ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

Демешов Аманат

VPN технологиясындағы желінің сапалы көрсеткіштерін зерттеу

Дипломдық жобаға

ТҮСІНІКТЕМЕЛІК ЖАЗБА

5В071900 – Радиотехника, электроника және телекоммуникация мамандығы

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
тех.ғыл.канд, профессор
_____ Е.Таштай
«29» 04 2019 ж.

Дипломдық жобаға

ТҮСІНІКТЕМЕЛІК ЖАЗБА

Тақырыбы: VPN технологиясындағы желінің сапалы көрсеткіштерін зерттеу

5В071900 – Радиотехника, электроника және телекоммуникация мамандығы

Орындаған: _____ Демешов Аманат

Рецензия беруші
ҚазҰАУ, ЭҮжА каф.
доктор PhD.,
қауымдастырылған профессор
_____ Әлібек Н.Б.
«24» 04 2019 ж.

Ғылыми жетекші
ЭТжҒТ каф. э.ғ.к.,
лекторы
_____ Куттыбаева А.Е.
«29» 04 2019 ж.

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
тех.ғыл.канд, профессор
_____ Е.Таштай
«08» 02 2019 ж.

Дипломдық жоба орындауға
ТАПСЫРМА

Білім алушы: *Демешов Аманат*
Тақырыбы: *VPN технологиясындағы желінің сапалы көрсеткіштерін зерттеу*
Университет ректорының *«16» қазан 2018 ж. №1162-б* бұйрығымен бекітілген
Аяқталған жобаны тапсыру мерзімі "21" 04 2019 жыл.
Дипломдық жұмыстаиқарастырылатын мәселелер тізімі Жеке корпоративтік желінің жағдайын талдау; IP/VPN бірыңғай корпоративтік желісін құру;
Дипломдық жұмыста қарастырылатын мәселелер тізімі:
1) Телекоммуникациялық желілердің құрылымы
2)Желі функцияларына қойылатын талаптар
3)VPN үшін жабдықтар.
Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс)
Сызбалық материалдар слайдпен көрсетілген
Ұсынылатын негізгі әдебиет 13 атау

дипломдық жұмысты (жобаны) дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
Жеке корпоративтік желінің жай-күйін талдау;	8.02.2019	орындалды
IP/VPN бірыңғай корпоративтік желісін құру; VPN хаттамалар стегі; VPN желілерін жіктеу;	22.03.2019	орындалды
Желінің өткізу қабілетін оңтайлы тарату есебін шешу; VPN желісінің өнімділігін талдау; Оптикалық талшықтың негізгі сипаттамаларын есептеу.	21.04.2019	орындалды

Дипломдық жұмыс (жоба) бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жұмысқа (жобаға) қойған **қолтаңбалары**

Бөлімдер атауы	Кеңесшілер (аты, әкесінің аты, тегі, ғылыми дәрежесі, атағы)	Қол қойылған күні	Қолы
Норма бақылау	Тайсариева Қ.Н. PhD., докторы, сениор лектор	28.04.19	

Ғылыми жетекшісі _____ А.Куттыбаева
(қолы)

Тапсырманы орындауға алған білім алушы _____ А.Демешов

Күні "24" 04. 2019 ж.

АҢДАТПА

Корпоративті желі үшін тұтынушыға сапалы қызмет көрсету, қызметтер мен кепілдікті ұсыну маңызды рөл атқарады. Осы мәселені шешу үшін виртуалды жеке желі VPN (Virtual Private Network) технологиясын пайдаланады. Бұл технология дестелі желілерде қосылыстарды кепілдікпен өткізуге, жиілік жолағы бар қорғалған арнаға ауыстыруға мүмкіндік береді. Арзан бағадағы қосылыстар мен кең спектірлі және қауіпсіздікті қамтамасыз етеді.

Бұл дипломдық жұмыста Алматы, Астана, Атырау қалалар ҚР аумағындағы мекемелер үшін IP VPN корпоративті байланыс желісін ұйымдастыру мәселесі қарастырылады. Аталып өткен қалада желіні құру кезінде «сонғы миля» байланыстарының оптикалы арнасы көмегімен жүзеге асырылады, бұл кезде байланыстың сапасы жоғарылайды.

АННОТАЦИЯ

Для корпоративной сети важную роль играет качественное обслуживание потребителя, предоставление услуг и гарантий. Для решения этой проблемы виртуальная частная сеть использует технологию VPN (Virtual Private Network). Эта технология позволяет гарантировать передачу соединений в пакетной сети, заменить защищенные каналы с частотной полосой. Обеспечивает широкий спектр и безопасность соединений по дешевой цене.

В дипломной работе рассматриваются вопросы организации корпоративной сети IP VPN для учреждений, находящихся на территории РК. В связи с тем, что в связи с тем, что в связи с тем, что в связи с тем, что в связи с тем, что он не был подключен к сети, в связи с тем, что он не был подключен к данной сети, он будет подключен к данной сети.

ANNOTAION

For the corporate network plays an important role quality customer service, services and guarantees. To solve this problem, the virtual private network uses VPN (Virtual Private Network) technology. This technology allows you to guarantee the transmission of connections in the packet network, replace the protected channels with a frequency band. Provides a wide range and security of connections at a cheap price.

The thesis deals with the organization of corporate IP VPN network for institutions located in the territory of the Republic of Kazakhstan. Due to the fact that due to the fact that due to the fact that due to the fact that due to the fact that due to the fact that he was not connected to the network, due to the fact that he was not connected to the network it will be connecte

МАЗМҰНЫ

КІРІСПЕ

Деректерді берудің ұлттық желісі-таңбалар (MPLS) бойынша көпжолақты коммутация технологиясы негізінде виртуалды жеке желілерді (VPN) ұйымдастыруды қамтамасыз ететін Қазақстан Республикасындағы деректерді берудің ірі магистральдық желісі. «Қазақтелеком» АҚ бүгінгі күні ҚР бүкіл аумағында таратылатын MPLS-желісіне ие. Кәсіпорын қызметкерлерінің корпоративтік желі компьютерлерінің орталық деректер базасында шоғырланған ақпараттық ресурстарға қашықтан қол жеткізуін ұйымдастыру соңғы уақытта көптеген кәсіпорындар үшін стратегиялық маңызды мәселелер қатарына өтті. Кез келген географиялық нүктеден корпоративтік ақпаратқа жылдам қол жеткізу қызметтің көптеген түрлері үшін оның қызметкерлерінің шешім қабылдау сапасын анықтайды. Бұл фактордың маңыздылығы қызметкерлер санының өсуімен және қаланың әр түрлі бөліктерінде және әр түрлі қалаларда орналасқан кәсіпорынның шағын филиалдары санының өсуімен өсуде. Корпоративтік желіге тұрақты компьютерлік қатынауды қажет ететін кәсіпорын қызметкерлерінің саны жыл сайын артып келеді. Осылайша, жыл сайын кәсіпорындардың көп бөлігі корпоративтік желілерді құруды және қолдауды қажет етеді. VPN қызметіне үлкен сұраныс бар. VPN технологиясы бірнеше кәсіпорындармен бөлінетін желілік инфрақұрылым көмегімен сапа бойынша жеке желі сервистеріне жақын сервистерді жүзеге асыруға мүмкіндік береді(қауіпсіздік, қол жетімділік, болжамды өткізу қабілеті, мекенжайларды таңдаудағы Тәуелсіздік).

Қызмет провайдері жеке желі негізінде өз клиентін оқшаулап және қорғай отырып, жеке желіні ойнатады. IP/MPLS технологиясына негізделген IP VPN желісі қауіпсіздік пен қызмет көрсету сапасының жоғары деңгейін барынша икемділігі мен масштабталуымен ұштастырады. IP/MPLS желісі 622Мбит/с дейін деректерді беру жылдамдығын қамтамасыз ететін жоғары жылдамдықты жер үсті арналарына негізделеді. Желісіне қосылу жүзеге асырылуы мүмкін көмегімен кез келген осы сәтте қол жетімді түрлерінің клиенттік порттар мен протоколдар: ADSL, FR, ATM, Ethernet, бұл ретте жылдамдық клиенттік порт жетуі мүмкін 100Мбит/с(Ethernet).

Дипломдық жұмыстың мақсаты Қазақстан Республикасының кез келген мекемесі үшін VPN корпоративтік желісін жобалау болып табылады. Корпоративтік желі Алматы, Астана және Атырау қалаларында орналасқан 3 нүктені қамтуы тиіс.

Бұл мақсатқа жету үшін жобалау әдіснамасы, яғни корпоративтік желіні құру кезінде орындалуы қажет жұмыстардың реті мен мазмұны таңдалған. Қабылданған әдістемеге сәйкес желілік жобаларды орындаудың кейбір типтік кезеңдерін тұжырымдауға болады.

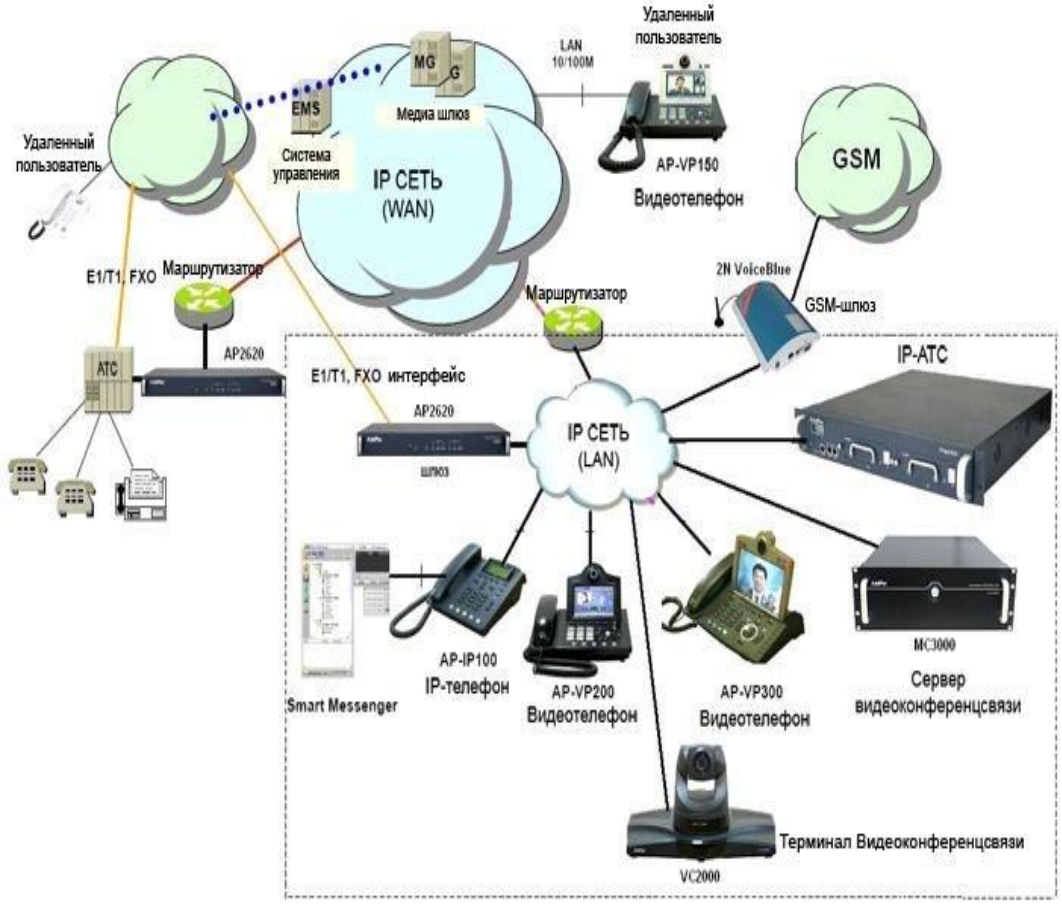
1 Жеке корпоративтік желінің жай-күйін талдау

1.1 Бірыңғай корпоративтік желіні құрудың өзектілігі

Internet Protocol (IP, «желіаралық хаттама») - TCP/IP стегінің желілік деңгейінің маршрутталатын ХАТТАМАСЫ. IP бөлек компьютерлік желілерді Дүниежүзілік Интернет желісіне біріктірген протоколға айналды. Желінің адресациясы Хаттаманың ажырамас бөлігі болып табылады. IP-желі сегменттерін бір желіге біріктіріп, кез келген желі тораптары арасында аралық түйіндердің (маршрутизаторлардың) еркін саны арқылы деректер пакеттерін жеткізуді қамтамасыз етеді (1.1-сурет). Ол OSI желілік моделі бойынша үшінші деңгейлі хаттама ретінде жіктеледі. IP пакетті адресатқа сенімді жеткізуге кепілдік бермейді — атап айтқанда, пакеттер жөнелтілген тәртіпте емес, қайталануы (бір пакеттің екі көшірмесі келеді), бүлінген болуы (әдетте бүлінген пакеттер жойылады) немесе мүлдем келмеуі мүмкін. Пакеттерді қатесіз жеткізу кепілдігі жоғары деңгейдегі кейбір протоколдарды береді — OSI желілік моделінің транспорттық деңгейі, мысалы, IP-көлік ретінде пайдаланатын TCP.

IP-желілер телефония қызметтерін айтарлықтай кеңейтетін бірқатар ерекшеліктерге ие:

- IP-желілер телефония мен оның ерекшеліктеріне байланысты физикалық шектерді жояды. Дәстүрлі телефон қызметтерінің барлық спектрін сақтай отырып, ЛВС желілік сервистеріне тән айтарлықтай жаңа мүмкіндіктер пайда болады;
- IP-желілер пайдаланушылардың орналасқан жері мен құнына байланысты дербес таңдап алатын көлік ортасына байланысты емес. IP ATM, Ethernet, Frame Relay, ISDN және тіпті аналогтық желілер арқылы таратуға болады. Өткізу жолағына қолданылатын қосымшалардың талаптарына негізделген қосылымды дұрыс таңдау маңызды мәселе болып табылады;
- IP-желілер бірқатар әмбебап жаһандық стандарттарға негізделген. Осы стандарттардың арқасында әр түрлі өндіруші фирмалардың жабдықтарымен түйісуі мүмкін болды. Нәтижесінде өндірушілер мен желілік қызмет провайдерлерінің бәсекелестігі бағалардың төмендеуіне және соңғы пайдаланушы үшін қызметтер спектрінің кеңеюіне алып келді;
- LAN/WAN желілері бойынша ақпарат беру сенімділігі мен сапасының жоғары деңгейіне байланысты байланыстың жоғары сенімділігі.



Сурет 1.1 - IP желісі

Әлемдік қоғамдастық өзінің өмір сүруінің ақпараттық желілердің жұмыс істеуіне тәуелділік дәрежесіне жақындады, ол электр энергиясымен қамтамасыз ету жүйелеріне тәуелділікпен салыстыруға болады. Осыған байланысты, корпоративтік желілердің сенімділігін қамтамасыз ету және ақпаратты қорғау мәселесі бірінші жоспарға шығады.

Корпоративтік желі-бұл әртүрлі байланыс түрлерін, коммуникациялық хаттамалар мен ресурстарды қосу тәсілдерін пайдаланатын өте күрделі құрылым. Жұмыс істейтін желі-бұл баға мен мүмкіндіктер тұрғысынан біртектес жүйе немесе әр түрлі өндірушілердің өнімдерін орнату мен басқаруда неғұрлым күрделі үйлесім. Корпоративтік желі деп 50 – ден кем емес компьютерлері бар ірі немесе орта кәсіпорын (ұйым) желісін түсінеміз, онда барлық қызметкерлер ұқсас, бір типті операцияларды-бухгалтерлік есепті, офистік қосымшалармен жұмысты және т.б. орындайды.

Кез келген корпоративтік желінің өз ерекшеліктері бар, дегенмен олардың жалпы саны көп. Корпоративтік желіде жалпы түрде бар:

- жеке офистердің жергілікті есептеу желілері;
- деректерді өңдеу орталықтарында жиналған ресурстар;
- Интернетке шығудың кіші жүйелері;
- мобильді пайдаланушылар және т. б.

Қазіргі уақытта типтік жергілікті есептеу желісі (ЛВС) Ethernet желісі,

желілік трафиктің негізгі түрі – IP болып табылады. Бұл ретте желі бойынша әртүрлі деректер – Интернеттен алынған веб-беттен бастап телефон трафигі мен бейнеконференцбайланыс сеанстарына дейін беріледі.

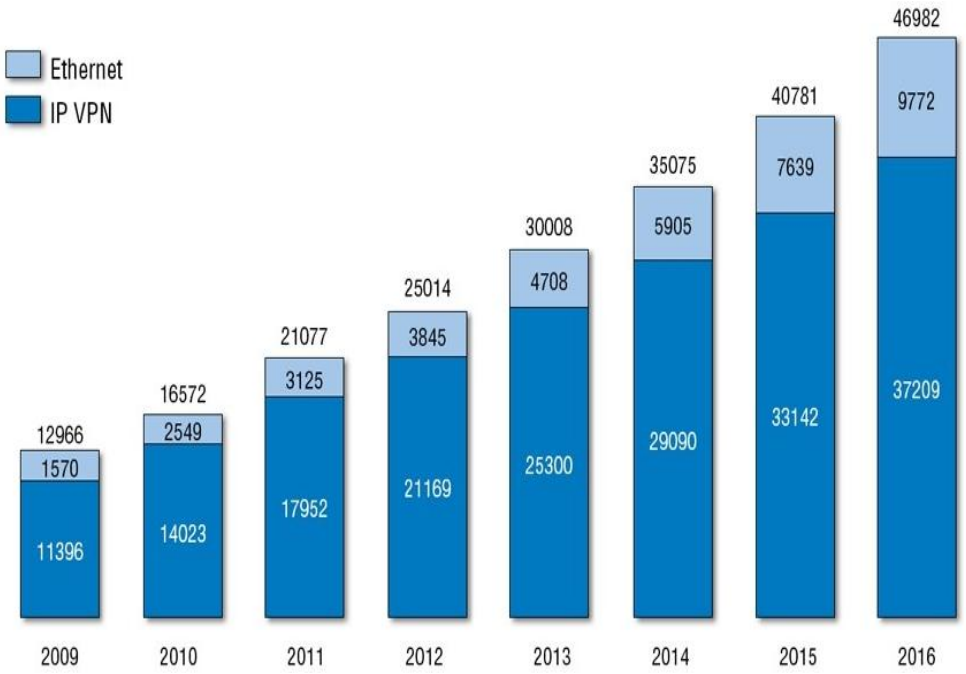
Қашықтағы кеңселерді (пайдаланушыларды) қосу үшін ең қарапайым және қолжетімді нұсқа телефон байланысын пайдалану болып табылады. Бұл жерде ISDN желісін пайдалануға болады. Желі тораптарын біріктіру үшін көптеген жағдайларда деректерді берудің жаһандық желілері қолданылады. Сонымен қатар, байланыс арналарының санын азайтуға мүмкіндік береді және де маңызды емес – қолданыстағы жаһандық желілермен жүйенің үйлесімділігін қамтамасыз етеді.

