низкая стоимость: для успешной атаки достаточно одного компьютера с качественным интернет-соединением (в условиях масштабной реализации существует возможность арендовать ботнеты).

Так, например, 20 июня 2024 года группа хакеров совершила DDoS-атаку на Национальную систему платежных карт (НСПК), прервав тем самым платежи по картам и систему быстрых платежей (СБП) на несколько часов.

1.3. DoS/DDoS-атаки

1.3.1. Основная идея DoS/DDoS-атак

Рассмотрение основных типов атак на компьютерные сети начнем с самого доступного, технически простого и распространенного вида – атаки типа «Отказ в обслуживании» или DoS (Denial of Service). Данная разновидность кибератак направлена на нарушение штатного функционирования информационных систем и сетей путем чрезмерного потребления ресурсов, перегрузки узлов некорректно сформированными пакетами и эксплуатации уязвимостей в работе сетевых протоколов, чтобы сделать информационную инфраструктуру недоступной для легитимных пользователей. Классическая

DoS-атака подразумевает использование одного устройства для осуществления воздействия на жертву. Но такой метод быстро показал свою неэффективность – от него легко защититься с помощью межсетевых экранов, заблокировав IP-адрес злоумышленника. Поэтому для увеличения эффективности применяют тактику нападения с нескольких устройств одновременно – Distributed Denial of Service. От количества атакующих устройств и объема отправляемого трафика зависит мощность нападения. Сеть зараженных устройств под управлением злоумышленника называется ботнет (рис. 2).

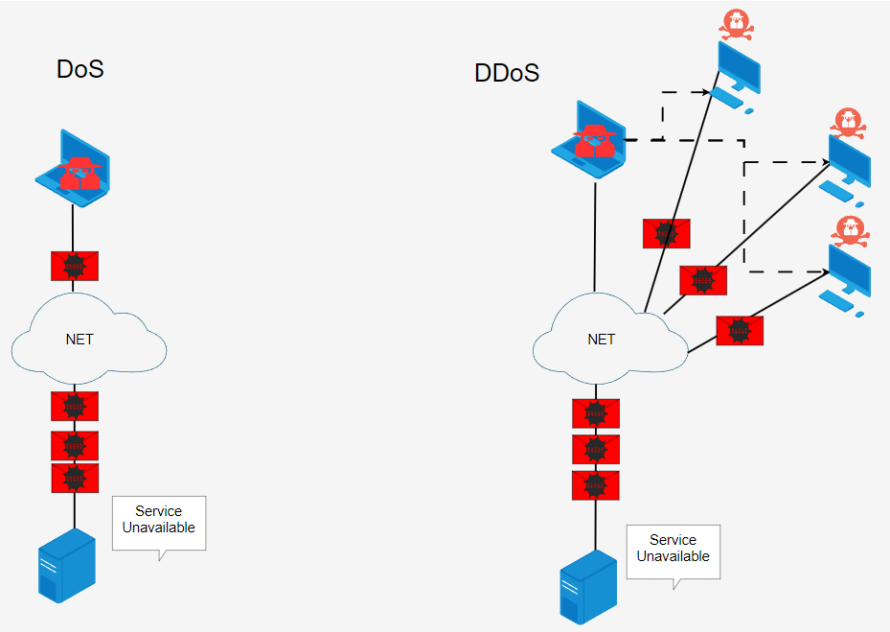


Рис. 2. DoS и DDoS атаки

Ключевой замысел любой кибератаки – нанести репутационный или финансовый ущерб. DoS-атаки не исключение: нападение с целью шантажа, мести, ради громкого инфоповода или как средство политической борьбы. Жертвой может быть как одиночный компьютер, так и корпоративная сеть. При этом, несмотря на примитивность атаки, последствия могут быть достаточно серьезными: при достаточных возможностях злоумышленника организовать многотысячный ботнет, не каждая инфраструктура способна противостоять такой атаке. Особо опасны DDoS-атаки на веб-ресурсы: ведь, если сайт больше двух суток окажется недоступен, то его ранжирование в поисковых системах будет снижено, что может сказаться на финансовом положении владельца.

1.3.2. Разновидности DoS/DDoS-атак и способы противодействия им

Большинство атак основаны на отправке большого числа пакетов за небольшое время, так называемый flood. При этом отдельные виды DoS-атак также включают в себя нарушение ожидаемого поведения протоколов,

подмену IP-адресов источника, использование пакетов большого объема или ошибки фрагментации пакетов для увеличения эффективности. Рассмотрим распространенные атаки в зависимости от уровня модели OSI, на котором они работают.

На третьем уровне (сетевом) для совершения DoS-атак часто используется протокол ICMP (Internet Control Message Protocol). Это служебный протокол, использующийся для обмена сообщениями об ошибках, возникающих при передаче данных, между узлами сети. Существуют две версии протокола - ICMPv4 для IPv4 и ICMPv6 для IPv6 соответственно. Протокол ICMP использует множество типов служебных сообщений, например, таких как:

- 0 – echo reply – ответ на echo request, применяется для проверки доступности узла.
- 3 – destination unreachable – недоступность целевого адреса.
- 8 – echo request – запрос echo reply, применяется для проверки доступности узла.
- 11 – time exceeded – истечение времени жизни пакета (TTL=0).

Классический ICMP-flood представляет собой огромное количество echo request-сообщений на целевой адрес жертвы, которая вынуждена тратить ресурсы на обработку и ответы echo reply. Атака очень проста в реализации, но требует больших объемов трафика для эффективности. Существуют различные модификации данной атаки, например:

- Ping of death: использование пакетов большего размера, чем предельно допустимые 65536 байт;
- Smurf attack: подмена адреса источника в ICMP echo request пакетах на IP-адрес жертвы с последующей рассылкой запроса по широковещательному адресу сети, в результате чего все узлы в сети отправляют echo reply на целевой адрес (рис. 3);
- Blacknurse attack: отправка на адрес межсетевого экрана (МСЭ) ICMP type 3 code 3 (Destination unreachable) вызывает выход из строя МСЭ из-за неэффективности обработки пакетов этого типа.

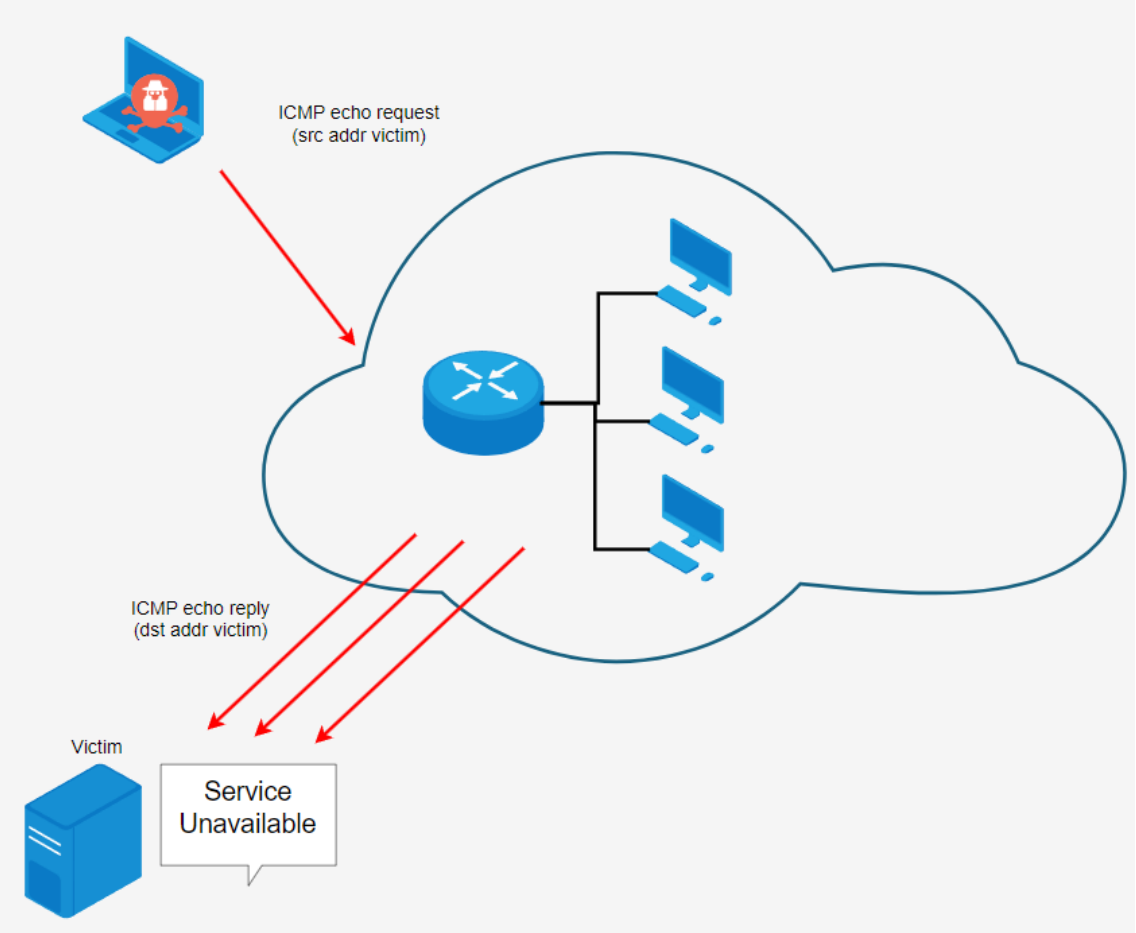


Рис. 3. Smurf-атака

Несмотря на очевидную возможность применения ICMP при атаках, полная блокировка протокола может привести к проблемам в работе сети. Конечно, в современных устройствах существуют механизмы защиты от такого рода атак – ограничение числа пакетов в секунду, блокировка отдельных типов ICMP-сообщений и подозрительно больших пакетов, однако, некорректные настройки, экономия на средствах защиты и низкая квалификация специалистов может сыграть в пользу злоумышленника даже в таких примитивных нападениях.

На транспортном уровне функционируют протоколы TCP и UDP. Разберем особенности и механизм передачи данных каждого протокола в отдельности, после чего рассмотрим их применение в DoS-атаках.

Transmission Control Protocol (TCP) – протокол управления передачей, обеспечивает гарантированную доставку пакетов с помощью механизма предварительного установления соединения – трехстороннего квитирования (three-way handshake). Структура TCP-сегмента представлена на рис. 4.

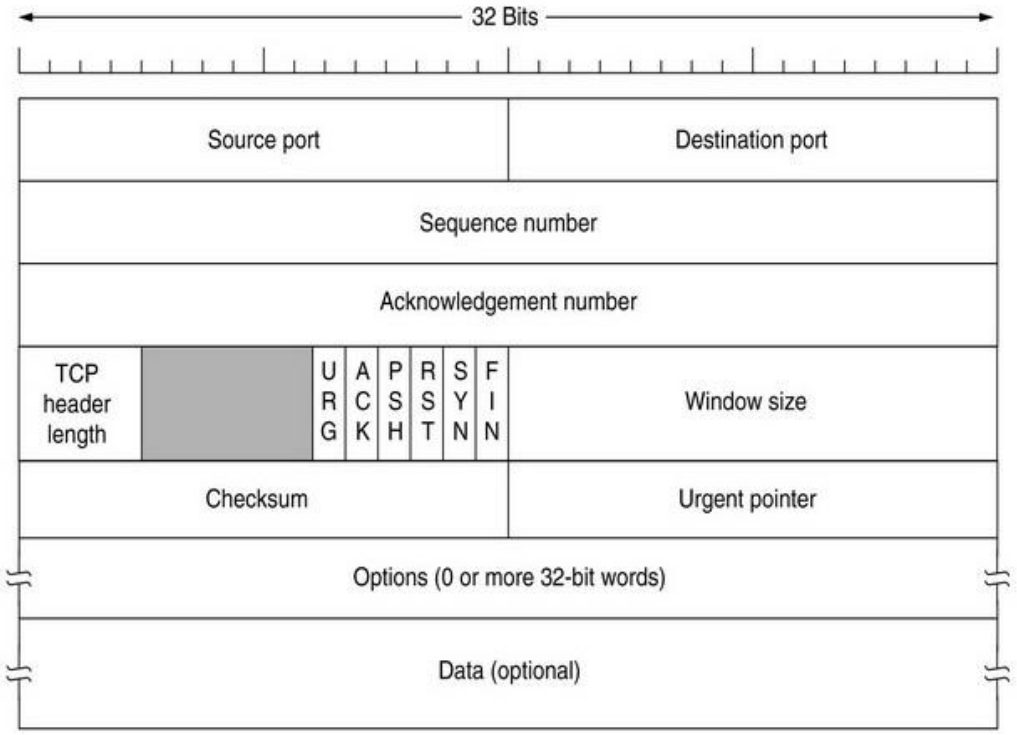


Рис. 4. TCP-сегмент

Остановимся подробнее на управляющих флагах протокола – битовые поля в заголовке сегмента, каждое из которых отвечает за определенную функцию:

- URG (Urgent Pointer) – пометка «срочных» данных для немедленной обработки вне очереди.
- ACK (Acknowledgment) – подтверждение получения сегментов данных, после установления соединения все сегменты, кроме первого, должны иметь его установленным.
- PSH (Push) – доставка данных без буферизации.
- SYN (Synchronize) – инициализация соединения, установлен в первом сегменте трехстороннего квитирования.
- FIN (No more data from Sender) – завершение соединения.
- RST (Reset Connection) – принудительное закрытие соединения или отказ от его установления, например, может быть ответом на попытку подключения к закрытому порту.

DoS-атаки эксплуатируют особенности управления TCP-сессией с помощью приведенных выше флагов. Изучим реализацию наиболее распространенных:

1. SYN-flood – отправка большого числа TCP-сегментов с флагом SYN к целевой системе и игнорирование ее ответов. На каждый SYN-запрос злоумышленника сервер отвечает ACK+SYN и ждет ACK от клиента, которое, соответственно, не поступает и

соединения остаются в полуоткрытом состоянии (half-open). Большое количество незавершенных соединений приводит к отказу в обслуживании легитимных пользователей. На рис. 5 представлен штатный алгоритм обмена сегментами при установлении TCP-сессии в сравнении с процессом атаки.

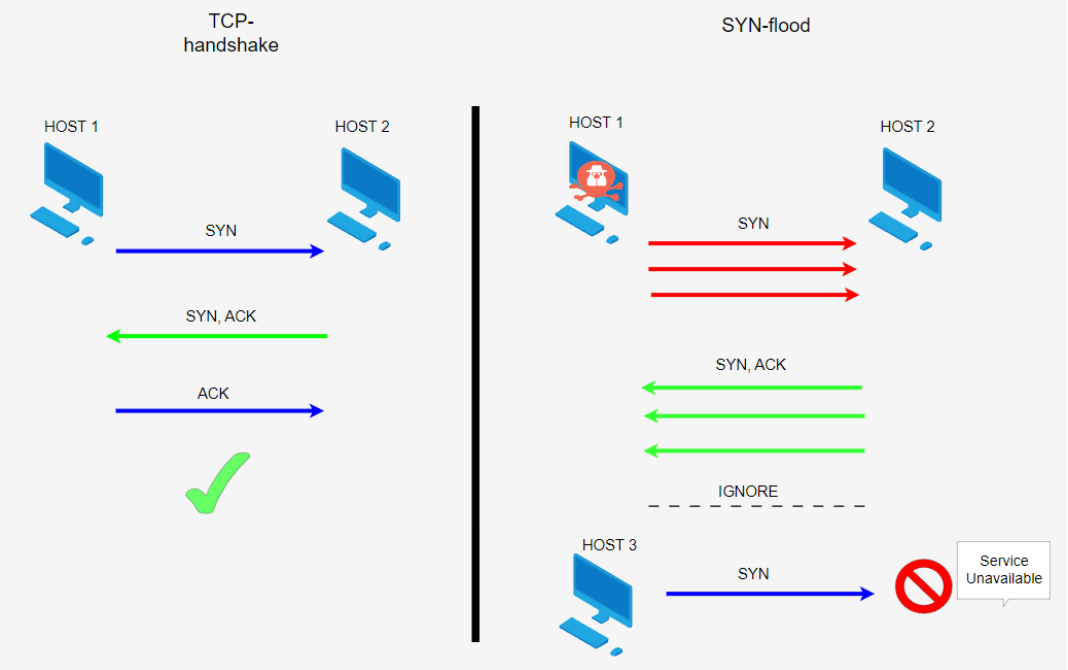


Рис. 5. SYN-flood атака

2. RST attack – отправка TCP-сегментов с флагом RST к одной или обеим сторонам соединения для несанкционированного завершения сессии. Злоумышленник анализирует трафик для поиска активных TCP-соединений и отправляет пакет с IP-адресом одной из сторон установленной сессии и флагом RST; получатель определяет пакет как легитимный и закрывает сессию.
3. Connection Exhaustion – атака основана на создании большого количества одновременных TCP-соединений, которые остаются активными максимально долго. Сервер больше не может принимать новые подключения, так как ресурсы заняты «застывшими» соединениями. Для реализации этого вида атаки необходимо большое количество IP-адресов, потому что каждое вредоносное соединение проходит стандартное квитирование TCP, при этом нет необходимости отправлять большие наборы данных для поддержания сессий открытыми.
4. Push flood – отправка большого числа сегментов с флагом PUSH. При наличии данного флага данные доставляются к получателю без буферизации. Содержимое сегмента может быть минимальным или вовсе отсутствовать, при этом обработка

таких сегментов потребляет ресурсы на проверку контрольной суммы, обработку флага и передачу данных приложению получателя.

Эффективно противостоять DoS-атакам возможно при грамотной настройке правил межсетевого экрана, оптимизации сетевых подключений и балансировке трафика, а также регулярном мониторинге. Установка максимального количества обрабатываемых SYN-запросов, ограничение числа одновременных соединений, сокращение времени ожидания неактивных соединений, фильтрация подозрительных пакетов (с неправильными номерами последовательности, без полезной нагрузки, с некорректно установленными флагами) позволят, если не полностью защититься от всех видов TCP-атак, то своевременно обнаружить и среагировать на инцидент.

User Datagram Protocol (UDP) – транспортный протокол, предоставляющий ненадежную передачу данных без установления соединения. Это позволяет получить высокие значения скорости передачи, в ущерб точности доставки. Небольшой размер заголовка в 8 байт, структура которого приведена на рис. 6, обеспечивает быструю обработку получателем и минимальную задержку, при этом происходит быстрая доставка данных в реальном времени и эффективное использование ресурсов. В общем виде механизм передачи данных выглядит так: приложение формирует данные, добавляет заголовок UDP, и датаграмма отправляется без каких-либо дополнительных проверок. Приемная сторона получает датаграмму, проверяет контрольную сумму и, в случае успеха, передает данные приложению.

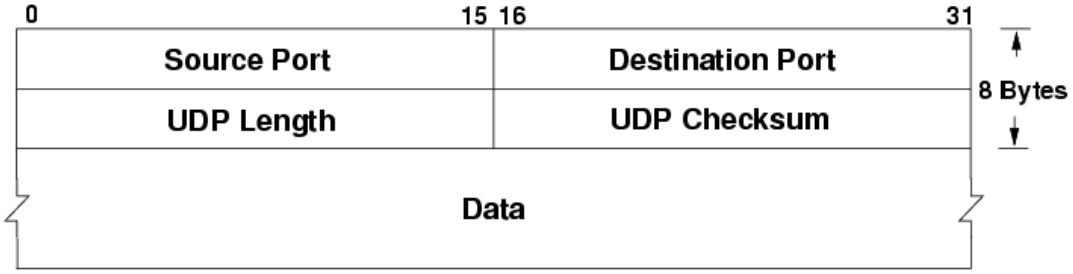


Рис. 6. UDP-заголовок

Использование классического UDP-flood, при котором злоумышленник отправляет огромное количество UDP-пакетов к целевой системе, не так эффективно при современных вычислительных мощностях и высокой скорости обработки UDP-пакетов, однако существует категория атак типа «Amplification» («Усиление»). В таком случае используются открытые службы, работающие по протоколу UDP (NTP, DNS и другие), для направления трафика на жертву. Злоумышленник отправляет запросы к открытым серверам (например, DNS) с подмененным IP-адресом жертвы, ответы от DNS-сервера в сторону жертвы будут гораздо больше по размеру, чем исходные запросы, так как будут включать в себя ответы всех DNS-серверов,

к которым обращался клиент, что вызывает перегрузку (рис. 7). Для защиты от такого типа атак владельцам DNS-серверов необходимо отключить функцию open-resolver – получение запросов из других сетей и отправка ответов без дополнительных проверок.

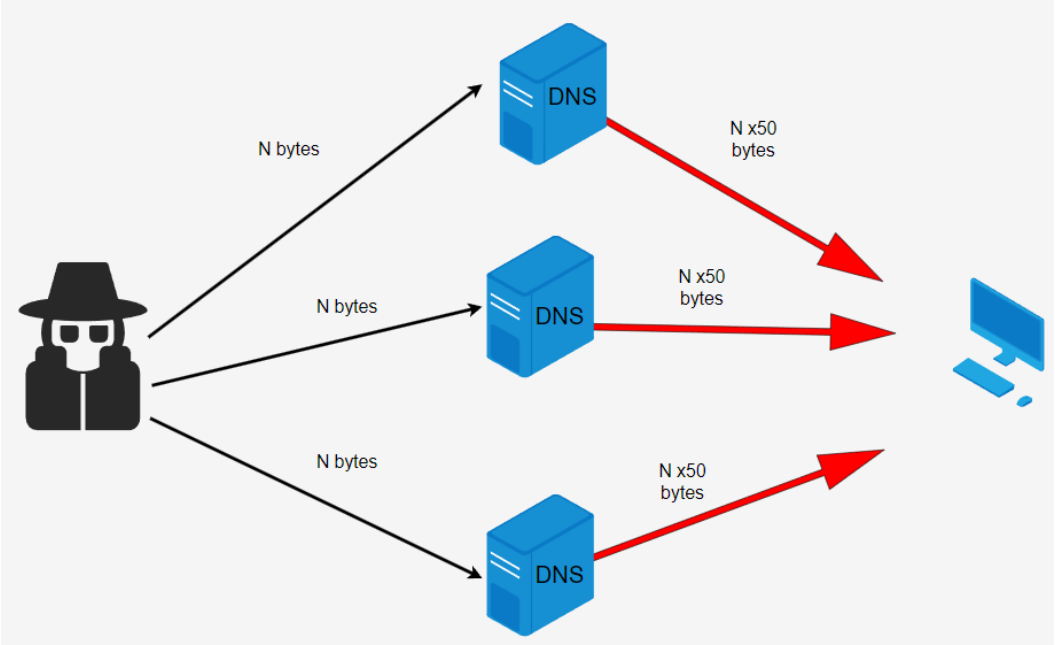


Рис. 7. Атака DNS-amplification

Седьмой и самый верхний уровень модели OSI, прикладной уровень, обеспечивающий взаимодействие с приложениями, которые используют сеть для обмена данными, также используется для осуществления DoS-атак. Самые распространенные протоколы прикладного уровня:

- HTTP/HTTPS для передачи веб-контента,
- SMTP/IMAP/POP3 для электронной почты,
- SIP/RTP для организации IP-телефонии,
- SSH для безопасного удаленного управления,
- DHCP для динамической конфигурации оконечных устройств и другие.

Наиболее популярными целями для злоумышленников являются веб-сервера организаций, располагающиеся в публичном доступе. Для осуществления DoS-атак, в данном случае, будут использованы особенности работы протокола HTTP и его защищенной версии. Изучим эти протоколы подробнее.

HTTP (S) – HyperText Transfer Protocol (Secure) – протокол передачи гипертекста (HTML, CSS, JavaScript и другие) между клиентом и сервером с помощью запросов и ответов. HTTP-запрос состоит из:

- Метод, определяет тип операции (GET, POST, PUT, DELETE).
- URL (Uniform Resource Locator), адрес запрашиваемого ресурса;

- Заголовки с метаданными о запросе.
- Тело запроса с данными (если используется метод POST или PUT).

HTTP-ответ, в свою очередь, имеет в своем составе три части – статусный код (200 OK, 404 Not Found, 503 Service Unavailable и другие), заголовки с метаданными (тип содержимого, размер файла), тело ответа с данными (HTML-страница).

Существует защищенная версия HTTPS, использующая TLS/SSL для шифрования содержимого запросов и ответов. На сегодняшний день есть новые версии HTTP/2 и HTTP/3 – модификации с целью снижения задержек и ускорения загрузки страниц.

Особенностью DoS-атак с использованием HTTP является имитация легитимных запросов от реальных пользователей, направленных на конкретный веб-сервер, сервис или приложение. Для обнаружения и предотвращения таких атак требуется глубокий анализ пакетов. Основные представители атак с использованием HTTP:

- HTTP flood – отправка огромного числа запросов GET или POST к веб-серверу с целью перегрузки. Использование сложных операций (поиск, авторизация) увеличивает нагрузку.
- Slowloris – открытие большого числа HTTP-соединений и поддержание их в активном состоянии, как можно дольше, с помощью частичных запросов, исчерпывая пул параллельных соединений, делая невозможным подключение легитимных клиентов.

Для обхода МСЭ или системы обнаружения вторжения (СОВ) может применяться фрагментация пакетов. Сам механизм разделения пакета на части предназначен для передачи данных в сетях с ограниченной максимальной длиной пакетов. Каждый фрагмент содержит общий идентификатор пакета, флаг MF (More Fragments) указывает на следующий фрагмент, поле Offset с позицией фрагмента в исходном пакете в 8-байтных блоках. Некоторые операционные системы уязвимы к некорректным фрагментированным пакетам (например, наличие измененного значения offset и атака «teardrop»). Для предотвращения вредоносного использования фрагментированных пакетов применяется техника дефрагментации до попадания подозрительных пакетов в корпоративную сеть на этапе инспекции.

Несмотря на снижение эффективности DoS/DDoS-атак за счет развития технологий и совершенствование средств противодействия, данный тип воздействия на сети все равно остается актуальным и широко применяется из-за легкости в реализации. Такие атаки могут применяться не только для выведения из строя целевой системы, но и как средство отвлечения ИБ-специалистов в момент осуществления основной атаки.

1.4. Сканирование сети: реализация и механизмы противодействия

1.4.1. Общая характеристика сетевого сканирования

В данном разделе рассмотрим следующий вид сетевых атак – разведывательные, в частности активное сетевое сканирование – процесс поиска информации о сетевой топологии цели, устройствах, их доступности, конфигурации, открытых портах и запущенных сервисах путем зондирования инфраструктуры жертвы через сетевой трафик. Такой вид воздействия не предполагает непосредственного ущерба компьютерным сетям: главная цель заключается в сборе данных для планирования будущих атак, первоначального доступа, определения приоритетной цели. Механизм активного сетевого сканирования заключается в рассылке пакетов различного формата в сети цели, получение ответов от устройств жертвы и их анализ. В зависимости от типа собираемой информации, можно классифицировать сетевое сканирование на три типа: поиск активных устройств, сканирование портов и определение операционных систем устройств. Рассмотрим каждый тип подробнее.

1.4.2. Поиск активных устройств

Это процесс обнаружения устройств в сети, реагирующих на запросы, для последующего анализа или атаки. Основные техники:

- ICMP-ping – отправка служебных сообщений ICMP 8 типа echo-request. Если устройство доступно, оно отвечает echo-reply. Способ малоэффективен, так как большинство систем блокирует сетевое обнаружение по ICMP.
- TCP-ping – отправка TCP-SYN пакетов на известные порты, которые чаще всего используются (80 или 443). Если процесс установления сессии начался (получен SYN-ACK), то хост считается активным.
- UDP-ping – отправка UDP пакетов на порты, которые, вероятно, будут закрыты (например 33434). Если получено ICMP сообщение 3 типа «Port Unreachable», значит, хост активен.
- ARP-сканирование – метод обнаружения активных устройств в локальной сети, отправка ARP-запросов на все IP-адреса в подсети. Если устройство получает запрос с его IP-адресом, оно отвечает своим MAC-адресом, в таком случае хост активен.

1.4.3. Сканирование портов

Процесс выявления открытых, закрытых или фильтруемых портов на сетевых устройствах производится для эксплуатации уязвимых протоколов, установления постоянной связи с компрометированной системой, хищения

данных или распространения вредоносного ПО. Распространенные техники:

- TCP Connect – отправка TCP-SYN пакетов по всему списку портов с целью установления полной TCP-сессии. Если получен SYN-ACK в ответ на запрос, то порт открыт, в ином случае будет получен TCP-RST, тогда порт закрыт. Легко обнаруживаемый способ из-за создания полноценных соединений.
- TCP-SYN – алгоритм схож с предыдущим, однако, вместо установления сессии при получении SYN-ACK от открытого порта, атакующий не завершает квитирование, отправляя RST. Более скрытный метод, чем TCP Connect.
- TCP-FIN – отправка TCP-FIN пакетов. Если порт закрыт, будет получен RST. Открытые порты игнорируют такой пакет, так как считают его ошибочным. Неэффективно против Windows-систем, так как они игнорируют данный тип пакетов независимо от состояния порта.
- TCP-SYN-FIN – отправка пакетов с одновременно установленными флагами SYN и FIN. Метод сочетает в себе особенности работы двух предыдущих способов. Такой пакет является нелогичным с точки зрения стандартной работы TCP. Если порт закрыт, будет получен RST. Открытые порты игнорируют такой пакет, так как считают его ошибочным. Неэффективно против Windows-систем, так как они игнорируют данный тип пакетов независимо от состояния порта.
- TCP XMAS – отправка TCP-пакетов с установленными флагами FIN, URG, PSH (или же все существующие, но без установленного ACK). Отсутствие ответа характерно для открытого порта, получение RST –закрытого.
- TCP NULL – отправка нулевых пакетов (без каких-либо установленных флагов). Если порт закрыт, будет получен RST. Открытые порты игнорируют такой пакет, так как считают его ошибочным. Windows-системы обычно игнорируют пакеты без флагов, независимо от состояния порта.
- UDP – отправка атакующим UDP-пакетов (пустых или с минимальным наполнением) на порты целевого хоста. Если получен ICMP тип 3 «Port Unreachable», то порт считается закрытым. В ином случае – порт открыт (ответ от службы или игнорирование запроса) или фильтруется межсетевым экраном. Способ малоэффективен, если генерация ICMP-ответов заблокирована.

