ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ЕЛЕКТРОТЕХНИКА И АВТОМАТИКА
гр. София

ДИПЛОМЕН ПРОЕКТ

ТЕМА: ХАРАКТЕРНИ ОСОБЕНОСТИ В ИЗГРАЖДАНЕТО И ПРИЛОЖЕНИЕТО НА **VPN** МРЕЖИТЕ

ДИПЛОМАНТ: **РУМЕН БОЖИДАРОВ ПАВЛОВ**

СПЕЦИАЛНОСТ: код 5230501 **КОМПЮТЪРНА ТЕХНИКА и ТЕХНОЛОГИИ**

ПРОФЕСИЯ: **КОМПЮТЪРЕН ТЕХНИК**

РЪКОВОДИТЕЛ-КОНСУЛТАНТ: **инж. ГЕОРГИ САЧКОВ**

СОФИЯ

2026

ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ЕЛЕКТРОТЕХНИКА И АВТОМАТИКА – гр. СОФИЯ

ЗАДАНИЕ ЗА ДИПЛОМЕН ПРОЕКТ

ДЪРЖАВЕН ИЗПИТ ЗА ПРИДОБИВАНЕ НА ТРЕТА СТЕПЕН НА ПРОФЕСИОНАЛНА КВАЛИФИКАЦИЯ

по професия код
специалност код

На **РУМЕН БОЖИДАРОВ ПАВЛОВ** ученик 12 клас

Тема: *ХАРАКТЕРНИ ОСОБЕНОСТИ В ИЗГРАЖДАНЕТО И ПРИЛОЖЕНИЕТО НА* **VPN** *МРЕЖИТЕ*

Изисквания за разработката на дипломния проект:

Теоретична част:

Практическа част:

График за изпълнение:

а) дата на възлагане на дипломния проект .....

б) контролни проверки и консултации 27.01.202 .

25.02.202. .

25.03.202 .

10.04.202 .

в) краен срок за предаване на дипломния проект 15.04.202 .

Ученик: **РУМЕН БОЖИДАРОВ ПАВЛОВ** .....
(име, фамилия) *(подпис)*

Ръководител-консултант: инж. .....
(име, фамилия) *(подпис)*

Директор: инж. ФИЛИП ФИЛИПОВ .....
(име, фамилия)

Съдържание

ТЕОРЕТИЧЕСКА ЧАСТ

УВОД

В условията на бързо развиващите се информационни технологии компютърните мрежи са основа за работата на почти всяка организация – от малки фирми до големи корпорации и държавни институции. Все по-често бизнес процесите разчитат на облачни услуги, централизирани системи за управление, отдалечени работни места и мобилни устройства. Това води до непрекъснато увеличаване на обема от пренасяни данни през публични мрежи, най-вече интернет. Публичната инфраструктура обаче е среда с повишен риск, тъй като трафикът може да бъде прихванат, анализиран или променен от злонамерени лица, както и да бъде наблюдаван от междинни доставчици.

В този контекст виртуалните частни мрежи (VPN – Virtual Private Network) са утвърдено решение за изграждане на защитени комуникационни канали и контролиране на достъпа до вътрешни ресурси. VPN създава логически „тунел“, чрез който данните се пренасят криптирано и автентично – така, сякаш устройствата се намират в една и съща локална мрежа, въпреки че са физически отдалечени.

Актуалността на темата се засилва и от тенденции като дистанционна работа, използване на публични Wi-Fi мрежи, работа в хибридни облачни среди и нужда от свързване на множество филиали към централна инфраструктура. В тези случаи VPN позволява достъп до корпоративни системи (файлови сървъри, ERP/CRM, бази данни, вътрешни уеб портали) без необходимост от откриване на тези услуги директно към интернет.

Обект на изследването са компютърните мрежи и средствата за осигуряване на сигурна комуникация. Предмет на изследването са принципите на изграждане, функциониране и приложение на VPN

мрежите, както и основните протоколи и компоненти, които ги реализират.

Целта на дипломния проект е да се анализират характерните особености при изграждането и използването на VPN мрежи, като се разгледат основните типове VPN (Site-to-Site и отдалечен достъп), принципът на действие, широко използваните протоколи, както и ролята на VPN сървърите и клиентите.

Задачите на проекта включват:

- да се дефинира същността на VPN и основните цели – поверителност, цялост, автентичност и контрол на достъпа;
- да се класифицират основните типове VPN и да се сравнят по предназначение и архитектура;
- да се опише принципът на тунелиране и криптиране, включително ключови понятия като тунел, капсулиране и маршрутизация;
- да се разгледат основни VPN протоколи (IPsec/IKEv2, OpenVPN, WireGuard, L2TP, PPTP и др.) и техните особености;
- да се анализират VPN сървъри и VPN клиенти – роли, функции, параметри за конфигурация и практическо приложение;
- да се обобщят рискове, ограничения и добри практики при внедряване на VPN решения.

Използваната методика включва анализ и обобщение на техническа литература, стандарти (RFC) и официална документация на водещи решения, както и сравнение на протоколи по отношение на сигурност и производителност.