Деректерді берудің бөлінген корпоративтік желілерін құру үшін әдетте деректерді беру желілерінің операторлары ұсынатын қызметтер пайдаланылады:

- коммутациялық қатынау;
- физикалық бөлінген байланыс желісі;
- сандық бөлінген желі;
- оператордың пакеттік желісіндегі арна (Frame Relay, ATM);
- VPN арнасы.

Интернет ғаламдық желісін кеңейту, IP-қосымшалардың кең таралуы-осының барлығы сервис-провайдерлерге өзінің тапсырыс берушілеріне бірқатар тартымды жаңа қызметтерді ұсынуға мүмкіндік берді. Жаңа Әлем телекоммуникация көрсетеді және көрсетіп, іргелі өзгерістер, бизнес-сервис-провайдерлердің, жиі қызмет бағдарланған желісі (мен тұрған қарапайым қолдау rsvp), және ауысады модельдерге, бағдарланған бизнес және қызмет көрсету қосылған құндылық (қоса алғанда пакетную телефония және электронды коммерция) ұсынылатын басқа қарапайым қызмет трафигін жіберу [1].

Cahners In-stat Group 2003 жылдан бастап желілік VPN (яғни аутсорсингке операторларға берілген виртуалды жеке желілер) нарықта ең таралған VPN түрі болады деп санайды (1.2 сурет). Соңғы пайдаланушылар қызмет көрсетудің кепілді сапасы (SLA), желілердің ауқымдылығы мен икемділігі және VPN тұрақты қолжетімді қызметтерін кең таңдау туралы келісімдерді жиі талап ететін болады. Осының бәрі компаниялардың көпшілігі өздерінің жеке иелерінен VPN-ге пайдаланылатын және сыртқы кәсіби мамандар қызмет көрсететін желілерге көшуге мәжбүр етеді.



Сурет 1.2 - Жеке желілерден VPN-ге өту.

Бүгінгі таңда бірнеше қашықтағы филиалдары бар көптеген ұйымдарда корпоративтік ақпараттық ресурстарға, мысалы, деректер базасына жедел қол жеткізу, филиалдармен байланысты ұйымдастыру проблемаларының әртүрлі шешімдерін іске асыру талап етіледі. Бұдан басқа, компаниялар мен банктер өздерінің алыс бөлімшелері мен басқа қалаларда немесе тіпті елдерде «мобильді» қызметкерлерге сапалы телефон, факсимильдік және бейнеконференциялық байланыс, сондай-ақ электрондық поштаға қол жеткізу.

Үйде жұмыс тәжірибесінің (telecommuting) дамуымен және SOHO (шағын және үй кеңсесі) секторының кеңеюімен ақпаратқа қол жеткізу жылдамдығы ерекше өзектілікке ие болады. Бұл бағытқа қызығушылықты тартуға оның кеңселердің ауданын айтарлықтай қысқартуға және жұмысқа бөле алатын уақытты ұлғайтуға, көлік магистральдарының жүктелуін азайтуға және нәтижесінде қоршаған ортаның автомобильдік газдармен ластануына мүмкіндік береді.

Көптеген компаниялар бар штатта ұялы пайдаланушылар, олар әдетте кеңседен тыс. Мобильді категорияға корпоративтік ЛС-мен байланыс сеанстары үшін желілік станциялардың бірі немесе жеке адаптер арқылы қосылатын портативті компьютерді, коммутацияланатын желіге, ұялы желіге немесе ISDN арнасына шығатын PC-card стандартының ішкі факс-модемін пайдаланатын тұлғалар жатқызылуы мүмкін.

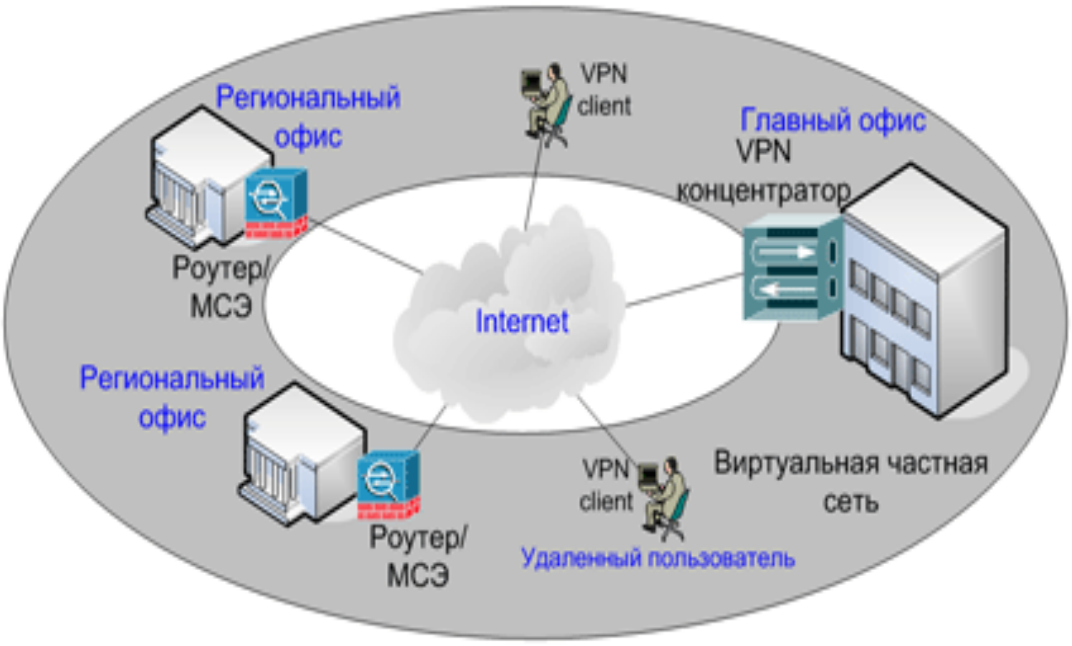
Қазіргі уақытта жабдықтарды қашықтықтан конфигурациялау, бағдарламалық қамтамасыз етуді жүктеу (БҚ), мониторинг және статистиканы Жинау мүмкіндіктері үлкен маңызға ие. Барлық өндірушілер осы функцияларды өз жабдықтарына кірістіреді және осылайша корпоративтік желіні басқаруды едәуір жеңілдетеді.

SOHO үшін жабдықтар көптеген өндіруші фирмалармен шығарылады. Ethernet-порты бар (шағын ЛС қосу үшін) және қосымша Аналогты порты немесе порттары бар (телефон/факс үшін) арзан автономды көпірлер/маршрутизаторлар ұсынатын фирмалардың шешімдері ерекше қызықты. Сонымен қатар, кейбір фирмалар берілетін ақпаратты компрессиялау мүмкіндігі бар жабдықты ұсынады.

Демек, қазіргі заманғы аумақтық-бөлінген корпоративтік есептеу желілері әртүрлі кәсіпорындар мен мекемелерді басқару жүйесінің маңызды құрамдас бөлігі болып табылады, олардың жұмысының тиімділігіне кәсіпорын қызметінің тиімділігі айтарлықтай тәуелді. IP-желілердің (ең алдымен Интернет) жылдам дамуы жаңа үрдісті тудырды – жалпы пайдаланудағы пакеттік желілердің (көпшілік желілер) тасымалының неғұрлым арзан және неғұрлым қолжетімді (бөлінген арналармен салыстырғанда) Ғаламдық корпоративтік байланыстарын құру үшін пайдалану.

Сонымен қатар, корпоративтік желілер үшін пайдаланушыларға қызмет көрсету сапасы, берілген қызметтер жиынтығын және кепілдіктерді ұсыну маңызды мәнге ие, бұл ашық желілерде әрдайым қамтамасыз ете алмайды.

Бұл мәселелерді шешу үшін VPN (Virtual Private Network) виртуалды жеке желілерінің технологиясы қолданылуы мүмкін. Бұл технология орнатылған қосылыстардың қолайлы құны кезінде қауіпсіздік пен сервистердің кең спектрін қамтамасыз ете отырып, жалпы пайдаланудағы пакеттік желілердегі қосылыстарды кепілді Өткізу жолағы бар қорғалған арналарға айналдыруға мүмкіндік береді. Сондықтан бұл технология өзінің желілік ресурстары жоқ көптеген кәсіпорындар мен ұйымдар, ең алдымен банк ұйымдары оның үнемділігіне, қол жетімділігіне және қауіпсіздігіне байланысты талап етеді. Виртуалды жеке желілер (VPN) жеке немесе жария желіде, мысалы Интернетте «нүкте-нүкте» түріндегі қосылымдарды білдіреді. VPN-клиент VPN-сервердің виртуалды портына виртуалды қатынау үшін туннель протоколдары деп аталатын TCP/IP негізіндегі арнайы хаттамаларды пайдаланады.



Сурет 1.3 - Виртуалды жеке желілер

VPN қалыпты жүзеге асыру кезінде клиент интернет арқылы қашықтан кіру серверіне «нүкте-нүкте» түріндегі виртуалды қосылымды бастайды. Алыстан кіру сервері шақыруға жауап береді, шақырушы тараптың түпнұсқалығын тексереді және VPN-клиент пен ұйымның жеке желісі арасында деректерді береді (1.3 сурет).

1.2 VPN технологиясын сыни талдау

VPN технологиясы физикалық қашықтағы объектілерді (желілерді немесе жеке хостарды) жалпы виртуалды желіге біріктіру үшін, қосымша байланыс арналарын салу қажеттілігін айналып өтіп, ортақ пайдалану желілерін пайдалана отырып қызмет етеді. Ақпарат жалпы пайдалану желісі арқылы өтетіндіктен, оны оқу мен өзгертуден қорғау қажет. Ол үшін әртүрлі кодтау құралдары қолданылады. Олар OSI моделінің үшінші (желілік) деңгейінде немесе туннелдеу функциясын пайдалана алады, бұл пайдаланушыларда интернеттен оқшауланған бір жергілікті желіде жұмыс істеу елесін жасайды.

IP-адрестерді қорғау үшін des (56-bit), 3DES (168-bit) және AES (128-bit / 256-bit) алгоритмдерін пайдаланатын IPSec, PPTP, L2TP және т. б. хаттамалары қолданылады. Құпия, құпия, өте құпия немесе аса маңызды санаттарға жатқызылған деректерді қорғау үшін МЕМСТ 28147-89 алгоритмін іске асыратын сертификатталған құралдарды қолдану талап етіледі. Бұл ретте, мұндай қаражатты пайдалану кезінде тиісті лицензиясы бар компаниямен лицензия алу немесе шарт жасасу талап етіледі.

VPN технологиясы ақпаратты сақтаудың негізгі өлшемдеріне жауап

береді: тұтастық, құпиялылық, авторизацияланған қол жеткізу. VPN дұрыс таңдау кезінде масштабтау қамтамасыз етіледі, яғни VPN пайдалану өсу проблемаларын туғызбайды және бизнесті кеңейту жағдайында жасалған инвестицияларды сақтауға көмектеседі. Сонымен қатар, Frame Relay негізінде бөлінген желілер мен желілермен салыстырғанда виртуалды жеке желілер ақпаратты қорғау тұрғысынан сенімді, бірақ 5-10, кейде 20 есе арзанырақ.

Бірақ барлығы кері жағы бар, және VPN технологиясы ерекшелік емес. VPN кемшіліктерінің бірі VPN - құрылғысы арқылы өтетін трафикті криптографиялық өңдеуге байланысты желі өнімділігінің төмендеуі болып табылады. Сонымен қатар, VPN - құрылғылар арасында қорғалған байланыс орнатылған кезде кідірістер; қорғалған деректерді шифрлау және шифрлеу, сондай-ақ олардың бүтіндігін бақылау үшін қажетті түрлендірулермен байланысты кідірістер; берілетін пакеттерге жаңа тақырып қосумен байланысты кідірістер.

Әрбір белгіленген үлгіге толығырақ тоқталайық.

Қолданылатын алгоритмдердің криптографиялық тұрақтылығын есепке ала отырып, кілтті ауыстыру ұзақ уақыт аралығы арқылы мүмкін. Сондықтан VPN құру құралдарын пайдалану кезінде мұндай кідірістер деректермен алмасу жылдамдығына әсер етпейді.

Бұл типтегі кідірістер жоғары жылдамдықты желілер бойынша деректерді беру кезінде ғана байланыс арналарының өнімділігіне әсер ете бастайды.

100 Мбит / с). Басқа жағдайларда таңдалған шифрлеу алгоритмдерін бағдарламалық немесе аппараттық іске асырудың жылдам әрекеті және тұтастықты бақылау әдетте жеткілікті үлкен және «шифрлеу - желіге беру» және «желіден қабылдау – шифрлеу» пакетінің операциялар тізбегінде шифрлау (шифрлеу) уақыты осы пакетті желіге беру үшін қажетті уақыттан едәуір аз.

Мұнда біз VPN-құрылғы арқылы өтетін әрбір пакетке қосымша тақырып қосу сияқты негізгі мәселемен бетпе-бет келеміз. Мысалы, нақты уақытта қашықтағы станциялар мен орталық пункт арасында деректер алмасуды жүзеге асыратын басқару жүйесін қарастыруға болады. Берілген деректер көлемі үлкен емес - 25 Байттан артық емес, бұл банк саласындағы (төлем тапсырмалары) және IP-телефониядағы деректер өлшемімен салыстыруға болады. Берілетін деректердің қарқындылығы - секундына 50-100 айнымалы. Бір айнымалы процестің мәні бар пакеттің ұзындығы 25 байт (айнымалы аты - 16 байт, айнымалы мәні - 8 байт, қызметтік тақырыбы - 1 байт). IP протоколы пакеттің ұзындығына тағы 24 байт қосады (IP-пакеттің тақырыбы).

Frame Relay арналарын пайдаланған жағдайда тағы 10 байт FR-тақырып қосылады. Барлығы 59 байт (472 бит). Осылайша, қалыпты үшін жұмыс өткізу қабілеті 64 кбит/с болатын шектеулерге жақсы сәйкес келетін Өткізу жолағы қажет.

VPN құралдарын пайдалану кезінде біз не аламыз? IPSec протоколы және көрсетілген параметрлер үшін талап етілетін өткізу қабілеті 6% - ға (67,8 кбит/с) артады. «Континент» бағдарламалық-аппараттық кешенінде

пайдаланылатын хаттама үшін әрбір пакетке қосылатын қосымша тақырып бар болғаны 36 байтты (немесе 26 - жұмыс режиміне байланысты) құрайды, бұл осы жағдайларда жұмыста кідіріс тудырмайды (тиісінше 57 және 51 кбит/с). SSL протоколы және сол шарттар үшін қосымша тақырып шифрлау алгоритміне байланысты 21 немесе 25 байт құрайды, бұл да өнімділіктің төмендеуін болдырмайды.

Мысалы көрнекілік үшін алынған, бірақ берілетін деректер көлемі көп болған сайын, енгізілген кідірістер соғұрлым көп болады. Мұндай желі өнімділігінің құлдырауы емес, сыни үшін көптеген қосымшалардың және сервистердің, бірақ, мысалы, губительно беру үшін ағынды аудио және видео. Ақпараттық технологиялардың дамуымен қоса үлкен көлемдегі трафикті жылдам беру қажеттілігі барлық өсуде, сәйкесінше байланыс арналарының өзіне де, сондай-ақ оларды қорғау құралдарына да талаптар да өсуде.

Батыс талдаушыларының пікірінше, мысалы, қаржы секторында жұмыс істейтін пайдаланушылардың тек 5% ғана осындай жоғары стандарттарды қажет етеді. Қалған 95% байланыспен байланысты проблемаларға соншалықты байыпты емес, ал ақпаратты алуға кететін уақыт көп шығын орасан шығындарға әкелмейді.

1.2.1 IPsec VPN және SSL VPN артықшылықтары мен кемшіліктері

Бизнес қажеттілігі және ақпараттық базаны (АҚ) құру тәсілдері қазіргі уақытта VPN технологиясын дамытудың екі негізгі бағытын қалыптастырды: бұл IPsec VPN және SSL VPN. Олардың әрқайсысының негізгі артықшылықтары мен кемшіліктері неде екенін көрейік.

IPSec (IP Security) - деректерді шифрлау, олардың тұтастығы және аутентификация мәселелерін шешетін хаттамалар жиынтығы. IPSec желілік деңгейде жұмыс істейді. Осылайша, деректерді қорғау желілік қолданбалар үшін ашық болады. SSL (Secure Socket Layer) - қосымшалар деңгейінің ХАТТАМАСЫ, негізінен қашықтағы қосымшалар арасында қорғалған ақпарат алмасу үшін пайдаланылады (көбінесе бұл Web - серверлерге жүгіну), IPSec жоғары деңгейдегі хаттамалар пакеттерімен бірдей жүгінеді, яғни олардың мазмұнына назар аудармай-ақ, аутентификацияланады және шифрланады. Бірақ SSL жұмыс істеу үшін сенімді көліктік хаттама (мысалы, TCP) қажет. IPSec сенімділігіне әлі байланыс орнатылған порт туралы ақпарат зиянкестер үшін қол жетімсіз екеніне кепілдік беріледі.

IPSec байланыс орнатудың үш түрін қолдайды: Gateway-to-Gateway (шлюзден шлюзге);

Gateway-to-Host; Host-to-Host.

SSL тек екі хост немесе клиент пен сервер арасындағы байланысты қолдайды.

IPSec сандық қолтаңбаны және Secret Key Algorithm пайдалануды

қолдайды, ал SSL - тек сандық қолтаңба. IPsec және SSL ашық кілттері бар инфрақұрылымды пайдалана алады - PKI. IPSec артықшылығы: шағын жүйелер үшін PKI орнына тапсырманы айтарлықтай жеңілдететін preshared keys қолдануға болады. SSL-да қолданылатын әдістер сервер мен клиент арасында қорғалған байланыс орнату үшін өте қолайлы. Сонымен қатар, IPSec-ті желілік деңгейде жұмыс істейді, бұл алушы мен көзінің мекен-жайын неғұрлым жоғары деңгейдегі аутентификация сияқты табыспен қадағалауға мүмкіндік береді. SSL тек көлік деңгейі және одан жоғары ақпаратқа қол жеткізуге болады. IPSec кемшіліктері арасында-бастапқы пакетке қосылатын қосымша ақпараттың үлкен көлемі. SSL жағдайында бұл өлшем әлдеқайда аз. IPSec қысу үшін IPComp протоколы қолданылады. SSL кем дегенде сығуды пайдаланады, және тек OpenSSL оны толық қолдайды. IPSec кезінде қысу алгоритмдерін пайдалану оларды әртүрлі жағдайларда қолдану кезінде әртүрлі нәтижелерге әкелуі мүмкін: өнімділік ұлғаяды да, азаяды да қабілетті.