1.4.4. Определение операционных систем

Процесс анализа характеристик сетевого трафика, поведения и ответов целевых устройств производится для определения используемой операционной системы. Основная идея в том, чтобы отправить на целевой хост специально созданные пакеты с нестандартными параметрами и проанализировать ответы, различающиеся в зависимости от используемой ОС. Злоумышленники используют информацию об операционных системах для выбора наиболее эффективных эксплойтов и методов атаки. Распространенные техники сканирования ОС:

1. TCP Sequence Predictability – анализ предсказуемости номеров последовательности TCP. Атакующий выполняет квитирование с целевым хостом и получает начальный номер последовательности (initial sequence number, ISN). Разные ОС используют различные алгоритмы генерации ISN. Полученные результаты сравниваются с базой данных известных операционных систем.
2. TCP Options – отправка TCP-пакетов с различными комбинациями опций и анализ получаемых ответов, так как разные ОС реализуют TCP-опции по разному. Основные опции, использующиеся в определении ОС при сканировании:

- Maximum segment size (MSS) – максимальный размер сегмента данных, Windows и Cisco OS часто использует значение 1460, Linux – 1460 или 536.
- Windows scale – опция увеличения размера окна приема более 65535 байт, некоторые виды ОС не поддерживают эту опцию.
- Timestamps – добавление меток времени для измерения задержек и анализа алгоритмов генерации значений. Некоторые ОС не поддерживают данную опцию.
- SACK Permitted (Selective Acknowledgment) – опция для повторной передачи пакетов в случае их потери. Некоторые ОС не поддерживают данную опцию.
- NOP (No Operation) – опция для заполнения пространства между другими опциями в заголовке TCP для разделения или выравнивания (для того, чтобы длина опций была кратна 4). Linux использует NOP только для выравнивания, Windows добавляет NOP перед важными опциями (Timestamp, Window Scale).

3. ICMP echo – определение операционной системы, основанное на различной реализации ICMP в разных операционных системах. В IP-заголовке ответа с Windows-системы значение TTL=128, а с Linux – 64. В системах Cisco TTL=255. Некоторые ОС дополняют ICMP ответы дополнительными метками (например, Windows и MacOS).

Для маскировки разведывательной деятельности в сети злоумышленники могут использовать фрагментацию сканирующих пакетов. Такая тактика может затруднить анализ трафика. Чтобы сетевое сканирование не выглядело для сотрудников ИБ-организации как аномальная активность, существует возможность замедлить процесс сканирования, отправляя запросы с большим интервалом времени, одновременно с этим, используя поддельные IP-адреса для запутывания специалистов.

Для противодействия активному сетевому сканированию необходимо настраивать правила на межсетевом экране: блокирующие входящие ICMP-запросы; ограничивающие число попыток подключения с одного адреса; блокирующие подозрительные IP-адреса; разрешающие внешние подключения к портам только по необходимости. Средства мониторинга должны обнаруживать и логировать попытки сканирования сети на основании сигнатуры аномального повышения сетевой активности.

1.5. Атаки в локальной сети

Предположим, что злоумышленнику удалось осуществить первоначальный доступ в корпоративную сеть, обнаружив уязвимости удаленного доступа или успешно реализовав фишинг по отношению к некомпетентному сотруднику. Рассмотрим возможности атакующего по перехвату и модификации сетевого трафика для хищения данных или нарушения работы сети, после чего рассмотрим принципы работы основных механизмов безопасности.

«Man-in-the-Middle» (MITM) – тип кибератак, при которой злоумышленник перехватывает или модифицирует коммуникации между двумя сторонами, при этом оставляя видимость штатного взаимодействия между участниками, чтобы в дальнейшем осуществлять прослушивание трафика (сниффинг) или его подмену. Реализация атак данного типа происходит через злоупотребление функциями сетевых протоколов, определяющих поток сетевого трафика (ARP, DNS, DHCP), заставляя легитимные устройства в сети взаимодействовать через контролируемую атакующим систему. Однако, если пользователи сети применяют криптографические средства защиты канала передачи, то атакующему придется использовать дополнительные методы для дешифрования перехватываемой информации, что может занять много времени. Подробнее рассмотрим способы осуществления MITM-атак с использованием разных протоколов.

1.5.1. ARP-poisoning

Этот вид MITM-атаки использует особенности работы протокола ARP.

Address Resolution Protocol (ARP) – протокол определения адреса, предназначен для сопоставления IP-адресов с физическими MAC-адресами в локальной сети. Функционирует на втором (канальном) уровне модели OSI.

Когда устройство хочет отправить пакет другому устройству в локальной сети с известным IP-адресом, ему необходимо знать MAC-адрес. Эта информация содержится в ARP-таблице каждого устройства. Эта структура хранит соответствия «IP-MAC-Интерфейс». Если в таблице не найден нужный MAC, отправляется широковещательный ARP-запрос, содержащий IP-адрес искомого устройства и MAC-адрес источника. Когда этот запрос получает владелец искомого IP, он отвечает на MAC-источник, высылая свой собственный MAC-адрес. В механизме работы протокола и кроется возможность отравления ARP-кэша: из-за широковещательной рассылки запроса его легко может перехватить другое устройство в пределах широковещательного домена (рис. 8).

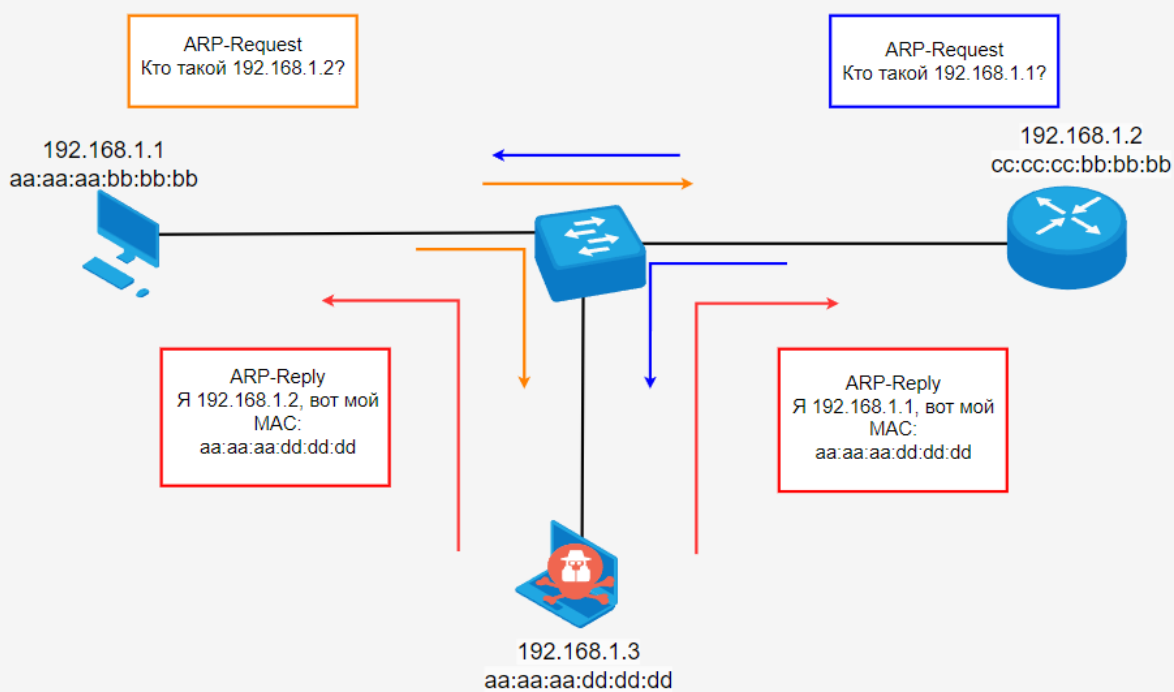


Рис. 8. Выполнение ARP-Poisoning

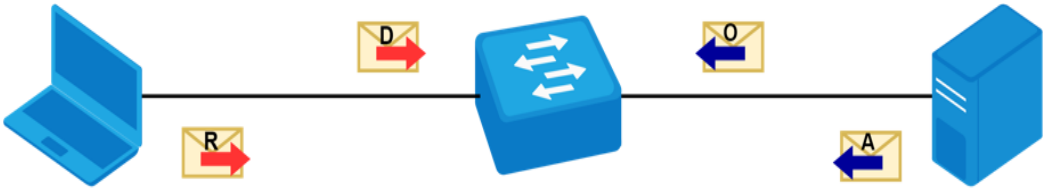
При выполнении атаки, злоумышленник ожидает ARP-запрос, чтобы отравить кэш запрашивающего устройства. Когда запрос получен, атакующий отвечает своим MAC-адресом, обманывая жертву. Для перехвата трафика между устройствами атакующий, таким образом, «навязывает» себя в качестве шлюза по умолчанию для устройств, становясь посредником между диалогом двух устройств. Другие устройства в подсети обновляют свои ARP-таблицы, добавляя запись соответствия IP-адреса шлюза с MAC-адресом злоумышленника. Теперь трафик может быть перехвачен и изменен в процессе передачи.

1.5.2. DHCP-spoofing и DHCP-starvation

Использование протокола DHCP и имитация действий легитимного DHCP-сервера в локальной сети с целью предоставления устройствам неверных сетевых параметров. Рассмотрим протокол DHCP и принципы его работы для лучшего понимания атаки.

Dynamic Host Configuration Protocol (DHCP) – протокол динамической конфигурации оконечных устройств, предназначен для автоматической конфигурации сетевых параметров – IP-адрес, шлюз, адрес DNS-сервера и другие параметры. Работа протокола основана на клиент-серверной модели: когда устройство подключается к сети, оно инициирует процесс получения параметров (DORA – Discover, Offer, Request, Acknowledge), представлен на рис. 9:

1. Discover (Обнаружение) – клиент отправляет широковещательный запрос в локальную сеть в поисках DHCP-сервера.
2. Offer (Предложение) – сервер получает запрос и отправляет предложение с сетевыми параметрами.
3. Request (Запрос) – клиент принимает предложение и отправляет серверу сообщение, подтверждая желание использовать предложенные параметры.
4. Acknowledge (Подтверждение) – сервер отправляет подтверждение, фиксируя аренду параметров для клиента.



	Destination MAC	Source MAC	Ether Type	Source IP	Dest. IP	Src Port	Dst Port	DHCP Data
D	FF:FF:FF:FF:FF:FF	AA:BB:CC:DD:EE:11	0800	0.0.0.0	255.255.255.255	68	67	MsgType: DISCOVER
O	AA:BB:CC:DD:EE:11	CC:DD:BB:AA:EE:22	0800	10.10.1.1	0.0.0.0	67	68	MsgType: OFFER YIADDR: 10.10.1.15
R	FF:FF:FF:FF:FF:FF	AA:BB:CC:DD:EE:11	0800	0.0.0.0	255.255.255.255	68	67	MsgType: REQUEST YIADDR: 10.10.1.15
A	AA:BB:CC:DD:EE:11	CC:DD:BB:AA:EE:22	0800	10.10.1.1	0.0.0.0	67	68	MsgType: ACK YIADDR: 10.10.1.15

Рис. 9. Работа протокола DHCP

Широковещательная природа и отсутствие встроенных механизмов аутентификации делают DHCP уязвимым к различным атакам. DHCP-starvation направлена на исчерпание пула доступных IP-адресов легитимного DHCP-сервера, что приводит к невозможности получения сетевых параметров санкционированными пользователями. В данном случае, злоумышленник генерирует множество DHCP Discover с уникальными MAC-адресами, вынуждая сервер резервировать IP-адрес для каждого уникального запроса, что неизбежно приводит к исчерпанию всех доступных адресов (рисунок 10). Как только это происходит, легитимные пользователи не могут получить сетевую конфигурацию от DHCP-сервера и подключиться к сети. При такой ситуации, злоумышленник может выполнить DHCP-Spoofing, выступая в роли DHCP-сервера и осуществляя раздачу поддельных сетевыхпараметров для пользователей.

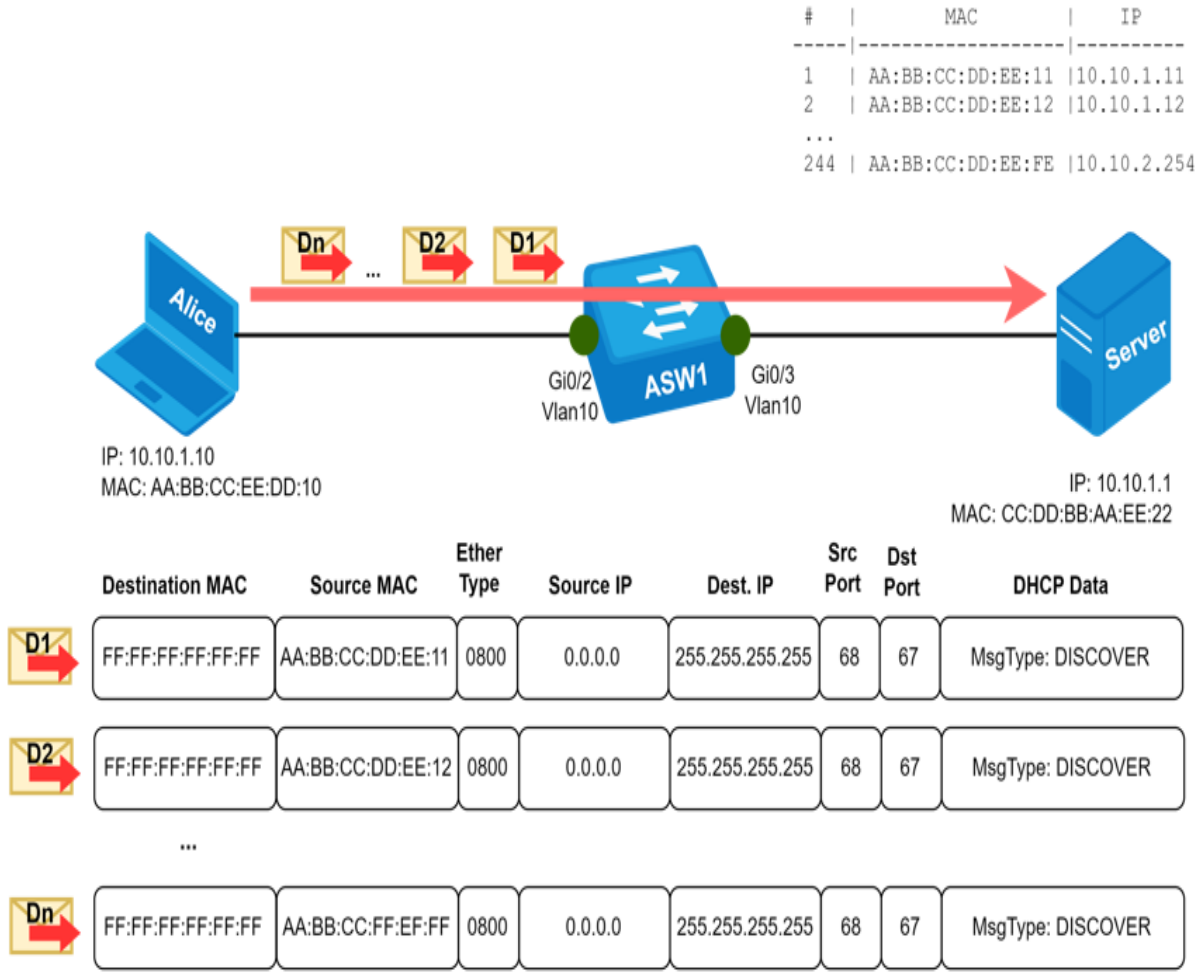


Рис. 10. DHCP-starvation

Для выполнения спуфинга, злоумышленник, находясь в одной локальной сети с жертвой, эмулирует работу DHCP-сервера. При получении широковещательного запроса от жертвы сервер атакующего предлагает свои

параметры вместо легальных – в случае успеха, цель получает адреса шлюза, DNS-сервера. Это приводит к тому, что весь исходящий трафик жертвы отправляется в сторону злоумышленника или подконтрольных ему устройств. Главное условие – DHCP ответ злоумышленника должен быть быстрее ответа легитимного сервера (рис. 11).

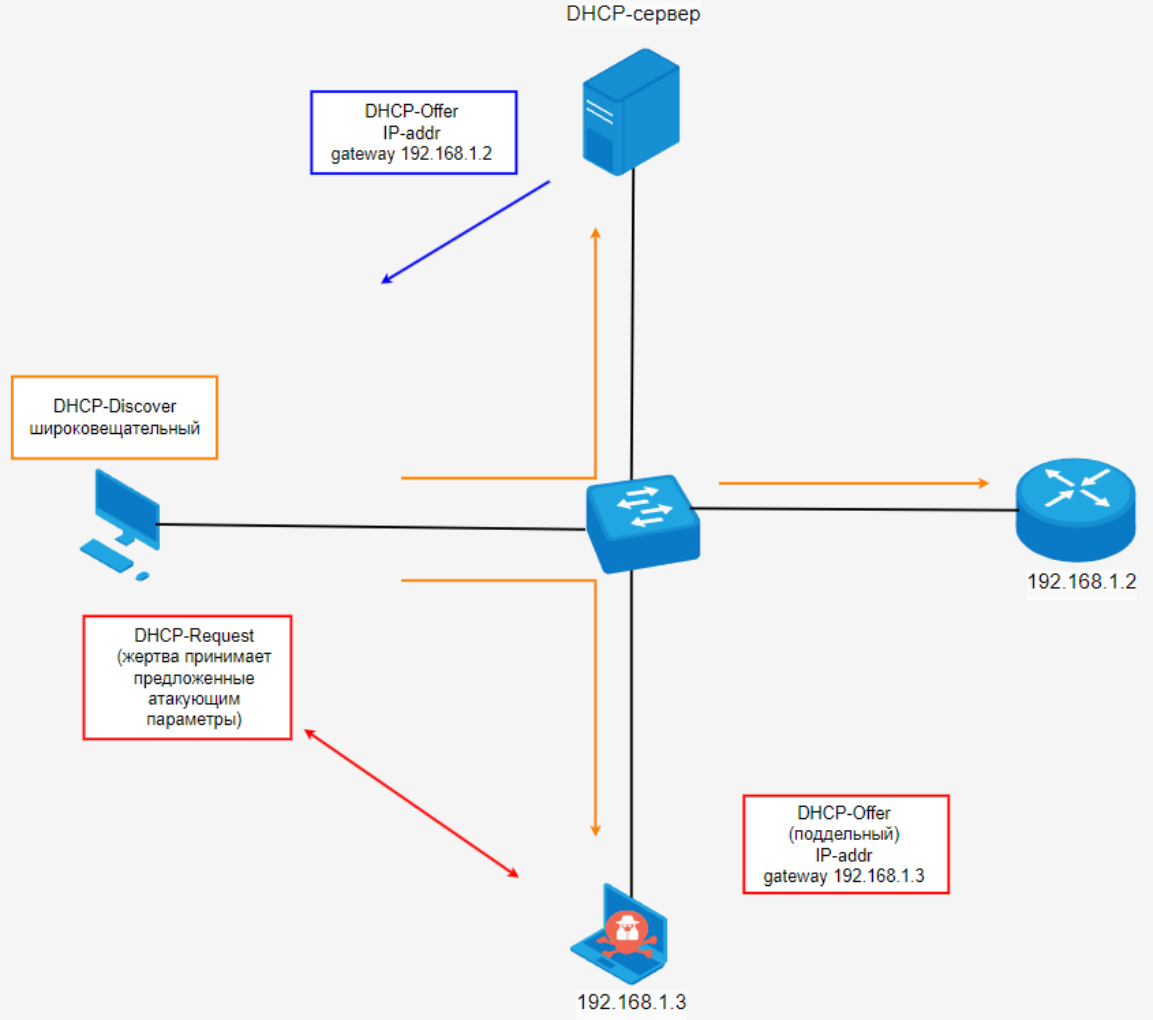


Рис. 11. Выполнение DHCP-Spoofing

Контрольные вопросы

Опишите текущее состояние информационной безопасности в России.
Какие объекты являются целями группировки Core Werewolf?
Что собой представляют Brute Force атаки?
Перечислите самые распространенные методы компьютерных атак.
Объясните значение термина «ботнет».
На что направлены атаки типа «Отказ в обслуживании» (DoS/DDoS)?
В чем заключаются преимущества атак типа «Отказ в обслуживании» (DoS/DDoS) по сравнению с другими видами кибератак?
Какова тактика нападения Distributed Denial of Service?

В чем заключается ключевой замысел любой кибератаки?
Опишите разновидности DoS/DDoS-атак.
Перечислите способы противодействия DoS/DDoS-атакам.
Что представляет собой активное сетевое сканирование?
Перечислите основные техники поиска активных устройств.
Перечислите распространенные техники сканирования операционных систем.
Что могут использовать злоумышленники для маскировки разведывательной деятельности в сети?
Перечислите способы противодействия активному сетевому сканированию.
Как осуществляется тип кибератак «Man-in-the-Middle»?
В чем заключается предназначение протокола Address Resolution Protocol?
Назовите принципы работы протокола ARP.
Опишите принцип действия ARP-poisoning – вида MITM-атаки.
Назовите принципы работы протокола Dynamic Host Configuration Protocol.
Опишите действия злоумышленника для выполнения спуфинга.
Каковы действия злоумышленника для проведения DHCP-starvation?

2. МЕТОДЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИБ В КОМПЬЮТЕРНЫХ СЕТЯХ: БЕЗОПАСНОСТЬ КОММУТАТОРОВ

2.1. Сущность сетевой безопасности коммутаторов

Коммутаторы, как компонент компьютерных сетей, играют фундаментальную роль в локальных сетях, обеспечивая возможность подключения к сети оконечных устройств (коммутаторы L2 или коммутаторы доступа). В случае несанкционированного воздействия на данный элемент сетевой инфраструктуры существенно возрастает риск компрометации всего сегмента сети. Поэтому в данной главе будут приведены способы защиты от атак в локальных сетях, поскольку на современном сетевом оборудовании рассматриваемые механизмы чаще всего являются компонентами программного обеспечения именно коммутаторов. Подробное рассмотрение механизмов противодействия атакам на втором уровне OSI будем производить в порядке, представленном на рисунке 12.

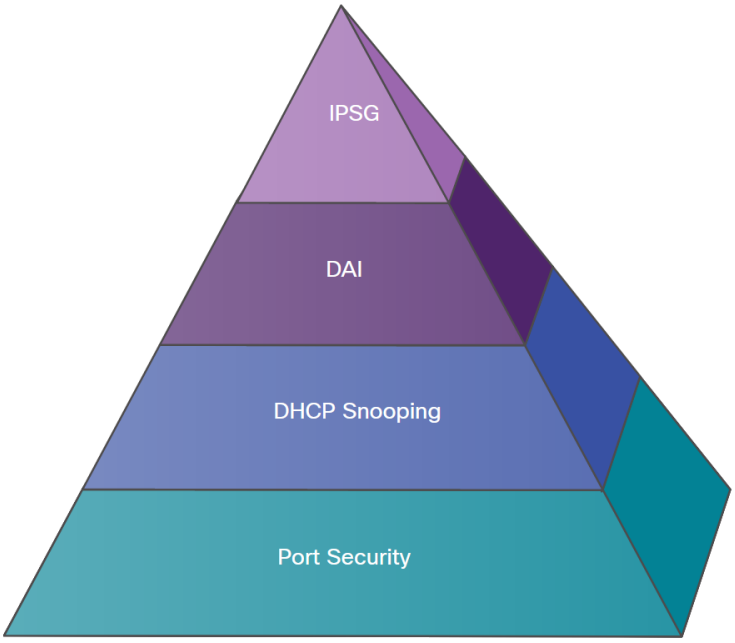


Рис. 12. Технологии противодействия сетевым атакам на коммутаторе

2.2. Механизмы защиты от атак в локальных сетях

2.2.1. Port Security

Таблица MAC-адресов имеет свои ограничения. Если кадры генерируются злоумышленником достаточно быстро, таблица MAC-адресов может переполниться, и, когда последний MAC-адрес будет изучен и больше нет свободных записей для изучения MAC-адресов, коммутатор начинает рассылать входящие кадры во все доступные порты, создавая шторм (рис. 13).

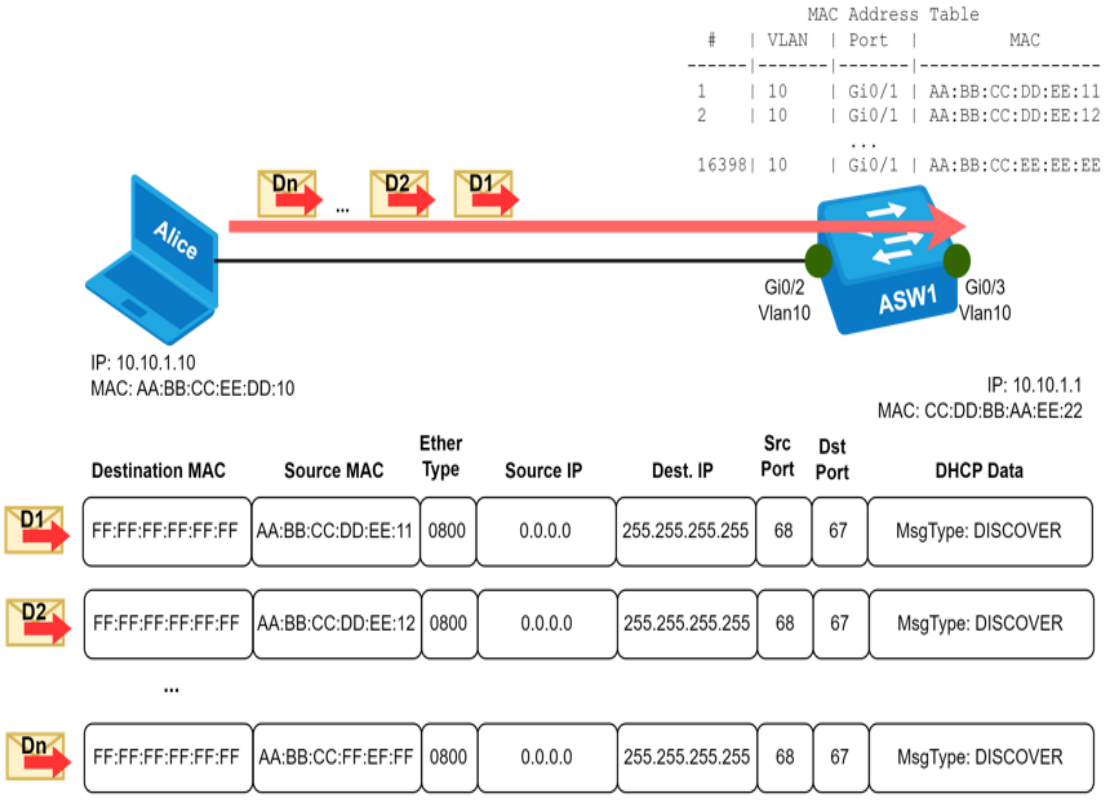


Рис. 13. Переполнение таблицы MAC-адресов

Функция Port Security помогает смягчить атаку по переполнению таблицы MAC-адресов за счет снижения скорости изучения MAC-адресов на определенном порту. После включения Port Security коммутатор отслеживает поступающие MAC-адреса и применяет к ним заданные политики безопасности. В случае нарушения установленных правил могут применяться различные меры воздействия, включая блокировку порта. Port Security способен работать в нескольких режимах:

- lock – сохраняются все изученные mac-адреса, связанные с интерфейсом и запрещается изучение новых адресов и старение уже изученных;
- max-address – удаление текущих изученных адресов и возможность изучения максимального количества адресов на порту;
- secure-delete-on-reset – удаление текущих изученных адресов и возможность изучения максимального количества адресов на порту без повторного изучения и старения MAC-адресов. Изученные адреса сохраняются до перезагрузки;
- secure-permanent – удаление текущих изученных адресов и возможность изучения максимального количества адресов на порту без повторного изучения и старения MAC-адресов. Изученные адреса сохраняются после перезагрузки.

2.2.2. DHCP Snooping

Данная функция при включении на коммутаторе формирует таблицу связок IP-адресов, выданных клиентам по DHCP, с их MAC-адресами. Также в данной таблице (таблица 1) содержится информация о типе записей – статическая или динамическая, номере VLAN, времени аренды IP-адреса и интерфейсе коммутатора, через который клиентское устройство подключено к сети.

Таблица 1

Пример таблицы DHCP Snooping binding

MAC	IP	Lease time (sec)	VLAN	Type	Interface
00:aa:bb:cc:dd:ee	192.168.1.100	7200	10	dynamic	gi1/0/1

Для полноценной работы защитного механизма, перед включением DHCP Snooping, необходимо классифицировать интерфейсы по двум категориям: надежный – к данному порту подключен легитимный DHCP-сервер или другое сетевое оборудование, ненадежный – порты, к которым подключаются оконечные устройства. Когда сообщение Discover поступает на недоверенный порт, коммутатор анализирует IP-адрес клиента и данные MAC-адреса клиента из соответствующих полей пакета DHCP (YIADDR и ClientMAC) и привязывает их к идентификатору порта и идентификатору VLAN в таблицу DHCP Snooping Binding. Поскольку на данном этапе DHCP-взаимодействия у Клиентов нет IP-адреса, соответствующее поле таблицы заполняется нулями (IP 0.0.0.0). Полю «Аренда» по умолчанию присвоено значение 120 секунд (рис. 14).

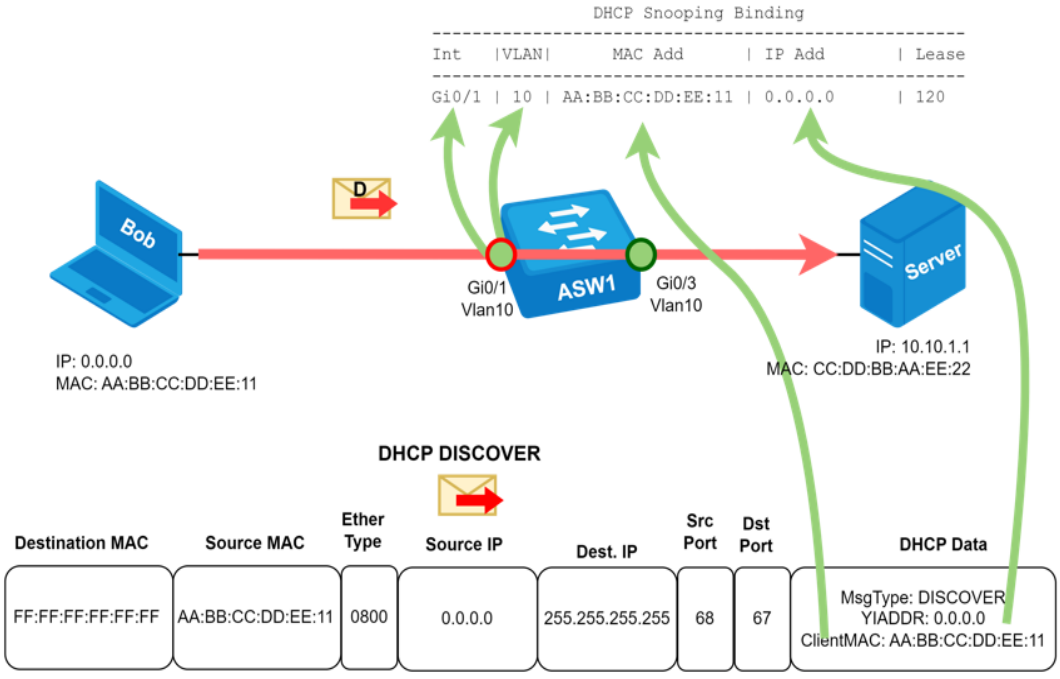


Рис. 14. Формирование таблицы DHCP Snooping Binding

При получении сообщения Ack от DHCP-сервера коммутатор извлекает значения полей YIADDR и LEASE и привязывает их к соответствующей строке таблицы DHCP Snooping. Теперь процесс связывания порта, VLAN, MAC-адреса клиента и IP-адреса клиента завершен, и соответствующая запись может использоваться для целей фильтрации кадров (рис. 15).

