Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

Защита информации

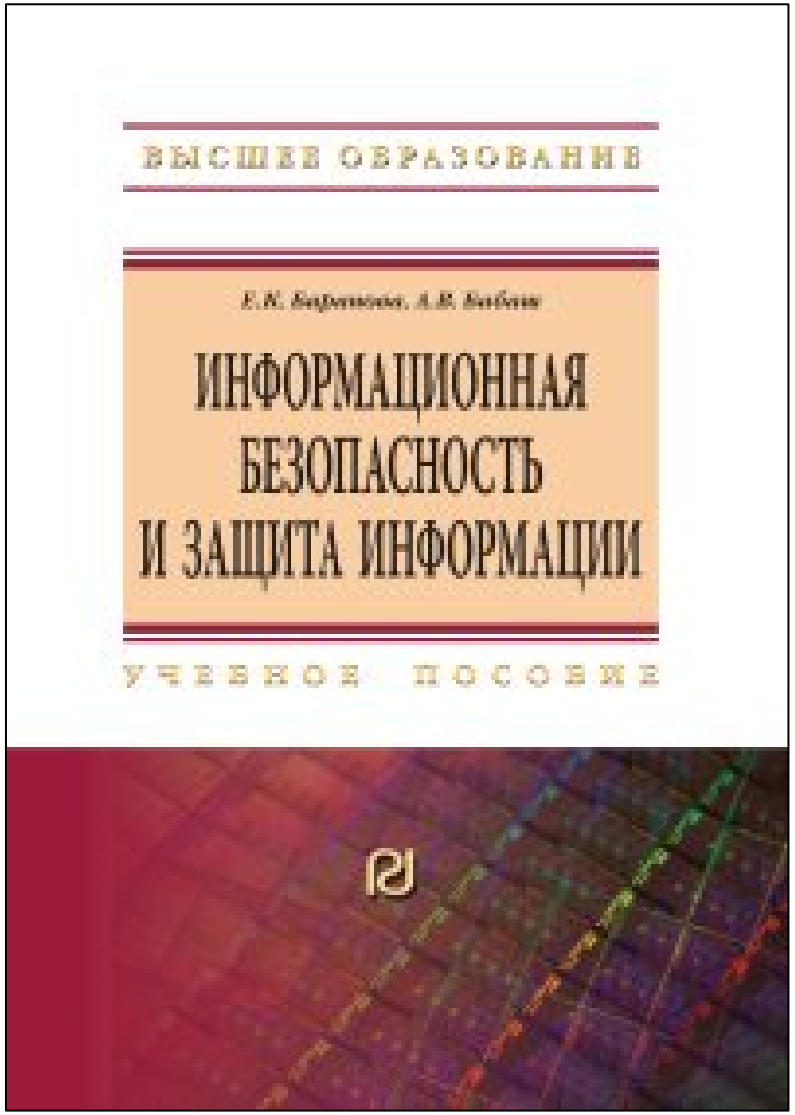
Сетевые атаки и защита информации в компьютерных сетях

КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024

Рекомендуемая литература по теме

Рекомендуемая литература по теме

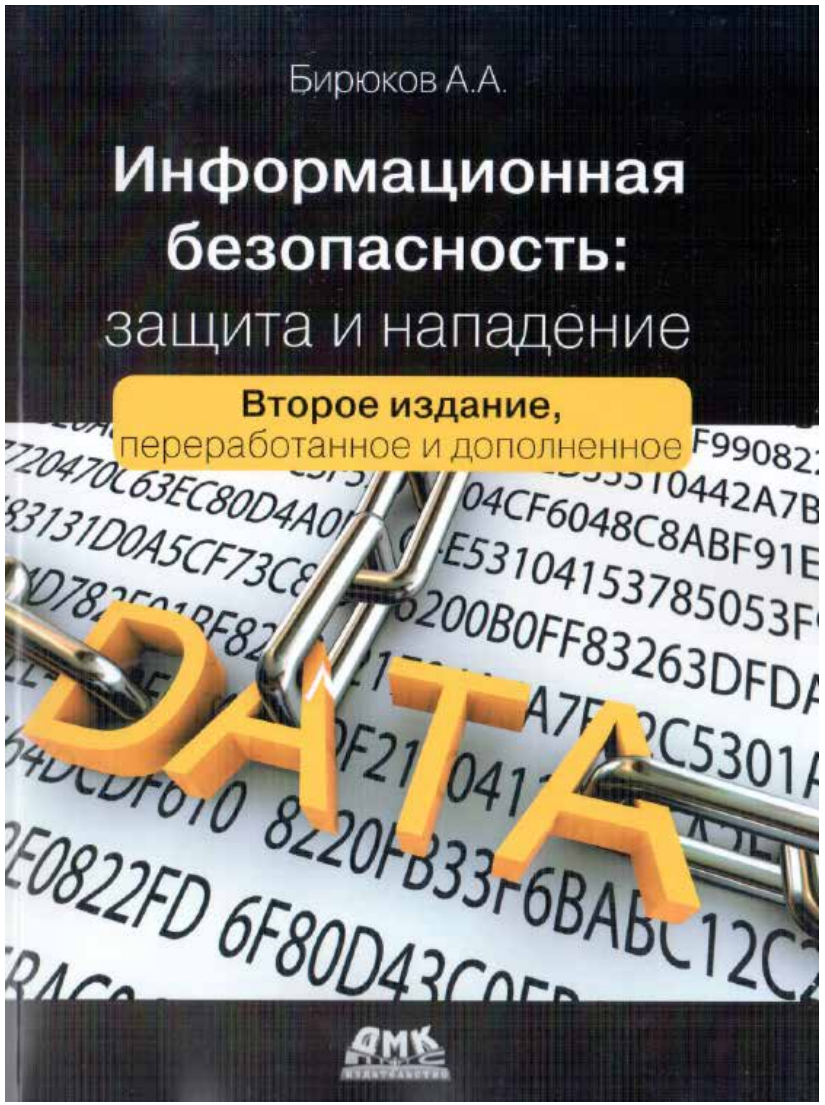


Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование).
DOI: https://doi.org/10.29039/1761-6.

ISBN 978-5-369-01761-6.
Текст : электронный. - URL: https://znanium.com/catalog/product/1189326

Стр.165-220
ГЛАВА 4. Информационная безопасность в компьютерных сетях

Рекомендуемая литература по теме

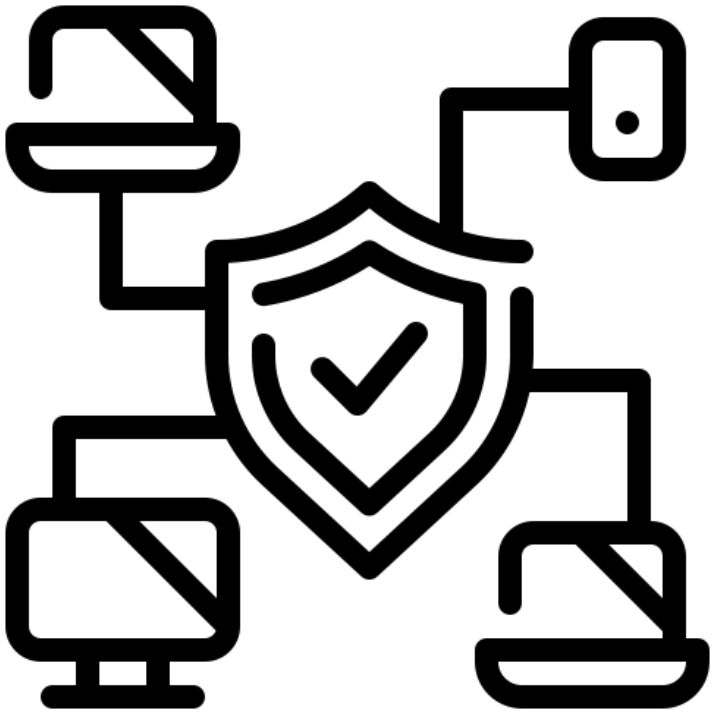


Бирюков А. А.

Информационная безопасность: защита и нападение. - Москва: ДМК Пресс, 2017. - 434 с.:

ISBN 978-5-97060-435-9

https://nnmclub.to/forum/viewtopic.php?t=1114555



1. Особенности обеспечения информационной безопасности в компьютерных сетях

Особенности обеспечения информационной безопасности в компьютерных сетях

- **Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве**, и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Особенности обеспечения информационной безопасности в компьютерных сетях

- **Сетевые системы характерны тем, что наряду с локальными угрозами**, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид угроз, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые **сетевые, или удаленные угрозы**. Они характерны, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по числу попыток, так и по успешности их применения и, соответственно, обеспечение безопасности вычислительных сетей с позиции противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных вычислительных систем состоит в том, что если в локальных вычислительных сетях наиболее частыми являются угрозы раскрытия и целостности, то в сетевых системах на первое место выходит угроза отказа в обслуживании.

Особенности обеспечения информационной безопасности в компьютерных сетях

- **Удаленная угроза** — потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи. Это определение охватывает обе особенности сетевых систем — распределенность компьютеров и распределенность информации.
- Поэтому при рассмотрении вопросов ИБ вычислительных сетей **рассматриваются два подвида удаленных угроз** — это **удаленные угрозы на инфраструктуру и протоколы сети и удаленные угрозы на телекоммуникационные службы**.
- **Первые** используют уязвимости в сетевых протоколах и инфраструктуре сети, а **вторые** — уязвимости в телекоммуникационных службах.

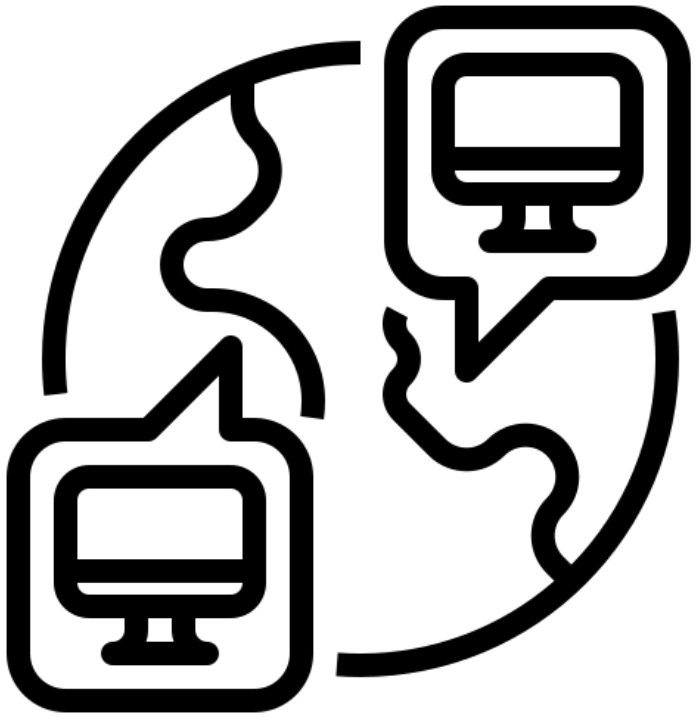
Особенности обеспечения информационной безопасности в компьютерных сетях

- **Цели сетевой безопасности** могут меняться в зависимости от ситуации, но обычно связаны с обеспечением следующих составляющих ИБ:
  - целостность данных;
  - конфиденциальность данных;
  - доступность данных.

- **Целостность данных** — одна из основных целей ИБ сетей — предполагает, что данные не были изменены, подменены или уничтожены в процессе их передачи по линиям связи, между узлами вычислительной сети. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.
- **Конфиденциальность данных** — вторая главная цель сетевой безопасности. При информационном обмене в вычислительных сетях большое количество информации относится к конфиденциальной, например, личная информация пользователей, учетные записи (имена и пароли), данные о кредитных картах и др.
- **Доступность данных** — третья цель безопасности данных в вычислительных сетях. Функциями вычислительных сетей являются совместный доступ к аппаратным и программным средствам сети и совместный доступ к данным. Нарушение И Б как раз и связано с невозможностью реализации этих функций.

Особенности обеспечения информационной безопасности в компьютерных сетях

- **В локальной сети** должны быть доступны принтеры, серверы, рабочие станции, данные пользователей и др.
- **В глобальных вычислительных сетях** должны быть доступны информационные ресурсы и различные сервисы, например почтовый сервер, сервер доменных имен, web-сервер и др.
- При рассмотрении вопросов, связанных с ИБ, в современных вычислительных сетях необходимо учитывать следующие факторы:
  - глобальная связанность;
  - разнородность корпоративных информационных систем;
  - распространение технологии «клиент/сервер».



2. Основы компьютерных сетей

Сетевые модели передачи данных

Транспортный протокол TCP и модель TCP/IP

- За время развития вычислительных сетей было предложено и реализовано много протоколов обмена данными, **самыми удачными из которых явились семейство протоколов TCP/IP (Transmission Control Protocol/ Internet Protocol — протокол управления передачей/межсетевой протокол).**
- **TCP/IP** — это стек протоколов, состоящий из следующих основных компонентов:
  - **межсетевой протокол** (Internet Protocol), обеспечивающий адресацию в сетях (IP-адресацию);
  - **межсетевой протокол управления сообщениями** (Internet Control Message Protocol — ICMP), который обеспечивает низкоуровневую поддержку протокола IP, включая такие функции, как сообщения об ошибках, квитанции, содействие в маршрутизации и т.п.;
  - **протокол разрешения адресов** (Address Resolution Protocol — ARP), выполняющий преобразование логических сетевых адресов в аппаратные, а также обратный ему RARP (Reverse ARP);
  - **протокол пользовательских датаграмм** (User Datagramm Protocol — UDP);
  - **протокол управления передачей** (Transmission Control Protocol — TCP).

Транспортный протокол TCP и модель TCP/IP

- **Протокол UDP** обеспечивает передачу пакетов без проверки доставки, в то время как протокол TCP требует установления виртуального канала и, соответственно, подтверждения доставки пакета с повтором в случае ошибки.
- Этот набор протоколов образует самую распространенную модель сетевого обмена данными, получившую название TCP/IP. **Модель TCP/IP иерархическая и включает четыре уровня.**

Уровни модели TCP/IP

Уровень	*Название*	*Функция*
4	Прикладной	Приложения пользователей, создание сообщений
3	Транспортный	Доставка данных между программами в сети
2	Межсетевой	Адресация и маршрутизация
1	Доступа к среде передачи данных	Сетевые аппаратные средства и их драйверы

Транспортный протокол TCP и модель TCP/IP

- **Прикладной уровень** определяет способ общения пользовательских приложений. В системах «клиент — сервер» приложение-клиент должно знать, как посылать запрос, а приложение-сервер должно знать, как ответить на запрос. Этот уровень обеспечивает такие протоколы, как HTTP, FTP, Telnet.
- **Транспортный уровень** позволяет сетевым приложениям получать сообщения по строго определенным каналам с конкретными параметрами.
- **На сетевом уровне** определяются адреса включенных в сеть компьютеров, выделяются логические сети и подсети, реализуется маршрутизация между ними.
- **На канальном уровне** определяется адресация физических интерфейсов сетевых устройств, например сетевых плат. К этому уровню относятся программы управления физическими сетевыми устройствами, так называемые драйверы.

Сравнительная схема уровневых моделей протоколов OSI и TCP/IP

OSI — Open Systems Interconnection (Модель взаимодействия открытых систем)

Модель OSI

- Модель взаимодействия открытых систем OSI определяет различные уровни взаимодействия систем в сетях с коммутацией пакетов, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень.
- **В модели OSI средства взаимодействия делятся на семь уровней:** прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический.
- Каждый уровень имеет дело с определенным аспектом взаимодействия сетевых устройств.

Сетевая модель стека сетевых протоколов OSI/ISO

Иерархическое представление семи уровней модели OSI

Уровень приложений (седьмой). На этом самом верхнем уровне модели OSI предоставляются средства для доступа пользователей к сетевым ресурсам. Как правило, это единственный уровень, доступный конечным пользователям, поскольку на нем предоставляется интерфейс, на основании которого они осуществляют всю свою деятельность в сети.

Уровень представления данных (шестой). На этом уровне получаемые данные преобразуются в формат, удобный для их чтения на уровне приложений. Порядок кодирования и декодирования данных на этом уровне зависит от протокола, применяемого на уровне приложений для передачи и приема данных. На уровне приложений может также использоваться несколько форм шифрования и дешифрования данных для их защиты.

Иерархическое представление семи уровней модели OSI

Сеансовый уровень (пятый). На этом уровне происходит диалог, или сеанс связи, между двумя компьютерами. Сеансовый уровень отвечает также за установление дуплексного (т.е. двунаправленного) или полудуплексного (т.е. однонаправленного) соединения, а также для корректного (т.е. не резкого и внезапного) разрыва связи между двумя хостами (т.е. сетевыми узлами).

Транспортный уровень (четвертый). Основное назначение транспортного уровня — предоставить надежные транспортные услуги нижележащим уровням. Благодаря управлению потоком данных, их сегментации и десегментации, исправлению ошибок на транспортном уровне обеспечивается безошибочная доставка данных из одной точки сети в другую. Обеспечить надежную доставку данных крайне сложно, поэтому в модели OSI для этой цели выделен отдельный уровень. На транспортном уровне используются протоколы как с установлением соединения, так и без него. Именно на этом уровне и действуют определенные брандмауэры и промежуточные, так называемые прокси-серверы.

Иерархическое представление семи уровней модели OSI

Сетевой уровень (третий). Один из самых сложных уровней модели OSI, обеспечивающий маршрутизацию данных между физическими сетями и правильную адресацию сетевых узлов (например, по IP-адресу). На этом уровне происходит также разбиение потоков данных на более мелкие части, а иногда и обнаружение ошибок. Именно на этом уровне и действуют маршрутизаторы.

Канальный уровень (второй). На этом уровне предоставляются средства для переноса данных по физической сети. Основное назначение данного уровня — предоставить схему адресации для обозначения физических устройств (например, MAC-адреса). Именно на этом уровне и действуют такие физические устройства, как мосты и коммутаторы.

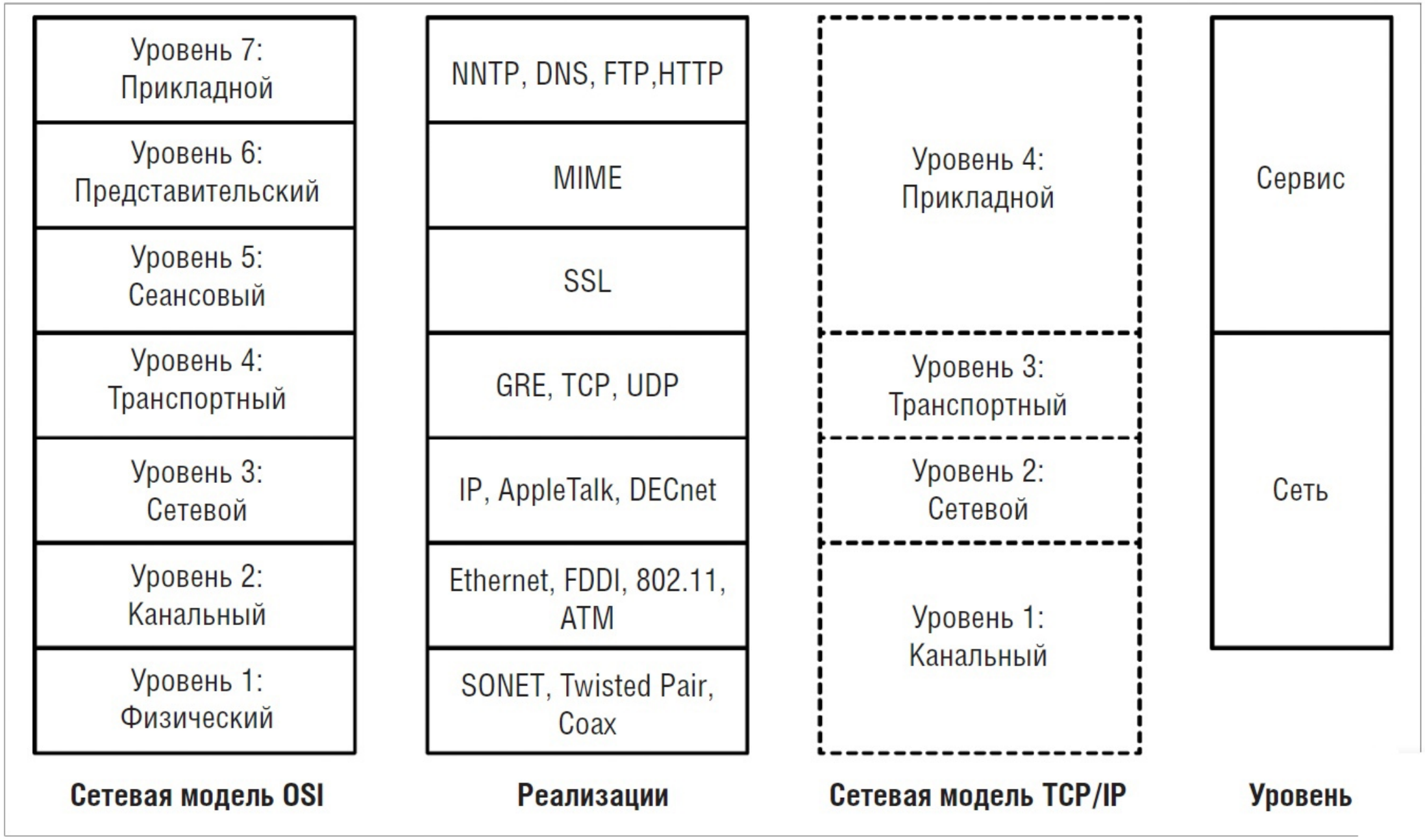
Иерархическое представление семи уровней модели OSI

Физический уровень (первый). Это самый нижний уровень модели OSI, где находится среда, по которой переносятся сетевые данные. На этом уровне определяется физические и электрические характеристики всего сетевого оборудования, включая уровни напряжений в сети, концентраторы, сетевые адаптеры, повторители и кабельную разводку. На физическом уровне устанавливаются и разрываются сетевые соединения, предоставляются средства для совместного использования общих сетевых ресурсов и преобразования сигналов из цифровой в аналоговую форму, и наоборот.

Типичные протоколы, используемые на каждом уровне модели OSI

Уровень	Протоколы
Приложений	HTTP, SMTP, FTP, Telnet
Представления	ASCII, MPEG, JPEG, MIDI
Сеансовый	NetBIOS, SAP, SDP, NWLink
Транспортный	TCP, UDP, SPX
Сетевой	IP, IPX
Канальный	Ethernet, Token Ring, FDDI, AppleTalk
Физический	Проводной или беспроводный

OSI


Уровень 7: Прикладной
Уровень 6: Представительский
Уровень 5: Сеансовый
Уровень 4: Транспортный
Уровень 3: Сетевой
Уровень 2: Канальный
Уровень 1: Физический
Сетевая модель OSI
NNTP, DNS, FTP,HTTP
MIME
SSL
GRE, TCP, UDP
IP, AppleTalk, DECnet
Ethernet, FDDI, 802.11, ATM
SONET, Twisted Pair, Coax
Реализации
Уровень 4: Прикладной
Уровень 3: Транспортный
Уровень 2: Сетевой
Уровень 1: Канальный
Сетевая модель TCP/IP
Сервис
Сеть
Уровень

Соответствие популярных стеков протоколов модели OSI

<table>
<tr><th>Модель OSI</th><th colspan="2">IBM/Microsoft</th><th>TCP/IP</th><th>Novell</th><th>Стек OSI</th></tr>
<tr><td>Прикладной</td><td rowspan="2">SMB</td><td rowspan="3">Telnet,
FTP,
SNMP,
SMTP,
WWW</td><td rowspan="3">NCP,
SAP</td><td>X.400,
X.500,
FTAM</td></tr>
<tr><td>Представления</td><td>Протокол уровня представления OSI</td></tr>
<tr><td>Сеансовый</td><td rowspan="2">NetBIOS</td><td>Сеансовый протокол OSI</td></tr>
<tr><td>Транспортный</td><td rowspan="2">TCP</td><td>SPX</td><td>Транспортный протокол OSI</td></tr>
<tr><td>Сетевой</td><td colspan="2"></td><td>IP,
RIP,
OSPF</td><td>IPX,
RIP,
NLSP</td><td>ES-ES,
IS-IS</td></tr>
<tr><td>Канальный</td><td colspan="5">802.3 (Ethernet), 802.5 (Token Ring), FDDI, Fast Ethernet, SLIP, 100VG-AnyLAN, X.25, ATM, LAP-B, LAP-D, PPP</td></tr>
<tr><td>Физический</td><td colspan="5">Коаксиал, экранированная и неэкранированная витая пара, оптоволокно, радиоволны</td></tr>
</table>

Распределение функций безопасности по уровням OSI

Функция безопасности	*Уровень OSI*						
	1	2	3	4	5	6	7
Аутентификация	–	–	+	+	–	–	+
Управление доступом	–	–	+	+	–	–	+
Конфиденциальность соединения	+	+	+	+	–	+	+
Конфиденциальность вне соединения	–	+	+	+	–	+	+
Избирательная конфиденциальность	–	–	–	–	–	+	+
Конфиденциальность трафика	+	–	+	–	–	–	+
Целостность с восстановлением	–	–	–	+	–	–	+
Целостность без восстановления	–	–	+	+	–	–	+
Избирательная целостность	–	–	–	–	–	–	+
Целостность вне соединения	–	–	+	+	–	–	+
Неотказуемость	–	–	–	–	–	–	+

«+» данный уровень может предоставить функцию безопасности;
«—» данный уровень не подходит для предоставления функции безопасности.

Протоколы, действующие на одном и том же уровне как в передающей, так и в принимающей системе

Графическое представление инкапсуляции данных при их обмене между клиентом и сервером

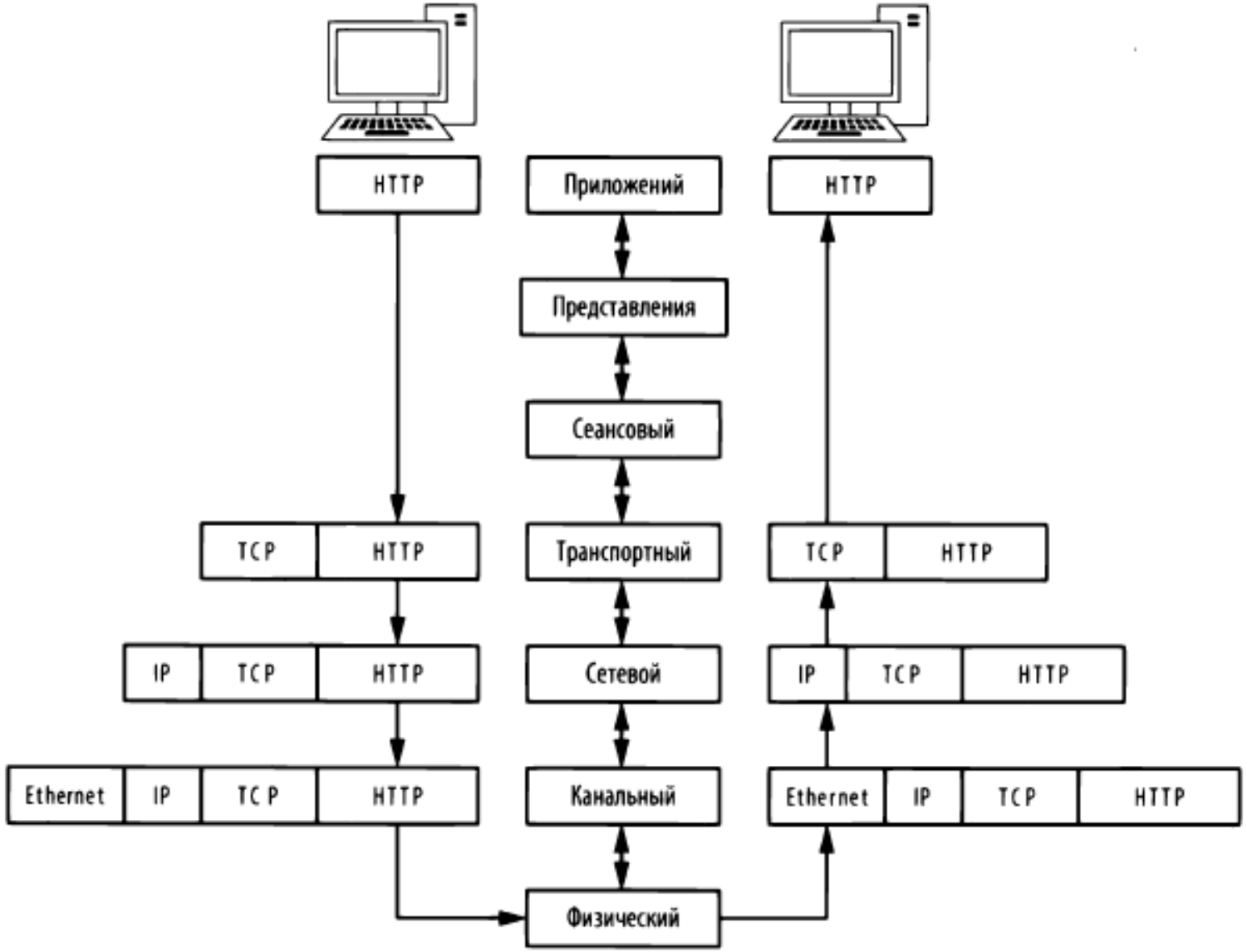
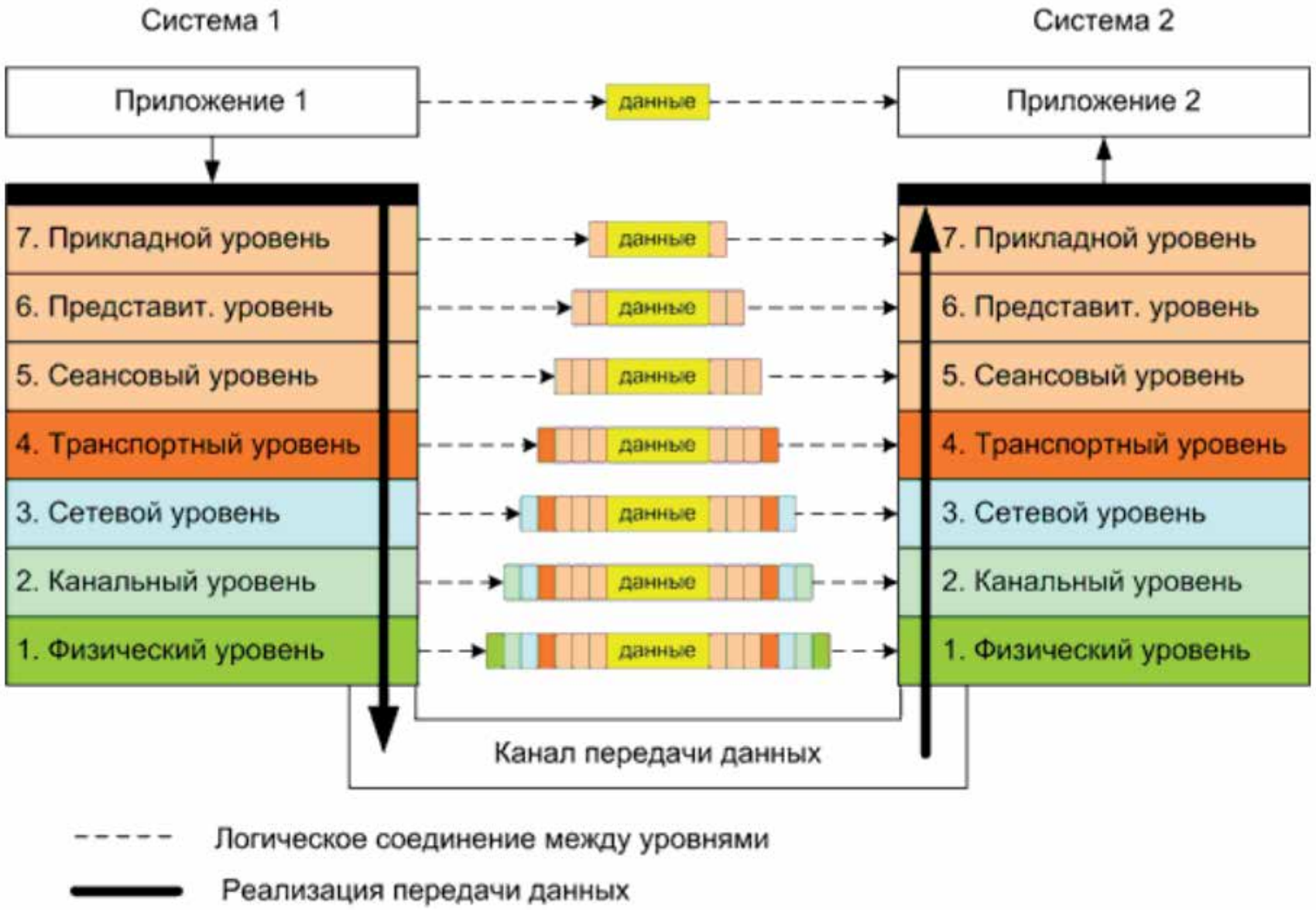


Схема пакета для различных уровней OSI



Порядок прохождения трофика, когда компьютер А передает данные компьютеру Б через концентратор

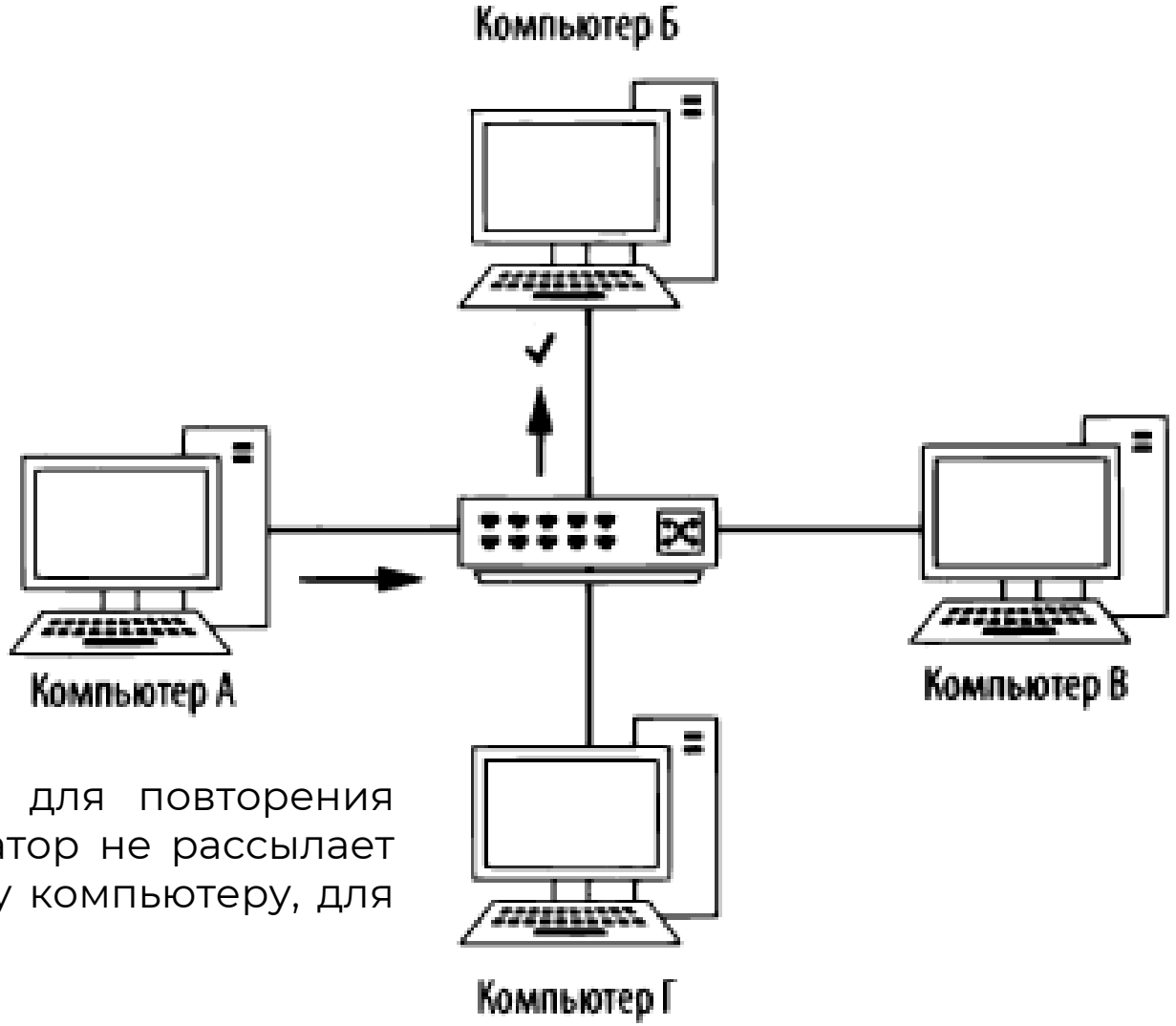
Концентраторы могут формировать немало излишнего сетевого трафика и **способны работать только в полудуплексном режиме**, т.е. они не в состоянии одновременно передавать и принимать данные. Поэтому **концентраторы, как правило, не применяются в большинстве современных сетей**, а также в сетях с высоким трафиком, где вместо них используются коммутаторы, рассматриваемые далее.

Единственное преимущество концентратора — низкая стоимость

Концентратор - это всего лишь повторитель работающий на физическом уровне модели OSI. Он принимает пакеты, посылаемые из одного порта, и передает их во все остальные порты , т.е. повторяет их, а обязанность приемного устройства - принять или отвергнуть каждый пакет.

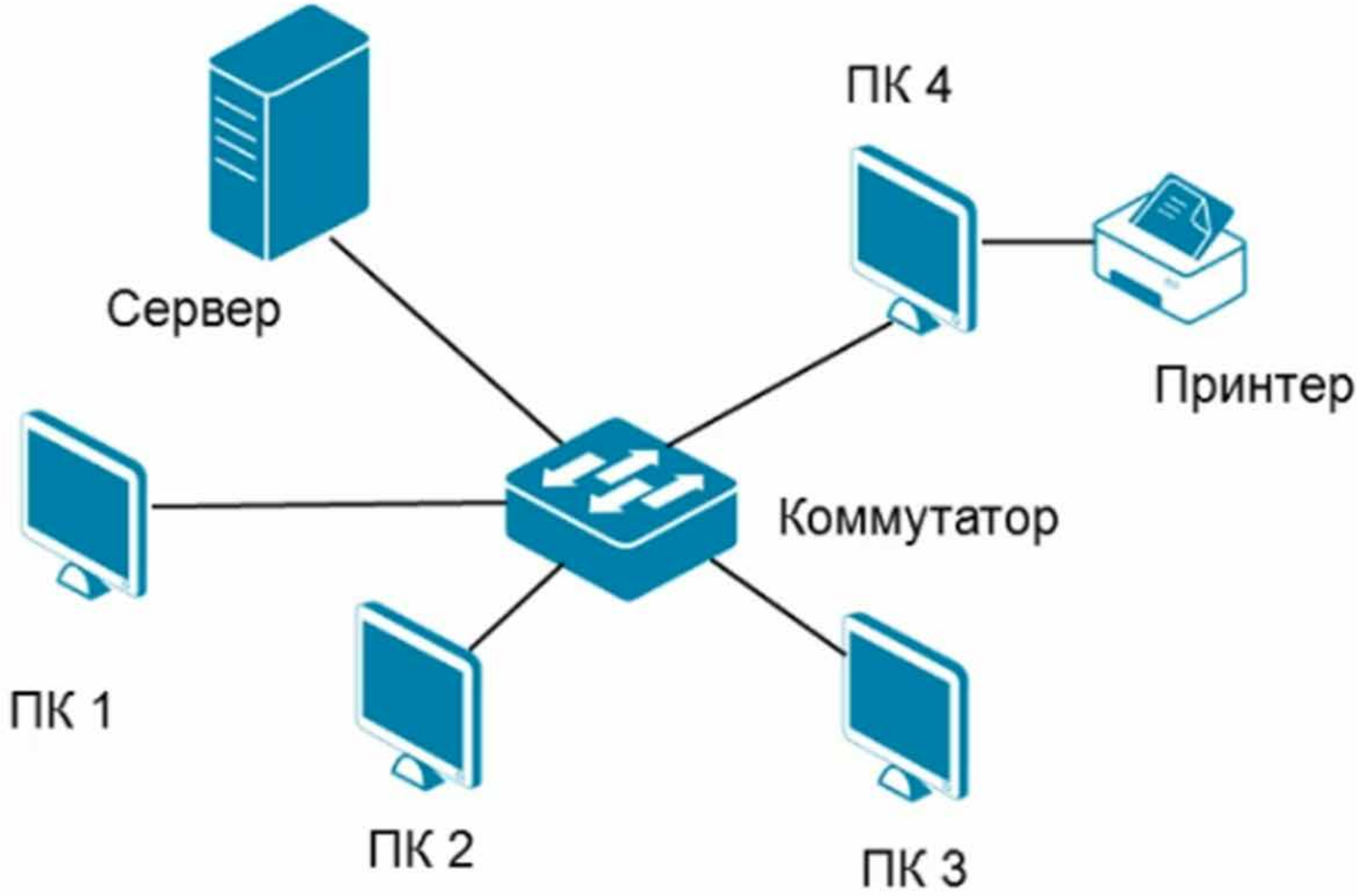
Порядок прохождения трафика, когда компьютер А передает данные компьютеру Б через коммутатор

Наилучшим вариантом замены концентраторов в производственных и сетях с высоким трафиком являются **коммутаторы - дуплексные устройства, способные синхронно передавать и принимать данные.**



Как и концентратор, коммутатор предназначен для повторения пакетов. Но в отличие от концентратора, коммутатор не рассылает данные в каждый порт, а посылает их только тому компьютеру, для которого они предназначены.

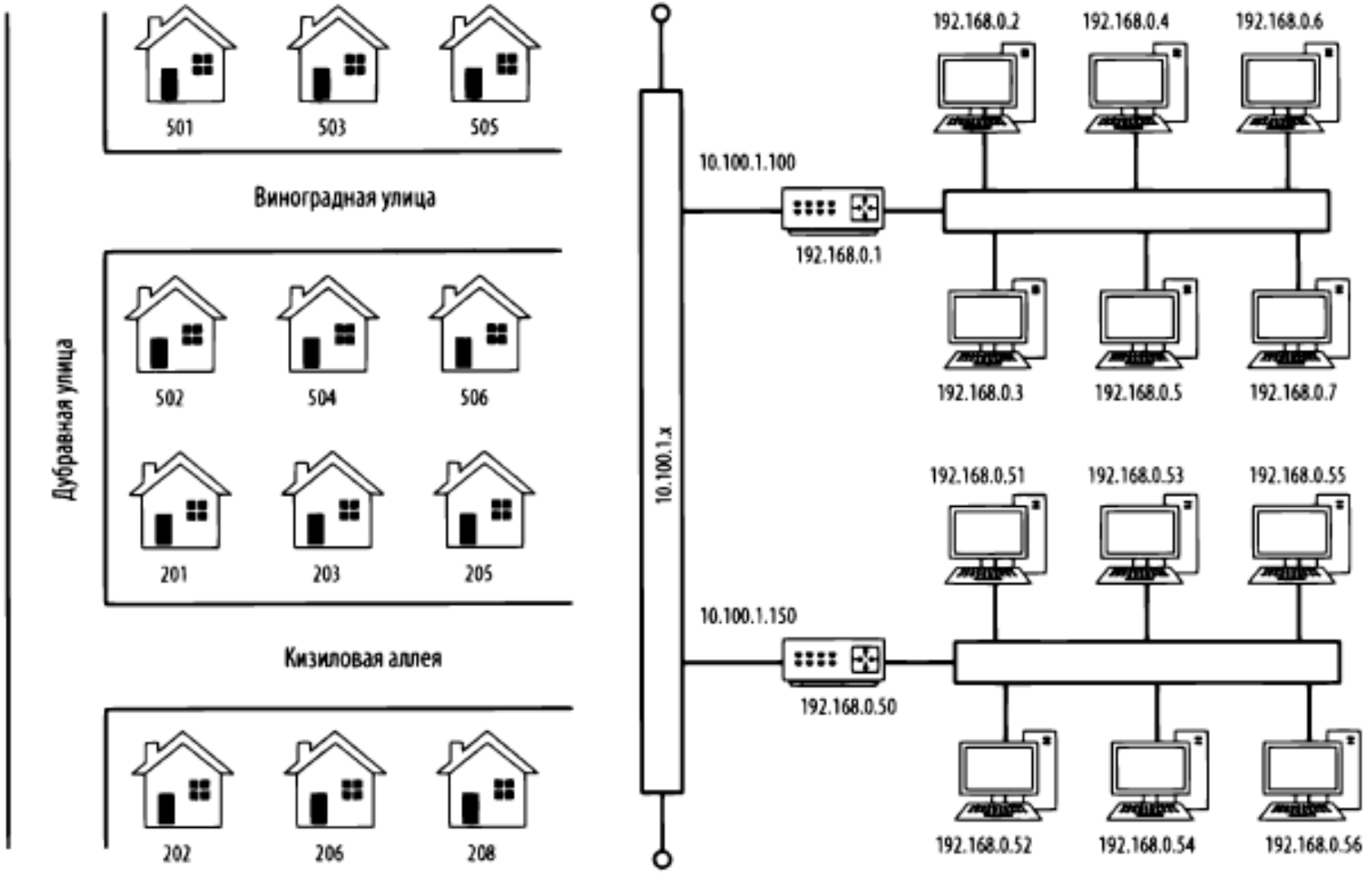
Типичная сеть небольшого офиса



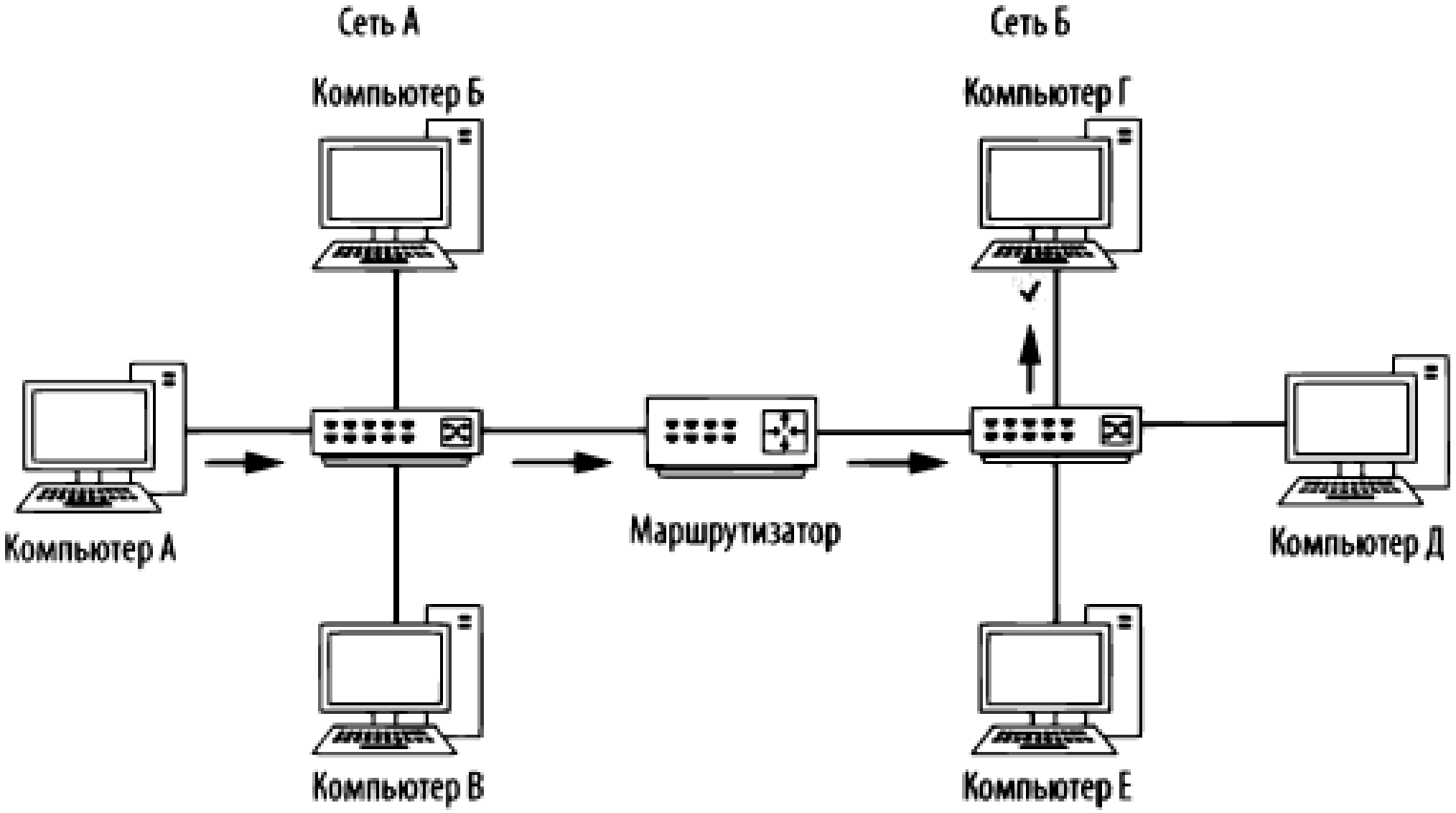
Маршрутизатор (router)

- **Маршрутизатор (от англ. router) или ро́утер** — специализированное устройство, которое пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации.
- Маршрутизатор может связывать разнородные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определённые правила, заданные администратором.
- Маршрутизаторы работают на «сетевом» (третьем) уровне сетевой модели OSI, в отличие от коммутаторов (свитчей) и концентраторов (хабов), которые работают соответственно на втором и первом уровнях модели OSI.