Нәтиже шифрлеу, сығу жылдамдығының және деректерді беру жылдамдығының арақатынасына байланысты. Көптеген шифрлау алгоритмдері жылдам қысу алгоритмдерін жұмыс істейді. Демек, бұл жұмыстың бәсеңдеуіне әкеледі. Бірақ жіберу жылдамдығы төмен болған жағдайда қысу өнімділігін айтарлықтай арттырады.

SSL «VPN клиент-сервері» сегментінде (IPSec-пен салыстырғанда) өте тез дамып келеді, өйткені аз шығындарда ақпараттың қорғалуының қажетті деңгейін ұсынады. Ал SSL IPSec-пен тең бәсекелесуге тырысса да, бірақ IPv6-дің пайда болуы және соңғы стандартталуымен жағдай өзгеруі тиіс.

Не таңдау-тек Тапсырыс берушіге ғана шешу. Ақпаратты қорғау құралдарын өндіру бойынша көшбасшылар екі бағытты дамытуды жақсы біледі және нақты клиенттің жеке қажеттіліктеріне сәйкес келетін оңтайлы шешім ұсынуға қабілетті.

1.3 IP VPN технологияларын талдау

Виртуалды жеке желі терминімен (Virtual Private Network - VPN) ашық жаһандық желі бойынша пайдаланушылардың бақыланатын тобы шегінде қауіпсіз және сапалы байланысты қамтамасыз ететін технологиялардың кең шеңберін түсінеді.

VPN-технологиялардың мақсаты бір кәсіпорынның деректер ағындарын жария желінің барлық басқа пайдаланушыларының деректер ағындарынан барынша оқшаулаудан тұрады. Оқшаулылық ағындардың өткізу қабілетінің параметрлеріне және берілетін деректердің құпиялылығына қатысты қамтамасыз етілуі тиіс.

IP VPN−бұл ұйымның құрылымдық бөлімшелерін өзара байланыстыруға және Қазақстанның бүкіл аумағында және шетелде серіктес компаниялардың желісін біріктіруге мүмкіндік беретін қызмет. Офистер мен аумақтық

бөлімшелердің өзара қашықтығына қарамастан IP VPN олардың кез келген бизнес−қосымшалардың толық байланысын, жұмысын және өзара іс-қимылын қамтамасыз етеді.

Қазіргі таңда MPLS (Multi Protocol Label Switching) технологиясын пайдалана отырып құрылған жеке корпоративтік байланыс желісі (VPN) барлық осы қажеттіліктерді ескеретін ақпараттық кеңістік құрудың орталық буыны бола алады. VPN көмегімен шешуге болатын негізгі міндеттер: толық байланыс топологиясын қолдайтын қорғалған корпоративтік желіні құру («әрқайсысы»); Frame Relay және ATM желілерінің қауіпсіздік деңгейіне сәйкес келетін ақпаратты берудің жоғары қауіпсіздігі; әр түрлі бизнес-қосымшаларды интеграциялау, олардың әрқайсысы трафиктің тиісті түріне арналған («деректер», «дауыс», «бейне») үш қызмет көрсету сыныптарымен қамтамасыз етіледі; файлдармен және хабарламалармен алмасу; телефония; бейнеконференцбайланыс; интерактивті қашықтықтан оқыту; құжаттар мен деректер базаларымен бірлескен жұмыс; корпоративтік ақпараттық http серверлеріне қол жеткізу.

Қызметтің артықшылықтары:

- VPN технологиясы желінің жұмысқа қабілеттілігін қолдау шығындарын айтарлықтай төмендетуге мүмкіндік береді: пайдаланушы тек арнаны жалға алу үшін абоненттік төлемді ғана төлейді. Айтпақшы, арналарды жалға алу Интернет желісінің кең ауқымдылығы салдарынан қандай да бір қиындық тудырмайды;
- желі құрылымын ұйымдастыру және қайта құру кезінде ыңғайлылығы мен жеңілдігі;
- IP VPN қызметі шеңберінде әртүрлі бизнес−қосымшалар үшін IP MPLS арқылы тарату сапасына қойылатын әртүрлі талаптарды ескере отырып, трафикке қызмет көрсетудің 3 сыныбы қолдау көрсетеді: «нақты уақыт» (дауысты/бейнені беру үшін), «премиальный» (EDI/http), «стандартты» (ftp/e−mail).);
- IP VPN интернеттен логикалық деңгейде бөлінген, ақпаратты тарату қауіпсіздігі Frame Relay және ATM желілерінің қауіпсіздік деңгейіне сәйкес келеді.
- Магистральды IP-желі Қазақстан Мемтехкомиссиясының ақпаратты қорғау жөніндегі талаптарына сәйкес келеді;
- «Әрқайсысымен бірге» схемасы бойынша салынған байланыс желісі бір-бірінен алшақ клиент офистерінің арасында ақпарат алмасуды оңай жүзеге асырады;

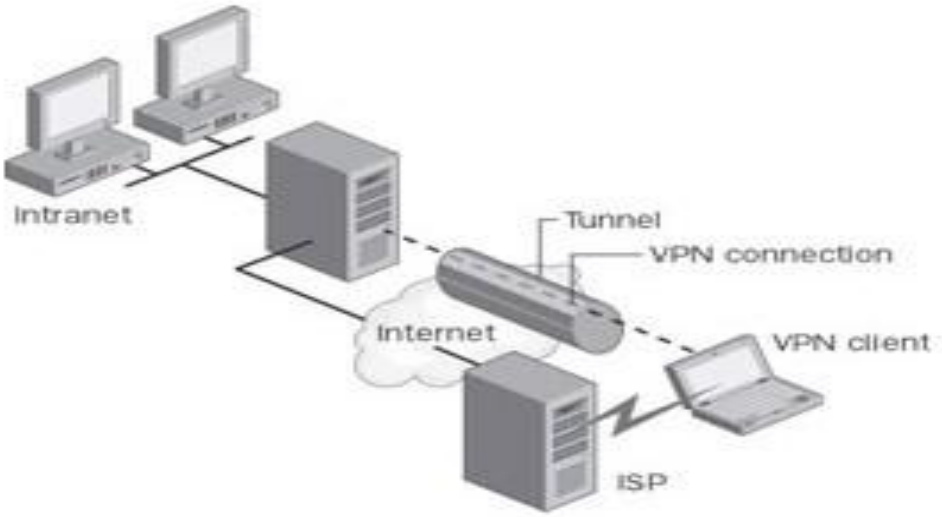
Барлық VPN желілерін шартты түрде үш негізгі түрге бөлуге болады:

- ішкі корпоративтік VPN (Intranet VPN);
- аралық VPN (Extranet VPN));
- Қашықтан қол жеткізу VPN (Remote Access VPN). Интражелі.

VPN ең қарапайым нұсқасы болып табылады, ол ашық байланыс арналары арқылы өзара іс-қимыл жасайтын бір ұйымның бірнеше таратылған филиалдарын бірыңғай қорғалған желіге біріктіруге мүмкіндік береді.

Қашықтағы қатынау VPN. Алыстан қатынайтын VPN жұмыс істеу принципі қарапайым: пайдаланушылар жаһандық желіге (POP) қатынаудың жергілікті нүктесімен байланыс орнатады, содан кейін олардың шақырулары Интернет арқылы туннелденеді, бұл қалааралық және халықаралық байланыс үшін төлемді немесе тегін қалааралық нөмір (Tollfree Numbers) иелеріне шоттар беруді болдырмауға мүмкіндік береді.

Содан кейін барлық шақырулар тиісті тораптарға шоғырланады және корпоративтік желіге жіберіледі. Алайда, Интернетті біріктіруші Магистраль ретінде пайдалануға байланысты ақпаратты қорғау тетіктері осы технологияның өмірлік маңызды элементтеріне айналады.



Сурет 1.4 - Алыстан қатынайтын ішкі корпоративтік VPN және VPN

IP VPN-ге бір қосылу шеңберінде клиент кез келген бизнес-қосымшаларды пайдалана алады: кеңселер арасында телефон байланысын немесе бейнеконференцбайланысты ұйымдастыру, компания қызметкерлерінің құжаттармен және деректер қорымен ұжымдық жұмысын қамтамасыз ету;

Сіз қандай да бір бизнес-қосымша үшін қызмет көрсету класын дербес орнатуға мүмкіндік аласыз: трафикті таңбалау клиенттің маршрутизаторында жүзеге асырылады.

Берілген ақпарат көлемінің өсуімен техникалық шешім бұрынғыдай қалады: оны гигабитті жылдамдыққа дейін оңай масштабтау.

1.3.1 VPN-да қызмет көрсету сапасы

VPN-да қызмет көрсету сапасының параметрлері Көліктік қызмет көрсету сипаттамасы болып табылады: кідіріс, кідіріс вариациясы және желі арқылы тасымалдау кезінде жоғалған пакеттердің үлесі. Бұл параметрлер желі

провайдері мен клиент арасында жасалатын қызмет көрсету сапасы туралы келісімде айтылады. Қызмет көрсету сапасын қамтамасыз ету үшін желінің протоколдары мен жабдықтарына кіріктірілген қосымша технологиялық механизмдер қажет.

FR технологиясы әртүрлі виртуалды арналар үшін дифференциалды қызмет көрсету сапасын қолдау үшін кіріктірілген мүмкіндіктерге ие. Кепілдік берілетін сапа параметрлері орташа келісілген өткізу қабілеті және трафиктің максималды пульсациясы болып табылады.

Егер клиент әр түрлі қызмет көрсету сапасымен трафик түрлерін беру керек болса, онда ол тек тиісті сападағы бірнеше виртуалды арналарға тапсырыс береді.

ATM технологиясы FR технологиясына қарағанда қызмет көрсету сапасының параметрлерін сақтаудың аса жұқа процедуралары бар. ATM берілетін пакеттердің кідірісі бойынша нақты уақыт трафигіне кепілдік береді.

Internet пайдаланушыларға сараланған қызмет көрсету кепілдігін бере алмайды.

Жеке IP-желілерде провайдер өз клиенттеріне дифференциалды қызмет көрсетуге арналған тетіктер жиынтығы бар. Мұндай механизмдерге басым қызмет көрсету (WFQ кезектеріне қызмет көрсету), өткізу жолағын резервтеу (RSVP ресурстарын резервтеу хаттама), виртуалды арналарды қолдау (MPLS таңбаларын коммутациялау хаттамасы) жатады.

VPN-да деректерді қорғау.

Виртуалды жеке желілер трафикті беру үшін толыққанды көлік ретінде пайдаланылу үшін, тарату сапасына кепілдік ғана емес, сонымен қатар берілетін деректердің қауіпсіздігіне кепілдік қажет. Көптеген мамандар, ең алдымен, термин – виртуалды жеке желілер деректерді қауіпсіздікпен байланыстырады.

Корпоративтік желіні кез келген ашық желіге қосу кезінде қауіптің екі түрі пайда болады:

1) осы желіге логикалық кіру нәтижесінде зиянкес алған корпоративтік желінің ішкі ресурстарына рұқсатсыз қол жеткізу;

2) ашық желі арқылы беру процесінде корпоративтік деректерге рұқсатсыз қол жеткізу.

Виртуалды жеке желі қауіпсіздік деңгейі бойынша осы қауіп-қатерлер іс жүзінде жоқ шынайы жеке желіге жақындау үшін, VPN бірінші және екінші типті қауіптерді бейнелеуге арналған құралдарды қамтуы тиіс.

1.3.2 VPN құрылғылар

Виртуалды жеке желілер бір-бірінен көптеген сипаттамалармен ерекшеленеді: VPN-құрылғылардың функционалдық мүмкіндіктерінің жиынтығы, VPN-құрылғылардың орналасу нүктелері, осы құрылғылар жұмыс

істейтін платформа типі, шифрлау және аутентификация хаттамаларымен қолданылатын.

VPN құрылғыларының бірнеше түрі бар:

екі немесе одан да көп желілік интерфейсі және аппараттық криптографиялық қолдауы бар жеке VPN аппараттық құрылғысы;

стандартты операциялық жүйені VPN функцияларымен толықтыратын жеке бағдарламалық шешім;

қорғалған арнаның қосымша функциялары есебінен брандмауэрді кеңейту;

маршрутизаторға немесе коммутаторға орнатылған VPN құралдары

VPN құрылғылары виртуалды жеке желілерде шлюз немесе клиент рөлін атқара алады.

VPN шлюзі-бұл бірнеше желілерге қосылған желілік құрылғы, ол артындағы көптеген хост үшін шифрлау және аутентификациялау функцияларын орындайды. Шлюзді орналастыру брандмауэрді орналастыруға ұқсас болуы тиіс, яғни ол арқылы ішкі корпоративтік желіге арналған барлық трафик өтетіндей болуы тиіс. Кәсіпорынның қауіпсіздік стратегиясына байланысты Шығыс пакеттері шифрланады немесе ашық түрде жіберіледі немесе шлюзбен бұғатталады. Сонымен қатар, VPN - шлюздің сыртқы мекен – жайы, ал ішкі мекен-жайы-шлюздің артындағы кейбір хосттың мекен-жайы болып табылады. VPN шлюзі жоғарыда аталған барлық тәсілдермен, яғни жеке аппараттық құрылғы, жеке бағдарламалық шешім түрінде, сондай-ақ VPN функцияларымен толықтырылған брандмауэр немесе маршрутизатор түрінде іске асырылуы мүмкін.

VPN клиенті-әдетте дербес компьютер базасында бағдарламалық немесе аппараттық-бағдарламалық кешен. Оның желілік көліктік қамтамасыз етуі құрылғы VPN шлюздерімен және/немесе VPN клиенттерімен алмасатын трафикті шифрлау және аутентификациялау үшін модификацияланған. Әдетте VPN-Клиентті іске асыру бағдарламалық шешім болып табылады.

Кәсіпорынның виртуалды жеке желісін құру үшін VPN - шлюздер де, VPN-клиенттер де қажет. Шлюздер райынан қорғау үшін жергілікті желілер, VPN-клиенттер үшін қашықтағы және мобильді пайдаланушыларды қажет ететін орнатуға қосылыстар корпоративтік желімен Интернет арқылы.

1.4 Тақырыптың қойылымы

Қазіргі таңда IP/VPN/MPLS технологиясы кез келген заманауи байланыс операторымен телекоммуникациялық қызметтерді ұсыну кезінде де - факто стандарты болып табылады. Бұл қазіргі уақытта IP протоколының көмегімен ақпаратты беруді біріздендіру жағына қарай қозғалыс жүруіне байланысты. Осы технология негізінде салынған желілер бұрынғысынша клиенттерге дәстүрлі қызметтерді ұсынуға және сонымен қатар қызметтердің прогрессивті

пакетіне біртіндеп көшуге мүмкіндік береді. Бұл ретте желіні пайдалану кезінде уақытша шығындар мен үстеме шығындарды қысқартумен ұштасқан кәбілдік Инфрақұрылым пайдаланылады. Нәтижесінде артықшылықтарды барлық тараптар алады: «Қазақтелеком» оператор ретінде, Кез келген мекемесіинвестор және негізгі клиент ретінде, Қазақстанның көптеген қаржы институттары.

Кез келген мекемесі бұрыннан бері қаржы компанияларының арасында Қазақстан Республикасындағы ең жоғары технологиялық банктердің бірі болып саналады. IP/VPN/MPLS жобасы бірнеше бірегей ерекшеліктерге ие, олардың бірі «қос мақсаттағы өнім» болып табылады. Яғни топ компаниялары ақпарат алмасу үшін сенімді көлік ортасын алады және сонымен бірге телекоммуникациялық қызметтерге маманданған еншілес компания коммерциялық қызметті жүзеге асыра алады.

Ірі банктердің бірі бола отырып, Кез келген мекемесі қаржы нарығының барлық сегменттерінде бар. Бүкіл тарихы жинақ ісінің дамуымен байланысты елдегі ең кең филиалдық желісі бар банк бола отырып, Кез келген мекемесі дәстүрлі түрде ұзақ мерзімді басымдық ретінде халықтың қалың жігі үшін қызмет көрсету спектрін кеңейтуді сақтап келеді.

Кез келген мекемеде желі құрудың мақсаттары:

- жалпы Қазақстан Республикасының Кез келген мекемесімен қаржы жүйесінің жұмыс істеу тиімділігін арттыру;

- Кез келген мекеменің филиалдары, сондай-ақ басқа да несие ұйымдары үшін виртуалды жеке желі (ТЖА) қызметін ұсыну;

- әр түрлі трафикті, соның ішінде басымдықтың, дауыстың, бейненің әр түрлі деңгейіндегі деректерді беру.

Жергілікті байланыс желілері нарығында дәстүрлі және баламалы операторлар арасындағы өсіп келе жатқан бәсекелестік құны тұрғысынан неғұрлым тиімді қызметтер ұсыну мақсатында сол және басқаларды да өз желілерін оңтайландыруға мәжбүр етеді. Әдетте, бұл сөйлеуді, деректерді, мультимедианы және Интернетке қатынауды қамтитын бірыңғай пакет.

Осы бітіру жұмысының мақсаты бірыңғай инфрақұрылымды ұйымдастыру міндеті жиі туындайтын кеңселердің географиялық бөлінген желісі бар бірыңғай корпоративтік желіні құру мүмкіндігі болып табылады. Корпоративтік желінің негізгі міндеті – әр түрлі тораптарда орналасқан дауысты, деректерді, жүйелік қосымшаларды-деректер базасы, пошта жүйелері, Есептеу ресурстары, файлдық сервис және оларға компания қызметкерлерінің қол жетімділігі сияқты бір мезгілде беру болып табылады.

Жоғарыда баяндалғанның негізінде корпоративтік желінің бірыңғай инфрақұрылымын ұйымдастыру мақсаты:

- біріктірілген АТ-инфрақұрылымын қалыптастыру;

- бірыңғай ақпараттық кеңістікті қалыптастыру;

- корпоративтік ақпараттық жүйені құру. Келесі міндеттерді шешу үшін көлік желісін ұйымдастыру:

- корпоративтік қосымшалардың деректерін беру (электрондық құжат

айналымы және мұрағат, корпоративтік ақпараттық жүйе (Oracle, 1C), электрондық пошта, хабарландыруларды орталықтандырылған тарату (Instant Messaging), жүйе файлдарын бөлу (DFS), коммерциялық және технологиялық есеп жүйелерінің деректерімен алмасу);

- корпоративтік телефония;
- видеоконференция және бейне бақылау;
- техникалық қолдау қызметі.

Дипломдық жобада қойылған мақсаттарды шешу үшін келесі міндеттерді орындау қажет:

- VPN жүзеге асыру нұсқасын таңдау;
- желілік архитектураның жобаланатын схемасын әзірлеу;
- VPN ұйымдастыру үшін жабдықты таңдау;
- VPN жүзеге асыру модельдері.

Бүгінгі күні ТМД елдері арасында Қазақстандағы телекоммуникация нарығы ең жылдам өсіп келе жатқан және ғылымды қажетсінетін нарықтардың бірі болып табылады.

