**№ 5 практикалық жұмыс: VPN – VirtualPrivateNetwork-виртуалды жеке желі**

**Мақсаты: VPN технологиясын зерттеу.**

**Жоспары:**

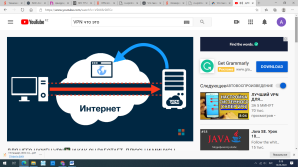
**1. Теориялық бөлім: VPN бұғаттау.**

**2. Практикалық тапсырма**

**1 теориялық бөлім: VPN құлыптау.**

**VirtualPrivateNetwork** - виртуалды жеке желі дегенді білдіреді. VPN ғаламдық Интернет желісінің ішінде бір немесе бірнеше шағын желілерді ұйымдастыру үшін қолданылады. Оған әлемнің кез келген нүктесінен қосылуға болады және қосылу берілетін деректер шифрланып, қорғалған арналар арқылы жүзеге асырылады. Виртуалды дегеніміз не? Бұл дегеніміз, сіздің деректеріңіз жалпыға ортақ желіге, әдетте Интернетке жіберілетініне қарамастан, сіз бен екінші тарап арасында қорғалған виртуалды туннель пайда болады және сіз мыңдаған шақырым қашықта болсаңыз да, бір желіде боласыз.

VPN - көптеген жолдарды байланыстыратын пайдаланушы деректерін қорғауға арналған туннель. Оған сырттан кіретін көліктердің қайда кететінін ешкім білмейді. Сондай-ақ, туннельде не болып жатқанын да ешкім білмейді.



VPN арқасында сіз қорғалмаған немесе жалпыға қолжетімді WI-FI нүктелерінде логин/парольдердіңізді ұстап алады деп қорықпайсыз, сайттарға кіру тарихыңызды ешкім білмейді және сайттардың бұғатталуы туралы ұмытасыз. Бұл торренттер мен тыйым салынған сайттарға қатысты.

VPN қосылымның үш түрін қамтамасыз ете алады: *түйіннен түйінге, түйіннен желіге және желіден желіге.*

Қарапайым тілмен айтқанда **VPN – қауіпсіз туннель**.

Браузерлер мен компьютерге (дербес компьютерге) орнатылған кеңінен қолданылады.

Дербес компьютерде (дербес компьютерде) орнатылған программалар мен браузерлерге арналған **кеңейтімдер** кеңінен таралған.

1. Кеңейтімдер. Сіз оны браузерде бөлек орната аласыз (Chrome үшін VPN - https://hyperione.com/vpn-for-chrome/), сондай-ақ кірістірілген VPN бар браузерді жүктеп алуға болады (мысалы, Opera).

1. Компьютерге арналған программалар. Тағы да екі нұсқасы бар – жеткізушіден немесе осы функцияны қамтитын программадан бөлек жеке софт (мысалы, Касперский антивирусы).

**VPN** (VirtualPrivateNetwork - виртуалды жеке желі) бұл технология басқа желінің үстінен бір немесе бірнеше желілік қосылыстарды (логикалық желі) қамтамасыз етуге мүмкіндік береді.

**VPN** көбінесе қашықтан жұмыс істеген кезде қолданылады. Қызметкер кеңседе болмаса да, сол жерде немесе жұмыс орнында отырғандай кеңсе желісіндегі қажетті ресурстарға қосыла алады. Сондай-ақ, географиялық тұрғыдан әр түрлі қалаларда орналасқан желілерді бір адрес кеңістігімен бір үлкен желіге біріктіру қажет болғанда осы технологияны қолдануға болады.



Қазіргі уақытта VPN қызметтерінің ақылы және ақысыз түрі өте көп. Тегін қызметтердің жылдамдығы әдетте төмен болады және баяу жұмыс істейді.

**Бірақ шартты тегін түрі де бар**. Мұндай VPN сізге айына белгілі бір трафикті пайдалануға мүмкіндік береді (мысалы, 4 гигабайт). Лимит таусылған соң, VPN тек ақылы режимде жұмыс істейді.