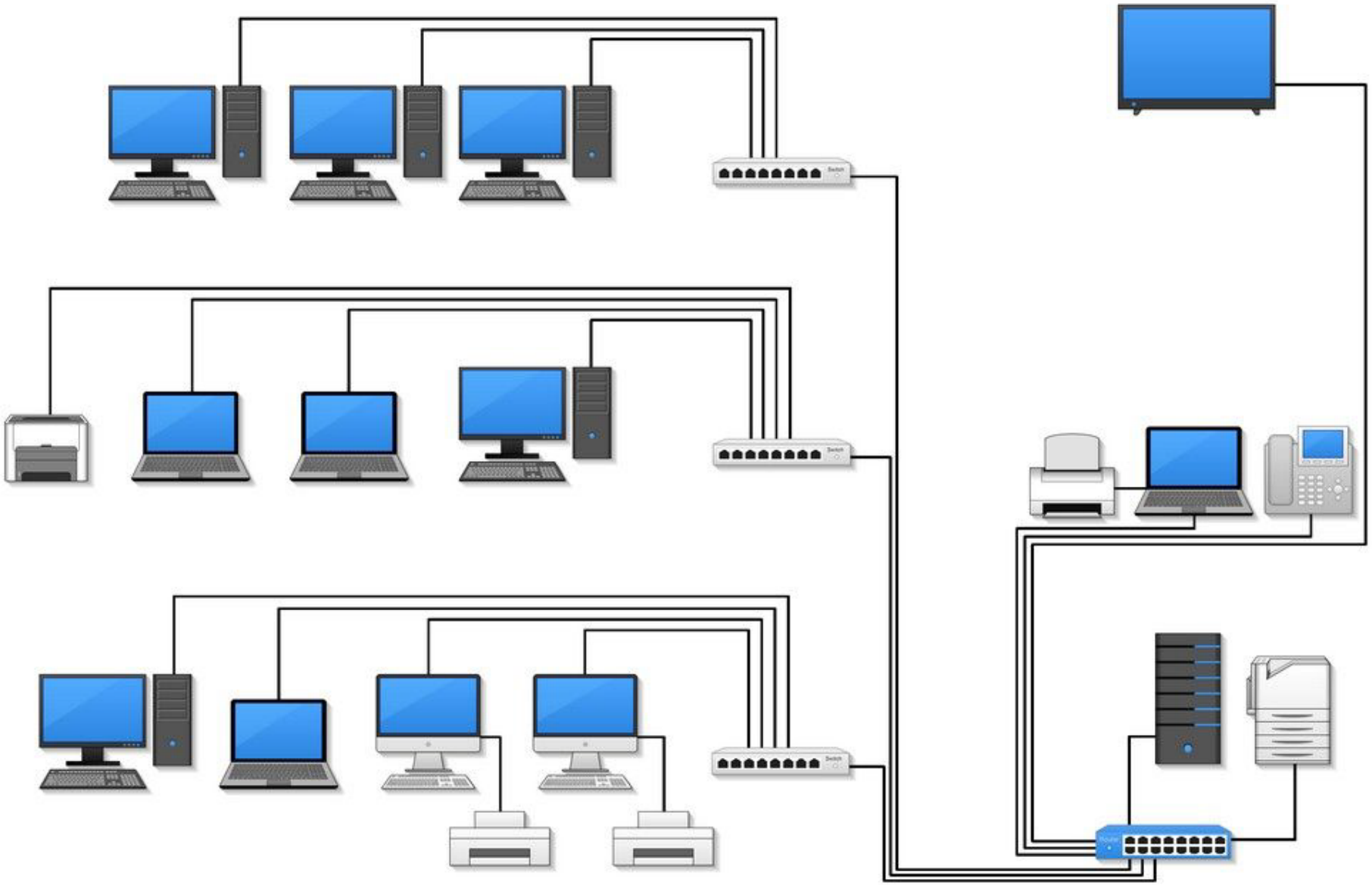
Сравнение маршрутизируемой сети с соседством городских улиц



Порядок прохождения сетевого трафика, когда компьютер А в одной сети передает данные компьютеру Г в другой сети через маршрутизатор

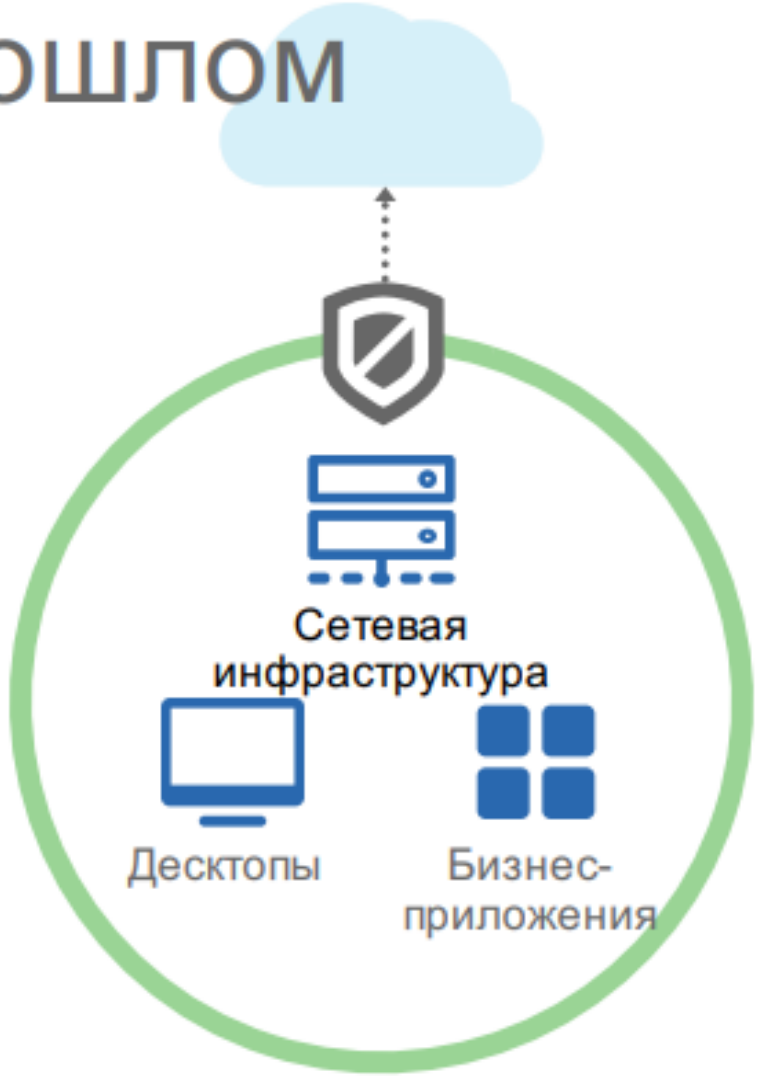


Пример компьютерной сети офиса

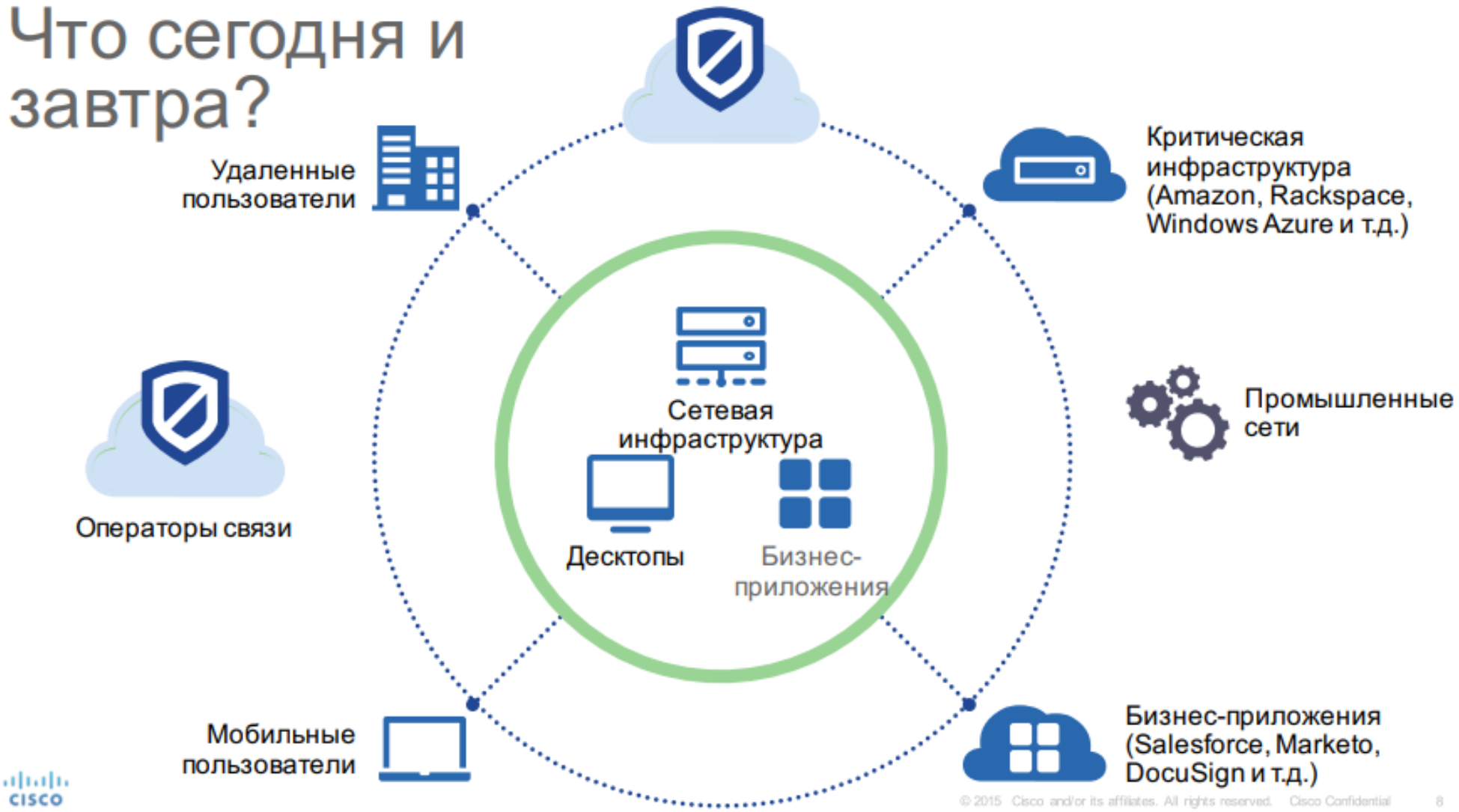


Компьютерные сети

Так было в прошлом



Компьютерные сети



Три компонента безопасности в компьютерных сетях

- **Обеспечение безопасности информации в компьютерных сетях следует рассматривать в виде единства трех компонентов**, оказывающих взаимное влияние друг на друга:
  - информация;
  - технические и программные средства;
  - обслуживающий персонал и пользователи.

Угрозы безопасности в компьютерных системах

3. Угрозы безопасности в компьютерных сетях

Классификация сетевых (удаленных) атак

Классификации атак

- **Эффективная защита от потенциальных сетевых атак невозможна без их детальной классификации**, облегчающей их выявление и задачу противодействия им.
- **В настоящее время известно большое количество различных типов классификационных признаков.**
- В качестве таких признаков может быть выбрано, например, разделение на пассивные и активные, внешние и внутренние атаки, умышленные и неумышленные и т.д..
- **К сожалению, несмотря на то, что некоторые из существующих классификаций мало применимы на практике, их активно используют при выборе систем обнаружения вторжений и атак и их эксплуатации.**

Виды классификаций атак

- **Классификация атак:**
  - По характеру воздействия
  - По цели воздействия
  - По наличию обратной связи с атакуемым объектом
  - По условию начала осуществления воздействия
  - По расположению субъекта атаки относительно атакуемого объекта
  - По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие
  - Классификация уязвимостей сканера Nessus
  - Классификация Питера Мелла в работе "Компьютерные атаки: что это и как им противостоять"
- Затем, более подробно разберем наиболее часто используемые

По характеру воздействия

- **По характеру воздействия: пассивное, активное**
- **Пассивное** воздействие на распределённую вычислительную систему (РВС) представляет собой некоторое воздействие, не оказывающее прямого влияния на работу системы, но в то же время способное нарушить её политику безопасности. Отсутствие прямого влияния на работу РВС приводит именно к тому, что пассивное удалённое воздействие (ПУВ) трудно обнаружить. Возможным примером типового ПУВ в РВС служит прослушивание канала связи в сети.
- **Активное воздействие** на РВС — воздействие, оказывающее прямое влияние на работу самой системы (нарушение работоспособности, изменение конфигурации РВС и т. д.), которое нарушает политику безопасности, принятую в ней. **Активными воздействиями являются почти все типы удалённых атак.** Связано это с тем, что в саму природу наносящего ущерб воздействия включается активное начало. Явное отличие активного воздействия от пассивного — принципиальная возможность его обнаружения, так как в результате его осуществления в системе происходят некоторые изменения. При пассивном же воздействии, не остается совершенно никаких следов (из-за того, что атакующий просмотрит чужое сообщение в системе, в тот же момент не изменится собственно ничего).

По цели воздействия

- **По цели воздействия**
  - **нарушение функционирования системы** (доступа к системе)
  - **нарушение целостности** информационных ресурсов
  - **нарушение конфиденциальности** информационных ресурсов

- Этот признак, по которому производится классификация, по сути есть прямая проекция трех базовых разновидностей угроз — отказа в обслуживании, раскрытия и нарушения целостности.

Классификация атак

По цели воздействия

- **Главная цель, которую преследуют практически при любой атаке — получение несанкционированного доступа к информации.**
- **Существуют два принципиальных варианта получения информации: искажение и перехват.**
- **Вариант перехвата информации** означает получение к ней доступа без возможности её изменения. Перехват информации приводит, следовательно, к нарушению её конфиденциальности. Прослушивание канала в сети — пример перехвата информации. В этом случае имеется нелегитимный доступ к информации без возможных вариантов её подмены. Очевидно, что нарушение конфиденциальности информации относится к пассивным воздействиям.
- **Возможность подмены информации следует понимать либо как полный контроль над потоком информации между объектами систем**ы, либо возможность передачи различных сообщений от чужого имени. Следовательно, понятно, что **подмена информации приводит к нарушению её целостности**. Такое информационное разрушающее воздействие есть характерный пример активного воздействия. Примером же удалённой атаки, предназначенной для нарушения целостности информации, может послужить удалённая атака (УА) **«Ложный объект РВС»**.

Классификация атак
По наличию обратной связи с атакуемым объектом

- **По наличию обратной связи с атакуемым объектом**
  - **с обратной связью**
  - **без обратной связи (однонаправленная атака)**

- **Атакующий отправляет некоторые запросы на атакуемый объект, на которые ожидает получить ответ**. Следовательно между атакующим и атакуемым появляется обратная связь, позволяющая первому адекватно реагировать на всяческие изменения на атакуемом объекте. В этом суть удалённой атаки, осуществляемой при наличии обратной связи с атакующим объектом. Подобные атаки наиболее характерны для распределенных вычислительных систем.
- **Атаки без обратной связи** характерны тем, что им не требуется реагировать на изменения на атакуемом объекте. Такие атаки обычно осуществляются при помощи передачи на атакуемый объект одиночных запросов. Ответы на эти запросы атакующему не нужны. Подобную удаленную атаку можно назвать также однонаправленной удаленной атакой. Примером однонаправленных атак является - «**DoS-атака**».

Классификация атак
По условию начала осуществления воздействия

- **По условию начала осуществления воздействия**
- Удалённое воздействие, также как и любое другое, может начать осуществляться только при определённых условиях.

- В распределённой вычислительной системе (сети) существуют три вида таких условных атак:
  - атака по запросу от атакуемого объекта
  - атака по наступлению ожидаемого события на атакуемом объекте
  - безусловная атака

Классификация атак
По условию начала осуществления воздействия

- Воздействие со стороны атакующего начнётся при условии, что потенциальная цель атаки передаст запрос определённого типа. Такую атаку можно назвать **атакой по запросу от атакуемого объекта**. Данный тип УА наиболее характерен для РВС. Примером подобных запросов в сети Интернет может служить DNS- и ARP-запросы.
- **Атака по наступлению ожидаемого события на атакуемом объекте.** Атакующий непрерывно наблюдает за состоянием ОС удалённой цели атаки и начинает воздействие при возникновении конкретного события в этой системе. Атакуемый объект сам является инициатором начала атаки. Примером такого события может быть прерывание сеанса работы пользователя с сервером без выдачи команды LOGOUT в Novell NetWare.
- **Безусловная атака** осуществляется немедленно и безотносительно к состоянию операционной системы и атакуемого объекта. Следовательно, атакующий является инициатором начала атаки в данном случае.
- При нарушении нормальной работоспособности системы преследуются другие цели и получение атакующим незаконного доступа к данным не предполагается. Его целью является вывод из строя ОС на атакуемом объекте и невозможность доступа для остальных объектов системы к ресурсам этого объекта. Примером атаки такого вида может служить удаленная атака «DoS-атака».

Классификация атак

По расположению субъекта атаки относительно атакуемого объекта

- **По расположению субъекта атаки относительно атакуемого объекта**
  - **межсегментное**
  - **внутрисегментное**

- С точки зрения удалённой атаки крайне важным является взаимное расположение субъекта и объекта атаки, то есть находятся ли они в разных или в одинаковых сегментах. Во время внутрисегментной атаки, субъект и объект атаки располагаются в одном сегменте. В случае межсегментной атаки субъект и объект атаки находятся в разных сетевых сегментах. Этот классификационный признак дает возможность судить о так называемой «степени удалённости» атаки.
- Практически внутрисегментную атаку осуществить намного проще, чем межсегментную. Однако межсегментная удалённая атака представляет куда большую опасность, чем внутрисегментная. Это связано с тем, что в случае межсегментной атаки объект её и непосредственно атакующий могут находиться на расстоянии многих тысяч километров друг от друга, что может существенно воспрепятствовать мерам по отражению атаки.

Классификация атак

По расположению субъекта атаки относительно атакуемого объекта

- **По уровню эталонной модели ISO/OSI**, на котором осуществляется воздействие
  - физический
  - канальный
  - сетевой
  - транспортный
  - сеансовый
  - представительный
  - прикладной

- Международной организацией по стандартизации (ISO) был принят стандарт ISO 7498, который описывает взаимодействие открытых систем (OSI), к которым принадлежат также и распределенные вычислительные системы и сети. Каждый сетевой протокол обмена, также как и каждую сетевую программу, удаётся так или иначе спроецировать на эталонную 7-уровневую модель OSI. Такая многоуровневая проекция даёт возможность описать в терминах модели OSI использующиеся в сетевом протоколе или программе функции.

Классификация сетевых атак по работе Питера Мелла «Компьютерные атаки: что это и как им противостоять»

- Классификация сетевых атак по работе Питера Мелла «Компьютерные атаки: что это и как им противостоять»
  - удаленное проникновение (remote penetration)
  - локальное проникновение (local penetration)
  - удаленный отказ в обслуживании (remote denial of service)
  - локальный отказ в обслуживании (local denial of service)
  - атаки с использованием сетевых сканеров (network scanners)
  - атаки с использованием сканеров уязвимостей (vulnerability scanners)
  - атаки с использованием взломщиков паролей (password crackers)
  - атаки с использованием анализаторов протоколов (sniffers)

Peter M. Mell - Computer Attacks: What They Are and How to Defend Against Them (May 26, 1999)
https://www.nist.gov/publications/computer-attacks-what-they-are-and-how-defend-against-them
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151188

Классификация сетевых атак

- **удаленное проникновение (от англ. remote penetration)** — это тип атак, которые позволяют реализовать удаленное управление компьютером через сеть;
- **локальное проникновение (от англ. local penetration)** — это тип атак, которые приводят к получению несанкционированного доступа к узлу, на который они направлены;
- **удаленный отказ в обслуживании (от англ. remote denial of service)** — тип атак, которые позволяют нарушить функционирование системы в рамках глобальной сети;

Классификация сетевых атак

- **локальный отказ в обслуживании (от англ. local denial of service)** — тип атак, позволяющих нарушить функционирование системы в рамках локальной сети. В качестве примера такой атаки можно привести внедрение и запуск враждебной программы, которая загружает центральный процессор бесконечным циклом, что приводит к невозможности обработки запросов других приложений;
- **атаки с использованием сетевых сканеров (от англ. network scanners)** — это тип атак, основанных на использовании сетевых сканеров — программ, которые анализируют топологию сети и обнаруживают сервисы, доступные для атаки; пример: атака с использованием утилиты `nmap`;

Классификация сетевых атак

- **атаки с использованием взломщиков паролей (от англ. password crackers)** — это тип атак, которые основаны на использовании взломщиков паролей — программ, подбирающих пароли пользователей;

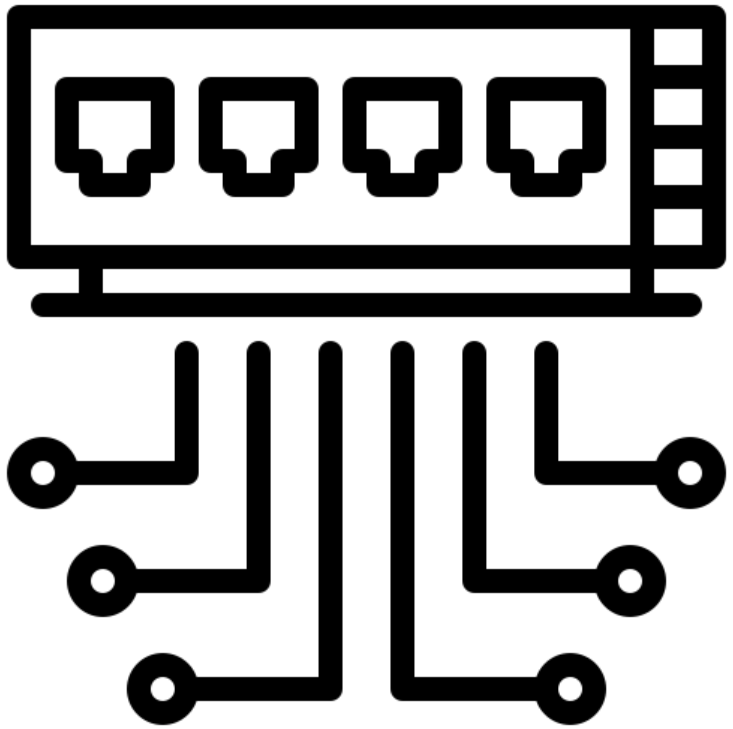
- **атаки с использованием сканеров уязвимостей (от англ. vulnerability scanners)** — тип атак, основанных на использовании сканеров уязвимостей — программ, осуществляющих поиск уязвимостей на узлах сети, которые в дальнейшем могут быть применены для реализации сетевых атак;

Классификация сетевых атак

- **атаки с использованием анализаторов протоколов (от англ. sniffers)** — это тип атак, основанных на использовании анализаторов протоколов — программах, "прослушивающих сетевой трафик. С их помощью можно автоматизировать поиск в сетевом трафике такой информации, как идентификаторы и пароли пользователей, информацию о кредитных картах и т. д.

Классификация уязвимостей сканера Nessus

- **В сканере уязвимостей Nessus используется классификация "по характеру уязвимости", используемой для реализации атаки:**
  - "черные ходы" (Backdoors);
  - ошибки в CGI скриптах (CGI abuses);
  - атаки типа "отказ в обслуживании" (Denial of Service);
  - ошибки в программах — FTP-серверах (FTP);
  - наличие на компьютере сервиса Finger или ошибки в программах, реализующих этот сервис (Finger abuses);
  - ошибки в реализации межсетевых экранов (Firewalls);
  - ошибки, позволяющие пользователю, имеющему терминальный вход на данный сервер, получить права администратора (Gain a shell remotely);
  - ошибки, позволяющие атакующему удаленно получить права администратора (Gain root remotely);
  - прочие ошибки, не вошедшие в другие категории (Misc);
  - ошибки в программах — NIS-серверах (NIS);
  - ошибки в программах — RPC-серверах (RPC);
  - уязвимости, позволяющие атакующему удаленно получить любой файл с сервера (Remote file access);
  - ошибки в программах — SMTP-серверах (SMTP problems);
  - неиспользуемые сервисы (Useless services).



4. По уровню эталонной модели OSI

Физический уровень (первый). Это самый нижний уровень модели OSI, где находится среда, по которой переносятся сетевые данные. На этом уровне определяется физические и электрические характеристики всего сетевого оборудования, включая уровни напряжений в сети, концентраторы, коммутаторы, роутеры, сетевые адаптеры, повторители, кабельная разводка и др. На физическом уровне устанавливаются и разрываются сетевые соединения, предоставляются средства для совместного использования общих сетевых ресурсов и преобразования сигналов из цифровой в аналоговую форму, и наоборот.

4.1. Атаки на физическом уровне, на сетевое оборудование

Атаки на коммутаторы (switch)

- Коммутатор (switch) является более интеллектуальным устройством, чем концентратор. Коммутаторы работают на канальном уровне модели OSI. Получая пакет на одни из своих портов, он, в отличие от концентратора, не пересылает его на все порты, а пересылает только на тот порт, к которому подключен получатель пакета.
- **На канальном уровне возможны следующие типы атак:**
  - переполнение CAM-таблицы;
  - VLAN Hopping;
  - атака на STP;
  - MAC-спуфинг;
  - атака на PVLAN;
  - атака на DHCP
  - ARP-spoofing.
- Рассмотрим каждую из атак более подробно.

12 миллионов роутеров и DSL-модемов с уязвимостями

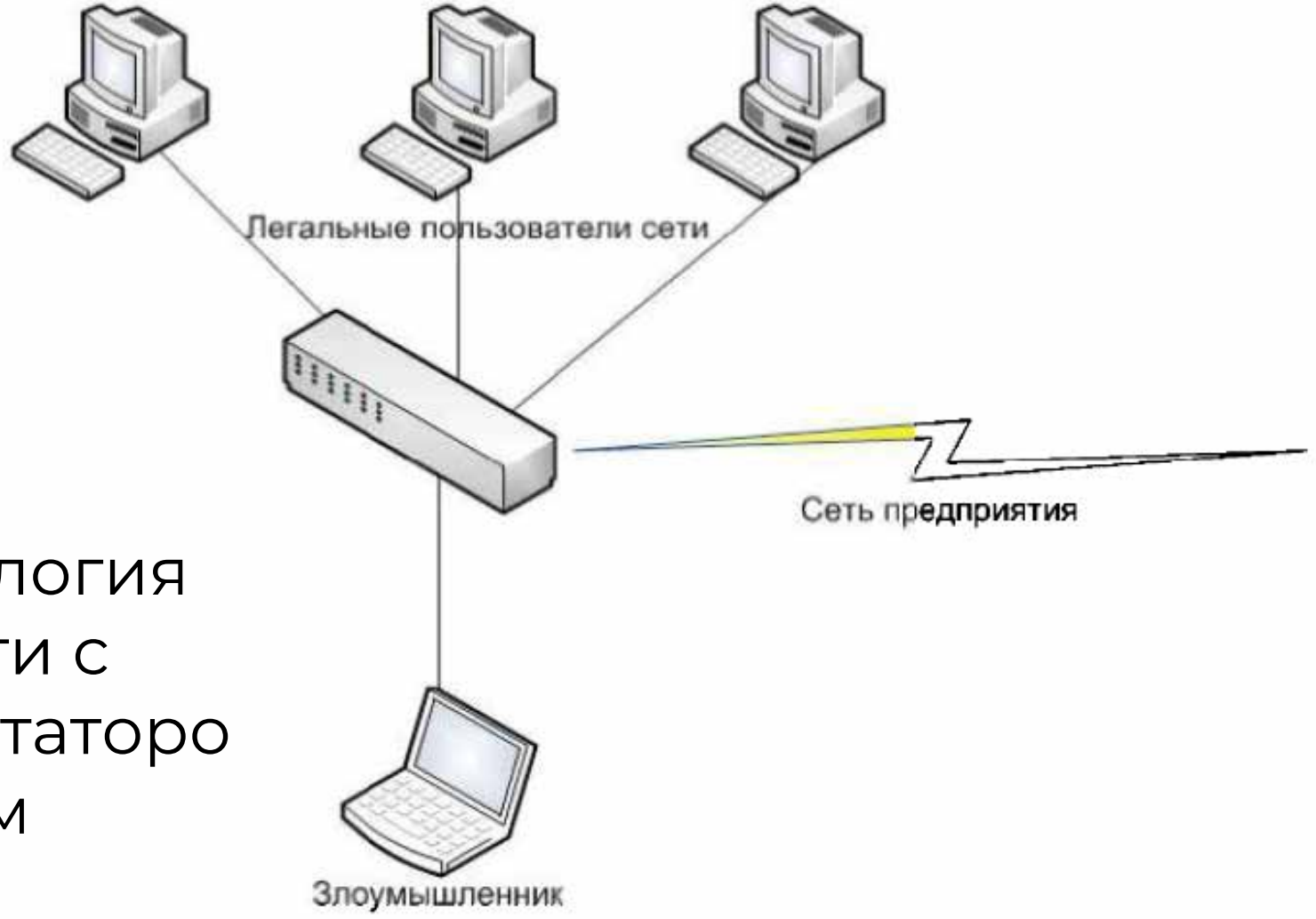
- В декабре 2020 года специалисты компании Check Point **обнаружили свыше 12 миллионов роутеров (в том числе топовых моделей) и DSL-модемов**, **которые можно взломать из-за уязвимости** в механизме получения автоматических настроек. Он широко применяется для быстрой настройки сетевого оборудования на стороне клиента (CPE — customer premises equipment).
- Последние десять лет провайдеры используют для этого протокол управления абонентским оборудованием CWMP (CPE WAN Management Protocol). Спецификация TR-069 предусматривает возможность отправлять с его помощью настройки и подключать сервисы через сервер автоконфигурации (ACS — Auto Configuration Server).
- Сотрудники Check Point установили, что **во многих роутерах есть ошибка обработки CWMP-запросов**, а провайдеры еще усложняют ситуацию: большинство из них никак не шифруют соединение между ACS и оборудованием клиента и не ограничивают доступ по IP- или MAC-адресам.
- **Вместе это создает условия для легкой атаки по типу man-in-the-middle — «человек посередине».**

Переполнение CAM-таблицы

- **Коммутатор имеет CAM-таблицу (Content Address Memory), где содержится привязка MAC-адресов к портам коммутатора. То есть в данной таблице указано, какие MAC-адреса на каком порту принимаются. CAM-таблица имеет ограниченный размер**, например для коммутатора Cisco Catalyst 2960 таблица может хранить до 8192 MAC-адресов, а Catalyst 6000-й серии - до 128 000 MAC-адресов.
- **В случае если таблица будет полностью занята, новые записи не смогут добавляться, и весь трафик будет проходить на все порты.** Тогда коммутатор начнет работать как обычный концентратор, и весь трафик, проходящий через данный сегмент сети, **можно будет прослушать с помощью утилиты Wireshark.**
- Конечно, прослушать весь график в локальной сети злоумышленнику таким способом не удастся, но инсайдер, работающий в одном сегменте сети, к примеру с бухгалтерией, сможет перехватывать трафик и получить конфиденциальную информацию.

Wireshark — программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других.
https://www.wireshark.org/download.html

Переполнение CAM-таблицы

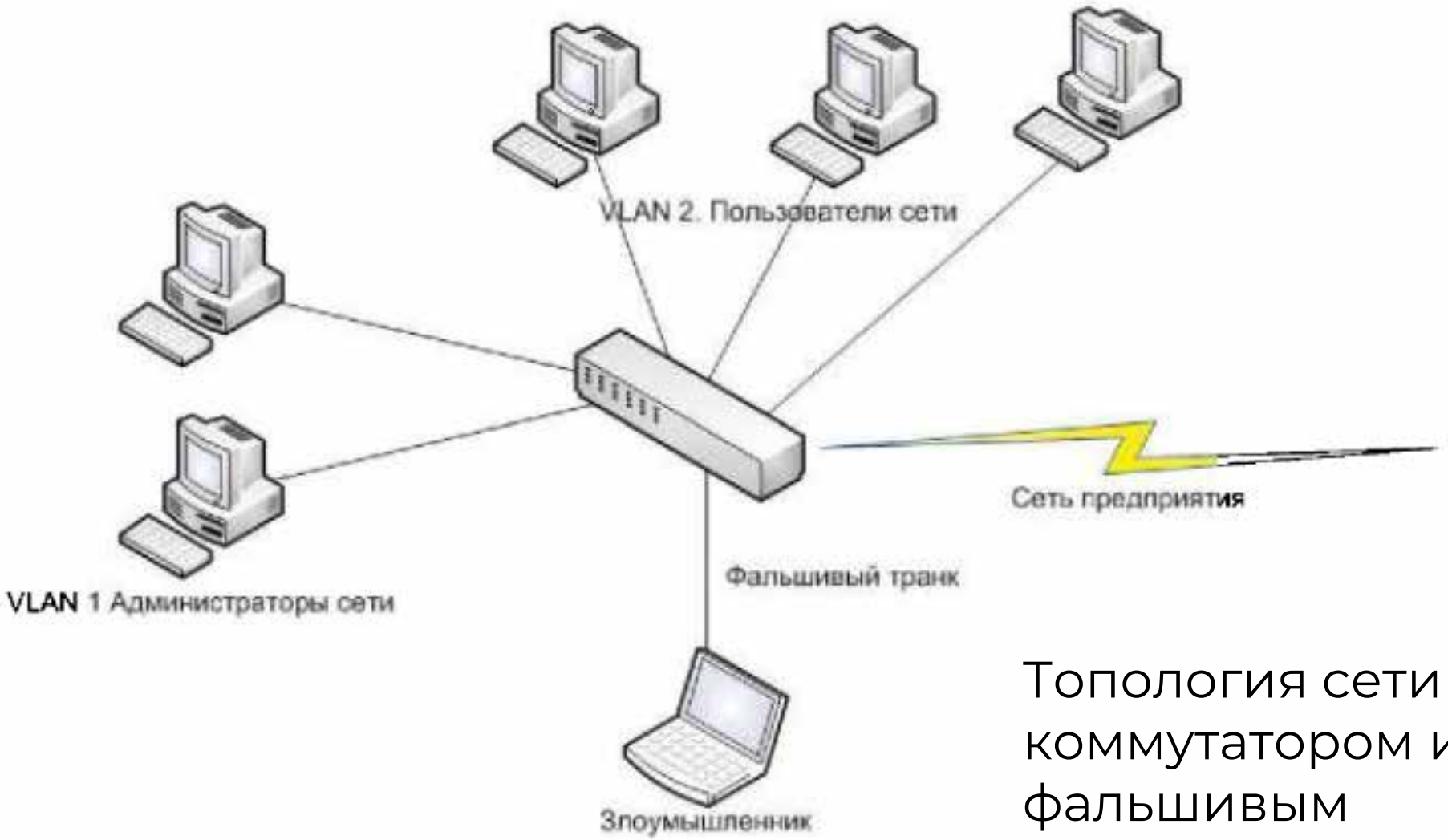


Топология сети с коммутатором

VLAN Hoping

- С помощью данной атаки злоумышленник может попытаться передать данные в другой VLAN.
- Как известно, для взаимодействия между виртуальными локальными сетями VLAN в коммутаторах используется режим trunk.
- В коммутаторах Cisco Catalyst по умолчанию порт работает не в режиме mode access и не в режиме mode trunk, таким образом, на порту **работает протокол DTP (Dynamic Trunk Protocol).**
- Очевидно, что при такой настройке портов коммутатора злоумышленнику достаточно притвориться коммутатором, как между ними будет установлено транковое соединение и, соответственно, будут доступны VLAN, сконфигурированные на коммутаторе, после чего передать данные в другой VLAN не составит труда.
- Как правило, в большинстве организаций серверы работают в одном сегменте сети (VLAN) рабочие станции администраторов - в другом, обычные пользователи - в третьем. Отдельно должен размещаться сегмент DMZ, правда, для его разграничения коммутаторов, как правило, не используют.
- Таким образом, в случае если злоумышленник, находясь в пользовательском сегменте, сможет проникнуть в VLAN администраторов, то он сможет попытаться атаковать машины администраторов или же прослушать трафик на наличие незашифрованных паролей и другой конфиденциальной информации.

VLAN Hoping



Топология сети с коммутатором и фальшивым транком

Атака на STP (Spanning Tree Protocol)

- **Протокол STP (Spanning Tree Protocol) предназначен для предотвращения зацикливания пакетов в сети при наличии дублирующих маршрутов.** Работает это следующим образом. Сначала производится обнаружение коммутаторов, которые связаны между собой. Затем выбирается Root Bridge, главный, корневой коммутатор. Далее но специальному алгоритму будут заблокированы порты коммутатора, которые создают петли в получившейся топологии.
- **Для построения древовидной структуры сети без петель в сети должен быть определен корневой коммутатор (root switch), от которого и строится это дерево.**
- **В качестве корневого коммутатора выбирается коммутатор с наименьшим значением идентификатора.** Идентификатор коммутатора - это число длиной восемь байт, шесть младших байтов которого составляет MAC-адрес его блока управления, а два старших байта конфигурируются вручную. Это позволяет администратору сети влиять на процесс выбора корневого коммутатора. Если администратор не вмешается в данный процесс, корневой коммутатор будет выбран случайным образом - им станет устройство с минимальным MAC-адресом блока управления. Такой выбор может оказаться далеко не рациональным. и назначить ему вручную наименьший идентификатор.

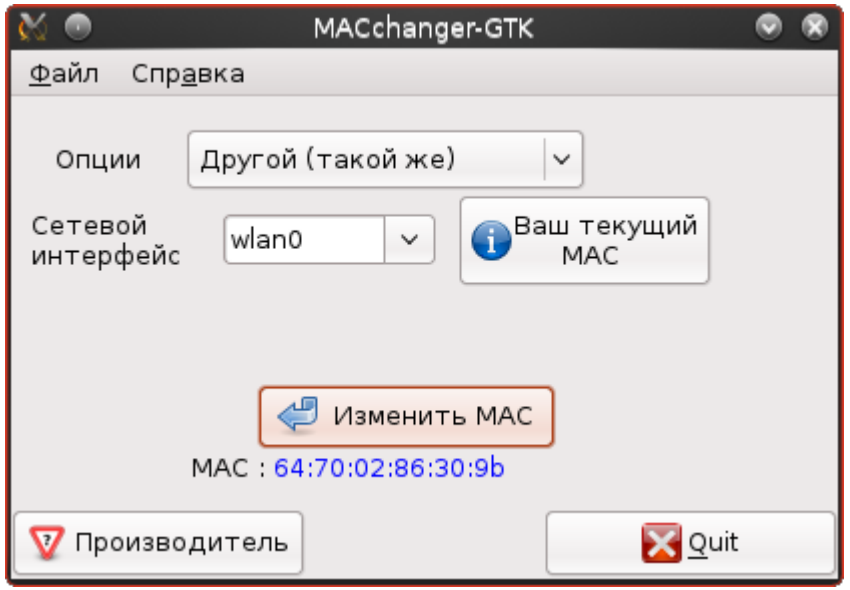
Атака на STP (Spanning Tree Protocol)

- **Что может предпринять атакующий?**
- **Он может притвориться коммутатором, направить в сторону атакуемого коммутатора BPDU-пакет, в котором может подделать приоритет, MAC-адрес, для того чтобы самому стать корневым коммутатором и с его помощью перехватить сетевой трафик.**
- Корневым коммутатором становится тот, у которого самый высокий приоритет.
- В случае если приоритет у нескольких коммутаторов одинаковый, то для выбора корневого коммутатора используется MAC-адрес, у кого он меньше, тот и становится корневым.

MAC Spoofing

- **MAC Spoofing.** Данный тип атак реализуется путем подделывания MAC-адреса, например атакующий может подделать MAC-адрес, который использовал другой хост сети. Злоумышленник может использовать эту атаку для осуществления сбора конфиденциальной информации
- Для реализации данной атаки, часто пользуются утилитой macchanger.

Утилита macchanger позволяет гибко управлять MAC-адресами сетевых интерфейсов.
Воспользовавшись macchanger можно быстро установить определенный MAC-адрес на сетевом интерфейсе, установить MAC-адрес случайным образом, установить MAC-адрес от конкретного производителя и др.



Атака на PVLAN (Private VLAN)

- С помощью этой атаки злоумышленник может получить доступ к соседнему устройству PVLAN посредством L3-устройства (маршрутизатора).
- В технологии PVLAN, в отличие от VLAN, порты могут находиться в трех режимах:
  - isolated,
  - promiscuus,
  - community.
- **Isolated** - порты не могут передавать данные в своем VLAN между клиентами. Данные могут передаваться только между портами Isolated и Promiscuous.
- Порты **promiscuous** - это порты PVLAN, в которые можно передавать данные со всех портов Isolated и Community, как и в обычном VLAN.
- **Community** - это группы портов, между членами которых можно передавать данные, можно назвать VLAN во VLAN.
- Если атакующему доступно устройство Layer 3 (например, маршрутизатор), он может установить связь между клиентами, которые находятся в одном PVLAN, между портами isolated.

Атака на PVLAN (Private VLAN)

- Для реализации данной атаки пользователь может подделать пакет, в котором он укажет в IP-адресе назначения необходимое ему устройство, находящееся на другом порту isolated, источник останется без изменения, а вот в качестве MAC-адреса назначения он укажет MAC-адрес устройства L3.
- Данное устройство, получив пакет, перенаправит его по указанному адресу. Принимающая сторона может сделать то же самое - таким образом обеспечить передачу данных между isolated-портами.
- Для таких атак может применяться утилита Private-VLAN-PVLAN-attack.

Атака на DHCP

- **Атаковать DHCP-сервер можно несколькими различными способами.**

  1. **Злоумышленник может сформировать и послать DHCP-серверу огромное количество DHCP-запросов с разными MAC-адресами.** Сервер будет выделять IP-адреса из пула, и рано или поздно весь DHCP-пул закончится, после чего сервер не сможет обслуживать новых клиентов. **По сути, это DoS-атака**, так как нарушается работоспособность сети. Метод борьбы с подобными атаками называется DHCP Snooping. Данный метод заключается в следующем. Когда коммутатор получает пакет, то он сравнивает MAC-адрес, указанный в DHCP-запросе, с MAC-адресом, который был прописан на порту коммутатора. Если адреса совпадают, то коммутатор отправляет пакет дальше, если не совпадают, то пакет отбрасывается.

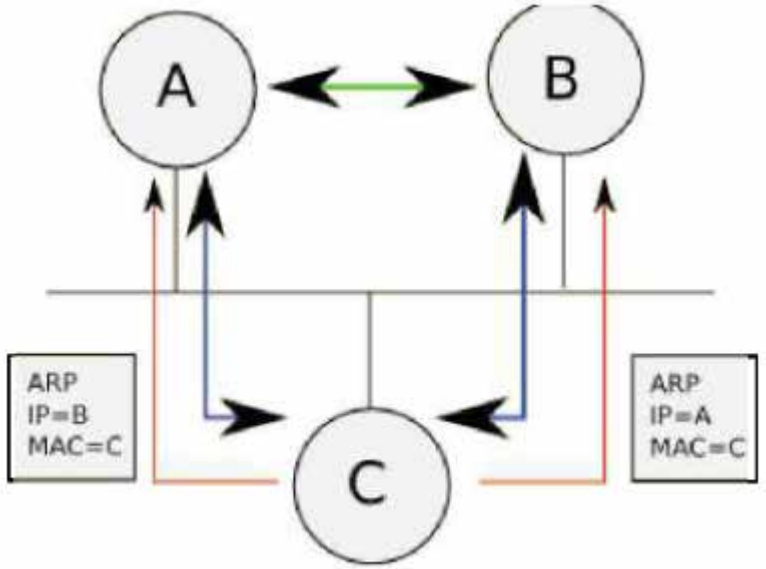
  2. **Злоумышленник может также развернуть свой DHCP-сервер и выдавать свои настройки пользователям сети** (может указать любой DNS, Gateway и г. д.) и воспользоваться уже по своему усмотрению, начиная от прослушивания трафика до подделки DNS-ответов и т. д.

ARP-spoofing

- **ARP spoofing (ARP Cache poisoning)** - это атака, используемая для прослушивания сети, построенной на коммутаторах.
  - *ARP (англ. Address Resolution Protocol - протокол определения адреса) - использующийся и компьютерных сетях протокол низкого уровня, предназначенный для определения адреса кинального уровня по известному адресу сетевого уровня.*
- **Суть этой атаки заключается в следующем**. Злоумышленник посылает ложные ARP-пакеты, для того чтобы убедить компьютер жертвы в том, что прослушивающий компьютер и есть конечный адресат. Далее пакеты с компьютера жертвы перехватываются и пересылаются реальному получателю, MAC-адрес отправителя в них подменяется, чтобы ответные пакеты тоже шли через прослушивающий Компьютер. Прослушивающий компьютер становится «шлюзом» для трафика жертвы, и злоумышленники получают возможность прослушивать трафик, осуществляя атаку «человек посередине» .

ARP-spoofing

- Стоит отмстить, что при попытке прослушать трафик нескольких активно общающихся компьютеров и, соответственно, возникающем при этом переполнении APR-таблиц возможна перегрузка, и, как следствие, падение сети. Это, помимо прочего, чревато обнаружением атаки.
- Также стоит отметить, что данная атака может быть реализована только при наличии доступа в локальную сеть.
- То есть злоумышленнику, находящемуся за пределами локальной сети, не удастся осуществить ARP-Spooling.
- Для реализации этой атаки ему придется сначала захватить контроль над одной из машин, находящейся в корпоративной локальной сети, а уже потом с этой машины осуществлять отравление ARP-кэша.



Схематический вид подмены MAC-адреса

Атаки на физическом уровне

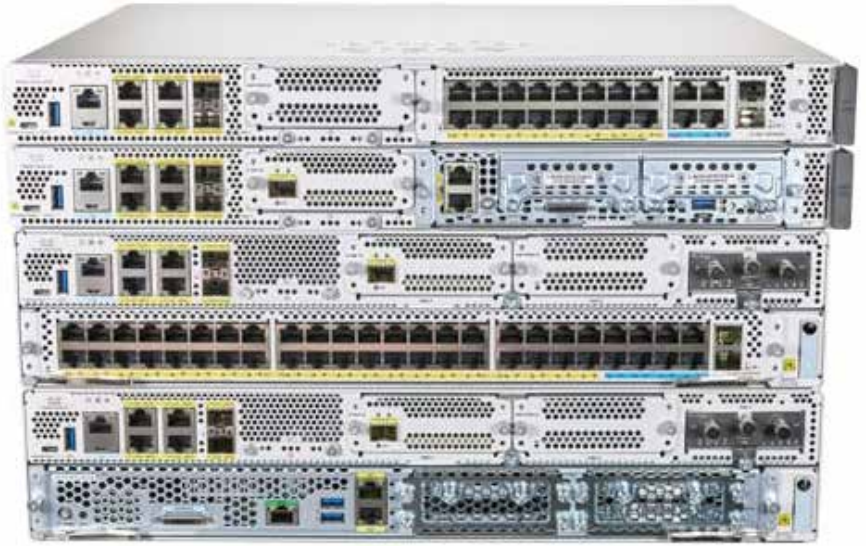
- **Что касается атак на физическом уровне, то стоит заметить, что для их успешной реализации злоумышленнику необходимо иметь (физический доступ к локальной сети.**
- То есть хакер должен предварительно удаленно взломать машину, находящуюся в локальной сети, и затем с этого компьютера пытаться реализовать описанные атаки.
- Или же злоумышленником является один из сотрудников компании, имеющий доступ к локальной сети. Об этом необходимо помнить при подготовке плана сетевой зашиты.

Сетевой уровень (третий уровень по модели OSI). Один из самых сложных уровней модели OSI, обеспечивающий маршрутизацию данных между физическими сетями и правильную адресацию сетевых узлов (например, по IP-адресу). На этом уровне происходит также разбиение потоков данных на более мелкие части, а иногда и обнаружение ошибок. Именно на этом уровне и действуют маршрутизаторы.

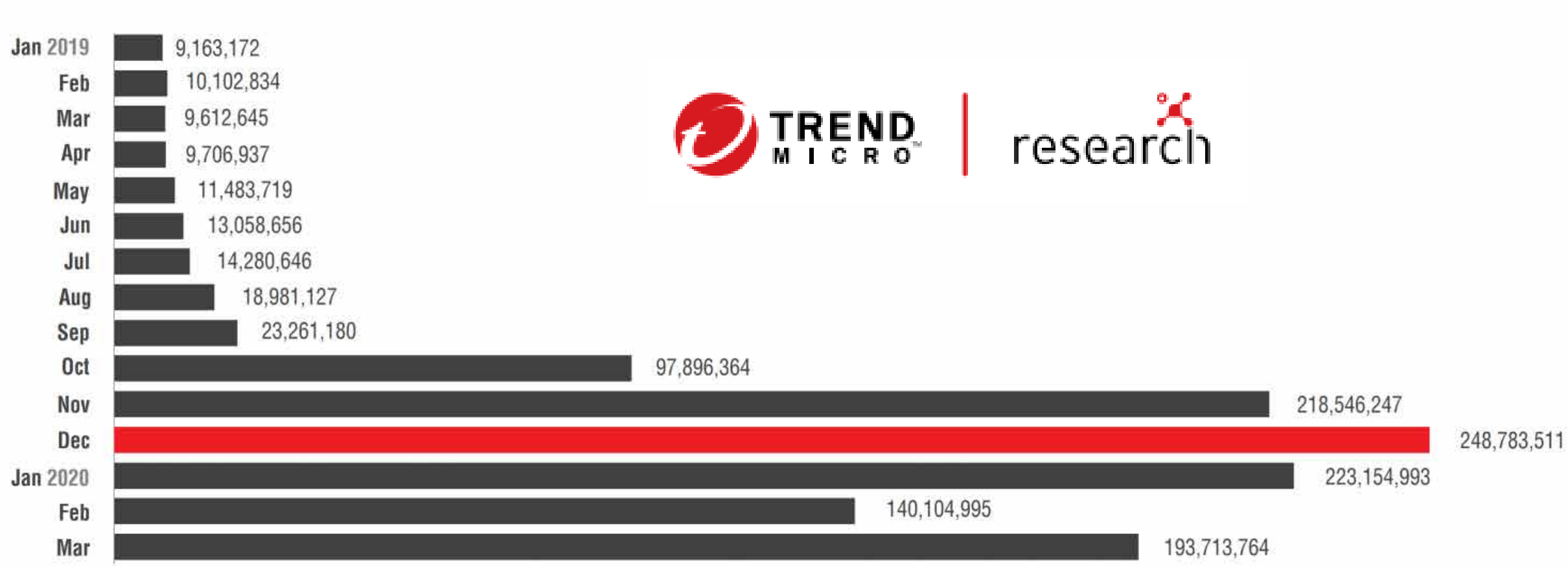
4.2. Атаки на сетевом уровне

Атаки на маршрутизаторы (роутеры)

- **Маршрутизатором** является устройство сетевого уровня эталонной модели OSI.
- **Роутер и маршрутизатор** – два названия одного устройства.
- **Маршрутизаторы** - одна из самых привлекательных точек сети для атак злоумышленников.
- **Эти широко распространенные сетевые устройства часто имеют несколько уязвимостей**, не говоря уже о последствиях, которые может иметь человеческий фактор при администрировании этих устройств.



Количество брутфорс-атак на маршрутизаторы в 2019-2020 году



Отчет TrendMicro - Worm War: The Botnet Battle for IoT Territory (2020)
https://documents.trendmicro.com/assets/white_papers/wp-worm-war-the-botnet-battle-for-iot-territory.pdf

Основная уязвимость маршрутизаторов (роутеров)

- По оценкам экспертов в 2020 году количество подключенных к интернету IoT-устройств превысит **31 млрд штук**.
- Каждое такое устройство содержит операционную систему с сетевым стеком и набор программ для выполнения основных задач.
- **Наиболее функциональные IoT-устройства — это роутеры.**
- **Обычно их прошивка представляет собой облегчённую и довольно редко обновляемую владельцами устройств версию Linux.**
- На многих устройствах **остаётся заданный производителем пароль**, что в сочетании с неисправленными уязвимостями старого Linux превращает роутеры в идеальную цель для захвата и подключения к ботнету.