Телекоммуникациялық сервистің қарқынды дамуына және барлық елдер мен континенттердің қашықтағы ақпараттық ресурстарына қол жеткізу мүмкіндігіне байланысты автоматтандырылған жүйелер мен технологиялардың тиімділік критерийлерін тұжырымдауда: жерсеріктік байланыс пен Дүниежүзілік Internet желісін пайдалану нәтижесінде ақпараттық технологияларды жаһандандыруға екпіндердің ауысуы болды, осының арқасында адамдар ғаламшардың кез келген нүктесінде бола отырып, өзара және жалпы деректер базасымен сөйлесе алады (жетекші тенденция).);

Соңғы онжылдықта компьютерлік техника мен ақпараттық технологиялар адамзат қызметінің барлық салаларына соншалықты терең еніп, қазір кеңселерінің саны кем дегенде екіден асатын кез келген ұйым өзінің ақпараттық және есептеу ресурстарын бірыңғай желіге біріктірмей өз жұмысын білдірмейді.

Бұл дипломдық жобада TCP/IP хаттамаларының стегі қолданылады, өйткені ол тек Internet желісінде желіаралық өзара іс-қимыл кезінде, сондай-ақ ашық жүйелерде қолданылады. Ашық жүйе-бұл халықаралық стандартты хаттамаларды іске асыру арқылы басқа жүйемен өзара іс-қимыл жасауға қабілетті жүйе. Ашық жүйелер соңғы және аралық жүйелер болып табылады. Алайда, ашық жүйе басқа ашық жүйелерге қол жетімді болуы мүмкін емес. Бұл оқшаулау компьютерлерде және коммуникация құралдарында ақпаратты қорғауға негізделген техникалық мүмкіндіктерді пайдалану арқылы немесе физикалық бөлу жолымен қамтамасыз етілуі мүмкін.

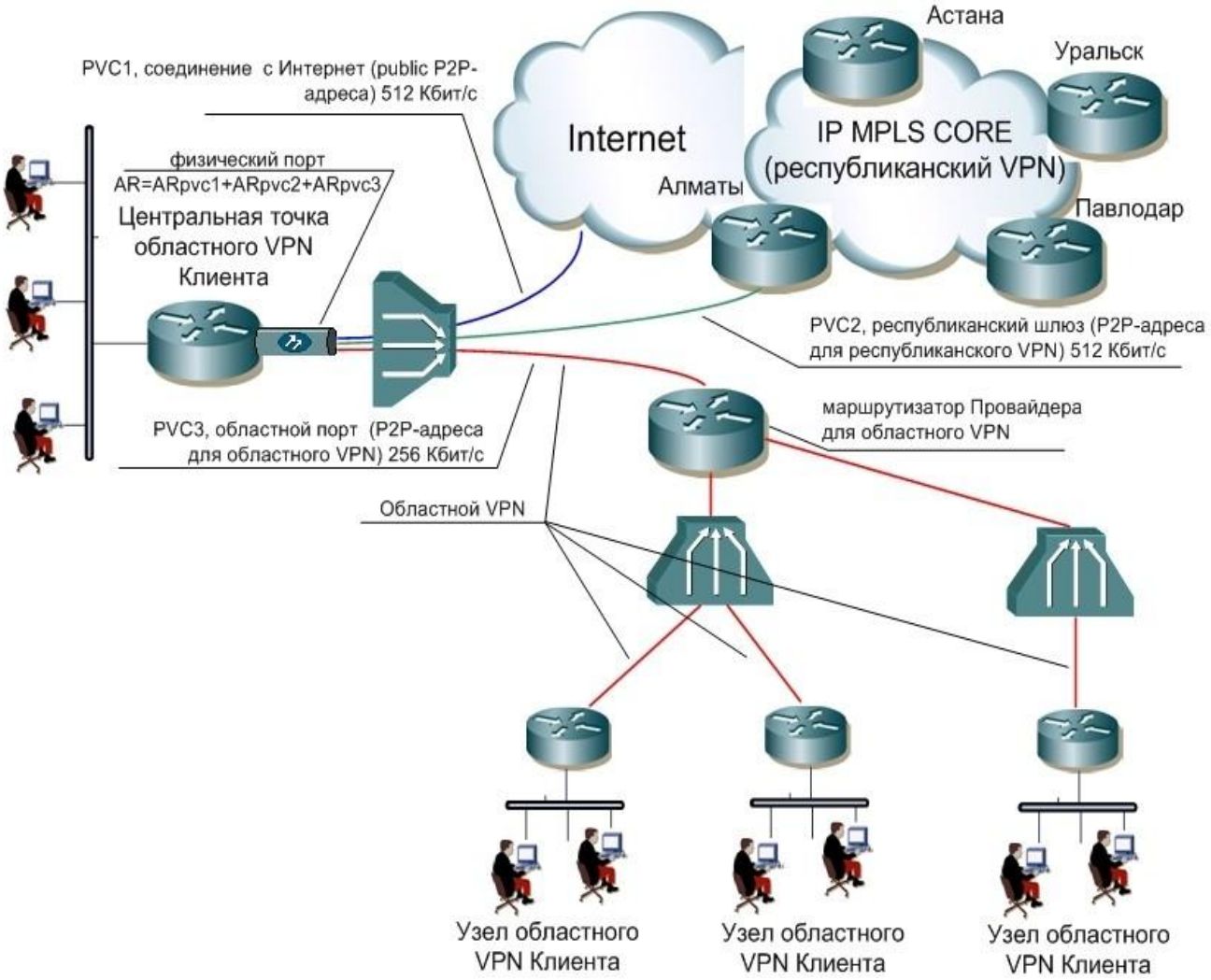
2 IP/VPN бірыңғай корпоративтік желісін құру

2.1 Желі құрылымы

Корпоративтік желіні құру бірнеше аумақтық бөлінген жергілікті желілер арасындағы өзара іс-қимылды қамтамасыз етуге негізделеді.

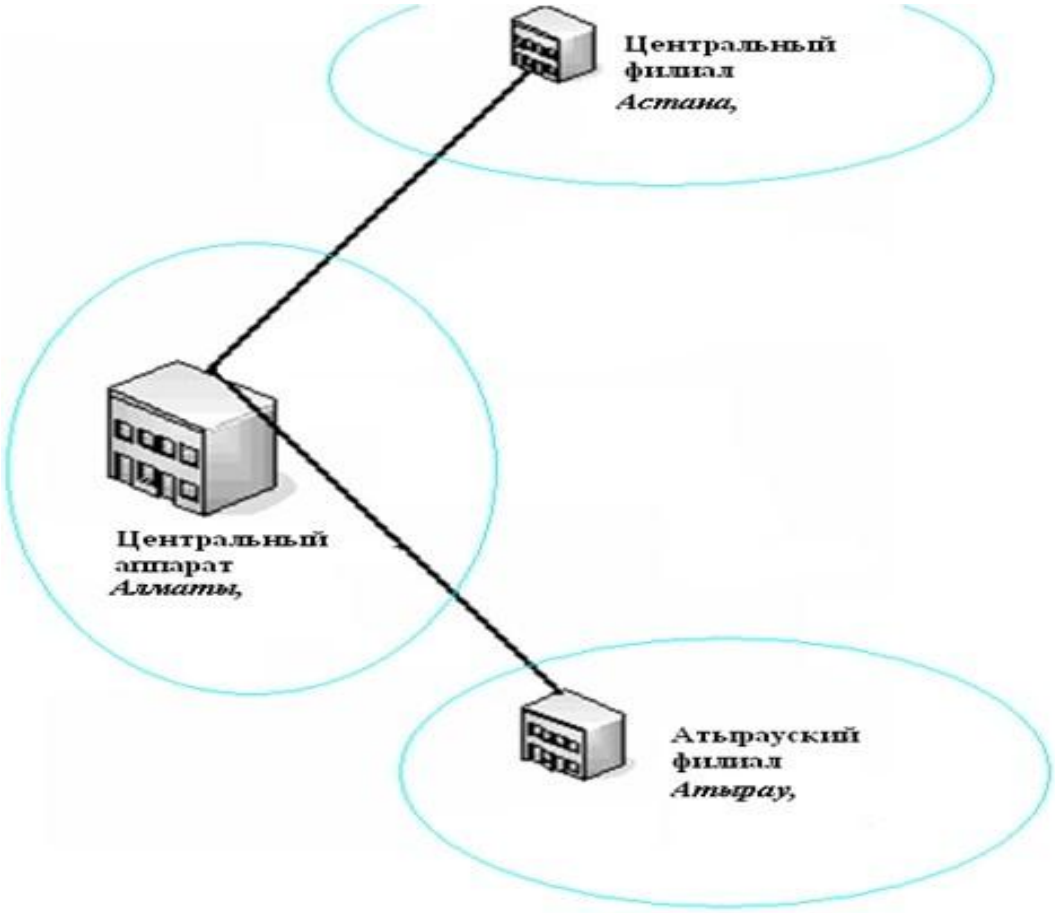
Ұйымдастырылған корпоративтік желінің топологиясы – Тапсырыс берушіге тапсырыс берушінің беж бөлімшелерін бірыңғай толық байланысқан желіге біріктіруге мүмкіндік беретін жалпақ топология (Multipoint Intranet). Тапсырыс берушінің талаптарына сәйкес, желі топологиясы-жұлдыз.

IP/VPN корпоративтік желісін құрудың логикалық сұлбасы 2.1-суретте келтірілген. Қызметті ұсыну сызбасы ҚР барлық облыстары үшін бірдей.



Сурет 2.1 - Корпоративтік желіні құрудың логикалық сұлбасы

2.2 суретіне сәйкес, біздің клиент – кез келген мекеме үшін тікелей қызмет көрсету схемасын қарастырайық.

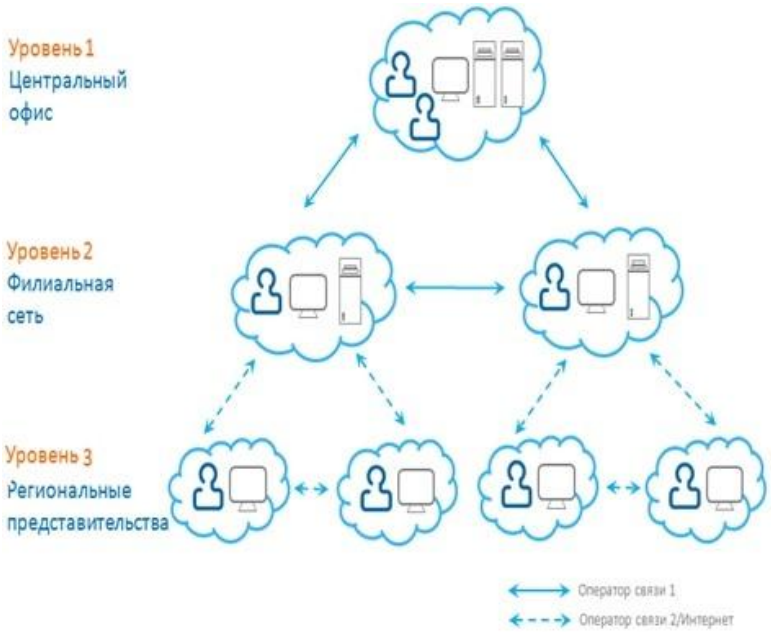


Сурет 2.2 - Кез келген мекеменің филиалдар үшін корпоративтік желіні құру схемасы

Әдетте, облыстық IP VPN ұйымдастыру үшін келісілген қатынау жылдамдығы бар порт беріледі. Республикалық IP VPN ұйымдастыру үшін келісілген қатынау жылдамдығы бар шлюз ұсынылады.

ҚР кез келген мекемесінің филиалдары орналасқан әрбір облыста (Атырау, Алматы, Ақмола) IP VPN бір республикалық шлюзі ұйымдастырылады. Бұл бір облыста бір ғана IP VPN республикалық шлюзі болуы мүмкін дегенді білдірмейді,ал осы саладағы қалған нүктелер міндетті түрде облыстық болуы тиіс. Көптеген клиенттер бір облыстың шегінде бірнеше республикалық шлюздерді ұйымдастырады. Бұл жүйенің сенімділігін арттыру үшін жасалады. Т. е. егер облыста бір республикалық VPN және облыстық VPN 20 нүктесі болса, онда Орталық нүкте бұзылған жағдайда клиенттің қалған 20 бөлімшесі көрсетілген орталық нүкте сервисін қалпына келтіргенге дейін жұмыс істемейді. Республикалық VPN арнасы үшін ай сайынғы жалдау ақысының құны облысқа қарағанда жоғары болғандықтан, көбінесе республикалық шлюздерді клиент клиенттің ірі кеңселері орналасқан және сервисті ұзақ уақытқа үзуге жол берілмейтін нүктелерді таңдайды.

Таратылған корпоративтік желі топологиясы



Сурет 2.3 - Таратылған корпоративтік желі топологиясы

Желі құру кезінде оңтайландырылатын критерий оны құру және пайдалану құнын барынша алуан түрлілік және ұсынылатын байланыс қызметтерінің жоғары сапасы кезінде барынша азайту болып табылады.

2.2 Кез келген филиалдары үшін республикалық корпоративтік желіні құру (республикалық IP VPN)

Республика ауқымындағы корпоративтік желіні құру қызметі ҚР түрлі салаларында орналасқан клиенттің сайттарын бірыңғай бөлінген виртуалды желіге біріктіруге мүмкіндік береді. Оператор желісі клиенттің тораптары арасында IP-трафикті бағыттауды қамтамасыз етеді. Клиентке ұсынылатын виртуалды желінің мекен-жай кеңістігі толығымен тәуелсіз және Клиент еркін таңдап алуы мүмкін. Клиент тұрғысынан, Оператор оған қалалық VPN клиентінің барлық орталық тораптарын қосатын виртуалды маршрутизаторды (IP/VPN/MPLS желісі) ұсынады. Бұл қызметті ұйымдастыру кезінде статикалық және динамикалық (BGP) маршруттау хаттамалары пайдаланылуы мүмкін.

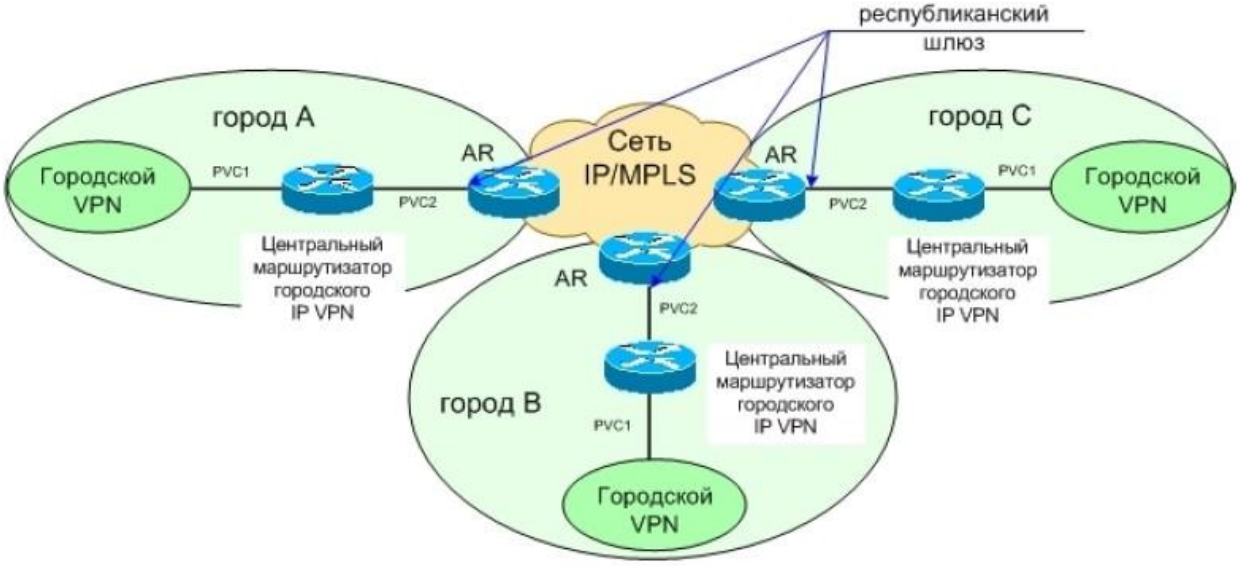
2.4 суретте қызмет көрсету тәртібін қарастырайық. IP VPN орталық торабының маршрутизаторында клиентте қолданыстағы жалғау желісі бойынша қалалық метр желісінің агрегациялық маршрутизаторына (AR) қосымша подинтерфейс (PVC) құрылады. AR маршрутизаторында VPN пакеттерін маршруттау үшін қолданылатын IP-маршруттаудың жеке кестесі (бұдан әрі-VRF-кесте) жасалады. RD және RT тиісті мәндерімен Республикалық VPN клиенттің тиесілі VRF, ол арқылы ҚР басқа да облыстарында корпоративтік желінің басқа орталық тораптарымен байланыс қамтамасыз

етіледі.

VLAN нөмірін таңдау «VLAN бөлу жөніндегі ұсыныстарға» сәйкес жүзеге асырылады.

RD және RT (export-import) мәндері талап етілетін топологияға және трафик матрицасына сәйкес беріледі.

RD тағайындау «RD және RT нөмірлерін бөлу жөніндегі ұсыныстарға» сәйкес жүргізіледі. Осы VRF (VPN) PE-маршрутизатордың тиісті порттарында SLA жасалған сәйкес policing теңшеледі.



Сурет 2.4 - Қызметті ұйымдастырудың логикалық схемасы.

Республикалық IP VPN. PE-оператор тарапынан (MPLS Домен) шекаралық маршрутизатор, оған клиент торабы тарапынан маршрутизаторлар қосылады.

Әр түрлі VPN ішкі жүйелері қиылысуы мүмкін болғандықтан, олардың бірегейлігін қамтамасыз ету үшін VPN ішкі желілерінің префикстері екі бөліктен тұрады:

- Route Distinguisher (RD) - маршруттық ақпаратты кемсітуші. RD vpn префиксінің бірегейлігін қамтамасыз етеді (8 байт);

- IPv4 network address - дәстүрлі IPv4 префиксі (4 байт).

RD және IPv4 жұбы ретінде ішкі желі префиксін ұсыну vpn-Ipv4 address family деп аталады.

RD үш өрістен тұрады:

- түрі (2 байт) - бұл өріс келесі өрістердің құрылымы мен өлшемін анықтайды;

- жаһандық (әкімшілік) компонент;

- жергілікті компонент (индекс).

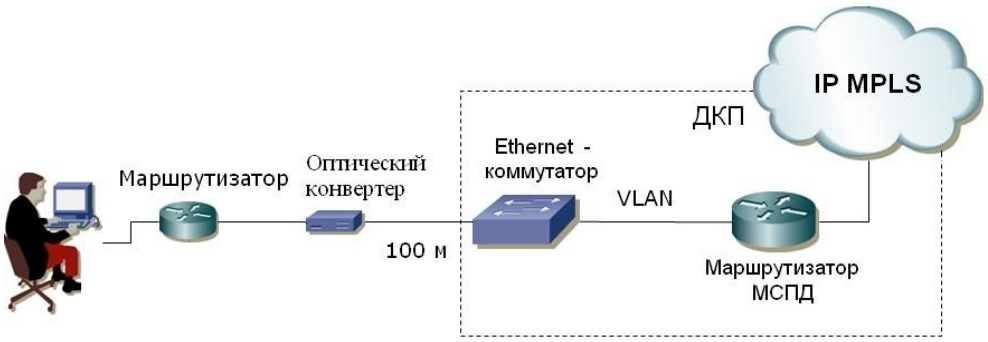
Route Target RT-импорт/экспорт ережелерін сипаттайтын идентификаторлар жиынтығы.

