Дәріс №11: ВИРТУАЛЬДЫ ЖЕКЕ ЖЕЛІНІҢ ҚАУІПСІЗДІК ХАТТАМАЛАРЫ

1) VPN арқылы шешілетін тапсырмалар

Internet-ті қолданудан көп мөлшерде пайда табу үшін екі маңызды қадам жасау керек. Бірінші қадам – Internet-ке қол жеткізу. Екіншісі – бірнеше алыстатылған кеңселердің бірлесіп жұмыс істеуі үшін Internet желісінің артықшылықтырын іске асыру.

VPN – virtual private network (виртуалды жеке желі). Ол желіні пайдаланушыға кіре алмай қалаған контентке кіруге, IP-мекен-жайын ауыстыруға, интернетте жасырын отыруға, сондай-ақ хакерлердің шабуылынан жеке мәліметтерін қорғауға мүмкіндік береді. VPN-сервис интернет бұғатталғанда оған кедергісіз кіруге жол ашады.

VPN технологиясы алыстатылған локалды желілердің қауіпсіз бірлесіп жұмыс істеуін қамтамасыз етеді. Байланыс орнату құны глобалды желілермен байланыс орнату құнының аз бөлігін ғана құрайды.

Жаңа технологияны қолдану түп тамырымен арналарды қолдануға кететін шығындарды азайтады. Басқа да көптеген компанияларға VPN технологиясы телекоммуникациялық жағынан максималды пайда әкеледі.

VPN-ді таңдауда төмендегі критерийлерге баса назар аудару керек:

- ***Қосылу типіне***. L2TP VPN таңдауға кеңес беріледі. Ол көптеген операциялық жүйелерге орнатылған. Сенімді әрі тез кіреді. Негізі қосылу типі туралы VPN сайттарындағы сипаттамаларда жазылған. Сонымен қатар сервистің қосымша OpenVPN-құрамасы болғаны дұрыс. Бұл қауіпсіздікпен каналдың ашылуын күшейтеді.

- ***Логқа назар аударыңыз***. VPN-сервер мұны жүргізгенде жасырыну мүмкін емес болады. ***Лог*** дегеніміз – әрбір клиентті бөлек-бөлек анықтауға көмектесе алатын кез-келген жазба. VPN-сервисті ұсынатын компанияның веб-сайтын мұқият зерттеу керек. Егер компанияның заңды мекен-жайы болса, онда лог жүргізілуі мүмкін. Өйткені барлық тіркелген компаниялар логтарды жүргізуге және өз клиенттерінің қызметін бақылауға міндетті. Сондай-ақ "Қызметті пайдалану туралы келісім"-ге назар аудару қажет. Кейде компанияның сайтында лог жүргізілмейтіні туралы жазылуы мүмкін. Алайда келісім логты сақтауды қарастыруы ғажап емес.

Егер сіз өзіңіздің жасырын түрде отырғаныңызға алаңдасаңыз, сізге арналғаны – ең жақсысы кеңсесі жоқ VPN-сервис. Егер кеңсесі болса, онда келіп, ресми сұраным жолдауға болатын орын бар. Яғни компанияның тіркелгені немесе кеңсесі бар екені VPN-сервисінің жасырын еместігін көрсетеді.

VPN таңдағанда өзіңіздің операциялық жүйеңіздің VPN-сервиске кіре алатынына көз жеткізу керек. Мәселен, Windows, Mac OS, Linux, iOS, Android

пен Windows Phone VPN-желілерге кіре алады. Кез-келген VPN-сервисте қандай операциялық жүйемен кіруге болатыны туралы ақпарат болады.

Ақылы және ақысыз VPN-сервистер бар. Ақысыз VPN-сервистерде интернет-трафигінің жылдамдығы төмен, желіден жиі ажыратылу, жұмыс уақытына шектеу қою, хакерлік және вирустық шабуылдарға ұшырау сынды кедергілер жиі кездеседі.