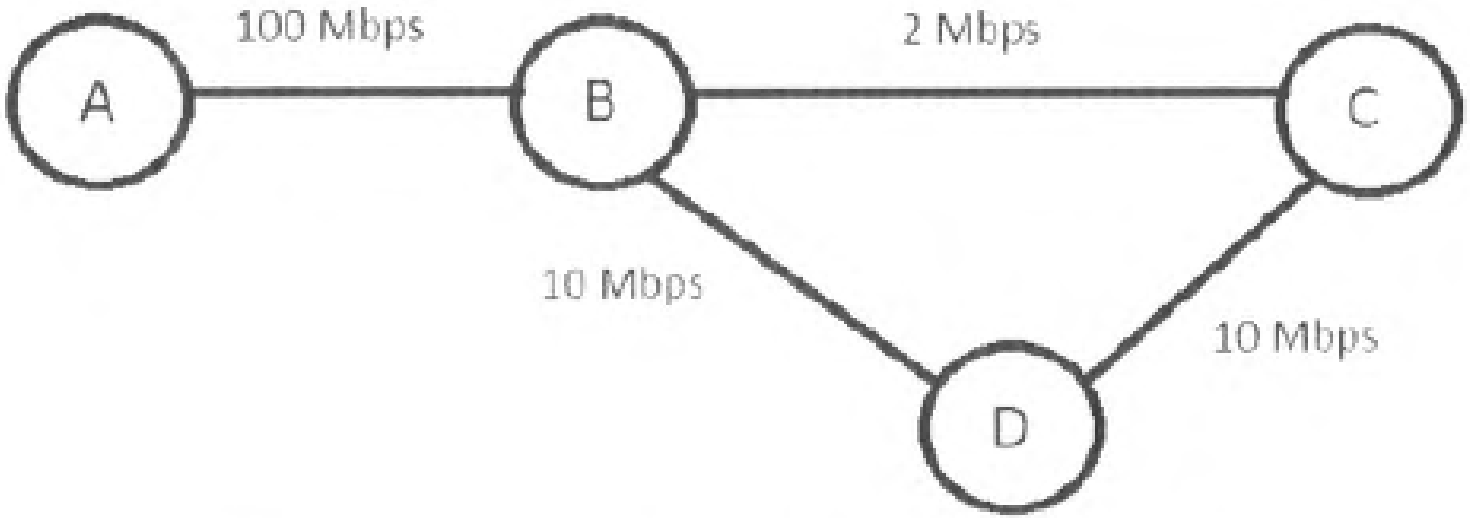
Маршрутизатор. Таблицы маршрутизации

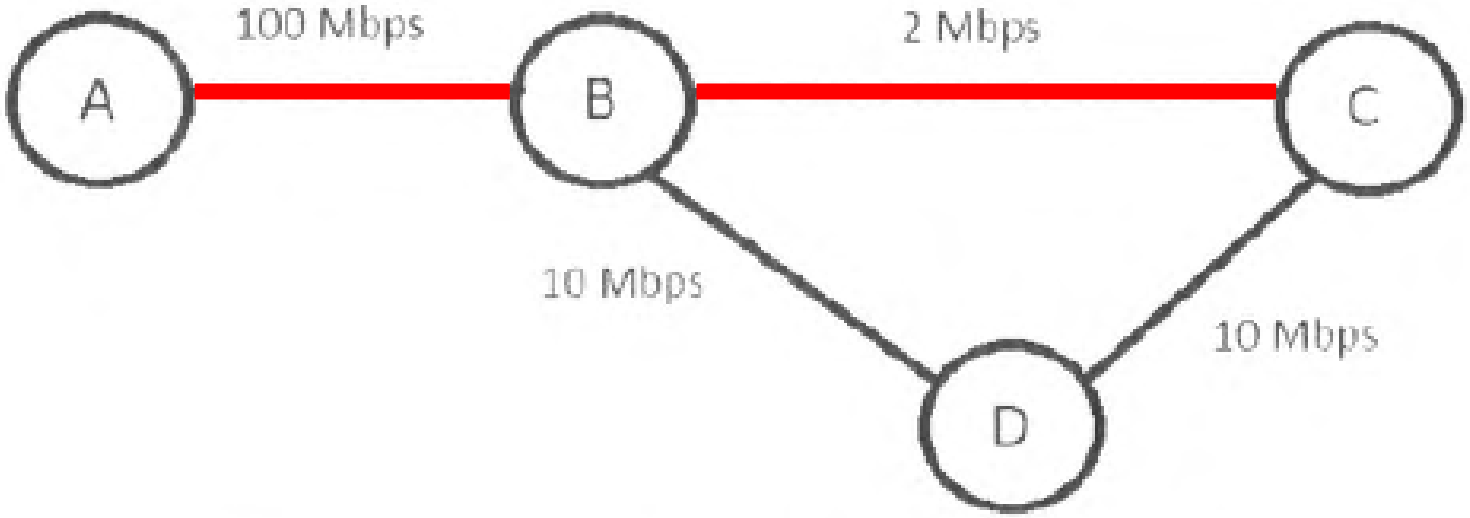
- Маршрутизатор или роутер пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации.
- **Таблица маршрутизации может составляться двумя способами:**
  - **статическая маршрутизация — когда записи в таблице вводятся и изменяются вручную**. Такой способ требует вмешательства администратора каждый раз, когда происходят изменения в топологии сети. С другой стороны, он является наиболее стабильным и требующим минимума аппаратных ресурсов маршрутизатора для обслуживания таблицы.
  - **динамическая маршрутизация** — когда записи в таблице обновляются автоматически при помощи одного или нескольких **протоколов маршрутизации — RIP, OSPF, IGRP, EIGRP, IS-IS, BGP,** и др. Кроме того, маршрутизатор строит таблицу оптимальных путей к сетям назначения на основе различных критериев — количества промежуточных узлов, пропускной способности каналов, задержки передачи данных и т. п. **Критерии вычисления оптимальных маршрутов чаще всего зависят от протокола маршрутизации, а также задаются конфигурацией маршрутизатора.** Такой способ построения таблицы позволяет автоматически держать таблицу маршрутизации в актуальном состоянии и вычислять оптимальные маршруты на основе текущей топологии сети. Однако динамическая маршрутизация оказывает дополнительную нагрузку на устройства, а высокая нестабильность сети может приводить к ситуациям, когда маршрутизаторы не успевают синхронизировать свои таблицы, что приводит к противоречивым сведениям о топологии сети в различных её частях и потере передаваемых данных.

Протокол RIP

- **Протокол динамической маршрутизации RIP (Routing Information Protocol)** является внутренним протоколом маршрутизации дистанционно-векторного типа, часто используется в небольших и средних размеров IP-сетях с множественными путями.
- Будучи одним из наиболее ранних протоколов обмена маршрутной информацией, он до сих пор чрезвычайно распространен в локальных сетях ввиду простоты реализации.
- **Протоколы динамической маршрутизации предназначены для нахождения оптимального маршрута в сетях с несколькими путями.** Критериями для признания маршрута оптимальным может быть несколько характеристик. Прежде всего по количеству переходов (хонов), которые необходимо сделать пакету для того, чтобы попасть из сети отправителя в сеть получателя.

Протокол RIP





Протокол RIP

- **Основными угрозами для протокола маршрутизации RIP являются:**
  - ложные маршруты;
  - понижение версии протокола RIP;
  - взлом хэша MD5.
- **Целями атак являются** прослушивание трафика, его модификация, перенаправление по ложным маршрутам.

Подробный разбор атаки и защиты на протокол RIP представлен в книге Бирюков А. А. Информационная безопасность: защита и нападение. - Москва: ДМК Пресс, 2017. - 434 с.
Стр.63 - 77

Протокол RIP. Атаки/Уязвимости

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾ NVD

Go to for: CVSS Scores CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 160549

NOTICE: CVE website transitioning to new "CVE.ORG" web address. Process to begin in late September 2021 and last one year. (details)

HOME > CVE > SEARCH RESULTS

Search Results

There are **32** CVE Records that match your search.

Name	Description
CVE-2020-24718	bhyve, as used in FreeBSD through 12.1 and illumos (e.g., OmniOS CE through r151034 and OpenIndiana through Hipster 2020.04), does not properly restrict VMCS and VMCB read/write operations, as demonstrated by a root user in a container on an Intel system, who can gain privileges by modifying VMCS_HOST_RIP.
CVE-2019-6961	Incorrect access control in actionHandlerUtility.php in the RDK RDKB-20181217-1 WebUI module allows a logged in user to control DDNS, QoS, RIP, and other privileged configurations (intended only for the network operator) by sending an HTTP POST to the PHP backend, because the page filtering for non-superuser (in header.php) is done only for GET requests and not for direct AJAX calls.
CVE-2019-13149	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the key passwd in Routing RIP Settings.
CVE-2018-19129	In Libav 12.3, a NULL pointer dereference (RIP points to zero) issue in ff_mpa_synth_filter_float in libavcodec/mpegaudiodsp_template.c can cause a segmentation fault (application crash) via a crafted mov file.
CVE-2017-2303	On Juniper Networks products or platforms running Junos OS 12.1X46 prior to 12.1X46-D50, 12.1X47 prior to 12.1X47-D40, 12.3 prior to 12.3R13, 12.3X48 prior to 12.3X48-D30, 13.2X51 prior to 13.2X51-D40, 13.3 prior to 13.3R10, 14.1 prior to 14.1R8, 14.1X53 prior to 14.1X53-D35, 14.1X55 prior to 14.1X55-D35, 14.2 prior to 14.2R5, 15.1 prior to 15.1F6 or 15.1R3, 15.1X49 prior to 15.1X49-D30 or 15.1X49-D40, 15.1X53 prior to 15.1X53-D35, and where RIP is enabled, certain RIP advertisements received by the router may cause the RPD daemon to crash resulting in a denial of service condition.
CVE-2016-9756	arch/x86/kvm/emulate.c in the Linux kernel before 4.8.12 does not properly initialize Code Segment (CS) in certain error cases, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.
CVE-2016-9378	Xen 4.5.x through 4.7.x on AMD systems without the NRip feature, when emulating instructions that generate software interrupts, allows local HVM guest OS users to cause a denial of service (guest crash) by leveraging an incorrect choice for software interrupt delivery.

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=RIP

Протокол OSPF

- **Протокол маршрутизации OSPF (Open Shortest Path First) это внутренний шлюзовый протокол**, используемый для распространения данных маршрутизации внутри одной автономной системы, преимущественно используется для динамических объединенных IP-сетей большого размера со множественными путями.
- Как правило, протокол маршрутизации OSPF используется при маршрутизации в корпоративных сетях, содержащих в среднем 50 локальных сетей и несколько тысяч хостов.

Протокол OSPF

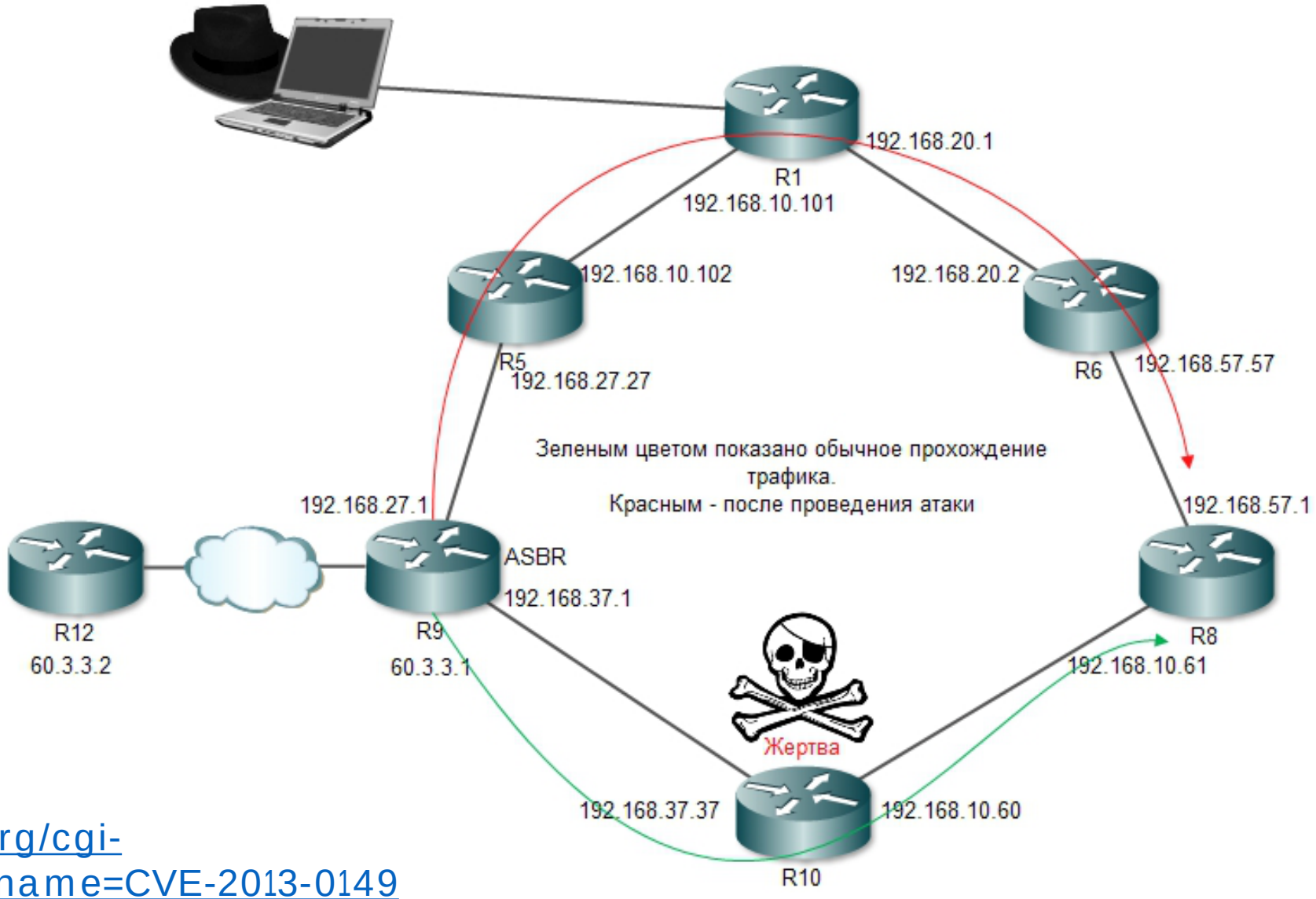
- **OSPF является протоколом состояния канала (link-state), в отличие от RIP, являющегося протоколом вектора расстояний (distance-vector). Каждый маршрутизатор обновляет свою таблицу маршрутизации на основании векторов расстояний, который он получает от своих соседей.**
- При использовании протокола состояния канала **маршрутизатор не осуществляет обмен информацией о расстояниях со своими соседями**. Вместо этого каждый маршрутизатор активно проверяет статус своих каналов, ведущих к каждому соседнему маршрутизатору, и посылает эту информацию другим своим соседям, которые могут направить поток данных в автономную систему.
- Каждый маршрутизатор принимает информацию о состоянии канала и уже на ее основании строит полную таблицу маршрутизации.

Протокол OSPF

- **Атаки на OSPF более сложны, чем на RIP.**
- Основные сложности заключаются в следующем:
  - 1) маршрутизатору злоумышленника необходимо симулировать пакет, для того чтобы обмениваться с другими роутерами маршрутной информацией;
  - 2) зависимость от иерархии маршрутизаторов, участвующих в обмене маршрутной информацией OSPE роутеры, участвующие в обмене, могут иметь различный уровень в иерархической схеме маршрутизации.

- Основными атаками на OSPF как и на RIP являются: ложные маршруты; взлом MD5.

Протокол OSPF. Пример атаки



CVE-2013-0149
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0149

Протокол OSPF. Атаки/Уязвимости

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾ NVD

Go to for: CVSS Scores CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 160549

NOTICE: CVE website transitioning to new "CVE.ORG" web address. Process to begin in late September 2021 and last one year. (details)

HOME > CVE > SEARCH RESULTS

Search Results

There are **51** CVE Records that match your search.

Name	Description
CVE-2020-5881	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, and 13.1.0-13.1.3.3, when the BIG-IP Virtual Edition (VE) is configured with VLAN groups and there are devices configured with OSPF connected to it, the Network Device Abstraction Layer (NDAL) Interfaces can lock up and in turn disrupting the communication between the mcpd and tmm processes.
CVE-2020-3528	A vulnerability in the OSPF Version 2 (OSPFv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to incomplete input validation when the affected software processes certain OSPFv2 packets with Link-Local Signaling (LLS) data. An attacker could exploit this vulnerability by sending a malformed OSPFv2 packet to an affected device. A successful exploit could allow the attacker to cause an affected device to reload, resulting in a DoS condition.
CVE-2020-3298	A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper memory protection mechanisms while processing certain OSPF packets. An attacker could exploit this vulnerability by sending a series of malformed OSPF packets in a short period of time to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device.
CVE-2020-3195	A vulnerability in the Open Shortest Path First (OSPF) implementation in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a memory leak on an affected device. The vulnerability is due to incorrect processing of certain OSPF packets. An attacker could exploit this vulnerability by sending a series of crafted OSPF packets to be processed by an affected device. A successful exploit could allow the attacker to continuously consume memory on an affected device and eventually cause it to reload, resulting in a denial of service (DoS) condition.

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=OSPF

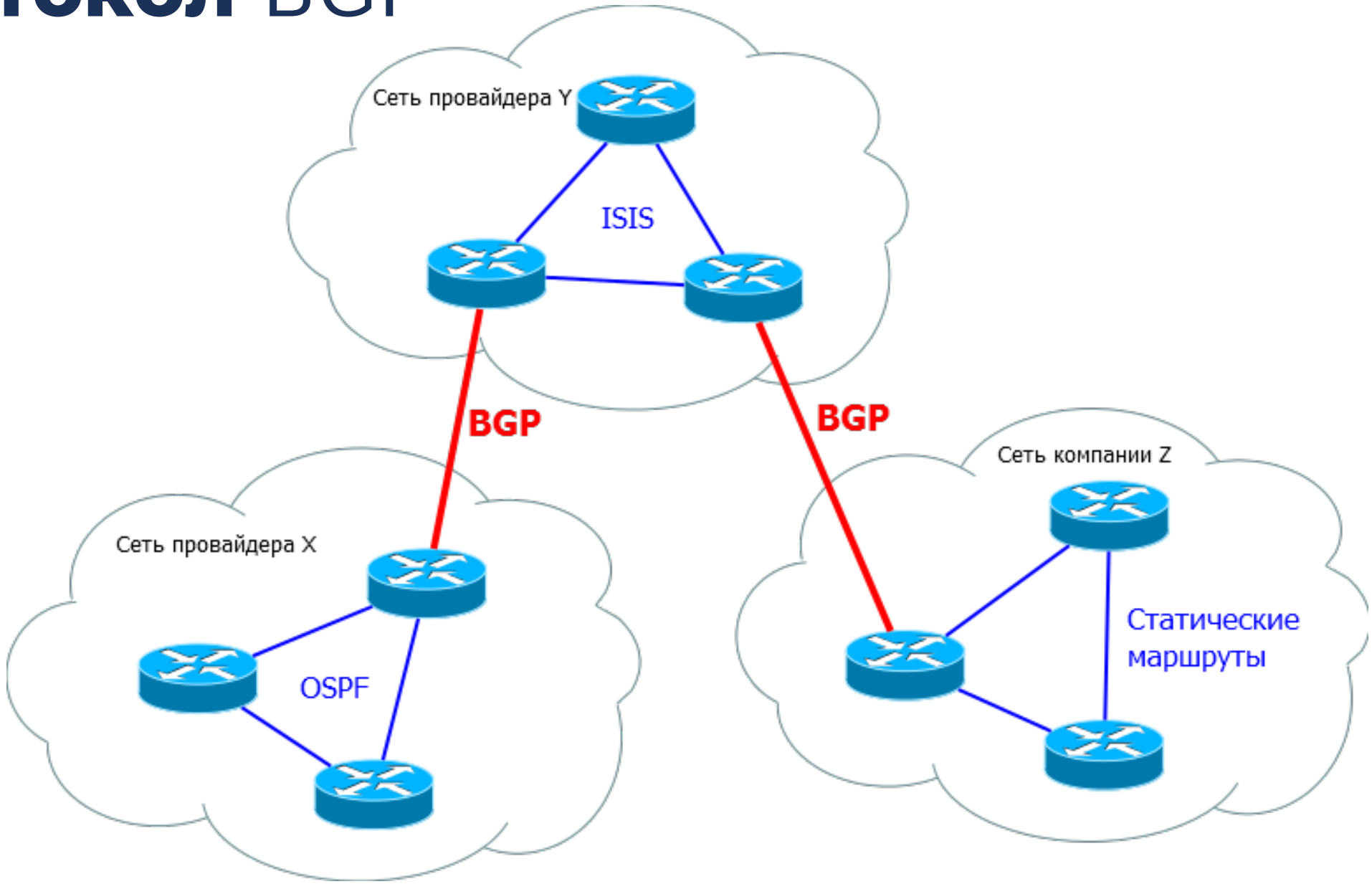
Протокол OSPF**. Полезные материалы.** URL

- Cisco Learn - Open Shortest Path First (OSPF)
  https://ciscolearning.ru/cisco-router/ospf/
- Понимание типов сетей OSPF
  https://wiki.shibaev.info/index.php?title=Понимание_типов_сетей_OSPF
- Исследуем дыры в OSPF
  https://xakep.ru/2014/09/03/ospf-vulnerabilities/
- Безопасность протокола OSPF
  https://www.elibrary.ru/download/elibrary_20464429_61862008.pdf

Протокол BGP

- Протоколы динамической маршрутизации RIP и OSPF применяются только и локальных сетях. В глобальных сетях, в силу их особенностей, используется протокол BGP.
- **BGP (Border Gateway Protocol, протокол граничного шлюза) — это протокол динамической маршрутизации.**
- Он относится к классу протоколов маршрутизации внешнего шлюза (EGP — External Gateway Protocol).
- На текущий момент является основным протоколом динамической маршрутизации в сети Интернет.
- BGP является протоколом прикладного уровня и функционирует поверх протокола транспортного уровня TCP (порт 179).
- Отличием BGP от других протоколов динамической маршрутизации является то, что он предназначен для обмена информацией о маршрутах не между отдельными маршрутизаторами, а между целыми автономными системами и поэтому, помимо информации о маршрутах в сети, переносит также информацию и маршрутах на автономные системы. BGP не использует технических метрик, а осуществляет выбор наилучшего маршрута, исходя из правил, принятых в сети.

Протокол BGP



Протокол BGP. Атаки

- BGP работает на основе протокола TCP, прослушивая порт 179. Следовательно, протокол BGP уязвим для атак на TCP, о которых говорилось ранее:
- **Атака confidentiality violations (нарушение конфиденциальности).** Как уже упоминалось ранее, маршрутные данные BGP передаются в открытом текстовом виде, что позволяет легко перехватывать информацию (это происходит потому, что конфиденциальность маршрутных данных по является общим требованием).
- **Атака replay (воспроизведение).** BGP не включает мер по предотвращению повторного использования перехваченных сообщений.
- **Атака message insertion (вставка сообщений).** BGP не включает защиты от вставки сообщений. Однако, поскольку BGP использует транспортный протокол TCP при завершенной организации соединения вставка сообщений внешним узлом потребует точного предсказания порядковых номеров (такое предсказание возможно, но весьма затруднено для хороших реализаций TCP) или перехвата сессий.

Протокол BGP. Атаки

- **Атака message deletion (удаление сообщений).** BGP не включает защиты от удаления сообщений. Опять-таки, такие атаки весьма затруднены для качественных реализаций TCP, но исключить их полностью нельзя.
- **Атака message modification (изменение сообщений).** BGP не включает защиты от изменения сообщений. Синтаксически корректная модификация без изменения размера данных TCP в общем случае будет незаметной.
- **Атака Man-in-the-middle (атаки с участием человека).** BGP не включает средств защиты от MITM-атак. BGP не использует аутентификации партнеров, и такие атаки становятся «детской игрушкой».
- **Атака denial of service (атаки на службы).** Хотя ложные маршрутные данные сами по себе могут служить DoS-атакой на конечную систему, пытающуюся передавать данные через сеть, и сеть в целом, некоторые виды ложной информации могут создавать DoS-атаки на сам протокол BGP.

Нарушение в протоколе BGP в результате атак

- **нарушение starvation (потеря пакетов)** - трафик, адресованный узлу, пересылается в ту часть сети, которая не может обеспечить его доставку, в результате чего происходит потеря трафика;
- **нарушение network congestion (перегрузка сети)** через какую-либо часть сети будет пересылаться больше данных, нежели эта сеть способна обработать. Это разновидность атаки на отказ в обслуживании;
- **нарушение blackhole (черная дыра)** - большое количество трафика направляется для пересылки через один маршрутизатор, который не способен справиться с возросшим уровнем трафика и будет отбрасывать часть, большинство или все пакеты;
- **нарушение delay (задержка)** - данные, адресованные узлу, пересылаются но более длинному пути, чем обычно. Это нарушение может привести как к задержкам при передаче данных, что особенно заметно при передаче потокового видео- или аудио-контента, так и к потере части трафика, так как у некоторых пакетов может истечь значение Time To Live, время жизни, из-за слишком длинного пути;

Нарушение в протоколе BGP в результате атак

- **нарушение looping (петли)** данные передаются по замкнутому пути и никогда не будут доставлены;
- **нарушение eavesdrop (перехват)** - данные пересылаются через какой-либо маршрутизатор или сеть, которые не должны видеть этих данных, информация при такой пересылке может просматриваться. Как правило, при таких нарушениях злоумышленники специально направляют трафик через сегмент сети, который они могут прослушивать. Обычно подобным способом добывается конфиденциальная информация о кредитных картах, паролях, кодах доступа и т. д.;
- **нарушение partition (разделение сети)** некоторые части кажутся отделенными от сети, хотя на самом деле это не так. В результате данного нарушения через части может не проходить трафик, что отрицательно скажется на работе сети в целом;
- **нарушение cut (отключение)** - некоторые части сети могут казаться отрезанными от сети, хотя реально они подключены. Но аналогии с предыдущим нарушением, через некоторые части может не проходить график;

Нарушение в протоколе BGP в результате атак

- **нарушение churn (волны)** - скорость пересылки в сеть изменяется быстрыми темпами, что приводит к значительным вариациям картины доставки пакетов (и может неблагоприятно влиять на работу системы контроля насыщения);
- **нарушение instability (нестабильность)** работа BGP становится нестабильной, и не удастся достичь схождения картины маршрутов;
- **нарушение overload (перегрузка)** - сообщения BGP сами по себе становятся значительной частью передаваемого через сеть трафика;
- **нарушение resource exhaustion (истощение ресурсов)** сообщения BGP сами но себе отнимают слишком много ресурсов маршрутизатора (например, пространства таблиц);
- **нарушение address-spoofing (обманные адреса)** - данные пересылаются через некий маршрутизатор или сеть, которые являются подставными и могут служить для перехвата или искажения информации. Данное нарушение аналогично нарушению перехват.

Протокол BGP. Атаки/Уязвимости

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾ NVD

Go to for:
CVSS Scores
CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 160549

NOTICE: CVE website transitioning to new "CVE.ORG" web address. Process to begin in late September 2021 and last one year. (details)

HOME > CVE > SEARCH RESULTS

Search Results

There are **141** CVE Records that match your search.

Name	Description
CVE-2021-3761	Any CA issuer in the RPKI can trick OctoRPKI prior to 1.3.0 into emitting an invalid VRP "MaxLength" value, causing RTR sessions to terminate. An attacker can use this to disable RPKI Origin Validation in a victim network (for example AS 13335 - Cloudflare) prior to launching a BGP hijack which during normal operations would be rejected as "RPKI invalid". Additionally, in certain deployments RTR session flapping in and of itself also could cause BGP routing churn, causing availability issues.
CVE-2021-26928	** DISPUTED ** BIRD through 2.0.7 does not provide functionality for password authentication of BGP peers. Because of this, products that use BIRD (which may, for example, include Tigera products in some configurations, as well as products of other vendors) may have been susceptible to route redirection for Denial of Service and/or Information Disclosure. NOTE: a researcher has asserted that the behavior is within Tigera’s area of responsibility; however, Tigera disagrees.
CVE-2021-1230	A vulnerability with the Border Gateway Protocol (BGP) for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an unauthenticated, remote attacker to cause a routing process to crash, which could lead to a denial of service (DoS) condition. This vulnerability is due to an issue with the installation of routes upon receipt of a BGP update. An attacker could exploit this vulnerability by sending a crafted BGP update to an affected device. A successful exploit could allow the attacker to cause the routing process to crash, which could cause the device to reload. This vulnerability applies to both Internal BGP (IBGP) and External BGP (EBGP). Note: The Cisco implementation of BGP accepts incoming BGP traffic from explicitly configured peers only. To exploit this vulnerability, an attacker would need to send a specific BGP update message over an established TCP connection that appears to come from a trusted BGP peer.
CVE-2021-0282	On Juniper Networks Junos OS devices with Multipath or add-path feature enabled, processing a specific BGP UPDATE can lead to a routing process daemon (RPD) crash and restart, causing a Denial of Service (DoS). Continued receipt and processing of this UPDATE message will create a sustained Denial of Service (DoS) condition. This BGP UPDATE message can propagate to other BGP peers with vulnerable Junos

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=BGP

Протокол BGP. Известные атаки

- Сегодня ИБ-специалисты фиксируют тысячи инцидентов, связанных с BGP. Большинство из них незначительные, однако есть и довольно крупные:
  - 2014 год — кража криптовалюты
  - 2017 год — отключение интернета в Японии
  - 2019 год — европейский трафик ушел в Китай
  - 2019 год — сбой в работе интернета по всему миру

Подробнее: Какие инциденты с Border Gateway Protocol можно выделить за последние несколько лет https://habr.com/ru/company/cloud_mts/blog/459400/

Протокол BGP. Полезные материалы. URL

- Border Gateway Protocol
  https://ru.wikipedia.org/wiki/Border_Gateway_Protocol
- BGP протокол (перевод на русский)
  https://www.opennet.ru/docs/RUS/bgp_rus/
- Принципы работы протокола BGP
  https://habr.com/ru/post/450814/
- Сети для самых маленьких. Часть восьмая. BGP и IP SLA
  https://linkmeup.ru/blog/1198/
- RFC 4272 — Анализ уязвимостей протокола BGP
  https://muff.kiev.ua/files/books/RFC_4272_Analysis_BGP.pdf

Протокол IS-IS

- **IS-IS — это протокол внутренней маршрутизации для использования во внутренних сетях.** Этим он отличается от протоколов внешней маршрутизации, в первую очередь от Border Gateway Protocol (BGP), который используется для маршрутизации между автономными системами.
- **IS-IS** - протокол, основанный на состояниях линков, он оперирует информацией о состоянии линков других маршрутизаторов. Каждый маршрутизатор IS-IS формирует собственную базу топологии сети, собирая полученную информацию.
- Как IS-IS, так и **OSPF** - протоколы, основанные на состояниях (link-state). Оба поддерживают переменную длину маски, могут использовать групповое вещание для обнаружения соседних маршрутизаторов посредством hello-пакетов и могут работать с аутентификацией обмена маршрутами.

Протокол IS-IS

- **Протокол маршрутизации промежуточных систем (IS-IS) — это протокол внутренних шлюзов (IGP), стандартизированный ISO и использующийся в основном в крупных сетях провайдеров услуг.**
- IS-IS может также использоваться в корпоративных сетях особо крупного масштаба.
- IS-IS — это протокол маршрутизации на основе состояния каналов. Он обеспечивает быструю сходимость и отличную масштабируемость. Как и все протоколы на основе состояния каналов, IS-IS очень экономно использует пропускную способность сетей.

Протокол IS-IS**. Атаки**

- Основные атаки на протокол IS-IS:
  - Ложные маршруты
  - «Затопление» Hello-пакетами

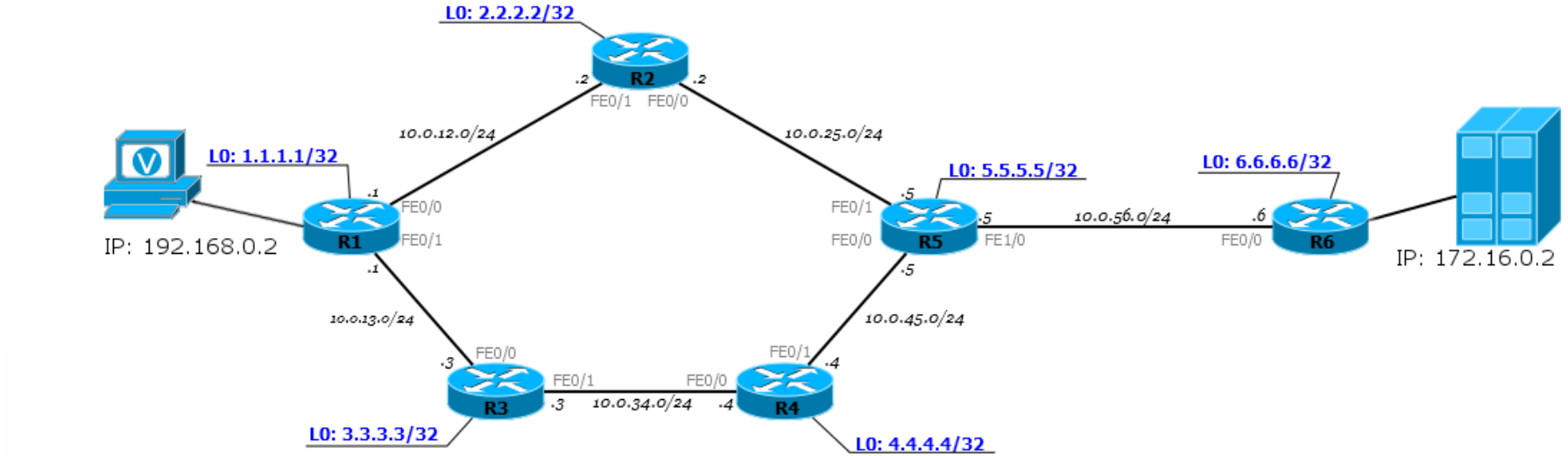
Протокол IS-IS**. Полезные материалы.** URL

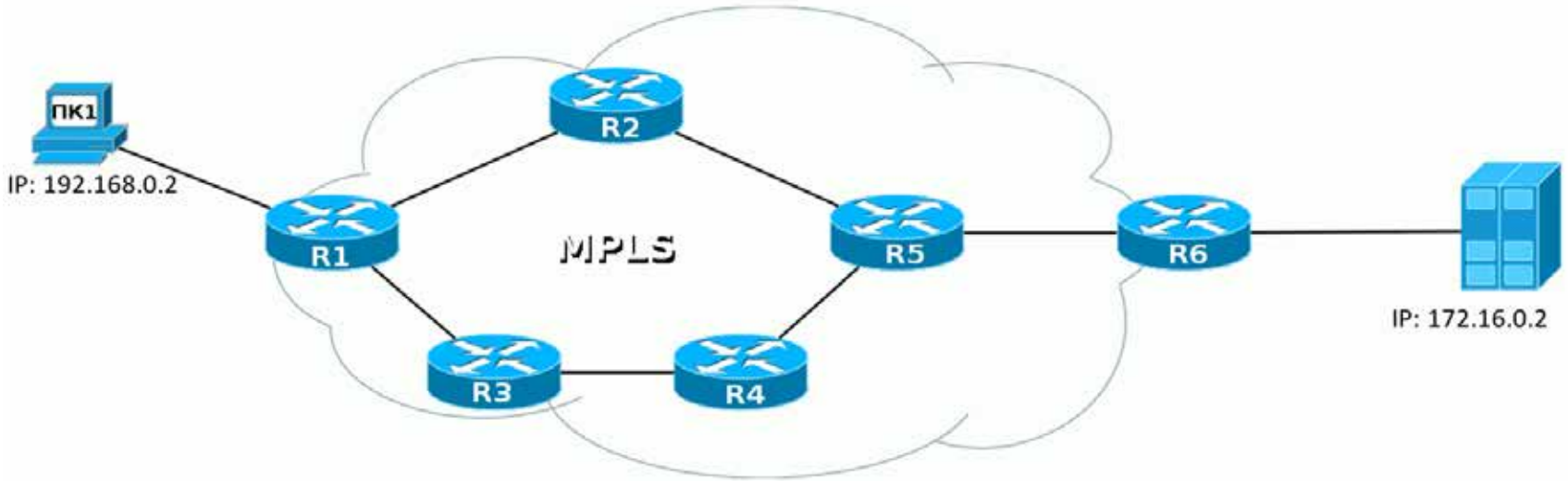
- IS-IS https://ru.wikipedia.org/wiki/IS-IS
- IS-IS для тех, кто понимает OSPF (Часть 1) https://community.cisco.com/t5/маршрутизация-и-коммутация-блоги/is-is-для-тех-кто-понимает-ospf-часть-1/ba-p/3103119
- IS-IS для тех, кто понимает OSPF (Часть 2) https://community.cisco.com/t5/маршрутизация-и-коммутация-блоги/is-is-для-тех-кто-понимает-ospf-часть-2/ba-p/3103435
- IS-IS для тех, кто понимает OSPF (Часть 3) https://community.cisco.com/t5/маршрутизация-и-коммутация-блоги/is-is-для-тех-кто-понимает-ospf-часть-3/ba-p/3104734

Протокол MPLS

- Представленные ранее протоколы сетевого уровня можно назвать «классическими», с точки зрения функционирования на сетевом уровне иерархической модели OSI.
- **Протокол MPLS** (мультипротокольная коммутация по меткам) взаимодействует сразу на двух уровнях модели: метка добавляется между заголовком кадра (второй уровень OSI) и заголовком пакета (третий уровень модели OSI).
- **MPLS (Multiprotocol Label Switching) — это технология быстрой коммутации пакетов в многопротокольных сетях, основанная на использовании меток.** MPLS разрабатывается и позиционируется как способ построения высокоскоростных IP-магистралей, однако область ее применения не ограничивается протоколом IP, а распространяется на график любого маршрутизируемого сетевого протокола.

Протокол MPLS





Протокол MPLS

- Безопасность в сетях MPLS и MPLS-VPN поддерживается с помощью сочетания протокола BGP и системы разрешения IP-адресов.
- Безопасность VPN обеспечивается на границе инфраструктуры, где пакеты, полученные от пользователя, отправляются в нужную VPN-сеть. В магистрали данные отдельных VPN-сетей перемешаются отдельно. Это достигается путем добавления стека MPLS меток перед IP-заголовком пакета.
- Механизм виртуального маршрутизатора полностью изолирует таблицы маршрутизации MPLS VPN от глобальных таблиц маршрутизации, что обеспечивает необходимые уровни надежности и масштабируемости решений MPLS VPN.

Протокол MPLS

- **Технология MPLS и MPLS VPN не обеспечивает безопасности за счет аутентификации или шифрования.** То есть информация перелается через сеть MPLS с использованием виртуальных каналов в открытом виде. В то же время **трафик пользователей, входящих в разные домены, изолирован друг от друга путем добавления уникальных меток**. Таким образом попытки перехвата пакета или потока Трафика не могут привести к прорыву нарушителя в VPN. **В сети MPLS VPN пакет данных, поступающих в магистраль, ассоциируется с конкретной сетью VPN на основании того, но какому интерфейсу пакет поступил на PE-маршрутизатор**. Затем происходит сверка IP-адреса с таблицей передачи конкретной VPN. Назначенные в таблице маршруты относятся только к VPN входящего пакета. Следовательно, входящий интерфейс определяет набор возможных исходящих интерфейсов. Эта функция также предотвращает как попадание несанкционированных данных в сеть VPN, так и передачу несанкционированных данных из неё.

Протокол MPLS. Атаки/Уязвимости

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾ NVD

Go to for:
CVSS Scores
CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 160550

NOTICE: CVE website transitioning to new "CVE.ORG" web address. Process to begin in late September 2021 and last one year. (details)

HOME > CVE > SEARCH RESULTS

Search Results

There are **59** CVE Records that match your search

Name	Description
CVE-2021-1614	A vulnerability in the Multiprotocol Label Switching (MPLS) packet handling function of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to gain access to information stored in MPLS buffer memory. This vulnerability is due to insufficient handling of malformed MPLS packets that are processed by a device that is running Cisco SD-WAN Software. An attacker could exploit this vulnerability by sending a crafted MPLS packet to an affected device that is running Cisco SD-WAN Software or Cisco SD-WAN vManage Software. A successful exploit could allow the attacker to gain unauthorized access to sensitive information.
CVE-2021-1588	A vulnerability in the MPLS Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper input validation when an affected device is processing an MPLS echo-request or echo-reply packet. An attacker could exploit this vulnerability by sending malicious MPLS echo-request or echo-reply packets to an interface that is enabled for MPLS forwarding on the affected device. A successful exploit could allow the attacker to cause the MPLS OAM process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition.
CVE-2021-0288	A vulnerability in the processing of specific MPLS packets in Juniper Networks Junos OS on MX Series and EX9200 Series devices with Trio-based MPCs (Modular Port Concentrators) may cause FPC to crash and lead to a Denial of Service (DoS) condition. Continued receipt of this packet will sustain the Denial of Service (DoS) condition. This issue only affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). This issue affects Juniper Networks Junos OS on MX Series, EX9200 Series: 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2;

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=MPLS

Протокол MPLS**. Полезные материалы.** URL

1. Сети для самых маленьких. Часть десятая. Базовый MPLS https://habr.com/ru/post/246425/?mobile=no
2. Технологии MPLS https://ppt-online.org/44154
3. Гольдштейн, А. Б. Транспортные сети IP/MPLS. Технология и протоколы : учебное пособие / А. Б. Гольдштейн, А. В. Никитин, А. А. Шкрыль : СПбГУТ. – СПб., 2016. – 80 с. http://rt-itt.sut.ru/sites/default/files/docs/metod-bk/31a_goldshteyn_nikitin_shkryl_mpls.pdf
4. Ответы на вопросы по MPLS для начинающих https://www.cisco.com/c/ru_ru/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.pdf

IPSec

- **IPSec (сокращение от IP Security)** это набор протоколов, предназначенных для шифрования, аутентификации и обеспечения зашиты при транспортировке IP-пакетов.
- IPSec - определенный IETF стандарт достоверной/ конфиденциальной передачи данных по сетям IP. Чаще всего IPSec используется для создания VPN (Virtual Private Network).
- IPSec является неотъемлемой частью IPv6 - Интернет-протокола следующего поколения, и расширением существующие версии Интернет-протокола IPv4.
- IPSec часто используется для создания защищенных туннелей между центрами обработки данных.

Протокол IPSec. Атаки/Уязвимости

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾ NVD

Go to for:
CVSS Scores
CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 160550

NOTICE: CVE website transitioning to new "CVE.ORG" web address. Process to begin in late September 2021 and last one year. (details)

HOME > CVE > SEARCH RESULTS

Search Results

There are **165** CVE Records that match your search.

Name	Description
CVE-2021-1422	A vulnerability in the software cryptography module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker or an unauthenticated attacker in a man-in-the-middle position to cause an unexpected reload of the device that results in a denial of service (DoS) condition. The vulnerability is due to a logic error in how the software cryptography module handles specific types of decryption errors. An attacker could exploit this vulnerability by sending malicious packets over an established IPsec connection. A successful exploit could cause the device to crash, forcing it to reload. Important: Successful exploitation of this vulnerability would not cause a compromise of any encrypted data. Note: This vulnerability affects only Cisco ASA Software Release 9.16.1 and Cisco FTD Software Release 7.0.0.
CVE-2020-5938	On BIG-IP 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, when negotiating IPSec tunnels with configured, authenticated peers, the peer may negotiate a different key length than the BIG-IP configuration would otherwise allow.
CVE-2020-3220	A vulnerability in the hardware crypto driver of Cisco IOS XE Software for Cisco 4300 Series Integrated Services Routers and Cisco Catalyst 9800-L Wireless Controllers could allow an unauthenticated, remote attacker to disconnect legitimate IPsec VPN sessions to an affected device. The vulnerability is due to insufficient verification of authenticity of received Encapsulating Security Payload (ESP) packets. An attacker could exploit this vulnerability by tampering with ESP cleartext values as a man-in-the-middle.
CVE-2020-3190	A vulnerability in the IPsec packet processor of Cisco IOS XR Software could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition for IPsec sessions to an affected device. The vulnerability is due to improper handling of packets by the IPsec packet processor. An attacker could exploit this vulnerability by sending malicious ICMP error messages to an affected device that get punted to the IPsec packet processor. A successful exploit could allow the attacker to deplete IPsec memory, resulting in all future IPsec packets to an affected device being dropped by the device. Manual intervention is required to recover from this situation.

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=IPSec

Протокол IPsec**. Полезные материалы.** URL

1. Анатомия **IPsec**. Проверяем на прочность легендарный протокол https://habr.com/ru/company/xakep/blog/256659/
2. Безопасность **IPSec** https://spy-soft.net/ipsec-security/
3. Методическое пособие. **IPSec**. http://dfe.petrsu.ru/koi/posob/security/
4. Лекция - Защита на сетевом уровне – протокол **IPSec**. http://yztm.ru/lekc2/l20/

Scapy – **универсальное средство для сетевых атак**

- **Scapy** – интерактивная оболочка и программная библиотека для манипулирования сетевыми пакетами на языке программирования Python
- https://scapy.net – Официальный сайт Scapy
- https://scapy.net/download/ - Скачать Scapy
- https://scapy.readthedocs.io/en/latest/ - Документация Scapy

- **Scapy** использует библиотеку libpcap и может использоваться как сниффер, для перехвата и анализа сетевого трафика, так и как конструктор пакетов. Помимо использование стандартных протоколов, в Scapy есть возможность создавать собственные и использовать их при анализе и генерации пакетов.
- **Отличительной особенностью Scapy является** возможность в несколько строчек кода подстраиваться под различные задачи, и по заверению автора она может заменить такие утилиты как hping, nmap, arpspoof, arp-sk, arping, tcpdump, tethereal, p0f.

Сниффинг пакетов

Снифферы пакетов

- **Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту**, работающую в режиме promiscuous mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки).
- При этом **сниффер перехватывает все сетевые пакеты**, которые передаются через определенный домен.
- В настоящее время **снифферы** работают в сетях на вполне законном основании. Они **используются для диагностики неисправностей и анализа трафика**. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Снифферы пакетов

- Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям.
- Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам.
- Хакеры слишком хорошо знают и используют наши человеческие слабости (методы атак часто базируются на методах социальной инженерии).
- Они прекрасно знают, что пользователи пользуются одним и тем же паролем для доступа к множеству ресурсов, и поэтому им часто удается, узнав наш пароль, получить доступ к важной информации. В самом худшем случае хакер получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает нового пользователя, которого можно в любой момент использовать для доступа в сеть и к ее ресурсам.

Снифферы пакетов

- Смягчить угрозу сниффинга пакетов можно с помощью следующих средств:
  - Аутентификация
  - Коммутируемая инфраструктура
  - Анти-снифферы
  - Криптография

Сниффферы пакетов

- SolarWinds
- tcpdump
- Windump
- Wireshark
- tshark
- Network Miner
- Fiddler (HTTP)
- Capsa

IP-спуфинг

- **IP-спуфинг происходит, когда хакер, находящийся внутри корпорации или вне ее выдает себя за санкционированного пользователя.**
- Это можно сделать следующим образом, хакер может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам.
- Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример - атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.
- Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами.
- Для двусторонней связи хакер должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые хакеры, однако, даже не пытаются получить ответ от приложений. Если главная задача состоит в получении от системы важного файла, ответы приложений не имеют значения.
- Если же хакеру удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, хакер получит все пакеты и сможет отвечать на них так, будто он является санкционированным пользователем.

IP-**спуфинг**

- Угрозу спуфинга можно ослабить (но не устранить) с помощью следующих мер:
  - Контроль доступа
  - Фильтрация RFC 2827

Транспортный уровень (четвертый по модели OSI). Основное назначение транспортного уровня — предоставить надежные транспортные услуги нижележащим уровням. Благодаря управлению потоком данных, их сегментации и десегментации, исправлению ошибок на транспортном уровне обеспечивается безошибочная доставка данных из одной точки сети в другую. Обеспечить надежную доставку данных крайне сложно, поэтому в модели OSI для этой цели выделен отдельный уровень. На транспортном уровне используются протоколы как с установлением соединения, так и без него. Именно на этом уровне и действуют определенные брандмауэры и промежуточные, так называемые прокси-серверы.

4.3. Атаки на транспортном уровне

Атаки на протокол TCP и UDP

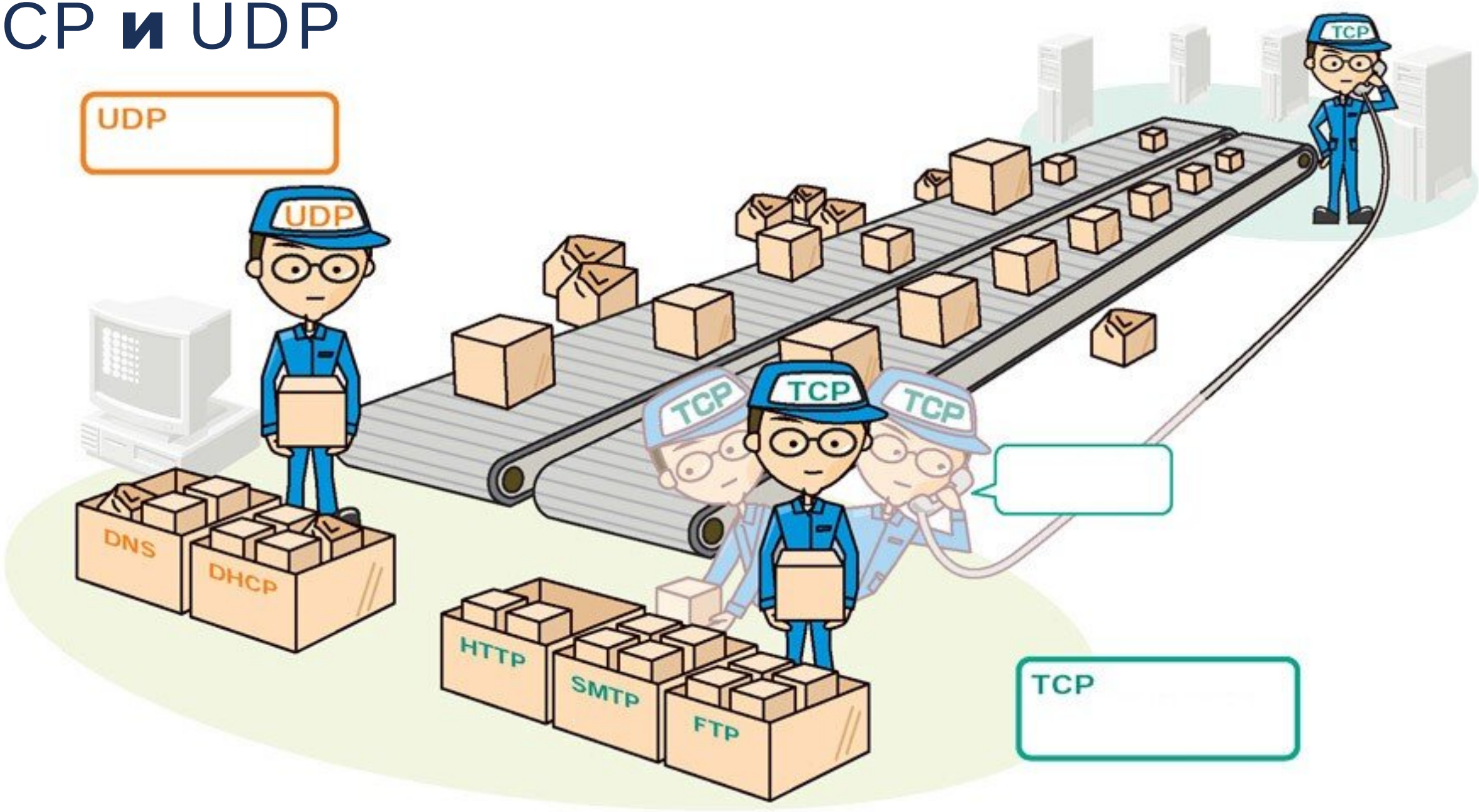
TCP и UDP

- **На транспортном уровне используются два основных протокола - это TCP и UDP:**

  - **TCP протокол - Transmission Control Protocol** (протокол управления передачей) — один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета. Механизм TCP предоставляет поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета, **гарантируя тем самым (в отличие от UDP) целостность передаваемых данных** и уведомление отправителя о результатах передачи.