Республикалық IP VPN қызметі бірнеше қалалық IP VPN бірыңғай корпоративтік желісіне біріктіруді білдіреді. Бұл ретте әрбір қалалық VPN тораптарының бірі орталық ретінде бөлінуі тиіс. Орталық торап арқылы осы елді мекеннің Metro-желісіне жатпайтын клиенттің корпоративтік желісінің басқа тораптарымен байланыс жүзеге асырылады.

Республикалық шлюзге қосылу үшін орталық торапта қосымша интерфейс құрылады, ол республикалық VPN (VRF) агрегациялаушы маршрутизаторда енгізіледі. Қалалық VRF-да орталық торапқа default route (әдепкі бағыт) жазылады. Орталық торапта әдепкі бойынша республикалық VRF маршрут және осы торапқа тиесілі қалалық VRF маршруты жазылады. Егер республикалық VPN топологиясы full mesh-тен өзгеше болса, маршрутизация жоспары клиенттің талаптарына, трафик матрицасына және т. б. сәйкес әзірленеді. Корпоративтік желінің жеке тораптары мен хостарына қатынауды шектеу IP/MPLS технологиясы құралдарымен, маршрутизация жоспарымен, ACL және т. б. қамтамасыз етіледі.

Егер корпоративтік желі торабы қосымша Интернетке шығатын болса, әдепкі бағыт (default route) желі интернетке қосылатын интерфейске жазылады. Корпоративтік желінің басқа тораптарымен байланыс үшін маршруттау кестесінде жинақталған маршруттардың жазбалары қолданылуы тиіс.

VPN қосылу үшін соңғы миль ұйымдастыру физикалық моделі 2.5 суретте көрсетілген.



Сурет 2.5 - IP VPN қосылу үшін соңғы миль ұйымдастырудың физикалық моделі

Әр түрлі қалаларда орналасқан ҚР кез-келген мекемелерінің филиалдары үшін VPN желісін ұйымдастыру схемасы әр нүкте үшін бірдей.

Көбінесе ірі клиенттерде кеңсенің ғимаратында серверлік бөлме бар. Серверлік банкте маршрутизатор бар. Серверлік оптикалық кәбіл кәбілдік канализациядан автоматты телефон станциясының ғимаратына жақындайды. Осы ғимараттың қабаттарының бірінде Корпоративтік сату дирекциясының торабы орналасқан. Бұл желі әртүрлі телекоммуникациялық жабдықпен серверлік бөлме ретінде көрінеді, негізінен коммутаторлар (Switch), мультиплексорлар (Dslam) және маршрутизаторлар. Нақты жағдайда клиент үшін желіні құру кезінде ҚР Кез келген мекемесі қызметтерді жеткізушіге банк

ғимаратынан ДКП торабына дейін оптикалық кәбілді төсеу арқылы қосылудың «соңғы миля» ұйымдастыруы және қажетті қайта құру жабдығын қоюы қажет. Оптикалық кабель бойынша сигнал оптикалық жүреді және оны мыстан сигналға түрлендіру үшін оптикалық конвертерді қою қажет. Үлкен клиенттер көбінесе сыртқы операторлардың бөлмесіндегі модемдердің тіреуі деп аталатын арнайы шкафты орнатады,онда ДКП желісіне қосылу үшін қажетті әртүрлі жабдықтар бар. Бұл шкаф кілтпен жабылады және шкафқа тек клиент тарапынан инженерлер ғана ие болады. Сонымен бірге, біз оптикалық орта бойынша бір VPN қызметін ұйымдастыруды қарастырамыз,сондықтан ұйымда бөлек шкаф жоқ. Бұл жағдайда оптикалық конвертер байланыс операторының тірегінде орналасады және оған тек қызмет көрсетуші ғана қол жеткізе алады.

2.3 VPN хаттамалар стегі

VPN желілері Интернетті жалпы пайдаланудағы байланыс желілері (ТҚС) арқылы деректерді туннелдеу хаттамаларын пайдалана отырып құрылады, туннелдеу хаттамалары деректерді шифрлеуді қамтамасыз етеді және оларды пайдаланушылар арасында тура таратуды жүзеге асырады. Бүгінгі күні VPN желілерін құру үшін OSI моделінің келесі деңгейлерінің хаттамалары қолданылады:

- арна деңгейі. Сонымен қатар, L2TP және PPTP деректерін туннелдеу протоколдары қолданылады. Сонымен қатар, туннелдерді ұйымдастыру үшін MPLS технологиясы қолданылуы мүмкін. Арна деңгейінде VPN ұйымдастыру бойынша шешімдер провайдер доменінің шеңберінде жеткілікті шектеулі әрекет ету саласы бар;
- желілік деңгей (IP деңгейі). Сондай-ақ, IPSec протоколы, шифрлауды және деректерді конфедициалдауды жүзеге асырады. «Шлюзден шлюзге» және
- «хосттан шлюзге». «IPSec сервер» деп аталатын Шлюз корпоративтік желі мен көпшілік желі арасында орналасқан және корпоративтік желінің барлық пайдаланушылары үшін трафикті қауіпсіз беруді қамтамасыз етеді. IPSec протоколын қолдану корпоративтік желіге эквивалентті физикалық қосылуға толық функционалды қол жеткізуді іске асыруға мүмкіндік береді. VPN орнату үшін әрбір қатысушы белгілі бір IPSec параметрлерін конфигурациялауы тиіс, яғни әрбір клиент іске асыратын IPSec бойынша болуы тиіс;
- көлік деңгейі. SSL/TLS (Secure Socket Layer/Transport Layer Security) протоколы қолданылады. SSL / TLS TCP трафигін қорғау үшін қолданылуы мүмкін, UDP трафигін қорғау үшін қолданылуы мүмкін емес. SSL/TLS негізінде VPN-ның жұмыс істеуі үшін арнайы бағдарламалық қамтамасыз етуді іске асырудың қажеті жоқ, өйткені әрбір боузер мен пошта клиенті осы хаттамалармен жабдықталған. SSL/TLS көлік деңгейінде іске

асырылатындықтан, қорғалған байланыс «соңынан-аяғына» орнатылады, осылайша «хосттан хостқа» архитектурасын іске асырады.

VPN желілерін құру үшін көптеген хаттамалар әзірленді. Осы хаттамалардың әрқайсысы VPN-ның белгілі бір мүмкіндіктерін қамтамасыз етеді. IPSec протоколы жалпы қол жетімді IP желілеріндегі соңғы нүктелер арасында аутентификация мүмкіндігін қамтамасыз ететін желілік деңгейді шифрлау әдістерін ұсынады. Басқа хаттамалар туннелдеу, яғни деректерді немесе хаттамаларды басқа хаттамаларға инкапсуляциялау арқылы VPN-ның белгілі бір мүмкіндіктерін қолдауды қамтамасыз етеді. Төменде VPN желілерін құру үшін пайдаланылатын ең танымал туннель хаттамаларының кейбірі көрсетілген:

- GRE хаттамасы (Generic Routing Encapsulation-бағыттау үшін жалпы инкапсуляция). IP – желінің қашықтағы нүктелерінде Cisco маршрутизаторларымен виртуалды екі нүктелі байланыс жасайды.;

- L2F хаттамасы (Layer 2 Forwarding-2 деңгейін жіберу хаттамасы). Сонымен қатар, бұл жүйе VPDN (Virtual Private Dialup Network – виртуалды жеке коммутацияланатын желі) желісін құруға мүмкіндік береді.;

- PPTP хаттамасы (Point-to-Point Tunneling Protocol-екі нүктелі қосылысты туннелдеу хаттамасы). IP-желілерден VPN желісін құру арқылы қашықтағы клиенттен кәсіпорынның жеке серверіне қорғалған деректерді беруді қамтамасыз ететін Microsoft желілік хаттамасы. PPTP хаттамасы талап бойынша маршруттауды қолдайды, көпжолақты алмасу және Internet типті ашық желілерде виртуалды жеке желілер;

- L2TP хаттамасы (Layer 2 Tunnel Protocol-PPP 2 деңгейдің қосылуын туннелдеу хаттамасы). VPDN желісін құруға мүмкіндік беретін Cisco және Microsoft туннель протоколы әзірленген. L2TP хаттамасы VPN желілері үшін пайдаланылатын PPP (Point-to-Point Protocol – нүктеден нүктеге дейінгі тарату хаттамасы) протоколының кеңейтілуі болып табылады және PPTP және L2F туннельді хаттамаларының ең жақсы мүмкіндіктерін біріктіреді;

- MPPE хаттамасы (Microsoft Point-to-Point Encryption-екі нүктелі қосылысты шифрлау хаттамасы). PPP пакеттерін шифрланған нысанға ауыстыру құралы. Коммутацияланатын немесе қашықтағы желі арқылы қорғалған VPN байланысын жасауға мүмкіндік береді. МРЛЕ шеңберінде деректердің құпиялылығын қамтамасыз ету үшін RC4 типті RSA шифрлау алгоритмі қолданылады.

Ethernet деңгейінде корпоративтік желілерді біріктіру үшін ең қолайлы шешім жоғары жылдамдықты жалға алынған арналарды немесе L2 VPN қызметтерін пайдалану болады. Тапсырыс беруші үшін L2 VPN арналарына қосылу әдетте Ethernet портына қосылу түрінде ұсынылады. Бұл ретте байланыс операторының желісі жеке кеңселердің ЖЕЖ арасында пакеттерді жіберетін «виртуалды коммутатор» рөлінде болады. Саны офистер-бұл теориялық тұрғыдан шектелмеген.

2.4 VPN желілерін жіктеу

VPN технологиясының арқасында көптеген компаниялар Интернетті ақпаратты берудің басты құралы ретінде пайдалануды ескере отырып, өз стратегиясын құра бастайды, тіпті осал немесе өмірлік маңызды болып табылады.

VPN классификациясының әртүрлі белгілері бар. Ең жиі қолданылады [4]:

- OSI моделінің «жұмыс» деңгейі;
- VPN техникалық шешімінің архитектурасы;
- VPN техникалық іске асыру тәсілі.

OSI моделінің «жұмыс» деңгейі бойынша VPN жіктелуі.

Жалпы қол жетімді (қорғалмаған) желі бойынша деректерді қауіпсіз беру технологиялары үшін жалпыланған атау – қорғалған арна (securechannel) қолданылады. «Арна» термині деректерді қорғау пакеттер коммутациясы бар желіде салынған кейбір виртуалды жолдың бойында желінің екі торабы (хост немесе шлюздер) арасында қамтамасыз етілетіндігін атап көрсетеді.

Қорғалған арнаны OSI ашық жүйелерінің өзара әрекеттесу моделінің әртүрлі деңгейлерінде іске асырылған жүйелік құралдардың көмегімен құруға болады.

VPN-ның «жұмыс» деңгейі бойынша жіктелуі OSI-дің таңдалған деңгейіне көп жағдайда іске асырылатын VPN функционалдығы және оның қосымшалармен, сондай-ақ басқа да қорғаныс құралдарымен үйлесімдігі байланысты.

OSI моделінің «жұмыс» деңгейінің белгісі бойынша келесі vpn топтары ажыратылады:

- VPN арналық деңгей;
- VPN желілік деңгейі;
- VPN сеанс деңгейі.

VPN арналық деңгей. OSI моделінің арналық деңгейінде қолданылатын VPN құралдары үшінші деңгейдегі (және одан жоғары) трафиктің әр түрлі түрлерінің инкапсуляциясын және типті виртуалды туннельдерді құруды қамтамасыз етуге мүмкіндік береді.

«Нүкте-нүкте» (маршрутизатордан маршрутизаторға немесе дербес компьютерден ЛВС шлюзіне). Бұл топқа L2F (Layer 2 Forwarding) және PPTP (Point-to-PointTunneling Protocol) протоколдарын пайдаланатын өнімдер, сондай-ақ Cisco Systems және Microsoft фирмалары әзірлеген L2TP (Layer 2 Tunneling Protocol) стандарты жатады.

VPN желілік деңгейі. VPN-желілік деңгейдегі өнімдер IP-де инкапсуляцияны орындайды. Осы деңгейдегі кең танымал хаттамалардың бірі IPSec протоколы болып табылады, ол аутентификация, туннелдеу және IP-пакеттерді шифрлауға арналған. IPSec протоколы Internet Engineering Task Force (IETF) консорциумымен стандартталған пакеттерді шифрлау бойынша

барлық үздік шешімдерді өзіне қосып, IPv6 протоколына міндетті компонент ретінде кіруі тиіс.

IPSec протоколына Ike (Internet Key Exchange) протоколы байланысты, алыстағы құрылғылар арасында криптографиялық кілттерді қауіпсіз басқару және алмасу міндеттерін шешеді. IKE ХАТТАМАСЫ кілттермен алмасуды автоматтандырады және қорғалған қосылуды орнатады, ал IPSec кодтайды және пакеттерге қол қояды. Сонымен қатар, IKE орнатылған қосылу үшін кілтті өзгертуге мүмкіндік береді, бұл берілетін ақпараттың құпиялылығын арттырады.

VPN сеанс деңгейі. Кейбір VPN «арналар делдалдары» (circuit proxy) деп аталатын басқа тәсілді қолданады. Бұл әдіс көлік деңгейімен жұмыс істейді және қорғалған желіден әрбір сокет үшін жеке Internet жалпыға қол жетімді желісіне трафикті қайта таратады. (IP сокеті TCP-байланыс және нақты портты немесе UDP портымен сәйкестендіріледі. TCP / IP стегінің бесінші сеанстық деңгейі жоқ, алайда сокеттерге бағытталған операциялар жиі сеанстық деңгейдегі операциялар деп аталады.)

Туннельдің бастамашысы мен терминаторы арасында берілетін ақпаратты шифрлау көбінесе TLS (Transport Layer Security) көлік деңгейін қорғау көмегімен жүзеге асырылады. Қазіргі уақытта socks v5 протоколы арналар делдалдарын стандартталған іске асыру үшін қолданылады.

Техникалық шешім архитектурасы бойынша VPN классификациясы виртуалды жеке желілердің үш негізгі түрін бөліп алу қабылданған:

- ішкі корпоративтік VPN (Intranet VPN);
- Қашықтан қол жеткізу VPN (Remote Access VPN);
- корпоративтік VPN (Extranet VPN).

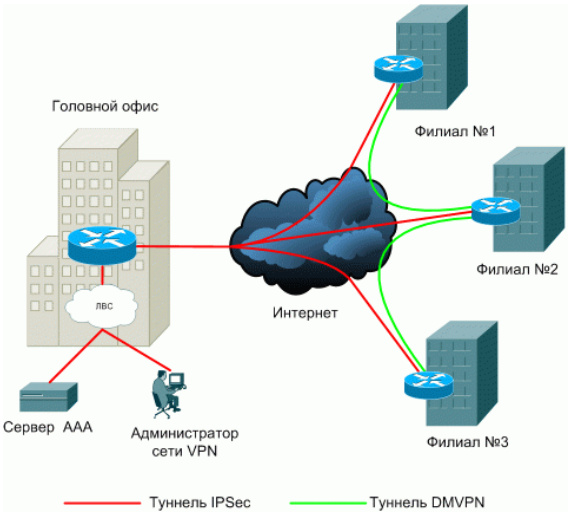
VPN ішкі корпоративтік желілері кәсіпорын ішіндегі бөлімшелер арасында немесе бөлінген желілерді қоса алғанда, корпоративтік байланыс желілерімен біріктірілген кәсіпорындар тобы арасында қорғалған өзара іс-қимылды қамтамасыз етуге арналған.

Алыстан қатынайтын VPN компанияның мобильді және/немесе алыстан (home-office) қызметкерлерінің корпоративтік ақпараттық ресурстарына қашықтан қатынауын қамтамасыз етуге арналған. Vpn корпоративтік желілері бизнес бойынша стратегиялық серіктестермен, жеткізушілермен, ірі тапсырыс берушілермен, пайдаланушылармен, клиенттермен және т.б. қорғалған ақпарат алмасуды қамтамасыз етуге арналған.

Соңғы уақытта VPN әр түрлі конфигурациялар конвергенциясының үрдісі байқалады. Техникалық іске асыру тәсілі бойынша VPN жіктелуі. Техникалық іске асыру тәсілі бойынша VPN:

- маршрутизаторлар;
- желі аралық экрандар;
- бағдарламалық шешімдер;
- кіріктірілген шифропроцессорлары бар мамандандырылған аппараттық құралдар

Vpn маршрутизаторлар негізінде (2.6 сурет).

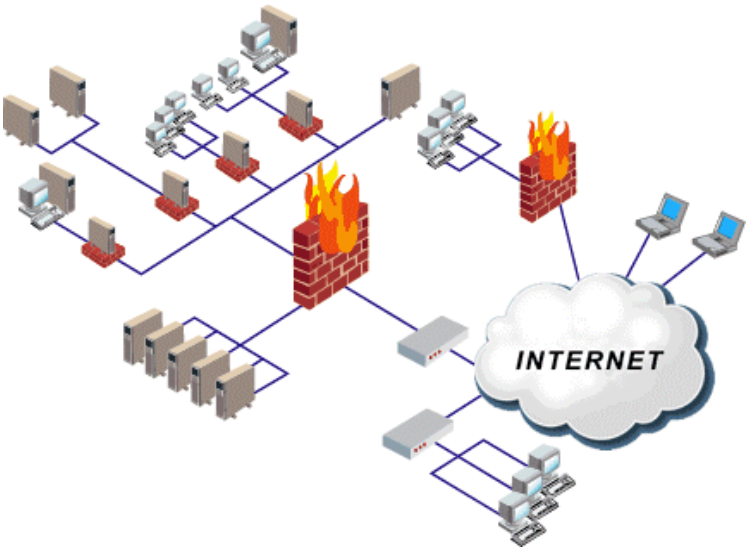


Сурет 2.6 - Маршрутизаторлар базасында VPN

VPN құрудың бұл тәсілі қорғалған арналарды құру үшін маршрутизаторларды қолдануды көздейді. Өйткені барлық ақпарат, шығыс хат-жергілікті желі арқылы арқылы өтеді маршрутизатор болса, әбден әрине оған жүктелсін мен міндеттері шифрлау.

VPN үшін маршрутизаторлардағы жабдық үлгісі – Cisco Systems компаниясының құрылғылары және т. б.

VPN желіаралық экрандар негізінде (МЭ) 2.7 суретте келтірілген.