1. СЪЩНОСТ, ОСНОВНИ ПОНЯТИЯ И ЦЕЛИ НА VPN

VPN (виртуална частна мрежа) е технология за изграждане на логически защитена връзка върху публична мрежова инфраструктура. Терминът „виртуална“ означава, че частната свързаност не изисква отделна физическа линия, а се реализира чрез софтуерни механизми за тунелиране, криптиране и контрол на достъпа. „Частна“ означава, че връзката е предназначена за ограничен кръг участници (организация/потребители) и се защитава от неоторизиран достъп.

На практика VPN позволява създаване на „оверлей“ (overlay) мрежа върху интернет. Това е особено полезно, когато трябва да се осигури сигурна комуникация между отдалечени точки (офиси, потребители, облачни ресурси), без да се изгражда скъпа частна физическа инфраструктура.

Основните цели на VPN могат да се разгледат и през класическата призма на информационната сигурност (CIA триада – Confidentiality, Integrity, Availability), като при VPN най-силно са изразени поверителността и цялостта. Достъпността също е важна, защото VPN често е „входна точка“ към критични ресурси. Една нестабилна или слабо защитена VPN инфраструктура може да доведе до прекъсване на работата, затруднена дистанционна работа и дори до пробив в сигурността.

1.1. Основни понятия

Тунел (tunnel) – логически канал, през който трафикът преминава капсулиран и обикновено криптиран.

Endpoint (крайна точка) – устройство/шлюз, което терминира тунела (клиент или сървър/шлюз).

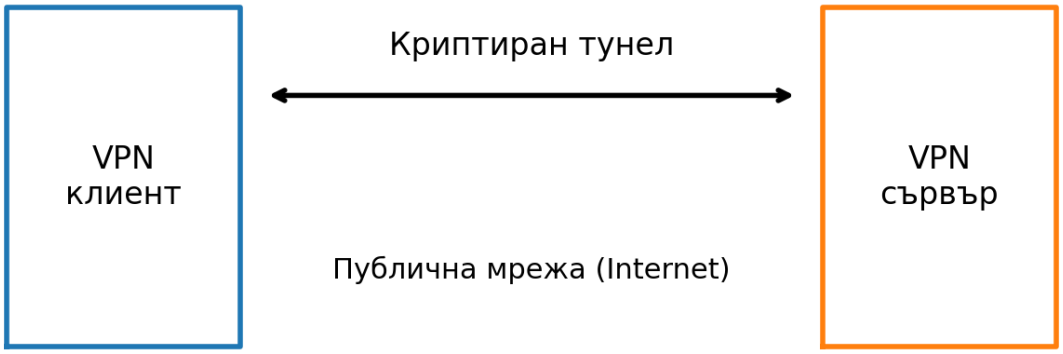
Капсулиране (encapsulation) – добавяне на външни заглавки към пакета, за да може той да бъде пренесен през друга мрежа.

Криптиране (encryption) – преобразуване на данните в нечетим вид за неоторизирани лица чрез криптографски алгоритми.

Автентикация (authentication) – доказване на самоличността на потребителя или устройството.

Упълномощаване (authorization) – определяне какви ресурси и услуги са достъпни след успешна автентикация.

Security Association (SA) – в контекста на IPsec: набор от параметри (алгоритми, ключове, срокове), определящи как се защитава трафикът.



Фигура 1. VPN връзка клиент–сървър: криптиран тунел през публична мрежа

1.2. Защо VPN е нужен при съвременни заплахи

Публичните мрежи са подложени на различни заплахи: подслушване (sniffing), атаки тип „man-in-the-middle“, подмяна на DNS отговори, компрометиране на точки за достъп, фишинг и др. При некриптирани връзки нападател може да прочете съдържанието или да го промени. VPN не заменя защитата на приложно ниво (например HTTPS), но добавя допълнителен слой защита и позволява централен контрол върху достъпа и политиките.

2. ТИПОВЕ VPN И СЦЕНАРИИ НА ПРИЛОЖЕНИЕ

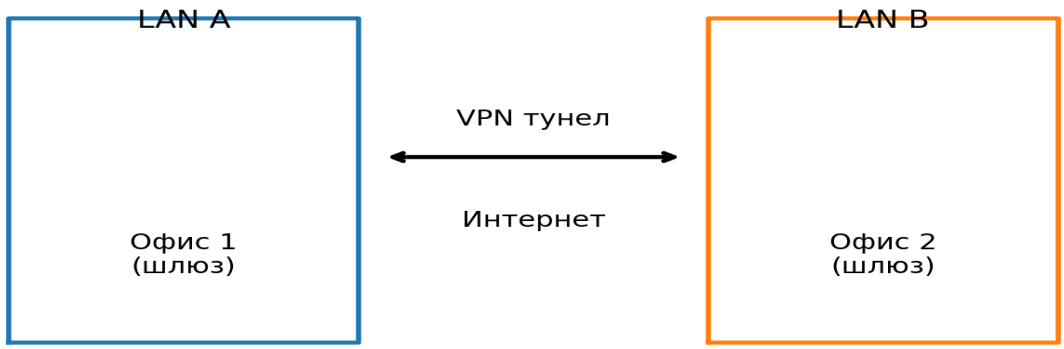
Класификацията на VPN може да се направи по предназначение (корпоративен/личен), по архитектура (клиент–сървър или мрежа–към–мрежа), по използван протокол (IPsec, TLS/SSL, WireGuard), по слой (L2 или L3) и по модел на предоставяне (самостоятелно управляван VPN или услуга от доставчик).