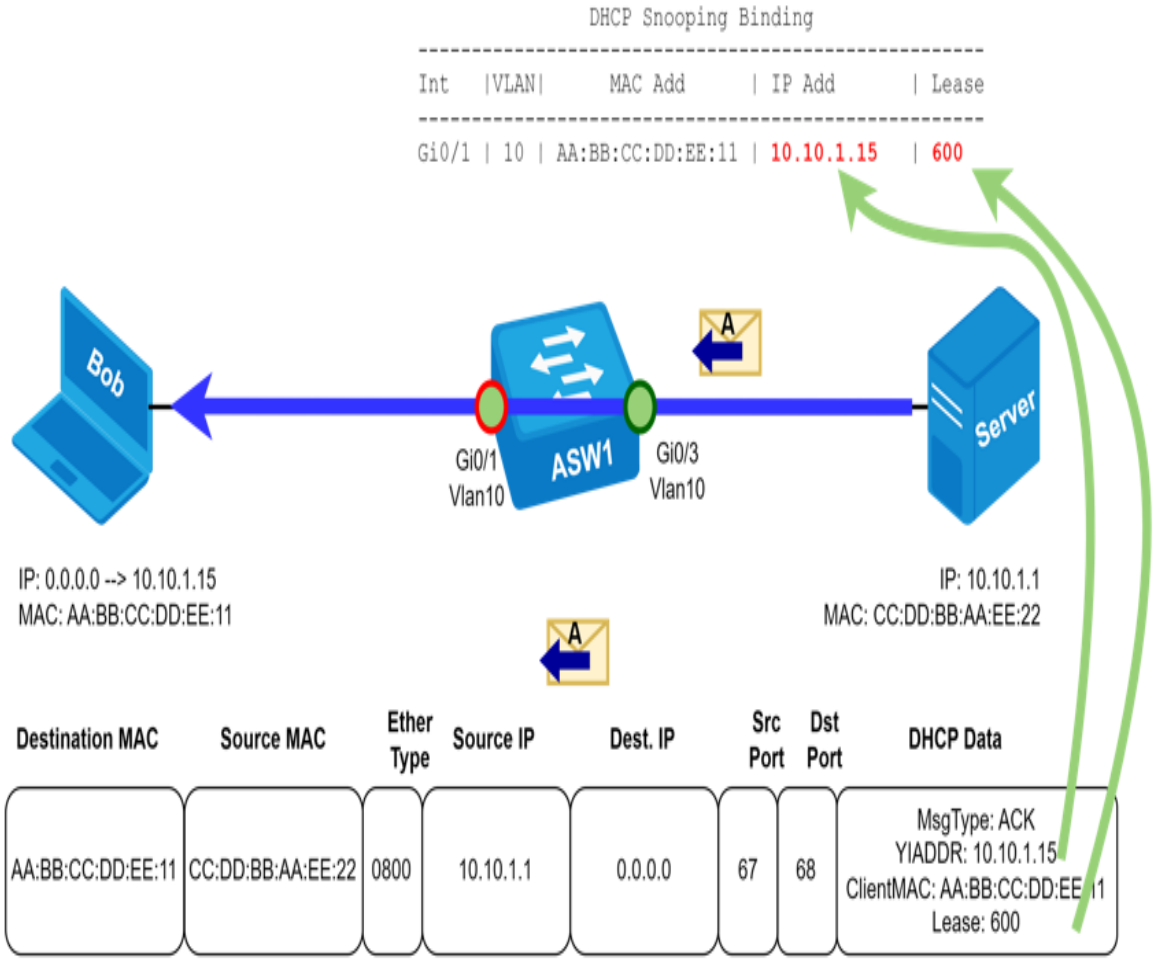


Рис. 15. Завершение формирования таблицы DHCP Snooping Binding

При таких условиях сообщение DHCP-offer может быть отправлено только через доверенный порт, а это означает, что, если злоумышленник попытается выполнить DHCP-spoofing атаку, его сообщение с поддельной конфигурацией сетевых параметров для оконечного устройства будет заблокировано, так как придет на недоверенный порт (рис. 16).

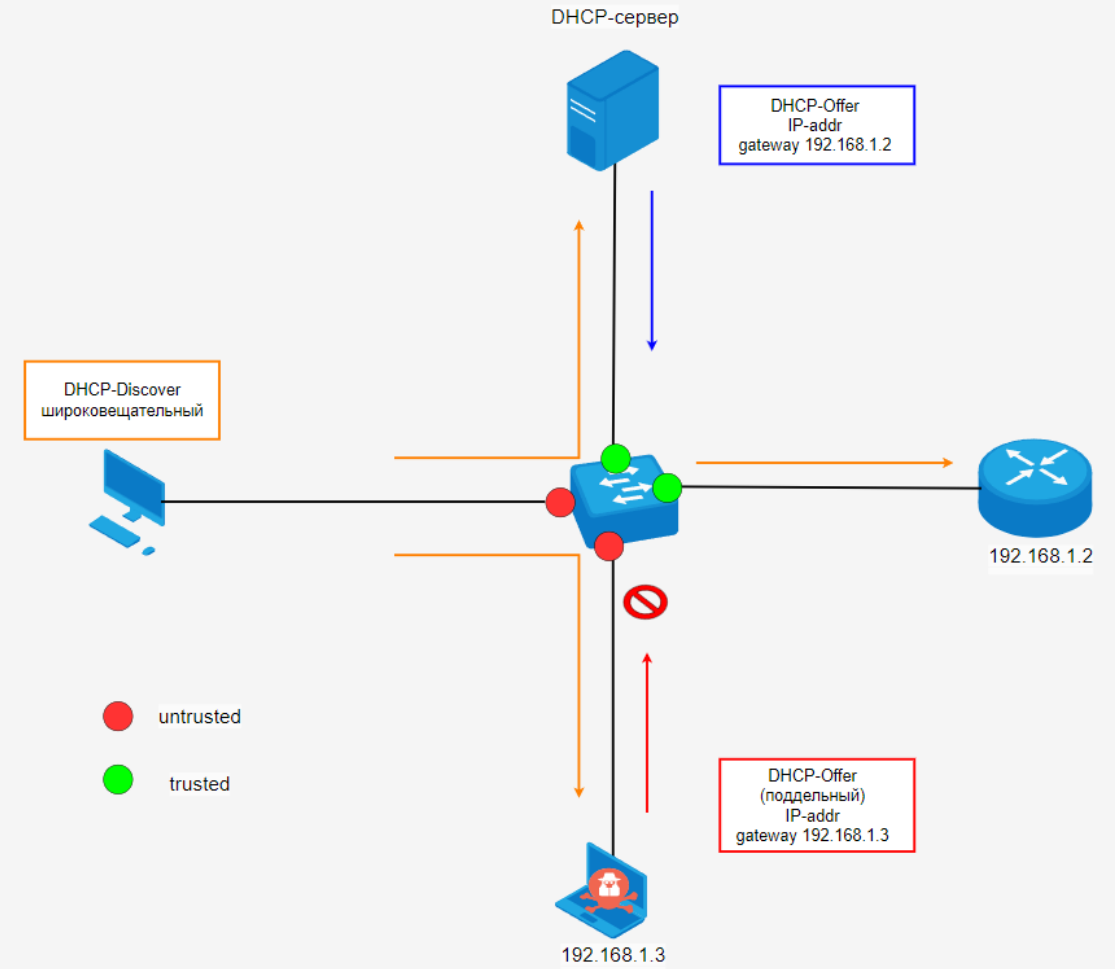


Рис. 16. Работа DHCP Snooping

2.2.3. ARP Inspection

Следующая технология предназначена для предотвращения ARP-poisoning атак. ARP Inspection предотвращает подмену MAC адреса, проверяя каждое сообщение ARP, попадающее на коммутатор. Если сообщение не соответствует базе данных доверенных связок «IP-MAC», оно блокируется. Этот механизм регулирует только сообщения протокола ARP и не может повлиять напрямую на трафик пользователей или другие протоколы. Существует два вида ARP Inspection – статический и динамический. В первом случае для проверки ARP-сообщений используются статические записи из ARP-таблицы, внесенные туда администратором вручную. Данный вариант используется для обеспечения безопасности устройств, не получающих настройки по DHCP (сервера, маршрутизаторы). Основным видом является DAI – Dynamic ARP Inspection, который работает в связке с DHCP Snooping и использует его таблицу соответствий «MAC-IP-Interface» при проверке ARP-пакетов. Если порт ненадёжный, то коммутатор перехватывает все ARP-запросы и ARP-ответы на этих портах, прежде чем перенаправлять их,

осуществляя проверку соответствия MAC-адреса IP-адресу на основе DHCP Snooping Binding или статических записей.

2.2.4. IP Source Guard

IP Source Guard (Dynamic IP Lockdown) – функция коммутатора, которая ограничивает IP-трафик на интерфейсах второго уровня, фильтруя трафик на основании таблицы привязок DHCP snooping и статических соответствий. Функция используется для борьбы с IP-spoofing. IP-Spoofing – это метод атаки, при котором злоумышленник подменяет исходный IP-адрес в заголовке пакета, маскируя себя под доверенный узел.

Для защиты от подмены IP-адресов применяется таблица привязок. Она позволяет различать санкционированные и несанкционированные DHCP- и ARP-пакеты. При привязке используются следующие атрибуты:

- MAC-адрес.
- VLAN ID.
- IP-адрес.
- Номер порта.

При получении коммутатором пакета DHCP или ARP производится поиск соответствующих MAC-адреса, идентификатора VLAN ID, IP-адреса и номера порта в таблице привязок. При наличии привязки коммутатор пересылает пакет. Если привязка не найдена, пакет коммутатором отбрасывается. Поскольку функция контроля защиты IP-адреса использует таблицы соответствий DHCP Snooping, имеет смысл использовать данную функцию, предварительно настроив и включив DHCP Snooping.

2.2.5. Защита от петель

Протокол Spanning Tree Protocol (STP) предназначен для предотвращения появления петлей в сети и является стандартным средством, поддерживаемым большинством коммутаторов разных вендоров. Однако существуют ситуации, в которых использование STP невозможно или запрещено из-за задержек при его работе или несовместимости с применяемыми технологиями. При таких условиях, механизм Loopback Detection (LBD) является альтернативой применения STP и его вариаций.

Когда функция LBD активирована, коммутатор начинает транслировать пакеты LDP (Loopback Detection Packets) на активные порты. Их единственная задача – вернуться на передающий коммутатор в случае возникновения петли в нисходящем направлении и быть обнаруженными передающим коммутатором (рис. 17). В зависимости от потребностей администратора можно использовать различные значения в качестве MAC-адреса назначения пакета LDP, например, широковещательный MAC-адрес (все), многоадресный MAC-адрес (CF:00:00:00:00:00), MAC-адрес коммутатора

(базовый MAC) и MAC-адрес исходного интерфейса. По умолчанию используется широковещательный MAC-адрес.

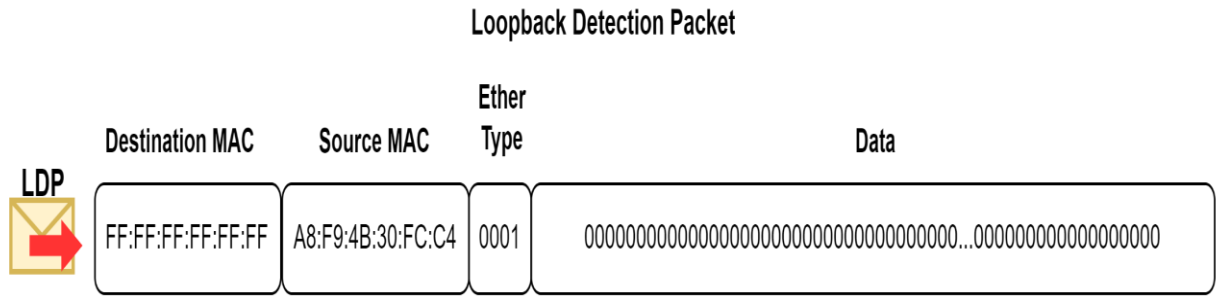


Рис. 17. LBD-пакет

Возвращающийся LDP сигнализирует о наличии петли, поэтому передающий коммутатор обнаруживает ее по прибытии пакета обратно и переводит соответствующий интерфейс в состояние Errdisable – нерабочее состояние из-за обнаружения ошибки до вмешательства администратора (рис. 18).

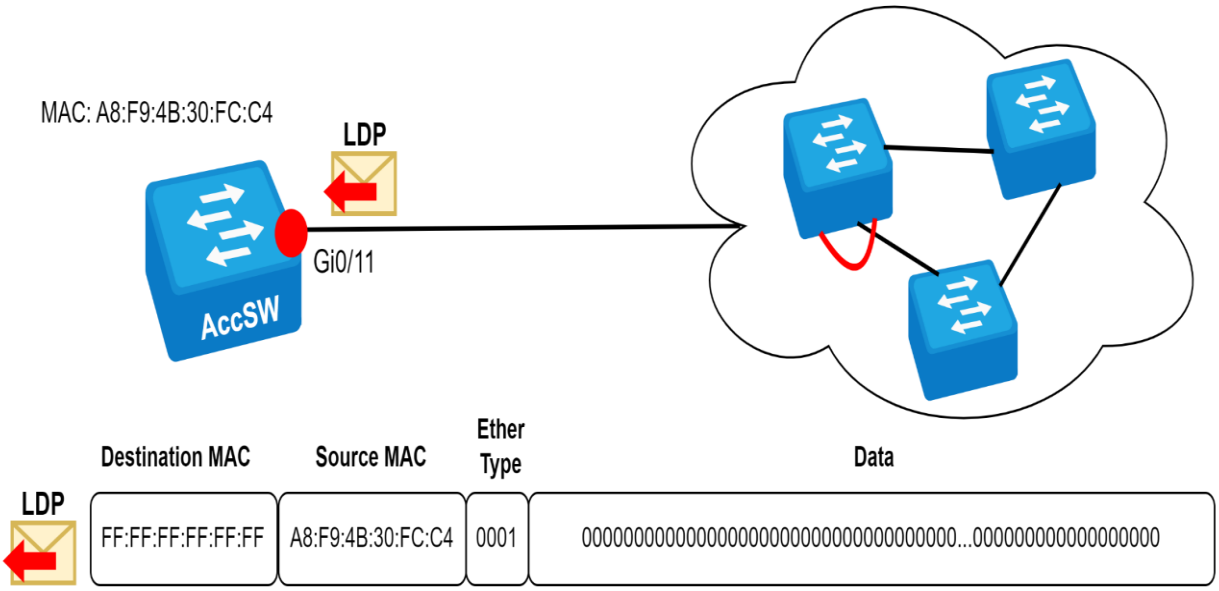


Рис. 18. Обнаружение петли

2.2.6. Защита от шторма

Существуют ситуации, когда вся полоса пропускания канала может быть занята каким-либо типом кадров, например, широковещательными кадрами. Поскольку кадры этого типа рассылаются из всех портов принимающего коммутатора, ситуация может быстро стать неконтролируемой и, следовательно, потребует немедленного реагирования (рис. 19). Для этого используется функция StormControl. Она подсчитывает кадры определенного типа (широковещательные, многоадресные или неизвестные

одноадресные) и предпринимает определенные действия, если они превышают предусмотренный лимит.

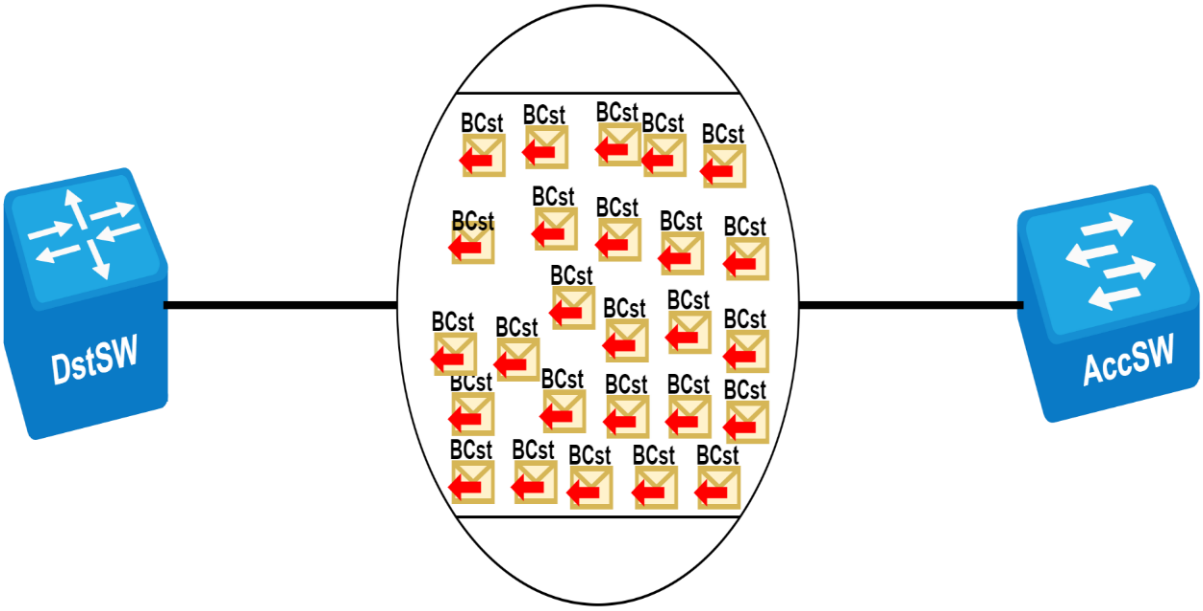


Рис. 19. Широковещательный шторм

При обнаружении шторма коммутатор генерирует автоматическое сообщение SNMP-trap, информирующее о событии, либо отключает интерфейс и регистрирует событие в Syslog. Также возможна комбинация действий по отключению интерфейса и генерации SNMP-trap.

2.2.7 Защита от атак с использованием VLAN

Технология VLAN (Virtual Local Area Network, виртуальная локальная сеть) является основой сегментированной коммутационной сети, позволяя разделять трафик внутри одной физической инфраструктуры. Стандарт IEEE 802.1Q определяет механизм маркировки Ethernet-кадров, обеспечивая передачу данных между VLAN через коммутаторы. Применение логической сегментации и изоляция сегментов друг от друга снижает риски несанкционированного доступа к передающимся данным.

Кратко повторим принципы работы данной технологии для лучшего понимания возможных векторов атак с использованием VLAN и защиты от них. Каждому коммутационному порту назначается определенный VLAN ID от 1 до 4094. Существует, как минимум, два основных типа портов – access (работает только в одной VLAN, используется для подключения оконечных устройств) и trunk (передают трафик нескольких VLAN между коммутаторами). Стандарт IEEE 802.1q определяет способ тегирования Ethernet-кадров (рис. 20), добавляя в стандартный кадр четыре дополнительных байта.

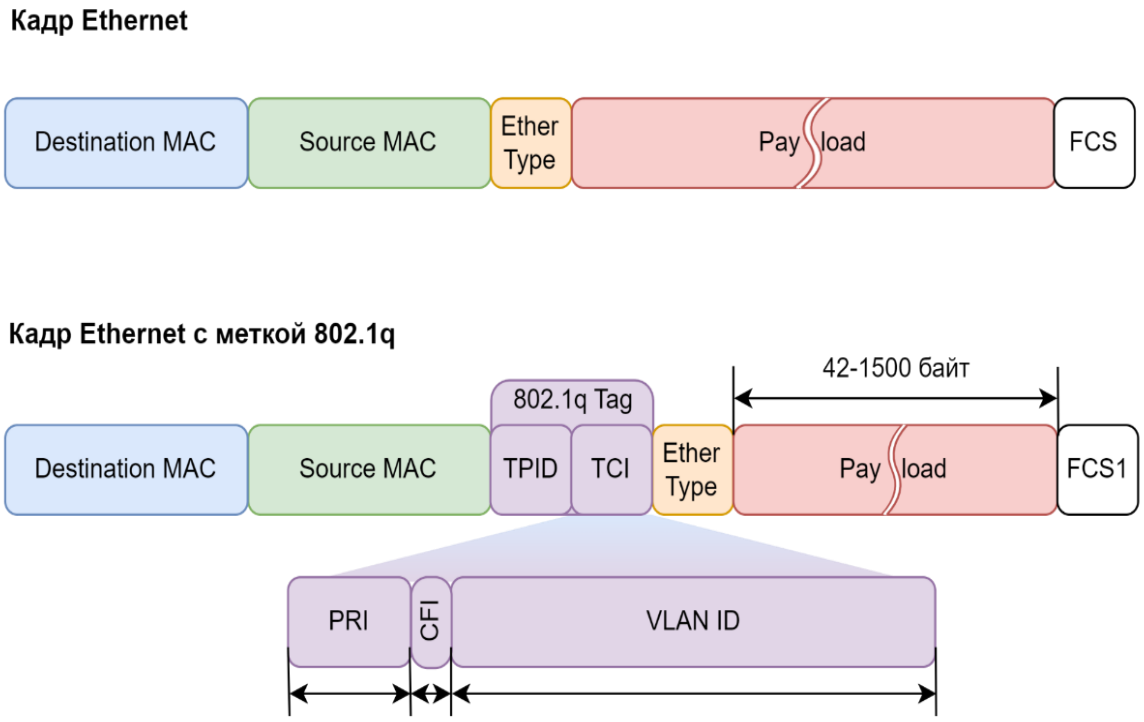


Рис. 20. Тегирование 802.1q

В заводской конфигурации все порты коммутатора назначены VLAN 1, которая, по умолчанию, используется для передачи служебных протоколов, например, STP. На транковых портах default VLAN применяется как Native – через него передаются все нетегированные кадры. Исходя из этого, формируется тип атаки, эксплуатирующий default VLAN.

VLAN Hopping – атака, основанная на манипуляции тегами для несанкционированного доступа к другим VLAN. Одна из реализаций данной атаки заключается в двойном тегировании кадра. Внешний тег – тег Native VLAN, а внутренний – VLAN ID, куда хочет передать трафик злоумышленник (рис. 21). При обработке кадра коммутатором, тег Native отбрасывается, так как такой трафик передается нетегированным, после чего кадры пересылаются дальше с внутренним тегом.

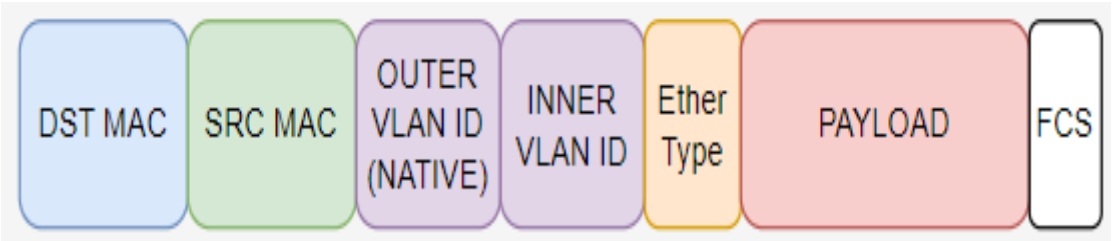


Рис. 21. Double Tagging

Для предотвращения данных атак необходимо запрещать default VLAN на портах, а Native VLAN на транковых портах изменять на отличную от единицы.

Контрольные вопросы

В чем заключается назначение коммутаторов?
Назовите причины, из-за которых важно знание способов защиты от атак в локальных сетях.
Какие действия злоумышленника могут привести к переполнению таблицы MAC-адресов?
Чему способствует включение функции Port Security?
В каких режимах способен работать Port Security?
Назовите предназначение функции коммутатора DHCP Snooping.
По какой причине перед включением функции DHCP Snooping необходимо провести классифицирование интерфейсов?
По каким категориям проводится классифицирование интерфейсов перед включением функции DHCP Snooping?
Что происходит при поступлении сообщения Discover на недоверенный порт?
Опишите действия коммутатора при поступлении сообщения Ack от DHCP-сервера при включенной функции DHCP Snooping.
Через какой порт может быть отправлено сообщение DHCP-offer?
Какая технология предназначена для предотвращения ARP-poisoning атак?
Объясните назначение технологии ARP Inspection.
Назовите виды технологий ARP Inspection.
В каком виде технологии ARP Inspection для проверки ARP-сообщений используются статические записи из ARP-таблицы, внесенные туда администратором вручную?
Для обеспечения безопасности каких устройств применяется статический вид технологии ARP Inspection?
В чем заключается принцип работы технологии Dynamic ARP Inspection?
Назовите предназначение функции коммутатора IP Source Guard (Dynamic IP Lockdown).
В чем заключается принцип работы функции коммутатора IP Source Guard?
В чем заключается метод атаки IP-Spoofing?
Что применяется для защиты от подмены IP-адресов?
Какие атрибуты используются для защиты от подмены IP-адресов?
Почему для противодействия методу атаки IP-Spoofing необходимо предварительно настроить и включить DHCP Snooping?
Для чего предназначен Spanning Tree Protocol (STP)?
В каких ситуациях использование протокола STP невозможно или запрещено?
Какой механизм является альтернативой применения STP и его вариаций?
Что происходит при активировании функции Loopback Detection (LBD)?
Какие MAC-адреса можно использовать в качестве MAC-адреса назначения пакета LDP (Loopback Detection Packets)?

Какой MAC-адрес используется по умолчанию в качестве адреса назначения пакета LDP?
О чем свидетельствует перевод интерфейса в состояние Errdisable?
В каких ситуациях используется функция StormControl?
Опишите принцип работы функции StormControl.
В каких ситуациях коммутатор генерирует автоматическое сообщение SNMP-trap?
Назовите предназначение технологии VLAN (Virtual Local Area Network).
Каковы принципы работы технологии VLAN?
За счет чего происходит снижение рисков несанкционированного доступа к передающимся данным при использовании технологии VLAN?
Чем отличаются между собой порты access и trunk при использовании технологии VLAN?
Что представляет собой атака VLAN Hopping?
Какие меры необходимо применять для предотвращения атак VLAN Hopping?

3. ПРОТОКОЛЫ AAA

3.1. Принципы AAA

AAA (Authentication, authorization, accounting) – аутентификация, авторизация и учет – это система и методология, используемая в целях обеспечения защиты от несанкционированного доступа. Она включает в себя три составляющих:

Аутентификация – процесс проверки подлинности клиента (пользователя или подключаемого устройства), пытающегося получить легитимный доступ к ресурсам сети. Цель данного мероприятия – убедиться, что клиент именно тот, за кого себя выдает. Происходит это за счет отправки пользователем учетных данных для проверки. В качестве аутентификационной информации может выступать логин и пароль, физический носитель, биометрические данные, криптографические сертификаты и ключи.

Авторизация – процесс определения полномочий, прав и привилегий пользователя по отношению к запрашиваемым ресурсам после успешного прохождения аутентификации. Права доступа могут быть определены на основании ролей, групп или индивидуальных политик. На сетевом оборудовании Eltex, как и на Cisco, данный процесс реализован с помощью пятнадцати уровней привилегий, назначаемых пользователю и разграничивающих доступ к различным видам команд конфигурирования сетевого оборудования.

Учет – процесс сбора информации о действиях клиента, например: время начала и завершения сеанса, объем и время использования ресурсов и другие метрики.

Существует два режима работы механизмов AAA. Рассмотрим каждый режим подробнее.

Локальный режим или локальная аутентификация – наиболее подходящая для небольших сетей модель. В данном случае аутентификационная информация, информация о правах доступа и журналирование действий клиента происходит в рамках одного устройства и его памяти (рис. 22). Отсюда вытекает главный недостаток этого подхода: при масштабировании сетевой инфраструктуры и появлении новых учетных записей необходимо выполнять настройку на каждом устройстве индивидуально. Также, в случае получения неправомерного доступа к сетевому оборудованию, есть вероятность компрометации локальной базы данных пользователей.