VPN-ді қолдану төмендегідей ***қауіп-қатерлерге*** әкелуі мүмкін:

- Бірде бір VPN-сервис пайдаланушыны 100 пайыздық қауіпсіздікпен қамтамасыз ете алмайды. Кейбір сервистерді алаяқтар жеке мәліметтерді жинауға пайдаланып, банк шоттарынан ақша ұрлануға немесе басқа да кибер-қылмыстарға әкеп соғуы мүмкін. Тіпті Google Play немесе AppStore ұсынған кейбір сервистердің өзі қауіпті болуы ықтимал.

- Пайдаланушының мәліметтері жарнама берушілерге сатылуы мүмкін, бұл кейін жарнама жолдай беретіндердің мазаңызды алуына әкеледі.

Ақылы VPN-сервисті сатып ала отырып, сіз өзіңізге қатысты мәліметтердің қауіпсіздігіне көзіңіз жетпеуі мүмкін. Желіде ресми деп көрсетілетін фейк сервистер көп. Сондықтан, сатып алмас бұрын, алатын өнімді мұқият зерделеген жөн. Сізге қызмет ұсынатын компанияның байланыс нөмірлері бар-жоқтығына да назар аударыңыз.

Қазақстанда VPN-сервистерді қолдануға ***заңнамамен тыйым салынбаған***.

"Бұқаралық ақпарат құралдары туралы" заңның 2 бабының 3 тармағына сәйкес, Мемлекеттік құпияларды немесе заңмен қорғалатын өзге де құпияны құрайтын мәліметтерді жария етуге, экстремизмді немесе терроризмді насихаттауға және ақтауға, терроризмге қарсы операцияларды жүргізу кезеңінде олардың техникалық тәсілдері мен тактикасын ашатын ақпаратты таратуға, есірткі, психотроптық заттарды, сол тектестер мен прекурсорларды, сондай-ақ қатыгездікті, зорлық-зомбылықты және порнографияны насихаттауға тыйым салынады.

2) Қорғалған арналар деңгейлері

Әрине ешқандай компания финансттық және басқа конфедициалды ақпаратты интернетке ашық түрде жібергісі келмейді. IPSec қауіпсіздік хаттамалар стандарттарына салынған VPN каналдары қуатты шифрлеу алгоритмдерімен қорғалады. IPSec (Internet Protocol Security – халықаралық қауымдастығы IETF – Internet Engeniring Task Force тобымен таңдалған стандарты) интернет – протокол хаттамасы (IP) үшін қауіпсіздік негіздерін қамтамасыз етеді. IPSec хаттамасы қорғанысты желілік деңгейде қамтамасыз етеді және байланыстың екі жағындағы құралдарынан ғана IPSec хаттамасының қолдауын талап етеді. Олардың арасында орналасқан, қалған барлық құралдар тек IP пакеттердің трафигін қамтамасыз етеді.

IPSec технологиясын пайдаланатын қолданушылардың әрекеттесу әдісін «қорғалған ассоцияция» – Security Association (SA) терминімен анықтайды. Қорғалған ассоцияция бір біріне жіберетін ақпаратты қорғау үшін IPSec құралдарымен пайдалынылатын қолданушылармен жасалған шарттар негізінде жұмыс істейді. Бұл шарт бірнеше параметрлерді реттейді: жіберуші мен алушының IP – адрестері, криптографиялық алгоритм, кілттердің өлшемі, кілттердің қызмет ету мерзімін, аутентификацияның алгоритмі.

Алшақтатылған қол жетімдік басқа стандарттар Microsoft дамытатын PPTP (Point to Point Tunneling Protocol), Cisco дамытатын L2F (Layer 2 Forwading) үшін хаттамаларын қосады. Microsoft және Cisco IETF бірігіп жұмыс істейді, бұл екі хаттамаларды L2P2 (Layer 2 Protocol) стандартына біріктіру мақсаты: IPSec – ті қолданып туннельдік аутентификация, жеке меншікті қорғау және тұтастықты тексеру.