Най-често в учебната и практическата литература се разграничават Site-to-Site и Remote Access VPN. Към тях можем да добавим и модели, при които доставчикът осигурява виртуална сегментация в своята мрежа (MPLS VPN).

2.1. Site-to-Site VPN (мрежа–към–мрежа)

Site-to-Site VPN се използва за свързване на цели локални мрежи. Два VPN шлюза (напр. firewall устройства) установяват постоянна или полу-постоянна защитена връзка. Трафикът между подмрежите се криптира на изхода на едната мрежа и се декриптира на входа на другата. Това позволява приложенията да работят прозрачно (например файлови услуги, вътрешни DNS, домейн контролери).

В практиката Site-to-Site VPN се реализира най-често с IPsec в тунелен режим, но е възможно и с OpenVPN или WireGuard.



Фигура 2. Site-to-Site VPN: свързване на две локални мрежи чрез VPN шлюзове

2.2. Remote Access VPN (отдалечен достъп)

Remote Access VPN е ориентиран към индивидуални потребители/устройства. Клиентът установява тунел към VPN сървър, след което получава виртуален IP адрес и правила за маршрутизация. В зависимост от политиката, клиентът може да достъпва само конкретни услуги (например RDP към един сървър) или по-широк набор от вътрешни ресурси.

Корпоративните решения често интегрират Remote Access VPN с централизирана идентичност (Active Directory), като прилагат групови политики и MFA.

2.3. Host-to-Host VPN и микросегментация

Освен класическите модели, съществуват и решения за „host-to-host“ VPN, при които се защитават връзки между конкретни машини. Това е полезно при микросегментация и Zero Trust подходи, където идеята е да се ограничи латералното движение в мрежата и да се разрешават само строго дефинирани комуникации.

2.4. Provider-Provisioned VPN и MPLS

При MPLS L3VPN доставчикът на свързаност изгражда виртуално отделени маршрутизиращи домейни (VRF) за клиента. Така трафикът на различни клиенти е изолиран в мрежата на оператора. Този модел е удобен за големи организации, които искат управляеми връзки между обекти и гарантирано качество на услугата (QoS). Ако се изисква криптографска поверителност, върху MPLS може да се добави IPsec тунел.

3. ПРИНЦИП НА ДЕЙСТВИЕ: ТУНЕЛИРАНЕ, КРИПТОГРАФИЯ И МАРШРУТИЗАЦИЯ

3.1. Етапи при установяване на VPN връзка

Независимо от конкретния протокол, установяването на VPN връзка обикновено включва:

(1) иницииране – клиентът се свързва към VPN сървър (IP/домейн и порт);

(2) автентикация – идентичност чрез парола, сертификат, токен или MFA;

(3) договаряне на параметри – избор на алгоритми и създаване на сесийни ключове;

(4) създаване на виртуален интерфейс – TUN/TAP или еквивалентен механизъм;

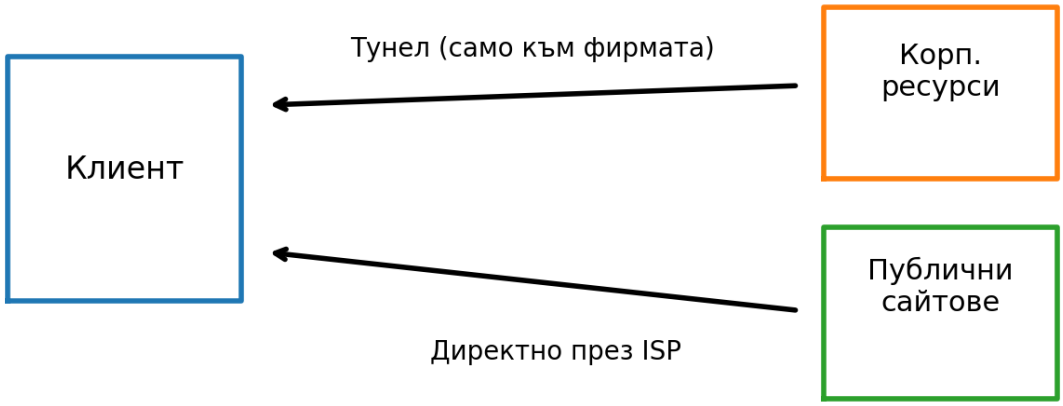
(5) прилагане на маршрути и политики – кой трафик минава през VPN;

(6) обмен на данни – криптиране/декриптиране и проверка на целостта;

(7) поддържане – keepalive, ротация на ключове, прекратяване при проблем.

3.2. Full tunnel и Split tunneling

Full tunnel означава целият изходящ трафик на клиента да бъде пренасочен през VPN. Това улеснява контрола и филтрацията, но може да натовари VPN шлюза и да увеличи латентността. Split tunneling пренасочва през VPN само трафика към вътрешните мрежи. Това е по-ефективно, но изисква силни политики за сигурност на крайното устройство.



Фигура 3. Split-tunneling: фирменият трафик минава през VPN, а публичният – директно

3.3. MTU, overhead и фрагментация

Тунелирането добавя допълнителни заглавки и криптографски полета към пакетите, което увеличава размера им (overhead). Ако размерът надвиши MTU по пътя, може да се стигне до фрагментация или загуба на пакети. Затова в практиката често се настройват MTU/MSS параметри за тунела, така че да се избегне фрагментация и да се подобри производителността.