  - **UDP протокол - User Datagram Protocol (протокол пользовательских датаграмм)** — один из ключевых элементов набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных. Природа UDP как протокола без сохранения состояния также полезна для серверов, отвечающих на небольшие запросы от огромного числа клиентов, например DNS и потоковые мультимедийные приложения вроде IPTV, Voice over IP, протоколы туннелирования IP и многие онлайн-игры.

TCP и UDP



Уязвимости протокола TCP (Transmission Control Protocol)

- **Синхронизация и подтверждение (SYN Flood):** TCP использует рукопожатие для установления соединения, которое уязвимо к перегрузке запросами на установление соединения, что может привести к отказу в обслуживании (DoS).
- **Предсказание последовательности номеров (Sequence Number Prediction):** Если злоумышленник может предсказать номера последовательности TCP пакетов, он может вставить свои пакеты в поток данных, что может привести к потере данных или компрометации сессии.
- **Сброс соединений (TCP RST Attacks):** Отправка поддельных TCP RST пакетов может привести к преждевременному разрыву установленных TCP-соединений.
- **Инъекция данных (TCP Injection):** Если злоумышленник может перехватить TCP-сессию, он может вставлять вредоносные данные в поток общения.
- **Захват сессии (TCP Session Hijacking):** Это когда злоумышленник берет контроль над существующей TCP-сессией без ведома одной или обеих сторон.
- **Man-in-the-Middle (MitM) атаки:** Поскольку TCP не имеет встроенной шифрования, данные, передаваемые через TCP, уязвимы к перехвату и модификации третьими лицами.
- **IP Spoofing:** Злоумышленник может отправить пакеты с фальшивым источниковым IP-адресом, что может использоваться для обмана системы получателя или проведения отказа в обслуживании (DoS).
- **Проблема нулевого окна (TCP Zero Window):** Злоумышленник может заставить хост установить размер окна приема на ноль, что приведет к блокировке потока данных.
- **Фрагментация пакетов (Fragmentation Attacks):** TCP пакеты могут быть фрагментированы и, следовательно, подвержены атакам, которые используют эту особенность для обхода сетевых защит.
- **Уязвимости в реализации:** Некоторые уязвимости проистекают из конкретных реализаций TCP в операционных системах, включая ошибки в обработке пакетов и недостатки в алгоритмах управления перегрузками.
- **Time-Wait Assassination:** Это техника, при которой злоумышленник может принудительно закрыть соединение, отправив поддельный запрос на завершение соединения, что может вызвать проблемы сетевого уровня.

Проблемы протокола TCP

- **Максимальный размер сегмента.** TCP требует явного указания максимального размера сегмента (MSS) в случае, если виртуальное соединение осуществляется через сегмент сети, где максимальный размер блока (MTU) менее, чем стандартный MTU Ethernet (1500 байт).
  - В протоколах туннелирования, таких как GRE, IPIP, а также PPPoE MTU туннель меньше, чем стандартный, поэтому сегмент TCP максимального размера имеет длину пакета больше, чем MTU. Это приводит к фрагментации и уменьшению скорости передачи полезных данных. Если на каком-либо узле фрагментация запрещена, то со стороны пользователя это выглядит как «зависание» соединений. При этом «зависание» может происходить в произвольные моменты времени, а именно тогда, когда отправитель использовал сегменты длиннее допустимого размера. Для решения этой проблемы на маршрутизаторах применяются правила Firewall-а, добавляющие параметр MSS во все пакеты, инициирующие соединения, чтобы отправитель использовал сегменты допустимого размера.
  - MSS может также управляться параметрами операционной системы.
- **Обнаружение ошибок при передаче данных.** Хотя протокол осуществляет проверку контрольной суммы по каждому сегменту, используемый алгоритм считается слабым.

Атаки на протокол TCP

- **Слабость TCP в том, что реализация протокола предполагает «честное» поведение всех участников сети.** В результате злоумышленник может получить доступ к передаваемым данным, выдать себя за другую сторону, привести систему в нерабочее состояние.

Атаки на протокол TCP

1. **Passive scan** – пассивное сканирование сети
2. **TCP Reset** – атакующий отправляет поддельные пакеты TCP RESET, чтобы прервать установленное соединение.
3. **Принуждение к ускорению/замедлению передачи**
4. **IP-spoofing** – атакующий подменяет IP-адрес, пытаясь воспользоваться доверием между двумя системами.
5. **IP-spoofing** (подделка IP-адреса) **+ TCP sequence prediction** (предсказание последовательности TCP)
6. **TCP Hijacking** – **перехват TCP-сессии**
7. **SYN Flood** – атакующий отправляет большое количество SYN-запросов, чтобы исчерпать ресурсы сервера и вызвать отказ в обслуживании.
8. **TCP Full Connection Flooding** – разновидность SYN Flood с удерживанием большого числа соединений на атакуемом узле , является видом DoS-атаки (отказ в обслуживании), при которой атакующий пытается исчерпать доступные системные ресурсы на целевом сервере, чтобы тот не смог обработать законные запросы.
9. **Sniffing** (Перехват) – атака заключается в перехвате и анализе сетевого трафика.
10. **Tiny Fragment Attack** – атака крошечными фрагментами
11. **Overlapping Fragment Attack** - атака накладывающимися фрагментами
12. **Teardrop Attack** – атака фрагментированными пакетами
13. **TCP Zero Window Attack** – десинхронизация нулевыми данными

- Важно отметить, что все приведенные атаки хорошо известны, и в большинстве моделей сетевого оборудования существуют механизмы для эффективной зашиты. Однако эти механизмы далеко не всегда используются но своему назначению.

Атака: Сканирование сети

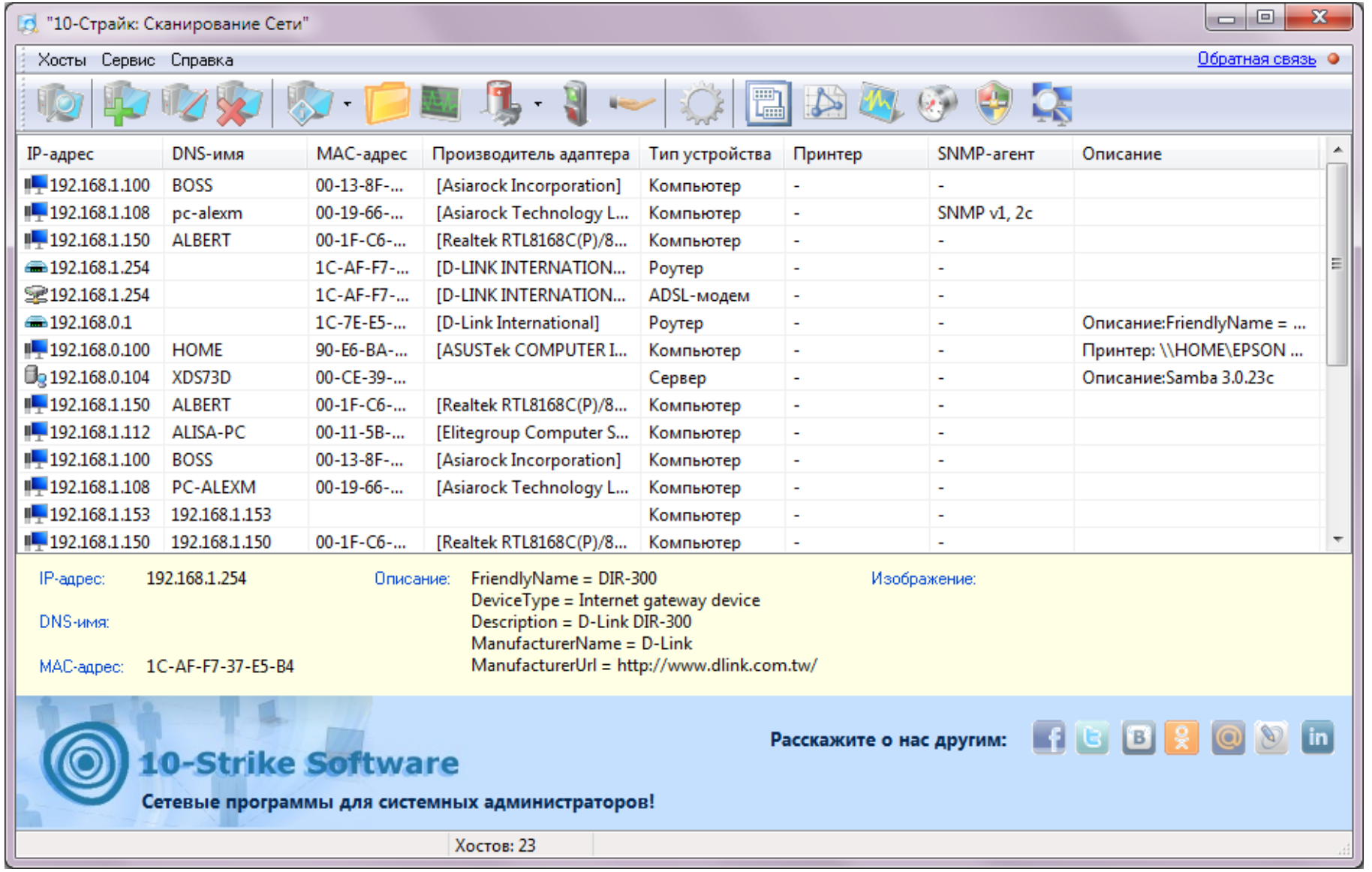
- **Passive scan** - **пассивное сканирование портов** SYNc-(SYNs-ACKc)-RSTc и SYNc-RSTs. При достаточно умном поведении сканера (например, сканирование с низкой скоростью или проверка лишь конкретных портов) детектировать пассивное сканирование невозможно, поскольку оно ничем не отличается от обычных попыток установить соединение.

- **Защита** - закрыть на firewall все сервисы, доступ к которым не требуется извне.

Атака: Сканирование сети

- **Цель этой атаки состоит в том, чтобы выяснить, какие компьютеры подключены к сети и какие сетевые сервисы на них запущены.**
- Первая задача в простейшем случае решается путем посылки Echo-собшений протокола ICMP с помощью утилиты ping с последовательным перебором всех адресов сети или отправкой Echo-сообщения по широковещательному адресу.
- Для сканирования TCP-портов существует несколько способов. Самый простой - установление TCP-соединений с тестируемым портом. В этом случае пошляется большое количество открытых и сразу прерванных соединении, поэтому и гаку в такой реализации просто обнаружить.
- **Наиболее известные сканеры сети:** Rapid7 Nexpose, Tenable Nessus, OpenVAS, Nmap и многие другие.

Пример сканера сети



Атака: TCP Reset

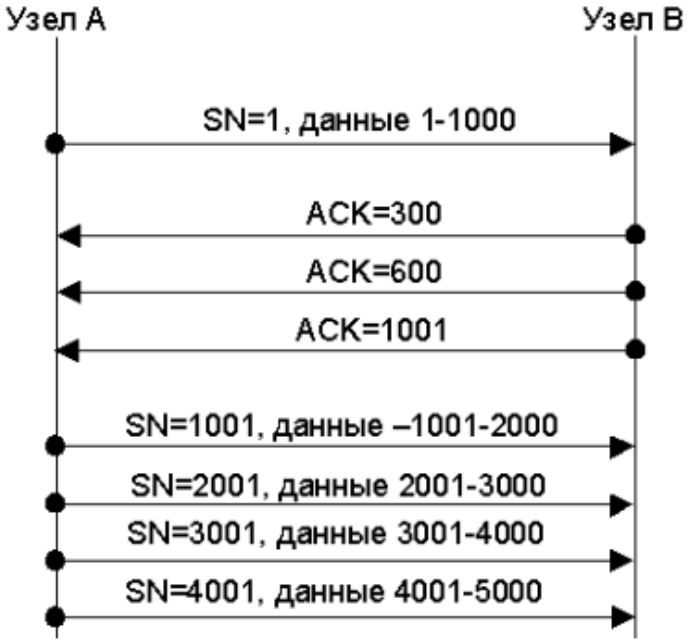
- **TCP Reset Attack: Атакующий отправляет поддельные пакеты TCP RESET, чтобы прервать установленное соединение.**
- **TCP Reset** - если бит RST=1, то получатель должен немедленно прекратить использовать данное соединение. Атакующий используя IP-spoffing и сфальсифицированный RST-сегмент с номером SN, находящимся в рамках доступного окна, может разрывать чужие сессии.
- Например, сбросить TCP-соединение между BGP-соседями, чтобы каждый из соседей удалил маршруты, полученные от другого, и распространил информацию о недостижимости этих маршрутов другим своим соседям.

- **Защита** - шифрование на уровне IP или BGP.

Атака: Принуждение к ускорению/замедлению передачи

- **3. Принуждение к ускорению/замедлению передачи** - злоумышленник отбирает себе ресурсы сервера или замедляет соединения прочих участников сети.

- **Варианты реализации атаки:**
  - а) ложные дубликаты подтверждений;
  - Ь) преждевременные подтверждения;
  - **с) расщепление подтверждений:**



Пусть сервер А начинает медленный старт с В. Окно перегрузки cwnd=1, поэтому клиенту В высылается один полноразмерный сегмент (например, 1000).

Нарушитель В вместо 1 подтверждения о получении сегмента (ACK, SN=1001), имитирует получение сегмента по частям и высылает серию подтверждений (ACK, SN=300, 600 и 1001).

Это воздействует на алгоритм медленного старта и вынудит А необоснованно увеличить cwnd до 4 (отправить 4 сегмента вместо 2). На к шаге узел А будет отправлять не V=N*2Ak байт, а V=N*MAk байт (где, V - скорость потока, N - размер сегмента, M - количество расщеплений).

При агрессивной атаке (1000 подтверждений на сегмент) уже на 4 шаге V=1 TiB/sec. Скорость ограничена лишь возможностями сети и узлов. Другие узлы диагностируют состояние затора и уменьшают скорость передачи данных, фактически освобождая канал для злоумышленника.

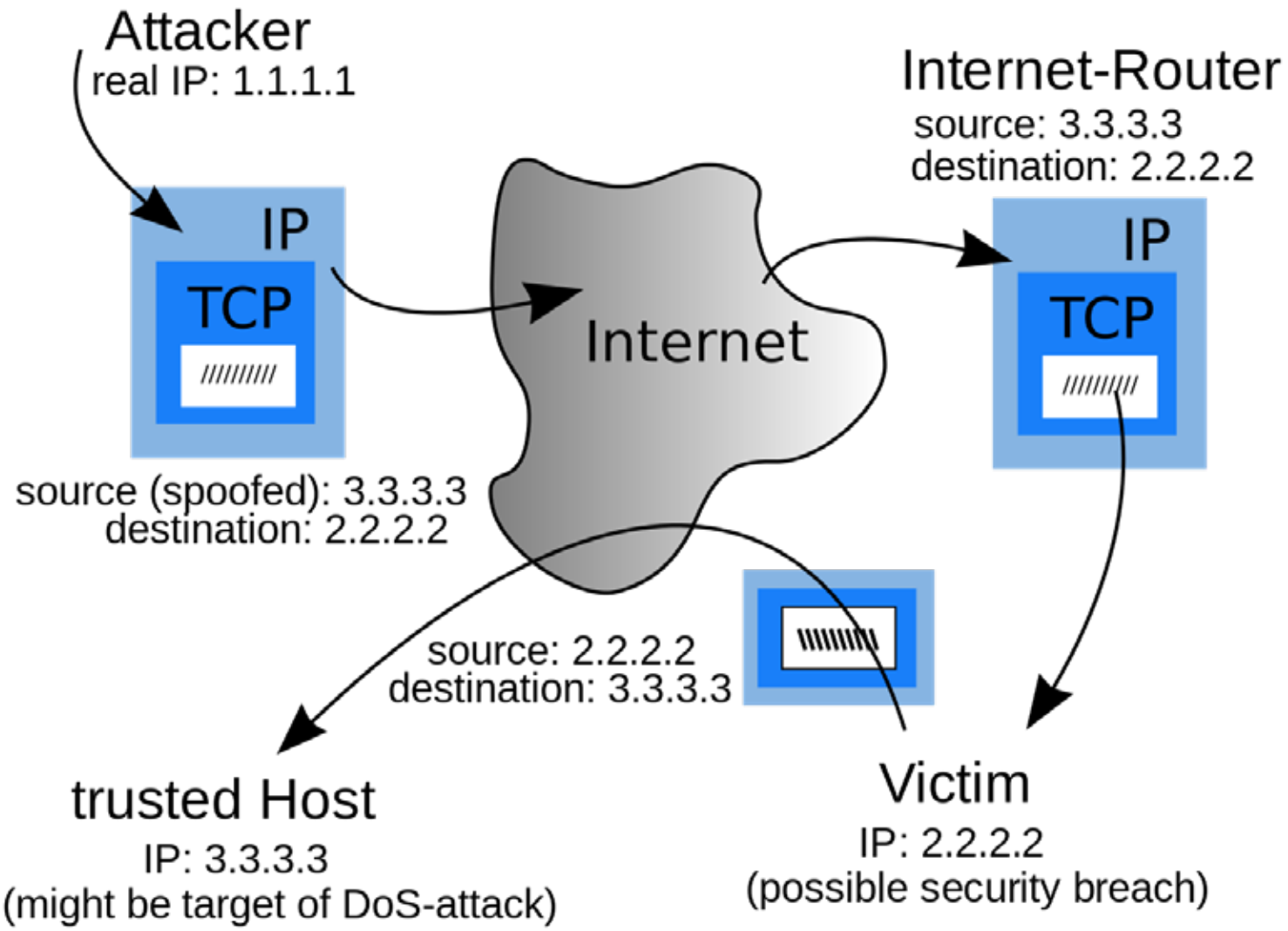
Защита - пока нет, нужны изменения алгоритмов регулировки потока в реализации стека TCP.

Атака: IP spoofing

- **IP-спуфинг (от англ. spoof — мистификация):**
  1. Вид атаки, заключающийся в **использовании чужого IP-адреса** источника с целью обмана системы безопасности.
  2. Метод, используемый в некоторых атаках. **Состоит в изменении поля «адрес отправителя» IP-пакета.** Применяется с целью сокрытия истинного адреса атакующего, с целью вызвать ответный пакет на нужный адрес, а также с иными целями.

- Для злоумышленника базовый принцип атаки заключается в фальсификации собственных заголовков IP-пакетов, в которых изменяется, среди прочего, IP-адрес источника. **Атака IP-спуфинг часто называется «слепой подменой» (Blind Spoofing).** Это связано с тем, что **ответы на фальсифицированные пакеты не могут прийти** машине крэкера, так как был изменён исходящий адрес. **Однако всё-таки существуют два метода получения ответов:**
  1. **Маршрутизация от источника (Source routing):** в протоколе IP существует возможность маршрутизации от источника, которая позволяет задавать маршрут для ответных пакетов. Этот маршрут представляет собой набор IP-адресов маршрутизаторов, через которые должен проследовать пакет. Для крэкера достаточно предоставить маршрут для пакетов до маршрутизатора, им контролируемого. В наше время большинство реализаций стека протоколов TCP/IP отбраковывают пакеты с маршрутизацией от источника;
  2. **Перемаршрутизация (Re-routing):** если маршрутизатор использует протокол RIP, то его таблицы можно изменить, присылая ему RIP-пакеты с новой информацией о маршрутах. С помощью этого крэкер добивается направления пакетов на подконтрольный ему маршрутизатор.

Атака: IP spoofing - Пример атаки



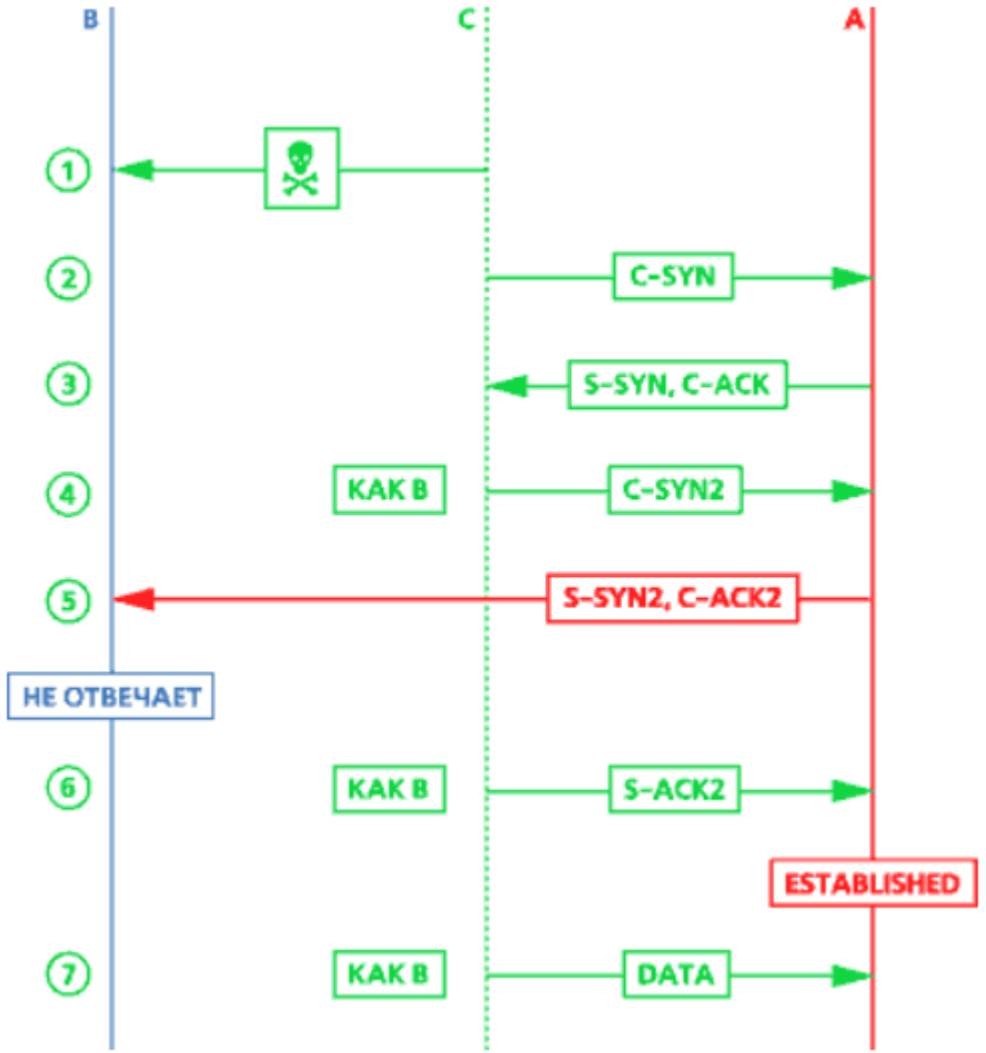
Атака: IP-spoofing + TCP sequence prediction

- **Атака с использованием IP-spoofing (подделка IP-адреса) в сочетании с TCP sequence prediction (предсказание последовательности TCP)** — это сложная техника, направленная на внедрение злоумышленника в установленную TCP-сессию.
  - **IP-spoofing** — это метод, при котором атакующий создает IP-пакеты с поддельным (спуфинговым) адресом отправителя, с целью обмана системы получателя и заставления её думать, что пакеты приходят от доверенного источника.
  - **TCP sequence prediction** — это метод, при котором атакующий пытается предсказать следующий номер последовательности пакетов в TCP-сессии. TCP использует номера последовательности для упорядочивания пакетов данных и подтверждения их доставки. Если злоумышленник может точно предсказать следующий номер последовательности, он может вставить в сессию свои пакеты, которые будут приняты как легитимные.
- **Комбинируя эти две техники, атакующий может не только отправлять поддельные пакеты от имени доверенного хоста, но и делать это таким образом, чтобы пакеты были приняты в правильном порядке, что позволяет ему вмешиваться в коммуникацию или вставлять вредоносные данные в открытую сессию.**
- Это может привести к несанкционированному доступу к данным, нарушению целостности данных или проведению дальнейших атак на систему.

Атака: IP-spoofing + TCP sequence prediction

- **IP-spoofing + TCP sequence prediction** - предсказание TCP ISN.

- Например, для захвата rlogin/rsh (доверительный удалённый логин) порядок атаки:
- 1. Через легитимный сервис (например web) провоцируем сервер (A) на TCP-связь (шлём SYN) от своего имени и узнаём алгоритм образования ISN;
- 2. Выводим жертву-клиента (B) из сети (например, SYN Flooding) на пару минут;
- 3. От имени клиента (IP-spoofing) формируем ложный запрос rlogin/rsh к серверу;
- 4. Клиент не сможет сделать RST на неожиданный SYN-ACK, т.к. выведен нами из строя на шаге 2;
- 5. Ответ мы не получим, его сервер отправит не нам, а настоящему клиенту, поэтому предсказываем диапазон возможных ISN-сервера и формируем один (или серию) ответов от имени клиента об успешном «тройном рукопожатии»;
- 6. Внутри этих ложных ответов уже будут содержаться telnet команды реконфигурации сервиса rlogin: “# echo **’ > -/.rhosts”, * - для включения доверия с любого узла.



Атака: IP-spoofing + TCP sequence prediction

- **Защита** - практически все перечисленные ниже компоненты защиты уже реализуются в сетях.
- Следует минимизировать доверие машин друг другу.
- Перейти на протокол ssh.
- Усложнить угадывание sequence number (ключевой элемент атаки). Например, можно увеличить скорость изменения sequence number на сервере или выбирать коэффициент увеличения sequence number случайно (желательно, используя для генерации случайных чисел криптографически стойкий алгоритм).
- Использовать рукопожатие с COOKIE.
- Шифрование TCP/IP-потока решает в общем случае проблему IP-spoofing.
- Настроить firewall для фильтрации пакетов, посланных нашей сетью наружу, но имеющих адреса, не принадлежащие нашему адресному пространству. Это защитит мир от подобных атак из вашей собственной сети.

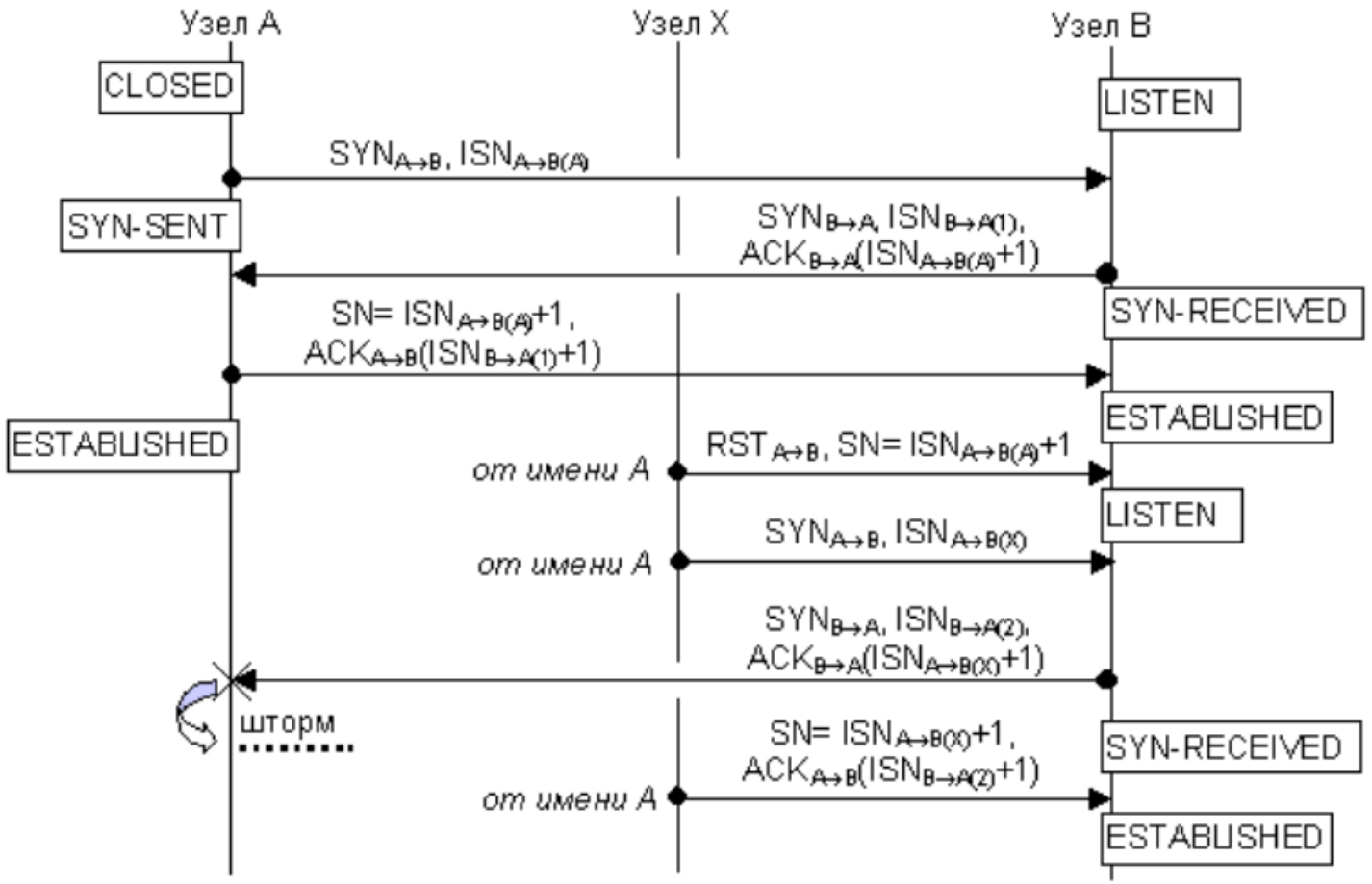
Атака: TCP Hijacking - **перехват** TCP-**сессии**

TCP Session Hijacking - перехват TCP-сессии через десинхронизацию, в данном случае перехватывается весь сетевой поток уже после установки соединения.

Далее сессия строится произвольным образом.

Атакующему нужно быть на пути трафика и работать как Man-in-the-Middle (MitM) .

Метод является комбинацией "подслушивания" и IP spoofing'a.



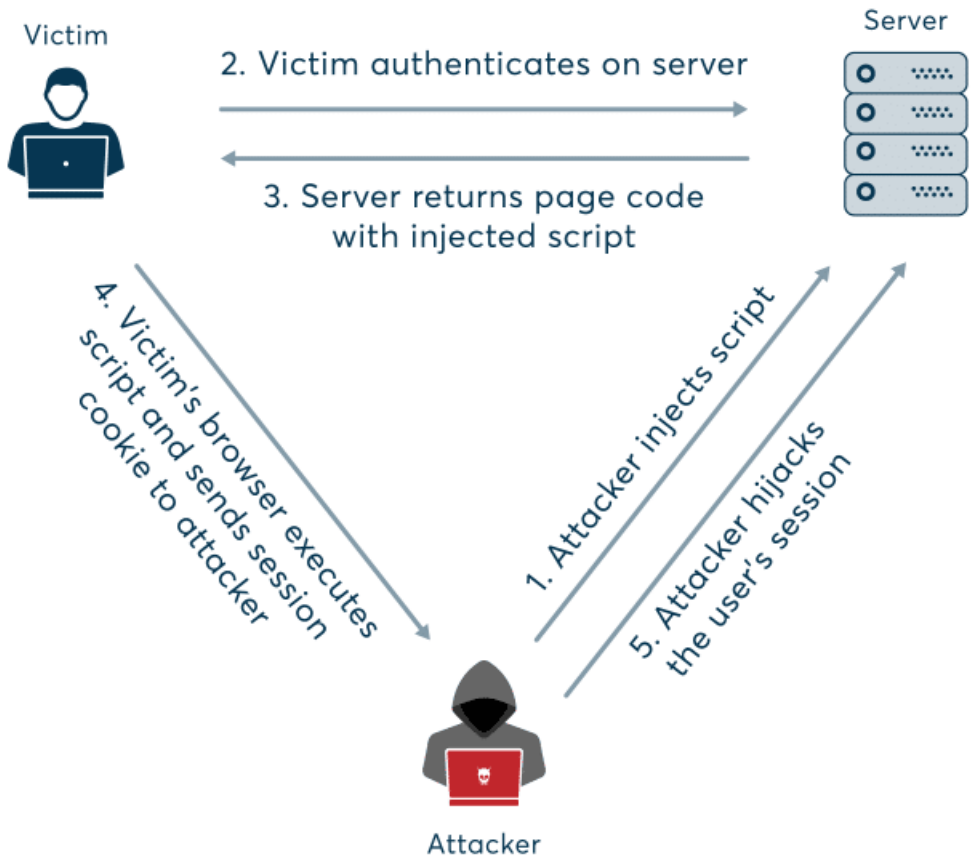
Защита - противодействие IP-spoofing и шифрование на уровне IP.

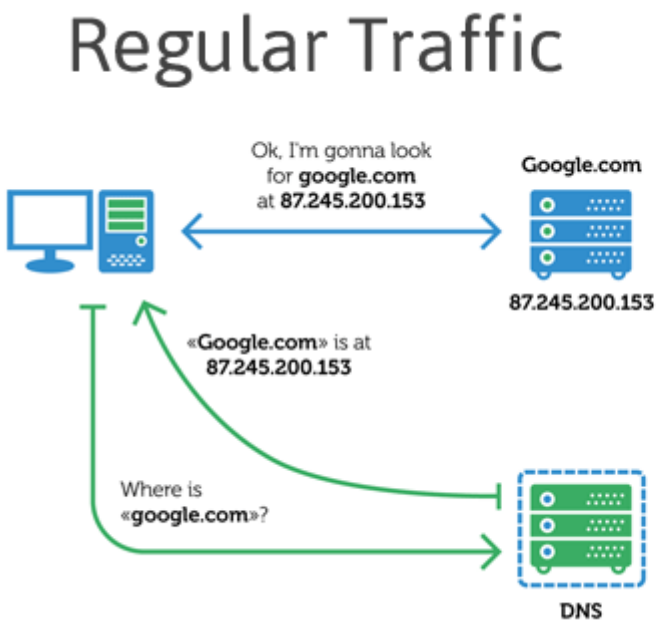
Атака: TCP Hijacking

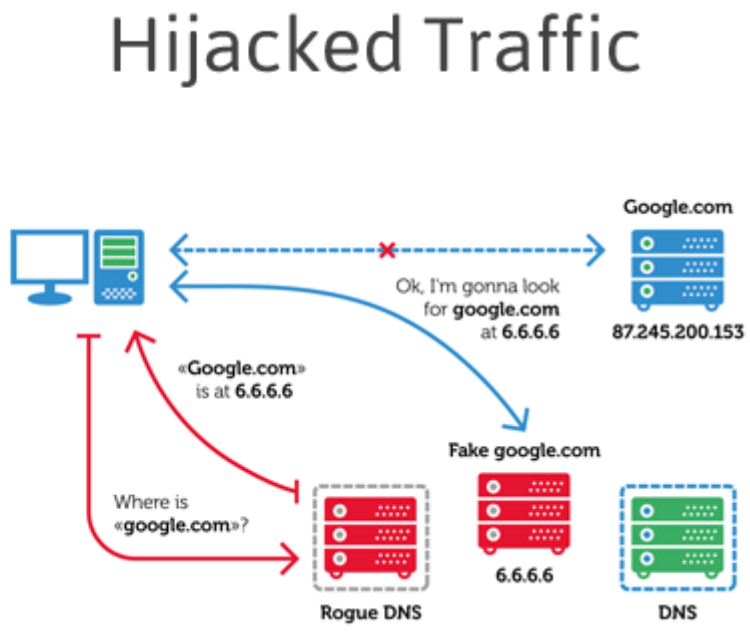
- **TCP Hijacking — Разновидность атаки «Человек посередине», когда атакующий способен просматривать пакеты участников сети и посылать свои собственные пакеты в сеть.** Атака использует особенности установления соединения в протоколе TCP, и может осуществляться как во время «тройного рукопожатия», так и при установленном соединении.

- Проблема возможной подмены TCP-сообщения важна, так как анализ протоколов FTP и TELNET, реализованных на базе протокола TCP, показал, что проблема идентификации FTP и TELNET-пакетов целиком возлагается данными протоколами на транспортный уровень, то есть на TCP.

Атака: TCP Hijacking – **Пример атаки**

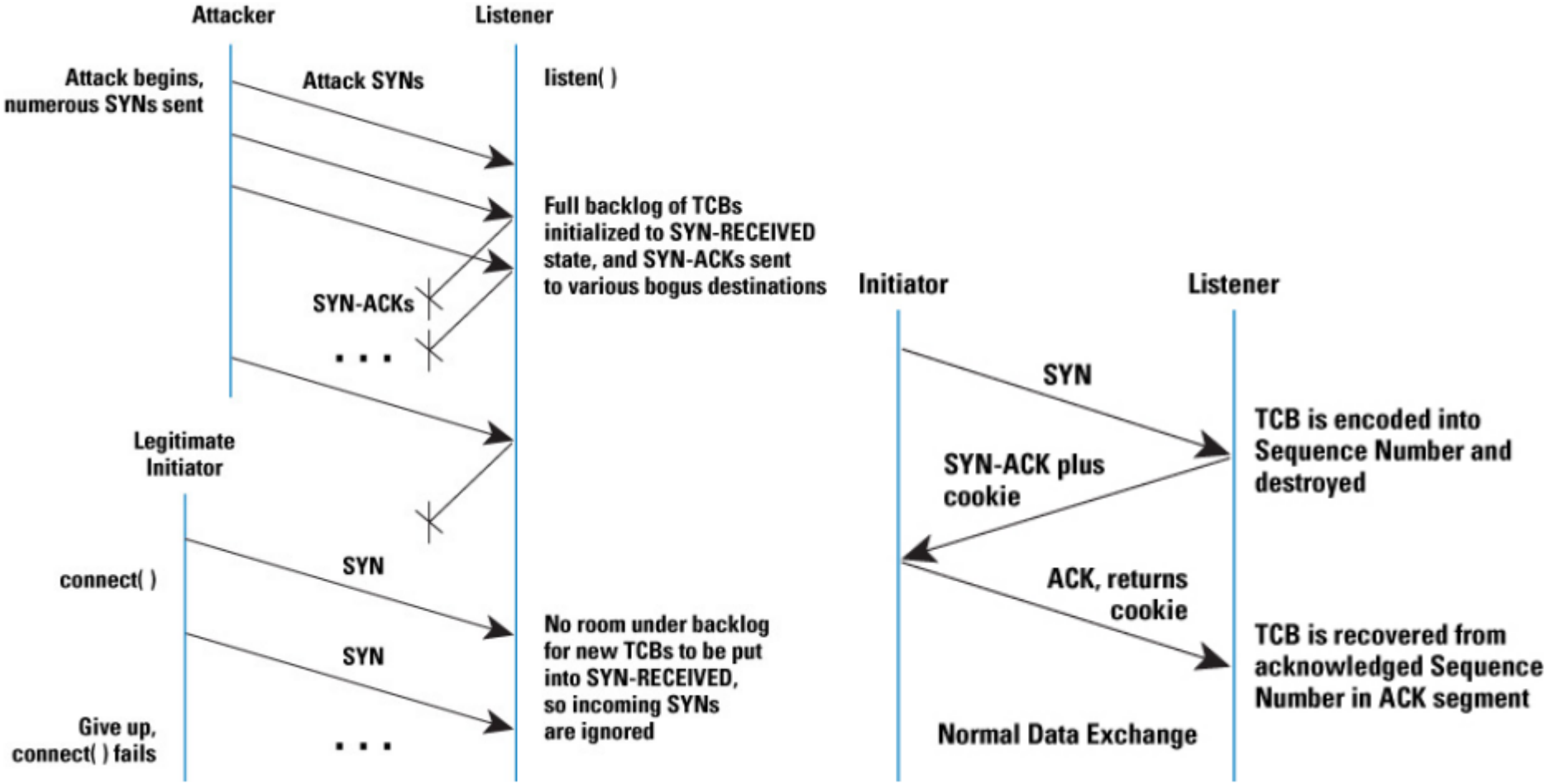






Атака: SYN Flood

SYN Flooding - затопление полуоткрытыми сессиями, переполняющими очереди сервера, после чего сервер перестает отвечать на запросы легитимных клиентов. Зачастую достаточно 50-100 ложных сессий и сервер будет «тормозить».



Защита - частичная за счёт уменьшения таймаутов между SYNs-ACK-с и ACK-s; полная защита за счёт введения cookie (квитанции), или за счёт четырёхкратного рукопожатия с cookie, см. протокол SCTP.

Атака: SYN Flood

- **SYN Flood (SYN-флуд) — одна из разновидностей сетевых атак типа отказ от обслуживания (Dos-атака), которая заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий срок (RFC 4987).**
- **Цель - привести узел в состояние, когда он не сможет принимать запросы на открытие новых соединений, а в худшем случае «зависнет».**

- Согласно процессу «трёхкратного рукопожатия» TCP, клиент посылает пакет с установленным флагом SYN (synchronize). В ответ на него сервер должен ответить комбинацией флагов SYN+ACK (acknowledges). После этого клиент должен ответить пакетом с флагом ACK, после чего соединение считается установленным.
- **Принцип атаки заключается в том, что** злоумышленник, посылая SYN-запросы, переполняет на сервере (цели атаки) очередь на подключения. При этом он игнорирует SYN+ACK пакеты цели, не высылая ответные пакеты, либо подделывает заголовок пакета таким образом, что ответный SYN+ACK отправляется на несуществующий адрес. В очереди подключений появляются так называемые полуоткрытые соединения (англ. half-open connection), ожидающие подтверждения от клиента. По истечении определенного тайм-аута эти подключения отбрасываются. Задача злоумышленника заключается в том, чтобы поддерживать очередь заполненной таким образом, чтобы не допустить новых подключений. Из-за этого клиенты, не являющиеся злоумышленниками, не могут установить связь, либо устанавливают её с существенными задержками.
- **Атака основывается на уязвимости ограничения ресурсов операционной системы для полуоткрытых соединений**, описанной в 1996 году группой CERT, согласно которой очередь для таких подключений была очень короткой (например, в Solaris допускалось не более восьми подключений), а тайм-аут подключений — достаточно продолжительным (по RFC 1122 — 3 минуты).

Атака: TCP Full Connection Flooding

- **TCP Full Connection Flooding – разновидность SYN Flood атаки.**
- **Атаку SYN flood удерживает большое число соединений на атакуемом узле в состоянии SYN-RECEIVED. Но, состояния множество ESTABLISHED и FIN-WAIT-1 также вызывают DoS.**
- С сервером-жертвой создаётся множество легитимных полных троекратных TCP соединений с одного узла (до 65 000 штук по количеству портов для сокета), что истощит очередь сессий.
- Дополнительно можно сформировать вредоносную нагрузку, разработанную под конкретный сервис, например можно:
  - запросить загрузку с сервера какого-нибудь большого файла, сервер загрузит первую часть этого файла в стек TCP для отправки, используя при этом буферы в памяти ядра системы. Вернуть эти буферы система не сможет пока нападающий не подтвердит, что данные им получены. Закончится доступная память на подвергающейся атаке системе.
  - провести манипуляции с размером окна TCP - установить в 0.
  - запросить создание динамической страницы, для истощения процессора (HTTP Flood).
  - подключить фрагментацию IP - отсылать множество пакетов больших размеров, в каждом из которых содержится один пропущенный фрагмент.
  - подключить сегментацию TCP - создать «дыру» в TCP потоке, отсылая данные из конца текущего окна, в середине которого ничего не содержится. Система зарезервирует эти данные до тех пор, пока вы не решите переслать недостающие пакеты.

- 100% защиты пока нет! - все варианты атаки эксплуатируют одну, но, фундаментальную слабость TCP -неконтролируемое число соединений к TCP-IP сокету жертвы. Можно ослабить воздействие атак используя специализированные системы защиты: FireProof фирмы Radware или TrafficMaster Enforcer фирмы Maze Networks.

Атака: Sniffing **(Перехват)**

- **5. Sniffing** - атака заключаются в перехвате и анализе сетевого потока.

- **Защита** - использование свитчей и шифрования данных.

Атака: Tiny Fragment Attack - атака крошечными фрагментами

- **9. Tiny Fragment Attack - атака крошечными фрагментами.**

- Если на вход фильтрующего маршрутизатора поступает фрагментированная дейтаграмма, маршрутизатор производит досмотр только первого фрагмента дейтаграммы (определяется по Fragment Offset=0 в IP).
- Если фрагмент не удовлетворяет условиям, он уничтожается. Остальные фрагменты пропускаются, без затрат вычислительных ресурсов фильтра, т.к. без первого фрагмента дейтаграмма все равно не может быть собрана на узле назначения.
- При конфигурировании фильтра перед сетевым администратором часто стоит задача: разрешить соединения с TCP-сервисами Интернет, инициируемые компьютерами внутренней сети, но запретить установление соединений внутренних компьютеров с внешними по инициативе последних.

IP-заголовок MF=1, Fragment Offset=0	
Source Port	Destination Port
Sequence Number (SN)	

IP-заголовок MF=0, Fragment Offset=1								
Acknowledgment Sequence Number (ACK SN)=0								
Data Offset	reserved	-	-	-	-	SYN	-	Window
Checksum								Urgent Pointer=0
Options								Padding

Атака: Tiny Fragment Attack - **атака крошечными фрагментами**

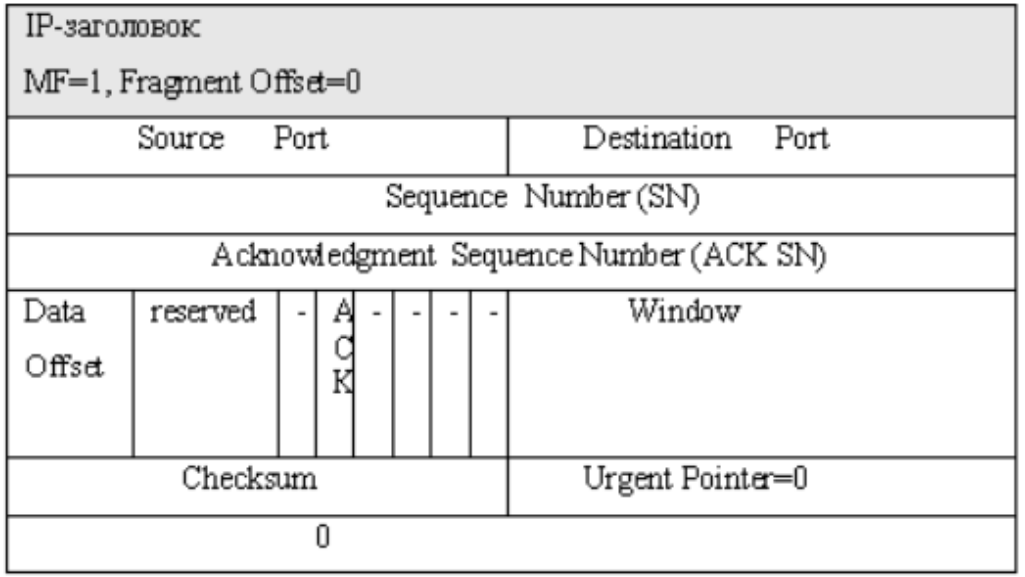
- Для решения поставленной задачи фильтр конфигурируется на запрет пропуска TCP-сегментов, поступающих из внешней сети и имеющих установленный бит SYN в отсутствии бита АСК; сегменты без этого бита беспрепятственно пропускаются в охраняемую сеть, поскольку они могут относиться к соединению, уже установленному ранее по инициативе внутреннего компьютера.
- Рассмотрим, как злоумышленник может использовать фрагментацию, чтобы обойти это ограничение, то есть, передать SYN-сегмент из внешней сети во внутреннюю.

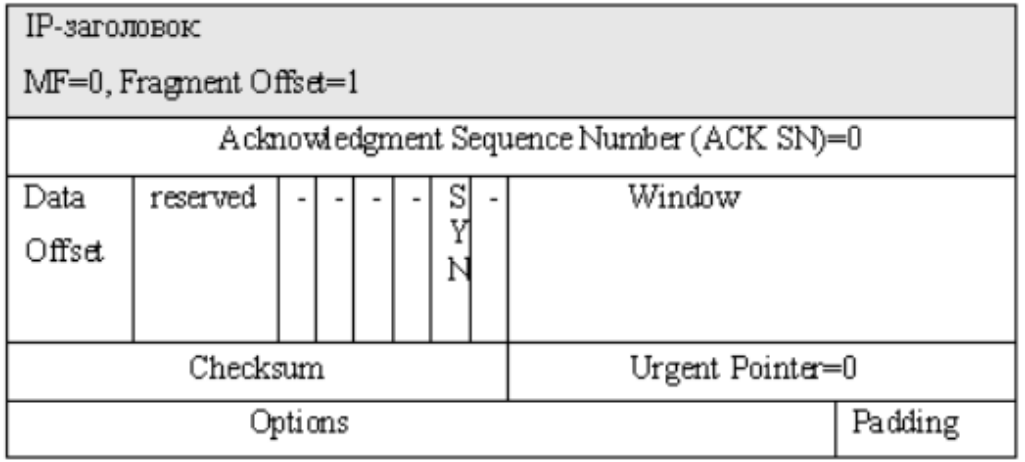
- **Защита** - фильтрующему маршрутизатору не следует инспектировать содержимое первых фрагментов датаграмм — это было бы равносильно сборке датаграмм на промежуточном узле, что быстро поглотит все вычислительные ресурсы маршрутизатора. Достаточно реализовать один **из двух следующих подходов:**
- **1) не пропускать датаграммы с Fragment Offset=0 и Protocol=6 (TCP),** размер поля данных которых меньше определенной величины, достаточной, чтобы вместить все «интересные поля» (например, 20);
- **2) не пропускать датаграммы с Fragment Offset=1 и Protocol=6 (TCP):** наличие такой датаграммы означает, что TCP-сегмент был фрагментирован с целью скрыть определенные поля заголовка и что где-то существует первый фрагмент с 8 октетами данных. Несмотря на то, что в данном случае первый фрагмент будет пропущен, узел назначения не сможет собрать датаграмму, так как фильтр уничтожил второй фрагмент.
- Т.к. в реальной жизни никогда не придется фрагментировать датаграмму до минимальной величины, риск потерять легальные датаграммы, применив предложенные выше методы фильтрации, равен нулю.