Желіде шифрленген ақпаратты алмастыру тез әрекет етуді қамтамасыз ету кейбір мәселелерді туғызады. Кодтау алгоритмдері процессордың едәуір есептеуіш ресурстарын, әдеттегі IP – маршрутизация кезінде 100 есе артық көлемді қажет етеді. Қажетті өнімділік болу үшін серверлердің және клиенттік компьютерлердің тез әрекет етуін қамтамасыздантыру керек. Одан басқа, шифрлеуді тездететін ерекше сұлбаларымен арнайы шлюздар бар.

IT – менеджер қажеттіліктерге байланысты виртуалды жеке желінің конфигурациясын таңдауы мүмкін. Мысалы, үйде жұмыс істейтін қызметкерге шектелген қол жетімдік беріледі, ал алшақтатылған офистің менеджеріне немесе компанияның директорына қол жетімдіктің кең құқықтары беріледі. Виртуалды желі арқылы жұмыс істегенде бір жоба минималды (56 – разрядты) шифрлеуімен шектелуі мүмкін, ал компанияның финанстық және жоспарлық ақпараты шифрлеудің қуатты құралдарын (168 – разрядты) талап етеді.

Желінің өнімділігі – бұл маңызды параметр. VPN – құралдары арқылы өтетін трафикті өңдеумен байланысты қосымша бөгелістерді туғызады, сондықтан да VPN құрастыру құралдары өнімділікті төмендетуі мүмкін. Трафикті өңдеу кезінде пайда болатын бөгелістерді үш типке бөлуге болады:

✓ VPN – құралдары арасында байланыс орнату кезінде туатын бөгелістер.

✓ Қорғалынатын деректерді шифрлеу мен қайта шифрлеу және біртұтастыққа тексеру үшін керекті өзгертулермен байланысты бөгелістер.

✓ Жіберілетін пакеттерге жаңа атауды қосумен байланысты бөгелістер.

VPN – құрастырудың бірінші, екінші және төртінші нұсқаларында желі абоненттері арасында емес, тек VPN – құралдары арасында ғана қорғалған байланысты орнату қарастырылады. Криптографиялық кілтттерінің беріктілігін есепке ала отырып кілтті өзгерту ұзақ уақыт интервалынан кейін мүмкін болады. Сондықтан да VPN – құрастырудың бірінші типін пайдаланғанда бөгелістердің бірінші типі деректердің алмасу жылдамдығына әсер етпейді. Бірақ бұл тек 128 биттен кем емес кілттерді пайдаланатын шифрлеудің берік

алгоритмдеріне тән. Бұрынғы DES стандартын пайдаланатын құралдар желі жұмысына кейбір бөгелістерді енгізеді.

Бөгелістердің екінші типі деректерді жоғары жылдамтықты каналдар (10 Мбит/с) арқылы жібергенде пайда болады. Басқа барлық жағдайларда таңдалған шифрлеу және біртұтастықты бақылау алгоритмдерінің программалық немесе аппараттық таратылуына тез әрекет етуі жоғары және «пакетті шифрлеу – пакетті желіге жіберу» және «пакеттерді желіден алу – пакетті қайта шифрлеу» операцияларының тізбегінде шифрлеу уақыты берілген пакетті жіберуге керекті уақытынан аз болады. Компаниялар алшақтатылған қол жетімдікті орнататын модемдер қызметін ұйымдастыруына үлкен сомаларды төлеуден босатылады.

Сондықтан да VPN – құрастырудың бірінші типін пайдаланғанда бөгелістердің бірінші типі деректердің алмасу жылдамдығына әсер етпейді.