4. VPN ПРОТОКОЛИ

4.1. IPsec и IKEv2

IPsec е стандартен набор от протоколи за защита на IP трафика на ниво мрежа. Основният протокол за защита на данните е ESP, който може да осигурява криптиране и целостта на пакета. За установяване на ключове и параметри се използва IKE, като IKEv2 е актуален стандарт (RFC 7296). IKEv2 управлява създаването и поддържането на Security Associations, както и процесите по автентикация и обновяване на ключовете.

IPsec може да работи в transport и tunnel режим. Tunnel режимът е типичен за Site-to-Site, защото скрива вътрешния IP пакет и позволява пренасяне на цели подмрежи. При NAT по пътя се използва NAT-Traversal (обикновено UDP 4500) за да се избегнат проблеми с ESP и състоянието на NAT устройствата.

4.2. OpenVPN

OpenVPN използва TLS за автентикация и обмен на ключове и може да пренася тунелен трафик през UDP или TCP. Силата му е гъвкавата конфигурация и широката поддръжка на платформи. OpenVPN разделя контролен канал (за договаряне) и канал за данни (за пренос на криптирани пакети). Може да работи на L3 (TUN) или L2 (TAP), което е важно за специфични сценарии.

4.3. WireGuard

WireGuard се отличава с минималистичен дизайн и фиксиран набор от модерни криптографски примитиви. Работи на Layer 3 и използва UDP. Конфигурацията е относително проста – базира се на публични ключове и разрешени IP мрежи за всеки peer. Това улеснява управлението и намалява риска от грешки при избор на шифри. WireGuard е известен с висока производителност и бързо установяване на връзка.

4.4. L2TP/IPsec и PPTP

L2TP сам по себе си е протокол за тунелиране и затова се комбинира с IPsec за криптиране. Поради вградената поддръжка в много операционни системи, L2TP/IPsec се използва често за Remote Access. PPTP е по-стар протокол с известни слабости и днес не се препоръчва за сигурни среди.

4.5. TLS VPN (SSL VPN) и SSTP

TLS-базираните VPN решения използват TLS по подобие на HTTPS. Предимството е лесното преминаване през защитни стени, особено когато се използва TCP 443. SSTP е пример за такъв подход в Windows среда. Недостатък може да бъде по-висока латентност и „TCP over TCP“ ефекти, ако тунелът пренася TCP трафик върху TCP транспорт.

4.6. Сравнителна таблица на основни протоколи

Протокол	Слой	Сигурност	Съвместимост	Типични случаи
IPsec/IKEv2	L3	Много висока (при добра конфигурация)	Отлична в корпоративни мрежи	Site-to-Site, Remote
OpenVPN	L3/L2	Висока (TLS, сертификати)	Много добра	Remote, Site-to-Site
WireGuard	L3	Висока (modern crypto)	Много добра (нови OS)	Remote, Site-to-Site
L2TP/IPsec	L2+L3	Висока (чрез IPsec)	Вградено в много OS	Remote
PPTP	L2	Ниска/остаряла	Намаляваща	Само при ниски изисквания

5. VPN СЪРВЪРИ И VPN КЛИЕНТИ

5.1. VPN сървър/шлюз

VPN сървърът е компонентът, който приема и управлява VPN връзки. В корпоративни среди той често е част от firewall/UTM устройство или специализиран концентратор. Основни функции са: автентикация и авторизация на потребители, договаряне на криптографски параметри, създаване на виртуални интерфейси,

раздаване на IP адреси, прилагане на маршрути и политики, както и логване и мониторинг.

5.2. VPN клиент

VPN клиентът е софтуер на крайното устройство, който установява връзката, управлява ключове/сертификати, създава виртуален интерфейс и прилага маршрути. Клиентът може да е вграден в операционната система (например IKEv2), или външно приложение (OpenVPN, WireGuard). Корпоративните клиенти често включват допълнителни функции като „always-on“ режим, проверка на състоянието на устройството и автоматично обновяване на конфигурацията.

5.3. Автентикация и управление на идентичности

Най-често използваните методи за удостоверяване са: потребител/парола, сертификати, предварително споделени ключове (PSK) и многофакторна автентикация. Добра практика е използването на MFA, особено за отдалечен достъп. Възможни са интеграции с RADIUS, LDAP/AD и SSO решения.

6. СИГУРНОСТ И ДОБРИ ПРАКТИКИ

6.1. Рискове при неправилна конфигурация

Основните рискове включват: слаби пароли и липса на MFA, остарели протоколи/шифри, недостатъчна сегментация, неправилни маршрути (leaks), DNS течове, както и липса на централен мониторинг. При split-tunneling без контрол компрометирано устройство може да стане мост между интернет и корпоративната мрежа.

6.2. Практически препоръки

- Използване на съвременни протоколи (IKEv2/IPsec, OpenVPN, WireGuard) и изключване на PPTP.

- MFA за всички потребители с отдалечен достъп, особено администратори.
- Сегментация: достъп само до нужните ресурси (принцип на най-малки привилегии).
- Редовни обновявания и ротация на ключове/сертификати; забрана на слаби cipher suites.
- Логове и мониторинг (SIEM/IDS), аларми при аномалии и множество неуспешни опити.
- Оптимизация на MTU/MSS и избор на UDP транспорт при възможност.