VPN -VirtualPrivateNetwork немесе виртуалды жеке желі дегенді білдіретінін жоғарыда айтып кеттік. Оның бұлай аталуы бекер емес, өйткені бұл технология сіздің құрылғыңызды немесе қашықта орналасқан басқа құрылғыны, тіпті бүкіл желі мен басқа қашықтағы желіге туннель деп аталатын виртуалды қосуға мүмкіндік береді.

### Жіктелуі

### VPN шешімдерін бірнеше негізгі параметрлер бойынша жіктеуге болады:

### Пайдаланылатын ортаның қорғалу дәрежесі бойынша

### *Қорғалған*

### Виртуалды жеке желілердің ең көп таралған нұсқасы. Оның көмегімен әдетте Интернеттің, сенімсіз желінің негізінде қорғалған және сенімді желіні құруға болады.

### Қорғалған VPN-ға мысал келтірер болсақ: IPSec, OpenVPN және PPTP.

### *Сенімді*

### Олар тарату ортасын сенімді деп санауға болатын және үлкен желі аясында виртуалды ішкі желіні құру мәселесін шешу қажет болған жағдайларда қолданылады. Қауіпсіздік мәселесі маңызды болмай қалады. Мұндай VPN шешімдерінің мысалдары: Multi-protocollabelswitching (MPLS) және L2TP (Layer 2 TunnellingProtocol) (дәлірек айтқанда, бұл протоколдар қауіпсіздік тапсырмасын басқаларға ауыстырады деп айтуға болады, мысалы L2TP әдетте IPSec-пен бірге қолданылады).

### Іске асыру тәсілі бойынша

### Арнайы программалық -техникалық құрал түрінде

### VPN желісін іске асыру программалық-аппараттық құралдардың арнайы кешенінің көмегімен жүзеге асырылады. Мұндай іске асыру жоғары өнімділікті және, әдетте, қауіпсіздіктің жоғары дәрежесін қамтамасыз етеді.

### Программалық шешім түрінде

### VPN функционалдығын қамтамасыз ететін арнайы программалық жасақтамасы бар жеке компьютерді қолданыңыз.

### Интеграцияланған шешім

### VPN функционалдығы желілік трафикті сүзу, желілік экранды ұйымдастыру және қызмет көрсету сапасын қамтамасыз ету мәселелерін шешетін кешенді қамтамасыз етеді.

### Мақсаты бойынша. *Intranet VPN.* Бір ұйымның бірнеше таратылған филиалдарын біріккен қорғалған желіге біріктіру үшін, ашық байланыс арналары арқылы мәліметтер алмасу үшін қолданылады.

### *RemoteAccess VPN.* Корпоративті (орталық кеңсе немесе филиал) желі сегменті мен үйде жұмыс істей отырып, үй компьютерінен, корпоративті ноутбуктен, смартфоннан немесе интернет-дүңгіршектен корпоративті ресурстарға қосылатын жалғыз пайдаланушы арасында қауіпсіз арна құру үшін қолданылады.

### *Extranet VPN.* "Сыртқы" пайдаланушылар (мысалы, клиенттер немесе тапсырыс берушілер) қосылатын желілер үшін қолданылады. Өйткені, оларға деген сенім деңгейі компания қызметкерлеріне қарағанда әлдеқайда төмен, сондықтан олардың ерекше құнды, құпия ақпаратқа қол жеткізуіне жол бермейтін немесе шектейтін арнайы "шекараны" қамтамасыз ету қажет.

### *Internet VPN.* Әдетте бірнеше пайдаланушы бір физикалық арнаға қосылған болса, провайдерлердің Интернетке қол жеткізуін қамтамасыз ету үшін қолданылады. PPPoE хаттамасы ADSL қосылымдары үшін стандарт болып табылады.