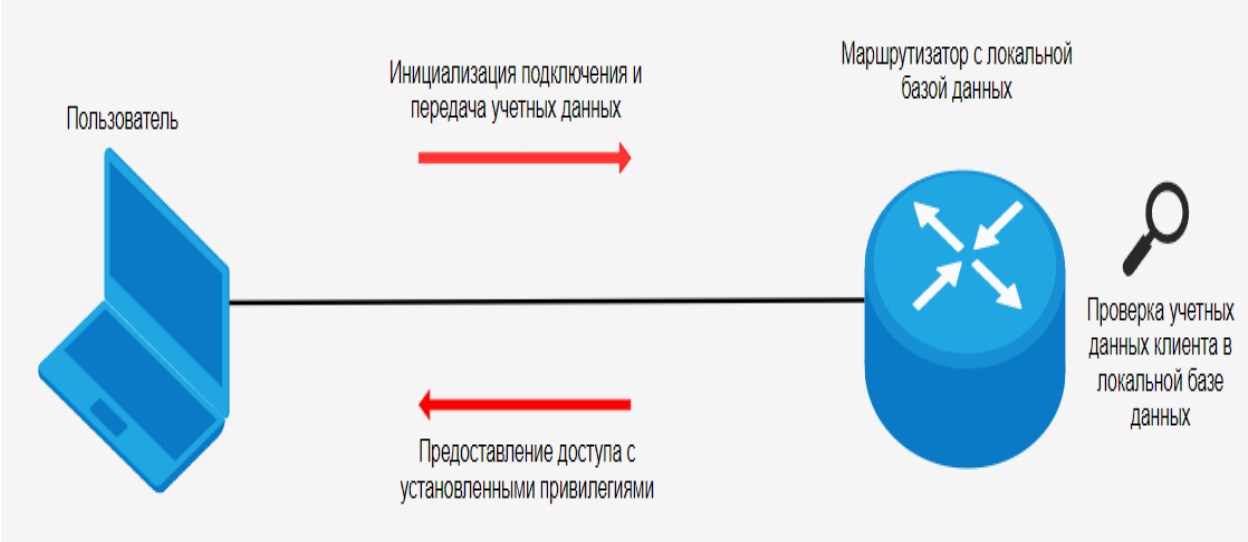


Рис. 22. Процесс локальной аутентификации

В крупных сетях с большим числом пользователей разного уровня прав доступа применяется серверная аутентификация. Существует три составляющие данного подхода (рис. 23):

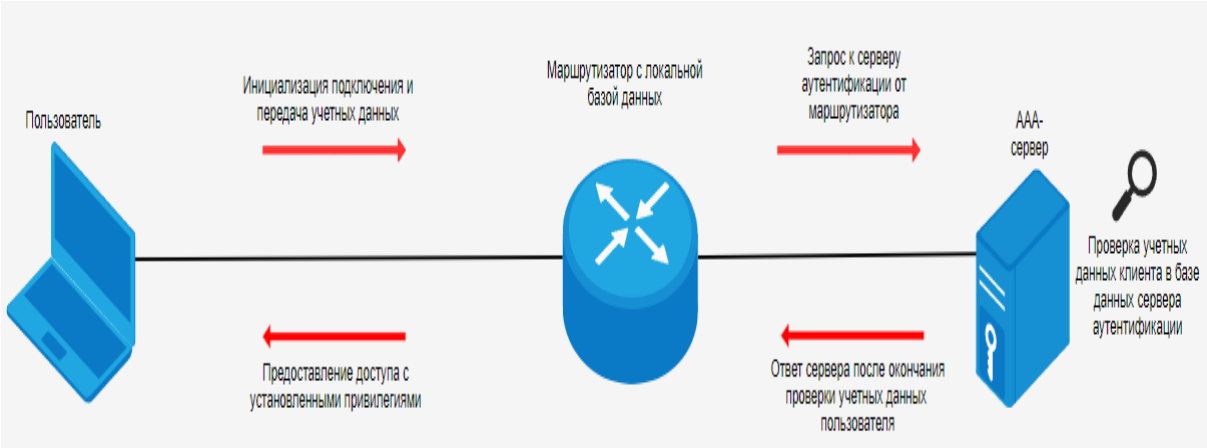


Рис. 23. Процесс серверной аутентификации

Сервер аутентификации (AAA-сервер) – серверная машина, хранящая учетные записи легитимных пользователей.

Аутентификатор – устройство, к которому подключается супликант, является клиентом для AAA-сервера и передает ему учетные данные супликанта.

Супликант – пользователь или устройство, запрашивающее доступ.

Такая модель аутентификации позволяет обеспечить централизованное управление сетевым доступом для всех узлов сети, не теряя возможности в гибкости и масштабируемости, однако требует настройки соответствующих протоколов на клиенте и сервере. В случае, если сервер станет недоступным, пользователи потеряют возможность аутентифицироваться, поэтому

чаще всего данный тип аутентификации применяется в совокупности с локальной аутентификацией, выступающей в качестве резервного метода.

Для осуществления процедуры серверной аутентификации чаще всего используются два типа протоколов: RADIUS и TACACS+. Рассмотрим работу каждого из них подробнее, выделив область применения, положительные стороны и недостатки.

3.2. Протокол RADIUS

Remote Authentication Dial-In User Service – служба удаленной аутентификации пользователей по коммутируемым линиям. Клиент-серверный протокол AAA используется для управления доступом к сетевым ресурсам. Разработан в 1991 году, стандартизирован IETF: RFC2865 Авторизация и аутентификация, RFC 2866 функциональность учета, RFC 2867, 2868 и 2869 определяют дополнительные спецификации, расширяющие возможности протокола. Широко применяется в различных сетевых сценариях, в том числе:

- предоставление доступа к Интернету провайдерами;
- обеспечение безопасного доступа к корпоративным ресурсам;
- аутентификация устройств и пользователей в беспроводных сетях.

Протокол RADIUS функционирует поверх транспортного протокола UDP на портах 1812 и 1813. UDP является протоколом без установления соединения, что обуславливает высокую скорость работы протокола и быструю пересылку клиентских запросов на резервные сервера аутентификации в случае необходимости, но затрудняет работу RADIUS в высоконагруженных сетях с низкой пропускной способностью из-за риска потери запросов. Структура пакета RADIUS, проиллюстрированная на рис. 24, состоит из пяти основных частей:

- Тип пакета (Code) – Access-Request (1)/Accept (2)/Reject (3), Accounting-Request (4)/Response (5).
- Уникальный идентификатор (Identifier) – назначается клиентом каждому запросу, используется для сопоставления с ответами сервера.
- Длина пакета (Length) – общая длина пакета в байтах, включающая в себя все поля и атрибуты.
- Аутентификатор (Authenticator) – применяется для проверки подлинности пакета. Для запросов – это случайное значение, а для ответов сервера это хэш секретного ключа, запроса и данных.
- Атрибуты – TLV, содержат дополнительную информацию: имя пользователя, зашифрованный пароль, тип услуги, идентификатор устройства и т.д.

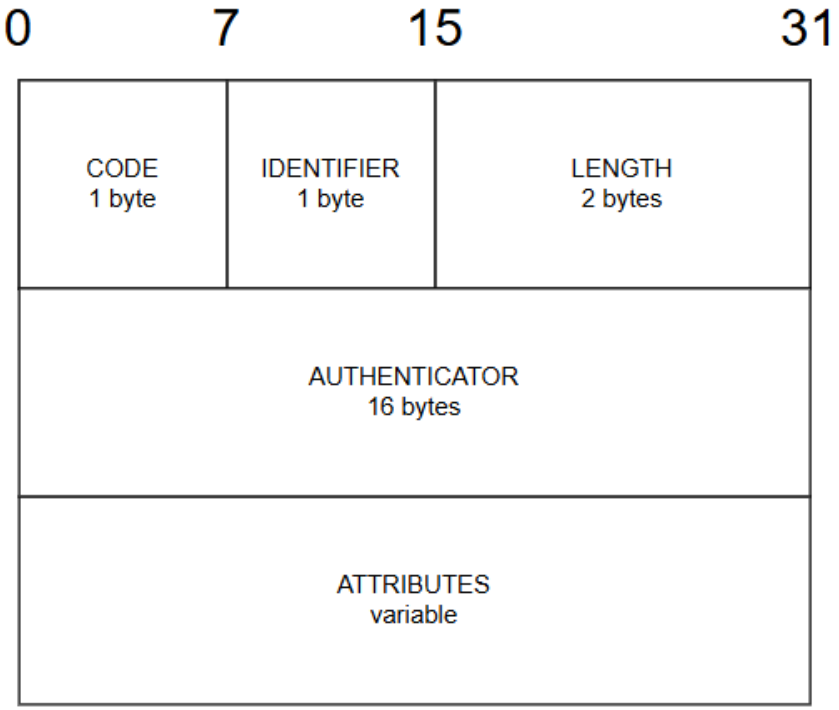


Рис. 24. Пакет RADIUS

Рассмотрим пошагово процесс аутентификации по протоколу RADIUS (рис. 25-28):

1. Ввод учетных данных суппликантом.

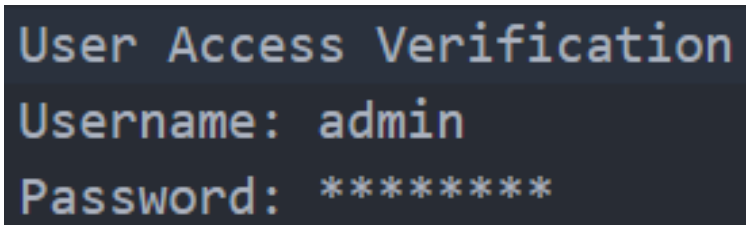


Рис. 25. Ввод логина и пароля

2. Формирование аутентификатором Access-Request и отправка запроса на сервер RADIUS.

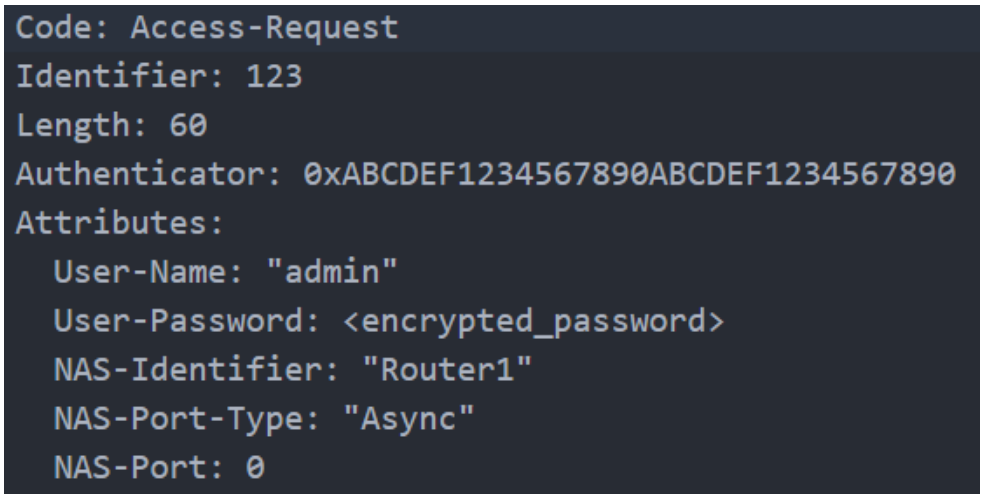


Рис. 26. Access-Request

3. Декодирование пароля секретным ключом, проверка имени пользователя и пароля с информацией в базе данных сервера, определение прав доступа.
4. Сервер отправляет ответ в зависимости от результатов проверки: в случае успеха Access-Accept, а если аутентификация не удалась – Access-Reject.

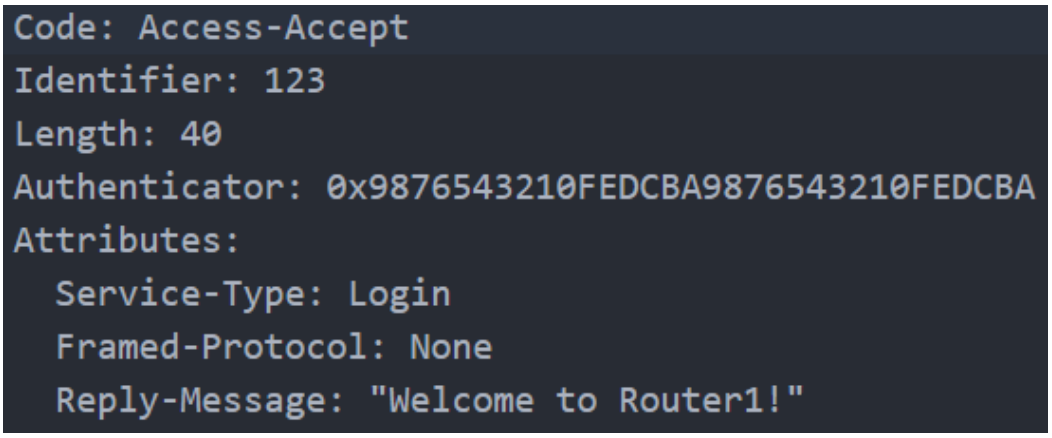


Рис. 27. Access-Accept

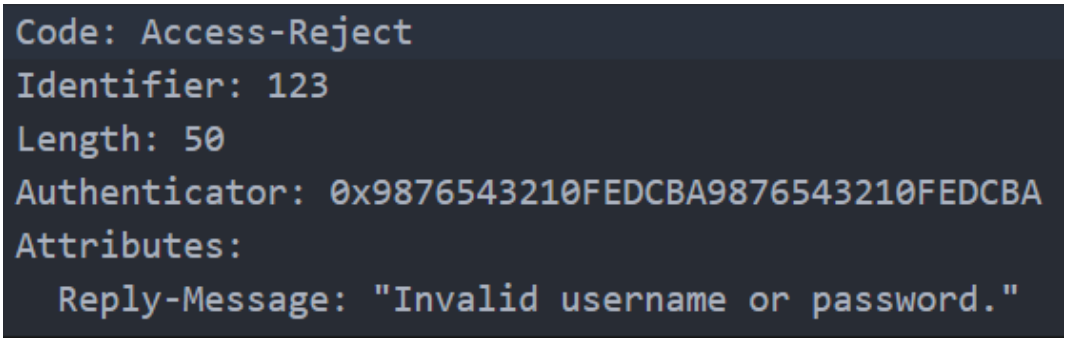


Рис. 28. Access-Reject

5. Обработка ответа аутентификатором и предоставление/не предоставление доступа супликанту.

После успешного доступа, клиент начинает процесс учета, отправляя на сервер Accounting-Request для отслеживания используемых ресурсов.

3.3. Протокол TACACS+

Terminal Access Controller Access-Control System Plus — это сетевой протокол, предназначенный для реализации функций аутентификации, авторизации и учета в сетях. Является проприетарным протоколом компании Cisco, модифицированная версия оригинального TACACS (RFC 1492). Несмотря на это, TACACS+ применяется и на устройствах других вендоров, в том числе на отечественных решениях.

Данный протокол наиболее подходит для аутентификации на сетевых устройствах за счет возможности управления доступом на уровне отдельных команд и привилегий. Работает поверх TCP на 49 порту.

Изучим структуру пакета протокола TACACS+ (рис. 29):

- Заголовок (Header) – содержит версию, тип операции (AUTHEN, AUTHOR, ACCT), номер пакета, идентификатор сессии, длину тела пакета, поле для флагов;
- Тело (Body) – содержит зашифрованные секретным ключом данные, например, имя пользователя и пароль.

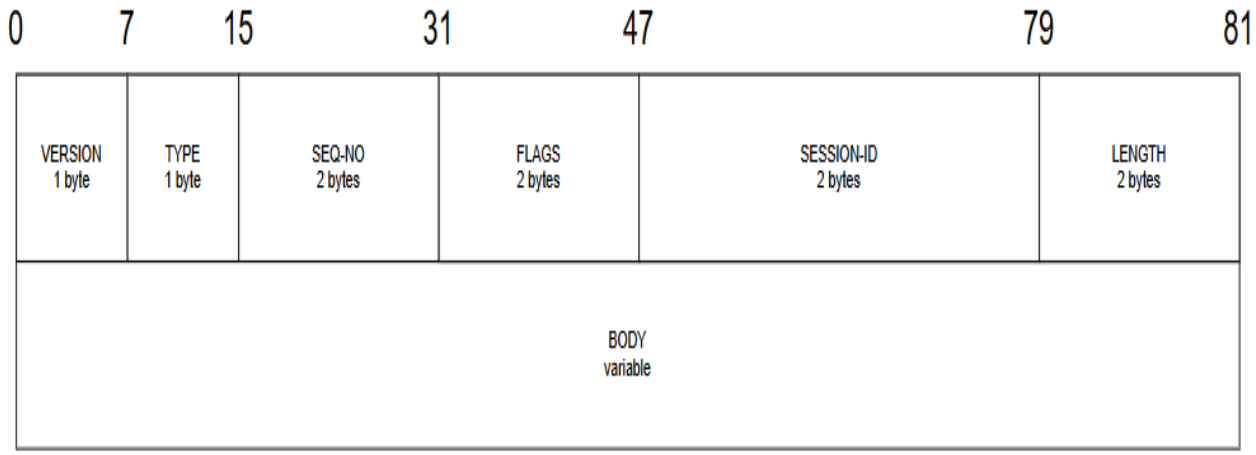


Рис. 29. Структура пакета TACACS+

Рассмотрим пошаговый процесс работы аутентификации по TACACS+ (рис. 30-33):

1. Попытка входа пользователя через консольный порт, SSH или Telnet на роутер.
2. Маршрутизатор формирует пакет AUTHEN-Request с именем пользователя.

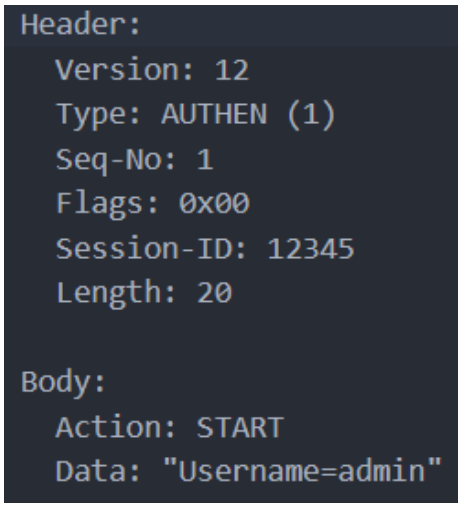


Рис. 30. Начало аутентификации

3. Сервер проверяет имя пользователя и запрашивает пароль, если они известны.

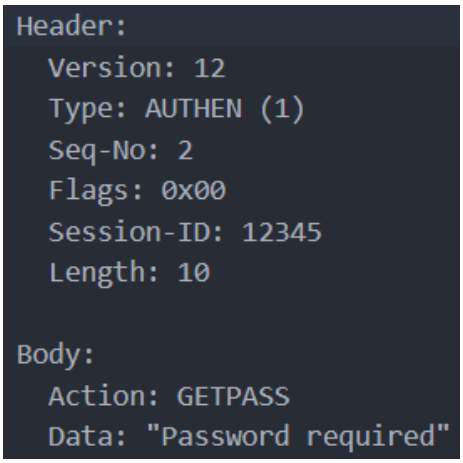


Рис. 31. Запрос пароля

4. Маршрутизатор отправляет зашифрованный пароль.

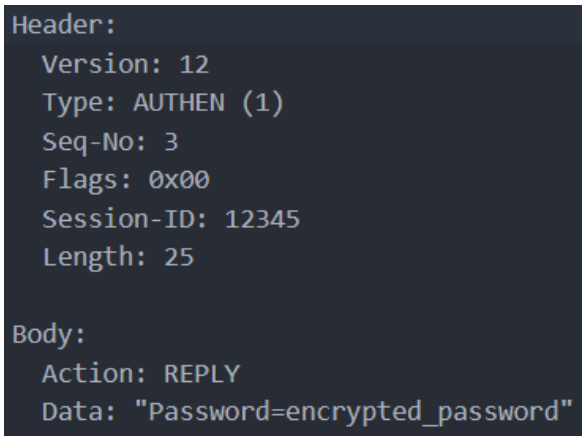


Рис. 32. Отправка пароля

5. Сервер проверяет пароль и возвращает сообщение об успешной/неуспешной аутентификации.

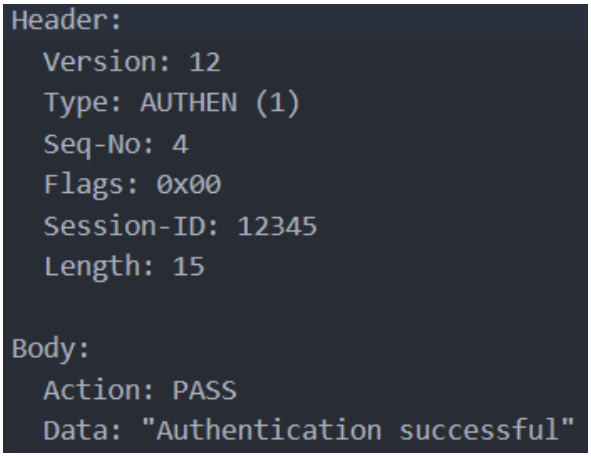


Рис. 33. Аутентификация пройдена

После успешной аутентификации сервер предоставляет список разрешенных команд или уровней привилегий, как изображено на рис. 34 и 35. Во время сеанса роутер отправляет на сервер пакеты учета ACCT-Request для отслеживания действий пользователя (рис. 36).

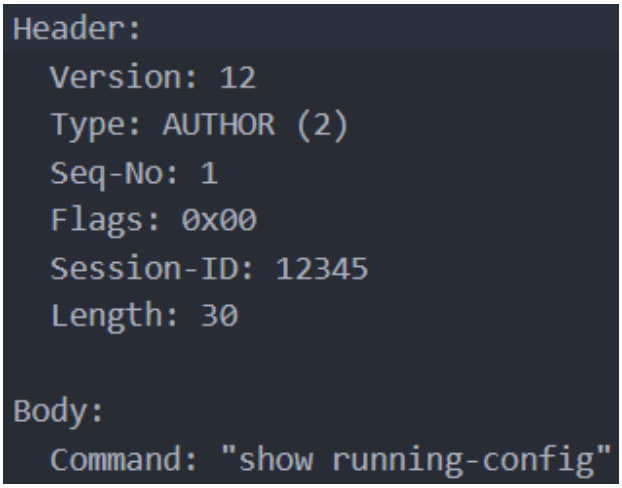


Рис. 34. Запрос на выполнение команды

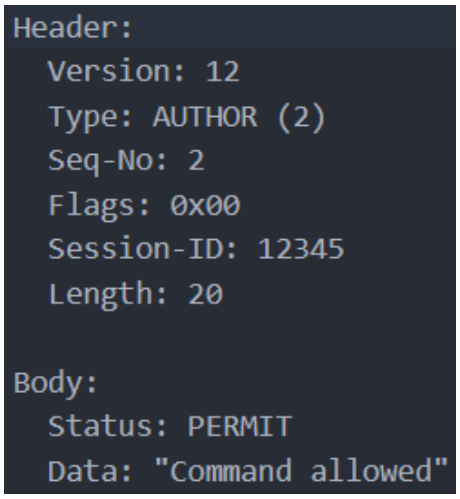


Рис. 35. Команда разрешена

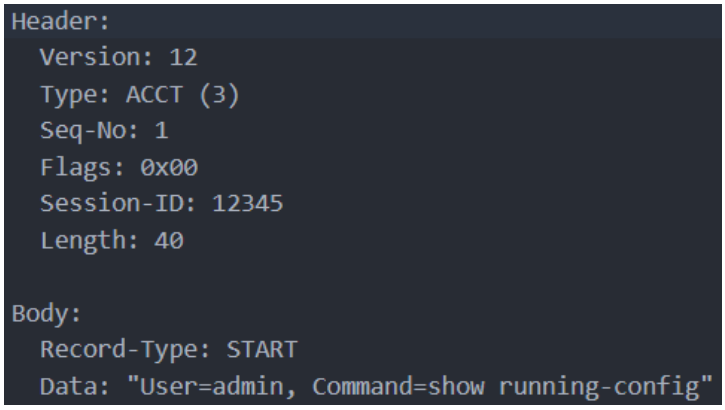


Рис. 36. Начало учета

3.4. Аутентификация по стандарту IEEE 802.1x

Стандарт IEEE 802.1X определяет механизм аутентификации устройств при их подключении к проводным и беспроводным сетям. Этот стандарт предназначен для управления доступом на канальном уровне (Layer 2) модели OSI и предотвращения несанкционированного доступа к сети.

Компоненты, входящие в стандарт 802.1X:

- EAP и методы.
- EAPoL.
- Протокол AAA (например, RADIUS).

Extensible Authentication Protocol (EAP) – протокол расширяемой аутентификации, описанный в RFC 3748, используемый в проводных и беспроводных сетях. Поддерживает различные методы передачи учетных данных пользователя, например:

- EAP-MD5 – передача пароля в виде хеша.
- EAP-TLS – использование цифровых сертификатов TLS/SSL.

- EAP-TTLS – передача учетных данных по TLS-туннелю.
- PEAP – protected EAP, модификация EAP-TLS.
- EAP-AKA – аутентификация в беспроводных сетях 3G/4G/5G.
- EAP over LAN (EAPoL) – протокол, используемый для передачи сообщений EAP между супликантом и аутентификатором на канальном уровне до получения IP-адреса. EAPoL функционирует поверх Ethernet или Wi-Fi.

Процесс получения доступа к сети по стандарту 802.1X происходит в несколько этапов (рис. 37):

1. Инициализация соединения – супликант обнаруживает сеть и отправляет EAPOL-Start на аутентификатор, запрашивая аутентификацию. Аутентификатор отвечает EAP-Request/Identity, требуя от клиента идентификационные данные.
2. Передача учетных данных – Супликант отправляет EAP-Response/Identity, содержащий имя пользователя или другой идентификатор. Аутентификатор пересылает этот запрос на Сервер аутентификации через RADIUS.
3. Выбор метода EAP и проверка данных – Сервер аутентификации выбирает метод аутентификации (например, EAP-TLS для сертификатов или PEAP для логина/пароля). В зависимости от метода Супликант отправляет дополнительные данные (пароль, сертификат). Сервер проверяет учетные данные в базе данных.
4. Принятие решения об аутентификации – если проверка успешна, сервер отправляет EAP-Success через Аутентификатор клиенту. Если проверка не пройдена, сервер отправляет EAP-Failure.
5. Предоставление доступа – если аутентификация успешна, Аутентификатор разрешает доступ в сеть, изменяя состояние порта с "Unauthorized" на "Authorized". Если аутентификация не удалась, клиент не получает сетевой доступ.

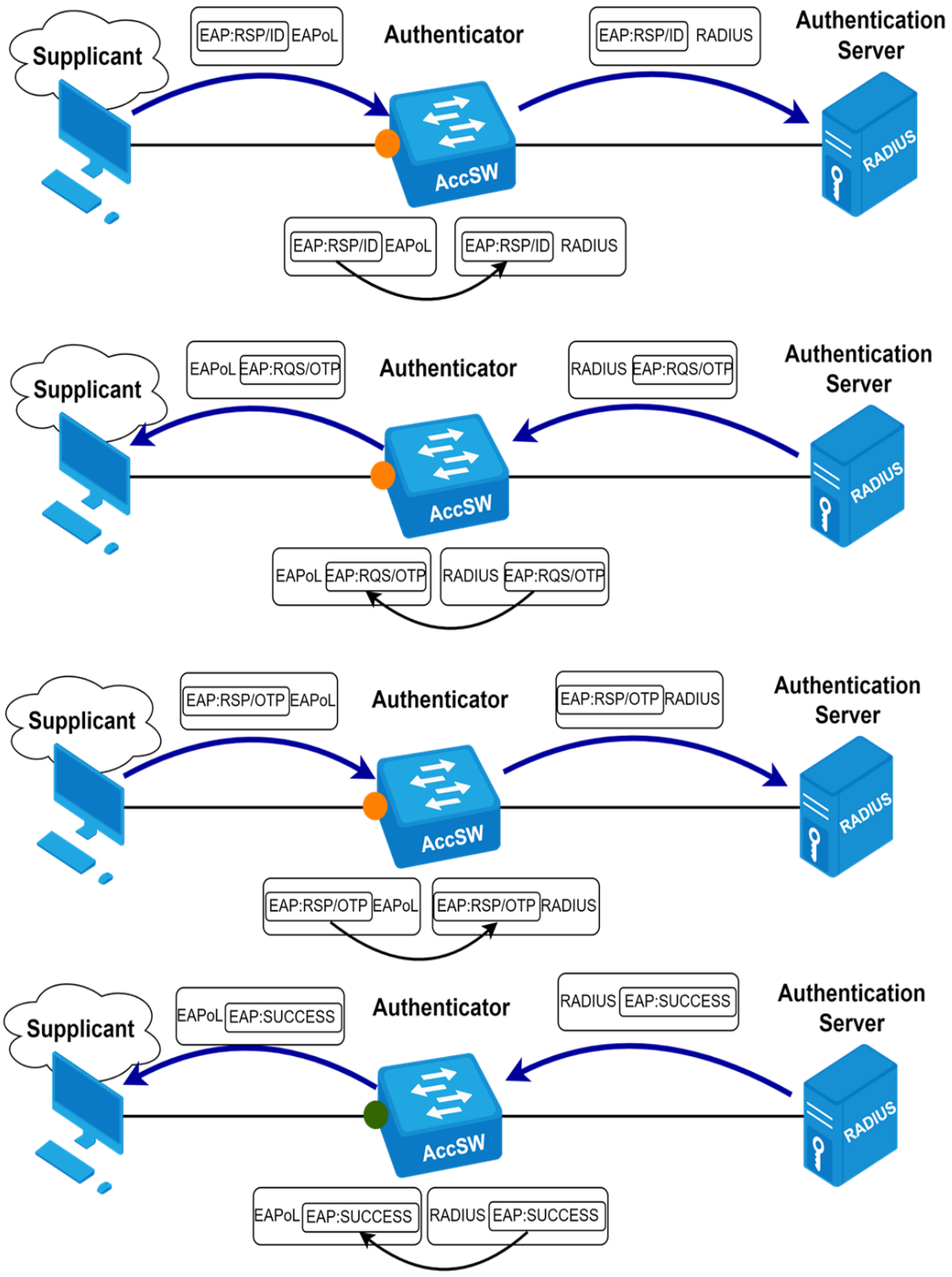


Рис. 37. Получение доступа к сети по стандарту 802.1x

Для предоставления ограниченного доступа неаутентифицированным или неизвестным пользователям, существует возможность настройки гостевой VLAN (guest VLAN). Это специальная отдельная VLAN, изолированная от корпоративной сети, в которую автоматически помещаются неаутентифицированные пользователи, не получившие доступ по 802.1X.

Обмен идентификаторами EAP и аутентификации происходят между запрашивающей стороной и сервером аутентификации. Аутентификатор не знает, какой тип EAP используется; он просто берет EAPoL кадр от заявителя и инкапсулирует его в RADIUS пакет, отправляет на сервер аутентификации, а затем открывает порт, если сервер аутентификации возвращает его. Следовательно, аутентификация EAP полностью прозрачна для аутентификатора.

3.5. MAC Authentication Bypass

MAC Authentication Bypass (MAB) – это механизм аутентификации устройств в сетях 802.1X, который позволяет обходить EAP-аутентификацию и предоставлять доступ на основе MAC-адреса устройства.

MAB используется для устройств, которые не поддерживают 802.1X, например: IP-телефоны, принтеры и камеры видеонаблюдения, IoT-устройства. Если конечное устройство не поддерживает аутентификацию 802.1X, коммутатор может идентифицировать его по MAC-адресу и разрешить доступ на основе списка доверенных MAC-адресов.