Қазіргі уақытта VPN – ның таралған хаттамалары екінүктелік туннельдік байланыстың хаттамалары (***Point – to – Point Tunnelling Protocol – PPTP***) болып табылады. Ол 3Com және Microsoft компанияларымен интернет арқылы корпоротивтік желілерге қауіпсіз алшақтатылған қол жетімдікті қамтамасыз ету мақсатында өндірілген. ***PPTP*** TCP/IP ашық стандарттарын пайдаланады және көбінесе ескірген PPP екінүктелік хаттамасына негізделеді. PPTP желі арқылы алушының серверіне туннельді жасайды және ол арқылы алшақтатылған қолданушының PPP – пакеттерін жібереді. Сервер және қолданушы виртуалды жеке желіні пайдаланады және олар арасындағы ғаламдық желі қаншалықты қауіпсіз және қол жетімді екеніне көңіл аудармайды. Сервер бастамасы бойынша байланыс сеансын аяқтау жергілікті желілердің әкімшелеріне алшақтатылған қолданушыларды жүйенің қауіпсіздік шекараларынан өткізбеуге мүмкіндік береді. Нәтижесінде қолданушы жалпы қол жетімді желіге функционалды мүмкіндіктеріне кедергі келтірмей виртуалды жеке желіні пайдаланады.

PPTP хаттамасының қызметі тек Windows басқармасында жұмыс істейтін құрылғыларға таратылады, бірақ ол компанияларға желілік инфракстураларымен әрекеттесу және өзінің қауіпсіздік жүйесіне кедергі келтірмей жұмыс істеу мүмкіндігін береді. Осылайша, алшақтатылған қолданушы аналогты телефон тізбегі арқылы жергілікті провайдер көмегімен интернетке қосылып, сервермен байланыс орната алады.

Компаниялар алшақтатылған қол жетімдікті орнататын модемдер қызметін ұйымдастыруына үлкен сомаларды төлеуден босатылады. Жақындағы болашақта жаңа екінші деңгейлі туннельдеу протоколының (Layer 2 Tunneling Protocol – L2TP) негізінде жұмыс істейтін виртуалды жеке желілердің саны өсуі күтіледі. Бұл хаттама екінші деңгейде жұмыс істейтін PPTP және L2F (Layer 2 Forwarding – екінші деңгейлі жіберу хаттамасы) хаттамаларын біріктіру және олардың мүмкіндіктерін кеңейту мүмкіндігін береді. Осы мүмкіндіктерінің бірі көпнүктелік туннельдеу, ол бірнеше VPN желіні құрастыруға, мысалы интернетке және корпоративтік желіге қосылуға мүмкіндік береді.

L2TP и PPTP хаттамалары туннельдеудің үшінші деңгей хаттамаларынан бірқатар ерекшеліктері бар:

Корпорацияларға қолданушылардың аутентификациясын және олардың өкілдігін өзінің желіде немесе интернет – провайдерінде тексеру әдістерін дербес таңдауға мүмкіндігін беру.

Туннель коммутацияларын қолдау – бір туннельдің аяқталуы және басқа көптеген потенциалды терминалдардың біреуіне қосылу мүмкіндігі. Туннелдердің коммутациясы PPP – байланыстарын керекті нүктеге дейін жалғастыру мүмкіндігін береді.

Корпоративтік желінің жүйелік әкімшісіне тікелей брандмауэр және ішкі желілерде қолданушыларға қол жетімдікті тағайындау стратегиясын орындау мүмкіндігін береді. Туннельдер терминаторлары қолданушылар туралы PPP пакеттерін алатындықтан, бөлек қолданушылардың трафиктеріне администратормен жасалған қауіпсіздік стратегиясын қолдануға құқылы болады. Туннельдеудің үшінші деңгейі провайдерден келетін пакеттерді айыра алмайды, сондықтан қауіпсіздік стратегиясының фильтрларын соңғы жұмыс станцияларында және желі құралдарда қолданылады. Одан басқа, туннельдік коммутаторды қолданған жағдайда бөлек қолданушылардың трафиктерін сәйкес серверге тікелей трансляциялау үшін екінші деңгейлі туннельдің «жалғасын» жасауға мүмкіндік береді. Осындай серверлерге қосымша пакеттерді фильтрациялау міндеті жүктеледі.