Атака: Overlapping Fragment Attack - **атака накладывающимися фрагментами**

- **10. Overlapping Fragment Attack - атака накладывающимися фрагментами.**
- Рассмотрим пример датаграммы, несущей TCP-сегмент и состоящей из двух фрагментов. В поле данных первого фрагмента находится полный TCP-заголовок, без опций, дополненный нулями до размера, кратного восьми октетам.
- В поле данных второго фрагмента — часть другого TCP-заголовка, начиная с девятого по порядку октета, в котором установлен флаг SYN.

Защита. Если для защиты от Tiny Fragment Attack применяется подход 1) из описанных выше (инспекция первого фрагмента датаграммы), то с помощью накладывающихся фрагментов злоумышленник может обойти эту защиту. Маршрутизатор, применяющий второй подход, будет успешно противостоять Tiny Fragment Attack с накладывающимися фрагментами.





Атака: Teardrop Attack **(Атака фрагментированными пакетами)**

- **TearDrop - разновидность DoS-нападения. Пакетная фрагментация.**
- Отказ в обслуживании, достигаемый с помощью пакетной фрагментации использует уязвимости некоторых стеков TCP/IP, связанных с дефрагментацией пакетов (сборкой IP-фрагментов).

- **Атака Teardrop – это один из вариантов DoS-атаки, особенно эффективный для устройств, работающих на базе устаревших операционных систем** (Windows 95, Windows NT, старые версии Linux).

- **Метод основан на отправке в адрес целевого хоста небольших фрагментов, которые невозможно собрать в единый объект.** Такой эффект достигается через манипуляцию полем Fragment offset в заголовке пакета. В случае корректной передачи данных там указывается смещение конкретного блока от начала объекта — его координаты относительно первого фрагмента.
- При атаке фрагментированными пакетами значение Fragment offset указывается некорректно. При сборке блоки накладываются друг на друга, что приводит к неработоспособности программы. Большинство современных ОС нечувствительны к этой атаке.

Overlapping Fragment Attack и Teardrop Attack

- **Overlapping Fragment Attack - вид атаки, при которой злоумышленник отправляет фрагментированные IP-пакеты с сегментами, которые перекрывают друг друга**. При попытке реассамблирования таких пакетов целевая система может столкнуться с конфликтом, что некоторые байты данных имеют два разных значения. Это может вызвать неопределенное поведение в сетевом стеке, вплоть до отказа в обслуживании. Злоумышленник может использовать это для обхода систем обнаружения вторжений или фильтрации трафика.
- **Teardrop Attack - атака эксплуатирующая уязвимости в обработке фрагментированных пакетов.** Атакующий отправляет фрагменты IP-пакетов с "перекрытыми" смещениями, что приводит к ошибке при попытке системы-жертвы реконструировать исходный пакет из фрагментов. В результате может произойти сбой в работе операционной системы из-за неспособности корректно обработать такие "испорченные" фрагменты.

- **Обе атаки используют фрагментацию для нарушения работы целевой системы, но Overlapping Fragment Attack более сосредоточена на запутывании процесса реконструкции пакетов для обхода защиты, тогда как Teardrop Attack направлена на вызывание сбоев в системе.**

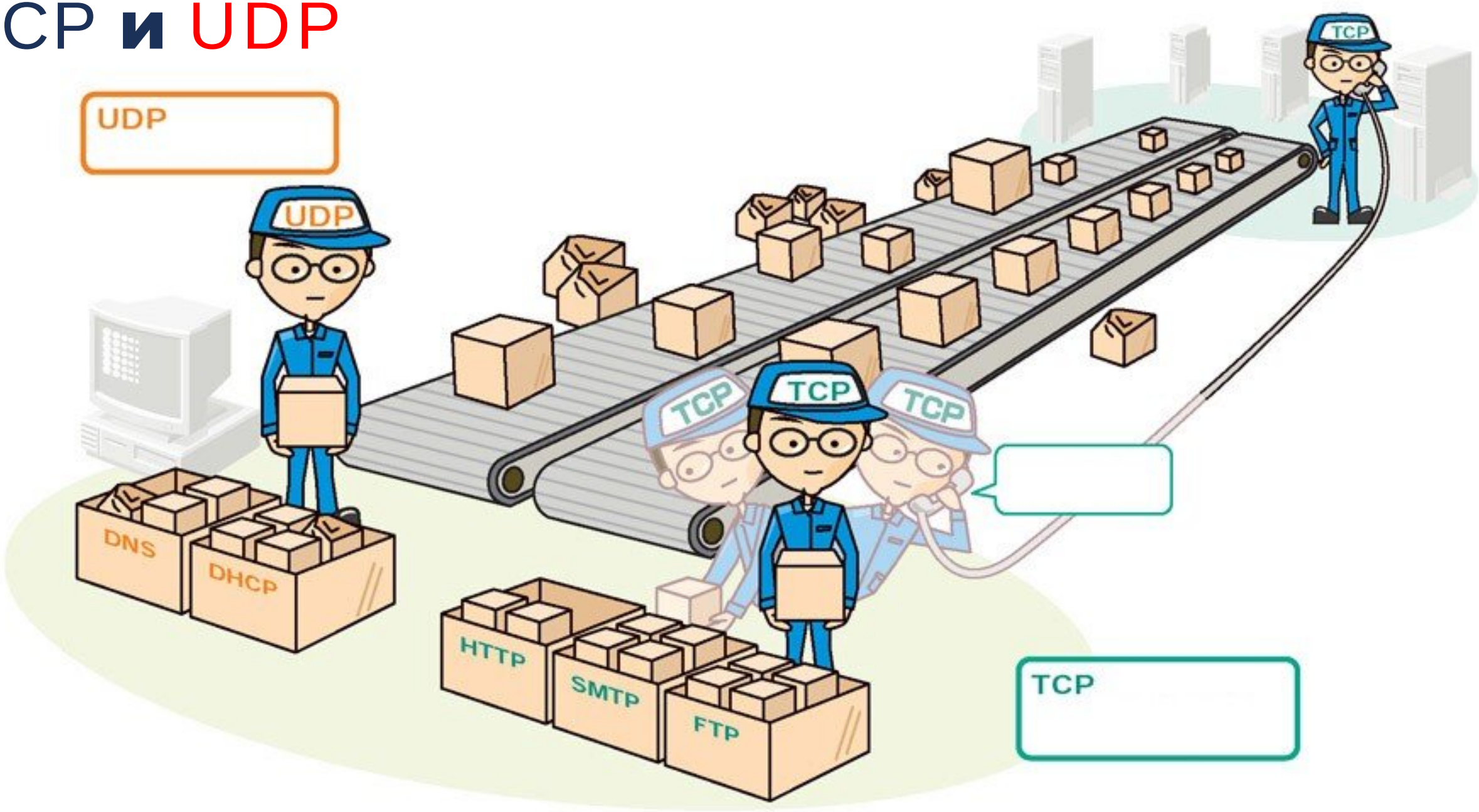
Атака : TCP Zero Window Attack (Десинхронизация нулевыми данными)

- **Атака десинхронизации нулевыми данными на TCP протокол (TCP Zero Window Attack) — это вид атаки, при которой атакующий целенаправленно отправляет пакеты с установленным размером окна в ноль в уже установленное TCP-соединение.** Размер окна в TCP-заголовке сообщает отправляющей стороне, сколько байтов данных получающая сторона готова принять и обработать до следующего подтверждения. Когда размер окна устанавливается в ноль, это указывает отправителю, что получатель в данный момент не может принять какие-либо данные.
- В нормальных условиях это механизм управления потоком, который позволяет получателю предотвратить переполнение своего буфера данных. Однако в контексте атаки, злоумышленник может намеренно отправлять пакеты с размером окна равным нулю, чтобы заблокировать передачу данных, даже если на самом деле получатель готов принимать данные. Это может вызвать десинхронизацию TCP-сессии, поскольку отправитель будет вынужден остановить отправку данных, ожидая, когда окно снова станет положительным.
- Такая атака может быть использована как часть более широкой стратегии DoS-атаки (отказ в обслуживании), с целью потребления сетевых и системных ресурсов жертвы, замедления или полного прекращения передачи данных.

Атака : TCP Zero Window Attack (Десинхронизация нулевыми данными)

- В этом случае взломщик Е дожидается момента, когда пользователи А и Б по обмениваются данными, и посылает пользователю А от имени Б сегменте «нулевыми» данными и еще один сегмент для Б от имени А также с «нулевыми» данными.
- Под «пулевыми» понимаются данные, которые будут проигнорированы па прикладном уровне, то есть приложение, которому они адресованы, не пошлет никаких данных в ответ.
- Такой метод десинхронизации удобен для Telnet-соединений, потому что и этом случае время ожидания неактивности невелико. Сегменте пулевыми данными может содержать некоторое число команд IAC NOP (нет операции).
- Защититься от такой атаки можно, контролируя переход в десинхронизованное состояние, обмениваясь информацией о sequence number, acknowledgement number. Но злоумышленник может менять эти значения, ведь он прослушивает пакеты. Более надежной защитой кажется отслеживание АСК-бурь.
- Применение криптографически стойкого алгоритма для шифрования TCP-потока - наиболее надежный способ защиты.

TCP и UDP



Атаки на протокол UDP

- На протокол UDP существует не так много атак, как на TCP. Это можно объяснить прежде всего тем, что этот протокол менее распространен. К тому же отсутствие установки соединения лишает самой возможности реализации целого ряда атак, характерных для TCP.

- **Виды атак на UDP**
  - UDP Storm
  - Атаки на протокол ICMP
    - Сброс соединений (reset)
    - Снижение скорости

UDP Storm

- Используется в том случае, если на жертве открыто как минимум два **UDP** порта, каждый из которых отсылает отправителю какой-нибудь ответ.

- **Например**, порт 37 с сервером time на запрос отправляет текущую дату и время. Взломщик отправляет UDP пакет на один из портов жертвы, но в качестве отправителя указывает адрес жертвы и второй открытый UDP порт жертвы. Тогда порты начинают бесконечно отвечать друг другу, что **снижает производительность.** Шторм прекратится, как только один из пакетов пропадёт (например, из-за перегрузки ресурсов).

- **Рекомендации**: по возможности исключить использование сервисов, которые принимают UDP пакеты, либо отрезать их от внешней сети межсетевым экраном.

UDP Storm

- Для протокола UDP так же, как и для других протоколов, характерны DoS-атаки **«отказ в обслуживании».**
- Для реализации данного вида атак необходимо сгенерировать большое количество UDP-пакетов, направленных на определенную машину.
- В результате успешной атаки происходит либо **зависание, либо его перезагрузка.** Осуществить атаку можно из-за того, что в UDP отсутствует механизм предотвращения перегрузок.

Атаки на протокол ICMP

- Протокол TCP в настоящее время является основным транспортным протоколом в сетях IP и, в частности, в сети Интернет.
- Широкое распространение этого протокола делает его привлекательным объектом атак.
- **Атаки на TCP соединения можно осуществлять с помощью пакетов ICMP.**
- С помощью ряда атак существует возможность **существенного снижения скорости обмена данными** и даже полного разрыва произвольных соединений TCP с помощью передачи потока специально подготовленных пакетов ICMP с удаленного хоста.

Сброс соединений (reset)

- **В соответствии со стандартом Интернета «Требования к хостам» хостам следуй разрывать соответствующее соединение TCP в ответ на получение сообщения ICMP о критичной ошибке.** Используя это, атакующий может вслепую сбросить соединение между парой станций, передавая одному из хостов сообщения ICMP, указывающие на такой тип ошибки.
- Например, можно передавать одной из сторон соединения сообщения о том, что другая сторона не поддерживает соответствующего протокола (Protocol Unreachable), от имени того самого хоста (другой стороны соединения). В таких сообщениях сложно усмотреть что-либо подозрительное, поэтому можно надеяться, что они не будут отброшены тем или иным фильтром па пути от атакующего. Необходимость выполнения атаки вслепую практически не осложняет ее организации, поскольку атакующему для успеха не требуется получать каких-либо пакетов от объекта атаки. Не требуется от атакующего и организации перехвата пакетов или изменения пути их доставки, поскольку он должен лишь направить подготовленные пакеты ICMP, содержащие код одной из критических ошибок и квартет идентификации соединения в ноль данных ICMP, по адресу сервера или клиента в атакуемом соединении. В соответствии с заданной для протокола TCP политикой обработки ошибок получение сообщения ICMP, в поле данных которого содержится заголовок IP с адресами клиента и сервера, а также заголовок TCP с используемыми в данном соединении номерами портов приведет к немедленному разрыву сообщения. При этом ни у одного из участников соединения не остается в журнальных файлах никакой информации об источнике атаки, поскольку в полученных пакетах могут исползоваться (и обычно используются) подставные адреса отправителя (обычно это адрес другой стороны атакуемого соединения).
- Следует отмстить, что на сегодняшний день далеко не все реализации стека TCP/IP подвержены этой уязвимости.

Снижение скорости

- Кроме возможности сброса соединений TCP пакеты ICMP позволяют существенно снизить скорость передачи данных через соединения, не нарушая их работы полностью.
- Для выполнения такой задачи передаются сообщения ICMP о некритических ошибках (тип 3 с кодом 4 и тип 4 с кодом 0). Механизм такой атаки весьма похож на описанную выше атаку для разрыва соединений.
- Следует отметить, что атаки, приводящие к снижению скорости передачи данных через соединение, в некоторых случаях могут доставить даже больше хлопот, нежели полный разрыв соединений.

Защита в целом

- Системный администратор, исходя из политики сетевой безопасности в своей организации, и имея четкое представление о возможных инцидентах и их последствиях, должен определить, какие меры являются необходимыми и приемлемыми для его сети.
- Он должен:
  - Настраивать фильтрацию на маршрутизаторе
  - Проводить анализ сетевого трафика
  - Выполнять защиту маршрутизатора
  - Осуществлять защиту хоста
  - И периодически проводить превентивное сканирование сети

Защита: 1. Фильтрация на маршрутизаторе

- **Фильтры на маршрутизаторе, соединяющем сеть предприятия с Интернетом, применяются для запрета пропуска датаграмм, которые могут быть использованы для атак как на сеть организации из Интернета**, так и на внешние сети злоумышленником, находящимся внутри организации.
- **1.** Запретить пропуск датаграмм с широковещательным адресом назначения между сетью организации и Интернетом.
- **2.** Запретить пропуск датаграмм, направленных из внутренней сети (сети организации) в Интернет, но имеющих внешний адрес отправителя.
- **3.** Запретить пропуск датаграмм, прибывающих из Интернета, но имеющих внутренний адрес отправителя.
- **4.** Запретить пропуск датаграмм с опцией «Source Route» и, если они не используются для групповой рассылки, инкапсулированных датаграмм (IP-датаграмма внутри IP-датаграммы).

Защита: 1. Фильтрация на маршрутизаторе

- **5.** Запретить пропуск датаграмм с ICMP-сообщениями между сетью организации и Интернетом, кроме необходимых (Destination Unreachable: Datagram Too Big— для алгоритма Path MTU Discovery; также Echo, Echo Reply, Destination Unreachable: Network Unreachable, Destination Unreachable: Host Unreachable, TTL exceeded).
- **6.** На сервере доступа клиентов по коммутируемой линии — разрешить пропуск датаграмм, направленных только с или на IP-адрес, назначенный клиенту.
- **7.** Запретить пропуск датаграмм с UDP-сообщениями, направленными с или на порты echo и chargen, либо на все порты, кроме используемых (часто используется только порт 53 для службы DNS).
- **8.** Использование TCP Intercept для защиты от атак SYN flood.

Защита: 1. Фильтрация на маршрутизаторе

- 9. Фильтрация TCP-сегментов выполняется в соответствии с политикой безопасности: разрешаются все сервисы, кроме запрещенных, или запрещаются все сервисы, кроме разрешенных (описывая каждый прикладной сервис в главе 3, мы будем обсуждать вопросы фильтрации сегментов применительно к сервису). Если во внутренней сети нет хостов, к которым предполагается доступ из Интернета, но разрешен доступ внутренних хостов в Интернет, то следует запретить пропуск TCP SYN-сегментов, не имеющих флага АСК, из Интернета во внутреннюю сеть1, а также запретить пропуск датаграмм с Fragment Offset=1 и Protocol=6 (TCP).

Защита: 1. Фильтрация на маршрутизаторе

- Отметим, что **более безопасным и управляемым решением**, чем фильтрация того или иного TCP-трафика следующего от или к компьютеру пользователя, **является работа пользователей через прокси-серверы.**

- **Преимущества этого решения следующие.**
- Прокси-сервер находится под контролем администратора предприятия, что позволяет реализовывать различные политики для дифференцированного управления доступом пользователей к сервисам и ресурсам Интернета, фильтрации передаваемых данных (защита от вирусов, цензура и т.п.), кэширования (там, где это применимо).
- С точки зрения Интернета от имени всех пользовательских хостов предприятия действует один прокси-сервер, то есть имеется только один потенциальный объект для атаки из Интернета, а безопасность одного прокси-сервера, управляемого профессионалом, легче обеспечить, чем безопасность множества пользовательских компьютеров.

Защита: 2. Анализ сетевого трафика

- Анализ сетевого трафика проводится для обнаружения атак, предпринятых злоумышленниками, находящимися как в сети организации, так и в Интернете.
- **1.** Сохранять и анализировать статистику работы маршрутизаторов, особенно— частоту срабатывания фильтров.
- **2.** Применять специализированное программное обеспечение для анализа трафика для выявления выполняемых атак (NIDS — Network Intrusion Detection System). Выявлять узлы, занимающие ненормально большую долю полосы пропускания, и другие аномалии в поведении сети.
- **3.** Применять программы типа arpwatch для выявления узлов, использующих нелегальные IP- или MAC-адреса.

- Применять программы типа Antisniff для выявления узлов, находящихся в режиме прослушивания сети.

Защита: 3. Защита маршрутизатора

- **Мероприятия по защите маршрутизатора проводятся с целью предотвращения атак, направленных на нарушение схему маршрутизации датаграмм или на захват маршрутизатора злоумышленником.**
- **1.** Использовать аутентификацию сообщений протоколов маршрутизации с помощью алгоритма MD5.
- **2.** Осуществлять фильтрацию маршрутов, объявляемых сетями-клиентами, провайдером или другими автономными системами. Фильтрация выполняется в соответствии с маршрутной политикой организации; маршруты, не соответствующие политике, игнорируются.
- **3.** Использовать на маршрутизаторе, а также на коммутаторах статическую ARP-таблицу узлов сети организации.
- **4.** Отключить на маршрутизаторе все ненужные сервисы (особенно так называемые «диагностические» или «малые» сервисы TCP: echo, chargen, daytime, discard, и UDP: echo, chargen, discard).
- **5.** Ограничить доступ к маршрутизатору консолью или выделенной рабочей станцией администратора, использовать парольную защиту; не использовать telnet для доступа к маршрутизатору в сети, которая может быть прослушана.
- **6.** Использовать последние версии и обновления программного обеспечения, следить за бюллетенями по безопасности, выпускаемыми производителем.

Защита: 4. Защита хоста

- **Мероприятия по защите хоста проводятся для предотвращения атак, цель которых — перехват данных, отказ в обслуживании, или проникновение злоумышленника в операционную систему.**
- **1.** Запретить обработку ICMP Echo-запросов, направленных на широковещательный адрес.
- **2.** Запретить обработку ICMP-сообщений Redirect, Address Mask Reply, Router Advertisement, Source Quench.
- **3.** Если хосты локальной сети конфигурируются динамически сервером DHCP, использовать на DHCP-сервере таблицу соответствия MAC- и IP-адресов и выдавать хостам заранее определенные IP-адреса.
- **4.** Отключить все ненужные сервисы TCP и UDP (читай: отключить все сервисы, кроме явно необходимых). Под отключением сервиса мы понимаем перевод соответствующего порта из состояния LISTEN в CLOSED.

Защита: 4. Защита хоста

- **5.** Если входящие соединения обслуживаются супердемоном inetd, то использовать оболочки TCP wrappers или заменить inetd на супердемон типа xinetd или tcpserver, позволяющий устанавливать максимальное число одновременных соединений, список разрешенных адресов клиентов, выполнять проверку легальности адреса через DNS и регистрировать соединения в лог-файле.
- **6.** Использовать программу типа tcplog, позволяющую отследить попытки скрытного сканирования (например, полуоткрытыми соединениями).
- **7.** Использовать статическую ARP-таблицу узлов локальной сети.
- **8.** Применять средства безопасности используемых на хосте прикладных сервисов.
- **9.** Использовать последние версии и обновления программного обеспечения, следить за бюллетенями по безопасности, выпускаемыми производителем.

Защита: 5. Превентивное сканирование

- **Администратор сети должен знать и использовать методы и инструменты злоумышленника и проводить превентивное сканирование сети организации для обнаружения слабых мест в безопасности до того, как это сделает злоумышленник.**
- Для этой цели имеется также специальное программное обеспечение — сканеры безопасности, network security scanners, типа Nessus.

Nessus — это один из самых известных и широко используемых сканеров уязвимостей в мире. Разработанный компанией Tenable, Inc., Nessus предоставляет комплексное решение для обнаружения уязвимостей, позволяя организациям и индивидуальным пользователям идентифицировать и устранять потенциальные угрозы безопасности в их сетевой инфраструктуре. С его помощью можно проводить глубокий анализ безопасности, охватывая различные аспекты, от простого обнаружения уязвимостей до сложных проверок на соответствие стандартам безопасности

Уязвимости Wi-Fi и атаки на него

Протоколы обеспечения безопасности Wi-Fi сетей

- **Существует четыре распространенных протокола обеспечения безопасности Wi-Fi сетей:**
- **1. WEP (Wired Equivalent Privacy):** предоставляет базовую защиту данных путем шифрования при помощи алгоритма RC4, но считается уязвимым и устаревшим.
- **2. WPA (Wi-Fi Protected Access):** популярное семейство протоколов, разработанных для замены WEP. WPA обеспечивает более надежное шифрование и аутентификацию, поскольку каждое устройство, подключенное к сети, имеет собственный уникальный ключ для шифрования и дешифрования данных. Протокол включает в себя методы WPA-Personal и WPA-Enterprise.

Протоколы обеспечения безопасности Wi-Fi сетей

- **3. Протокол WPA2** представляет собой улучшенную версию WPA, с использованием AES-шифрования и внедрением сразу нескольких механизмов защиты от атак: 4-way Handshake и Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP).
- **4. WPA3**, в свою очередь, представляет новый стандарт безопасности, совместимый с устройствами, поддерживающими предыдущие версии протоколов. Он предоставляет индивидуальное шифрование каждому устройству, позволяя использовать более безопасные методы установления соединения и защиту от атак перебора паролей.

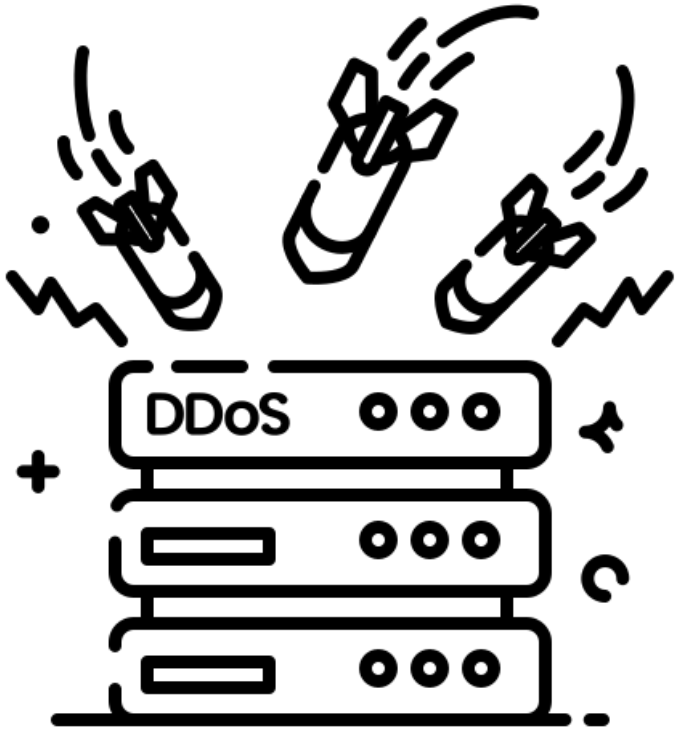
WPA-Personal и WPA-Enterprise

WPA-Personal	**WPA-Enterprise**
Метод предназначен для защиты беспроводных сетей с использованием предварительно согласованного пароля или общего ключа PSK (Pre-Shared Key), который должны знать все устройства и пользователи, чтобы получить доступ к сети.	Вместо PSK здесь используется аутентификация на сервере RADIUS (Remote Authentication Dial-In User Service). Сервер проверяет учетные данные пользователей и управляет всеми процессами централизованно. Снижение рисков компрометации учетных данных происходит благодаря тому, что каждый пользователь имеет свой собственный идентификационный ключ для доступа к сети.
Этот вариант часто используется для обеспечения безопасности Wi-Fi для домашних сетей и небольших офисов.	В основном используется для защиты корпоративных сетей.

WEP

	WEP	WPA	WPA2	WPA3
Основные характеристики	Обеспечение конфиденциальности данных в беспроводной сети на уровне, сравнимом с проводными сетями	Основан на стандарте 802.11i	Функционирует на стандарте 802.11i, но для его работы требуется новое аппаратное ПО, которое обеспечивает более надежную защиту беспроводной сети	Современный стандарт, анонсированный и поддерживаемый Wi-Fi Alliance
Шифрование	RC4	TKIP+RC4	CCMP/AES	GCMP-256
Метод аутентификации	Wep open и Wep shared	WPA-PSK и WPA-Enterprise (WPA-802.1X)	WPA2-Personal WPA2- Enterprise	WPA3-Personal WPA3-Enterprise
Технологии обеспечения целостности данных	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Протоколы аутентификации и обмена ключами	Нет	4-way handshake	4-way handshake	Elliptic Curve DiffieHellman (**ECDH**) exchange and Elliptic Curve Digital Signature Algorithm (**ECDSA**)
Уровень безопасности	□□□	□□□	□□□	□ □ □ □

5. Обзор отдельных видов сетевых атак



5.1. DoS \ DDoS Атаки

Denial of Service «отказ в обслуживании»

Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»

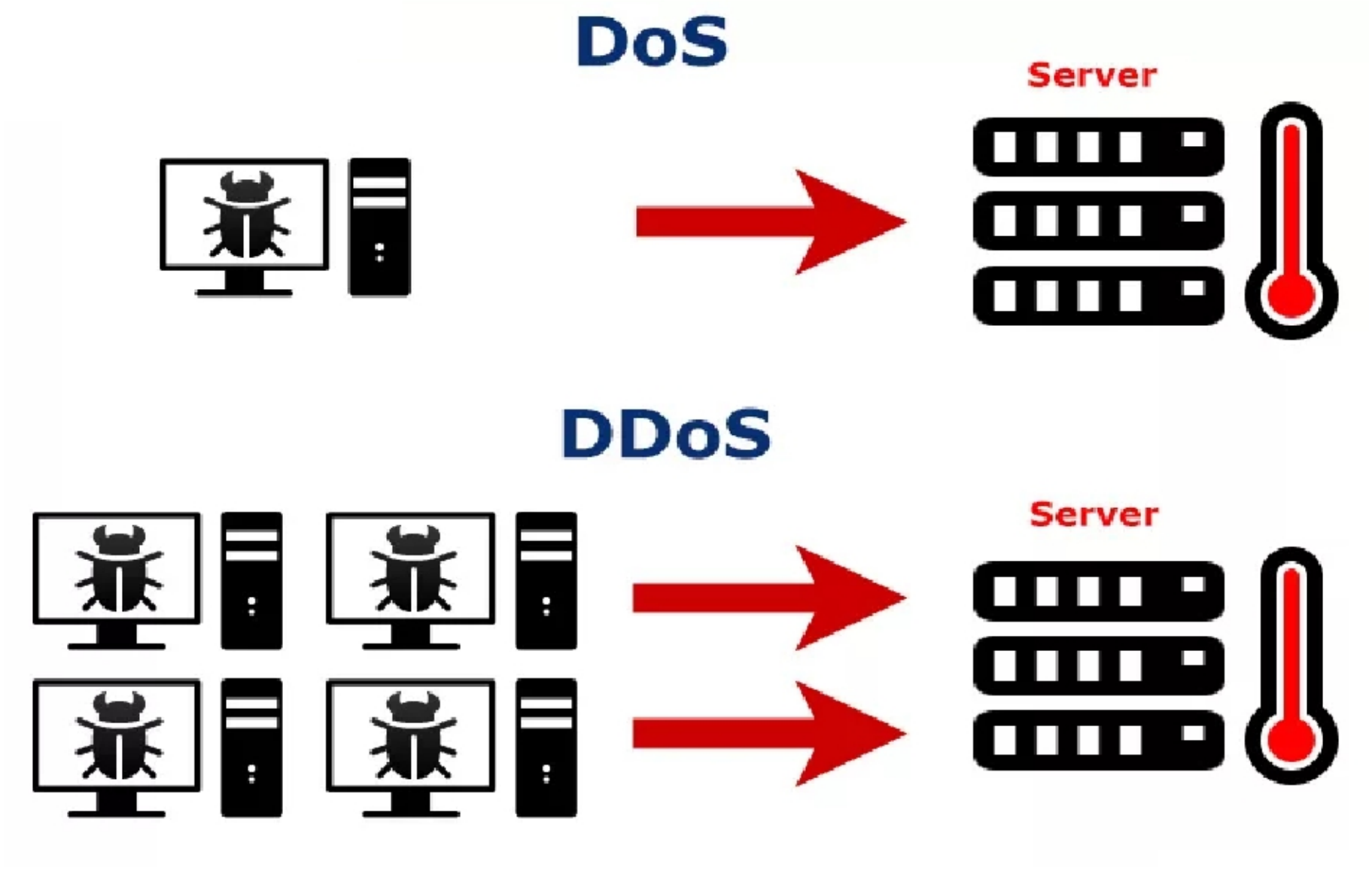
DoS-**атака**

- **DoS (аббр. англ. Denial of Service «отказ в обслуживании»)** —атака на вычислительную систему **с целью довести её до отказа**, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён.
- **Отказ «вражеской» системы может быть и шагом к овладению системой** (если в нештатной ситуации ПО выдаёт какую-либо критическую информацию — например, версию, часть программного кода и т. д.).
- **Но чаще это мера экономического давления**: потеря простой службы, приносящей доход, счета от провайдера и меры по уходу от атаки ощутимо бьют «цель» по карману. **В настоящее время DoS и DDoS-атаки наиболее популярны, так как позволяют довести до отказа практически любую плохо написанную систему, не оставляя юридически значимых улик**.

Классификация DoS-атак

- **Хакерам гораздо легче осуществить DoS-атаку на систему, чем получить полный доступ к ней.**
- Существуют различные причины, из-за которых может возникнуть DoS-условие, то есть такая ситуация, при которой пользователи не могут получить доступ к ресурсам, которые предоставляет сервер, либо доступ к ним существенно затруднен:
  - Насыщение полосы пропускания
  - HTTP-флуд и ping-флуд
  - Smurf-атака (ICMP-флуд)
  - Атака Fraggle (UDP-флуд)
  - Атака с помощью переполнения пакетами SYN (SYN-флуд)

Отличие DoS от DDoS атак



DDoS **атаки (**Distributed Denial of Service)

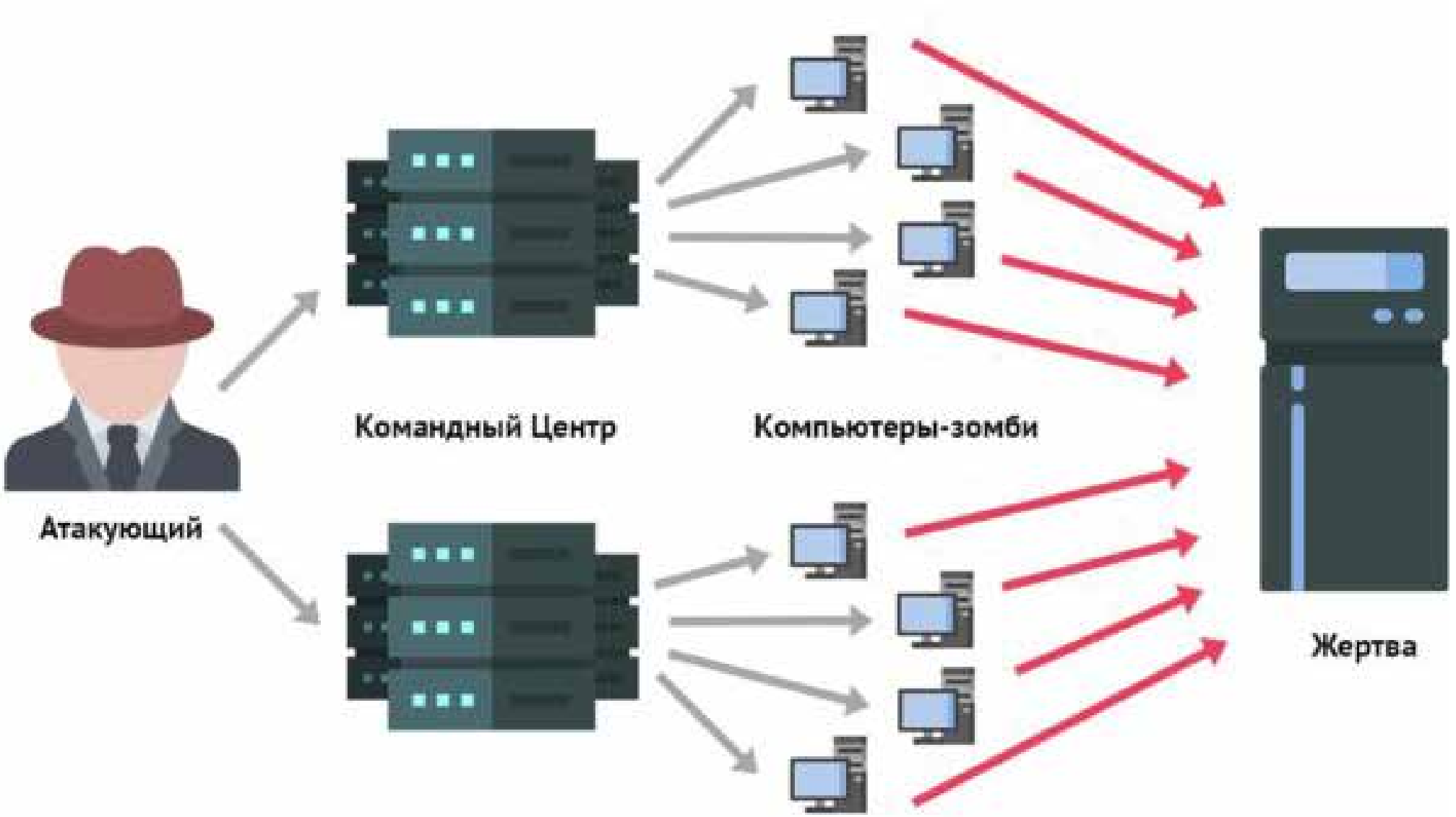
- **DDoS (распределенный отказ в обслуживании)** — атака на компьютерную систему или сетевую службу с целью предотвращения операции путем захвата всех свободных ресурсов, осуществляемой одновременно со многих компьютеров (например, зомби).
- **DDoS-атака — это тип DoS-атаки, которая включает в себя атаку жертвы из нескольких мест одновременно.**
- Компьютеры чаще всего используются для проведения атаки, над которой они взяли управление, используя специальное программное обеспечение (различные типы так называемых ботов и троянов). По заданному сигналу компьютеры одновременно атакуют систему жертвы, наводняя ее ложными попытками использовать предлагаемые услуги.
- Для каждого такого вызова атакованный компьютер должен выделять некоторые ресурсы (память , процессорное время, пропускную способность сети), что при очень большом количестве запросов приводит к истощению доступных ресурсов и, как следствие, к сбою в работе или даже к системному сбоям.

DDoS-**атаки — Layer 3 и Layer 7** OSI

- **Основные типы DDoS-атак — Layer 3 и Layer 7**. Они названы так в соответствии с уровнями сетевой модели OSI, на которых выполняются.
- **Layer 3 DDoS нацелен на сетевое оборудование и соединения.** В ходе атаки создаётся огромный паразитный трафик, например, с помощью SYN-пакетов (syn-flood). Этот трафик забивает канал связи и блокирует прохождение легитимных пакетов. В настоящее время большинство крупных хостинг-провайдеров и дата-центров сегодня хорошо защищены от атак Layer 3, поэтому в этом посте мы сосредоточимся на другой разновидности атак, противостоять которой несколько сложнее.
- **DDoS-атаки Layer 7 нацелены непосредственно на приложения, которые работают на сервере.** Цель здесь — не отключить сеть, а добиться остановки приложения или даже сервера путём перегрузки его штатными прикладными запросами. Это приводит к нехватке ресурсов процессора, оперативной памяти или и того и другого и фактически останавливает работу.

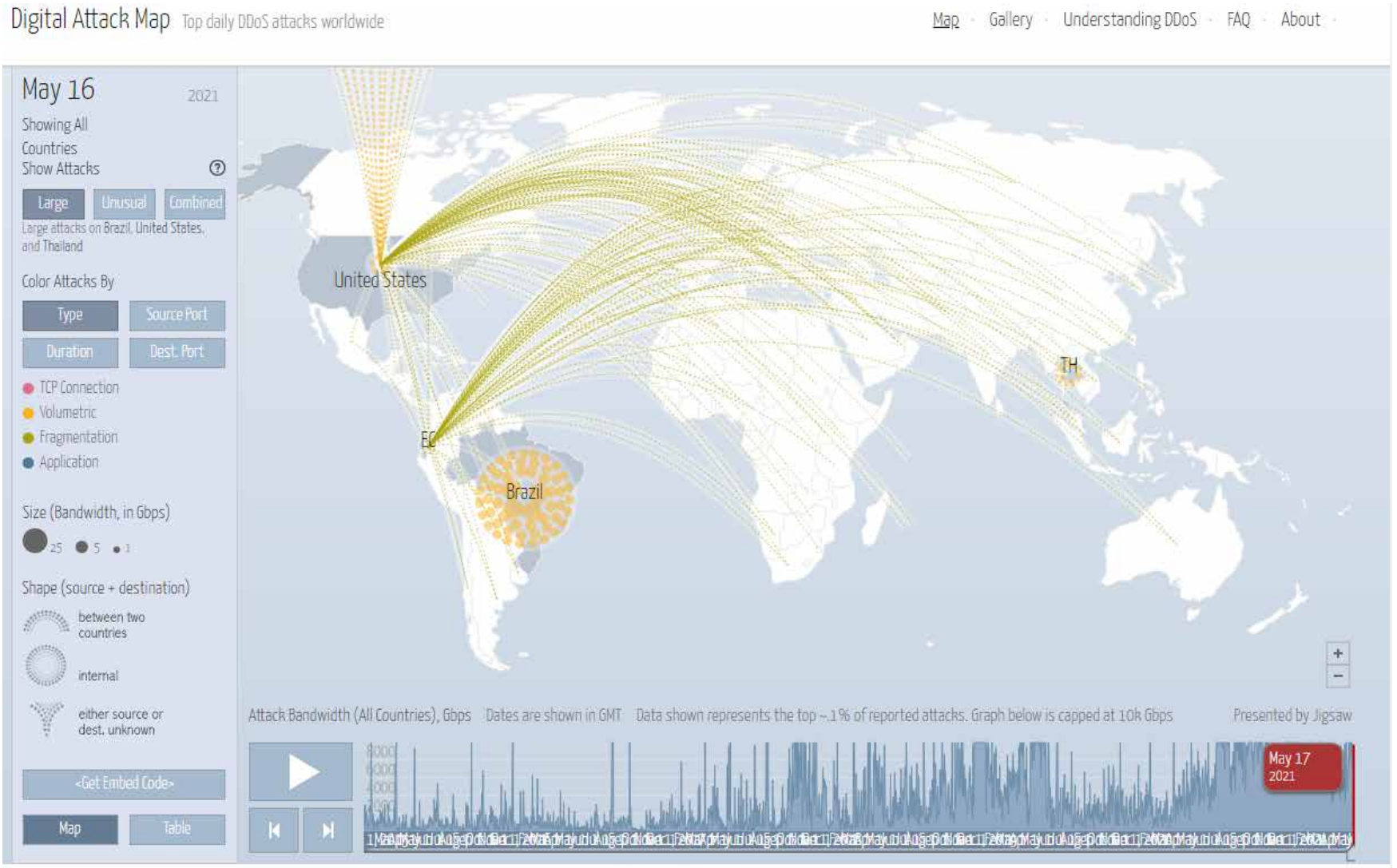
Архитектура DDoS-Атаки

Архитектура DDoS-Атаки



Карта DDoS-атак в реальном времени

https://www.digitalattackmap.com/



Виды DDoS атак

- **ICMP-флуд (Smurf-атака).** В этом случае по широковещательному адресу злоумышленник отправляет поддельный ICMP-пакет, в котором адрес атакующего меняется на адрес жертвы. Все узлы присылают ответ на данный ping-запрос.
- **UDP-флуд.** Этот вид атак использует UDP-протокол. Его характерные особенности — отсутствие необходимости в установлении сессии и отправки какого-либо ответа. На случайные порты хост-машины приходит бесчисленное количество пакетов, принуждая постоянно проверять, слушает ли данный порт какое-то приложение, и в случае ошибки возвращать пакет «ICMP Destination Unreachable». Естественно, такая активность поглощает ресурсы хост-машины, приводя к ее недоступности.

Виды DDoS атак

- **SYN-флуд.** Данный вид атаки основан на попытке запуска большого числа одновременных TCP-соединений через посылку SYN-пакета с несуществующим обратным адресом. После нескольких попыток отослать в ответ АСК-пакет на недоступный адрес большинство операционных систем ставят неустановленное соединение в очередь. И только после п-ой попытки закрывают соединение. Поскольку поток АС К-пакетов очень большой, вскоре очередь оказывается заполненной, и ядро отказывает в попытках открыть новое соединение.
- **HTTP-флуд.** В этом случае атакующий отсылает небольшие HTTP-пакеты, которые заставляют в свою очередь отвечать сервер пакетами, размеры которых значительно больше. Тем самым злоумышленник имеет большой шанс насытить полосу пропускания жертвы и вызвать отказ в работе сервисов.

Виды DDoS атак

- **Отраженная DDoS-атака с усилением.** Эта атака основана на транспортном протоколе UDP. который активно используется многими важными интернет-сервисами, в частности DNS (всем известный Domain Name Service) и NTP (менее известный Network Time Protocol), хотя сегодня уже ведутся атаки и с помощью сервисов потокового вещания. Самое главное в этом случае, что нет «рукопожатия», т.е. сервис «не проверяет» адрес отправителя. Другими словами, кто угодно может послать U DP-пакет от чьего угодно имени (I P-адреса). Соответственно, атакующий посылает UDP-пакет на сервис (обычно DNS или NTP) от имени жертвы (с ее IP-адреса) и сервис отвечает не на IP-адрес атакующего, а на IP-адрес жертвы. Вот почему и название у атаки — «отражение». Но этого недостаточно для успешной DDoS-атаки. В названии присутствует еще слово «усиление». В данном случае у DNS- и NTP-служб есть приятная для атакующего особенность — множитель. Это выглядит следующим образом: атакующий от имени жертвы отправляет на DNS-или NTP-сервер пакет размером 1 кбайт, а DNS-или NTP-сервер отвечает на адрес жертвы пакетом в n-раз больше. Вот это и есть то самое усиление, о котором было сказано в самом начале. Отсюда и название «усиленная отраженная DDoS-атака».

Виды DDoS атак

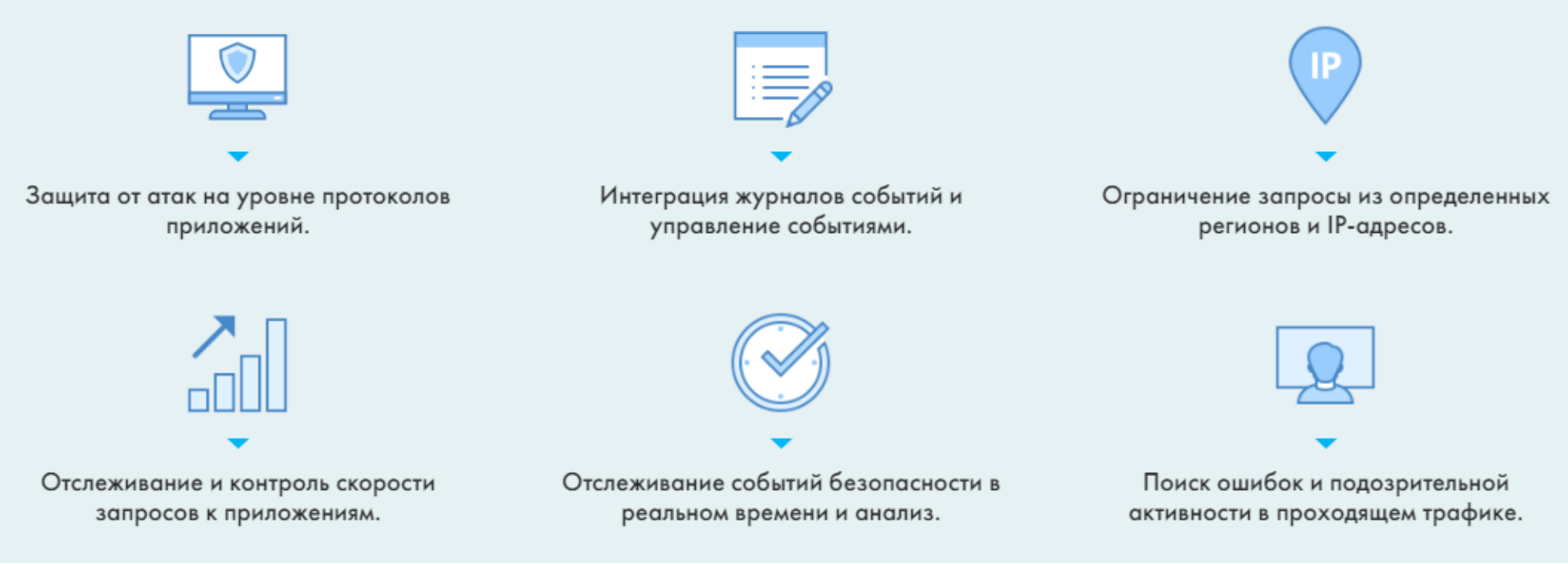
- **Slow HTTP Post.** Атака заключается в отправке серверу большого HTTP POST-запроса маленькими частями (по 1 байту). По стандарту HTTP-сервер должен дождаться полной передачи данных (получив содержимое размером 1 байт) и может закрывать соединение только по таймауту. Таким образом, в случае подобной DDoS-атаки медленными соединениями атакуемый сервер открывает огромное количество соединений, катастрофически расходуя свои ресурсы.
- **Slow HTTP headers.** Эта атака аналогична методу Slow HTTP Post, только вместо пост-запроса используется медленная отправка заголовка HTTP. Как и при атаке методом Slow Post, сервер ждет окончания заголовков, прежде чем закрыть соединение, что приводит к большому количеству открытых соединений и как следствие — к перегрузке сервера. Подобные DDoS-атаки сложно отличить от обычных запросов с медленным соединением.

Виды DDoS атак

- **Фальшивые Googlehots.** Это сравнительно новая технология совершения DDoS-атак. Ее особенностью является использование ботов, маскирующихся под Googlebots — роботов поисковой системы Google, которые отслеживают появление и обновление web-страниц для индексации сайтов в поисковых системах.

Защита от DDoS-атак

- Защита от **DDoS**-атак работает с использованием алгоритмов и передового программного обеспечения для отслеживания входящего трафика на веб-сайт. Любому незаконному трафику отказывается в доступе, в то время как законный трафик продолжает фильтроваться на сайт.