Алгоритм работы MAB можно описать в три этапа (рис. 38):

1. Коммутатор инициирует аутентификацию, отправив сообщение запроса идентификации EAPoL на конечную точку каждые 30 секунд по умолчанию. После трех таймаутов (по умолчанию 90 секунд) коммутатор определяет, что конечная точка не поддерживает 802.1X и переходит к аутентификации через MAB.
2. Коммутатор начинает MAB, открывая порт для приема одного пакета, от которого узнает исходный MAC-адрес конечной точки. После того, как коммутатор узнает MAC-адрес источника, он отбрасывает пакет. Формируется сообщение запроса доступа RADIUS с использованием MAC-адреса конечной точки в качестве идентификатора. Сервер RADIUS получает сообщение запроса доступа и выполняет аутентификацию по MAC.
3. Сервер RADIUS определяет, следует ли предоставить устройству доступ к сети и с каким уровнем. Сервер отправляет ответ access-accept аутентификатору, разрешая конечной точке доступ к сети.

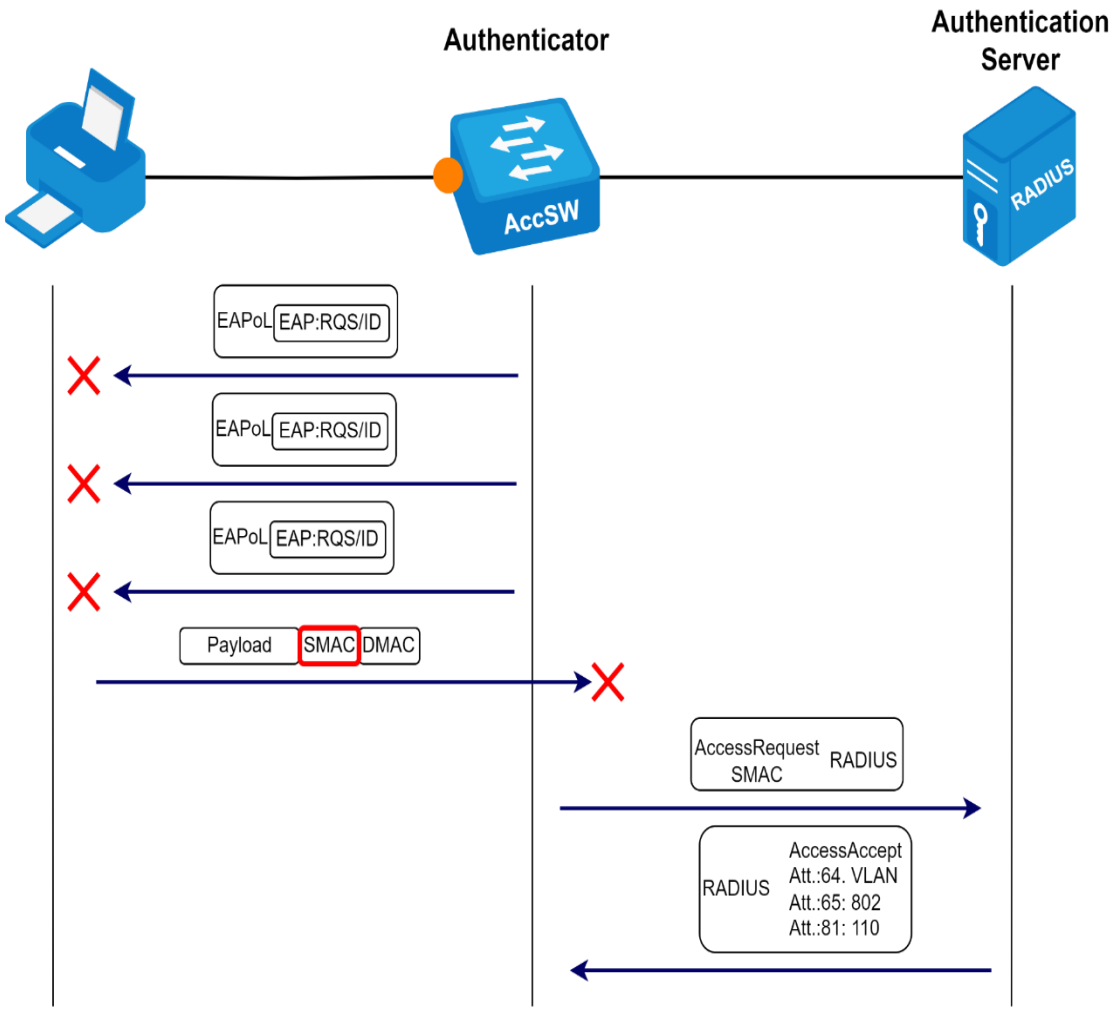


Рис. 38. Получение доступа к сети с помощью MAB

Контрольные вопросы

Почему у протоколов AAA такое название?
Что подразумевает термин «аутентификация»?
Назовите цель аутентификации.
Что может выступать в качестве аутентификационной информации?
Что подразумевает термин «авторизация»?
На каком основании могут быть определены права доступа?
Какие уровни привилегий могут быть получены пользователями в процессе авторизации на сетевом оборудовании Eltex?
Как называется процесс сбора информации о действиях клиента?
Сколько существует режимов работы механизмов AAA?
Какой режим AAA наиболее подходит для небольших сетей?
Какие недостатки у локальной аутентификации?
В каких сетях применяется серверная аутентификация?
Что такое сервер аутентификации?
Что такое аутентификатор?

Что подразумевает термин «супликант»?
Какая модель аутентификации позволяет обеспечить централизованное управление сетевым доступом для всех узлов сети, не теряя возможности в гибкости и масштабируемости, но требует настройки соответствующих протоколов на клиенте и сервере?
Какие протоколы чаще всего используются для осуществления процедуры серверной аутентификации?
Как работает протокол Remote Authentication Dial-In User Service?
В каких сетевых сценариях применяется протокол Remote Authentication Dial-In User Service?
Из каких основных частей состоит структура пакета RADIUS?
Как происходит процесс аутентификации по протоколу RADIUS?
Что такое Terminal Access Controller Access-Control System Plus?
Какой протокол наиболее подходит для аутентификации на сетевых устройствах за счет возможности управления доступом на уровне отдельных команд и привилегий?
Из каких основных частей состоит структура пакета протокола TACACS+?
Как происходит процесс аутентификации по протоколу TACACS+?
В каких сетях (проводных, беспроводных) применяется протокол Extensible Authentication Protocol (EAP)?
Какие методы передачи учетных данных пользователя поддерживает протокол Extensible Authentication Protocol (EAP)?
Как происходит процесс получения доступа к сети по стандарту 802.1X?
Как предоставляется ограниченный доступ неаутентифицированным или неизвестным пользователям по стандарту 802.1X?
Какой механизм аутентификации устройств используется в сетях 802.1X, который позволяет обходить EAP-аутентификацию и предоставлять доступ на основе MAC-адреса устройства?
Опишите принцип работы механизма MAC Authentication Bypass (MAB).

4. МЕЖСЕТЕВОЙ ЭКРАН НА ОСНОВЕ ЗОН

4.1. Межсетевые экраны

Для обеспечения защиты корпоративного сегмента сети от проникновения извне используются межсетевые экраны или Firewall. В данной главе рассмотрены принципы функционирования межсетевых экранов и порядок обработки трафика с помощью правил.

Межсетевой экран (firewall) — это программное или аппаратное решение, предназначенное для контроля и фильтрации сетевого трафика между различными сетями или частями одной сети. Сама идея обеспечения периметральной сетевой безопасности с помощью межсетевого экрана возникла в 80-х годах прошлого столетия, тогда же на рынок попал первый коммерческий межсетевой экран SEAL от компании DEC (Digital Equipment Corporation). Спустя почти 40 лет, технологии шагнули далеко вперед, на сегодняшний день существуют технические решения, совмещающие в себе возможности классических межсетевых экранов и систем обнаружения/предотвращения вторжений.

4.1.1 Принципы работы Firewall

Приведем общую идею функционирования такого механизма, как межсетевой экран. Основная цель – обеспечить разграничение движения трафика между сетями или сегментами сетей. Суть заключается в том, чтобы анализировать каждый пакет данных, проходящий через него, и принимать решение о его пропуске или блокировке на основании политик. В зависимости от поколения, межсетевой экран работает на разных уровнях модели OSI и обеспечивает разную полноту функционала. Рассмотрим алгоритм работы типового межсетевого экрана (рис. 39):

1. Получение пакета.
2. Анализ заголовка в соответствии с правилами – если пакет удовлетворяет первому правилу, проверка продолжается по остальным правилам, в ином случае пакет отбрасывается.
3. Если ни одно правило из списка не выполняется – применяется действие по умолчанию. Чаще всего это блокировка, в соответствии с принципом «запрещено все, что явно не разрешено».
4. Если пакет был «одобрен», он передается дальше в сеть.

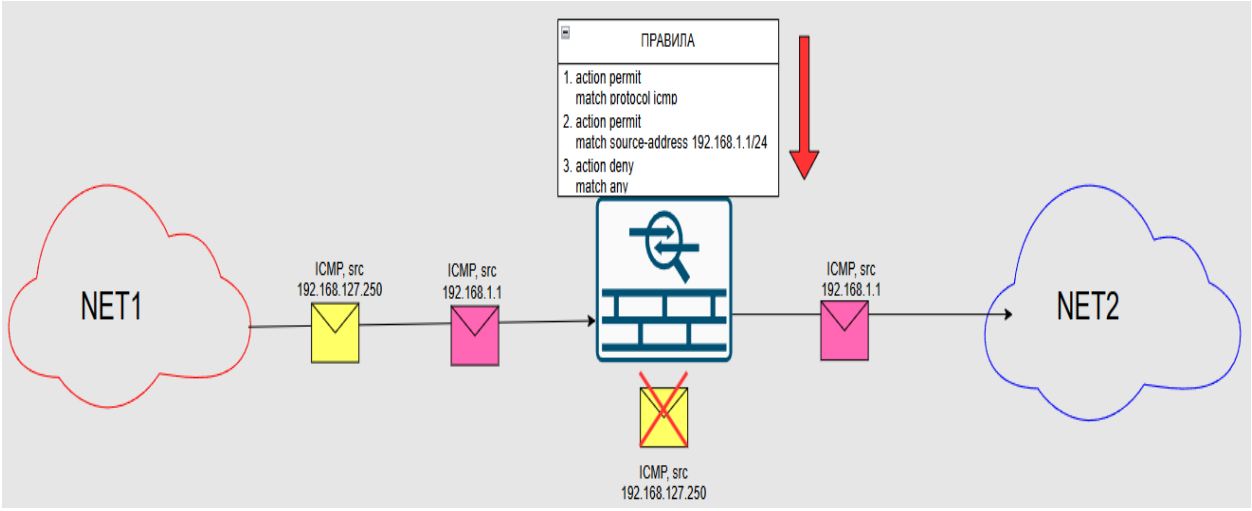


Рис. 39. Алгоритм работы МСЭ

4.1.2. Поколения и типы МСЭ

Проследим развитие технологий межсетевых экранов, их преимущества, недостатки, отличия и модели применения.

Первым поколением межсетевых экранов считаются пакетные фильтры. Это самое базовое и простое решение, работающее на сетевом и транспортном уровнях модели OSI, фильтруя поступающие пакеты на основе содержимого заголовков: IP-адресов источника и назначения, типа протокола (TCP, UDP, ICMP) и номеров портов (рис. 40).

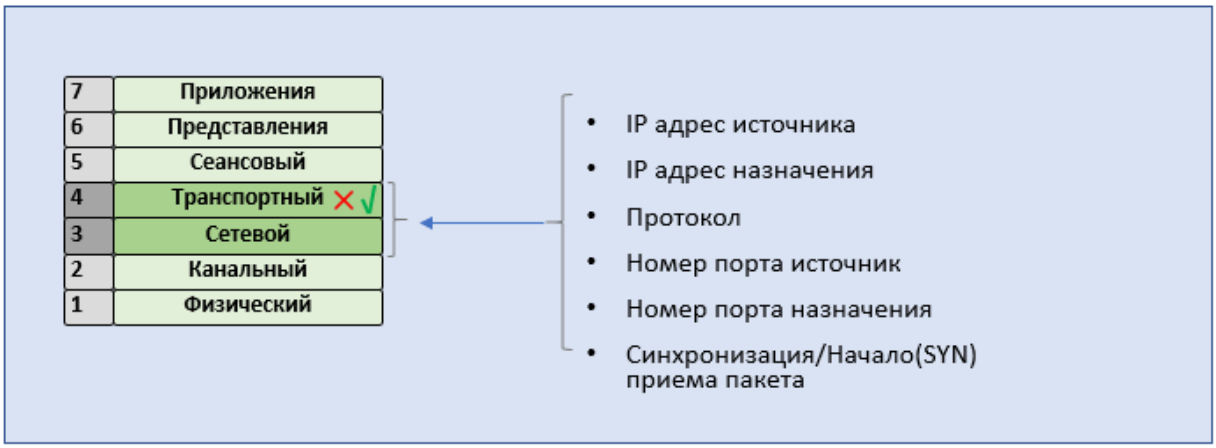


Рис. 40. МСЭ с фильтрацией пакетов

Межсетевой экран осуществляет проверку каждого пакета по списку правил. Как только найдено подходящее правило, применяется указанное действие (пропустить или отбросить). Если пакет не подошел ни под одно правило, то выполняется действие по умолчанию. Преимуществом использования пакетных фильтров является высокая производительность (так как анализируется только заголовок пакета), простота реализации и низкая

стоимость, что позволяет применять данную технологию не в виде специальных аппаратных средств, а как элемент операционной системы маршрутизатора или коммутатора, существенно экономя ресурсы на оборудовании. Однако, отсутствие анализа состояния соединений (например, TCP-сессии) и содержимого пакетов, в современных сетевых инфраструктурах позволяет злоумышленнику выполнить некоторые виды DoS-атак (например, SYN-flood) или отправить вредоносную нагрузку через разрешенный канал (рис. 41).

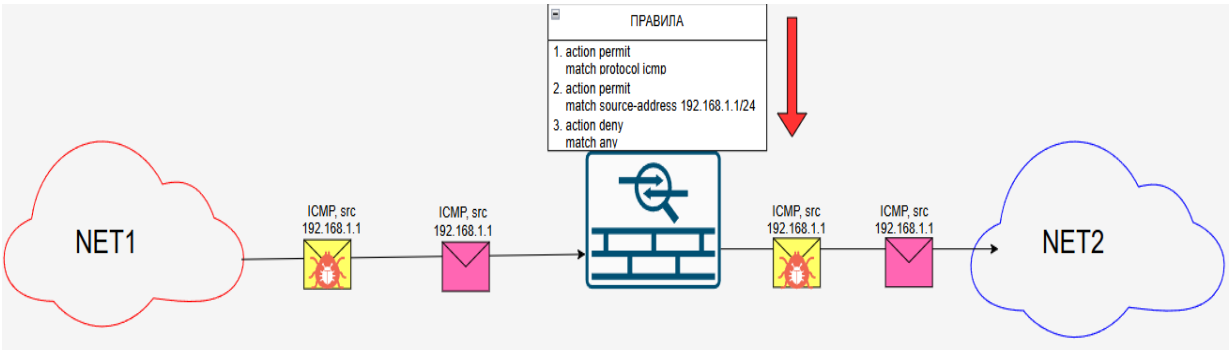


Рис. 41. Пакетная фильтрация

Второе поколение МСЭ связано с появлением технологии отслеживания состояния соединения – Stateful Inspection. Данный тип МСЭ работает на уровнях 3, 4 и 5 модели OSI, и, в отличие от пакетной фильтрации, отслеживают состояние соединений, что позволяет предотвращать более сложные сетевые атаки (рис. 42).



Рис. 42. Уровни работы МСЭ с сохранением состояния

Например, клиент установил TCP-соединение с сервером, межсетевой экран в таком случае запоминает эту сессию и автоматически пропускает все связанные с ней пакеты без повторной проверки. Также анализируется

корректность TCP-handshake (SYN и FIN пакеты) на предмет подозрительных или неправильно сформированных пакетов, даже если они соответствуют правилам. Это достигается за счет введения таблицы состояний: когда приходит запрос на установление сессии (например, TCP-SYN), МСЭ создает запись в таблице – IP, порт, протокол, текущее состояние. Если приходит SYN-пакет без предварительного запроса на установление подключения, это считается атакой. Когда соединение завершается (получен TCP-FIN), запись удаляется из таблицы состояний (рис. 43). Несмотря на значительные преимущества в области защиты от сетевых атак, такая технология требует дополнительных ресурсов процессора и все еще неспособна анализировать содержимое пакетов на прикладном уровне.

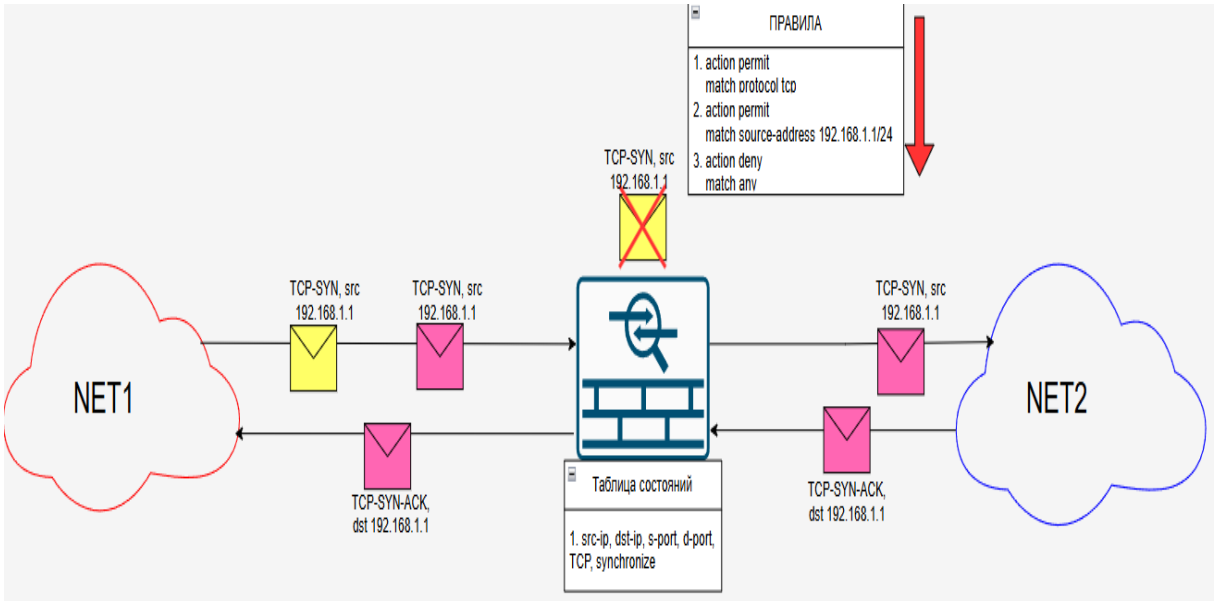


Рис. 43. МСЭ с отслеживанием состояния соединения

Следующим поколением межсетевых экранов принято считать прикладные шлюзы (Application Gateway). Целью данной технологии является устранение тянущегося с предыдущих поколений недостатка – отсутствия анализа содержимого пакетов. За счет того, что в архитектуру данного типа МСЭ включен прикладной уровень (7) модели OSI, эту проблему удалось решить, проверяя протоколы высокого уровня, такие как HTTP, FTP, SMTP и другие. МСЭ, например, может проверять URL-адреса, методы запросов HTTP или обнаруживать и предотвращать атаки типа SQL-injection, XSS, CSRF и другие уязвимости на прикладном уровне. В связи с этим данное техническое решение часто работает как прокси-сервер, анализируя запросы клиентов и пересылая их дальше после проверки (рис. 44). Из недостатков можно выделить низкую производительность и ограниченную масштабируемость в условиях высоконагруженных сетей.

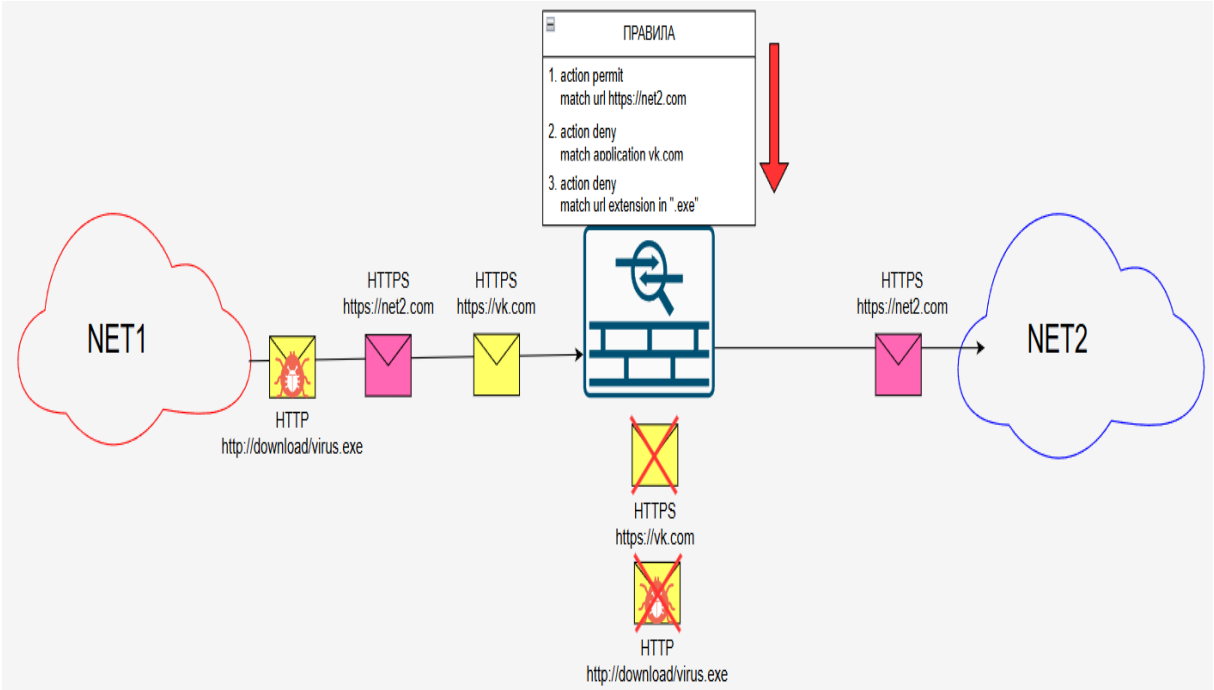


Рис. 44. МСЭ уровня приложений

4.2. Способы применения межсетевых экранов в архитектуре сети

Существует несколько подходов к размещению межсетевых экранов в сетевой архитектуре. Разберем основные использующиеся топологии.

Самая простая архитектура – разделение внутренней и внешней сети. В таком случае инспектируется входной и выходной трафик между Internet и LAN (рис. 45). Недостатком данной топологии является размещение сервисов с легитимным публичным доступом во внутренней части корпоративной сети.

Подход с организацией демилитаризованной зоны (DMZ) позволяет нивелировать недостатки предыдущей архитектуры. DMZ представляет собой изолированную сеть, в которой размещаются публичные сервисы, такие, как веб-серверы, почтовые серверы. Межсетевой экран инспектирует трафик между тремя зонами: LAN, WAN и DMZ. В таком случае трафик из внешней сети может проходить только в демилитаризованную зону, трафик из DMZ в локальную сеть строго инспектируется, а трафик из внутренней сети может проходить в DMZ и WAN в соответствии с правилами (рис. 46). При такой архитектуре, даже в случае компрометации публичных сервисов, безопасность корпоративной сети остается на высоком уровне.

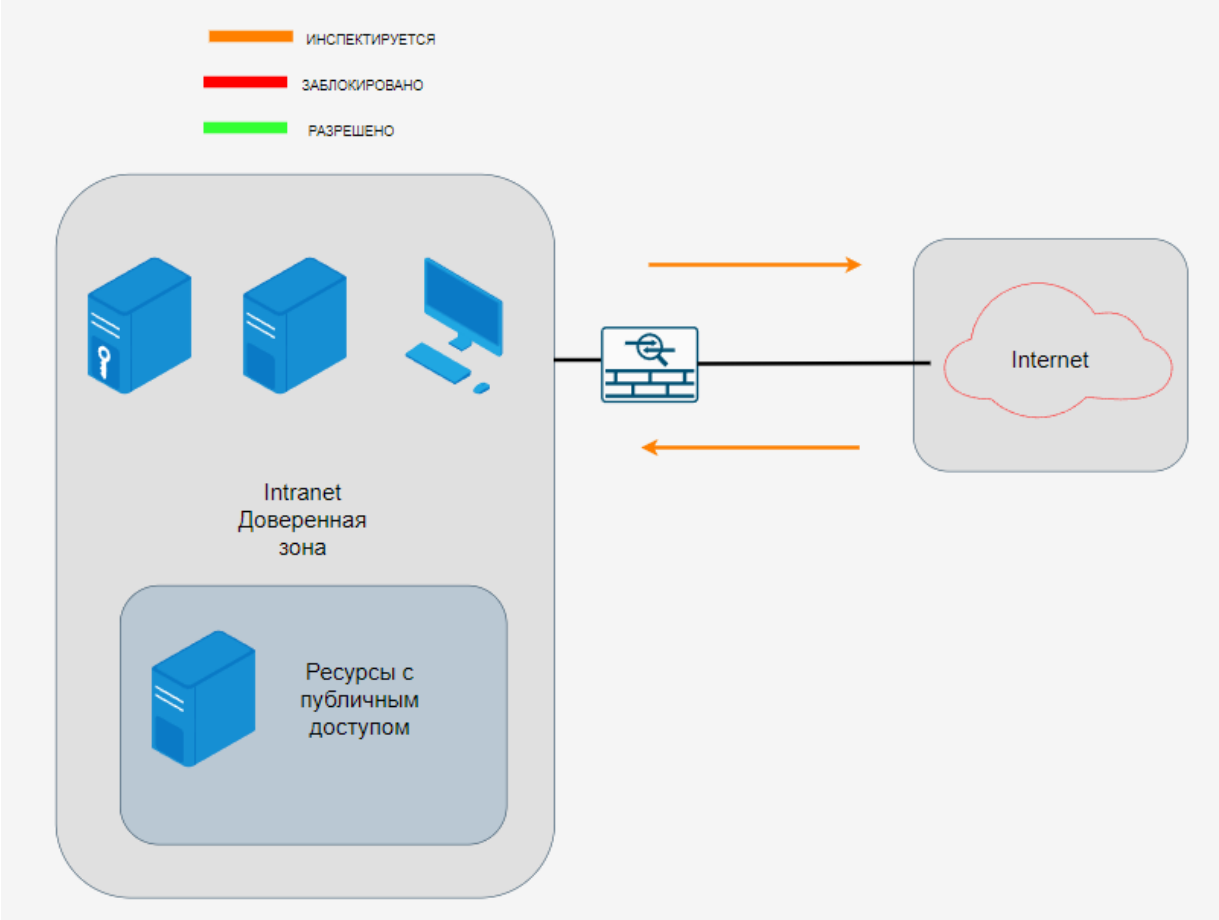


Рис. 45. Архитектура с внутренней и внешней сетью

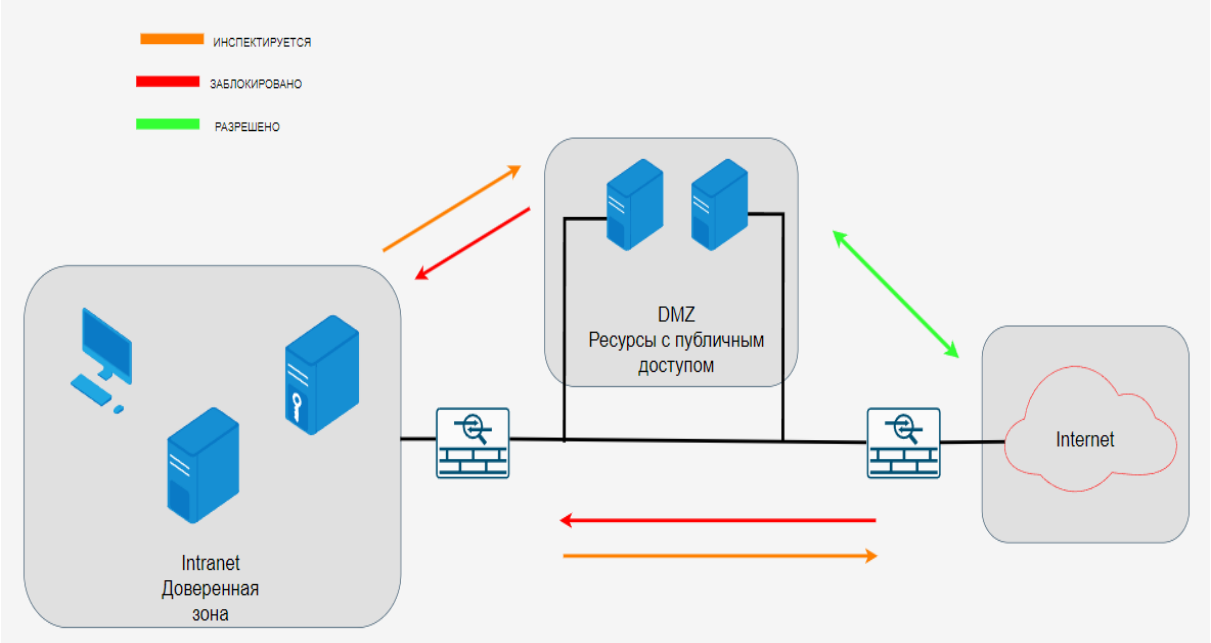


Рис. 46. Архитектура с демилитаризованной зоной

Наиболее современный и безопасный подход в сетевой архитектуре с использованием МСЭ – это зональный межсетевой экран (Zone-based Policy

Firewall). Такая модель реализует принцип микросегментации концепции Zero Trust и позволяет применять собственные политики взаимодействия зон, тщательно организуя разграничение доступа. Это достигается за счет разделения внутренней сети на несколько логических зон (например, отделы по направлениям деятельности) и применения правил межзонового взаимодействия (рис. 47), воздействуя на весь трафик между зонами, без необходимости применения множества правил инспектирования. Например, разрешить прохождение трафика между IT- и финансовым отделом для почтовых приложений.