### *Client / Server VPN.* Ол корпоративті желідегі екі түйін (желілер емес) арасында берілетін деректерді қорғайды. Бұл опцияның ерекшелігі - VPN, әдетте, бір желі сегментінде орналасқан түйіндер арасында, мысалы, жұмыс станциясы мен сервер арасында құрастырылған. Мұндай қажеттілік көбінесе бір физикалық желіде бірнеше логикалық желілерді құру қажет болған жағдайда туындайды. Мысалы, қаржы бөлімі мен кадрлар бөлімі арасында трафикті бөлу қажет болғанда, сол физикалық сегментте орналасқан серверлерге кіру. Бұл опция VLAN технологиясына ұқсас, бірақ трафикті бөлудің орнына шифрлауды қолданады.

### Хаттама түрі бойынша. TCP/IP, IPX және AppleTalk үшін виртуалды жеке желілерді жүзеге асыру. Бірақ бүгінде жалпы TCP / IP хаттамасына көшу үрдісі байқалады және VPN шешімдерінің басым көпшілігі мұны қолдайды. Ондағы адресация көбінесе RFC5735 стандартына сәйкес, TCP / IP жеке желілері ауқымынан таңдалады.

### Желілік хаттама деңгейі бойынша. ISO/OSI желілік эталондық модель деңгейлерімен салыстыруға негізделген желілік протокол деңгейі бойынша.

### *Маршрутизаторлардағы VPN қосылымы.* VPN технологияларының кең таралуына байланысты көптеген пайдаланушы желінің қауіпсіздігін арттыру мақсатында маршрутизаторларда VPN қосылымын белсенді түрде конфигурациялай бастады. [ 1] Маршрутизаторда конфигурацияланған VPN қосылымы барлық қосылған құрылғылардың, соның ішінде VPN технологияларын қолдамайтындардың трафигін шифрлайды. Көптеген маршрутизаторлар VPN байланысын қолдайды және кіріктірілген VPN клиентіне ие. OpenVPN протоколына қолдау көрсету үшін DD-WRT, OpenWrt және Tomato сияқты бағдарламалық жасақтаманы қажет ететін маршрутизаторлар бар.

### Осалдықтар. Әр шолғышта әдепкі бойынша қосылған WebRTC технологиясын пайдалану үшінші тарапқа VPN арқылы жұмыс істейтін құрылғының нақты IP адресін анықтауға мүмкіндік береді. Бұл құпиялылыққа тікелей қауіп төндіреді, өйткені пайдаланушының нақты IP адресін біле отырып, оны желіде сәйкестендіре отырып, анықтауға болады. Адрестің жария болуына жол бермеу үшін Браузер параметрлерінде WebRTC-ді толығымен өшіру немесе WebRTCNetworkLimiter арнайы қондырмасын орнату ұсынылады.

### VPN мысалдары

### IPSec (IP security) – көбінесе IPv4 қолданылады.

### PPTP (point-to - pointtunnelingprotocol) – бірнеше компанияның, соның ішінде Microsoft корпорациясының қатысуымен жасалды.

### PPPoE (PPP (Point-to-Point Protocol) over Ethernet)

### L2TP (Layer 2 Tunnelling Protocol) –Microsoft және Cisco компанияларының өнімдерін пайдаланады.

### L2TPv3 (Layer 2 Tunnelling Protocol version 3).

### OpenVPN SSL VPN ашық бастапқы кіріс кодымен, PPP, bridge, point-to-point, multi-client server режимдерін қолдайды

### freelan SSL P2P VPN ашық кіріс кодымен

### Hamach – бір рангалық VPN желісін құруға арналған программа.

### NeoRouter – zeroconf (конфигурацияны қажет етпейді) Nat үшін компьютерлердің тікелей байланысын қамтамасыз ететін программа, өз серверін таңдау мүмкіндігі бар.