Защита от DDoS-атак

- **Cloud Flare** — фильтрует трафик прежде, чем он попадает на сайт, имеет инструментарий для экстренной зашиты от DDoS-атак, имеет бесплатную версию; https://www.cloudflare.com

- **Kaspersky DDoS Prevention** — использует методы статистического, поведенческого и экспертного анализа; https://www.kaspersky.ru/enterprise-security/ddos-protection

- **Arbor**— позволяет конфигурировать систему защиты в зависимости от потребностей, обеспечивая тем самым комплексный подход к защите от атак, имеет дружественный интерфейс, что позволяет комфортно и продуктивно работать администратору безопасности. https://www.netscout.com/arbor-ddos

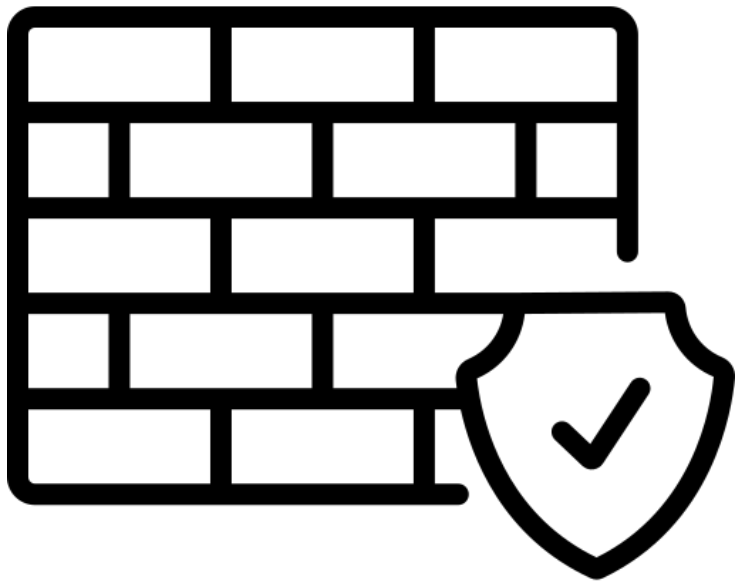
- **FortiDDoS** - Расширенная защита от Fortinet для корпоративных центров обработки данных. Включает контроль тысяч параметров, защиту от всех DDoS-атак с учетом приложений и управлением трафиком. https://www.fortinet.com/ru/products/ddos/fortiddos

Защита от DDoS-атак

- **Check Point DDoS Protector** - Защита от DDoS-атак нулевого дня с блокировкой широкого спектра атак. Наличие локальных и облачных решений для смягчения последствий. Аппаратные механизмы SSL (проверка стандартов SSL / TLS). https://www.checkpoint.com/ru/products/ddos-protector/

- **Cisco DDoS Protection Solution** - Обнаруживает аномалий трафика и отбрасывает аномальные пакеты. Обеспечивает доступность сети и непрерывность бизнеса. Осуществляет возврат чистого трафика в сеть клиента и работает в режиме реального времени. https://www.cisco.com/c/en/us/products/security/secure-ddos-protection/index.html

- **Imperva Incapsula** - Использует многоуровневый подход к блокировке DDoS-трафика. Фильтрует трафик через брандмауэр веб-приложений, механизм правил DDoS и ряд прогрессивных проблем, которые невидимы для легитимного трафика. https://www.imperva.com



6. Программно-аппаратные средства защиты компьютерных систем

6. Программно-аппаратные средства защиты компьютерных систем

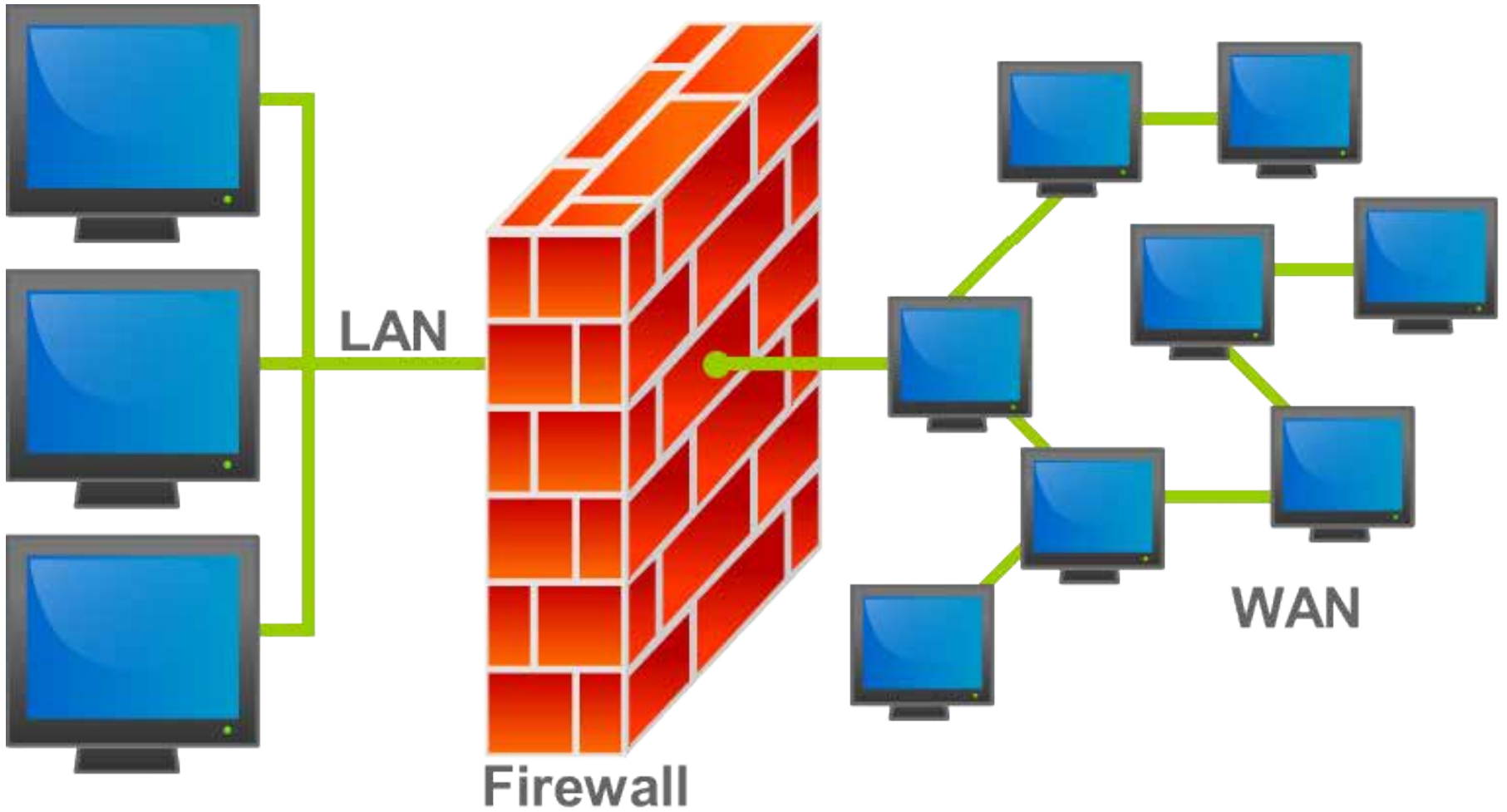
6.1. Межсетевые экраны (Firewall)

Межсетевой экран

- **Межсетевой экран (МСЭ), сетевой экран (СЭ)** — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

- Другие названия:
  - **Брандмауэр** (нем. **Brandmauer** — противопожарная стена) — заимствованный из немецкого языка термин;
  - **Файрвол** (англ. **Firewall** — противопожарная стена) — заимствованный из английского языка термин.

Межсетевой экран (Firewall)



Межсетевой экран на границе сетевого периметра.

Межсетевые экраны (Firewall)

- **Межсетевое экранирование** повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым обеспечивая все составляющие ИБ. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.
- **Функции экранирования выполняет межсетевой экран, или брандмауэр (firewall),** под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в ИС и/или выходящих из нее, и обеспечивает защиту ИС посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны (Firewall)

- Межсетевые экраны **классифицируются** по следующим признакам:
  - **по месту расположения в сети** — на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;
  - **по уровню фильтрации**, соответствующему эталонной модели OSI.

- Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет.
- Внутренние сетевые экраны могут поддерживать несколько протоколов.

Межсетевые экраны (Firewall)

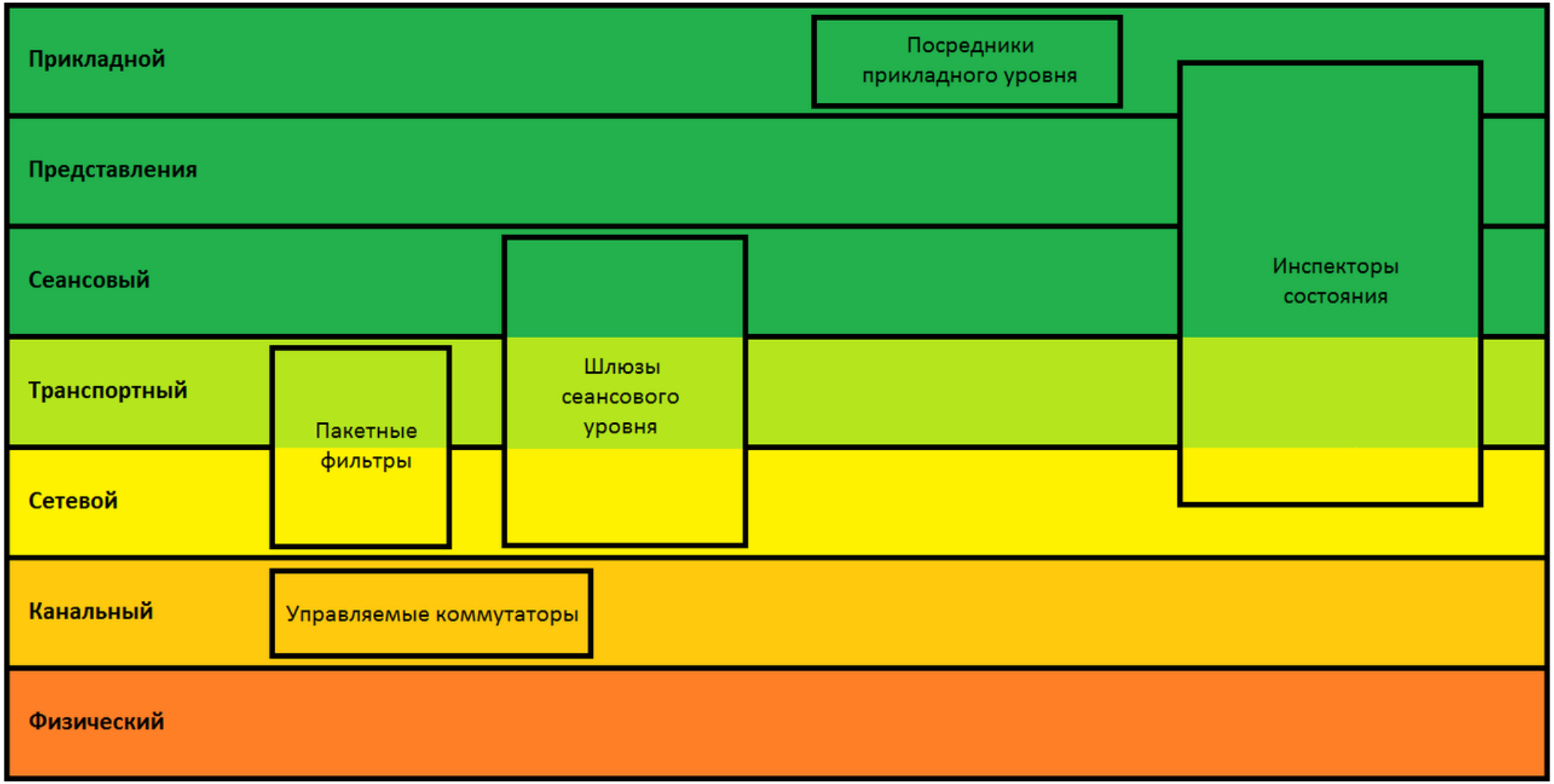
- Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI. Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

- **Межсетевые экраны разделяют на четыре типа:**
  - межсетевые экраны с фильтрацией пакетов;
  - шлюзы сеансового уровня;
  - шлюзы прикладного уровня;
  - межсетевые экраны экспертного уровня.

Типы межсетевых экранов и уровни модели OSI

№	Уровень модели OSI	Протокол	Тип межсетевого экрана
1	Прикладной	Telnet, FTP, DNS, NFS, SMTP, HTTP	Шлюз прикладного уровня. Межсетевой экран экспертного уровня.
2	Представления данных	—	—
3	Сеансовый	TCP, UDP	Шлюз сеансового уровня
4	Транспортный	TCP, UDP	—
5	Сетевой	IP, ICMP	Межсетевой экран с фильтрацией пакетов
6	Канальный	ARP, RAP	—
7	Физический	Ethernet	—

Типы межсетевых экранов и уровни модели OSI



Схематическое изображение классификации межсетевых экранов на основе сетевой модели OSI

Межсетевые экраны (Firewall)

- **Межсетевые экраны с фильтрацией пакетов** представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их со сконфигурированной таблицей правил. Эти межсетевые экраны просты в использовании, дешевы, оказывают минимальное влияние на производительность вычислительной системы. Основным недостатком является их уязвимость при подмене IP-адресов. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

Межсетевые экраны (Firewall)

- **Шлюзы сеансового уровня** контролируют допустимость сеанса связи. Они следят за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т.е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функцию трансляции сетевых адресов, которая скрывает внутренние IP-адреса, тем самым исключая подмену IP-адреса. Однако в таких межсетевых экранах отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

Межсетевые экраны (Firewall)

- **Шлюзы прикладного уровня** проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип межсетевого экрана, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб сети Интернет (HTTP, FTP, Telnet и т.д.) и служат для проверки сетевых пакетов на наличие достоверных данных.
- Описываемые шлюзы снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно при работе в Интернет при работе по низкоскоростным каналам, но существенно при работе во внутренней сети.

Межсетевые экраны (Firewall)

- **Межсетевые экраны экспертного уровня** сочетают в себе элементы всех трех описанных ранее категорий. Как и межсетевые экраны с фильтрацией пакетов, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Рассматриваемые экраны также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И, наконец, брандмауэры экспертного уровня берут на себя функции шлюза прикладного уровня, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.
- Вместо применения связанных с приложениями программ-посредников брандмауэры экспертного уровня используют специальные алгоритмы распознавания и обработки данных на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами данных, что теоретически должно обеспечить более эффективную фильтрацию пакетов.

Типы межсетевых экранов

- **Типы межсетевых экранов**
  - Межсетевой экран на прокси-сервере
  - Межсетевой экран с контролем состояния сеансов
  - Межсетевой экран нового поколения (NGFW) next-generation firewall
  - NGFW с активной защитой от угроз

Типы межсетевых экранов (Firewall)

- **Межсетевой экран на прокси-сервере**
- **Межсетевой экран на прокси-сервере служит шлюзом между сетями для конкретного приложения**. Прокси-серверы могут выполнять дополнительные функции, например кеширование контента и его защиту путем предотвращения прямых подключений из-за пределов сети. Однако это может отрицательно сказаться на пропускной способности и производительности поддерживаемых приложений.

Типы межсетевых экранов (Firewall)

- **Межсетевой экран с контролем состояния сеансов**
- **Сегодня Firewall с контролем состояния сеансов считается «традиционным».** Он пропускает или блокирует трафик с учетом состояния, порта и протокола. Он отслеживает все действия с момента открытия соединения до его закрытия. Решения о фильтрации принимаются на основании как правил, определяемых администратором, так и контекста. Под контекстом понимается информация, полученная из предыдущих соединений и пакетов, принадлежащих данному соединению.

Традиционные межсетевые экраны

Типы межсетевых экранов (Firewall)

- **Межсетевой экран нового поколения (NGFW)**
- Современные межсетевые экраны не ограничиваются фильтрацией пакетов и контролем за состоянием сеансов. Большинство компаний внедряет межсетевые экраны нового поколения, чтобы противостоять современным угрозам, таким как сложное вредоносное ПО и атаки на уровне приложений.
- **Согласно определению компании Gartner, межсетевой экран нового поколения должен иметь:**
  - Возможности стандартных межсетевых экранов, такие как контроль состояния.
  - Встроенные средства предотвращения вторжений.
  - Средства контроля работы приложений и возможность управления ими для поиска и блокирования небезопасных приложений.
  - Возможности обновления для включения будущих информационных каналов.
  - Средства защиты от постоянно возникающих новых угроз безопасности.
  - Эти возможности постепенно становятся стандартными для большинства компаний, но межсетевые экраны нового поколения способны на большее.

Типы межсетевых экранов (Firewall)

- **NGFW с активной защитой от угроз**
- Эти межсетевые экраны сочетают в себе функции традиционного NGFW с возможностями обнаружения и нейтрализации сложных угроз.
- Межсетевые экраны нового поколения с активной защитой от угроз позволяют:
  - **Определять наиболее подверженные риску ресурсы** благодаря учету всего контекста
  - **Быстро реагировать на атаки** благодаря интеллектуальным средствам автоматизации функций безопасности, которые устанавливают политики и укрепляют защиту в динамическом режиме
  - **Более надежно выявлять отвлекающую или подозрительную деятельность**, применяя корреляцию событий в сети и на оконечных устройствах
  - **Значительно сократить время с момента обнаружения до нейтрализации** благодаря использованию ретроспективных средств обеспечения безопасности, которые осуществляют непрерывный мониторинг для выявления подозрительной деятельности и поведения даже после первоначальной проверки
  - **Упростить администрирование и снизить уровень сложности** с помощью унифицированных политик, обеспечивающих защиту на протяжении всего жизненного цикла атаки

Традиционный Firewall VS NGFW

TRADITIONAL FIREWALL VS NGFW

ТРАДИЦИОННЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ

Контролируют входящий и исходящий трафик на основе сконфигурированных правил

Поддерживают VPN

NGFW (NEXT GENERATION FIREWALL)

Все функции традиционных МСЭ

Интегрированная система предотвращения вторжений (IPS)

Расширенная защита от угроз (ATP)

Управление приложениями

Веб-фильтрация

Антивирус и антиспам

Песочница (опционально)

Обычные межсетевые экраны не видят угроз: большинство атак идет через разрешенные сетевые подключения (http, smtp, tcp и др.)

ПЕСОЧНИЦА: ЕЩЕ ОДИН УРОВЕНЬ ЗАЩИТЫ

К NGFW можно подключить песочницу (локально или в облаке) и проверять подозрительные файлы, чтобы защититься от целевых кибератак (APT)

ЭТАПЫ РАБОТЫ С ФАЙЛАМИ

1. ОТКРЫТЬ ФАЙЛ В БЕЗОПАСНОЙ СРЕДЕ
2. ОТСЛЕДИТЬ АКТИВНОСТЬ (ИЗМЕНЕНИЯ В РЕЕСТРЕ, ЗАПУСК СИСТЕМНЫХ ПРОЦЕССОВ И Т.Д.)
3. ЗАБЛОКИРОВАТЬ ИЛИ ДОПУСТИТЬ К ИСПОЛЬЗОВАНИЮ

МИФЫ И ЗАБЛУЖДЕНИЯ

У нас уже есть межсетевой экран, NGFW нам не нужен

Современная практика показывает, что блокировки на уровне протоколов и портов недостаточно. Портовые сканнеры легко обходятся, туннелирование и шифрование – за пределами действия обычного межсетевого экрана.

Антивирус нам поможет и заблокирует угрозы

Обычные антивирусы не справляются с изменчивостью вирусов и потоком свыше 10Гбит/сек. И реагируют не сразу: шифровальщики успеют зашифровать данные. Нужны и другие средства защиты, например, песочница.

Мы надежно защищаем периметр, враг не пройдет

Пользователи перемещаются, атака может идти через облачные приложения или анонимайзеры, через вложения в почте или мессенджерах, полученные даже от коллег. Трафик надо проверять в песочнице, чтобы уберечься от целевых атак.

Аппаратные межсетевые экраны Cisco

Межсетевой экран как главный элемент платформы безопасности

Выберите свой межсетевой экран

Firepower серии 1000

Для малого и среднего бизнеса, а также филиалов. Упрощенное управление с помощью Cisco Defense Orchestrator экономит время на администрирование, следовательно, у вас остается больше времени на развитие бизнеса.

Firepower серии 2100

Для крупных филиалов, коммерческих и промышленных предприятий. Выберите вариант управления, который соответствует вашей среде и рабочим процессам.

Firepower серии 4100

Для крупных комплексов зданий и центров обработки данных: создание логических межсетевых экранов для гибкого развертывания, анализ зашифрованного веб-трафика, защита от DDoS-атак, кластеризация устройств для повышения производительности и обеспечения высокой доступности, масштабирование VPN, блокировка сетевых вторжений и многое другое.

Firepower 9300

Для поставщиков услуг и высокопроизводительных центров обработки данных: эта модульная платформа операторского класса позволяет создавать отдельные логические межсетевые экраны и масштабируемые VPN, анализировать зашифрованный веб-трафик, защищаться от DDoS-атак, группировать устройства в кластеры для повышения производительности и обеспечения высокой доступности, блокировать сетевые вторжения и многое другое.

Аппаратные межсетевые экраны Cisco

Многофункциональное устройство обеспечения безопасности Cisco 5500-X с сервисами FirePOWER

Блокируйте больше угроз с помощью ориентированного на устранение угроз межсетевого экрана нового поколения серии 5500-X

Непревзойденный уровень защиты позволяет отражать кибератаки повышенной сложности. Мы предлагаем первый в отрасли межсетевой экран нового поколения с активной защитой от угроз – Cisco ASA 5500-X.

Смотреть демонстрацию | Сравнить нас с другими

Показать 3D-модель | Дополнения для МСЭ нового поколения в 3D

https://www.cisco.com/c/ru_ru/products/security/asa-firepower-services/index.html

Межсетевой экран следующего поколения (Next-Generation Firewall, NGFW)

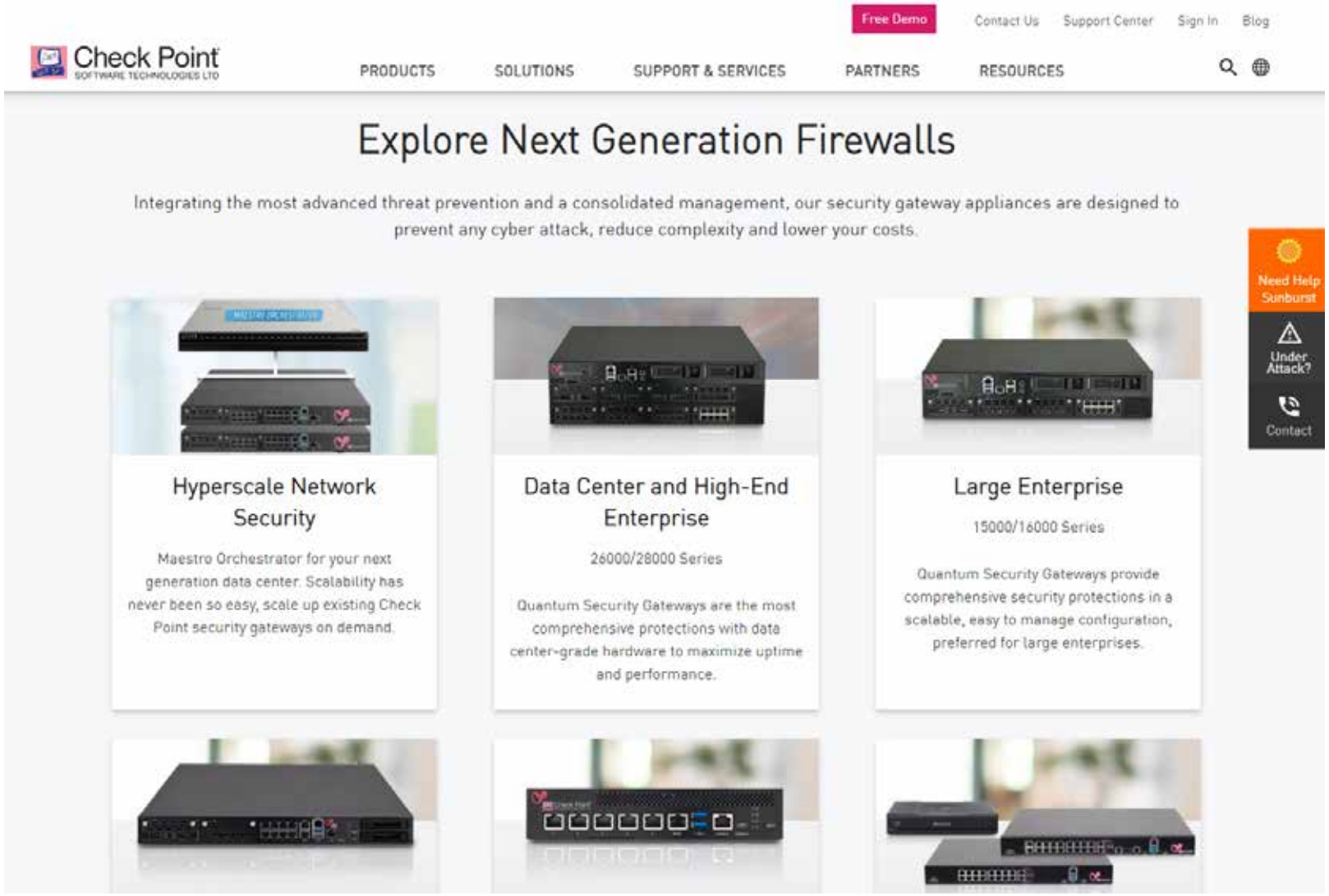
Check Point NGFW

Check Point обеспечивают превосходную безопасность за пределами любого межсетевого экрана следующего поколения (NGFW). Эти шлюзы разработаны для защиты сети Sandblast, и являются лучшими в предотвращении кибератак нового поколения с помощью более 60 инновационных служб безопасности. Обеспечивает производительность по предотвращению угроз до 1,5 Тбит/с и может масштабироваться.

ForcePoint NGFW

Устройства Forcepoint NGFW основаны на унифицированном ядре и предоставляют согласованные возможности управления в центрах обработки данных, на периферии, в филиалах и в облаке. Обеспечивается эффективность, доступность и безопасность с широким спектром встроенных (без дополнительных лицензий или установки) функций безопасности, включая: VPN, IPS, защиту от уклонений, зашифрованную проверку, SD-WAN и прокси.

Межсетевой экран следующего поколения (Next-Generation Firewall, NGFW)



https://www.checkpoint.com/quantum/next-generation-firewall/#

Межсетевой экран следующего поколения (Next-Generation Firewall, NGFW)

Cisco Firepower NGFW

Cisco Talos постоянно анализирует данные об угрозах и создает меры защиты, которые межсетевой экран Cisco нового поколения использует для автоматического предотвращения нарушений. Автоматизация процессов для экономии времени и упрощения среды. И контроль для быстрого обнаружения и блокировки угроз.

Palo Alto Networks NGFW

Первый в мире NGFW на базе машинного обучения. Обеспечьте безопасность вашей сети с помощью тесно интегрированных инноваций, эффективных действий за счет автоматизации и аналитики. Межсетевой экран Palo Alto обеспечивает постоянную безопасность с полной видимостью.

Gartner. **Магический квадрат по межсетевым экранам**

Source: Gartner (November 2020)

"Completeness of Vision" ("Полнота Видения" - очень плохой перевод, но лучше не получается). Это когда аналитики Gartner оценивают вендоров по их возможностям убедительно формулировать утверждения о текущих и будущих потребностях рынка, инновациях и возможных конкурентных силах. Обычно это ось "X".

"Ability to Execute" ("Возможность Исполнения) – оценка по качеству и эффективности процессов, систем, методов и процедур, которые в итоге обеспечивают вендору конкурентоспособность и положительно влияют на доходы. Ось "Y".

Gartner. **Магический квадрат по межсетевым экранам**

- **Полнота видения (Completeness of Vision):**
  - **Понимание рынка (Market Understanding)** – способность вендора понимать потребности клиентов и транслировать это в продукте.
  - **Маркетинговая стратегия (Marketing Strategy)** – чёткие и понятные формулировки маркетинговых посланий.
  - **Стратегия продаж (Sales Strategy)** – стратегия продаж продуктов, обеспечиваемая налаженной сетью прямых и косвенных продаж.
  - **Предлагаемая стратегия для продукта (Offering (Product) Strategy)** – подход вендора к разработке продукта, обеспечивающий потребности рынка.
  - **Бизнес-модель (Business Model)** – обоснованность и логичность бизнес-предложения вендора.
  - **Стратегия для отдельных сегментов рынка (Vertical/Industry Strategy)** – стратегия вендора по удовлетворению потребностей отдельных сегментов рынка. Включая вообще способность внятно сегментировать эти рынки.
  - **Инновации (Innovation)** – Одно из самых трудных для понимания российскими читателями место (слово "инновации" безнадежно испорчено). Но тут всё проще, ибо пункт специализирован: что конкретно делает вендор для удовлетворения будущих требований инфраструктуры на уровне доступа. В том числе с точки зрения более тесной интеграции с проводными сетевыми продуктами, а также поддержки сетевых сервисов "голос, видео и приложений" (далее - ГВП, или на английском - VVA - Voice/Video/Apps)? Существует ли что-то новое в этих предложениях? Что делается для удовлетворения потребностей клиентов по упрощению установки и/или развёртывания инфраструктуры и последующей эксплуатации/управления? И если вендор смог успешно это всё объяснить с горизонтом планирования от двух до пяти лет, то оценка в критерии "инновационность" повышается.
  - **Географическая стратегия (Geographic Strategy)** – стратегия вендора по захвату мирового господства по удовлетворению потребностей в географических регионах за пределами "домашнего региона/страны".

Gartner. **Магический квадрат по межсетевым экранам**

- **"Возможность исполнить" (Ability to Execute)** - и этот раздел отличается от стандартного отчёта, поскольку проводится довольно глубокий анализ, привязанный к отрасли, которая, напомню, про "сетевое оборудование":
  - **Продукт/Услуга (Product/Service)** – здесь Gartner оценивает поставщиков с точки зрения полноты своих продуктов для строительства инфраструктуры доступа, которая в идеале должна состоять из всей линейки устройств: коммутаторы, маршрутизаторы, точки доступа и связанных с ними компонентов – внешние антенны, наружные/внутренние шкафы, кейсы и т.п. Всё это необходимо для оценки способности вендора комплексно решать задачи клиентов на различных вертикальных рынках. В данном отчете Gartner решил уделить особое внимание различным сетевым приложениям, таким как управление, мониторинг, гостевой доступ, управление политиками доступа, сервисы определения местоположения, сетевая аналитика и приложения безопасности. Отчёт довольно серьезно относится к действующим вендорским стратегиям по сегментации предлагаемых продуктов и стратегии архитектурной миграции из унаследованных систем. Причём, как внутри линеек вендорских решений, так и миграция с/на других поставщиков. Кроме того, рассматривается возможности обслуживания и развёртывания в глобальном пространстве реализации проектов с участием сторонних производителей и/или компаний интеграторов и OEM-поставщиков.
  - **Жизнеспособность (Overall Viability)** – оценка финансового состояния вендора в целом. А ещё – возможность инвестиций в развитие и текущую разработку продуктов.
  - **Продажи/Ценообразование (Sales Execution/Pricing)** – эффективность каналов продаж, ценообразование и возможности договорных процессов.
  - **Отзывчивость к требованиям рынка/История реакций на предыдущие требования (Market Responsiveness and Track Record)** – способность реагировать на требования рынка для достижения конкурентного успеха и обеспечения потребностей клиентов. Параметр включает в себя историю реагирования на предыдущие требования.
  - **Маркетинг (Marketing Execution)** – эффективность маркетинговых каналов, позитивная идентификация продуктов. В данном случае оценка была сфокусирована на том, насколько хорошо поставщик инфраструктуры уровня доступа мог влиять на рынок "рядом". Например, на поставщиков чипсетов или платформ. Учитывалось участие в консорциумах и влиянии вендора на разработку отраслевых стандартов.
  - **Клиентский опыт (Customer Experience)** – истории успеха клиентов, использующих продукт. Включая опыт по предпродажной подготовке проектов и организацию технической поддержки.

Gartner. **Магический квадрат по межсетевым экранам**

- **И все квадранты можно совершенно четко позиционировать по группам:**
  - **ЛИДЕРЫ (Leaders)** – это когда вендор имеет широчайшую "полноту видения" при неоспоримой "возможности исполнить". То есть, вендор в целом соответствует функциональным требованиям рынка, имеет лояльную клиентскую базу, показывает стабильный рост выручки и/или доли рынка. У вендора имеется приличный портфель продуктов без существенных проблем с интеграцией и поддержкой. Лидеры обеспечивают своевременную реализацию потребностей рынка и имеют инновационный подход. В общем: "есть желания и они совпадают с возможностями".
  - **ПРЕТЕНДЕНТЫ (Challengers)** – компании, по праву занимающие существенную долю рынка и способные делать крупные инсталляции. У них очень высокая "возможность исполнить", но низкая "полнота видения". Такие компании, как правило, концентрируют усилия на модернизации модельного ряда и внутренней интеграции архитектур и наборов функций для серьёзной конкуренции с лидерами рынка, но не производят чего-то действительно нового и свежего. Это когда: "возможности широки, но нет желания".
  - **ВИЗИОНЕРЫ (Visionaries)** – те самые "живопырки", которые не дают спокойно спать "жирным котам". Компании-визионеры имеют существенную продуктовую линейку, но портфель решений находится в стадии разработки. Имеют меньшее соответствие требованиям раздела "возможность исполнить" (в отличие от Лидеров), что связано с новизной решений, которая влечет дополнительные риски и снижает финансовую прочность. "Желания огромны, но нет возможности".
  - **Нишевые игроки (Niche Players)** – производители, которые не демонстрируют выдающихся результатов. Разумеется, это самая многочисленная группа, но при этом не нужно думать, что это что-то плохое. Само попадание в отчет Gartner - уже честь для производителя. А то, что коротко это положение называется "нет ни желания, ни возможностей", то это только потому, что требования у Gartner очень высокие. Очень.

Gartner. **Магический квадрат по межсетевым экранам**

Source: Gartner (November 2020)

"Completeness of Vision" ("Полнота Видения" - очень плохой перевод, но лучше не получается). Это когда аналитики Gartner оценивают вендоров по их возможностям убедительно формулировать утверждения о текущих и будущих потребностях рынка, инновациях и возможных конкурентных силах. Обычно это ось "X".

"Ability to Execute" ("Возможность Исполнения) – оценка по качеству и эффективности процессов, систем, методов и процедур, которые в итоге обеспечивают вендору конкурентоспособность и положительно влияют на доходы. Ось "Y".

Check Point Software Technologies

- **Check Point Software Technologies** - израильский вендор. По итогам 2020 года он является одним из лидеров Magic Quadrant.
- **Преимущества**:
  - Централизованное управление. Разработчики стремятся создать единую платформу для управления всеми своими продуктами. Smart Console постоянно улучшается и получает все больше опций. Также уже сейчас доступны порталы управления (например Smart1-Cloud).
  - Удобная работа с политиками безопасности.
  - Развитие современных направлений по защите ресурсов в облаке. (CloudGuardDome9, CloudGuard Workload и прочие сервисы для управления).
  - Глубокая инспекция трафика. В части Threat Prevention (блейды безопасности Check Point) постоянно улучшается режим распознавания и расследования инцидентов. Для активной работы пользователей с документами предлагаются проприетарные блейды Threat Emulation (песочница), Threat Extraction (извлечение активных элементов из документов).

Fortinet

- **Fortinet** - Американская компания, которая специализируется на разработке и продвижении программного обеспечения, решений и сервисов в области информационной безопасности: межсетевых экранов, антивирусных программ, систем предотвращения вторжений и обеспечения безопасности конечных точек и других продуктов. По итогам 2020 года является одним из лидеров Magic Quadrant в части NGFW.
- **Преимущества**:
  - Вендор является одним из лидеров в части полной поддержки SD-WAN технологии для файрволлов. Fortinet Fabric Management Center (FMC) предлагает полную автоматизацию и оркестрацию для своих продуктов.
  - Централизованное управление. Такие решение как: FortiSwitch, FortiAP, FortiWifi, FortiWLM, FortiExtender и FortiAnalyzer могут управляться из одного портала управления.
  - Гибкое ценообразование. Эксперты Gartner отмечают хорошую зависимость между ценой и производительностью.

Palo Alto Networks

- **Palo Alto Networks** - Лидер 2020 года, среди решений по защите периметра сети по мнению Gartner. Вендор приобрел ведущего поставщика в области облачных решений - CloudGenix, что позволит ему и далее развивать свой продукт Palo Alto Networks Prisma Access (SASE) и применять технологию SD-WAN.
- **Преимущества**:
  - Palo Alto Networks были одними из первых, кто предложили Firewall-as-a-Service (FWaaS).
  - Для инспекции трафика встроена поддержка TLS 1.3 (раньше чем у конкурентов).
  - Вендор активно развивает облачное направление и наращивает количество своих продуктов у заказчиков.

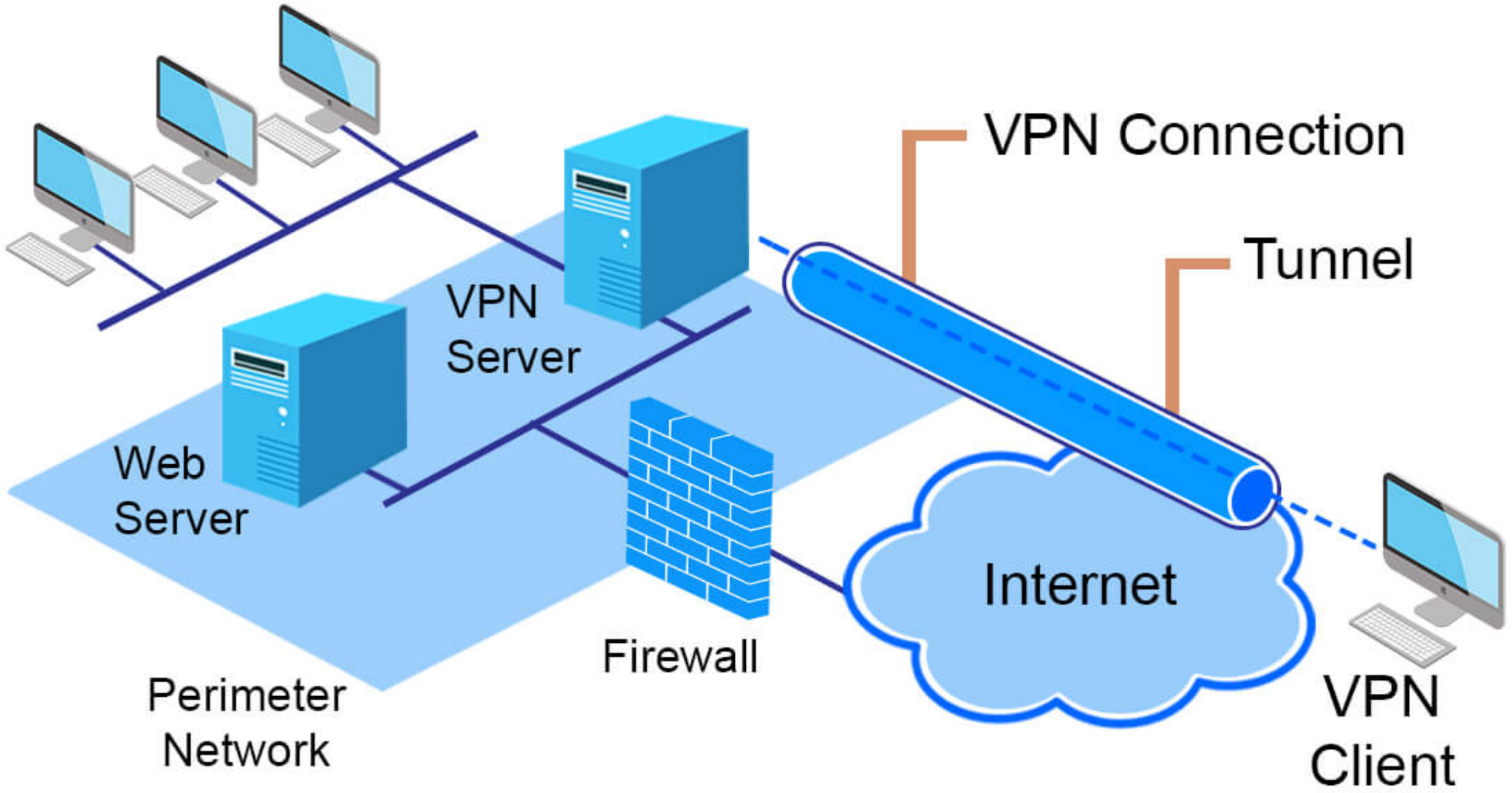
6. Программно-аппаратные средства защиты компьютерных систем

6.2. Технология виртуальных частных сетей

Технология виртуальных частных сетей (VPN)

- **Технология виртуальных частных сетей (VPN — Virtual Private Network)** является одним из эффективных механизмов обеспечения ИБ при передаче данных в распределенных вычислительных сетях.
- **Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов** (механизмов) безопасности:
  - **шифрования** (с использование инфраструктуры криптосистем) на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);
  - **экранирования** (с использованием межсетевых экранов);
  - **туннелирования**.

Технология виртуальных частных сетей (VPN)



Принцип работы VPN

- На все компьютеры, имеющие выход в Интернет, устанавливаются VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.
- **Перед отправкой IP-пакета VPN-агентом выполняются следующие операции:**

  1) анализируется IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета (VPN-агенты могут поддерживать одновременно несколько алгоритмов шифрования и контроля целостности), кроме того, пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится;

  2) вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;

  3) пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);

  4) формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета).

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например внутренние IP-адреса сети, в этом случае недоступна.

Принцип работы VPN

- **При получении IP-пакета выполняются обратные действия:**

  1) из заголовка пакета извлекается информация о VPN-агенте отправителя пакета, если такой отправитель не входит в число разрешенных, то пакет отбрасывается (то же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком);

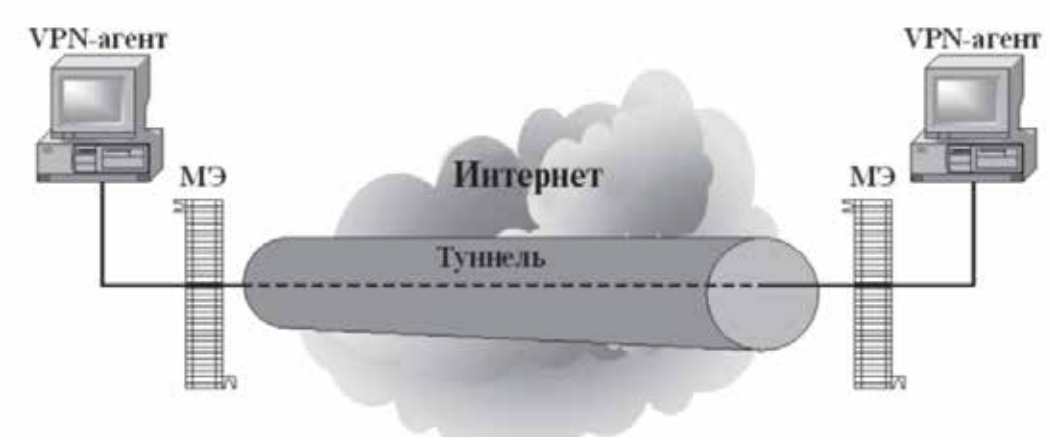
  2) согласно настройкам выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);

  3) после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера, на котором он установлен.

Технология виртуальных частных сетей (VPN)

- Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами. Такой канал называется туннелем, а технология его создания называется туннелированием. Вся информация передается по туннелю в зашифрованном виде.



Пример расположения межсетевых экранов

- Одной из обязательных функций VPN-агентов является фильтрация пакетов. Она реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети. Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.

Протоколы VPN

- **Point-to-Point Tunneling Protocol (PPTP)** — один из старейших VPN протоколов, используемых до сих пор, изначально был разработан компанией Microsoft.
- **Secure Socket Tunneling Protocol (SSTP)** — проприетарный продукт от Microsoft. Как и PPTP, SSTP не очень широко используется в индустрии VPN, но, в отличие от PPTP, у него не диагностированы серьезные проблемы с безопасностью.
- **Internet Protocol Security (IPsec)** — это набор протоколов для обеспечения защиты данных, передаваемых по IP-сети. В отличие от SSL, который работает на прикладном уровне, IPsec работает на сетевом уровне и может использоваться нативно со многими операционными системами, что позволяет использовать его без сторонних приложений (в отличие от OpenVPN). IPsec стал очень популярным протоколом для использования в паре с L2TP или IKEv2.

Протоколы VPN

- **Layer 2 Tunneling Protocol (L2TP)** был впервые предложен в 1999 году в качестве обновления протоколов L2F (Cisco) и PPTP (Microsoft). Поскольку L2TP сам по себе не обеспечивает шифрование или аутентификацию, часто с ним используется IPsec. L2TP в паре с IPsec поддерживается многими операционными системами, стандартизирован в RFC 3193.
- **Internet Key Exchange version 2 (IKEv2) является протоколом IPsec**, используемым для выполнения взаимной аутентификации, создания и обслуживания Security Associations (SA), стандартизован в RFC 7296. Так же защищен IPsec, как и L2TP, что может говорить об их одинаковом уровне безопасности. Хотя IKEv2 был разработан Microsoft совместно с Cisco, существуют реализации протокола с открытым исходным кодом (например, OpenIKEv2, Openswan и strongSwan).

Протоколы VPN

- **OpenVPN** — это универсальный протокол VPN с открытым исходным кодом, разработанный компанией OpenVPN Technologies. На сегодняшний день это, пожалуй, самый популярный протокол VPN. Будучи открытым стандартом, он прошел не одну независимую экспертизу безопасности.

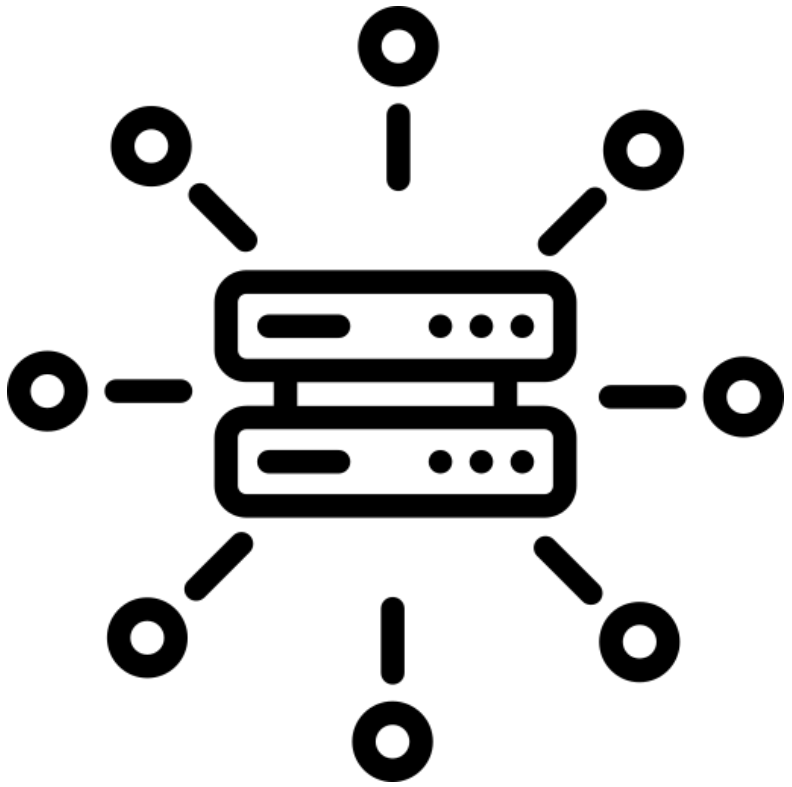
- **WireGuard.** Самый новый и неизведанный протокол VPN — WireGuard. Позиционируется разработчиками как замена IPsec и OpenVPN для большинства случаев их использования, будучи при этом более безопасным, более производительным и простым в использовании.

Сравнение протоколов VPN

	PPTP	SSTP	L2TP/IPsec	IKEv2/IPsec	OpenVPN	WireGuard
Компания-разработчик	Microsoft	Microsoft	L2TP — совместная разработка Cisco и Microsoft, IPsec — The Internet Engineering Task Force	IKEv2 — совместная разработка Cisco и Microsoft, IPsec — The Internet Engineering Task Force	OpenVPN Technologies	Jason A. Donenfeld
Лицензия	Proprietary	Proprietary	Proprietary	Proprietary, но существуют реализации протокола с открытым исходным кодом	GNU GPL	GNU GPL
Развертывание	Windows, macOS, iOS, некоторое время GNU/Linux. Работает “из коробки”, не требуя установки дополнительного ПО	Windows. Работает “из коробки”, не требуя установки дополнительного ПО	Windows,Mac OS X, Linux, iOS, Android. Многие ОС (включая Windows 2000/XP +, Mac OS 10.3+) имеют встроенную поддержку, нет необходимости ставить дополнительное ПО	Windows 7+, macOS 10.11+ и большинство мобильных ОС имеют встроенную поддержку	Windows, Mac OS, GNU/Linux, Apple iOS, Android и маршрутизаторы. Необходима установка специализированного ПО, поддерживающего работу с данным протоколом	Windows, Mac OS, GNU/Linux, Apple iOS, Android. Установить сам WireGuard, а затем настроить по руководству

Сравнение протоколов VPN

	PPTP	SSTP	L2TP/IPsec	IKEv2/IPsec	OpenVPN	WireGuard
Шифрование	Использует Microsoft Point-to-Point Encryption (MPPE), который реализует RSA RC4 с максимум 128-битными сеансовыми ключами	SSL (шифруются все части, кроме TCP- и SSL-заголовков)	3DES или AES	Реализует большое количество криптографических алгоритмов, включая AES, Blowfish, Camellia	Использует библиотеку OpenSSL (реализует большинство популярных криптографических стандартов)	Обмен ключами по 1-RTT, Curve25519 для ECDH, RFC7539 для ChaCha20 и Poly1305 для аутентификационного шифрования, и BLAKE2s для хеширования
Порты	TCP-порт 1723	TCP-порт 443	UDP-порт 500 для первонач. обмена ключами и UDP-порт 1701 для начальной конфигурации L2TP, UDP-порт 5500 для обхода NAT	UDP-порт 500 для первоначального обмена ключами, а UDP-порт 4500 — для обхода NAT	Любой UDP- или TCP-порт	Любой UDP-порт
Недостатки безопасности	Обладает серьезными уязвимостями. MSCHAP-v2 уязвим для атаки по словарю, а алгоритм RC4 подвергается атаке Bit-flipping	Серьезных недостатков безопасности не было выявлено	3DES уязвим для Meet-in-the-middle и Sweet32, но AES не имеет известных уязвимостей. Однако есть мнение, что стандарт IPsec скомпрометирован АНБ США	Не удалось найти информации об имеющихся недостатках безопасности, кроме инцидента с утечкой докладов АНБ касательно IPsec	Серьезных недостатков безопасности не было выявлено	Серьезных недостатков безопасности не было выявлено



6. Программно-аппаратные средства защиты компьютерных систем

6.3. Протоколы безопасности

Протоколы безопасности

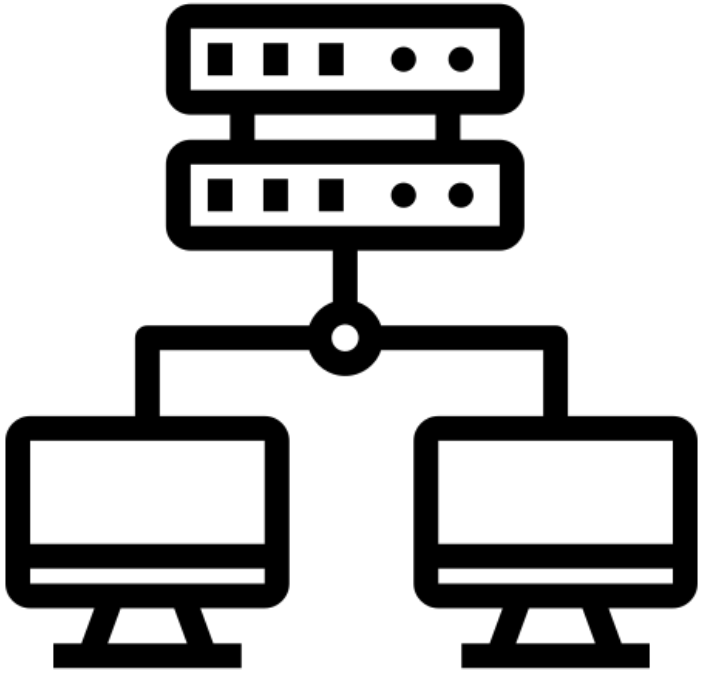
- **Сетевые протоколы безопасности используются для защиты компьютерных данных и связи при их передаче по сети.**
- Основным инструментом, **используемым для защиты информации при пересылке через сеть является криптография**. Криптография использует алгоритмы для шифрования данных, так чтобы они не были прочитаны не авторизованными пользователями.
- Без криптографических протоколов сетевой безопасности, Интернет-функции, такие как электронная коммерция будет невозможной.
- Безопасное общение необходимо, потому что злоумышленники пытаются подслушать коммуникации, чтобы изменить сообщения и захватить обмен данными между системами. Некоторые задачи сетевого протокола безопасности используются для защиты передачи файлов, веб-общения, и виртуальных частных сетей (VPN).

Протоколы SSL **и** TLS

- **SSL (англ. Secure Sockets Layer — уровень защищённых сокетов)** — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений. Протокол широко использовался для обмена мгновенными сообщениями и передачи голоса через IP (англ. Voice over IP — VoIP) в таких приложениях, как электронная почта, интернет-факс и др.
- **TLS (англ. transport layer security — Протокол защиты транспортного уровня)**, как и его предшественник SSL (англ. secure sockets layer — слой защищённых сокетов), — криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет. TLS и SSL используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений. Данный протокол широко используется в приложениях, работающих с сетью Интернет, таких как веб-браузеры, работа с электронной почтой, обмен мгновенными сообщениями и IP-телефония (VoIP).