6.3. Производителност

Скоростта на VPN зависи от криптографските алгоритми и наличието на хардуерно ускорение, от натоварването на сървъра, качеството на интернет връзката и настройките на тунела. При планиране се оценяват брой едновременни потребители, необходима пропускателна способност и възможности за резервираност (high availability).

7. ПРИЛОЖЕНИЕ И ТЕНДЕНЦИИ

VPN технологията остава ключова, но все по-често се комбинира с концепции като Zero Trust. При този подход се добавят допълнителни контекстни проверки (идентичност, устройство, местоположение), а достъпът е динамичен и минимален. Въпреки това VPN продължава да бъде базов инструмент за изграждане на защитен канал през публични мрежи, особено при свързване на офиси и осигуряване на сигурна дистанционна работа.

8. ДЕТАЙЛЕН ПРЕГЛЕД НА IPsec: КОМПОНЕНТИ, РЕЖИМИ И ПОЛИТИКИ

8.1. Архитектура на IPsec: AH, ESP, SPD и SAD

IPsec не е единичен протокол, а архитектура от механизми и правила, които работят на мрежово ниво. Основните му елементи са:

• AH (Authentication Header) – добавя заглавка, която осигурява автентичност и цялост на пакета. AH не криптира полезния товар и на практика се използва по-рядко, защото ESP може да осигури и целостта.

• ESP (Encapsulating Security Payload) – добавя защита на полезния товар чрез криптиране и/или автентичност. В реални внедрявания ESP е стандартният избор за VPN тунели.

IPsec използва и логически бази данни/таблици (концептуално):

• SPD (Security Policy Database) – политика, която определя кои пакети подлежат на защита, какъв тип защита и към кои крайни точки.

• SAD (Security Association Database) – съдържа активните Security Associations (SA) – параметри като алгоритми, ключове, SPI идентификатори, срокове и броячи.

Този модел позволява гъвкаво управление: една част от трафика може да бъде защитена (например между подмрежи), а друга – да се пропуска без IPsec, според изискванията.

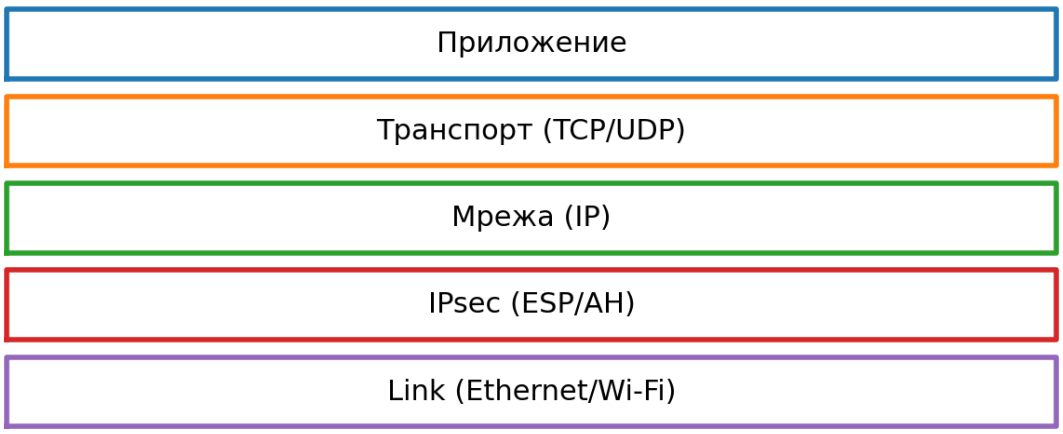
8.2. Transport mode и Tunnel mode – практическо значение

В transport mode защитата се прилага върху полезния товар на оригиналния IP пакет, а оригиналният IP header остава видим. Това е подходящо при комуникация между два конкретни хоста (например сървър–сървър), когато няма нужда да се скриват вътрешните адреси.

В tunnel mode оригиналният IP пакет се капсулира и се добавя нов външен IP header. Така вътрешната адресация и съдържанието са

защитени и невидими за интернет. Това е типичният режим за Site-to-Site VPN, защото позволява пренасяне на трафик между цели подмрежи, като междинните устройства виждат само външните адреси на VPN шлюзовете.

При планиране на IPsec VPN е важно да се отчете, че tunnel mode увеличава overhead-а (добавя нов IP header), което влияе на MTU и може да наложи настройка на MSS/fragmentation.



Фигура 4. Мястото на IPsec в мрежовия стек: защита на IP трафика на ниво 3

8.3. IKEv2 процес: установяване на SA и обновяване на ключове

IKEv2 е протоколът, който управлява жизнения цикъл на IPsec тунела: договаря алгоритми, удостоверява страните и създава ключовете. В опростен вид процесът включва:

• IKE_SA_INIT – обмен на криптографски параметри и Diffie-Hellman стойности за създаване на обща тайна.

• IKE_AUTH – взаимна автентикация (сертификати/PSK/EAP) и установяване на първата Child SA (обикновено за ESP).

След установяване IKEv2 поддържа тунела чрез:

• rekey – периодично обновяване на ключове (важно за ограничаване на риска при компрометиране);

• MOBIKE (в определени внедрявания) – по-добра работа при смяна на IP адрес (роуминг);

• Dead Peer Detection/keepalives – откриване на отпаднали крайни точки.

Практически IKEv2 обикновено работи на UDP 500 и при NAT-Traversal на UDP 4500.