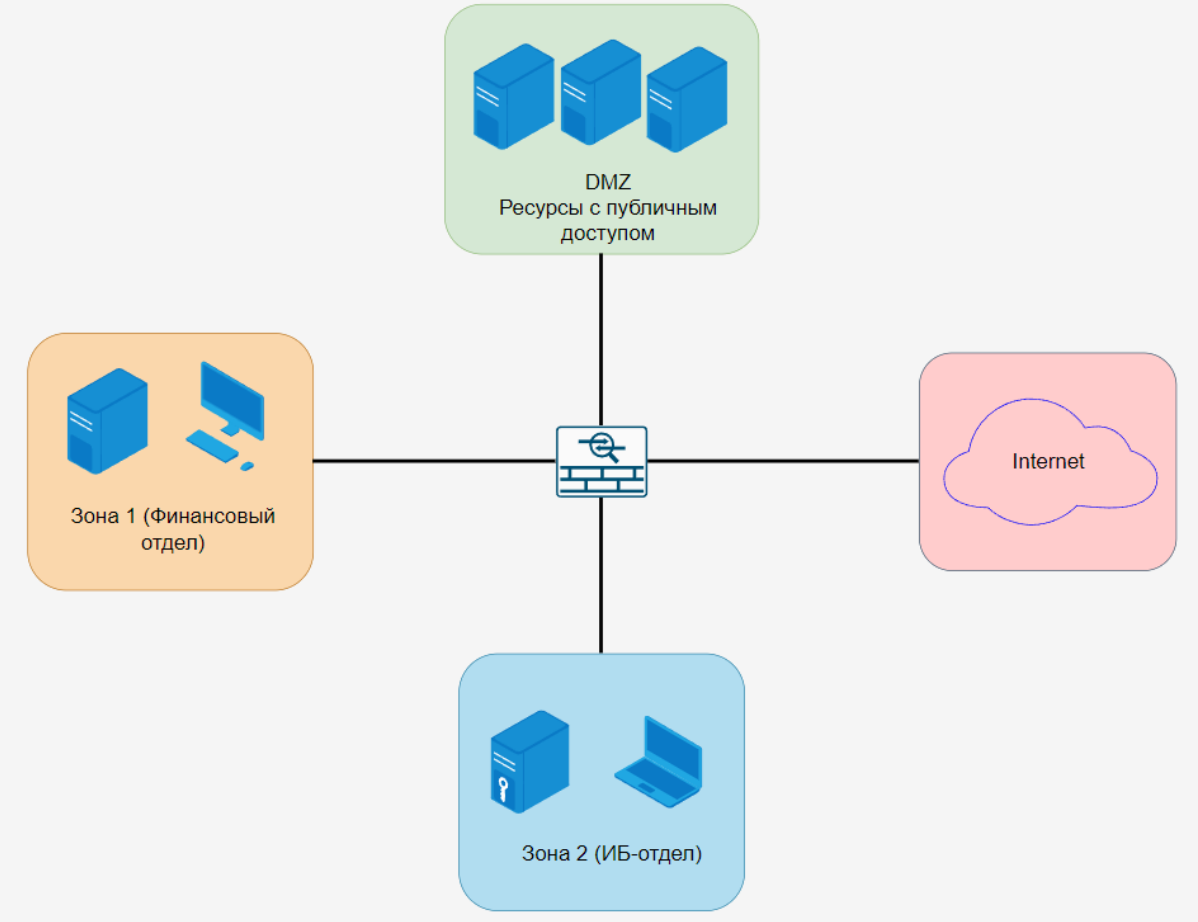


Рис. 47. Зональный межсетевой экран

Контрольные вопросы

Что такое межсетевой экран (firewall)?
Какова цель использования межсетевых экранов или Firewall?
Когда появился первый коммерческий межсетевой экран? Назовите компанию, которая его выпустила.
На каких уровнях модели OSI работает межсетевой экран?
Приведите алгоритм работы типового межсетевого экрана.
Что можно назвать первым поколением межсетевых экранов?

На каких уровнях модели OSI работало первое поколение межсетевых экранов?
На основе содержимого каких заголовков фильтровало поступающие пакеты первое поколение межсетевых экранов?
В чем преимущества использования пакетных фильтров?
Назовите недостатки применения пакетных фильтров.
На каких уровнях модели OSI работало второе поколение межсетевых экранов?
В чем отличие второго поколения межсетевых экранов от первого?
Какие атаки предотвращаются при использовании второго поколения межсетевых экранов в отличие от первого?
Какие недостатки у технологии второго поколения межсетевых экранов?
Какова цель технологии прикладных шлюзов (Application Gateway)?
Что могут проверять прикладные шлюзы (Application Gateway)?
Какие недостатки у прикладных шлюзов?
Какие подходы существуют к размещению межсетевых экранов в сетевой архитектуре?
Что является недостатком при разделении внутренней и внешней сети, когда инспектируется входной и выходной трафик между Internet и LAN?
Как подход с организацией демилитаризованной зоны (DMZ) позволяет нивелировать недостатки самой простой архитектуры?
Что считается наиболее современным и безопасным подходом в сетевой архитектуре с использованием межсетевых экранов?
В чем достоинства наиболее современного и безопасного подхода в сетевой архитектуре с использованием межсетевых экранов?

5. ПРОТОКОЛ IPSEC И ПОСТРОЕНИЕ VPN ТУННЕЛЕЙ

5.1. Способы организации изолированных каналов связи

В процессе эксплуатации крупной распределенной сетевой инфраструктуры актуальным становится вопрос безопасной передачи данных между сегментами сети одной организации или организации защищенного удаленного доступа для пользователей. В зависимости от материальных возможностей и требований к соединению существует несколько вариантов обеспечения защищенного канала передачи данных:

1. Создание физического канала (витая пара, оптоволоконные линии, радиорелейные линии).
2. Аренда канала передачи у провайдера (физический канал, VPN решения на уровне L2 и L3 с использованием технологии мультипротокольной коммутации по меткам - MPLS).
3. Туннель через публичную сеть.

Первые два варианта будут актуальны для крупных организаций с большими финансовыми возможностями, поэтому подробнее рассмотрим третье решение, как самое экономичное.

Туннелирование в компьютерных сетях – это процесс создания логического канала связи между двумя точками посредством инкапсуляции одного сетевого протокола в другой. В общем виде структура туннеля представляет собой:

1. инициатор туннеля – устройство, инкапсулирующее пакеты локальной сети в новый заголовок;
2. терминатор – устройство, выполняющее процесс обратной инкапсуляции, удаляет новые заголовки и направляет исходные пакеты адресатам в локальной сети;
3. маршрутизируемая сеть между этими устройствами.

В качестве инициатора и терминатора чаще всего выступают маршрутизаторы на границе между локальной и глобальной сетью. Основное требования при организации данного решения – наличие публичных адресов на двух концах туннеля. Самым простым протоколом туннелирования является GRE (Generic Routing Encapsulation, RFC 2784) – исходный IP-пакет помещается в GRE-заголовок и передается через публичную сеть с новым IP-заголовком (рис. 48).

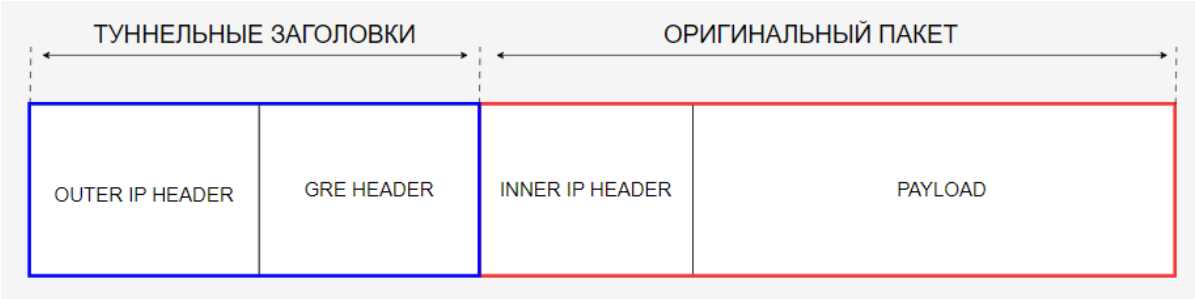


Рис. 48. GRE-пакет

На принимающей стороне маршрутизатор проверяет внешний IP-заголовок на соответствие, что пакет адресован именно ему. Далее извлекается GRE-заголовок и проверяются его параметры (например, тип инкапсулируемого протокола), затем внешние заголовки удаляются и исходный пакет передается в соответствии с изначальным IP-заголовком по локальной сети.

Главным недостатком данного решения является отсутствие защиты при передаче пакетов через GRE-туннель: шифрование и аутентификация исходных пакетов не обеспечивается. Эту проблему призван решить стандарт IPsec, который будет рассмотрен далее.

5.2. Стек протоколов IPsec

5.2.1. Структура стека протоколов IPsec

IPsec — это набор протоколов, которые обеспечивают защиту передаваемых с помощью IP-протокола данных. Данный набор протоколов позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и шифрование IP-пакетов, а также включает в себя протоколы для защищенного обмена ключами в сети Интернет. Компонентами данного набора являются протоколы (рис. 49-50):

- AH (Authentication Header, RFC 4302) – используется для обеспечения аутентификации и целостности пакета, добавляя аутентификационный заголовок к каждому передаваемому пакету, проверяя подлинность отправителя и корректность содержимого, а также защиту от автоповтора. Применяемые протоколы аутентификации: md5, sha1/2-256/2-384/2-512;
- ESP (Encapsulating Security Payload, RFC 4303) – протокол, обеспечивающий шифрование полезной нагрузки пакета, аутентификацию, проверку целостности пакета и защиту от автоповтора. Применяемые криптографические протоколы: des, 3des, desx, aes128/192/256;
- IKE (Internet Key Exchange) – протокол обмена ключами, применяемый для согласования работы участников защищенного соединения (IPsec Security Association).

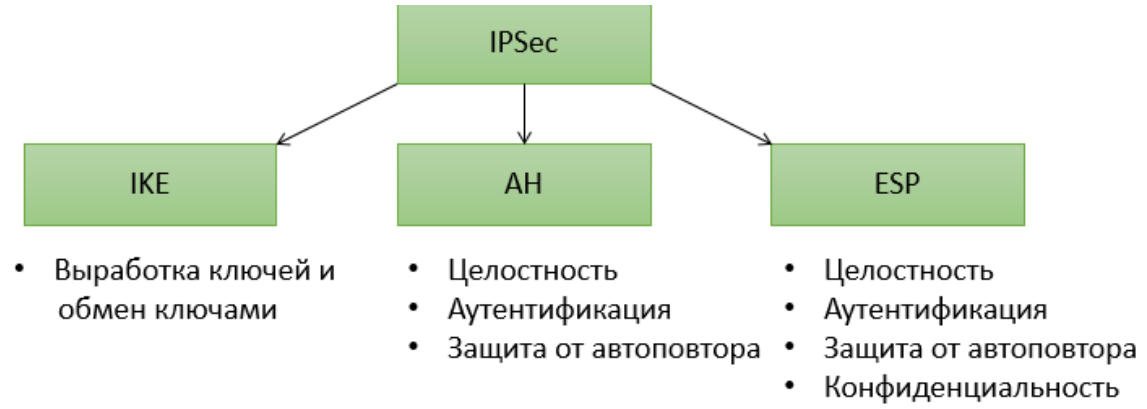


Рис. 49. Структура IPsec

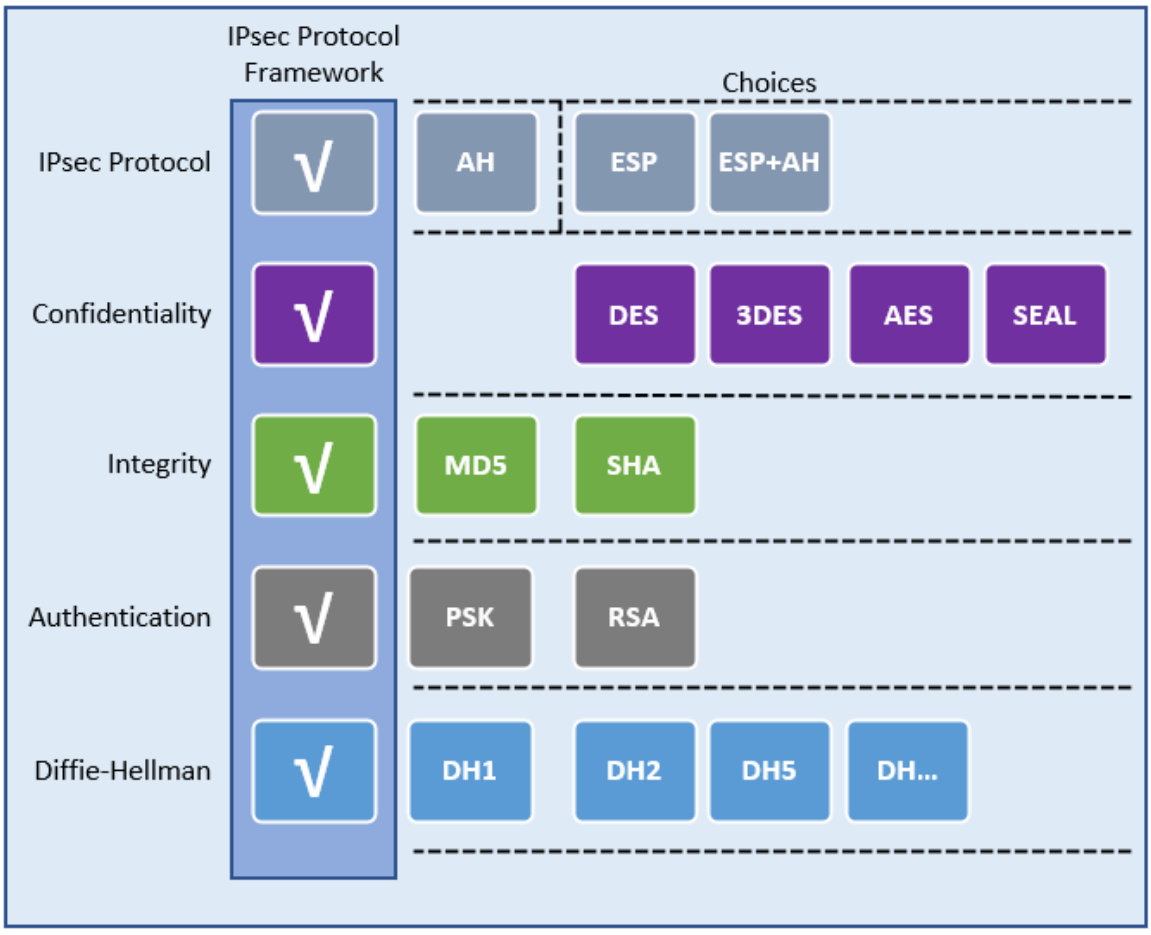


Рис. 50. Структура IPsec

Детальнее изучим процесс установления соединения в IPsec. Для начала подробнее рассмотрим протокол обмена ключами, с помощью которого и происходит согласование параметров участников (рис. 51).

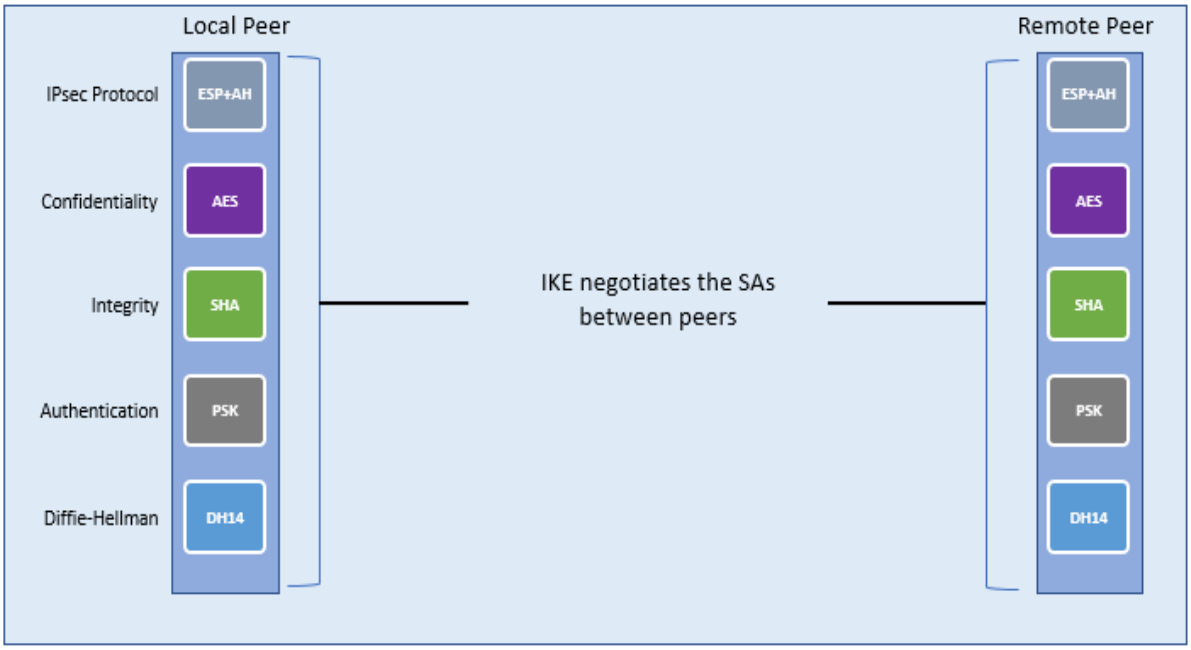


Рис. 51. Согласование параметров IPsec

Существует две версии IKE.

IKEv1 – первая версия, разработанная в 1998 году (описан в RFC 2409), работает в два этапа – создание канала управления ISAKMP SA и IPsec SA для передачи данных. Диалог двух участников защищенного соединения состоит из девяти частей:

Первая фаза

1. Клиент А предлагает параметры протоколов Клиенту В для создания ISAKMP (IKE_SA Proposal Request);
2. Клиент В принимает предложенные параметры (IKE_SA Proposal Response);
3. Клиент А отправляет Клиенту В открытый ключ DH (Key Exchange Request);
4. Клиент В отправляет Клиенту А открытый ключ DH (Key Exchange Response);
5. Клиент А отправляет аутентификационную информацию Клиенту В (Auth Request);
6. Клиент В отправляет аутентификационную информацию Клиенту А (Auth Response).

Первая фаза завершена.

Вторая фаза

7. Клиент А предлагает Клиенту В параметры туннеля IPsec SA (IPsec Proposal Request);
8. Клиент В принимает предложенные параметры (IPsec Proposal Response);
9. Клиент А обменивается подтверждениями с Клиентом В (IPsec Auth & Key Confirmation).

Канал готов к передаче данных.

Также для установления соединения существует Aggressive mode. Он сокращает число сообщений до трех за счет передачи большего количества информации в одном сообщении:

- В первом сообщении от инициатора передаются предлагаемые криптографические параметры, DH и ID.
- Во втором сообщении сервер отвечает выбранными параметрами, DH, также может быть отправлен запрос на аутентификацию.
- В последнем сообщении инициатор подтверждает аутентификацию.

Данный способ является менее безопасным, так как наиболее уязвим к MITM-атакам на ранних этапах из-за аутентификации на последнем шаге установления соединения.

Главными недостатками первой версии является громоздкий процесс установления соединения, наличие отдельного протокола для управления (ISAKMP) и отсутствие поддержки работы с NAT.

IKEv2 разработан в 2005 году (описан в RFC 7296, последнее обновление было получено в 2014). С его помощью произошло избавление от ключевых недостатков первой версии – поддержка NAT-Traversal, объединение двух фаз установления соединения с сокращением числа сообщений до четырех. Также появилась поддержка технологии MOBIKE, позволяющей изменять IP-адреса клиентов без разрыва защищенного соединения, что нашло применение в беспроводных сетях и мобильных устройствах. Диалог двух клиентов, устанавливающих соединение с помощью IKEv2 (рис. 52):

1. Клиент A отправляет Клиенту B сообщение IKE_SA_INIT Request с параметрами аутентификации и шифрования;
2. Клиент B соглашается на предложенные параметры и отправляет свои в ответ IKE_SA_INIT Response;
3. Клиент A отправляет Клиенту B IKE_AUTH Request со своим идентификатором, аутентификационной информацией, параметрами будущего IPsec SA;
4. Клиент B отправляет Клиенту A IKE_AUTH Response со своим идентификатором, аутентификационной информацией и выбранными параметрами IPsec SA с заключительным подтверждением.

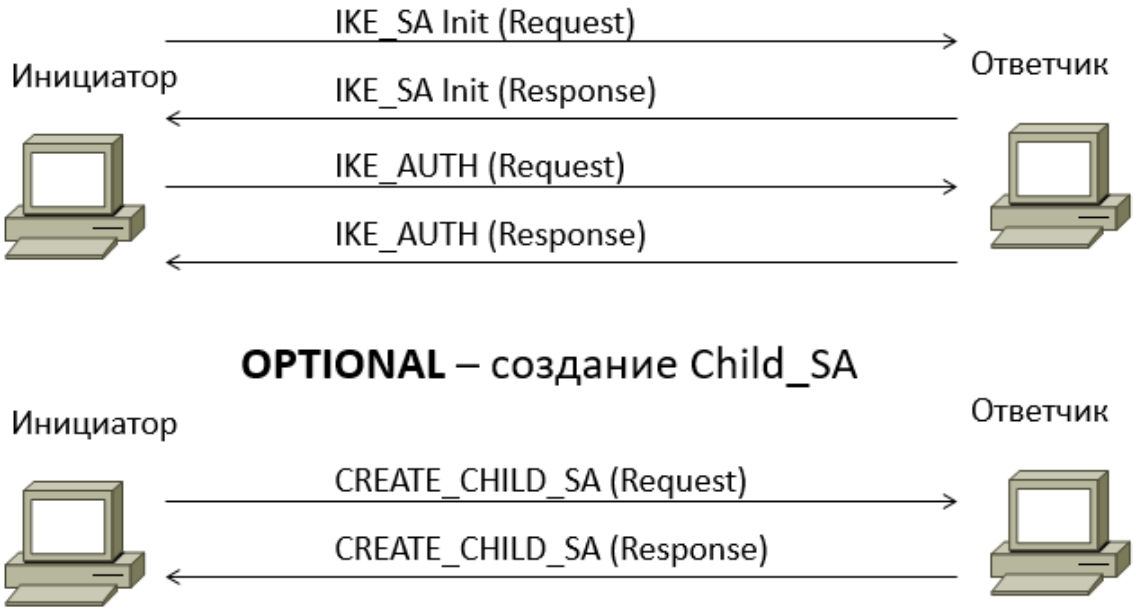


Рис. 52. Обмен сообщениями IKEv2

Для защиты от атак с целью исчерпания активных сессий и вызова отказа в обслуживании, в данной версии был осуществлен механизм проверки инициатора с помощью cookie. Представим, что на сервер приходит множество запросов на соединение с разными IP. В этом случае вместе с ответным сообщением IKE_SA_INIT сервер отправит специальное cookie. Если инициатор не поддельный, он повторяет запрос, вкладывая в него полученное cookie. При таком условии сервер не затрачивает вычислительные мощности на установление поддельных сессий.

5.2.2. Режимы работы IPsec. IPsec VPN

Использование IPsec возможно в двух режимах – транспортном и туннельном. Выбор режима зависит от архитектуры сети и целей применения. В транспортном режиме обеспечивается шифрование всей полезной нагрузки пакета выше сетевого уровня, оставляя нетронутым и видимым для всех промежуточных узлов оригинальный IP-заголовок. Данный режим эффективно применяют для защиты соединений между оконечными устройствами, например, сервером и клиентом (рис. 53).



Рис. 53. Структура пакета IPsec в транспортном режиме

Туннельный режим отлично подходит для организации виртуальный частных сетей (VPN), так как происходит полная инкапсуляция оригинального IP-пакета и назначается новый IP-заголовок. Это повышает конфиденциальность, потому что промежуточные узлы в сети не видят содержимое оригинального заголовка (рис. 54).

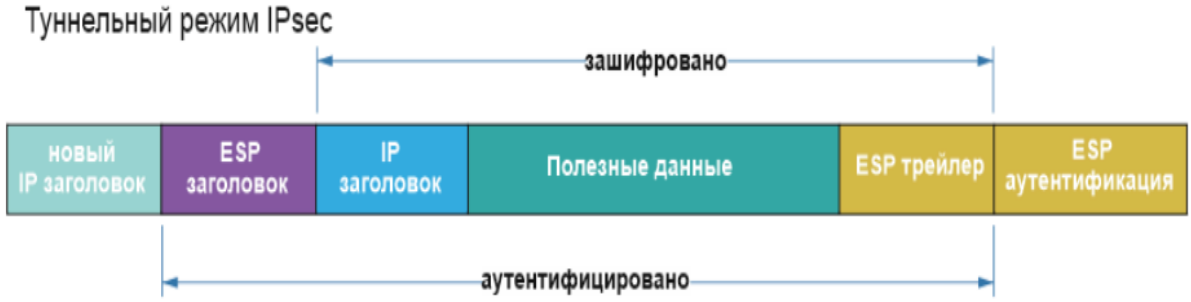


Рис. 54. Структура пакета IPsec в туннельном режиме

Рассмотрим способы организации защищенного соединения site-to-site с помощью IPsec в туннельном режиме. Существует два подхода к управлению трафиком в IPsec VPN – policy-based и route-based.

Policy-based предполагает использование политик маршрутизации для определения, какой трафик подлежит инкапсуляции и шифрованию, а какой – нет. Отсутствует необходимость явно задавать маршруты, что обеспечивает гибкость по различным критериям для разных типов трафика, однако, в случае масштабной сетевой инфраструктуры, обработка большого числа политик для принятия решений о маршрутизации в защищенный туннель может значительно замедлиться. Схема IPsec policy-based VPN представлена на рис. 55. Когда пакет приходит на пограничный маршрутизатор (с Ipsec VPN), он проверяется в соответствии с настроенными политиками (route-map, acl, crypto-map). К примеру, если IP-адрес источника и назначения соответствует условиям политик, то данный поток трафика инкапсулируется и шифруется, а затем отправляется в туннель.

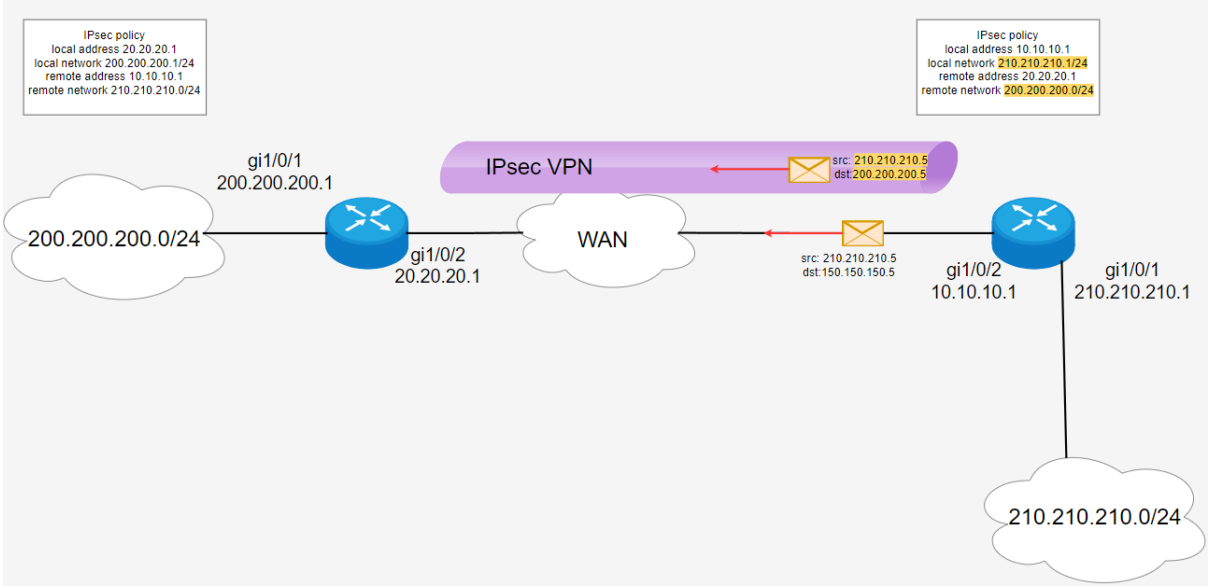


Рис. 55. IPsec policy-based VPN

При использовании route-based VPN создаются отдельные логические интерфейсы (VTI), к которым привязывается профиль IPsec. Маршрутизация при этом осуществляется через стандартные механизмы, явно указывая маршрут до подсети через защищенный туннель, а не политики. Схема функционирования route-based IPsec VPN изображена на рис. 56. Для создания защищенного канала передачи с помощью IPsec route-based, необходимо сконфигурировать логические туннельные интерфейсы на обоих концах туннеля, создать статический маршрут до нужной подсети, в котором шлюзом будет являться интерфейс VTI. После чего применить настроенный IPsec-профиль для обеспечения защищенности. Таким образом, если трафик предназначается подсети, маршрут до которой пролегает через туннельный интерфейс с IPsec-профилем, в соответствии с таблицей маршрутизации, то он шифруется, инкапсулируется и направляется в VPN-туннель.

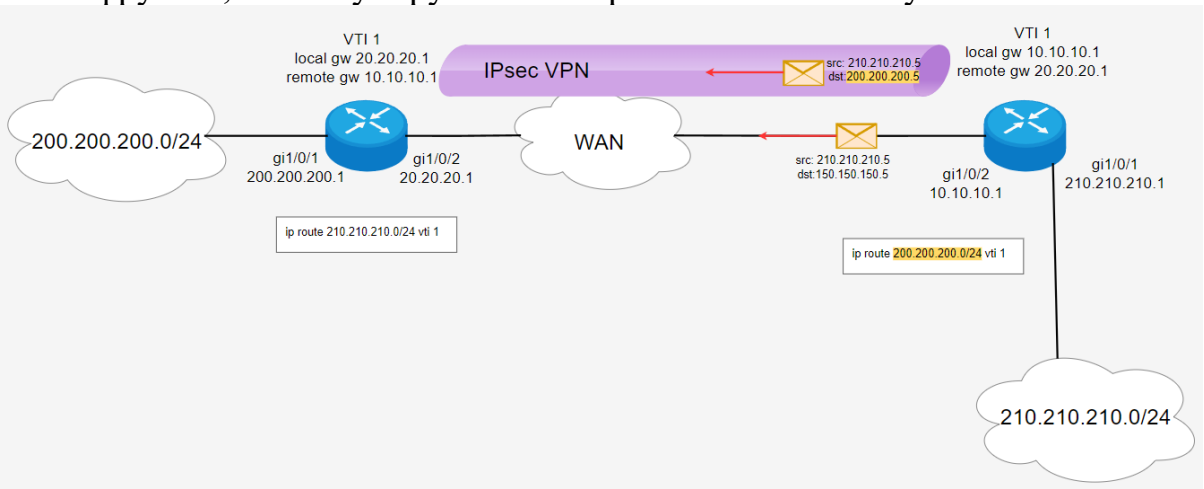


Рис. 56. IPsec route-based VPN

Контрольные вопросы

Назовите способы организации изолированных каналов связи.
Какие варианты обеспечения защищенного канала передачи данных актуальны для крупных организаций с большими финансовыми возможностями?
Что собой представляет процесс туннелирования в компьютерных сетях?
Что собой представляет структура туннеля?
Какой протокол является самым простым протоколом туннелирования?
Опишите принцип работы протокола GRE.
Какой недостаток применения протокола GRE?
Каковы компоненты набора протоколов IPsec?
Как происходит процесс установления соединения в IPsec?
Как работает IKEv1?
За счет чего происходит сокращение числа сообщений до трех при установлении соединения IKEv1?
Какие недостатки у первой версии IKEv1?
Какие недостатки первой версии IKEv1 были исключены с помощью появления IKEv2?
Как происходит диалог двух клиентов, устанавливающих соединение с помощью IKEv2?
Как происходит защита от атак с целью исчерпания активных сессий и вызова отказа в обслуживании в версии IKEv2?
В каких режимах можно использовать IPsec?
От чего зависит выбор режима при использовании IPsec?
Когда применяется транспортный режим IPsec?
Какой режим IPsec подходит для организации виртуальный частных сетей (VPN)?
Какова структура пакета IPsec в туннельном режиме?
Какие подходы существуют для управления трафиком в IPsec VPN?
Какой подход предполагает использование политик маршрутизации для определения, какой трафик подлежит инкапсуляции и шифрованию, а какой – нет?
Объясните принцип функционирования policy-based IPsec VPN.
При использовании какого подхода создаются отдельные логические интерфейсы (VTI), к которым привязывается профиль IPsec?
Объясните принцип функционирования route-based IPsec VPN.