HTTPS

- **HTTPS (аббр. от англ. HyperText Transfer Protocol Secure)** — расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов TLS или устаревшего в 2015 году SSL. В отличие от HTTP с TCP-портом 80, для HTTPS по умолчанию используется TCP-порт 443.
- **HTTPS не является отдельным протоколом. Это обычный HTTP, работающий через шифрованные транспортные механизмы SSL и TLS.** Он обеспечивает защиту от атак, основанных на прослушивании сетевого соединения — от снифферских атак и атак типа man-in-the-middle, при условии, что будут использоваться шифрующие средства и сертификат сервера проверен и ему доверяют.



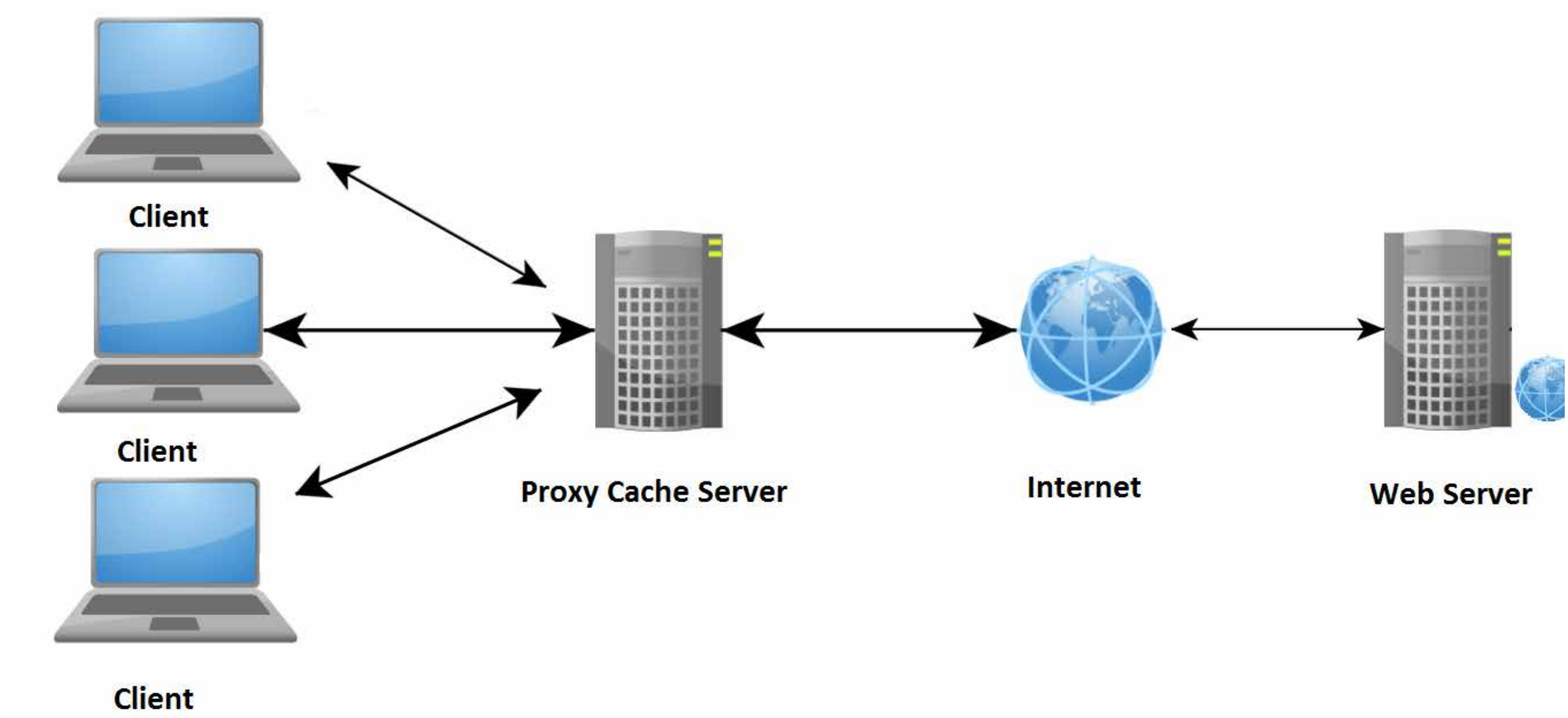
6. Программно-аппаратные средства защиты компьютерных систем

6.4. Proxy

Прокси-сервер (Proxy)

- **Прокси-сервер** (proxy — представитель, уполномоченный; часто просто прокси, сервер-посредник) — **промежуточный сервер (комплекс программ) в компьютерных сетях, выполняющий роль посредника между пользователем и целевым сервером** (при этом о посредничестве могут как знать, так и не знать обе стороны), **позволяющий клиентам как выполнять косвенные запросы** (принимая и передавая их через прокси-сервер) **к другим сетевым службам, так и получать ответы**.
- Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например e-mail), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (в случаях, если прокси имеет свой кэш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Прокси-сервер позволяет защищать компьютер клиента от некоторых сетевых атак и помогает сохранять анонимность клиента, но также может использоваться мошенниками для скрытия адреса сайта, уличённого в мошенничестве, изменения содержимого целевого сайта (подмена), а также перехвата запросов самого пользователя.

Прокси-сервер (Proxy)



Использование Proxy

- **Чаще всего прокси-серверы применяются для следующих целей:**
  - **обеспечение доступа** компьютеров локальной сети к сети Интернет;
  - **кэширование данных**: если часто происходят обращения к одним и тем же внешним ресурсам для снижения нагрузки на канал во внешнюю сеть и ускорения получения клиентом запрошенной информации;
  - **сжатие данных**: прокси-сервер загружает информацию из Интернета и передаёт информацию конечному пользователю в сжатом виде для экономии внешнего сетевого трафика клиента или внутреннего — организации, в которой установлен прокси-сервер;
  - **защита локальной сети от внешнего доступа**: например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным вообще (они «видят» только прокси-сервер);
  - **ограничение доступа из локальной сети к внешней**: например, можно запрещать доступ к определённым веб-сайтам, ограничивать использование интернета каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, фильтровать рекламу и вирусы;
  - **анонимизация доступа к различным ресурсам**: прокси-сервер может скрывать сведения об источнике запроса или пользователе. В таком случае целевой сервер видит лишь информацию о прокси-сервере, например IP-адрес, но не имеет возможности определить истинный источник запроса; существуют также искажающие прокси-серверы, которые передают целевому серверу ложную информацию об истинном пользователе;
  - **обход ограничений доступа**: используется, например, пользователями стран, где доступ к некоторым ресурсам ограничен законодательно и фильтруется.

Виды Proxy

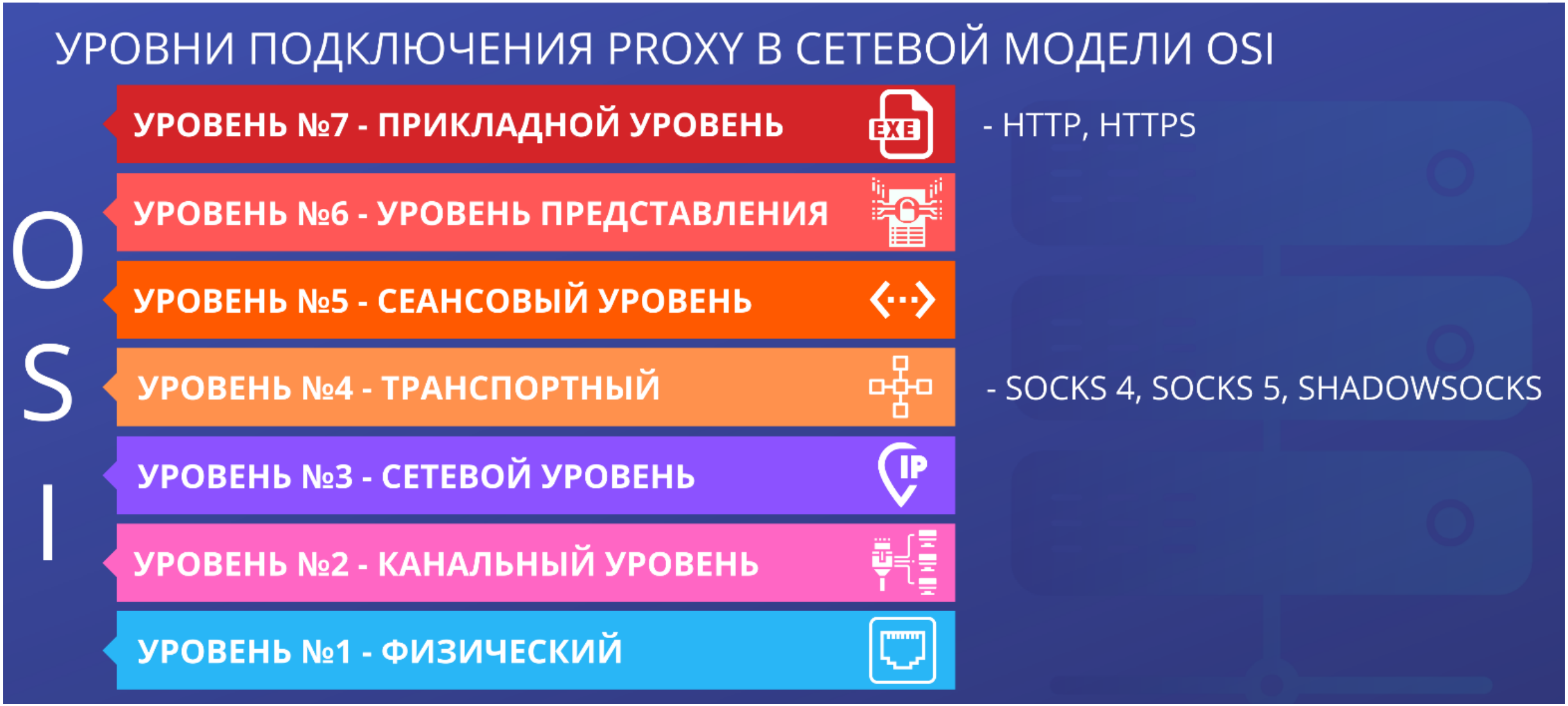
- **Прокси бывают нескольких видов:**
- **CGI - или по-другому web прокси.** Это веб страница, на которой вам предлагается ввести адрес сайта и он откроется в этой же странице с другим IP. Браузерный вариант.
- **HTTP** - Простой прокси для HTTP запросов. Бесполезное решение в нашем случае.
- Ко всему прочему HTTP делятся еще на три условные группы:
  - **Прозрачные прокси** - Сообщат всем веб ресурсам ваш реальный IP. Пример - заголовок x-forwarded-for. Бесполезно.
  - **Анонимные прокси** - Скроют ваш IP, но сообщат о том, что используется прокси. Бесполезно.
  - **Элитные прокси** - Скроют ваш IP, не сообщат о том, что используется прокси, ну и на этом все. Бесполезно.
- **HTTPS** - Тот же бесполезный для нас прокси HTTP но уже +S - а это значит, что он поддерживает шифрование, то есть у нас будут проксифицироватся вебстраничкиhttps - формы авторизации, ввод и передача чувствительной информации и т.д. Но этот прокси все равно издалека виден Антифрод системам, плюс ко всему еще и может модифицировать наши пакеты.
- **Socks 4** - Первый пригодный для работы протокол Прокси. Пытается скрыть проксификацию, не модифицирует пакеты и в целом неплох, но имеет свои минусы.
- **Socks 5** - Практически идеальный вариант, то же что и Socks 4, но добавилась так нам нужная поддержка UDP протокола, и соответственно возможность подмены DNS и IPv6.
- **ShadowSocks** - Китайское опенсорс изобретение, которое по функционалу лидирует среди всех конкурентов. Идеал.

Сравнительная таблица современных Proxy протоколов

	HTTP (элитные)	HTTPS	SOCKS 4	SOCKS 5	SHADOWSOCKS
СКРЫВАЕТ РЕАЛЬНЫЙ IP	✓	✓	✓	✓	✓
ПОДДЕРЖКА SSL ШИФРОВАНИЯ	✗	✓	✓	✓	✓
СКРЫВАЕТ ФАКТ ПРОКСИФИКАЦИИ	✗	✗	✓	✓	✓
НЕ ИЗМЕНЯЕТ ЗАГОЛОВОК ПАКЕТА	✗	✗	✓	✓	✓
ПРОКСИФИКАЦИЯ ВСЕХ ПРОТОКОЛОВ	✗	✗	✓	✓	✓
РАБОТА ЗА ФАЕРВОЛОМ	✗	✗	✓	✓	✓
ПОДДЕРЖКА UDP ПРОТОКОЛА	✗	✗	✗	✓	✓
ПРОКСИФИКАЦИЯ DNS ЗАПРОСОВ	✗	✗	✗	✓	✓
АДРЕСАЦИЯ IPV6	✗	✗	✗	✓	✓
РАСШИРЕННЫЕ ПРОТОКОЛЫ ШИФРОВАНИЯ	✗	✗	✗	✗	✓
МАСКИРОВКА ТРАФИКА	✗	✗	✗	✗	✓
ЗАЩИТА ОТ DPI	✗	✗	✗	✗	✓
	HTTP (элитные)	HTTPS	SOCKS 4	SOCKS 5	SHADOWSOCKS

НЕКОТОРЫЕ ПУНКТЫ ИМЕЮТ ВАРИАТИВНЫЕ ЗНАЧЕНИЯ, КОТОРЫЕ ЗАВИСЯТ ОТ НАСТРОЕК

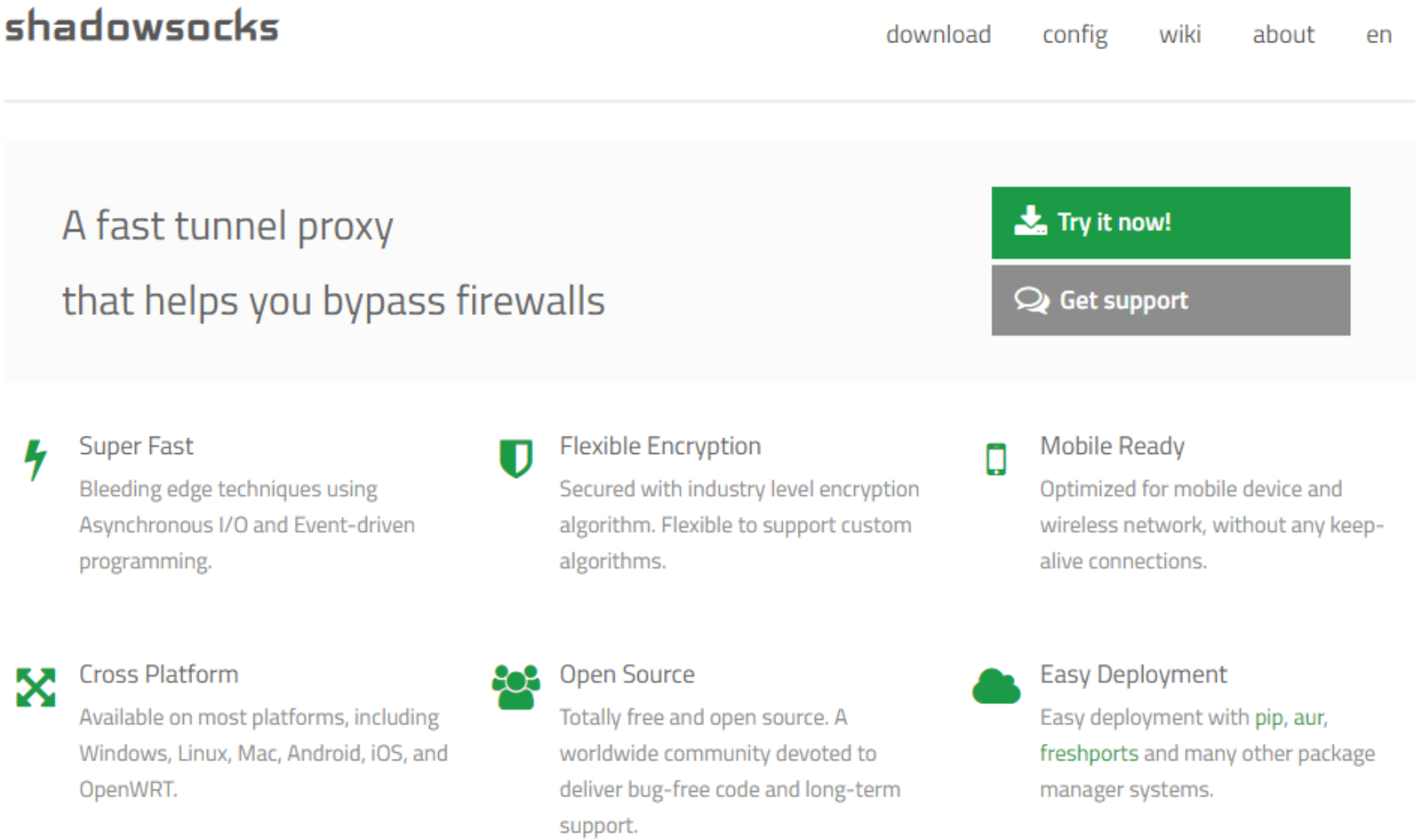
Сравнительная таблица современных Proxy протоколов

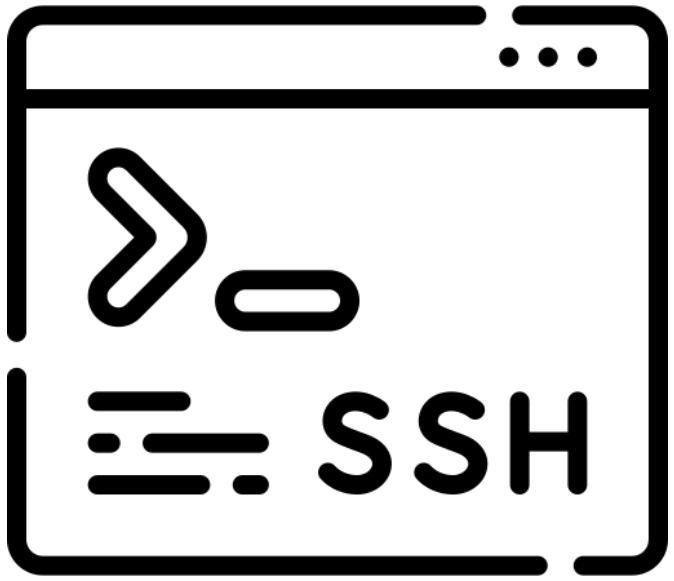


Shadowsocks

https://shadowsocks.org/en/index.html

https://github.com/shadowsocks/



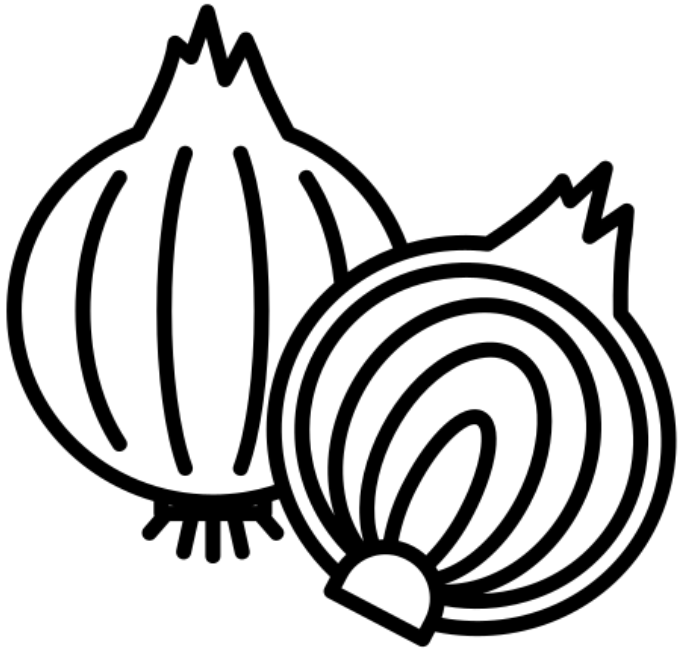


6. Программно-аппаратные средства защиты компьютерных систем

6.5. SSH туннели

SSH **туннели**

- Вторая по популярности после Proxy технология.
- Удаленный сервер, который по нашему принуждению стал сервером посредником.
- Работает это так - при соединении SSH-клиента и SSH-сервера со стороны SSH-клиента поднимается SOCKS-прокси, например, на localhost'е, на который можно указывать приложениям с поддержкой SOCKS. Само проксирование будет через SSH-сервер, с которым вы соединяетесь.
- В сумме - Интернет вас будет видеть от имени SSH-сервера, соединение между SSH-клиентом и SSH-сервером зашифровано, так что не видно вложенных данных приложения, а для приложения все выглядит как обращение к обычному SOCKS-прокси.



6. Программно-аппаратные средства защиты компьютерных систем

6.6. Tor

Tor

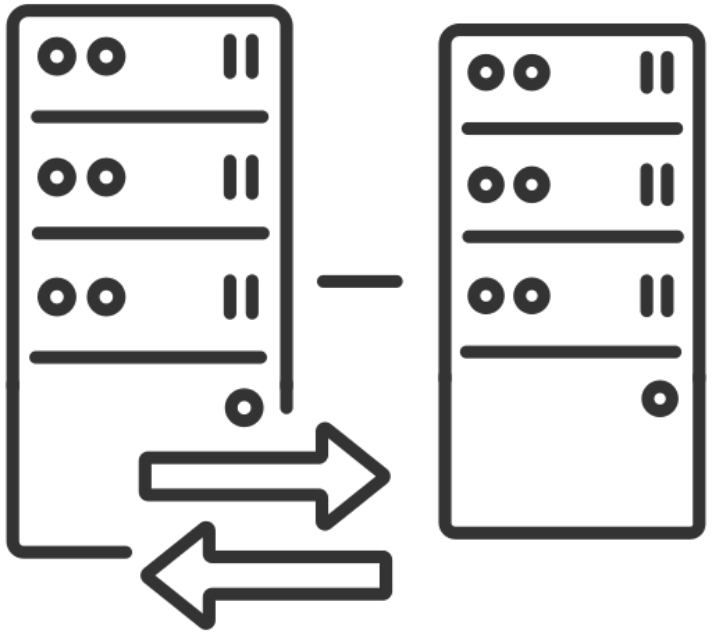
- **Tor – это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания.** Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.
- С помощью Tor пользователи могут сохранять анонимность в Интернете при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими протокол TCP. Анонимизация трафика обеспечивается за счёт использования распределённой сети серверов — узлов. Технология Tor также обеспечивает защиту от механизмов анализа трафика, которые ставят под угрозу не только приватность в Интернете, но также конфиденциальность коммерческих тайн, деловых контактов и тайну связи в целом.
- Tor оперирует сетевыми уровнями onion-маршрутизаторов, позволяя обеспечивать анонимные исходящие соединения и анонимные скрытые службы.

Tor

- В TOPe в нашем случае есть основные проблемы:
- 1. TOP Браузер не изменяет отпечатки нашей цифровой личности.
- 2. TOP Браузер имеет свои уникальные особенности, которые нас выдадут.
- 3. Все знают что сеть TOP официально выступает за интернет без цензуры, ну а по факту там в основном наркотики и детское порно. Ни одна уважающая себя система защиты не позволит ничего сделать с IP адреса входящего в сеть выходных узлов сети TOP. Просто забываем про использование TOPa в работе.

Сравнение технологий

- И по результатам, среди всех популярных технологий, по смене IP адреса можно выделить 4 технологии пригодные для работы:
  1. Socks 5
  2. ShadowSocks
  3. SSH туннели
  4. VPN
- Ну признаются непригодными для работы:
  1. CGI Proxy
  2. HTTP Proxy
  3. HTTPS Proxy
  4. Socks 4 Proxy
  5. TOR

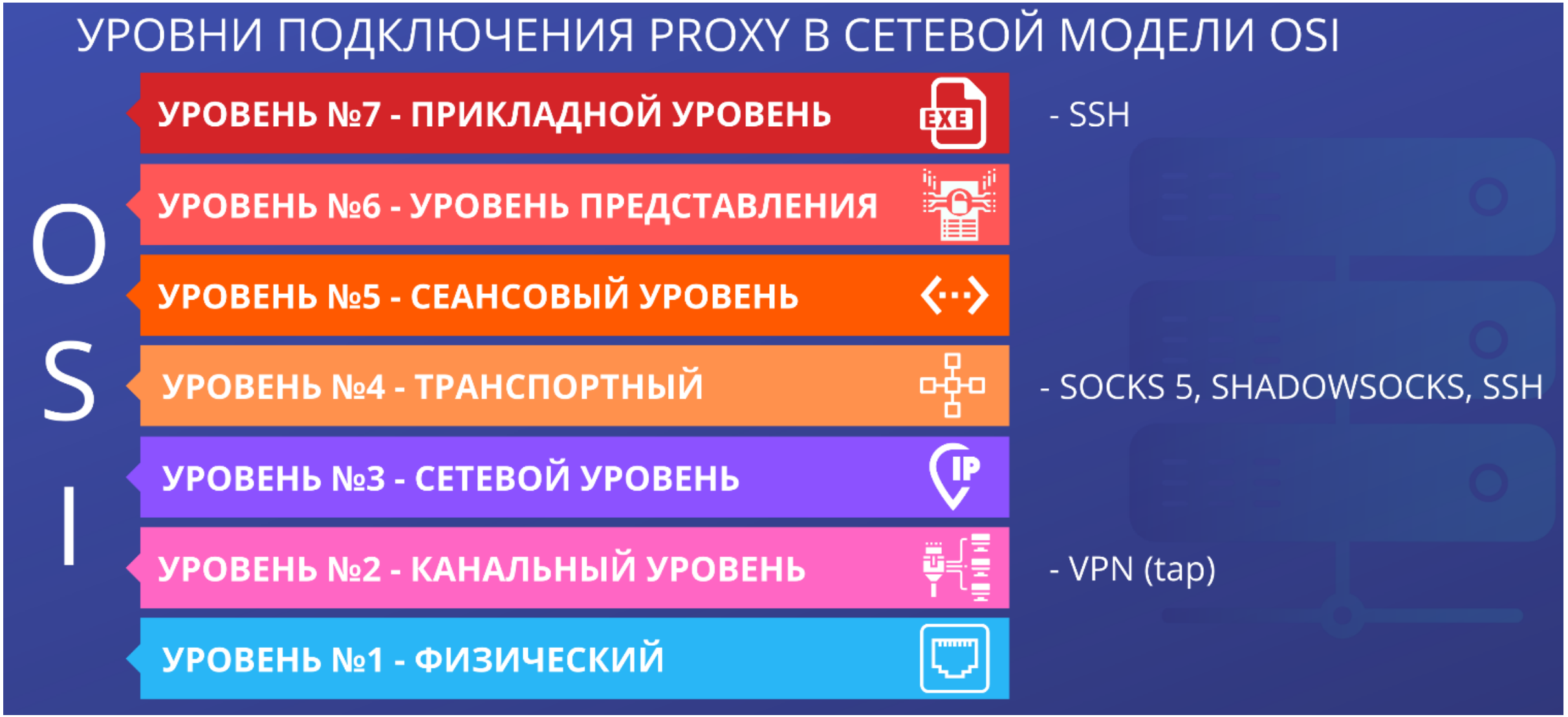


6. Программно-аппаратные средства защиты компьютерных систем

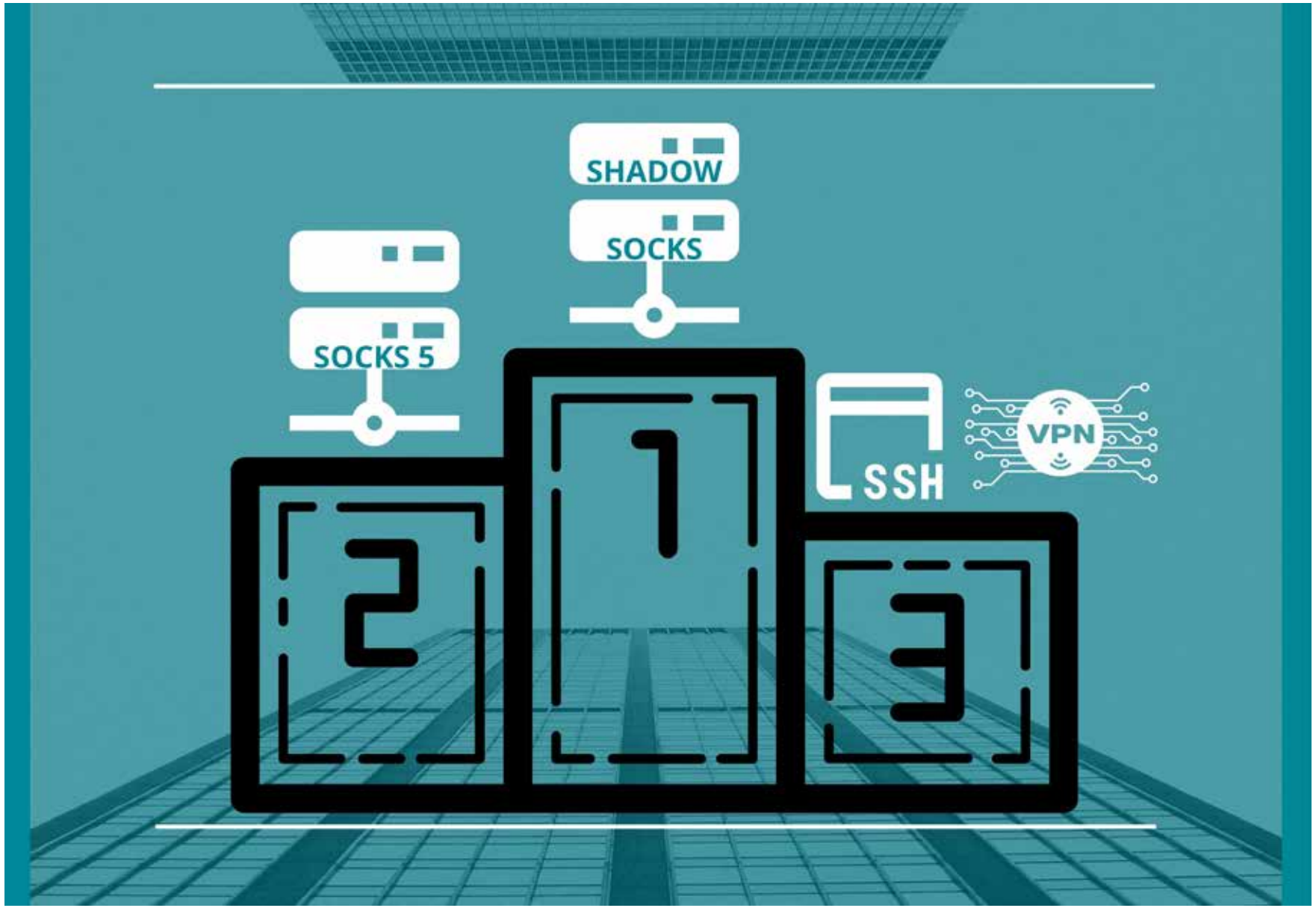
6.7. VPN \ Proxy \ Tor \ Протоколы

Сравнение технологий

Сравнение технологий



Сравнение технологий



Выбор технологий

БАЗОВАЯ АНОНИМНОСТЬ (DOUBLE/TRIPPLE/QUADRO VPN)

Стоимость: средняя Скорость: высокая

Защита от деанонимизации административными методами: средняя

Защита от активной деанонимизации вредоносным ПО: отсутствует

Защита от деанонимизации тайминг-атаками: низкая

Защита от деанонимизации путем эксплуатирования уязвимостей в элементах связки: отсутствует

Защита от деанонимизации путем экслуатирования уязвимостей веб-браузера: отсутствует

Выбор технологий

Защита от деанонимизации административными методами: высокая

Защита от активной деанонимизации вредоносным ПО: отсутствует

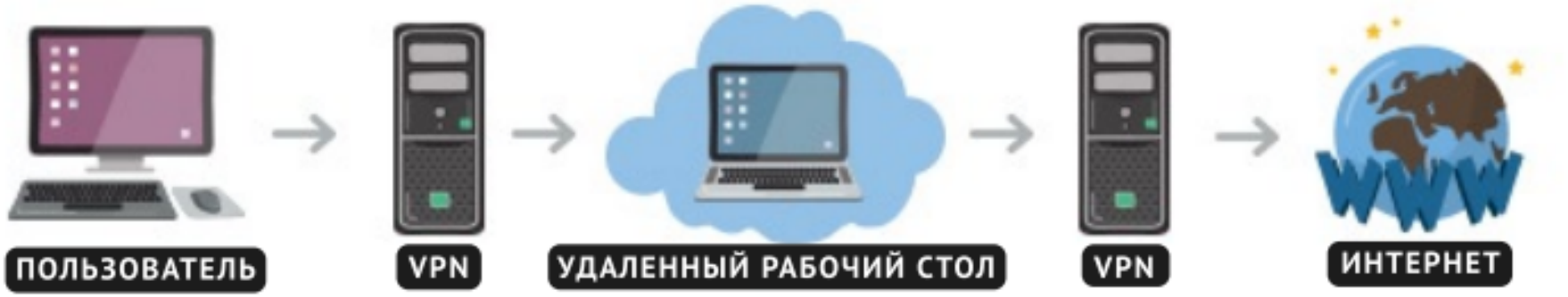
Защита от деанонимизации тайминг-атаками: средняя

Защита от деанонимизации путем эксплуатирования уязвимостей в элементах связки: отсутствует

Защита от деанонимизации путем экслуатирования уязвимостей веб-браузера: отсутствует

Выбор технологий

VPN-УДАЛЕННЫЙ РАБОЧИЙ СТОЛ-VPN



Стоимость: высокая

Скорость: высокая

Защита от деанонимизации административными методами: средняя

Защита от активной деанонимизации вредоносным ПО: высокая

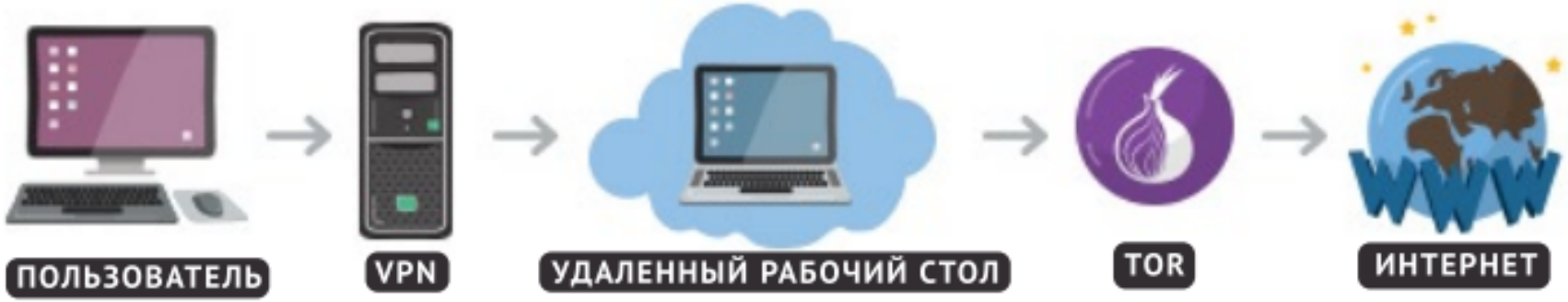
Защита от деанонимизации тайминг-атаками: высокая

Защита от деанонимизации путем эксплуатирования уязвимостей в элементах связки: средняя

Защита от деанонимизации путем экслуатирования уязвимостей веб-браузера: высокая

Выбор технологий

VPN-УДАЛЕННЫЙ РАБОЧИЙ СТОЛ-TOP



Стоимость: высокая Скорость: средняя

Защита от деанонимизации административными методами: высокая

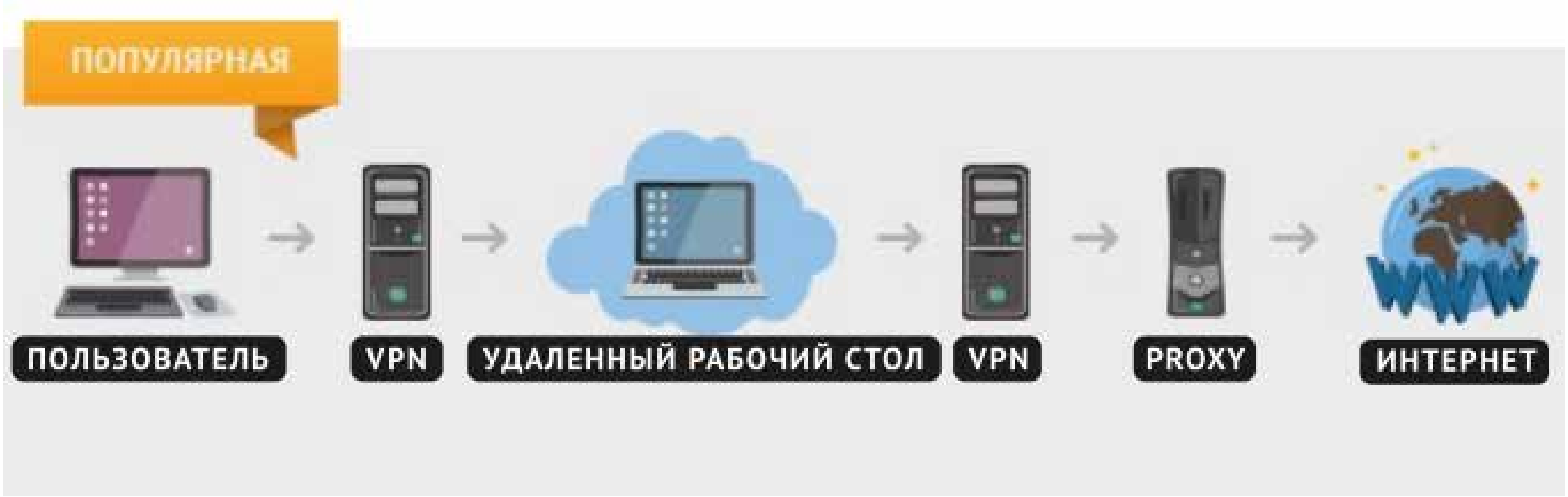
Защита от активной деанонимизации вредоносным ПО: высокая

Защита от деанонимизации тайминг-атаками: высокая

Защита от деанонимизации путем эксплуатирования уязвимостей в элементах связки: высокая

Защита от деанонимизации путем экслуатирования уязвимостей веб-браузера: высокая

Выбор технологий



6. Программно-аппаратные средства защиты компьютерных систем

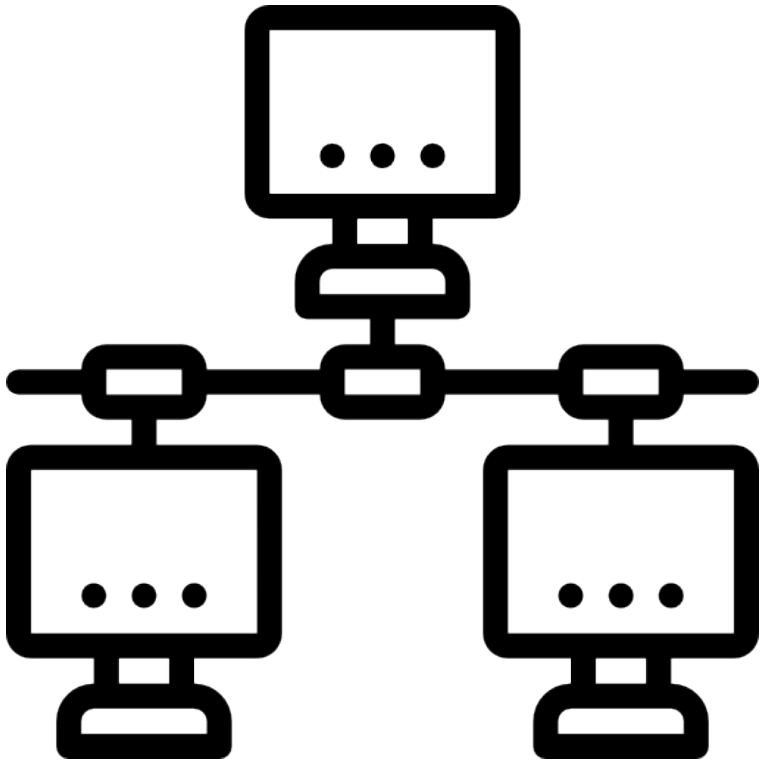
6.8. Антивирусная защита

Антивирусная защита

Антивирусное программное обеспечение

- **Антивирусное программное обеспечение** представляет собой компьютерную программу, которая защищает компьютер от входящих угроз, ищет, уничтожает и предупреждает о возможных угрозах для системы.

- **Антивирус защищает от:**
- 1 Потери всех данных компании ввиду заражения шифровальщиком или другим вредоносным кодом.
- 2 Хищения конфиденциальных данных, либо вывода финансовых средств.
- 3 Потери контроля над конкретным хостом и сетью в целом.



6. Программно-аппаратные средства защиты компьютерных систем

6.9. Мониторинг ИТ-инфраструктуры

Зачем использовать мониторинг

- Успех и развитие современных компаний во многом зависит от стабильности и защищенности ИТ-инфраструктуры. Чем чаще в компании происходят сбои, простои после атак, тем больше вероятности, что это приведет к проблемам в бизнес-процессах.
- Компании почему-то недооценивают важность мониторинга как части информационной безопасности.
- Если в компании были лишь небольшие проблемы с ИТ-инфраструктурой, компания всё также может столкнуться с нехваткой прибыли, нестабильностью и низкой эффективностью.
- Во избежание подобных результатов внедряются решения по мониторингу ИТ-инфраструктуры. Они помогают с отслеживанием того, что происходит в корпоративной сети. В результате значительно повышается реакция на возможные сбои и атаки.

Какие бывают виды мониторинга?

- На рынке появляется всё больше различных систем мониторинга корпоративной сети, но даже такое разнообразие имеет свои узкие специальности.
- Их выделяют в определённые группы:
  - **Бесплатные системы с открытым исходным кодом**, вроде Zabbix. Хоть подобные системы и бесплатные, но качество их работ ничуть не хуже. Также подобная группа отличается возможностью гибко настраивать все инструменты под корпоративные задачи. Ведь с помощью открытого кода сетевые администраторы могут адаптировать решение для стандартного мониторинга без посторонней помощи.
  - **Коммерческие системы с закрепленным функционалом**. Их особенность состоит в том, что такие системы с легкостью разворачиваются и решают характерные задачи мониторинга. Единственный недостаток состоит в том, что коммерческие системы менее гибки и не так легко адаптируются под нестандартные сценарии.
  - **Коммерческие системы платформенного типа** подразумевают под собой комплекс решений, которые нацелены на мониторинг, управление процессов и решение нестандартных задач. Хоть подобные системы и дороже в сравнении с другими группами, компании не придется внедрять их в общую консоль управления и далее подстраивать под другие решения.

Zabbix

- **Zabbix** – это бесплатная система с открытым доступом и обширным функционалом. Система известна тем, что она быстро настраивается, помогает с визуализацией данных о сбоях и других проблемах.
- Почему стоит обратить внимание на эту систему?
  - Автоматическое обнаружение угроз;
  - Обширный веб-интерфейс для настройки и администрирования;
  - Комплексная реакция на различные события в сети;
  - Возможность внедрения расширений.

Zabbix

- **Функции**
  - Автоматическое обнаружение серверов и сетевых устройств.
  - Низкоуровневое обнаружение.
  - Децинтрализованный мониторинг с централизованным веб-администрированием.
  - Централизованный мониторинг лог-файлов.
  - Серверное программное обеспечение для GNU/Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X.
  - Родные высокопроизводительные агенты (клиентское программное обеспечение для GNU/Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X, Tru64/OSF1, Windows NT4.0, Windows 2000, Windows 2003, Windows XP, Windows Vista).
  - Безагентный мониторинг.
  - Безопасная авторизация пользователей.
  - Веб-интерфейс.
  - Уведомления о предопределенных событиях.

Zabbix

- **Возможности**
  - Распределенный мониторинг вплоть до 1000 узлов. Конфигурация младших узлов полностью контролируется старшими узлами, находящихся на более высоком уровне иерархии.
  - Сценарии на основе мониторинга
  - Автоматическое обнаружение
  - Централизованный мониторинг лог-файлов
  - Веб-интерфейс для администрирования и настройки
  - Отчетность и тенденции
  - SLA мониторинг
  - Поддержка высокопроизводительных агентов (zabbix-agent) практически для всех платформ
  - Комплексная реакция на события
  - Поддержка SNMP v1, 2, 3
  - Поддержка SNMP ловушек
  - Поддержка IPMI
  - Поддержка мониторинга JMX приложений из коробки
  - Поддержка выполнения запросов в различные базы данных без необходимости использования скриптовой обвязки
  - Расширение за счет выполнения внешних скриптов
  - Гибкая система шаблонов и групп
  - Возможность создавать карты сетей

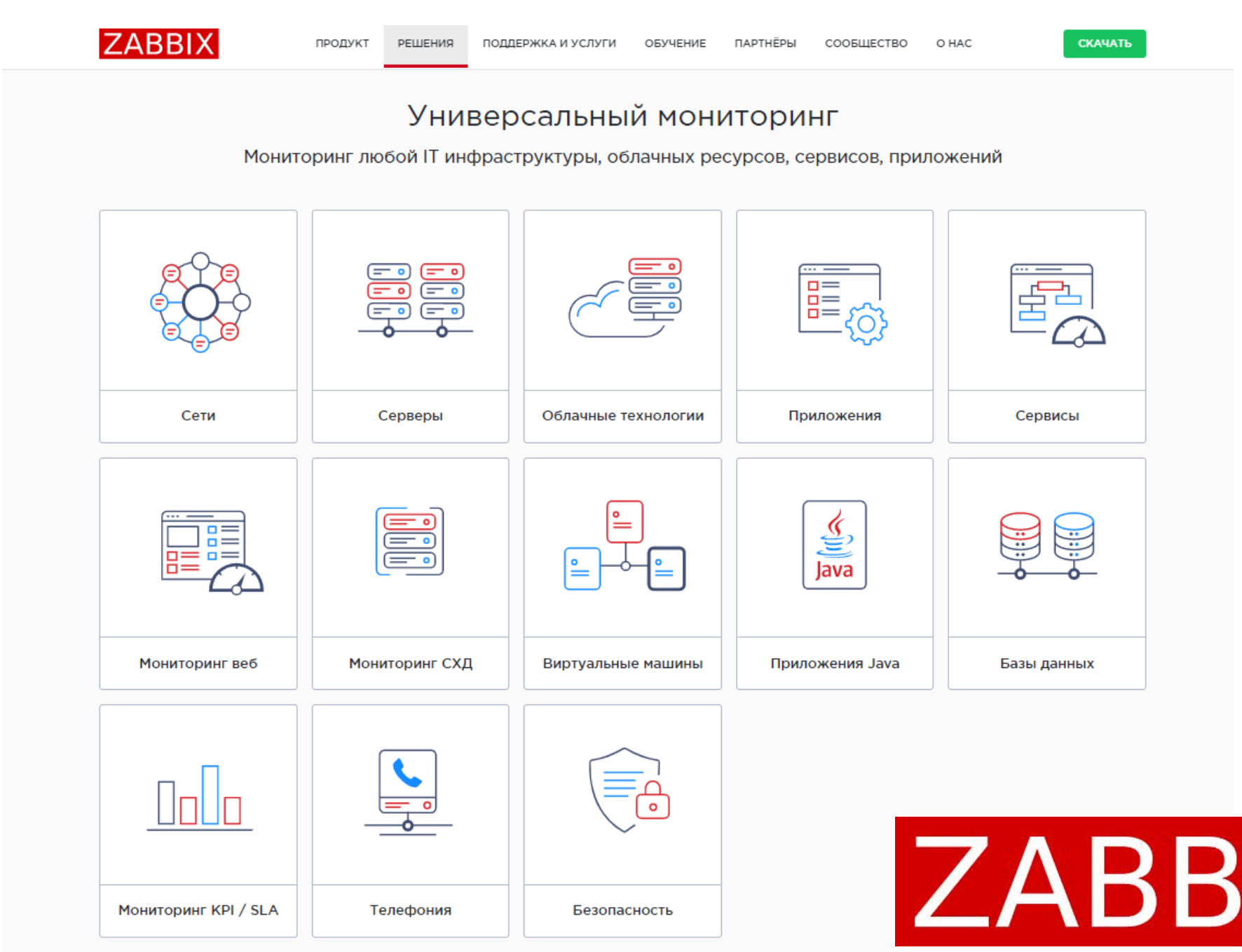
Zabbix

- Официальный сайт Zabbix
- https://www.zabbix.com/ru/

- Скачать и установить Zabbix
- https://www.zabbix.com/ru/download

- Готовые решения Zabbix
- https://www.zabbix.com/ru/download_appliance

Zabbix



ZABBIX

Dell Foglight

- **Dell Foglight** – решение по мониторингу, которое можно внедрять в различные технологические среды. Это решение пользуется своей популярностью из-за возможности улучшать качество обслуживания всех клиентов и создавать безопасные условия для работы в ИТ-инфраструктуре.
- Среди главных причин, почему Dell Foglight может быть полезен компании:
  - Возможность снизить эксплуатационные расходы;
  - Снижение количества сбоев;
  - Сокращение времени простоя;
  - Работа в соответствии с SLA.

Foglight

- **Foglight — это основное решение для мониторинга производительности и управления ею во множестве различных технологических сред** (например, Java, .NET, виртуальные и физические серверы, базы данных и т.д.), а также для контроля за действиями пользователей, взаимодействующих с этими бизнес-приложениями.
- Ведущие организаций всего мира используют Foglight, чтобы повысить уровень обслуживания пользователей и обеспечить соответствие среды ИТ потребностям организации. Foglight также поможет вам обнаружить основную причину любого инцидента, который влияет на производство, чтобы вы могли быстро исправить проблему.
- Если Вы развертываете программное обеспечение для мониторинга производительности в первый раз или используете его, чтобы восполнить пробел мониторинга, модульная архитектура и стоимость Foglight могут помочь Вашей организации провести выравнивание и идти в ногу с растущими потребностями бизнеса и конечных пользователей.
- Foglight упрощает управление производительностью приложений, баз данных и инфраструктуры, помогая в следующем
  - Снижение эксплуатационных расходов по управлению средами ИТ
  - Снижение риска простоя при одновременном повышении производительности труда сотрудников
  - Повышение уровня соответствия SLA приложений, баз данных и инфраструктуры конечного пользователя
  - Сокращение числа инцидентов и среднего времени восстановления после инцидентов
  - Обеспечение видимости ИТ и заинтересованных лиц

Quest DELL Software

Foglight

- Foglight
- https://www.quest.com/foglight/

- Foglight. Download Free Trial
- https://www.quest.com/register/127815/

- Foglight for Cross-Platform Databases. Download Free Trial
- https://www.quest.com/register/55612/

- Foglight Evolve
- https://www.quest.com/register/55511/

Microsoft SCOM (System Center Operations Manager)

- **Microsoft SCOM или System Center Operations Manager** имеет компонент мониторинга за ИТ-инфраструктурой, с помощью которого управляются облачные среды и ЦОД.