9. ДЕТАЙЛЕН ПРЕГЛЕД НА OpenVPN: АРХИТЕКТУРА, РЕЖИМИ И КРИПТОГРАФИЯ

9.1. Контролен и канал за данни

OpenVPN използва TLS за контролния канал – в него се извършва удостоверяване на клиента и сървъра, обмен на ключове и разпределяне на конфигурация (например виртуален IP адрес, маршрути, DNS настройки). След успешна TLS сесия се установява каналът за данни, през който реалният трафик се пренася криптирано.

Това разделение позволява гъвкавост: контролният канал може да използва надежден транспорт, докато каналът за данни (особено върху UDP) може да бъде оптимизиран за минимална латентност.

9.2. TUN срещу TAP режим

OpenVPN може да работи в два режима:

• TUN (Layer 3) – създава виртуален IP интерфейс. Подходящ за класически маршрутизиран VPN (най-често срещан).

• TAP (Layer 2) – създава виртуален Ethernet интерфейс и позволява пренос на broadcast/ARP кадри. Полезно при специфични сценарии (например когато трябва да се „разтегне“ LAN сегмент), но може да бъде по-тежко като трафик и по-сложно за мащабиране.

Изборът между TUN и TAP влияе на производителността, сложността и възможностите за сегментация.

9.3. Предимства и ограничения

Предимства на OpenVPN:

• широка поддръжка и зрялост на решението;

• богати механизми за автентикация и интеграция (сертификати, потребител/парола, MFA);

• възможност за работа върху UDP или TCP и лесно преминаване през NAT/Firewall;

• детайлна конфигурация и възможност за централен контрол.

Ограничения:

• по-голяма сложност на конфигурацията в сравнение с WireGuard;

• възможни проблеми при „TCP over TCP“, ако се използва TCP транспорт;

• производителността зависи от криптографския стек и настройките.

10. ДЕТАЙЛЕН ПРЕГЛЕД НА WireGuard: ПРОТОКОЛ, КОНФИГУРАЦИЯ И ОСОБЕНОСТИ

10.1. Концепция за peers и AllowedIPs

WireGuard работи с модел peer-to-peer: всяка крайна точка има ключова двойка (public/private) и списък с разрешени IP мрежи (AllowedIPs) за всеки peer. AllowedIPs играе двойна роля: (1) определя какъв трафик се маршрутизира през дадения тунел и (2) ограничава какви адреси peer-ът може да използва, което добавя елемент на контрол.

Конфигурацията е кратка, но изисква внимателно планиране на адресацията (например отделна „VPN“ подмрежа) и правилно разпределяне на AllowedIPs.

10.2. Криптографски избори и простота

WireGuard използва фиксирани, съвременни примитиви (например ChaCha20-Poly1305 и Noise handshake), което премахва необходимостта от сложен избор на cipher suites. Това намалява риска от грешки и улеснява одита. От друга страна, по-малката гъвкавост означава, че администраторът трябва да разчита на вградените решения на протокола, вместо да настройва специфични алгоритми.

10.3. Работа при роуминг и NAT

Практическо предимство на WireGuard е добрата работа при смяна на IP адрес (например мобилни устройства). Понеже протоколът е изцяло върху UDP и използва периодични „keepalive“ пакети, връзката може да се поддържа и през NAT. Често се използва постоянен публичен адрес/порт на сървъра и динамични клиенти.

11. УПРАВЛЕНИЕ НА VPN ИНФРАСТРУКТУРА: СЕРТИФИКАТИ, ПОЛИТИКИ, МОНИТОРИНГ

11.1. PKI и жизнен цикъл на сертификатите

При протоколи, които използват сертификати (IPsec с X.509, OpenVPN с TLS), управлението на PKI е централно. Включва:

• създаване на вътрешен CA (Certificate Authority) или използване на външен;

• издаване на клиентски сертификати за устройства/потребители;

• подновяване и отнемане (revocation) при загубени устройства или напуснали служители;

• защита на private ключове (например чрез TPM/secure storage).

Липсата на управление на отнемането може да доведе до ситуация, при която компрометиран сертификат остава валиден и предоставя достъп.

11.2. Политики за достъп и сегментация

Ефективният VPN не означава „пълен достъп до всичко“. В практиката се прилагат:

• групи потребители (например „служители“, „администратори“, „външни партньори“);

• политики по подмрежи и услуги (достъп само до конкретни VLAN/сървъри);

• split DNS и вътрешни домейни;

• time-based и context-based ограничения (когато е възможно).

Така се минимизира рискът при компрометиране на един акаунт.

11.3. Логове, SIEM и откриване на атаки

VPN инфраструктурата е цел за атаки, тъй като често е публично достъпна. Затова е важно:

• да се събират логове за успешни и неуспешни опити за вход;

• да се следят геолокации/аномалии (например вход от необичаен регион);

• да се анализира трафикът за подозрителни модели (IDS/IPS);

• да се интегрира със SIEM за корелация на събития.

12. ОГРАНИЧЕНИЯ НА VPN И ЧЕСТИ ГРЕШКИ

12.1. VPN ≠ пълна анонимност

VPN криптира трафика между клиента и VPN сървъра, но не „прави потребителя невидим“. След изхода от VPN сървъра трафикът продължава към крайните сайтове/услуги, където могат да се използват други механизми за проследяване. Освен това доставчикът на VPN има техническа възможност да наблюдава трафика след декриптиране

(освен ако той е допълнително защитен, например чрез HTTPS). Поради това е важно да се избира надежден VPN доставчик или да се използва самостоятелно управлявана инфраструктура в организации.