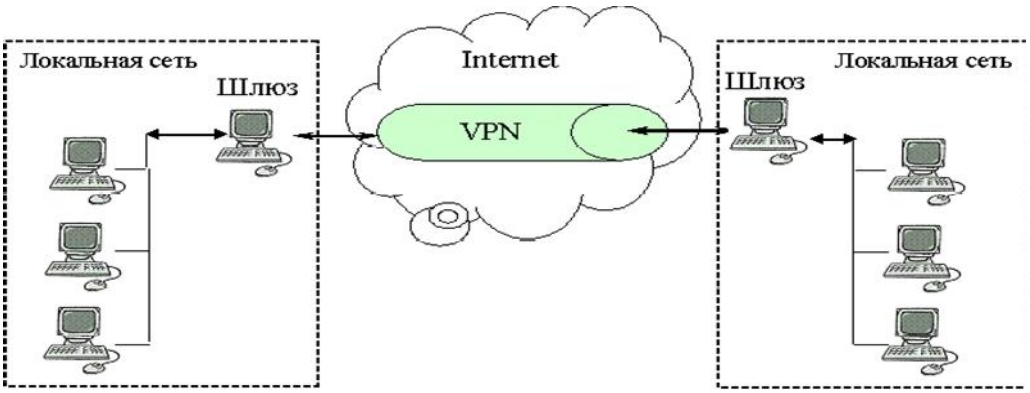


Сурет 2.7 - ЭМ мен VPN клиенттерінің арасында VPN іске асыру

Көптеген өндірушілердің МЭ деректерді туннелдеу және шифрлау мүмкіндіктерін қолдайды, мысалы, Check Point Software Technologies компаниясының Fire Wall - 1 өнімі. Пайдаланғанда ЭМ базасында ДК есте сақтау керек, мұндай шешім тері шағын желілер аз көлемі берілетін ақпарат.

Бұл әдістің кемшіліктері бір жұмыс орнына қайта есептегенде шешімнің жоғары құны және өнімділіктің ЭМ жұмыс істейтін аппараттық қамтамасыз етуден тәуелділігі болып табылады.

VPN бағдарламалық жасақтама негізінде 2.8 суретте көрсетілген

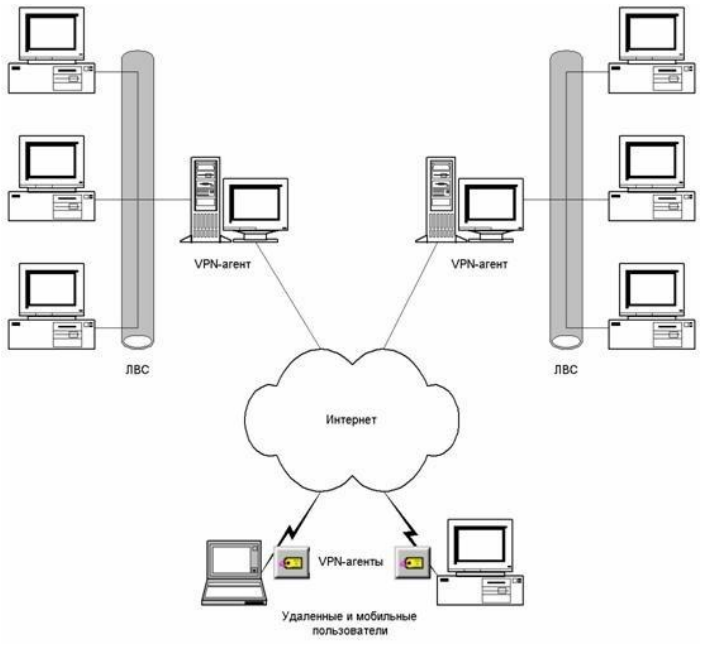


Сурет 2.8 - Бағдарламалық қамтамасыз ету базасында VPN

VPN-бағдарламалық тәсілмен іске асырылған өнімдер өнімділік тұрғысынан мамандандырылған құрылғыларға жол береді, алайда VPN-желілерін іске асыру үшін жеткілікті қуатқа ие. Алыстан рұқсат етілген жағдайда қажетті өткізу жолағына қойылатын талаптар үлкен емес екенін атап өткен жөн. Сондықтан таза бағдарламалық өнімдер қашықтан қол жеткізу үшін жеткілікті өнімділікті қамтамасыз етеді. Бағдарламалық өнімдердің сөзсіз артықшылығы қолданудағы икемділік пен ыңғайлылық, сондай-ақ салыстырмалы түрде жоғары емес құн болып табылады [4]. VPN мамандандырылған аппараттық құралдар негізінде 2.9 суретте көрсетілген. Мұндай VPN – ның басты артықшылығы-жоғары өнімділік, оларда шифрлау арнайы микросхемалармен жүзеге асырылады. Арнайы VPN құрылғылары қауіпсіздіктің жоғары деңгейін қамтамасыз етеді, алайда олар жолдар. VPN - бұл сыртқы периметрлерде VPN-агенттер орнатылған желілердің жиынтығы. Оны 2.8 суреттен көруге болады.

VPN-бағдарламалық тәсілмен іске асырылған өнімдер өнімділік тұрғысынан мамандандырылған құрылғыларға жол береді, алайда VPN-желілерін іске асыру үшін жеткілікті қуатқа ие. Алыстан рұқсат етілген жағдайда қажетті өткізу жолағына қойылатын талаптар Үлкен емес екенін атап өткен жөн. Сондықтан таза бағдарламалық өнімдер қашықтан қол жеткізу үшін жеткілікті өнімділікті қамтамасыз етеді. Бағдарламалық өнімдердің сөзсіз артықшылығы қолданудағы икемділік пен ыңғайлылық, сондай-ақ салыстырмалы түрде жоғары емес құн болып табылады [4]. VPN мамандандырылған аппараттық құралдар негізінде 2.9 суретте көрсетілген. Мұндай VPN – ның басты артықшылығы-жоғары өнімділік, оларда шифрлау арнайы микросхемалармен жүзеге асырылады. Арнайы VPN құрылғылары қауіпсіздіктің жоғары деңгейін қамтамасыз етеді, алайда олар жолдар. Шын мәнінде, VPN – сыртқы периметрі vpn-агенттер орнатылған желілер

жиынтығы.



Сурет 2.9 - Аппараттық құралдар базасында VPN

VPN-агент-бұл төменде сипатталған операцияларды орындау арқылы берілетін ақпаратты қорғауды қамтамасыз ететін бағдарлама (немесе бағдарламалық-аппараттық кешен). Кез келген VPN IP - пакетін желіге жібермес бұрын-агент келесілерді шығарады:

- IP-пакеттің атауынан оның адресаты туралы ақпарат бөлінеді. Осы ақпаратқа сәйкес, VPN-агенттің қауіпсіздік саясаты негізінде қорғау алгоритмдері (егер VPN-агент бірнеше алгоритмдерді қолдаса) және осы пакет қорғалатын криптографиялық кілттер таңдалады. Егер VPN-агенттің қауіпсіздік саясатында осы адресатқа IP-пакетті немесе осы сипаттамалары бар IP-пакетті жіберу қарастырылмаған болса, IP-пакетті жіберу бұғатталады;

- таңдалған тұтастықты қорғау алгоритмінің көмегімен IP-пакетке электрондық цифрлық қолтаңба (ЭЦҚ), имито қою немесе ұқсас бақылау сомасы қалыптасады және қосылады;

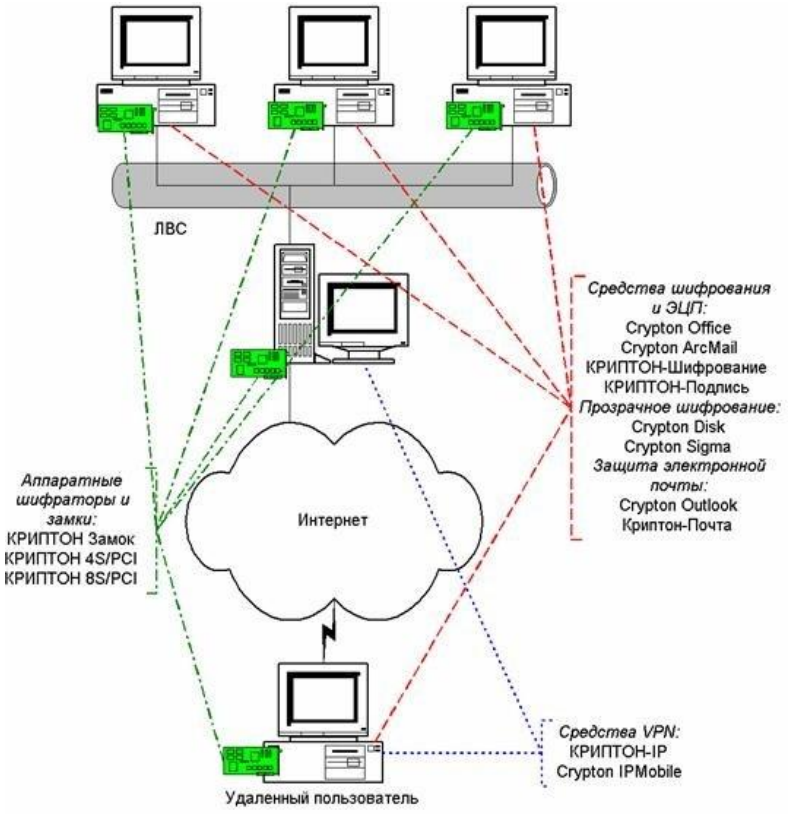
- таңдалған шифрлеу алгоритмінің көмегімен IP-пакетті шифрлеу жүргізіледі;

- пакеттерді инкапсуляциялаудың белгіленген алгоритмінің көмегімен шифрланған IP-пакетке жіберуге дайын IP-пакетке орналастырылады, оның тақырыбы адресат пен жіберуші туралы бастапқы ақпараттың орнына адресаттың VPN-агенті және жіберушінің VPN-агенті туралы тиісінше ақпаратты қамтиды;

- пакет адресаттың VPN-агентіне жіберіледі.

Кешенді қорғау. Электрондық құлып аппараттық шифрлау базасында әзірленуі мүмкін. Бұл кездейсоқ сандарды шифрлеу, генерациялау және НСД қорғау функцияларын орындайтын бір құрылғы. Мұндай шифрлеуші барлық

компьютердің қауіпсіздік орталығы бола алады, оның базасында келесі мүмкіндіктерді қамтамасыз ететін деректерді криптографиялық қорғаудың толық функционалды жүйесін құруға болады: компьютерді физикалық қол жетімділіктен қорғау; компьютерді желі бойынша ЖСҚ қорғау және VPN ұйымдастыру; файлдарды талап ету бойынша шифрлеу; компьютердің логикалық дискілерін автоматты шифрлеу, ЭЦҚ есептеу/тексеру; электрондық пошта хабарын қорғау. Бағдарламалық және аппараттық шешімдер базасында компьютерлерді кешенді қорғауды және деректер алмасуды ұйымдастыру мысалы 2.10-суретте келтірілген.



Сурет 2.10 - Кешенді қорғау

2.5 MPLS VPN

Қазіргі уақытта MPLS технологиясы VPN құрудың ең перспективті технологияларының бірі болып табылады.

VPN MPLS желісі екі аймаққа бөлінеді: клиенттердің IP-желісі және клиенттік желілерді біріктіру үшін қызмет ететін провайдердің ішкі (магистральды) желісі.

Жалпы жағдайда әрбір клиентте бірнеше аумақтық оқшауланған IP желілері болуы мүмкін, олардың әрқайсысы өз кезегінде маршрутизаторлармен байланысты бірнеше кіші желілерді қамтуы мүмкін. Корпоративтік желінің

мұндай аумақтық оқшауланған желілік элементтері сайттар деп аталады. Бір клиентке тиесілі сайттар IP пакеттерімен MPLS провайдері желісі арқылы алмасады және осы клиенттің виртуалды жеке желісін құрайды. Сайт шегінде маршруттық ақпаратпен алмасу IGP маршруттаудың ішкі хаттамаларының бірі бойынша жүзеге асырылады.

MPLS VPN құрылымы үш негізгі компоненттің болуын көздейді:

- Customer Enge Router, CE – клиенттің шекаралық маршрутизаторы;
- Provider Router, P-провайдердің магистральдық желісінің ішкі маршрутизаторы;
- Provider Enge Router, PE - провайдер желісінің шекаралық маршрутизаторы.

Клиенттің шекаралық маршрутизаторлары клиент сайтын провайдердің магистралдық желісіне қосу үшін қызмет етеді. Бұл маршрутизаторлар клиент желісіне тиесілі және VPN бар екендігі туралы ештеңе білмейді. - Шекара маршрутизаторам желісін провайдер арқылы маршрутизаторлар CE сайттар мен клиенттерге ішкі маршрутизаторлар желі провайдері.

Маршрутизаторлардың өзара әрекеттесуі TCP / IP стегінің стандартты хаттамаларының негізінде жүзеге асырылады. Әр түрлі сайттардың се-маршрутизаторлары тікелей маршруттық ақпаратпен алмаспайды және тіпті бір-бірінің білмейтін болуы мүмкін. VPN құрамына кіретін шағын тораптардың мекен-жай кеңістігі жабылуы мүмкін, яғни адрестердің бірегейлігі нақты ішкі желі шегінде ғана сақталуы тиіс. Бұл IP мекенжайын VPN-IP адресіне түрлендіруге және осы адрестермен жұмыс істеу үшін MP-BGP протоколын пайдалануға қол жеткізілді. CE маршрутизаторы бір сайтқа жатады деп саналады, бірақ сайт бірнеше VPN тиесілі болуы мүмкін. PE маршрутизаторға әртүрлі сайттардағы және тіпті қатысты бірнеше се маршрутизаторлар қосылуы мүмкін.

CE маршрутизаторлары көпжолақты коммутация технологиясын қолдауға міндетті емес, MPLS қолдауы тек ре маршрутизаторлардың ішкі интерфейстері үшін және р маршрутизаторлардың барлық интерфейстері үшін қажет.

Функционалдық құру бойынша провайдер желісінің шекаралық маршрутизаторлары неғұрлым күрделі болып табылады. Оларға VPN қолдау функциясы жүктеледі, атап айтқанда: әртүрлі клиенттерден түсетін бағыттар мен деректерді шектеу. Сонымен қатар, бұл маршрутизаторлар Тапсырыс берушінің сайттары арасындағы LSP жолдарының соңғы нүктелері болып табылады.

Әрбір PE-маршрутизатор бірнеше маршруттау кестелерін қолдауы тиіс, пайдаланушылар қанша сайттар оған қосылған, яғни бір физикалық маршрутизаторда бірнеше виртуалды ұйымдастырылады. Сонымен қатар, нақты VPN қатысты маршруттық ақпарат тек PE маршрутизаторларда ғана бар, оған осы VPN сайттары қосылған. Осылайша, оператор желісінің барлық маршрутизаторларында осы ақпарат болған жағдайда пайда болатын масштабтау мәселесі шешіледі.

Әрбір жаңа сайт клиенттің PE жеке қауымдасқан маршрутизация кестесін жасайды.

PE маршрутизаторында әрбір байланыстырылған маршрутизатор кестесі нақты VPN кіретін сайттар жиынтығын анықтайтын бір немесе бірнеше RT атрибуттары беріледі. Бұдан басқа, маршрут vpn of Origin атрибутымен, сайттардың тобын және осы сайттардағы маршрутизаторлардың бірі жариялаған тиісті маршрутты бірдей сәйкестендіретін болуы мүмкін; және маршрутизатор осы маршрут туралы ақпарат алған сайтты сәйкестендіретін Site of Origin атрибутымен байланысты болуы мүмкін.

Ре маршрутизаторлары арқылы клиенттік сайттар аймағы мен провайдер ядросының аймағы арасында көрінбейтін шекара өтеді. Бір жағынан ре маршрутизаторларымен өзара әрекеттесетін интерфейстер, ал екінші жағынан - клиенттердің сайттары қосылатын интерфейстер орналасады. Бір жағынан PE - ге магистральдық желінің маршруттары туралы хабарландырулар, екінші жағынан-клиенттер желілеріндегі маршруттар туралы хабарландырулар келіп түседі.

Маршруттық ақпаратты жекелеген VPN шегінен тыс тарату аймағын шектеу әрбір VPN мекен-жай кеңістігін оқшаулайды, оның шегінде Интернеттің жария адрестерін де, сондай-ақ жеке (private) адрестерді де қолдануға мүмкіндік береді. Бір VPN мекен-жай кеңістігінің барлық мекен-жайларына маршруттарды ажыратушы (Route Distinguisher, RD) деп аталатын префикс қосылады, ол осы VPN бірегей сәйкестендіреді. Ре маршрутизаторында әр түрлі VPN қатысты барлық мекенжайлар, тіпті олар сәйкес келетін бөлігі - IP мекенжайы болса да, бір-бірінен ерекшеленетін болады.

Әрбір жеке VPN сайттары арасындағы маршруттық ақпаратпен алмасу MP-BGP (Multiprotocol BGP) протоколының басқаруымен орындалады.

MPLS жоқ қауіпсіздігін қамтамасыз етеді есебінен шифрлау және аутентификация, ол IPSec, бірақ қателіктер жібереді, бұл технологиялар ретінде қосымша қорғау шараларын. MPLS провайдерлері клиенттерге Traffic Engineering немесе DiffServ әдістерін қолданған кезде кепілді қызмет көрсету сапасын ұсына алады.

VPN MPLS виртуалды желілері бір компанияның жеке желілік инфрақұрылымы базасында клиенттің қорғалған корпоративтік желісін құруға бағытталған. Бұл әдіс IP протоколын жеке желілердің қауіпсіздігімен және MPLS технологиясы беретін қызмет көрсету сапасымен қолдану артықшылықтарын біріктіреді.

VPN MPLS желілері корпорацияның бөлімшелері үшін бірыңғай желілік ортаны және экстрасетей ұйымдастыруды қамтамасыз ететін электрондық коммерция үшін корпоративтік кеңістік құру үшін ең көп қолайлы. Олар сондай-ақ кәсіпорынның электрондық коммерциялық қызметіне негіз бола алады.

2.6 MPLS-VPN желілеріндегі қауіпсіздік

Бұл VPN технологиясының қауіпсіздігі арнайы құрылғылар мен қорғау механизмдерін қолдану есебінен қамтамасыз етіледі. Vpn пайдаланушысы желіге қатынауды алу үшін брандмауэр арқылы өтеді, онда оны аутентификациялау және авторизациялау жүзеге асырылады, осының арқасында VPN желі ресурстарына тек авторизацияланған пайдаланушылар ғана қолжетімділікке кепілдік береді.