### Көптеген ірі провайдерлер бизнес-клиенттерге VPN ұйымдастыру қызметтерін ұсынады.

### VPN қалай жұмыс істейді?

### Әдетте, Интернетке кіру үшін сіз алдымен Интернет-провайдеріне қосыласыз, ол сізді сұраған веб-сайттарға (немесе Интернеттегі басқа ресурстарға) бағыттайды. Сіздің барлық Интернет-трафигіңіз Интернет-провайдерлердің серверлері арқылы өтетіндіктен, олар сіздің Интернетте не істегеніңізді көріп, жазып ала алады. Олар сіздің қаралым тарихыңызды жарнама берушілерге, билік органдарына және басқа үшінші тұлғаларға бере алады. Бірақ бұл жерде VPN сіздің интернет трафигіңізді арнайы конфигурацияланған қашықтағы сервер арқылы бағыттайды. Осылайша VPN сіздің IP-адресіңізді жасырады және барлық кіріс және шығыс деректерін шифрлайды. Шифрланған деректерді ұстап алудың еш мәні жоқ, өйткені оны оқу мүмкін емес.

**2.Практикалық тапсырма: төмендегі VPN бұғаттау мысалын компьютерде орындаңыз. Скриншоттап, есепті скриншоттармен жасаңыз.**