12.2. Чести проблеми при внедряване

• Конфликтни IP адреси между офиси (две LAN мрежи със същата адресация).

• Липса на ясни маршрути – трафикът се „губи“ или се връща по грешен път.

• MTU проблеми – „някои сайтове работят, други не“ поради фрагментация.

• DNS течове – вътрешни домейни не се резолват или се резолват през публичен DNS.

• Неправилно отворени портове/Firewall правила – тунелът се установява, но няма трафик.

Решаването изисква систематична диагностика: проверка на маршрути, MTU, DNS, логове и политики.

КРАТЪК РЕЧНИК НА ТЕРМИНИТЕ (GLOSSARY)

CIA – Confidentiality, Integrity, Availability (поверителност, цялост, достъпност).

MFA – Multi-Factor Authentication (многофакторна автентикация).

NAT-T – NAT Traversal (механизъм за преминаване на IPsec през NAT).

TUN/TAP – виртуални интерфейси за пренасяне на IP (TUN) или Ethernet (TAP) трафик.

SA – Security Association (IPsec „договор“ за защита).

PKI/CA – инфраструктура за публични ключове/сертифициращ орган.

Split tunneling – маршрутизация, при която само част от трафика минава през VPN.

ЗАКЛЮЧЕНИЕ

В теоретичната част бяха разгледани основните концепции при VPN мрежите: същност, типове, принцип на действие и ключови протоколи. Сравнението показва, че протоколи като IKEv2/IPsec, OpenVPN и WireGuard са най-подходящи за съвременни изисквания. За да бъде VPN ефективен, е необходимо правилно проектиране – силна автентикация (препоръчително MFA), актуална криптография, сегментация на достъпа и постоянен мониторинг.

СПИСЪК НА ИЗПОЛЗВАНАТА ЛИТЕРАТУРА (ОНЛАЙН ИЗТОЧНИЦИ)

1. Cisco. What Is a Virtual Private Network (VPN)?

2. Palo Alto Networks. What is a VPN?

3. IETF. RFC 7296 – Internet Key Exchange Protocol Version 2 (IKEv2).

4. OpenVPN Community Docs. OpenVPN Protocol; OpenVPN Cryptographic Layer; TLS control channel overview.

5. WireGuard. WireGuard: Next Generation Kernel Network Tunnel (J. A. Donenfeld); WireGuard Protocol & Cryptography.

6. NCSC (UK). Virtual Private Networks (VPNs) – Device Security Guidance.

7. eduVPN. What is a VPN?

Интернет адреси

https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-virtual-private-network-vpn.html

https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn

https://datatracker.ietf.org/doc/html/rfc7296

https://openvpn.net/community-docs/openvpn-protocol.html

https://openvpn.net/community-docs/openvpn-cryptographic-layer.html

https://openvpn.net/as-docs/tls-control-channel.html

https://www.wireguard.com/papers/wireguard.pdf

https://www.wireguard.com/protocol/

https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks

https://www.eduvpn.org/what-is-a-vpn/

ПРАКТИЧЕСКА ЧАСТ

1. Практически насоки и особености при инсталиране на VPN мрежа

VPN (Virtual Private Network) мрежите се използват за осигуряване на защитена комуникация през публични или недоверени мрежи. Правилното им инсталиране и конфигуриране е критично за сигурността, производителността и надеждността на информационните системи.

1.1. Планиране и предварителен анализ

Преди инсталиране на VPN мрежа е необходимо да се извърши детайлен анализ на нуждите на организацията или потребителите. Това включва определяне на броя потребители, типа достъп (отдалечен достъп или site-to-site VPN), както и необходимото ниво на сигурност. Следва да се оцени съществуващата мрежова инфраструктура и нейната съвместимост с избраната VPN технология.

1.2. Избор на VPN технология и протокол

Съществуват различни VPN протоколи, като IPsec, OpenVPN, L2TP/IPsec и WireGuard. Изборът трябва да се базира на баланс между сигурност, производителност и лекота на поддръжка. Например IPsec е широко използван в корпоративна среда, докато OpenVPN предлага по-голяма гъвкавост и лесна конфигурация.

Съвременните и доказани протоколи с високо ниво на защита включват:

WireGuard – модерен VPN протокол с минималистична архитектура, висока производителност и използване на съвременни криптографски алгоритми като ChaCha20 и Curve25519. Подходящ е за среди, в които се търси висока скорост и лесна поддръжка.

OpenVPN – широко използван и утвърден протокол, който поддържа силни алгоритми за криптиране (AES-256, TLS) и предлага висока гъвкавост и съвместимост с различни платформи.

IKEv2/IPsec – стабилно и сигурно решение, предпочитано в корпоративни среди, особено при мобилни потребители, поради бързото възстановяване на връзката и добрата поддръжка от операционните системи.

По-стари протоколи като PPTP не се препоръчват, тъй като не отговарят на съвременните изисквания за сигурност.