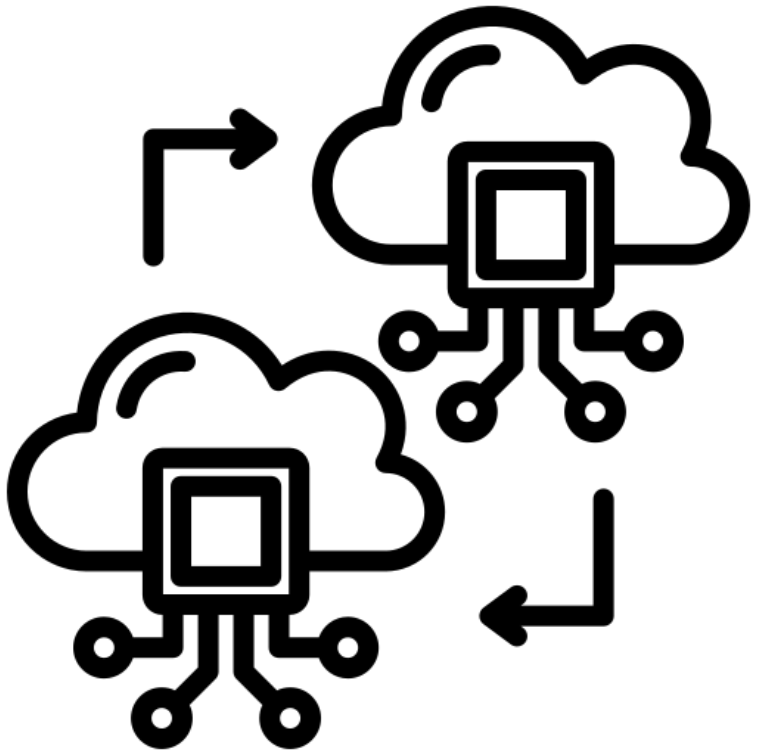
- Основные преимущества:
  - Возможность гибко настраивать мониторинг в соответствии с потребностями;
  - Возможность обеспечивать желательную производительность корпоративной сети;
  - Комплексный подход к вопросу мониторинга.

Microsoft SCOM

- История версий
  - 1994 — Microsoft Systems Management Server 1.0
  - 1995 — Microsoft Systems Management Server 1.1
  - 1996 — Microsoft Systems Management Server 1.2
  - 1999 — Microsoft Systems Management Server 2.0
  - 2003 — Microsoft Systems Management Server 2003
  - 2007 — System Center Configuration Manager 2007 [Changed from: Microsoft Systems Management Server version 4]
  - 2007 — System Center Essential 2007 (комбинация Microsoft SCOM и SMS серверов)
  - 2010 — System Center Essential 2010 (комбинация Microsoft SCOM и SMS серверов)
  - 2012 — System Center 2012 Configuration Manager
  - **2019 — Microsoft Endpoint Configuration Manager**

Microsoft SCOM

- Microsoft Endpoint Manager Ознакомительные версии
- https://www.microsoft.com/ru-ru/evalcenter/evaluate-microsoft-endpoint-configuration-manager
- Документация по Microsoft Endpoint Configuration Manager
- https://docs.microsoft.com/ru-ru/mem/configmgr/

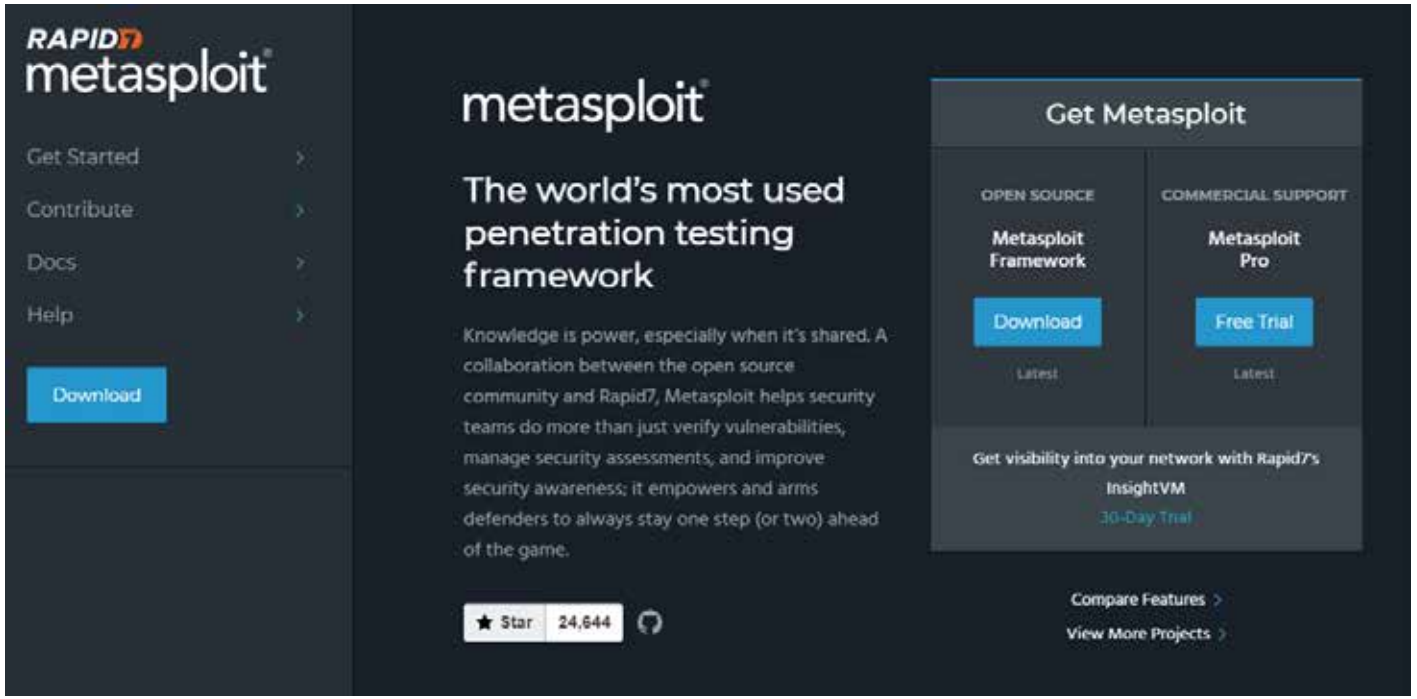


6. Программно-аппаратные средства защиты компьютерных систем

6.10. Сканеры уязвимостей

Metasploit
https://www.metasploit.com

- **Metasploit** – это проект с открытым исходным кодом, написанный на Ruby, который позволяет использовать различные инструменты кибербезопасности для обнаружения уязвимостей и функций удаленного программного обеспечения в качестве модуля разработки эксплойтов.



Impacket
https://github.com/SecureAuthCorp/impacket

Impacket
https://github.com/SecureAuthCorp/impacket

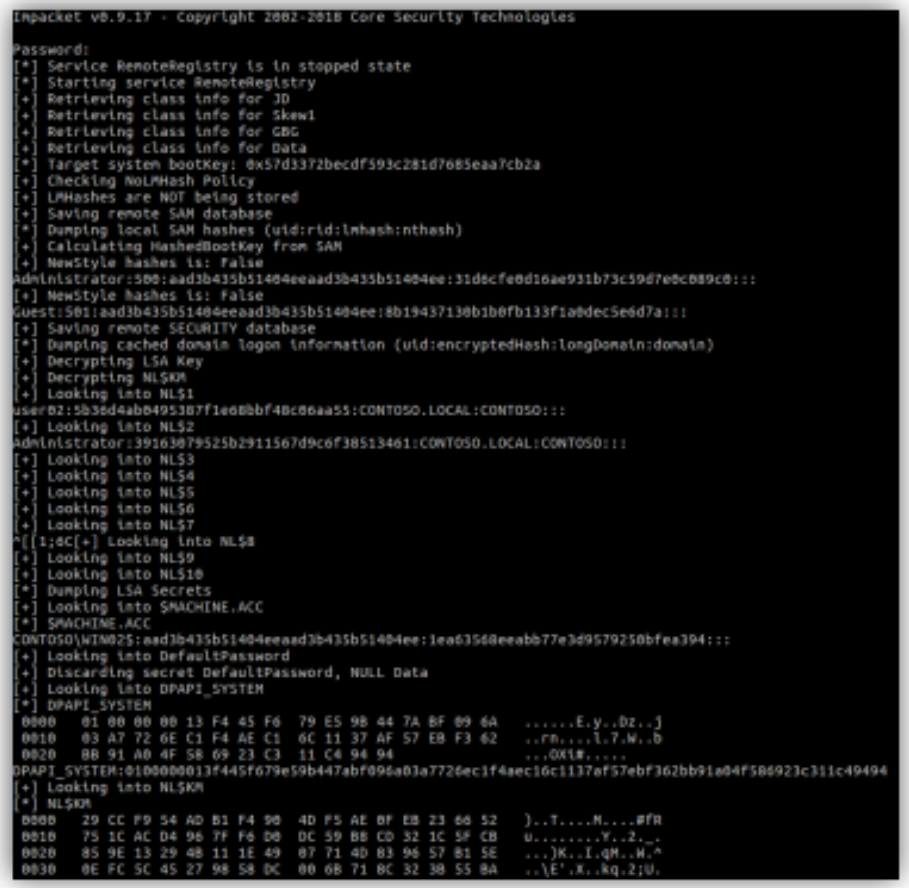
Impacket secretsdump

Что делает:

Получение различных хешей с машины жертвы – SAM, LSA, NTDS.dit (с DC)

Как работает:

1. Аутентифицируется через SMB
2. Подключается к SCM и удаленному реестру
3. Запрашивает ключ реестра по протоколу WINREG
4. Сохраняет полученное на машину атакующего
5. Зачищает следы



Impacket https://github.com/SecureAuthCorp/impacket

Impacket smbexec

Что делает:

выполняет команды удаленно

Как работает:

1. Аутентифицируется через SMB
2. Отправляет запрос на открытие ServiceControlManager
3. Отправляет запрос на создание сервиса
4. Отправляет запрос на старт сервиса
5. Отправляет команды и получает ответы

```
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

Password:
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.241.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.241.100

Tunnel adapter isatap.{8E2E72AC-F463-4D3A-A0C4-1CE5EFAD7182}:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5efe:192.168.241.102%12
   Default Gateway . . . . . . . . . :

C:\Windows\system32>
```

Nmap

- **Network Mapper** – это бесплатный инструмент безопасности с открытым исходным кодом, используемый для аудита и управления операционной системой и сетевой безопасностью для локальных и удаленных хостов. Используя этот инструмент, мы можем обнаруживать открытые порты на удаленных хостах, сопоставление сети, исследование уязвимостей внутри сети и аудит устройств безопасности.

Wireshark

- **Wireshark** – еще одно бесплатное программное обеспечение с открытым исходным кодом, позволяющее анализировать сетевой трафик в режиме реального времени. У него есть технология сниффинга, благодаря которой вы можете перехватывать и видеть результаты в удобочитаемой форме. Это также сохраняет анализ для автономной работы, делая его более эффективным.

OpenVAS

- **OpenVAS** или **Nessus** – один из лучших сканеров сетевых уязвимостей, используемых для обнаружения удаленных уязвимостей на любых хостах. В основном системные администраторы и специалисты DevOps используют этот инструмент для одновременного сканирования нескольких хостов. Он имеет мощный веб-интерфейс, способный экспортировать все результаты в HTML, XML, LateX и в виде обычного текста.

OpenVAS

- **OpenVAS** — это сканер уязвимостей с открытым исходным кодом. OpenVAS предназначен для активного мониторинга узлов вычислительной сети на предмет наличия проблем, связанных с безопасностью, оценки серьезности этих проблем и для контроля их устранения. Активный мониторинг означает, что OpenVAS выполняет какие-то действия с узлом сети: сканирует открытые порты, посылает специальным образом сформированные пакеты для имитации атаки или даже авторизуется на узле, получает доступ к консоли управления, и выполняет на нем команды. Затем OpenVAS анализирует собранные данные и делает выводы о наличии каких-либо проблем с безопасностью. Эти проблемы, в большинстве случаев касаются установленного на узле необновленного ПО, в котором имеются известные и описанные уязвимости, или же небезопасно настроенного ПО.

Ettercap

- **Ettercap** – еще один известный инструмент для отслеживания пакетов в сетях LAN, способный обрабатывать как активные, так и пассивные сканирования и различные зашифрованные протоколы, такие как SSH и HTTPS. Он выполняет анализ сети и хоста с манипуляциями с сетью по установленным соединениям, упрощая тестирование атак «человек посередине».

Koadic
https://github.com/zerosum0x0/koadic

- Отличительной особенностью Koadic является использование встроенных в Windows интерпретаторов JavaScript и VBScript. В этом смысле он следует тренду living off the land — то есть не имеет внешних зависимостей и пользуется стандартными средствами Windows. Это инструмент для полноценного Command & Control (CnC), поскольку после заражения на машину устанавливается «имплант», позволяющий ее контролировать. Такая машина, в терминологии Koadic, называется «зомби». При нехватке привилегий для полноценной работы на стороне жертвы Koadic имеет возможность их поднять, используя техники обхода контроля учетных записей (UAC bypass).

CrackMapExec (CME)
https://github.com/byt3bl33d3r/CrackMapExec

- Инструмент CME призван в первую очередь автоматизировать те рутинные действия, которые приходится выполнять атакующему для продвижения внутри сети. Он позволяет работать в связке с небезызвестными Empire agent и Meterpreter. Чтобы выполнять команды скрытно, CME может их обфусцировать. Используя Bloodhound (отдельный инструмент для проведения разведки), атакующий может автоматизировать поиск активной сессии доменного администратора.

Bloodhound

- **Bloodhound** как самостоятельный инструмент позволяет вести продвинутую разведку внутри сети. Он собирает данные о пользователях, машинах, группах, сессиях и поставляется в виде скрипта на PowerShell или бинарного файла. Для сбора информации используются LDAP или протоколы, базирующиеся на SMB. Интеграционный модуль CME позволяет загружать Bloodhound на машину жертвы, запускать и получать собранные данные после выполнения, тем самым автоматизируя действия в системе и делая их менее заметными. Графическая оболочка Bloodhound представляет собранные данные в виде графов, что позволяет найти кратчайший путь от машины атакующего до доменного администратора.

Rapid7 Nexpose

- **Rapid7 Nexpose** – это сканер уязвимостей, который выполняет активное сканирование IT-инфраструктуры на наличие ошибочных конфигураций, дыр, вредоносных кодов, и предоставляет рекомендации по их устранению. Под анализ попадают все компоненты инфраструктуры, включая сети, операционные системы, базы данных и web-приложения. По результатам проверки Rapid7 Nexpose в режиме приоритетов классифицирует обнаруженные угрозы и генерирует отчеты по их устранению.

Tenable Nessus Scanner

- **Tenable Nessus Scanner** – это сканер, предназначенный для оценки текущего состояния защищённости традиционной ИТ-инфраструктуры, мобильных и облачных сред, контейнеров и т.д. По результатам сканирования выдаёт отчёт о найденных уязвимостях. Рекомендуется использовать, как составную часть Nessus Security Center.

PT Network Attack Discovery

https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/

- **Positive Technologies Network Attack Discovery — система глубокого анализа сетевого трафика** (NTA) для выявления атак на периметре и внутри сети. PT NAD знает, что происходит в сети, обнаруживает активность злоумышленников даже в зашифрованном трафике и помогает в расследованиях.

Nikto (**сканер веб-сервера**)

https://github.com/sullo/nikto

- **Nikto – это простой открытый сканер веб-серверов, который проверяет веб-сайт и сообщает о найденных уязвимостях, которые могут быть использованы для эксплойта или взлома.** Кроме того, это один из наиболее широко используемых инструментов сканирования веб-сайтов на уязвимости во всей отрасли, а во многих кругах он считается отраслевым стандартом.

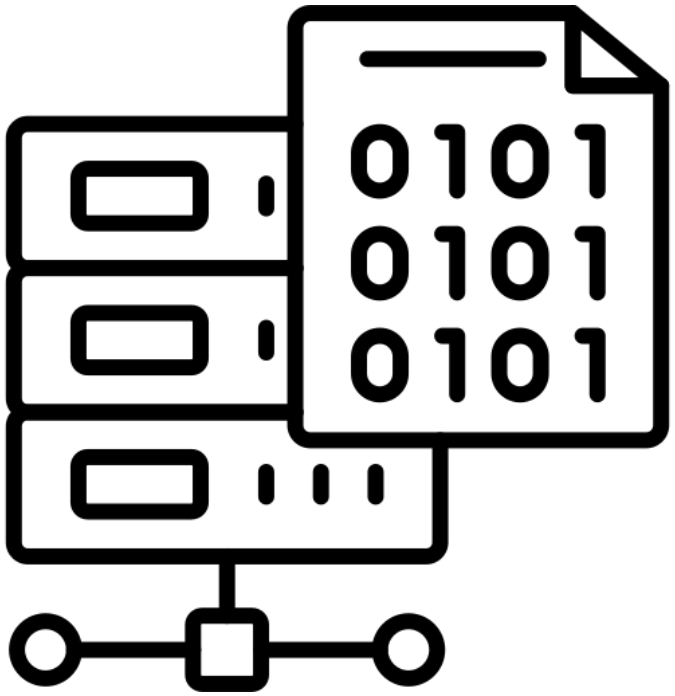
- **Несмотря на то, что этот инструмент чрезвычайно эффективен, он не действует скрытно.** Любой сайт с системой обнаружения вторжений или иными мерами безопасности поймет, что его сканируют. Nikto был разработан для тестирования безопасности и о скрытности его работы никто не задумывался.

Secretsdump

- **Secretsdump** - Это модуль, целью которого могут быть как машины пользователей, так и контроллеры домена. С его помощью можно получать копии областей памяти LSA, SAM, SECURITY, NTDS.dit, поэтому его можно увидеть на разных стадиях атаки. Первым шагом в работе модуля является аутентификация через SMB, для которой необходим либо пароль пользователя, либо его хеш для автоматического проведения атаки Pass the Hash. Далее идет запрос на открытие доступа к Service Control Manager (SCM) и получение доступа к реестру по протоколу winreg, используя который атакующий может узнать данные интересующих его веток и получить результаты через SMB.

Enum_avproducts

- **Enum_avproducts**
- Весьма интересен с точки зрения функциональности и реализации модуль enum_avproducts. WMI позволяет с помощью языка запросов WQL получать данные различных объектов Windows, чем по сути и пользуется этот модуль CME. Он генерирует запросы к классам AntiSpywareProduct и AntiMirusProduct о средствах защиты, установленных на машине жертвы. Для того чтобы получить нужные данные, модуль выполняет подключение к пространству имен root\SecurityCenter2, затем формирует WQL-запрос и получает ответ.



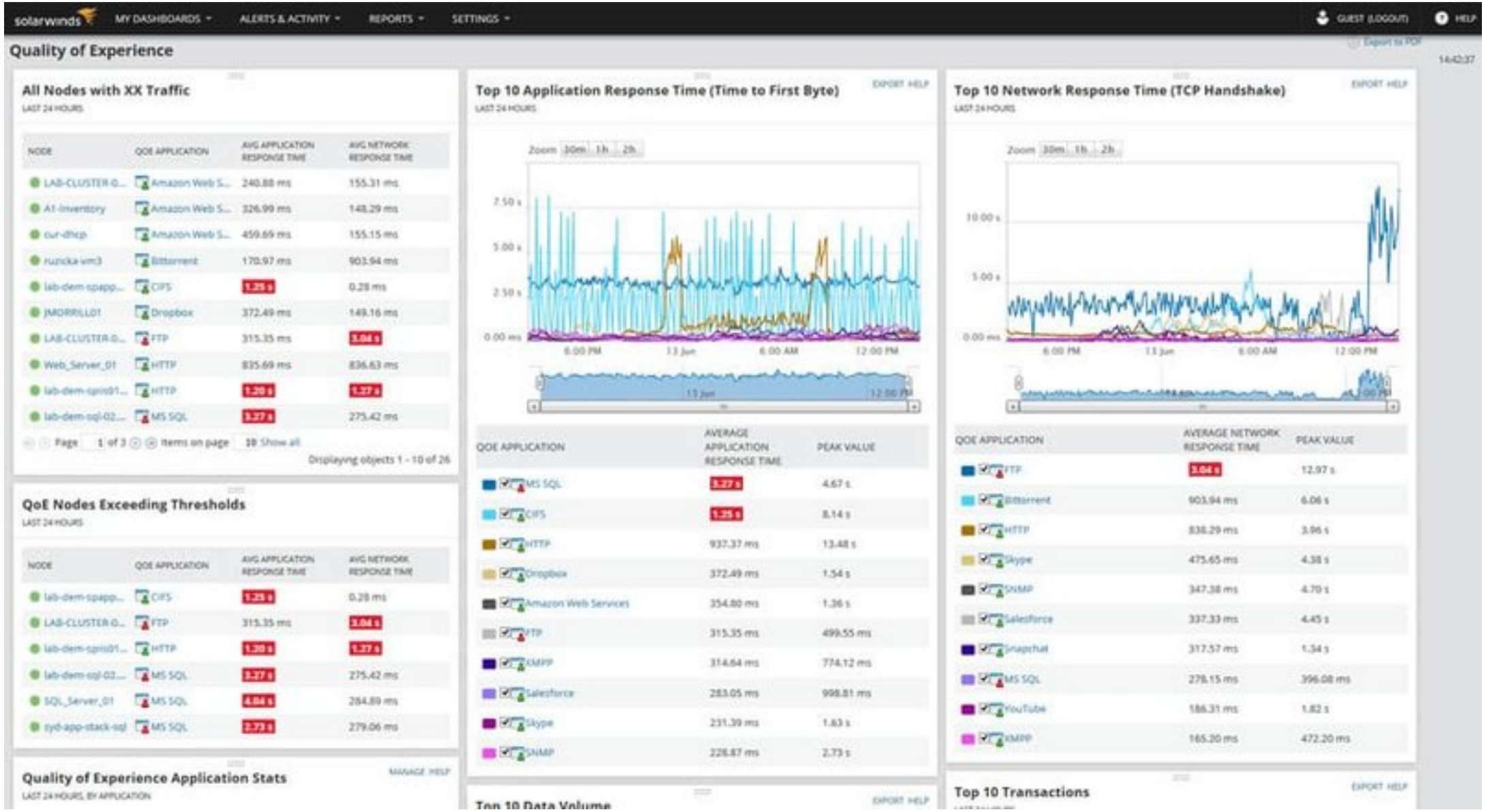
6. Программно-аппаратные средства защиты компьютерных систем

6.11. Программы для анализа сетевого трафика Сниферы пакетов (packet sniffers and network analyzers)

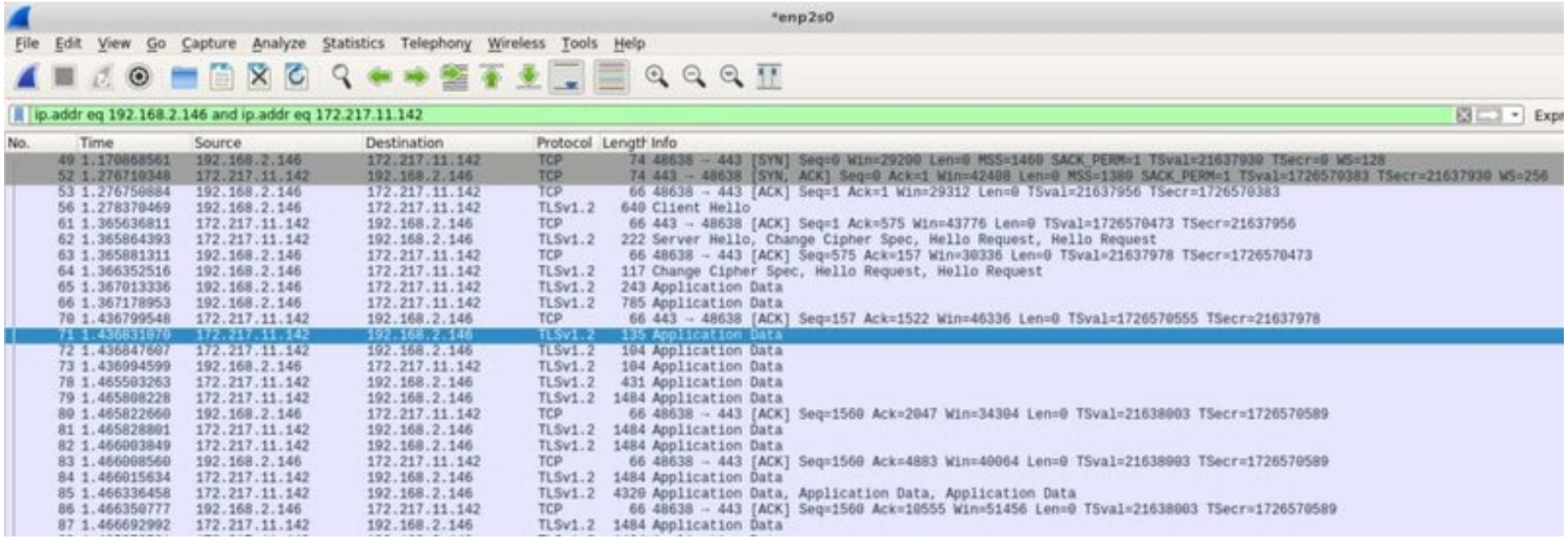
Снифферы пакетов

- SolarWinds
- tcpdump
- Windump
- Wireshark
- tshark
- Network Miner
- Fiddler (HTTP)
- Capsa

SolarWinds

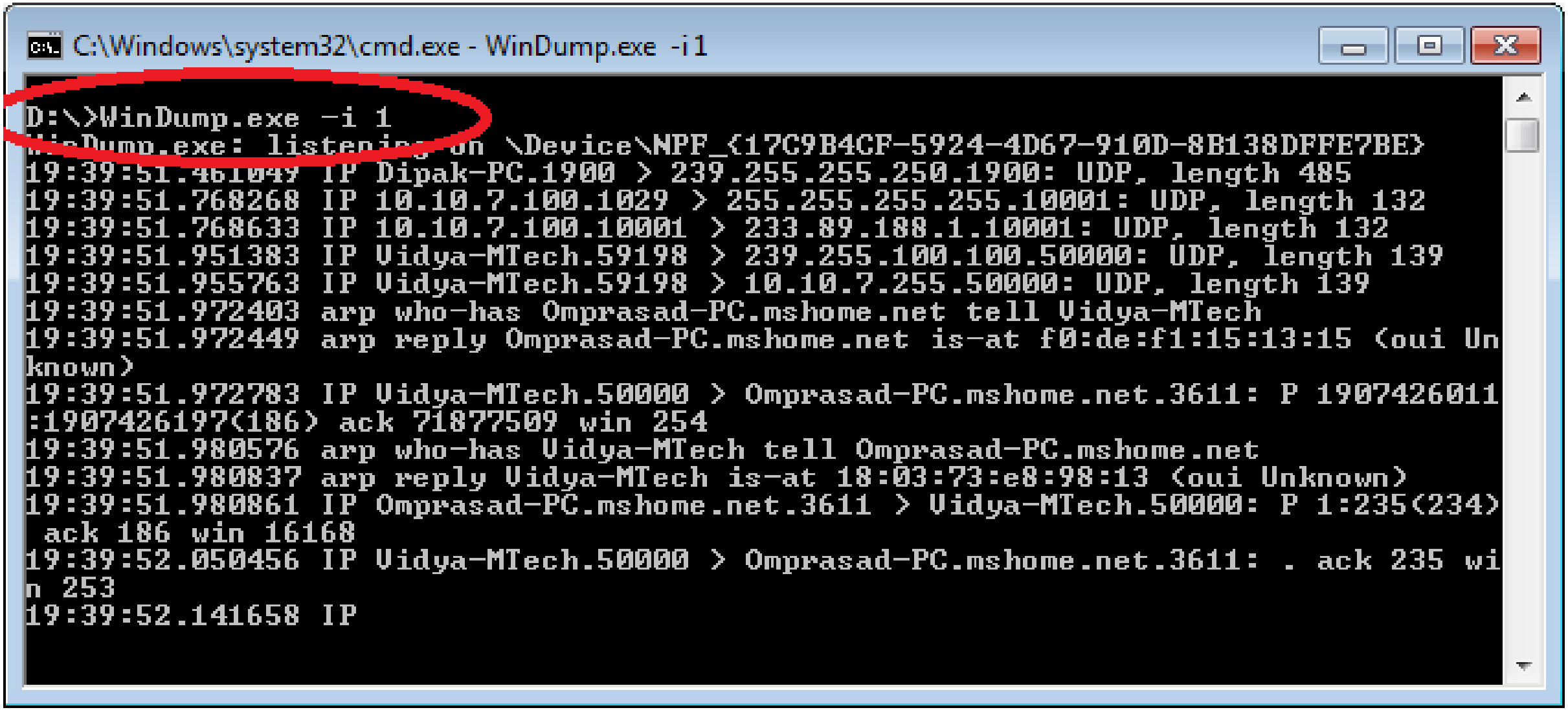

solarwinds
MY DASHBOARDS
ALERTS & ACTIVITY
REPORTS
SETTINGS
GUEST (LOGOUT)
HELP
Quality of Experience
All Nodes with XX Traffic
LAST 24 HOURS
NODE
QOE APPLICATION
AVG APPLICATION RESPONSE TIME
AVG NETWORK RESPONSE TIME
LAB-CLUSTER-0...
Amazon Web S...
240.88 ms
155.31 ms
A1-Inventory
Amazon Web S...
326.99 ms
148.29 ms
our-dhcp
Amazon Web S...
459.69 ms
155.15 ms
ruzicka-vm3
Bittorrent
170.97 ms
903.94 ms
lab-dem-spapp...
CIFS
1.25 s
0.28 ms
JMORRILL01
Dropbox
372.49 ms
149.16 ms
LAB-CLUSTER-0...
FTP
315.35 ms
3.04 s
Web_Server_01
HTTP
835.69 ms
836.63 ms
lab-dem-spnis01...
HTTP
1.20 s
1.27 s
lab-dem-sql-02...
MS SQL
3.27 s
275.42 ms
Page 1 of 3
Items on page 10
Show all
Displaying objects 1 - 10 of 26
QoE Nodes Exceeding Thresholds
LAST 24 HOURS
NODE
QOE APPLICATION
AVG APPLICATION RESPONSE TIME
AVG NETWORK RESPONSE TIME
lab-dem-spapp...
CIFS
1.25 s
0.28 ms
LAB-CLUSTER-0...
FTP
315.35 ms
3.04 s
lab-dem-spnis01...
HTTP
1.20 s
1.27 s
lab-dem-sql-02...
MS SQL
3.27 s
275.42 ms
SQL_Server_01
MS SQL
4.84 s
284.89 ms
syd-app-stack-sql
MS SQL
2.73 s
279.06 ms
Quality of Experience Application Stats
LAST 24 HOURS, BY APPLICATION
MANAGE HELP
Top 10 Application Response Time (Time to First Byte)
LAST 24 HOURS
EXPORT HELP
Zoom 30m 1h 2h
7.50 s
5.00 s
2.50 s
0.00 ms
6:00 PM
13 Jun
6:00 AM
12:00 PM
QOE APPLICATION
AVERAGE APPLICATION RESPONSE TIME
PEAK VALUE
MS SQL
3.27 s
4.67 s
CIFS
1.25 s
8.14 s
HTTP
937.37 ms
13.48 s
Dropbox
372.49 ms
1.54 s
Amazon Web Services
354.80 ms
1.36 s
FTP
315.35 ms
499.55 ms
XMPP
314.64 ms
774.12 ms
Salesforce
283.05 ms
998.81 ms
Skype
231.39 ms
1.63 s
SNMP
228.87 ms
2.73 s
Top 10 Data Volume
EXPORT HELP
Top 10 Network Response Time (TCP Handshake)
LAST 24 HOURS
EXPORT HELP
Zoom 30m 1h 2h
10.00 s
5.00 s
0.00 ms
6:00 PM
13 Jun
6:00 AM
12:00 PM
QOE APPLICATION
AVERAGE NETWORK RESPONSE TIME
PEAK VALUE
FTP
3.04 s
12.97 s
Bittorrent
903.94 ms
6.06 s
HTTP
836.29 ms
3.96 s
Skype
475.65 ms
4.38 s
SNMP
347.38 ms
4.70 s
Salesforce
337.33 ms
4.45 s
Snapchat
317.57 ms
1.34 s
MS SQL
278.15 ms
396.08 ms
YouTube
186.31 ms
1.82 s
XMPP
165.20 ms
472.20 ms
Top 10 Transactions
EXPORT HELP

tcpdump



`Tcpdump` - это приложение с открытым исходным кодом, которое устанавливается практически во всех `Unix`-подобных операционных системах. `Tcpdump` - отличная утилита для сбора данных, которая имеет очень сложный язык фильтрации. Важно знать, как фильтровать данные при их сборе, чтобы в итоге получить нормальный набор данных для анализа. Захват всех данных с сетевого устройства даже в умеренно загруженной сети может породить слишком много данных, которые будет очень трудно проанализировать.

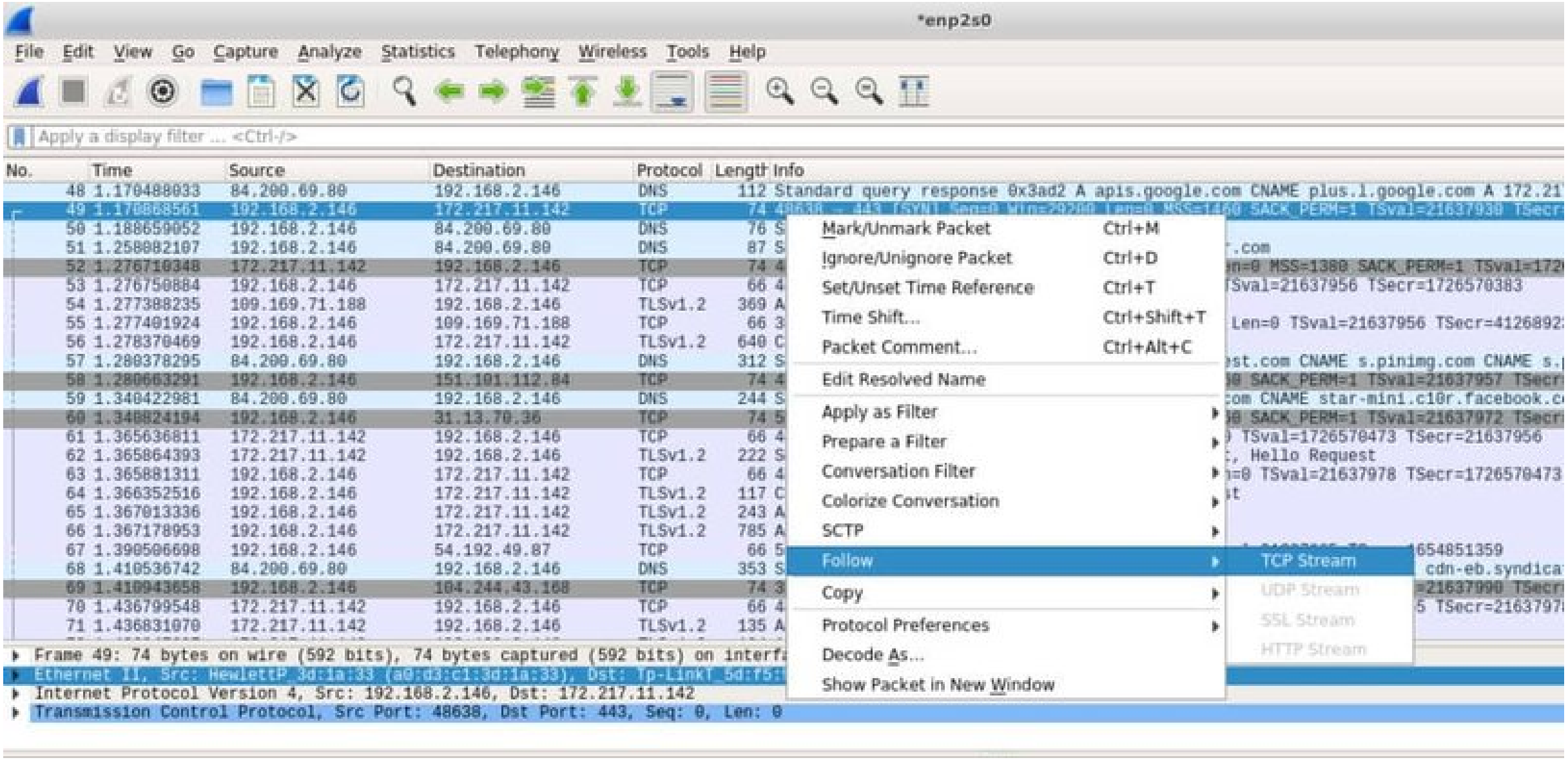
Windump


C:\Windows\system32\cmd.exe - WinDump.exe -i 1
D:\>WinDump.exe -i 1
WinDump.exe: listening on \Device\NPF_{17C9B4CF-5924-4D67-910D-8B138DFFE7BE}
19:39:51.461049 IP Dipak-PC.1900 > 239.255.255.250.1900: UDP, length 485
19:39:51.768268 IP 10.10.7.100.1029 > 255.255.255.255.10001: UDP, length 132
19:39:51.768633 IP 10.10.7.100.10001 > 233.89.188.1.10001: UDP, length 132
19:39:51.951383 IP Vidya-MTech.59198 > 239.255.100.100.50000: UDP, length 139
19:39:51.955763 IP Vidya-MTech.59198 > 10.10.7.255.50000: UDP, length 139
19:39:51.972403 arp who-has Omprasad-PC.mshome.net tell Vidya-MTech
19:39:51.972449 arp reply Omprasad-PC.mshome.net is-at f0:de:f1:15:13:15 (oui Unknown)
19:39:51.972783 IP Vidya-MTech.50000 > Omprasad-PC.mshome.net.3611: P 1907426011:1907426197(186) ack 71877509 win 254
19:39:51.980576 arp who-has Vidya-MTech tell Omprasad-PC.mshome.net
19:39:51.980837 arp reply Vidya-MTech is-at 18:03:73:e8:98:13 (oui Unknown)
19:39:51.980861 IP Omprasad-PC.mshome.net.3611 > Vidya-MTech.50000: P 1:235(234) ack 186 win 16168
19:39:52.050456 IP Vidya-MTech.50000 > Omprasad-PC.mshome.net.3611: . ack 235 win 253
19:39:52.141658 IP

Wireshark

- **Wireshark** является следующим самым известным инструментом в наборе системного администратора. Он позволяет не только захватывать данные, но также предоставляет некоторые расширенные инструменты анализа. Кроме того, Wireshark является программой с открытым исходным кодом и перенесен практически на все существующие серверные операционные системы. Под названием Etheral, Wireshark теперь работает везде, в том числе в качестве автономного переносимого приложения.

Wireshark


*enp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
48 1.170488033 84.200.69.80 192.168.2.146 DNS 112 Standard query response 0x3ad2 A apis.google.com CNAME plus.l.google.com A 172.21
49 1.170868561 192.168.2.146 172.217.11.142 TCP 74
50 1.188659052 192.168.2.146 84.200.69.80 DNS 76
51 1.258082107 192.168.2.146 84.200.69.80 DNS 87
52 1.276710348 172.217.11.142 192.168.2.146 TCP 74
53 1.276750884 192.168.2.146 172.217.11.142 TCP 66
54 1.277388235 109.169.71.188 192.168.2.146 TLSv1.2 369
55 1.277401924 192.168.2.146 109.169.71.188 TCP 66
56 1.278370469 192.168.2.146 172.217.11.142 TLSv1.2 640
57 1.280378295 84.200.69.80 192.168.2.146 DNS 312
58 1.280663291 192.168.2.146 151.101.112.84 TCP 74
59 1.340422981 84.200.69.80 192.168.2.146 DNS 244
60 1.340824194 192.168.2.146 31.13.70.36 TCP 74
61 1.365636811 172.217.11.142 192.168.2.146 TCP 66
62 1.365864393 172.217.11.142 192.168.2.146 TLSv1.2 222
63 1.365881311 192.168.2.146 172.217.11.142 TCP 66
64 1.366352516 192.168.2.146 172.217.11.142 TLSv1.2 117
65 1.367013336 192.168.2.146 172.217.11.142 TLSv1.2 243
66 1.367178953 192.168.2.146 172.217.11.142 TLSv1.2 785
67 1.390506698 192.168.2.146 54.192.49.87 TCP 66
68 1.410536742 84.200.69.80 192.168.2.146 DNS 353
69 1.410943658 192.168.2.146 104.244.43.168 TCP 74
70 1.436799548 172.217.11.142 192.168.2.146 TCP 66
71 1.436831070 172.217.11.142 192.168.2.146 TLSv1.2 135
Frame 49: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interf
Ethernet II, Src: HewlettP 3d:1a:33 (a0:d3:c1:3d:1a:33), Dst: Tp-LinkT 5d:f5:
Internet Protocol Version 4, Src: 192.168.2.146, Dst: 172.217.11.142
Transmission Control Protocol, Src Port: 48638, Dst Port: 443, Seq: 0, Len: 0
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
HTTP Stream

tshark

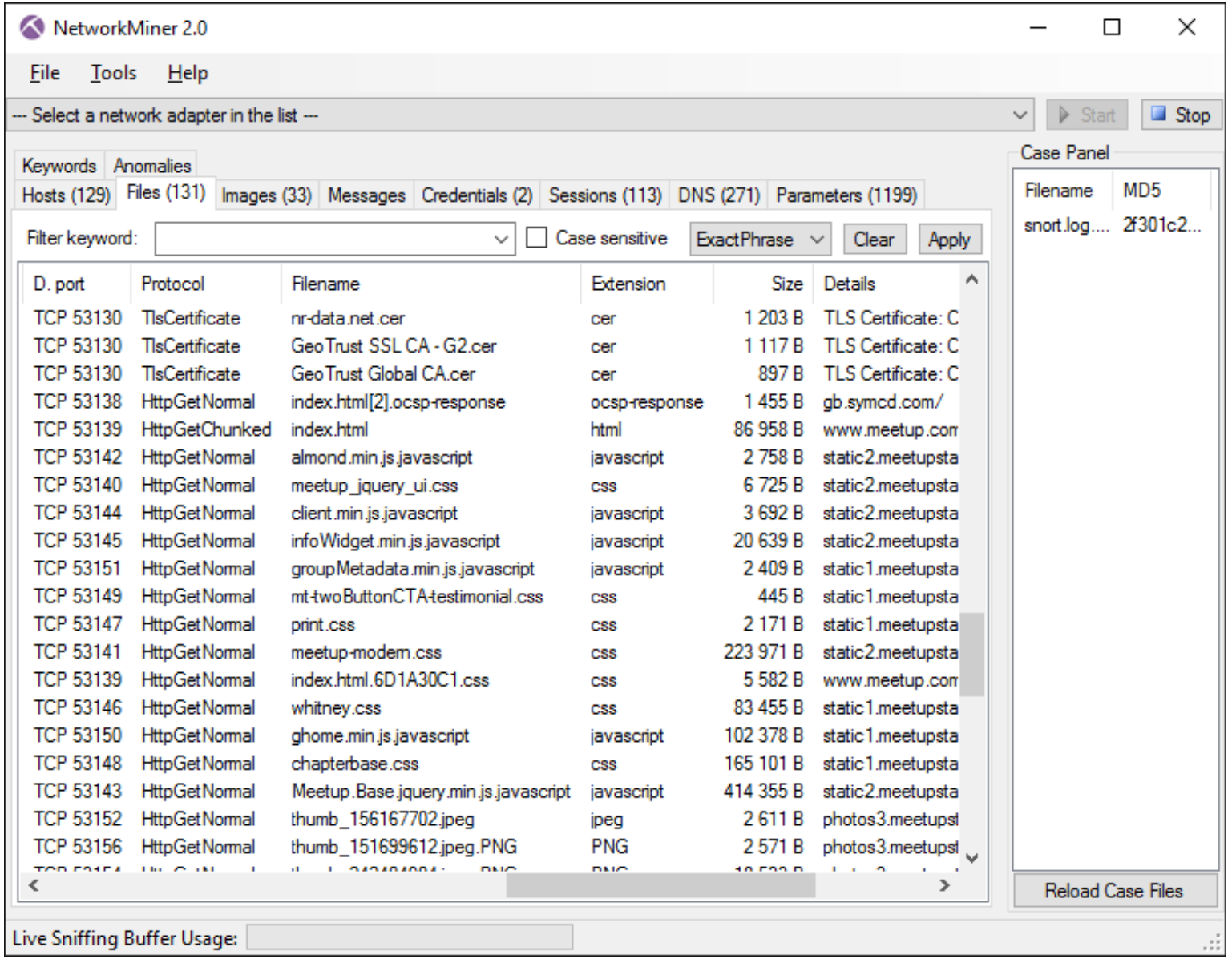
- **Tshark** - это очень полезное звено между tcpdump и Wireshark. Tcpdump превосходит их при сборе данных и может хирургически извлекать только те данные, которые вам нужны, однако его возможности анализа данных очень ограничены. Wireshark отлично справляется как с захватом, так и с анализом, но имеет тяжелый пользовательский интерфейс и не может использоваться на серверах без графического интерфейса. Tshark работает в командной строке.
- Tshark использует те же правила фильтрации, что и Wireshark, что не должно удивлять, так как они по сути являются одним и тем же продуктом.

Network Miner

- **Network Miner** - это очень интересный инструмент, который скорее попадает в категорию инструментов сетевого криминалистического анализа, а не просто снифферов. Сфера криминалистики, как правило, занимается расследованиями и сбором доказательств, и Network Miner выполняет эту работу просто отлично. Также, как wireshark может следовать потоку TCP, чтобы восстановить всю цепочку передачи паков, Network Miner может следовать потоку для того, чтобы восстановить файлы, которые были переданы по сети.

- https://www.netresec.com/index.ashx?page=NetworkMiner

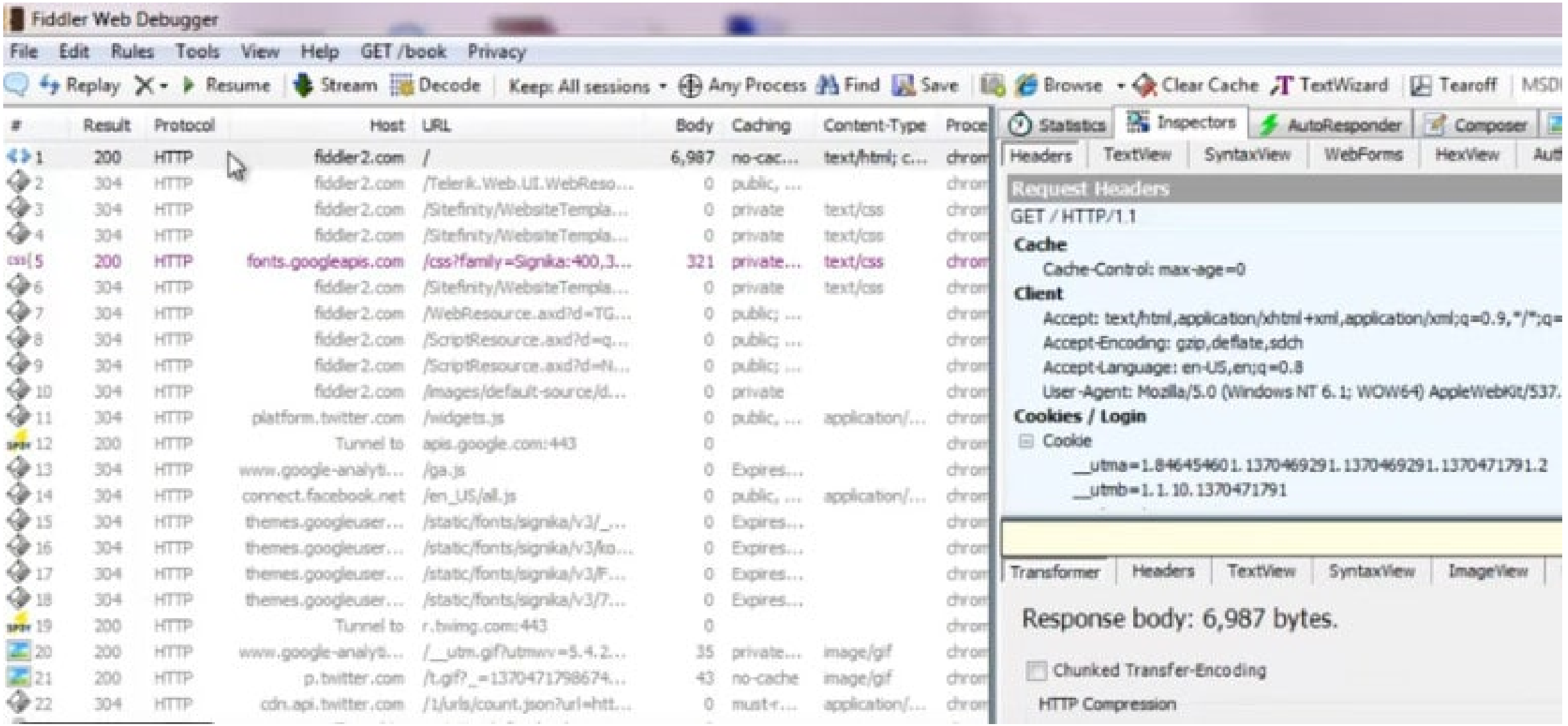
Network Miner



Fiddler (HTTP)

- **Fiddler** технически не является утилитой для захвата сетевых пакетов, но он так невероятно полезен, что попал в этот список. В отличие от других перечисленных здесь инструментов, которые предназначены для захвата трафика в сети из любого источника, Fiddler скорее служит инструментом отладки. Он захватывает HTTP трафик. Хотя многие браузеры уже имеют эту возможность в своих средствах разработчика, Fiddler не ограничивается трафиком браузера. Fiddler может захватить любой HTTP-трафик на компьютере, в том числе и не из веб-приложений.
- https://www.telerik.com/download/fiddler

Fiddler (HTTP)



Capsa

- **Анализатор сети Capsa** имеет несколько редакций, каждая из которых имеет различные возможности. На первом уровне Capsa бесплатна, и она по существу позволяет просто захватывает пакеты и производить их базовый графический анализ. Панель мониторинга уникальна и может помочь неопытному системному администратору быстро определить проблемы в сети. Бесплатный уровень предназначен для людей, которые хотят узнать больше о пакетах, и наращивать свои навыки в анализе.
- https://www.colasoft.com/capsa/
- https://www.colasoft.com/download/products/capsa_free.php

Capsa

Colasoft®
Maximize Network Value

Защита информации

Тема: Сетевые атаки и защита информации в компьютерных сетях

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Белорусско-Российский университет, Кафедра «Программное обеспечение информационных технологий»
Республика Беларусь, Могилев, 2024