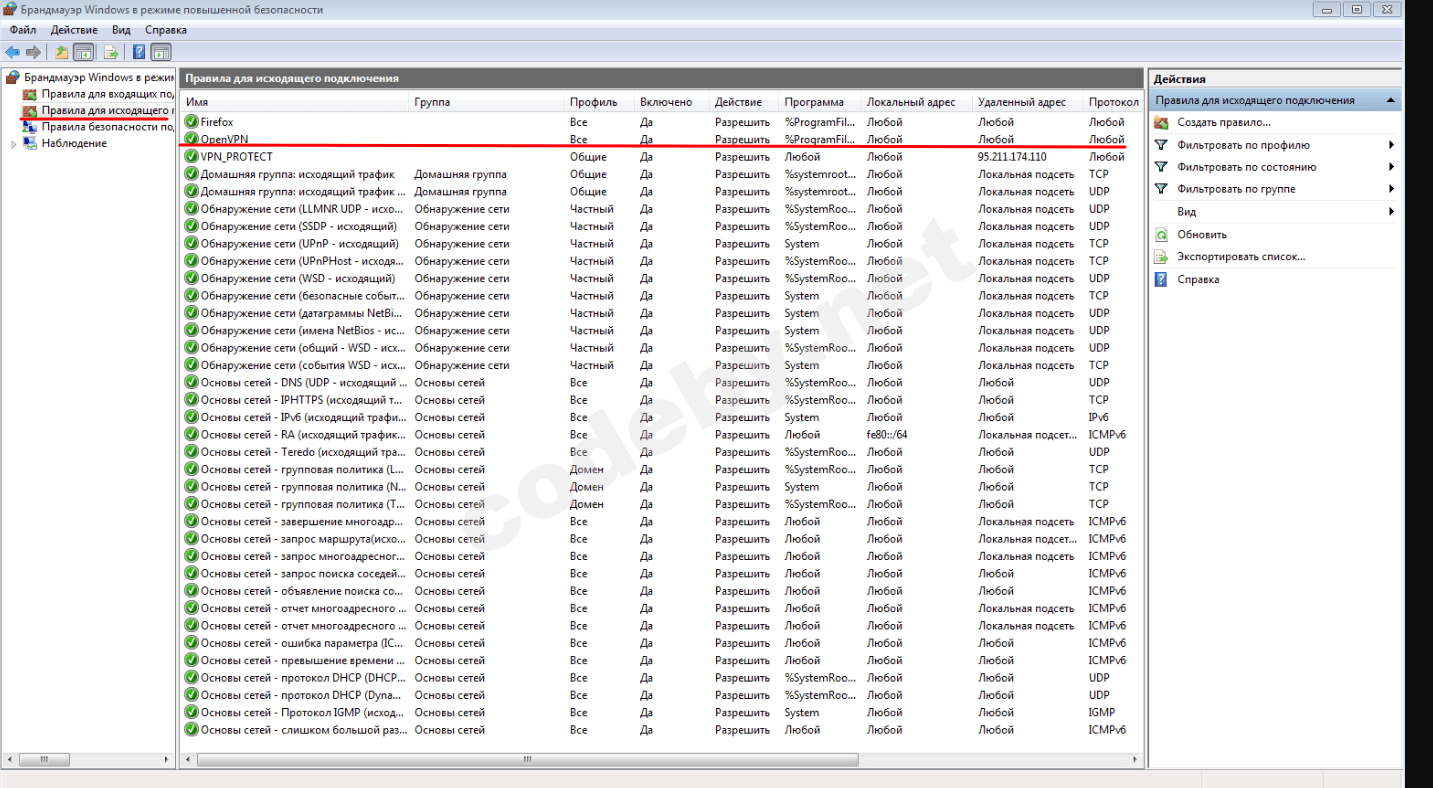
Сіздерге тек екі ережені жазу керек

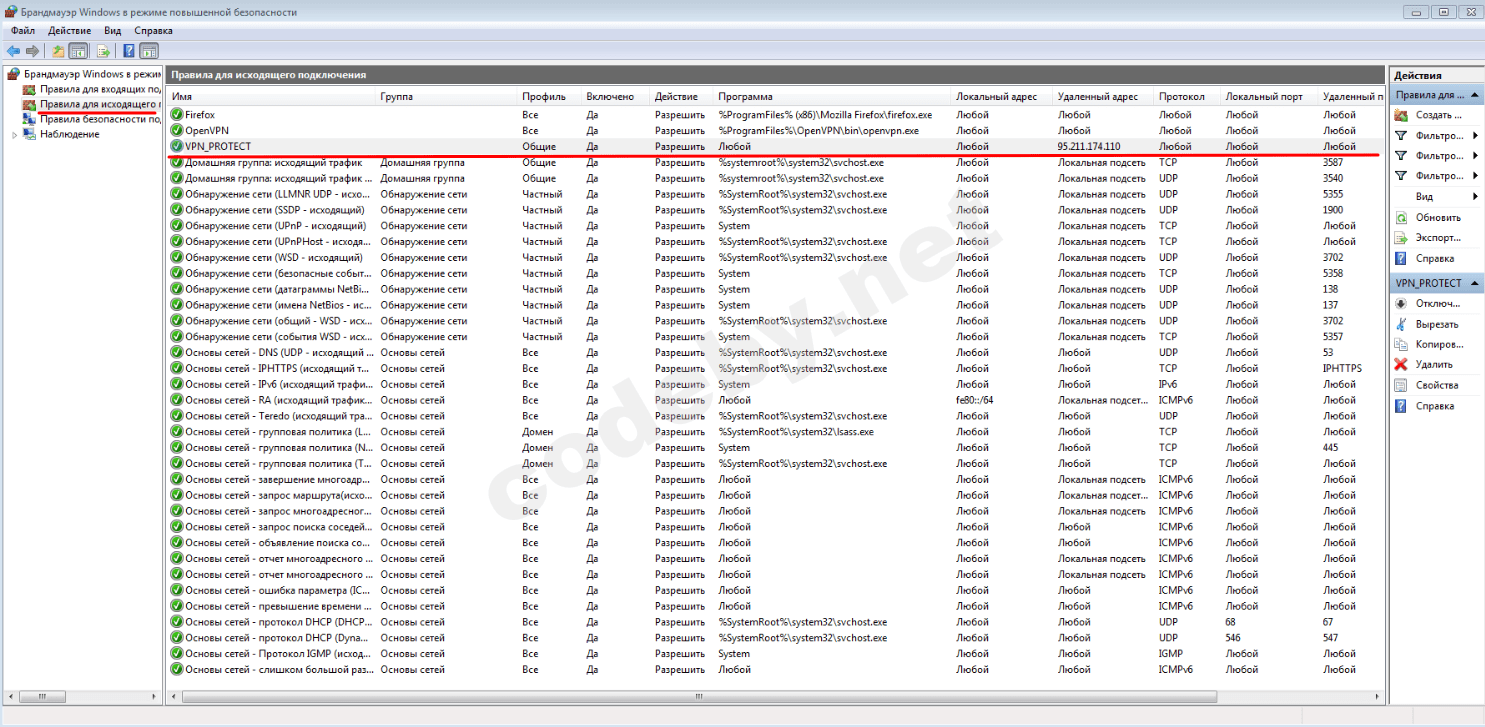
1) OpenVPN.exe рұқсат ету;

2) VPN серверінің (лердің) ажыратылған адресін (немесе диапазонын) тіркеу.