1.3. Конфигуриране и управление на сигурността

Ключов аспект при инсталиране на VPN е правилната конфигурация на механизмите за удостоверяване и криптиране. Препоръчва се използване на силни криптографски алгоритми, многофакторна автентикация и редовно обновяване на ключове и сертификати. Ограничаването на достъпа според ролите на потребителите допълнително повишава нивото на защита.

1.4. Тестване и поддръжка

След инсталацията VPN мрежата трябва да бъде тествана за функционалност, стабилност и производителност. Необходимо е да се предвиди постоянен мониторинг, логване на събития и регулярни актуализации на софтуера, за да се предотвратят уязвимости и прекъсвания на услугата.

1.5. Съвременни и доказани VPN протоколи с високо ниво на сигурност

При проектиране и инсталиране на VPN мрежа изборът на протокол е ключов за гарантиране на защитена, стабилна и ефективна връзка между клиентите и корпоративните ресурси. Следват основните съвременни опции:

1.5.1. WireGuard

Описание: Съвременен VPN протокол с минималистичен код (около 4 000 реда), което намалява повърхността за уязвимости и улеснява одита.

Private Internet Access

Криптография: Използва ChaCha20 за шифроване, Poly1305 за удостоверяване и Curve25519 за обмен на ключове.

Blackhat

Предимства:

Отлична производителност и ниска латентност.

Private Internet Access

По-малка кодова база означава по-малко уязвимости.

Private Internet Access

1.5.2. OpenVPN

Описание: Един от най-широко използваните VPN протоколи, доказан в продължение на години.

ExpressVPN

Криптография: Поддържа силни алгоритми като AES-256 и TLS за обмен на ключове.

Предимства:

Високо ниво на съвместимост с различни платформи.

ExpressVPN

Добре документиран и поддържан.

1.5.3. IKEv2/IPsec

Описание: Комбинация от Internet Key Exchange (IKEv2) и IPsec – широко използвана в корпоративни среди.

Zyxel Support

Криптография: AES, SHA-2, Diffie-Hellman и Elliptic Curve Diffie-Hellman (ECDH).

Blackhat

Предимства:

Отлична стабилност и поддръжка при мобилни връзки.

Zoogvpn

Подходящ за site-to-site и отдалечен достъп.

Забележка: Протоколи като PPTP и SSTP все още съществуват, но поради по-слаба защита и уязвимости не се препоръчват за съвременни корпоративни внедрявания.

ExpressVPN

1.6. Силни политики за автентикация и многофакторна идентификация

Автентикацията е ключов елемент от сигурността на VPN: дори ако тунелът е криптиран, недостатъчно силната идентификация може да компрометира достъпа.

1.6.1. Основи на многофакторната идентификация (MFA)

Многофакторната идентификация (MFA) изисква от потребителя да представи две или повече различни категории доказателства за самоличност:

нещо, което знае (парола);

нещо, което притежава (токен, смартфон, сертификат);

нещо, което е (биометрични данни).

Този подход значително намалява риска от компрометиран достъп в случай на изтичане на пароли или фишинг атаки.

IS Decisions

1.6.2. Практически MFA техники за VPN

Time-based One-Time Passwords (TOTP): временни кодове, генерирани чрез мобилни приложения (например Authenticator).

OpenVPN

Push нотификации: потребителят потвърждава вход чрез съобщение на мобилното си устройство.

InstaSafe

Хардуерни токени: физически устройства за генериране на кодове.

InstaSafe

Биометрични данни: отпечатък, лицево разпознаване и др., при поддръжка от инфраструктурата.

IS Decisions

1.6.3. Добри практики при внедряване на MFA

За да се гарантира ефективност и удобство за потребителите, се препоръчва:

Избор на MFA решение, което се интегрира с корпоративен каталог (например Active Directory или RADIUS).

IS Decisions

Въвеждане на адаптивна автентикация, която коригира изискванията според контекст (локализация, устройство, време на достъп).

Окта

Постоянно обучение на потребителите за важността на MFA и най-добрите практики при използване.

Check Point SASE

Регулярно преглеждане на политики и актуализиране на методите за автентикация съгласно нови заплахи и регулаторни изисквания.

NordLayer

2. Препоръки

Да се извършва детайлно планиране преди внедряване на VPN, с ясно дефинирани цели и изисквания.

Да се използват съвременни и доказани VPN протоколи с високо ниво на сигурност.

Да се прилагат силни политики за автентикация, включително многофакторна идентификация.

Да се осигури редовна поддръжка, мониторинг и актуализация на VPN инфраструктурата.

Да се обучават потребителите относно добри практики за сигурна работа с VPN услуги.

Да се използват само съвременни и доказани VPN протоколи като WireGuard, OpenVPN или IKEv2/IPsec.

Да се прилагат силни криптографски алгоритми и актуални стандарти за защита.

Да се внедрява многофакторна идентификация за всички VPN потребители без изключение.

Да се използва централизирано управление на достъпа и потребителските роли.

Да се осигури непрекъснат мониторинг, редовна поддръжка и обучение на потребителите по въпросите на сигурността.

За корпоративни VPN внедрявания препоръчително е да се използват WireGuard или IKEv2/IPsec, в зависимост от изискванията за производителност и оперативна съвместимост.

Приоритетно да се внедрява MFA за всички VPN потребители, като част от корпоративните политики за контрол на достъпа.

Да се прилагат централизирани системи за управление на самоличността (IAM), които поддържат MFA, адаптивна автентикация и интеграция с VPN услуги.