6. ТЕХНОЛОГИЯ DMVPN

6.1 Предпосылки к появлению DMVPN

В предыдущей главе были рассмотрены решения проблемы безопасной передачи данных в распределенной сетевой инфраструктуре с помощью статических VPN-туннелей, однако остается еще одна проблема – масштабируемость.

В классическом варианте Full-mesh каждый участник распределенной сети соединен друг с другом в полно связной топологии с помощью статических туннелей site-to-site. В данном случае при добавлении нового участника сети необходимо настраивать новые туннельные соединения со всеми уже существующими участниками, что приводит к экспоненциальному росту сложности управления сетью.

Можно использовать топологию Hub-and-Spoke с центральным узлом и подключенными к нему филиалами. При таком условии, снижение производительности будет обуславливаться прохождением трафика через центральный узел при передаче данных между филиалами (рис. 57).

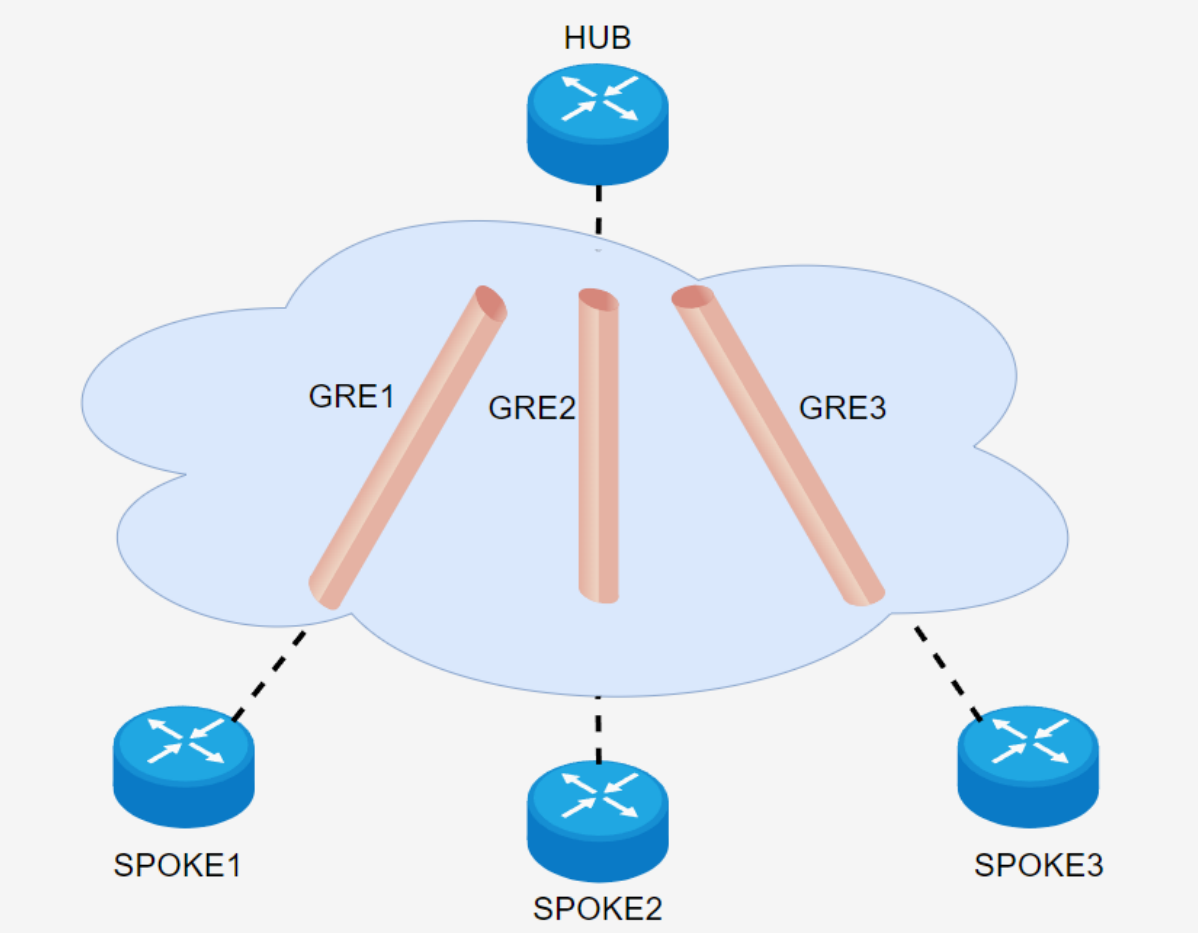


Рис. 57. Классическая топология hub-and-spoke с GRE-туннелями

Для решения проблемы масштабируемости site-to-site VPN-туннелей без значительного снижения производительности сетевых устройств компания Cisco представила в 2009 г. технологию DMVPN.

Dynamic Multipoint Virtual Private Network (DMVPN) – решение, являющееся объединением функционала нескольких протоколов: NHRP, mGRE и Ipsec (рис. 58).

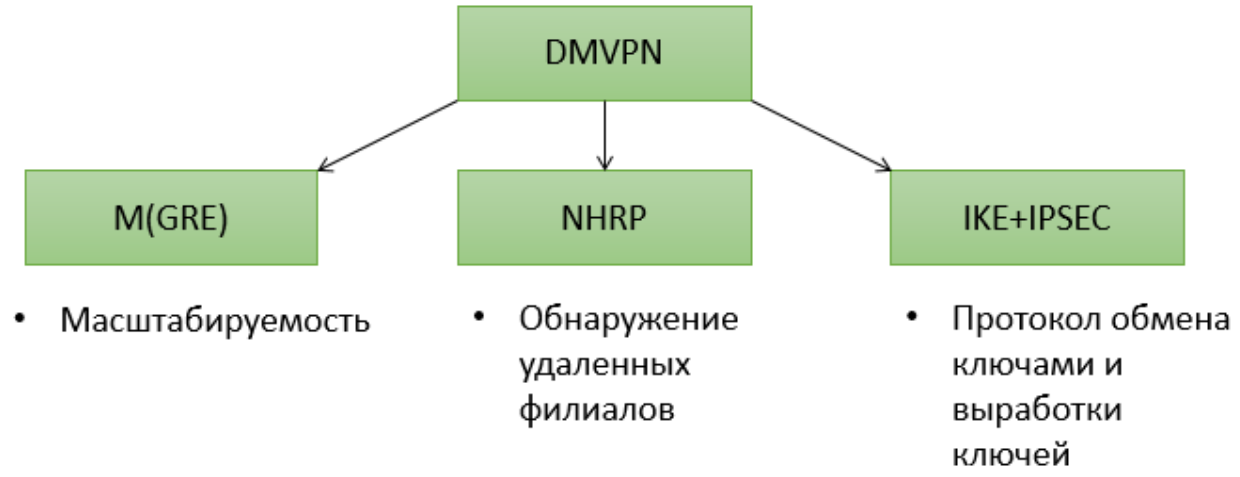


Рис. 58. Компоненты DMVPN

Суть этой технологии – возможность динамического установления защищенных туннельных соединений между узлами. Базовые принципы и технологии, являющиеся основой DMVPN:

- Топология Hub-and-Spoke или ее вариации.
- Использование mGRE для point-to-multipoint туннелирования.
- Шифрование GRE-трафика с помощью IPsec.
- Протокол динамической маршрутизации.

6.2. Принципы работы DMVPN и его составляющих

Рассмотрим механизм работы DMVPN и его составляющих. Выбирается центральная точка распределенной сетевой инфраструктуры, например, головной офис некой организации. К данной точке будут подключаться все остальные, например, филиалы организации, расположенные в других городах. Идея в том, чтобы клиенты подключались к центру и, по необходимости, устанавливали прямые туннельные соединения между друг другом, минуя центральный хаб. Это становится возможным с помощью совместной работы протоколов mGRE и NHRP.

Multipoint Generic Routing Encapsulation (mGRE) – расширение протокола GRE, которое позволяет одному туннельному интерфейсу поддерживать и обрабатывать множество динамических соединений с помощью NHRP (рис. 59).

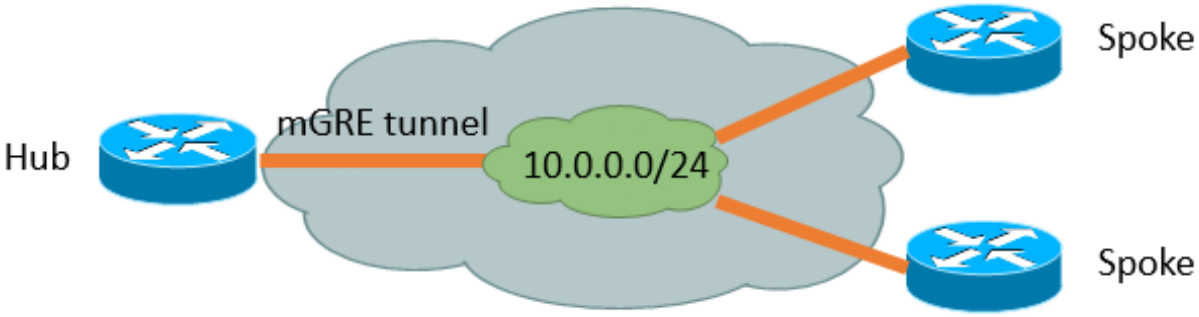


Рис. 59. mGRE-подсеть

Next Hop Resolution Protocol (NHRP, RFC 2332) – протокол разрешения следующего перехода, используется для установления соответствий между приватными IP туннельных интерфейсов с публичными WAN адресами. Основными компонентами данного протокола являются Next Hop Server (NHS) и Next Hop Client (NHC). Каждый NHC регистрирует свой публичный и локальный IP-адрес в NHS. В случае необходимости установить соединение с другим маршрутизатором NHC информация об узле запрашивается у сервера, после чего два NHC могут обмениваться трафиком напрямую, снижая нагрузку на центральный узел. Чтобы не перегружать NHS запросами, таблица зарегистрированных на центральном узле клиентов кэшируется на каждом NHC. Для защиты от подмены NHRP-сообщений реализуется аутентификация в NHRP с помощью pre-shared key, который должен быть одинаковым на каждом маршрутизаторе в DMVPN-сети и добавляться в поле Authentication заголовка NHRP.

В DMVPN-сетях не последнюю роль играет протокол динамической маршрутизации, позволяющий легко добавлять новые узлы в сеть без необходимости перенастраивать всю сеть. Технология DMVPN совместима со всеми основными протоколами динамической маршрутизации: EIGRP, RIP, BGP, IS-IS, OSPF. Чаще всего применяется протокол OSPF (RFC 2328), являющийся открытым стандартом. Это делает его подходящим для мультивендорных сетей, однако механизм выбора Designated Router/Backup Designated Router может осложнить применение OSPF совместно с DMVPN: необходимо сформировать приоритеты узлов так, чтобы NHS являлся DR, для этого на центральном узле назначается максимальное значение приоритета, в то время, как на spoke-узлах выставляется ноль.

Исходя из особенностей функционирования данных технологий, алгоритм работы DMVPN будет иметь следующий вид:

1. На каждом узле настроен mGRE, центральный узел (hub) настроен как NHS, остальные узлы (spoke) настроены как NHC.
2. Регистрация spoke на hub – NHRP Registration Request (tunnel IP, public IP).

3. Spoke получает NHRP Registration Reply и сохраняет hub как NHS.
4. Если Spoke A хочет отправить данные Spoke B, то он отправляет запрос на NHS – NHRP Resolution Request (tunnel IP).
5. Hub отправляет NHRP Resolution Reply (public IP).
6. Spoke A устанавливает mGRE-туннель до Spoke B, используя публичный адрес.
7. GRE-трафик шифруется с помощью IPsec и передается до Spoke B.
8. Spoke A и Spoke B кэшируют информацию друг о друге для последующего соединения.

С момента появления DMVPN происходило его эволюционное развитие. Три основные фазы данной технологии привносили новые возможности.

В первой фазе DMVPN реализуется строгая централизованная топология, в которой узлы устанавливали туннельное соединение только с хабом, на котором функционировал протокол mGRE (рис. 60). Главная цель состояла в уменьшении сложности администрирования множеством туннелей в случае масштабирования сетевой инфраструктуры, однако трафик передавался через центральный узел, даже если spoke-узлы хотели передавать данные между собой. Этот основной недостаток привел к появлению второй фазы.

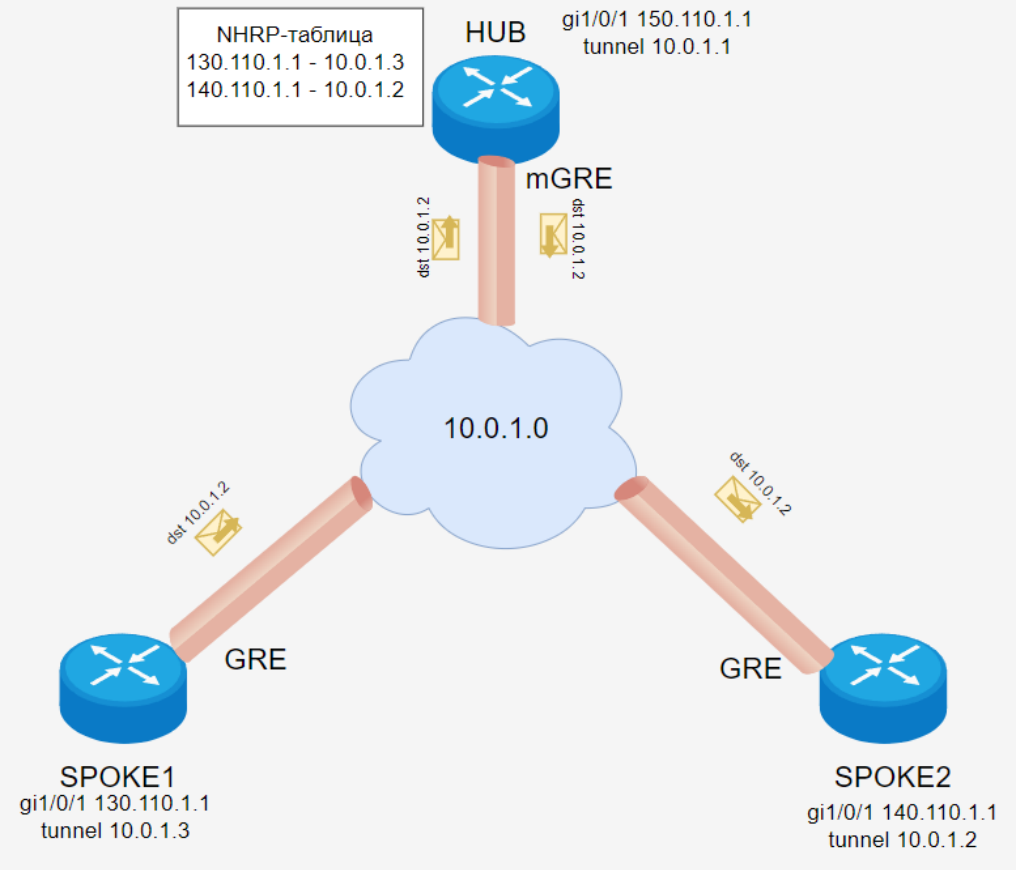


Рис. 60. Первая фаза DMVPN

Вторая фаза расширила функционал первой, дав возможность устанавливать прямые GRE-туннели между узлами благодаря поддержке mGRE. Теперь spoke могут не только регистрироваться на hub-узле, но и запрашивать информацию о других узлах по NHRP (рис. 61). Прямое взаимодействие между spoke-узлами снизило задержки и разгрузило центральный узел, при этом в случае изменения физического IP-адреса узла, например, из-за переподключения к другому провайдеру, существующие туннели не обновляются в автоматическом режиме, требуя ручного вмешательства администратора. Также существенным недостатком остается зависимость от хаба в маршрутизации: когда hub-узел получает маршрут от spoke, он автоматически не пересылает его другим узлам.

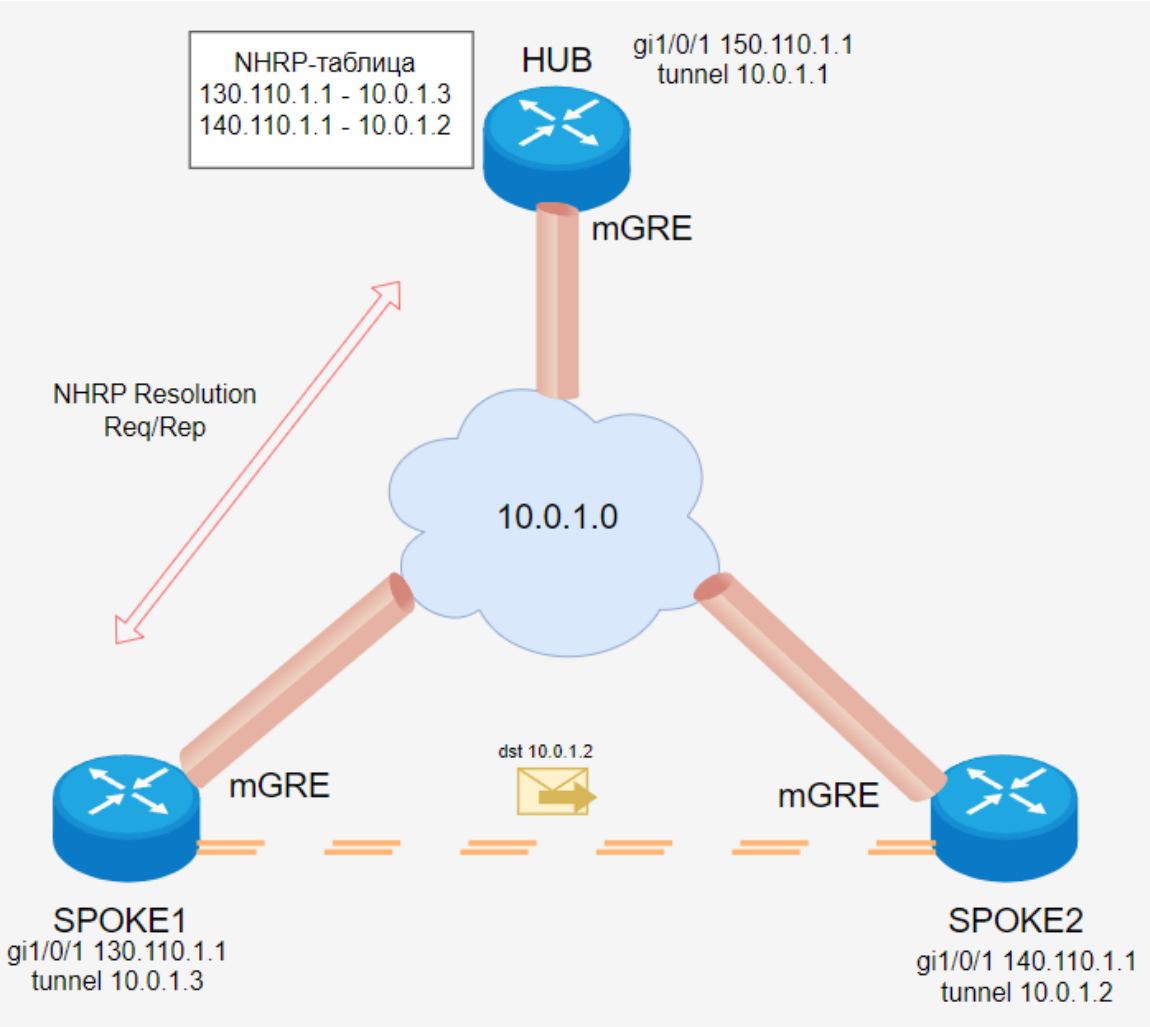


Рис. 61. Вторая фаза DMVPN

В третьей фазе DMVPN проблема маршрутизации в масштабируемых VPN-сетях была решена с помощью механизмов NHRP Redirect (функционирует на хабе) и NHRP Shortcut (позволяет обрабатывать Redirect-сообщения на узлах). Рассмотрим работу этих решений на примере двух узлов (S1, S2) и хаба (Hub):

1. S1 первоначально отправляет трафик до S2 через Hub.
2. Hub замечает неэффективность маршрута и генерирует для S1 NHRP Redirect Message.
3. S1, получив сообщение, отправляет NHRP Resolution Request до Hub.
4. Hub передает реальный адрес S2.
5. S1 устанавливает прямой туннель до S2.

Таким образом, увеличивается скорость сходимости сети как при первоначальной установке туннельных соединений между spoke-узлами, так и при обновлении маршрутной информации, минимизируя участие центрального узла (рис. 62).

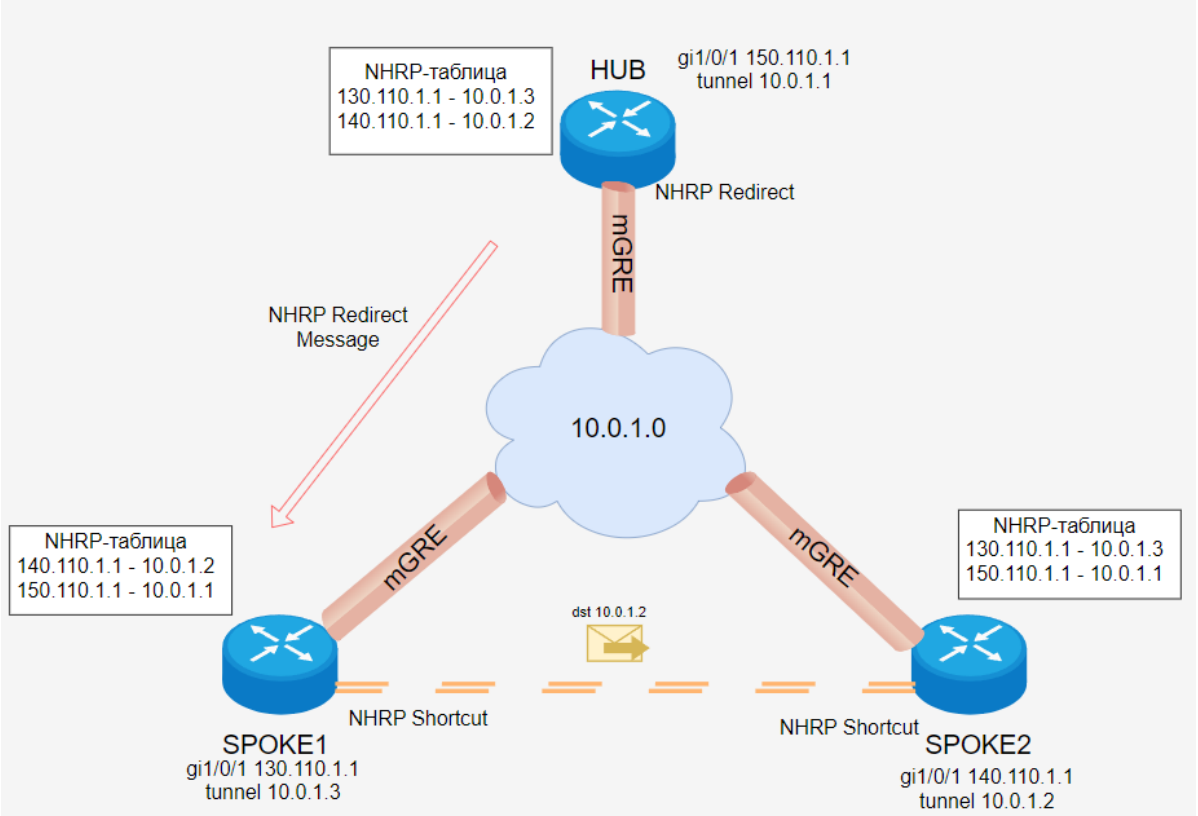


Рис. 62. Третья фаза DMVPN

6.3. Отказоустойчивые топологии в DMVPN

В классической топологии DMVPN хаб играет важнейшую роль, но в то же время представляет собой единую точку отказа в VPN-сети. Для обеспечения отказоустойчивости используются различные архитектурные решения, добавляющие избыточность в сетевую инфраструктуру. Рассмотрим примеры отказоустойчивых топологий, их преимущества и недостатки.

Single Hub-Single Cloud – простейшая топология DMVPN с одним центральным узлом и одним облаком. Облако DMVPN – логическая группа туннелей, работающих в рамках одной сети, с единым адресным пространством, NHRP-таблицей и параметрами (IPsec-политики, протокол маршрутизации). В данной топологии отсутствует какая-либо отказоустойчивость и балансировка нагрузки. Такая топология подходит для небольших сетей.

В топологии Dual Hub-Single Cloud используются два хаба, функционирующие в рамках одного DMVPN-облака. Оба хаба имеют доступ к одной таблице маршрутизации и общей NHRP-конфигурации. Данная топология способна предоставлять отказоустойчивость в двух режимах: оба центральных узла работают единовременно, либо же один является основным, а другой резервным (рис. 63).

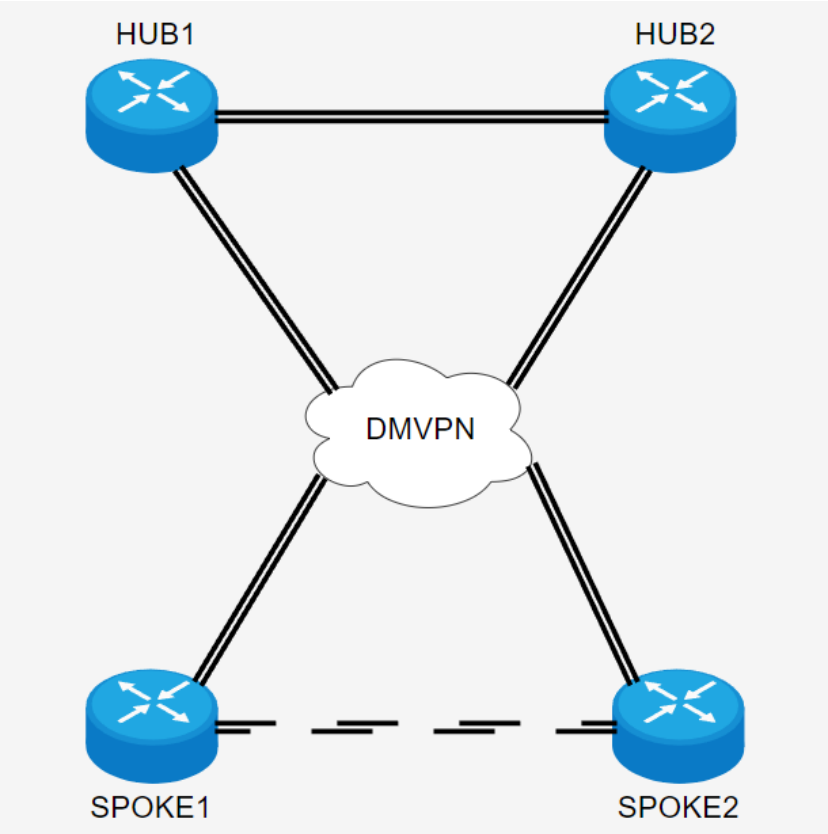


Рис. 63. Dual Hub-Single Cloud

В Single Hub-Dual Cloud используется один хаб, обслуживающий две независимые VPN-сети. Каждая сеть может иметь свои политики IPsec и предназначаться для определенных типов трафика или группы узлов. Однако, несмотря на преимущество в логическом разделении сетей, в случае выхода из строя единственного центрального узла оба облака перестанут функционировать (рис. 64).