Егер қашықтан қосылу қажет болған жағдайда Кіріс қосылыстарында ештеңені жазудың қажеті жоқ.

Шығыс қосылыстары 1-ші мысалда көрсетілген:

  
2-ші мысал:



VPN\_PROTECT ережесін құру кезінде барлық программалар таңдалғанын ескеріңіз. Сіздерге барлық программалар рұқсат етілген, ал мен Firefox-ты мысалға келтірдім. Өңір деген жерде IP адресті қосыңыз (егер сіздің vpn-да динамикалық адрес болса, онда диапазон), вхоер-да статикалық болған соң, мен біреуін қостым. Скринде бәрі түсінікті болады.

Осындай қарапайым әрекет арқылы біз файрволдағы барлық рұқсат етілген программалардың VPN кенеттен ажыратылған жағдайда бірден бұғатталатынына қол жеткіздік, интернетке қосылу VPN серверіне қайта қосылған кезде ғана мүмкін болады.

Тексереміз

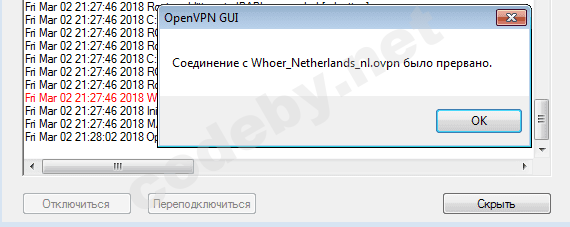
Біз клиенттің процесін бұзуға тырысатын батник жасаймыз, осылайша желі ажыратылады. Клиент бұл туралы бізге хабарлауы керек.

Код:

ping -n 5 127.0.0.1>nul

taskkill /f /im openvpn.exe

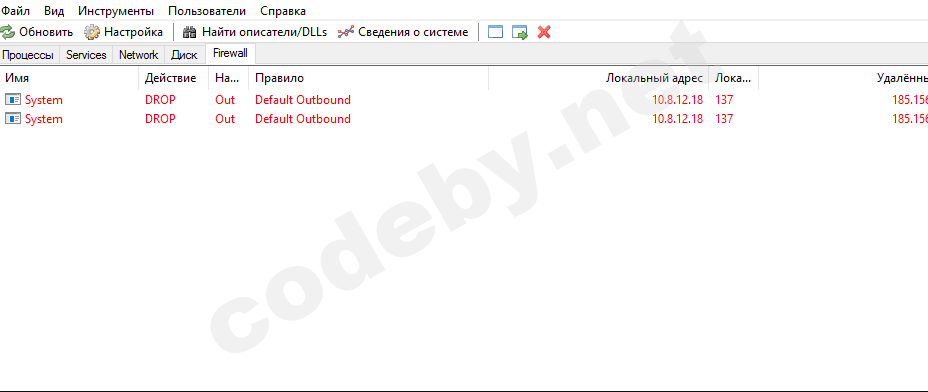
Іске қосамыз және VPN-нан ажыратуға қол жеткіземіз.



Бұған дейін кез-келген пакеттік сниферді іске қосып, пакеттердің берілуі бірден тоқтайтынына көз жеткізе аласыз.

Мысалы: сіз VK-да отырасыз, VPN арқылы кірдіңіз егер VPN ажыратылып, қайта қосылса, VK-серверлеріне трафиктің бірнеше пакеті VPN-ді айналып өтпейді.

Кейде рұқсат беруде қиындықтар туындауы мүмкін, оны журнал арқылы білуге болады, бірақ бұл мен үшін ыңғайсыз. Сондықтан мен ProcessHacker утилитінің көмегіне жүгіндім, өйткені онда Firewall плагині бар



қызыл түспен белгіленгендер Интернетте қосылуға талпынулар, процесс арқылы біз орындалатын файлды табамыз және оны ережелерге енгіземіз.