VPN таңдап біз:

- ❖ интернетке қолжетімдік бағасымен қорғалатын байланыс каналдарын аламыз, ол бөлінген тізбектерге қарағанда бірнеше есе арзан;
- ❖ VPN орнату кезінде желінің топологиясын өзгерту, қосымшаларды қайта жазу, қолданушыларды оқыту керек емес – бұл маңызды үнемдеу;
- ❖ масштабталу қамтамасыз етіледі, себебі VPN өсу мәселелерін тудырмайды және жасалған инвестицияларды сақтайды;
- ❖ криптографиядан тәуелсізсіз және кез келген мемлекеттің ұлттық стандартына сәйкес криптографияның модульдерін қолдана аламыз.
- ❖ ашық интерфейстер сіздің желіңізді басқа бизнес қосымшалар мен программалық өнімдермен интеграциялау мүмкіндігін береді.

3) VPN түрлері

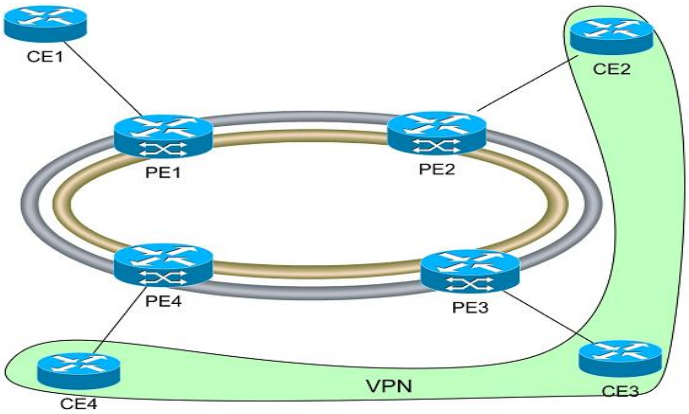
Виртуалды жеке желілерінің түрлері көп. Олардың түрлілігі қолданушыларға қызмет көрсетуді басқаруына байланысты. Қазіргі кезде виртуалды жекеше желінің негізгі төрт түріне тоқталып кетейік:

- ➢ ішкі корпоративті VPN (Intranet VPN);
- ➢ қашықтан қатынас құрылатын VPN (Remote Access VPN);
- ➢ корпоративтер арсындағы VPN (Extranet VPN);
- ➢ Client/Server VPN.

Intranet VPN. Виртуалды жекеше желісінің бұл түрі, бір мекеменің ашық байланыс арналары арқылы қатынасып отырған бірнеше таралған филиалдарын бір қорғалған желіге біріктіруге мүмкіндік береді. Виртуалды жекеше жілісін құру түрлерінің осы түрі – бүкіл дүние жүзінде ең көп тарағаны және де өңдеушілер компаниялары ең алдымен осы түрін өңдейді. Ішкікорпоративті (Intranet VPN) түрі.

Intranet VPN қызметтерін ұсыну сұлбасы төмендегі 1-суретте көрсетілген. Мұнда Intranet VPN желісін тұтынушыладың маршрутизаторларының жиыны құрайды. Ол маршрутизаторлар суретте CE-маршрутизаторлары ретінде көрсетілген. CE-маршрутизаторлары өз кезегінде шекаралық PE-маршрутизаторларына қосылған.