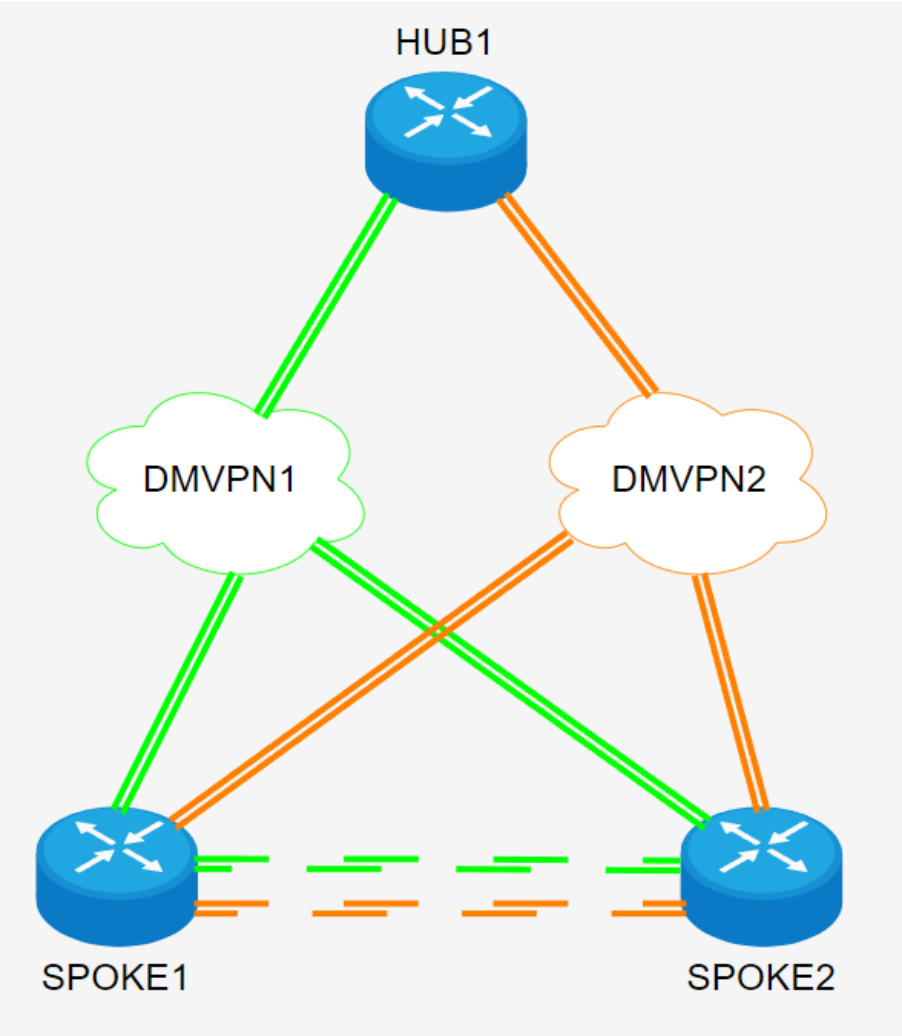


Рис. 64. Single Hub-Dual Cloud

Топология Dual Hub-Dual Cloud является самой сложной и отказоустойчивой, сочетающей в себе преимущества всех предыдущих. Используются два хаба, обслуживающих два DMVPN-облака (рис. 65). Оба центральных узла являются резервными друг для друга, при этом сохраняя возможность логического разделения сетей и балансировки нагрузки. Такое решение является экономически затратным и сложным в администрировании и настройке, поэтому подходит для крупных распределенных корпоративных сетевых инфраструктур.

Сложная, многокомпонентная организация DMVPN-сети делает процесс поиска и устранения неполадок (troubleshooting), если они все же возникли, достаточно проблематичным. Для начала необходимо выполнить диагностику физической исправности – статус интерфейсов и физическое подключение. Если проблема не устранена, переходим к проверке каждого компонента DMVPN. Для IPsec необходимо удостовериться в согласовании криптографических параметров сторон, корректном секретном ключе. Если проблема в NHRP, например, не устанавливаются динамические spoke-to-spoke туннели, то стоит убедиться в том, что именно хаб является NHS. Но

чаще всего проблема кроется в некорректной настройке GRE-туннелей и динамической маршрутизации.

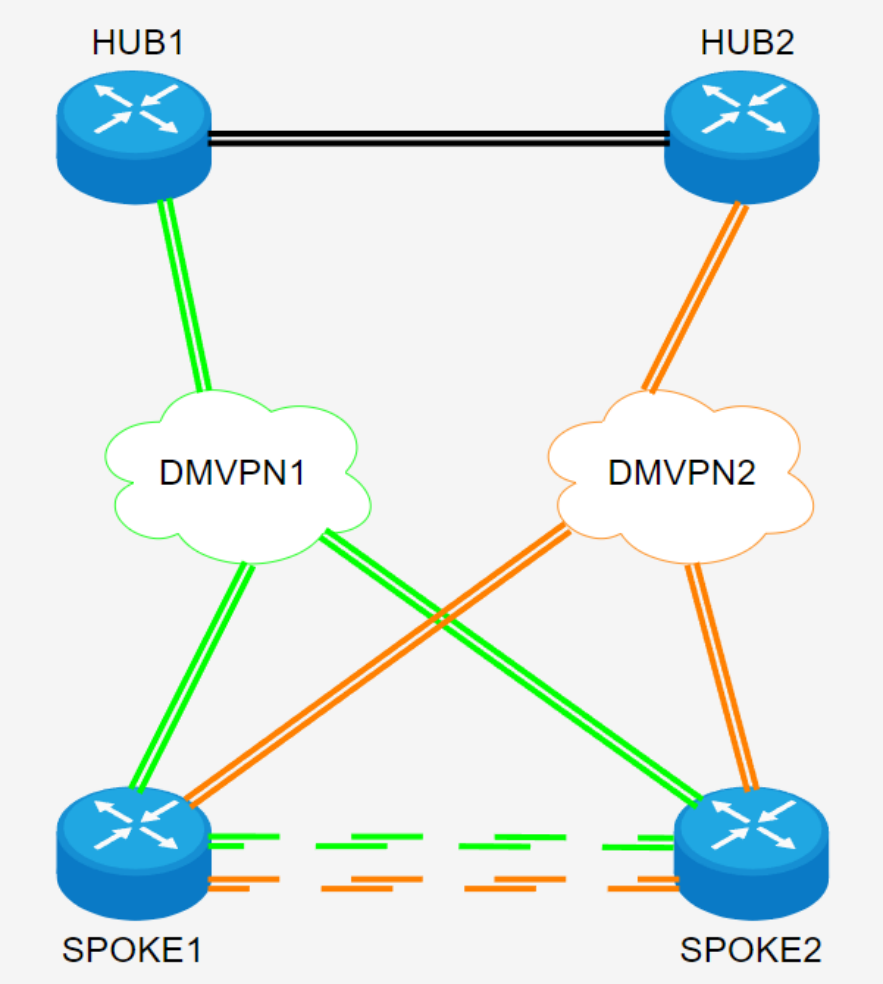


Рис. 65. Dual Hub-Dual Cloud

Несмотря на то, что технология DMVPN принадлежит компании Cisco и является проприетарной, остальные вендоры сетевого оборудования, в том числе и российские, создают свои собственные аналоги или копируют решение Cisco.

Контрольные вопросы

Что вызвало необходимость появления Dynamic Multipoint Virtual Private Network (DMVPN)?
Почему применение классической топологии hub-and-spoke с GRE-туннелями не является эффективным при решении проблемы масштабируемости?
Что собой представляет Dynamic Multipoint Virtual Private Network (DMVPN)?
Что является базовыми принципами и технологиями DMVPN?

Как работает механизм DMVPN и его составляющих?
Что такое Multipoint Generic Routing Encapsulation (mGRE)?
С какой целью используется протокол Next Hop Resolution Protocol (NHRP, RFC 2332)?
Какие компоненты протокола Next Hop Resolution Protocol (NHRP, RFC 2332) являются основными?
Какова роль протокола динамической маршрутизации в DMVPN-сетях?
С какими основными протоколами динамической маршрутизации совместима технология DMVPN?
Что необходимо предпринять для совместимости OSPF с DMVPN для мультивендорных сетей?
Каков алгоритм работы DMVPN при применении протокола OSPF (RFC 2328)?
Что реализуется в первой фазе эволюции DMVPN?
Какой основной недостаток у первой фазы эволюции DMVPN?
Что реализуется во второй фазе эволюции DMVPN?
Какие недостатки у второй фазы эволюции DMVPN?
С помощью каких механизмов была решена проблема маршрутизации в масштабируемых VPN-сетях в третьей фазе DMVPN?
Объясните принцип работы NHRP Redirect и NHRP Shortcut?
Какие архитектурные решения используются в сетевой инфраструктуре для обеспечения отказоустойчивости?
Что представляет собой топология Single Hub-Single Cloud?
Что представляет собой топология Dual Hub-Single Cloud?

7. СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ IPS

7.1. Атаки нулевого дня

В современных реалиях существуют ситуации, когда злоумышленники обнаруживают уязвимость в системах раньше, чем разработчик, получая возможность эксплуатировать ее наиболее эффективно.

«Нулевой день» – это общий термин, описывающий недавно обнаруженные уязвимости в системе безопасности, которые могут быть использованы злоумышленниками для атаки на систему. Термин «нулевой день» показывает, что поставщик или разработчик только что узнали об уязвимости, и у них есть «ноль дней» на ее исправление. Это создает уникальную ситуацию, когда защитные механизмы не могут быть своевременно адаптированы для предотвращения эксплуатации данной уязвимости.

Для выявления уязвимостей нулевого дня применяется эвристический анализ, позволяющий выявить признаки вредоносных программ нулевого дня на основе их взаимодействия с целевой системой (рис. 66). Для того, чтобы обнаружить данные о ранее зафиксированных эксплойтах, все чаще используют машинное обучение. При этом устанавливается эталон безопасного поведения системы на основе данных о прошлых и текущих взаимодействиях с системой. Чем больше данных доступно, тем надежнее обнаружение.



Рис. 66. Жизненный цикл Zero-day атаки

7.2. Intrusion Prevention Systems (IPS)

7.2.1. Технология и формы ее реализации

Системы предотвращения вторжений предназначены для обнаружения и блокировки потенциально вредоносного воздействия на защищаемую информационную инфраструктуру в реальном времени. Технология IPS эволюционировала из систем обнаружения вторжений (IDS), которые появились в конце 1980-х годов. Первая IDS была разработана Дороти Деннинг в 1986 году и называлась IDES (Intrusion Detection Expert System). Эта система

основывалась на анализе сетевого трафика и использовании правил для выявления аномалий. Однако IDS имели существенный недостаток: они могли только оповещать администраторов о возможных угрозах, не предпринимая никаких действий для их устранения. К середине 1990-х годов стало очевидно, что пассивное обнаружение угроз недостаточно для защиты корпоративных сетей. Это привело к разработке технологий, которые могли бы не только обнаруживать, но и предотвращать атаки. Первые системы предотвращения вторжений начали появляться в начале 2000-х годов и дополнили функционал IDS. С развитием технологий и усложнением киберугроз современные IPS стали использовать передовые методы анализа данных такие, как машинное обучение, искусственный интеллект и поведенческий анализ (рис. 67). Эти технологии позволяют IPS эффективно противостоять новым типам атак, включая атаки нулевого дня.

Реализация системы предотвращения вторжений может быть осуществлена двумя способами:

- Host-based IPS (HIPS) – развертывается непосредственно на защищаемых устройствах для защиты от угроз на уровне ОС, файловой системы и приложений. За счет отслеживания выполняемых команд, взаимодействий с сетью и изменений конфигурации систем данный вариант реализации IPS эффективен против атак, осуществляющихся внутри корпоративной инфраструктуры.
- Network-based IPS (NIPS) – развертывается в качестве сенсора, анализируя сетевой трафик на предмет вредоносных паттернов и сигнатур. Позволяет обрабатывать весь трафик, входящий в сеть организации, а не только на конкретном устройстве.

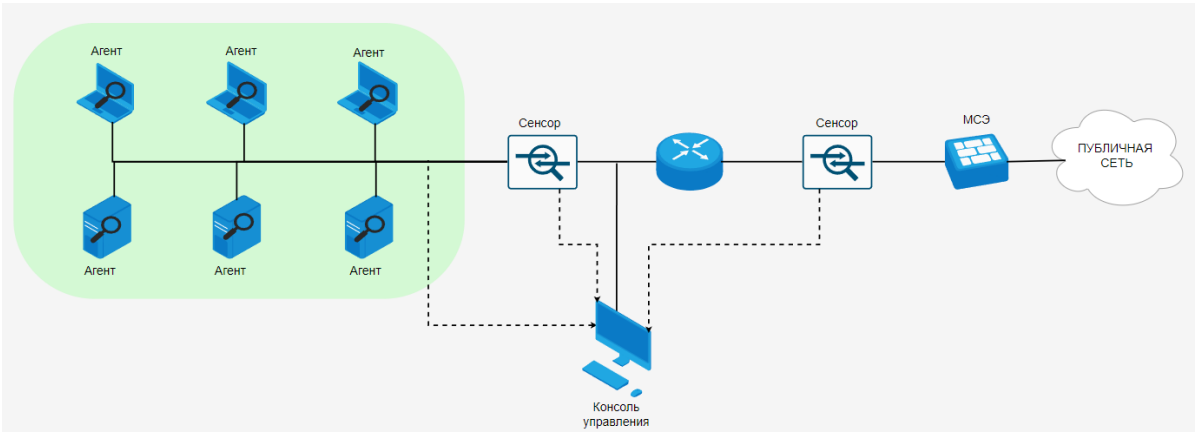


Рис. 67. IPS в сетевой инфраструктуре

По способу обнаружения угроз IPS классифицируются следующим образом:

- Сигнатурные – анализ сетевого трафика по принципу идентификации известных атак с помощью базы данных сигнатур. При

оптимально созданных сигнатурах гарантирована высокая точность выявления известных угроз при минимальном уровне ложных срабатываний, однако не позволяет эффективно выявлять атаки «нулевого дня» и требует регулярного обновления баз сигнатур.

- Аномальные – анализ сетевого трафика на основе сравнения с нормальной моделью поведения. Устанавливаются пороговые значения частоты запросов, объема передаваемых данных и другие параметры, характеризующие штатную работу сетевой инфраструктуры. Такой подход позволяет определять вредоносное поведение и выявлять сложные угрозы, в том числе и zero-day. Из недостатков можно выделить высокие требования к точности настройки «нормального профиля» и повышенного риска ложных срабатываний.
- IPS на основе политик, в отличие от сигнатурных и аномальных, не выявляют атаки напрямую, а ограничивают или запрещают действия, которые могут привести к возникновению угрозы и вторжению. Политики безопасности определяются администратором. Данный вариант наиболее эффективен для противодействия внутренним угрозам.

7.2.2. Принципы функционирования и варианты применения в топологии сети

IPS работает как активный барьер между локальной и глобальной сетью, выявляя паттерны подозрительных событий. Данное решение функционирует на четырех уровнях модели OSI:

- Канальном – анализ кадров и протоколов второго уровня, обнаружение атак с использованием ARP и MAC;
- Сетевом – мониторинг IP-пакетов, маршрутизации;
- Транспортном – анализ поведения транспортных протоколов TCP и UDP, отслеживание соединений, предотвращение сканирования и DoS;
- Прикладном – полный анализ содержимого пакетов, мониторинг http-запросов, выявление sql-инъекций, межсайтового скриптинга и других атак на седьмом уровне.

Работа IPS происходит в три этапа, рассмотрим каждый из них подробнее.

Перехват трафика в ключевых точках сети. Для последующего анализа необходимо, чтобы весь трафик прошел через сенсор IPS. Существует два варианта размещения системы в сетевой архитектуре – inline и promiscuous.

Inline – активный вариант работы IPS, при котором система размещается непосредственно в потоке трафика, становясь частью маршрута

передачи данных, что позволяет немедленно реагировать на угрозы и своевременно их блокировать, однако такой вариант требует значительной вычислительной мощности, в ином случае возможно возникновение задержек (рис. 68).

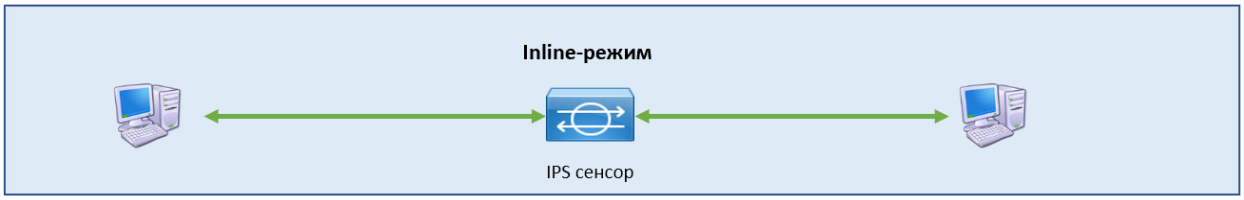


Рис. 68. Inline расположение IPS

Promiscuous – пассивный режим работы, при котором система не является частью маршрута прохождения трафика, а лишь «прослушивает», анализируя копии пакетов без возможности повлиять на передачу данных (рис. 69). Поступление копий пакетов на сенсоры IPS становится возможным благодаря технологии SPAN. Switch Port Analyzer (SPAN) – технология на коммутаторах для копирования сетевого трафика с портов-источников на порт назначения. Такое расположение не влияет на пропускную способность сети и позволяет собирать информацию для SIEM-систем.

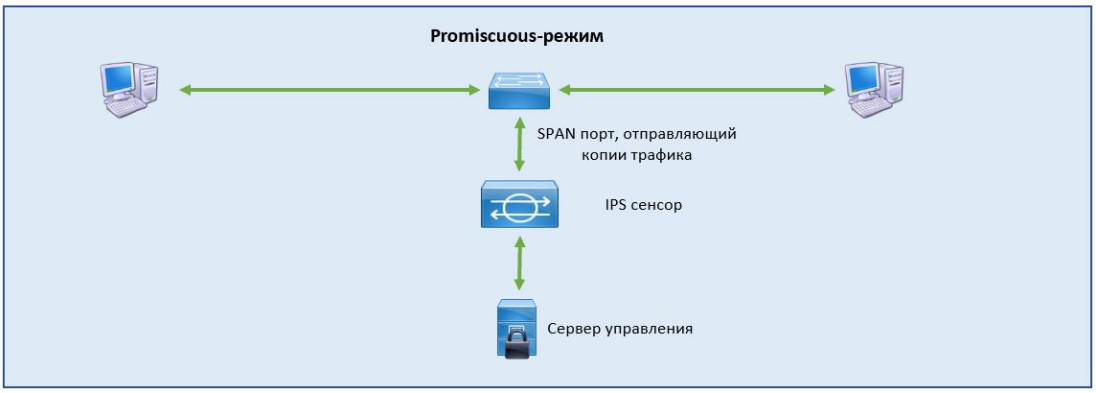


Рис. 69. Promiscuous-режим IPS

После попадания трафика на сенсор IPS, происходит эвристический анализ на основании сигнатур – шаблонов, характерных для эксплойтов и ВПО, и поведения, например, выявление внезапного увеличения числа запросов к серверу. Для реализации данного метода часто применяется машинное обучение.

При обнаружении подозрительного события при анализе трафика, начинается этап реагирования на угрозы. В зависимости от настроенных политик и правил, существует четыре варианта реагирования:

- alert – прохождение трафика разрешается и генерируется сообщение от IPS;

- reject – прохождение трафика запрещается, отправляется TCP-RESET или ICMP-ERROR, также генерируется сообщение;
- pass – прохождение трафика разрешается;
- drop – прохождение трафика запрещается, IPS генерирует сообщение.

7.2.3. Сигнатуры

Сигнатура – это формализованное описание угрозы, которое включает набор характеристик, уникально идентифицирующих конкретную атаку или вредоносное поведение. Сигнатуры разделяются следующим образом:

- Атомарная – простейший тип сигнатуры, заключающийся в проверке одиночного пакета, действия или события на предмет его соответствия сконфигурированной сигнатуре. Если соответствие установлено, подается сигнал тревоги и предпринимается определенное сигнатурой действие.
- Составная (композитная) сигнатура обнаруживает последовательность операций, распределенных по разным хостам в течение произвольного периода времени.

Каждая сигнатура содержит набор атрибутов, которые определяют её характеристики и условия срабатывания. Основные атрибуты включают:

1. Идентификатор сигнатуры – уникальный номер или код, который позволяет идентифицировать сигнатуру в базе данных.
2. Краткое описание того, что именно обнаруживает сигнатура.
3. Уровень риска – оценка серьезности угрозы, например, низкий, средний, высокий или критический.
4. Паттерн или правило – конкретный шаблон, который используется для сравнения с трафиком.
5. Контекстные параметры – дополнительные условия, такие как IP-адреса, порты, протоколы или время суток.
6. Заданный ответ системы на срабатывание сигнатуры.

Эффективность современных систем предотвращения вторжений достаточно высока, однако существует вероятность ошибки. Это выражается в ложно-положительных (False Positive) и ложно-отрицательных (False Negative) событиях.

Ложно-положительное событие – событие, которое система ошибочно классифицирует как угрозу. Причинами возникновения ошибок данного типа могут быть слишком общие сигнатуры, отсутствующий контекст, избыточная чувствительность IPS для минимизации рисков.

Ложно-отрицательное событие – ошибочное определение вредоносного трафика, как легитимного из-за устаревших сигнатур, ограниченных возможностей конкретной системы, ошибок конфигурации.

Для эффективного поддержания информационной безопасности сетевой инфраструктуры, специалист по безопасности не должен полагаться

исключительно на возможности программно-аппаратных комплексов, а обрабатывать подозрительные спорные события вручную, не игнорируя сигналы системы.

Наиболее популярными IDS/IPS с открытым исходным кодом являются Suricata и Snort. Оба инструмента используют сигнатуры для анализа сетевого трафика и выявления угроз. Они поддерживают как сигнатурный анализ, так и более сложные методы, такие как эвристика и поведенческий анализ. Suricata, как более современная система, является более производительной и обладает поддержкой многопоточности. Ниже приведен пример правила Suricata по обнаружению эксплуатации EternalBlue (CVE-2017-0144):

alert smb $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Request (CVE-2017-0144)";
flow:established,to_server;
app-layer-event:smb.trans2_invalid_secondary_offset;
classtype:attempted-admin;
sid:2023536; rev:1;
metadata:created_at 2017_04_17, updated_at 2017_04_17;)

1. alert: Действие — отправить оповещение.
2. smb: Протокол — SMB.
3. $EXTERNAL_NET any -> $HOME_NET any: Трафик от внешней сети к внутренней.
4. flow:established,to_server: Проверка установленного соединения с сервером.
5. app-layer-event:smb.trans2_invalid_secondary_offset: Условие — некорректное смещение в SMB-транзакции.
6. classtype:attempted-admin: Категория события — попытка административного доступа.
7. sid:2023536: Уникальный идентификатор сигнатуры.
8. metadata: Дополнительная информация о создании и обновлении правила.

7.3. NGFW

В типовом наборе атак на сетевую инфраструктуру входят DDoS, фишинговая активность, попытки подбора паролей к сервисам, а также эксплуатация уязвимостей в программном обеспечении. Однако существуют так называемые APT-атаки (Advanced Persistent Threat) – это сложные и продолжительные кибератаки, организуемые хакерскими группировками (обычно спонсируемыми государством или крупными организациями) с целью хищения данных, саботажа или шпионажа. Данный вид атак характеризуется целевым воздействием на конкретных сотрудников организации с помощью фишинга, социальной инженерии, создания различных бэкдоров, распространения ВПО. Такое воздействие отличается многоэтапностью и

скрытностью за счет высокого уровня профессионализма и возможностей нападающих. Классических средств защиты инфраструктуры может оказаться недостаточно для предотвращения APT.

Наиболее современным и комплексным решением для обеспечения безопасности компьютерных сетей на текущий момент является Next-Generation Firewall (NGFW) – межсетевой экран нового поколения, программно-аппаратный комплекс, объединяющий в себе функциональность межсетевого экрана, системы обнаружения и предотвращения вторжений, потокового антивируса и дополнительные технологии для существенного увеличения уровня безопасности. NGFW фильтрует трафик на уровнях от канального до прикладного, определяет пользователей и группы и все еще решает задачи классического МСЭ. Он способен фиксировать, какие приложения использует сотрудник, что передается в транзакциях, и блокирует сессии на основе их содержимого. Базовый набор функций современного NGFW выглядит следующим образом (рис. 70):

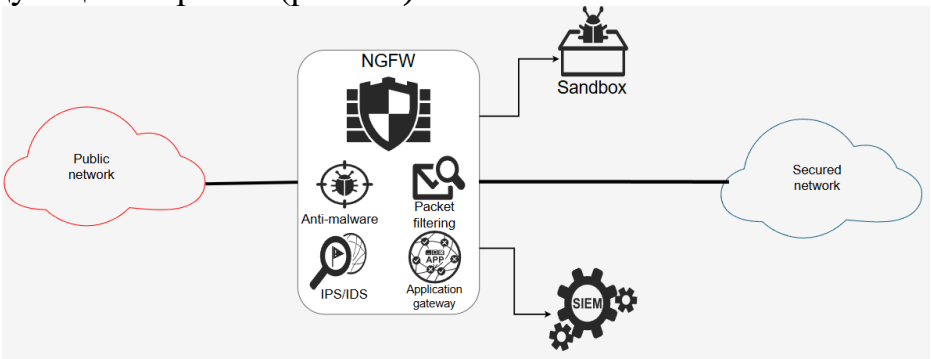


Рис. 70. МСЭ нового поколения (NGFW)

- контроль приложений. Производится анализ содержимого пакетов с сетевого до седьмого уровня OSI. Позволяет предотвратить атаки с использованием разрешенных протоколов (например, DNS);
- фильтрация по URL – ограничение доступа к сайтам на основе репутационных списков подозрительных сайтов. В случае использования HTTPS, трафик расшифровывается непосредственно на NGFW с помощью TLS-инспекции;
- управление VPN подключениями для реализации нулевого доверия при предоставлении доступа к сети;
- IPS-функционал с использованием широкой базы сигнатур и потоковым антивирусом;
- интеграция с контроллером домена для построения политик «пользователь/группа – приложение»;
- централизованное управление и возможность работы в кластере;
- защита от DoS и DDoS атак;

- интеграция с SIEM и песочницами;
- маршрутизация и коммутация;
- поддержка QoS.

Безусловными преимуществами использования NGFW являются: высокий уровень сетевой безопасности, комплексная защита, в том числе от вредоносного ПО, гибкость управления и возможность создания сложных правил управления трафиком, интеграция с SIEM-системами для создания единой экосистемы безопасности. К недостаткам можно отнести низкую скорость работы при всех включенных средствах защиты, сложность администрирования и повышенные квалификационные требования к специалистам для работы с данным типом устройств.

Контрольные вопросы

Что подразумевает термин «нулевой день»?
Какой анализ применяется для выявления уязвимостей нулевого дня?
Опишите жизненный цикл Zero-day атаки.
Какова цель применения систем предотвращения вторжений – Intrusion Prevention Systems (IPS)?
Когда появилась система обнаружения вторжений (IDS)?
На чем основывался принцип обнаружения вторжений системы IDS?
Какой недостаток у систем обнаружения вторжений (IDS)?
Когда появились первые системы предотвращения вторжений?
Какие передовые методы анализа данных стали использовать современные IPS?
Какими способами может быть осуществлена реализация системы предотвращения вторжений?
Какие системы предотвращения вторжений можно выделить при их классификации по способу обнаружения угроз?
Как происходит обнаружение угроз в сигнатурных системах предотвращения вторжений?
Что представляют собой аномальные системы предотвращения вторжений?
Что представляют собой системы предотвращения вторжений на основе политик?
Какой вариант систем предотвращения вторжений наиболее эффективен для противодействия внутренним угрозам?
На каких уровнях модели OSI функционирует система предотвращения вторжений?
Какие этапы работы у систем предотвращения вторжений?
Что представляет собой активный вариант работы системы предотвращения вторжений в сетевой архитектуре?
Что представляет собой пассивный вариант работы системы предотвращения вторжений в сетевой архитектуре?

Для чего предназначена технология Switch Port Analyzer (SPAN)?
Как происходит эвристический анализ для выявления уязвимостей нулевого дня?
Какие варианты реагирования происходят при обнаружении подозрительного события при анализе трафика?
Что представляет собой сигнатура?
Как работает атомарная сигнатура?
Как работает составная сигнатура?
Что включают в себя основные атрибуты сигнатуры?
Что такое ложно-положительное событие?
Что такое ложно-отрицательное событие?
Какие инструменты являются наиболее популярными у IDS/IPS с открытым исходным кодом?
Что представляют собой APT-атаки (Advanced Persistent Threat)?
Какова цель APT-атак (Advanced Persistent Threat)?
Что собой представляет Next-Generation Firewall (NGFW)?
Какая цель применения межсетевого экрана Next-Generation Firewall (NGFW)?
Что собой представляет базовый набор функций Next-Generation Firewall (NGFW)?
Какие преимущества обеспечивает применение межсетевого экрана Next-Generation Firewall (NGFW)?

ЗАКЛЮЧЕНИЕ

Обеспечение безопасности компьютерных сетей государственных учреждений и бизнес-компаний в настоящее время имеет первостепенное значение. Это вызвано участившимися кибератаками, утечками конфиденциальной информации, несанкционированным доступом и иными угрозами безопасности, что становится серьезной проблемой для разного рода организаций.

Поэтому внутриполитический курс Российской Федерации направлен на импортозамещение в вопросах информационной безопасности и отказ от использования иностранных решений в области сетевых технологий.

В текущих условиях образовательные учреждения и предприятия сталкиваются с отсутствием широко распространенных российских программных и виртуальных решений, аналогичных по функциональности и доступности, например, продукции компании Cisco Systems Inc. Это создает серьезные вызовы для подготовки специалистов в области безопасности компьютерных сетей. Поэтому так важны разработки ООО «Предприятия ЭЛТЕКС» для повышения квалификации существующих специалистов и обучения новых.

Разработанное учебное пособие на основе отечественного виртуального оборудования ООО «Предприятия ЭЛТЕКС» и свободно распространяемых дистрибутивов UNIX-систем призвано способствовать укреплению образовательной и технологической независимости страны, а также повышению квалификации выпускающихся специалистов в области информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Основы сетевых технологий: Учебник / В. Е. Сокол, И. А. Ушаков, А. В. Красов, С. В. Черепанов. Часть 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – 200 с. – ISBN 978-5-6049330-8-4.
2. RFC протокол Internet Key Exchange Protocol Version 2 (IKEv2) [Электронный ресурс]. – URL: https://datatracker.ietf.org/doc/html/rfc5996. (дата обращения: 17.12.2025).
3. RFC Security Architecture for the Internet Protocol [Электронный ресурс]. – URL: https://datatracker.ietf.org/doc/html/rfc4301. (дата обращения: 21.01.2026).
4. RFC протокол RADIUS [Электронный ресурс]. – URL: https://datatracker.ietf.org/doc/html/rfc2865. (дата обращения: 15.02.2026).
5. RFC протокол TACACS+ [Электронный ресурс]. – URL: https://datatracker.ietf.org/doc/html/rfc8907. (дата обращения: 15.02.2026).
6. RFC протокол 802.1X [Электронный ресурс]. – URL: https://datatracker.ietf.org/doc/html/rfc3580. (дата обращения: 10.03.2026).
7. RFC Source Address Validation Improvement (SAVI) Solution for DHCP [Электронный ресурс]. – URL: https://datatracker.ietf.org/doc/html/rfc7513. (дата обращения: 10.03.2026).
8. Протокол Generic Routing Encapsulation (GRE) [Электронный ресурс]. – URL: https://datatracker.ietf.org/doc/html/rfc2784. (дата обращения: 15.03.2026).
9. Протокол NHRP [Электронный ресурс]. – Режим доступа: https://datatracker.ietf.org/doc/html/rfc2332. (дата обращения: 15.03.2026).
10. IP Encapsulating Security Payload (ESP) [Электронный ресурс]. – URL: https://datatracker.ietf.org/doc/html/rfc4303. (дата обращения: 15.03.2026).