MPLS-VPN функционалдығы Frame Relay және ATM желілеріндегі виртуалды арналардың қауіпсіздігіне баламалы қауіпсіздік деңгейін қолдайды. MPLS-VPN желілеріндегі қауіпсіздікті BGP протоколы мен IP адрестерін шешу жүйесі арқылы қолдайды.BGP-хаттама маршруттар туралы ақпаратты тарату үшін жауап береді. Ол community атрибуттары мен көпжолды кеңейтулер арқылы кім және кіммен байланыса алатынын анықтайды. VPN мүшелігі VPN желісіне біріктірілетін және BGP Route Distinguisher (RD) бірегей параметрін беретін логикалық порттарға байланысты. RD параметрлері соңғы пайдаланушыларға белгісіз, сондықтан олар осы желіге басқа порт арқылы қатынай алмайды және бөтен деректер ағынын ұстай алмайды. VPN құрамына тек белгілі бір тағайындалған өнімдер кіреді. VPN желісінде MPLS функциялары бар BGP протоколы VPN туралы ақпараты бар FIB (Forwarding Information Base) кестелерін осы VPN қатысушыларына ғана таратады, осылайша трафикті логикалық бөлу арқылы деректерді беру қауіпсіздігін қамтамасыз етеді. Тапсырыс беруші емес, провайдер оны қалыптастыру кезінде белгілі бір VPN порттарын береді. Желі провайдері әрбір пакет ассоциирован бастап RD, сондықтан талпыныстары ұстайтын пакетін немесе ағынының үйдегі әкелуі мүмкін байқаудан алған серпілістің батыр VPN. Пайдаланушылар қажетті физикалық немесе логикалық портқа байланысты және қажетті RD параметрі бар болса ғана интранет немесе экстранет желісінде жұмыс істей алады. Бұл схема Cisco MPLS-VPN желілеріне өте жоғары қорғаныс деңгейін береді. Тірек желісінде маршруттар туралы ақпарат OSPF немесе IS-IS сияқты Interior Gateway Protocol (IGP) стандартты протоколының көмегімен беріледі. Ре шекаралық құрылғылары провайдер желісінде LDP арқылы белгілерді тағайындау үшін өзара байланыс орнатады. Сыртқы (пайдаланушылық) маршруттар үшін таңбаларды тағайындау PE-маршрутизаторлар арасында LDP арқылы емес, көпжолақты BGP кеңейтулері арқылы таратылады. Community BGP атрибуты желілердің қол жетімділігі туралы ақпараттың шеңберін шектейді және өте ірі желілерді маршруттық ақпараттың өзгерістері туралы ақпаратпен шамадан тыс жүктемеместен ұстап тұруға мүмкіндік береді. BGP провайдер желісіндегі барлық ре перифериялық құрылғыларында ақпаратты жаңартпайды, ал FIB кестесін нақты VPN тиесілі PE ғана сәйкестендіреді. Егер виртуалды арналар оверльдік модельде жасалса, кез келген жеке деректер пакетінің Шығыс интерфейсі тек кіріс интерфейс функциясы болып табылады. Бұл дегеніміз, пакеттің IP мекенжайы оны магистральды желі арқылы жіберу

бағытын анықтамайды. Бұл VPN желісіне рұқсат етілмеген трафиктің түсуін және рұқсат етілмеген трафиктің берілуін болдырмауға мүмкіндік береді. Желілерінде MPLS-VPN пакеті, оқуға түсуші осы магистраль, бірінші кезекте байланыстырылады нақты VPN желісімен болу негізінде қандай интерфейске (подинтерфейсу) пакет түсіп, PE-маршрутизатор.

2.7 Жабдықты таңдау

Негізгі және алыстағы офистерді vpn-туннельдің көмегімен корпоративтік деректермен қауіпсіз алмасуды, сондай-ақ Intranet-ресурстарға ашық қорғалған қолжетімділікті қамтамасыз ете отырып біріктіру мәселесін шешу үшін жабдықты таңдау қажет.

Gartner талдаушыларының зерттеулеріне сәйкес, vpn нарығының әлемдік көлемі желіаралық экрандарды шығару бойынша оның өндірушілері арасында бөлінеді, үлестерді бөлу 3.1-кестеде көрсетілген.

Кесте 3.1 - VPN функциялары бар ЭМ әлемдік нарығы

Өндіруші мекемелер	Нарықтағы орны	Нарықтағы үлесі, %	Өсімі 2017-2018, %
Cisco Systems	1	31,3	0,2
Check Point+Nokia	2	17,3	- 1,7
Juniper Networks	3	11,6	5,7
Fortinet	4	5,2	65,2
SonicWall	5	4,6	43,9
Secure Computing	6	3,6	95,6
Watchguard	7	2,3	12,3
Check Point+Crossbeam	8	1,7	-
SateNet	9	1,2	- 14,1
StoneSoft	10	0,7	8
Прочие компании	-	21,5	-

Жұмыста Cisco Systems фирмасының желіаралық экраны қолданылады.

2.8 Cisco Systems желіаралық экран үлгісін таңдау

Cisco Systems PIX корпоративтік шешімдер үшін желіаралық экранның модельдері:

- Cisco PIX 501 (10 пайдаланушы);
- Cisco PIX 501 (50 пайдаланушы);
- Cisco PIX 506 E (50 пайдаланушы);
- Cisco PIX 515 E (250 пайдаланушыдан).

Кесте 3.2 - Өнімнің сипаттамасы

Сипаттамалар	Мәні
Экран арқылы ашық мәтінді жіберу жылдамдығы, Мбит/с	10
Бір рет DES-шифрлау кезінде VPN бойынша беру жылдамдығы, Мбит/с	6
3 Мбит/с үш есе DES-шифрлау кезінде VPN бойынша тарату жылдамдығы	3, 3500 қосылымға дейін қолдау
VPN немесе ашық кілттер инфрақұрылымын пайдаланатын 5 клиенттерге бір мезгілде қолдау көрсету	+
Жады, Мбаит	64-ке дейін
Өткізу қабілеті, Мбит/с	188
Бір мезгілде сессияларды қолдау	130000
VLAN қолдау	10
IPSec протоколын қолдайтын VPN-сессияларды қолдау, Мбит / с	Accelerator Card 2000 VPN; VPN throughput 140 168-bit 3DES (VAC+) 63(VAC) 128-bit AES VPN throughput 135; AES VPN throughput 140 256-bit
Қолдау көрсетілетін интерфейстер	FE 6-ға дейін

Желіаралық экран кең мүмкіндіктерге ие, соның ішінде::

- брэндмауэр жағдайын толық бақылауды, VPN технологиясын қолдауды, басып кіруден қорғауды қоса алғанда, SOHO корпоративтік деңгейі желісін сенімді қорғау;

- интеграцияланған 4/100 Мбит/с 4 порттық коммутатордың көмегімен бірден бірнеше құрылғыларды бірлесіп жұмыс істеу үшін қарапайым және ыңғайлы кеңжолақты қосу;

- telnet/SSH, SNMP және syslog сияқты қашықтан басқару стандарттарын қолдайтын Web - технологияның көмегімен желілік басқару үшін бай мүмкіндіктер; AVVID архитектурасын қолдау; масштабталу.

Бұл жұмыста Cisco PIX 515 E желіаралық экран қолданылады.

Cisco PIX Firewall Internet жоғары жылдамдықты қатынауды пайдаланатын корпоративтік қашықтағы қызметкерлер немесе шағын офис қызметкерлерінің пайдалануына арналған.

Ол сондай-ақ осындай қол жеткізу үшін қажетті қауіпсіздік деңгейін қамтамасыз етуге арналған. Қазіргі уақытта Internet жоғары жылдамдықты қатынау бүкіл әлемде 20 млн. жуық пайдаланушыны пайдаланады және жақын арада бұл сан 100 млн. дейін өседі.

2.9 PIX Firewall желі аралық экраны

Cisco компаниясының Private Internet Exchange (PIX) желіаралық экраны корпоративтік желілер қауіпсіздігінің жаңа деңгейін біріктіріп және пайдалану қарапайымдылығына әкеледі. PIX толық қауіпсіздікті қамтамасыз ете отырып, ішкі желіні сыртқы әлемнен толық жасыра алады. Сонымен қатар, PIX үлкен өнімділікті қамтамасыз ете отырып, нақты уақыттың арнайы, UNIX емес операциялық жүйесін қолданады.

PIX желіаралық экранның жоғары өнімділігінің негізі-хакерлерден пайдаланушылардың адрестерін тиімді жасыратын бейімдік қауіпсіздік алгоритміне негізделген қорғаныс схемасы болып табылады. Тұрақты, қосылысқа бағытталған адаптивті қауіпсіздік алгоритмі жіберушінің және алушының мекенжайларына, TCP пакеттерін нөмірлеу бірізділігіне негізделген қосылыстар үшін қауіпсіздікті қамтамасыз етеді. Бұл ақпарат кестеде сақталады және барлық кіріс пакеттер осы кестедегі жазбалармен салыстырылады. PIX арқылы қатынауға тиісті Байланыс сәтті өткен жағдайда ғана рұқсат етіледі. Бұл әдіс ішкі пайдаланушылар мен авторизацияланған сыртқы пайдаланушылар үшін ашық қол жеткізуді қамтамасыз етеді, бұл ретте ішкі желіні рұқсатсыз қол жеткізуден толығымен қорғайды.

Cisco PIX сондай-ақ «тура делдал» (Cut-Through Proxy) технологиясы есебінен UNIX ОС базасында желіаралық экрандар – «делдалдар» салыстырғанда өнімділіктің Елеулі артықшылығын қамтамасыз етеді. PIX «делдалдар» – қарапайым серверлер сияқты қолданбалы деңгейде қосылысты орнатуды бақылайды. Пайдаланушы қауіпсіздікті қамтамасыз ету саясатына сәйкес сәтті сәйкестендірілген соң, PIX сессия деңгейінде абоненттер арасындағы деректер ағынын бақылауды қамтамасыз етеді. Мұндай технология PIX желіаралық экранына кәдімгі желіаралық экрандарға қарағанда анағұрлым жылдам жұмыс істеуге мүмкіндік береді – «делдалдар».

Жоғары өнімділікке қосылған нақты уақыт операциялық жүйесі, сондай-ақ қауіпсіздік деңгейін арттырады. Бастапқы мәтіні кең қол жетімді UNIX ОС -ге қарағанда Cisco PIX-қауіпсіздікті қамтамасыз ету үшін арнайы әзірленген арнайы бөлінген жүйе.

Сенімділігін арттыру үшін желіаралық экран PIX белгіленуі мүмкін арнайы нұсқалары қамтамасыз ету ыстық резервтеу, осының есебінен алдын болуы бірыңғай нүктесінің мүмкін болатын істен шығу. Егер PIX екі желіаралық экраны параллель режимде орнатылса және жұмыс істесе және олардың біреуі істен шықса, онда екінші PIX қауіпсіздікті қамтамасыз ету

бойынша барлық функцияларды мөлдір режимде орындайды.

МЭ Cisco PIX 256 мыңнан астам бір мезгілде қосылыстарды қолдайды және тиісінше жүздеген және мыңдаған пайдаланушыларды өнімділікті азайтпай қолдауды қамтамасыз етеді. Толық жүктелген ЭМ PIX 170 Мб / сек дейін өткізу қабілетін қамтамасыз етеді. Мұндай өткізу қабілеті UNIX ОЖ немесе Microsoft Windows NT ОЖ негізделген кез келген МЭ-ден айтарлықтай асып түседі.

Арнайы дайындығы жоқ пайдаланушылар PIX-ті кемінде бес минут ішінде теңшей алады. PIX желіаралық экранды одан әрі баптауды оңайлату үшін пайдалану оңай Security Manager графикалық қабықшасын қамтиды.

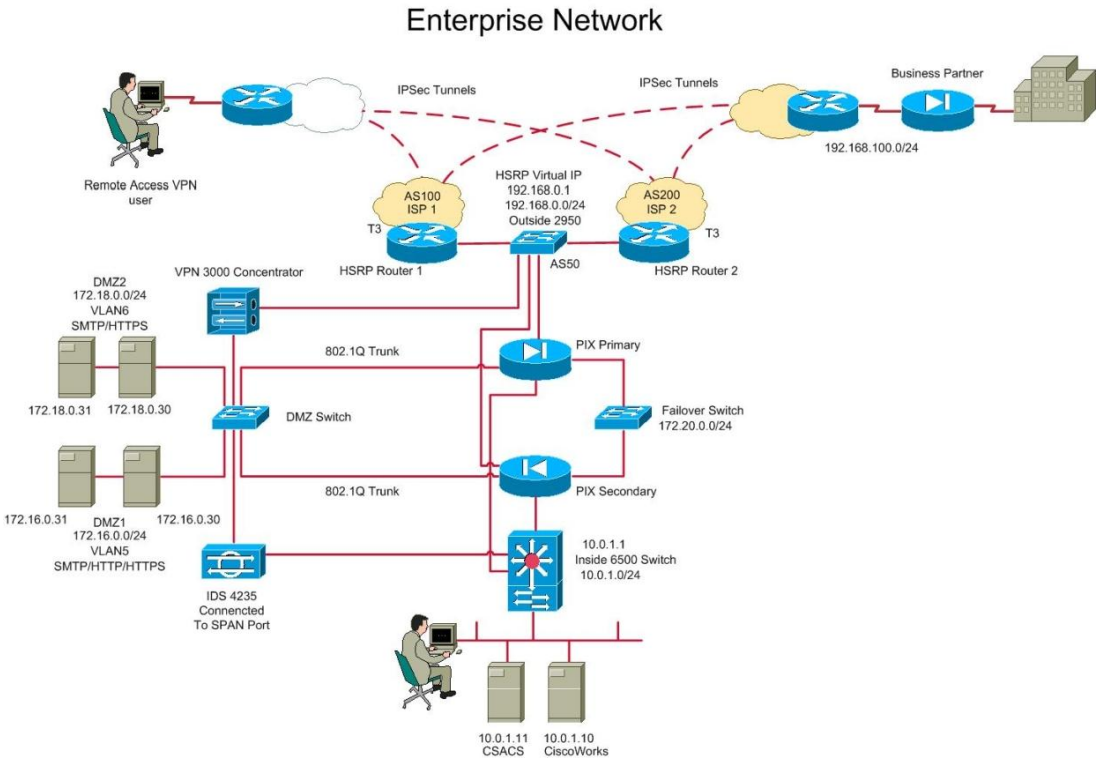
Cisco сондай-ақ Cisco PIX Private Link encryption card шифрлау адаптерін ұсынады. Осы PIX адаптерін пайдалану арқылы шифрланған IP пакеттерін интернет сияқты көпшілік IP желілері арқылы жіберуге мүмкіндік береді. PIX Private Link адаптері Pix-те IPSec стандартты технологиясы мен IETF хаттамаларын пайдалана отырып, сәйкестендірілген тақырып (Authentication Header-AH) және оралған қорғалған деректер (Encapsulating Security Payload-ESP) сияқты қосылыстарды қорғай отырып орнатылуы мүмкін.

Сондай-ақ, МЭ Cisco PIX IP адрестерінің жетіспеу проблемасымен қақтығыспай IP желілерін кеңейту және өзгерту мүмкіндігін ұсынады. NAT желілік адрестерді тарату технологиясы қолданыстағы адрестерді де, сондай-ақ жеке желілер үшін резервтік адрестерді де пайдалануға мүмкіндік береді. PIX, сондай-ақ жеке IP желілері үшін адрестік кеңістікті, сондай-ақ тіркелген IP адрестерін пайдалануға мүмкіндік беретін трансляцияланатын және таратылмайтын мекенжайларды бірлесіп пайдалану үшін бапталуы мүмкін. Негізгі мүмкіндіктер:

- қатаң, қосылысқа бағытталған қауіпсіздік жүйесі, авторланбаған пайдаланушылардың ішкі желі ресурстарына кіруін болдырмайды;
- тура «делдал» технологиясы Terminal Access Controller Access Control System (TACACACS)+ немесе Remote Access Dial-In User Service (RADIUS);
- кеңейтілген қорғау саясаты үшін алты желілік интерфейске дейін;
- Security Manager әкімшілік графикалық интерфейсі 100 МЭ PIX дейін теңшеуге арналған;
- адрестердің динамикалық және статикалық трансляциясы;
- SNMP желілік басқару қарапайым протоколын қолдау;
- жүйелік оқиғалар журналын (syslog);
- WWW, File Transfer Protocol (FTP), Telnet, Archie, Gopher сияқты барлық негізгі желілік сервистерді мөлдір қолдау;
- progressive Networks RealAudio & ReadVideo, Xing StreamWorks, White Pines CU-SeeMe, Vocal Tec Internet Phone, VDOnet VDOLive, Microsoft Networshow және VXtreme Web Theater;
- қауіпсіз кіріктірілген нақты уақыт жүйесі;
- жұмыс станциялары мен маршрутизаторлар бойынша жаңарту қажеттілігі жоқ;
- тіркелмеген ішкі желіні пайдаланушылар үшін Интернет желісі

ресурстарына толық қол жеткізу;

- Cisco IOS бойынша маршрутизаторлармен үйлесімділік;
- Microsoft NetMeeting, Intel Internet Video Phone және White Pine Meeting Point қоса алғанда, h. 323 протоколын пайдаланатын бейнеконференцияларды қолдау;
- бірнеше ықтимал бағдарламалық және аппараттық қамтамасыз ету жиынтығы;
- орталықтандырылған әкімшілендіру құралдары;
- пейджерді немесе электрондық поштаны пайдалана отырып ақпараттандыру;
- Ethernet, Fast Ethernet, Token Ring және FDDI интерфейстерін қолдау;
- IPSec стандартты технологиясын пайдалана отырып, виртуалды жеке желілерді қолдау (Virtual Private Network) ;
- жоғары өнімділік;
- Cisco компаниясының ciscosecure идентификация сервері сияқты басқа шешімдермен интеграциялау.



Сурет 3.1 - Cisco PIX МЭ қолдану мысалы

3 Есептеу бөлімі

3.1 Желінің өткізу қабілетін оңтайлы тарату есебін шешу

Желі инфрақұрылымы N тораптардан және M сандық желілерден тұрады, олар өткізу қабілеті U_m бит/с бар m буынымен бірнеше тораптарды жалғайды. Бір бағытта ғана трафик беріледі. Сондай-ақ, желі бойынша жүктеме ағындары k беріледі деп болжаймыз. M буынындағы k класына қызмет көрсету үшін W_{km} бит/с өткізу жолағы қажет деп санаймыз [11].

Негізгі беру бірлігі анықталады:

$$\delta \quad ЕҮОБ(u_1,...,u_M, w_1,...,w_K), \tag{3.1}$$

мұнда ЕҮОБ - өткізу жолағының ең үлкен бөлгіші;

$u_1,...,u_M$ - желіде бар барлық қосқыш сандық желілер;

$w_1,...,w_K$ - өткізу жолағы

k – қызмет көрсету класы.

Нәтижесінде негізгі беріліс бірліктері түрінде m-буынды өткізу жолағының бүтін санын аламыз:

$$u_m = \frac{U_m}{\delta} \tag{3.2}$$

Жалпы өрнек k класын шақыру үшін өткізу жолағына қойылатын талаптар (3.3) негізгі беріліс бірлігі түрінде:

$$w_{km} = \frac{W_{km}}{\delta} \tag{3.3}$$

Бұл пакеттік коммутациясы бар желілер үшін арналар коммутациясы бар желілер модельдерін зерттеу кезінде телетрафик теориясында дамыған модельдер мен әдістерді пайдалануға мүмкіндік береді. Бұл жағдайда арнаның аналогы негізгі беріліс бірлігі болады.