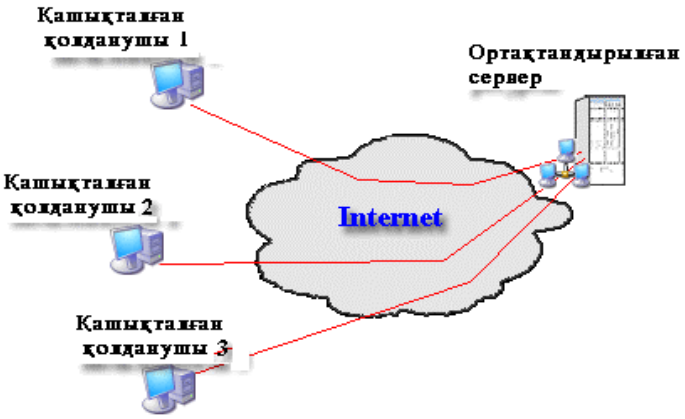
Әрбір клиенттің желісі провайдер желісі арқылы жүргізілген туннелдер арасында байланысқан территориалды тармақталған кеңселерден тұрады. Интражелі VPN желісінің қарапайым нұсқасы болып табылады. 1 - суретте Intranet VPN Қызметтерін ұсыну нұсқасы берілген.



1 -сурет. Intranet VPN қызметтерін ұсыну

Бұл суретте мекеме филиалдарының Intranet VPN желісі арқылы өзара ақпарат алмасуы бейнеленген. Мұнда филиалдар ашық желі арқылы орталықтандырылған серверге біріктірілген.

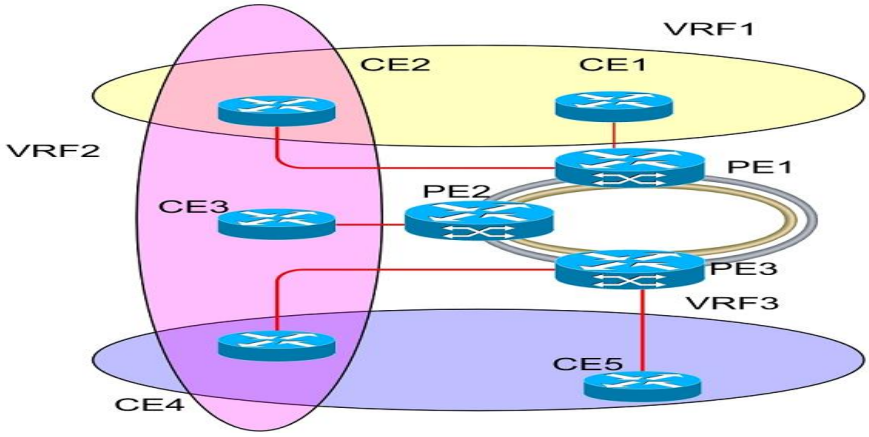
Remote Access VPN. “Remote Access VPN” түрі корпоративті ресурстарға үйінен (үйдегі қолданушы) немесе notebook арқылы (жылжымалы қолданушы) қосылатын жай қолданушымен корпоративті желі сегментінің (орталық офис немесе филиалдар арасында) арасындағы қорғалған тасымалдауды орындайды. Виртуалды жекеше желісінің бұл түрінің біріншісінен айырмашылығы қашықталған қолданушы статикалық мекен-жайға ие болмауы және ол қорғалған ресурстарға арнайы VPN құрылғысы арқылы емес тікелей VPN функциясын орындайтын бағдарламалық қамтамасы орнатылған өзінің компьютерінен қосылады. Қашықтан қатынас құрылатын (Remote Access VPN) түрі 2 - суретте келтірілген.



2 -сурет. Remote Access VPN

Бұл суретте жылжымала қолданушы орталық офиспен қорғалған арна арқылы құпия деректерді тасымалдауы бейнеленген.

Extranet VPN. Extranet – іскерлік қарым – қатынастар кезінде байланыстың сенімділігінің арттырылуын қолдайтын бір компания желісінен екінші басқа компания желісіне тікелей қатынауды қамтамасыз ететін тораптық технология. Extranet VPN желісі жалпы ішкікорпоративті виртуалды жекеше желісіне ұқсас келеді, тек айырмашылығы оның дерек қорғау проблемасы қиынырақ. Бірнеше компаниялар бірге жұмыс істеуді келісіп бір-біріне өздерінің желілерін ашқанда олар, өздерінің серіктестерінің белгілі ғана мәліметтерге қатынас құруларын алдын – ала қарастырулары қажет. Сонымен қатар құпия деректер рұқсатсыз кіруден қорғалған болуы тиісті, сондықтан корпоративтер арасындағы желілерде брандмауэрлер арқылы қатынас құруды бақылау маңызды. Корпоративтер арсындағы VPN (Extranet VPN) түрі 3- суретте келтірілген.

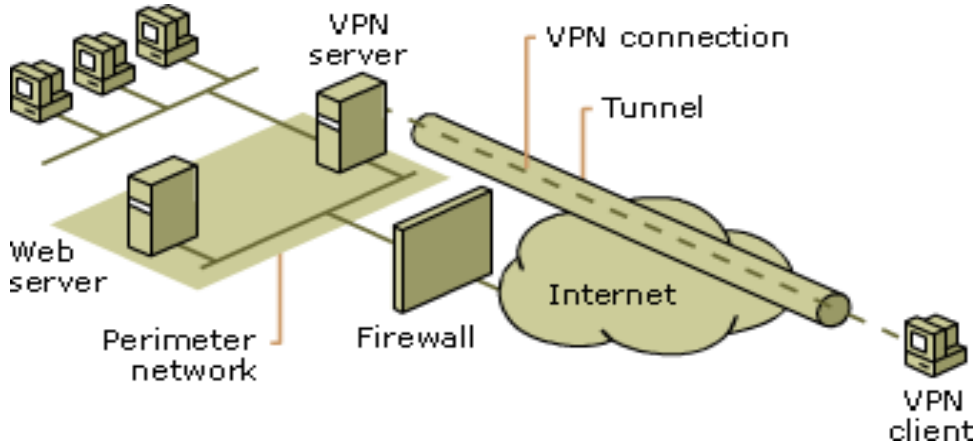


3 -сурет. Extranet VPN Қызметтерін ұсыну

Client/Server VPN. “Client/Server VPN” түрі корпоративті желінің екі түйін (тораптар емес) арасында тасымалданатын деректерді қорғалуын қамтамасыз етеді. Виртуалды жеке желісінің бұл түрінің ерекшелігі мұнда, VPN мысалы,

жұмыс станциясы мен сервер арасында, желінің бір сегментінде орналасқан түйіндер арасында құрылады.

Мұндай қажеттілік кейде бір физикалық желіде бірнеше логикалық желіні құру қажет болғанда туады. Мысалы, бір физикалық сегментте орналасқан, серверге қатынасқан, финанстық департаментімен кадрлар бөлімі арасындағы трафикті бөлу керек болғанда. Client/Server VPN түрі 4 - суретте көрсетілген.



4 -сурет.Client/Server VPN

Суретте желінің бір сегментінде орналасқан түйіндер арсында құрылған Client/Server VPN желісі көрсетілген. Мұнда қолданушы мен сервер арасындағы желіге брандмауэр (firewall) орнатылған. Себебі брандмауэр құпия деректерді бекітілмеген енулерден қорғайды.

Смартфонға VPN-сервисті сатып алу үшін Appstore-ға (iPhone) немесе Play market-ке (Android) кіру керек. Смартфондарға арналған VPN-сервистің десктоптарға (дербес компьютер) арналған VPN-сервистен айырмашылығы Android пен Play Market-тегі барлық бағдарламалардың лицензиясы барлығында және вирустың жоқтығына тексерілгендігінде.

VPN (Virtual Private Network – виртуалды жеке желі) технологиясы – бұл желі қауіпсіздігін және ол арқылы берілетін деректер қауіпсіздігін жалғыз тәсілі. VPN – агенттерді автоматты түрде шығатын ақпаратты шифрлайды (және сәйкесінше қабылданған ақпаратты кері шифрлайды) және де олар ЭЦП көмегімен оның тұтастығын қадағалайды.