Желі ресурстары барлық VPN үшін, Саны s тең болсын. k буынында s-VPN бөлінген өткізу жолағы u_{ks} арқылы, яғни:

$$\sum_{s=1}^{S} u_{ks} = u_k \tag{3.4}$$

Бұл мәнде жиынтықтау трафигін тарату маршруттары k буыны арқылы өтетін VPN бойынша ғана жүріп жатыр деп жауап берген жөн.

h символы «дерек көзі-адресат» бірнеше түйіндерін, ал (k,h) – «дерек көзі-

адресат» h арасында k сервисі бар шақырулар ағынын білдіреді. VPNs қатысты шамалар s төменгі индексімен белгіленген. Ағындарға арналған ықтимал маршруттар жиынтығы(k,h) R_s (k, h) белгіленген. Олар белгілі және бекітілген. Маршруттар жиынтығы сервис түріне байланысты болады деп болжаймыз. Мысалы, кідіріске сезімтал трафик (дауыстық, бейне және т.б.) қысқа маршрут бойынша, яғни бірнеше аралықпен маршрут бойынша, ұзын жолмен өтетін деректер трафигіне қарағанда жүреді.

Егер маршрут бойынша қажетті өткізу жолағын қамтамасыз ететін буын болмаса, шақыру жоғалуы мүмкін. Егер шақыру қабылданған болса, онда осы шақыруға қажетті Өткізу жолағы шақырудың жүру бағытын құрайтын әрбір буындағы шақыру ұзақтығының барлық уақытында айналысады.

$VPN(k,h)_s$ келіп түсетін шақырулар $L(k,h)_s$ орташа мәні бар Пуассон Заңы бойынша бөліңсін,ал $r \cdot R_s(k,h)$ - h жұбы арасындағы нақты маршрут. Сонымен қатар, резервтелетін өткізу жолағын алу уақыты экспоненциалды заң бойынша орташа мәнмен бөлінген, алдыңғы шақырулар мен оларға қызмет көрсету уақытына байланысты. 1/ z_{khs} және $(k,h)_s$ шақырулар түсімдерінің арасындағы интервалдар r нақтымаршруты бойынша R орташа мәні l(k,h)s болатын Пуассон бөлінісі бар, бұл ретте:

Трафиктің тиісті қарқындылығы, $q(k,h)_s = l(k,h)_s/z(k,h)_s$, демек,

$$\sum_{r \in R_s(k,h)} q(k,h)_s \leq \underline{O}(k,h) \tag{3.6}$$

мұндағы $\underline{O}(k,h)_S$. = $L(k,h)_s/z(k,h)_s$.

Пайдалана отырып, сипатталған жоғары үлгісін қалыптастырамыз міндетін оңтайлы бөлу желілік ресурстарды іске асыру үшін VPN базасында арналық моделі.

$$D_s = \sum_{(k,h)} \sum_{r \in R_S(k,h)} d(k,h)_s q(k,h)_s (1 - P(k,h)_s) \tag{3.7}$$

Сонда барлық S VPN жалпы табыс:

$$D = \sum_{s=1}^{S} \mathrm{D}_s \tag{3.8}$$

Әдетте $d\,(k,\,h)_S$ профиль қажетті өткізу жолағына сәйкес келеді. Алайда, басқа да өлшемдер қолданылуы мүмкін, мысалы, кіріс көзі мен адресат арасындағы қашықтыққа байланысты болуы мүмкін. Осылайша, d part k, h, s параметрі табысты арттыру жылдамдығы мен үздік қызмет көрсету жоғары болатын қызмет көрсету сапасының осындай деңгейін теңшеу үшін пайдаланылуы мүмкін.

Жалпы VPN оңтайлы жобалау есебі:

$$\max_{\{u_{ms}\},\{q_{khs}\}} D, \tag{3.9}$$

$$\sum_{r \in R_s(k,h)} q(k,h)_s \leq Q(k,h)_s \forall (k,h)_s,\ \forall_s$$

Сонымен қатар, әрбір арнада маршрутизацияның шешімі VPN жүзеге асыру үшін желі буындарында өткізу қабілетін қайта бөлумен сүйемелденеді. (3.9) өрнектен көрініп тұрғандай, оңтайлы маршруттау есебі әрбір VPN үшін бөлек шешіледі және сызықты емес бағдарламалаудың міндеті болып табылады.

$$q(k,h)_s \geq 0, \sum_{s=1}^{S} u_{ms} = u_m \forall m,\ \ u_{ms} \geq |0\ \forall (k,h)_s, \forall m. \tag{3.10}$$

Өткізу қабілетін оңтайлы қайта бөлу міндеті алдыңғы итерацияда оңтайлы маршруттау міндетін шешуден алынған деректер негізінде шешіледі. VPN-дің жалпы кірісі өсуі үшін VPN арасында желі учаскелерінің өткізу қабілетін қайта бөлу қажет. Бұл үшін M буынында s VPN бөлінген өткізу жолағының өзгеруінен табыстың тәуелділігін анықтау қажет:

$$\frac{\partial D_s}{\partial u_{ms}} \sim d_{ms} \tag{3.11}$$

Сонда алып отырған өткізу жолағын азайту кезінде табыс шығынының шамасын экстраполяциялау төменегідей өрнектеледі:

$$D_s(u_s - b_s) - D_s(u_s) \approx -\sum_{m-1}^{M} d_{ms} b_{ms} \tag{3.12}$$

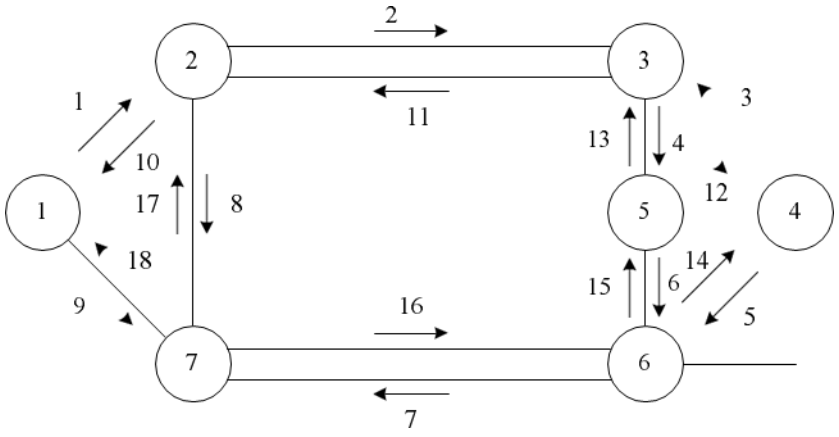
VPN бойынша желілік ресурстарды оңтайлы тарату әдістемесін қарастырайық. Болсын анализируемая желісі тұрады, N=7 тораптар мен 18 бір бағыттағы, еркін түрде, нөмірленген буындарының M=18 (3.1-сурет).

2-м және 3-м тораптар арасындағы буындарды қоспағанда, 155 Мбит/с БІР бағыттағы буындардың өткізу қабілеті, сондай-ақ 2х155=310 Мбит/с өткізу қабілеті бар 7-м және 6-м.желілерде сервистің үш сыныбы қолданылады. Бұл қызметтердің бір шақыруын өткізудің тиімді жолағы, бастапқы деректерді ескере отырып, тиісінше 16, 48 және 160 кбит/с тең, негізгі беріліс бірлігі үшін 16 кбит/с тең жолақ қолданылады.

Кесте 3.1 - VPN жүктемелердің қарқындылығы матрицасы

VPN 1	1	2	3	4	5	6	7
1	0	70,8	48	7,2	62,4	34,8	13,8
2	82,8	0	165,6	21	214,2	103,8	41,4
3	55,2	172,8	0	13,8	127,8	62,4	24
4	7,2	21	10,2	0	12	6	3,6
5	76,2	227,4	134,4	15	0	70,8	31,2
6	34,8	96,6	55,2	6	62,4	0	13,8
7	13,8	34,8	21	3,6	27,6	13,80	0
VPN 2	1	2	3	4	5	6	7
1	0	18	48	3,6	31,2	17,4	7,2
2	21	0	165,6	10,2	106,8	51,6	21
3	55,2	172,8	0	27,6	255,6	124,2	48
4	3,6	10,2	21	0	12	6	3,6
5	37,8	114	269,4	15	0	70,8	31,2
6	17,4	48	110,4	6	62,4	0	13,8
7	7,2	17,4	41,4	3,6	27,6	13,8	0
VPN 3	1	2	3	4	5	6	7
1	0	18	24	3,6	31,2	17,4	13,8
2	21	0	82,8	10,2	106,8	51,6	41,4
3	27,6	86,4	0	13,8	127,8	62,4	48
4	3,6	10,2	10,2	0	12	6	7,2
5	37,8	114	134,4	15	0	70,8	62,4
6	17,4	48	55,2	6	62,4	0	27,6
7	13,8	34,8	41,4	7,2	55,2	27,6	0
VPN 4	1	2	3	4	5	6	7
1	0	18	24	7,2	62,4	34,8	7,2
2	21	0	82,8	21	214,2	103,8	21
3	27,6	86,4	0	27,6	255,6	124,2	24
4	7,2	21	21	0	47,4	23,4	7,2
5	76,2	227,4	269,4	59,4	0	283,8	62,4
6	34,8	96,6	110,4	23,4	248,4	0	27,6
7	7,2	17,4	21	7,2	55,2	27,6	0

Сонымен қатар, барлық бағыттарда жүктемені біркелкі бөлу кезінде және буындардың өткізу қабілетінің тепе-тең бөлінуіне сәйкес келетін VPN арқылы түсетін жүктеме үшін мәндер келтірілген. Бастапқы деректерді ескере отырып, берілген жүктеме саннан алынған табысқа тең.



Сурет 3.1 - Желі үлгісі

Осылайша, барлық m үшін тиісінше k -1, 2, 3 үшін w_{km} =1, 3, 10 сервисінің әрбір сыныбы үшін талап етілетін нормаланған жолақ. 155 және 310 Мбит/с жолағы бар буындарды сәйкесінше 9688 және 19375 беру бірлігі ретінде ұсынуға болады. Яғни u_m -бұл 9688 немесе m=1, 2 үшін 19375.. М. провайдердің Желісі қызмет көрсетеді төрт пайдаланушылық VPN. Осы VPN-ның соңғы нүктелері әрбір нүктеден әрбір сервис түріне қарай трафикті құрады.

Мұндай мәнде табыс өткізу жолағының бірліктеріндегі тасымалданған жолаққа тең. Маршруттар жиынтығы келесі қарапайым ереже негізінде құрастырылған:

$$\varepsilon = \frac{D_j - D_{j-1}}{D_j}, \tag{3.13}$$

$$R_s(k,h) = \{\text{маршрут саны } r \leq 3\} \tag{3.14}$$

Бұл әрбір VPN үшін маршруттардың жалпы саны 90-ға тең, яғни 360 маршруттың желісінде.

Кесте 3.2 - Белгілі бір сервис жүктемесінің қарқындылығын анықтауға арналған коэффициенттер

Сервистер	1	2	3
Коэффициенттер	0.5	1	0,5

Сонымен қатар, бұл жүйе барлық желі бойынша орташа табыстың 5,4% - ға ұлғаюын және жоғалтулар ықтималдығының екі еседен астамын азайтуды қамтамасыз етеді.

3.4-кестеде келтірілген бөлу жолақтары жекелеген буындарының арасында желі VPN. Алынған шамалардың мәндері бастапқы мәндерден орташа алғанда 20% - ға ерекшеленеді.

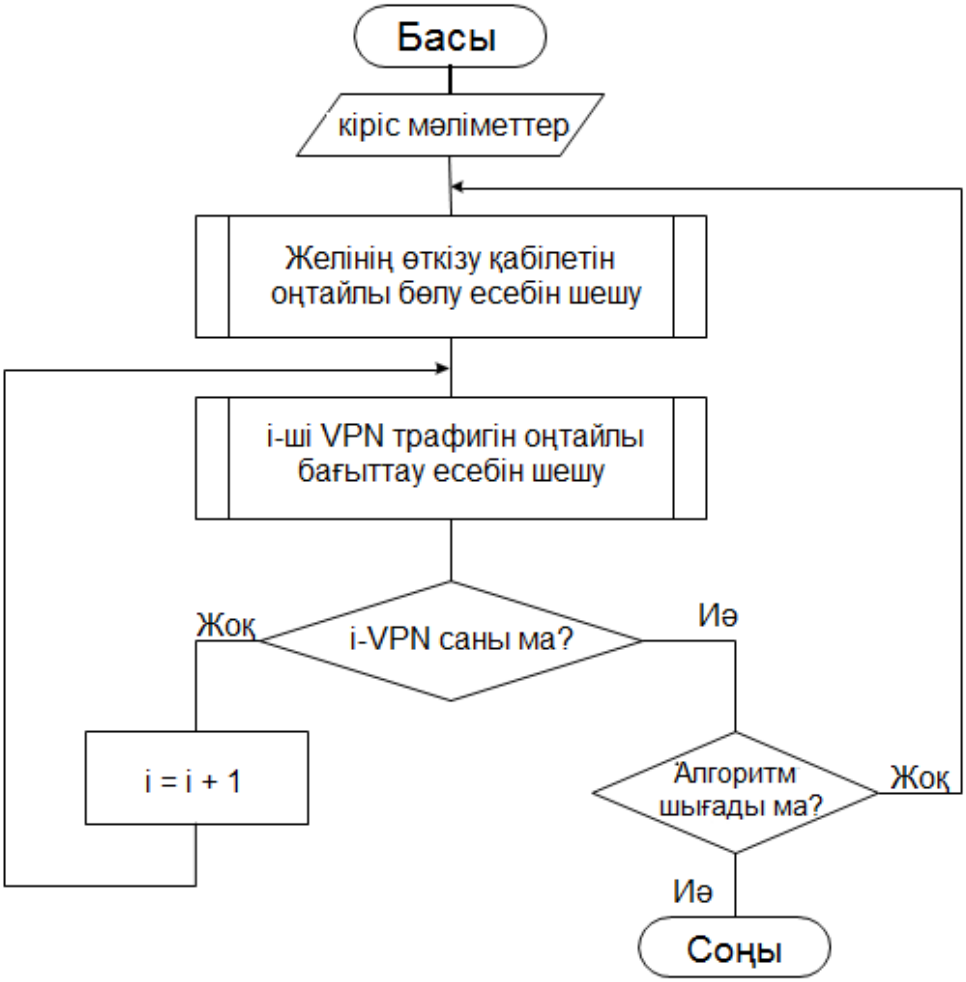
Кесте 3.3 - Жүктемені біркелкі және оңтайлы бөлу кезінде VPN арқылытүсетінжүктеме.

VPN	Ең жоғары табыс	Жүктемені біркелкі бөлу		Жүктемені оңтайлы бөлу	
		Кіріс	Жоғалту ықтималдығы, %	Кіріс	Жоғалту ықтималдығы, %
1	19781,7	17690,0	10,6	18861,5	4,2
2	18273,1	16074,8	12,1	17272,5	5,5
3	14188,0	12479,9	12,1	13387,9	5,4
4	25025,9	21880,5	12,8	23440,0	6,3
Барлық желі	77178,7	6815,2	11,8	72971,9	5,6

Кесте 3.4 - VPN арасында желінің жекелеген буындарын өткізу жолағын тарату

Буындары	VPN 1	VPN 2	VPN 3	VPN 4
1	3355	2011	1942	2380
2	5828	4953	3626	4968
3	1756	2530	1591	3811
4	2102	2299	1710	3577
5	1728	2535	1623	3802
6	2173	2128	1632	3755
7	5392	3753	3976	6254
8	2947	2021	2030	2690
9	3321	1947	1977	2443
10	3362	2016	1942	2368
11	5864	4974	3578	4959
12	1738	2578	1613	3759
13	2035	2245	1628	3780
14	1766	2573	1579	3770
15	2106	2139	1696	3747
16	5380	3780	3937	6278
17	3021	1992	1944	2731
18	3415	1943	1909	2421

Қаралып отырған мысал уақыт кеткен 5 итерация қол жеткізу үшін шектен жинақтылық 10^{-3} (3.2-сурет).



Сурет 3.2 - Арналық модель базасында VPN оңтайландыру алгоритмі

3.2 Жаһандық желінің өткізу қабілетін есептеу

Бір арналы екі фазалы жүйе деп аталатын басқа типті кезектер жүйесіне ұқсас. Екі Жергілікті желілерді көпірлердің немесе маршрутизаторлардың көмегімен қосу схемасы. Бір жергілікті желіден екіншісіне мәліметтер кадрын беру үшін ол екі құрылғымен (бұл жағдайда екі көпірмен немесе екі маршрутизатормен) қызмет көрсетілуі тиіс, сондықтан мұндай схема бір арналы көпфазалы модель шеңберінде сипатталуы мүмкін. Бір – бірінен алыстатылған екі жергілікті желілер арасындағы ақпараттық ағынның ең тар орны-өткізу қабілеті әдетте жергілікті желі жұмысының жылдамдығынан айтарлықтай аз ғаламдық желінің байланыс арнасы. Желі жұмыс станциясы деректер кадрын Ethernet желісіне жібереді-алдымен желі сегментінен көпірге немесе маршрутизаторға желі жұмыс істейтін жылдамдықпен (4, 10, 16 Мбит/с). Қалай орындалады қызмет көрсету кадр қарама-қарсы аяғында арна ғаламдық желілер. Кіре отырып келген жаһандық желісін көпір/маршрутизатор,

кадр өзгертіледі форматына lan беріледі желі. Себебі ақпаратты беру жылдамдығы бойынша ғаламдық желісі әрқашан төмен жылдамдықты беру, кадрларды жергілікті ешқандай кезектегі жағдайда, осындай қызмет көрсету емес, болды мүмкін негізгі үлесі қызмет көрсету кезінде кадрдың екінші мосте/қосып, дұрыста орнату енгізеді өзі құрылғысы. Және бұл бірінші көпірде/маршрутизаторда кадрлардың кідіруі уақытының аз үлесі ғана. Сондықтан жергілікті желілер арасындағы байланыстың екі нүктелік желілерін сипаттау үшін бір арналы бірфазалы модельді тыныш пайдалануға болады. ТМО-ның математикалық аппаратын қолдана отырып, кадрларды тарату уақытының жаһандық желі жұмысының жылдамдығына тәуелділігін нақты арналарға қоспай есептеуге болады. Мұндай есептеулер желі өнімділігіне қатысты көптеген сұрақтарға жауап беруге мүмкіндік береді; сонымен қатар, байланыс арнасының жұмыс істеу жылдамдығының өсуіне қалай әсер етуі мүмкін және ғаламдық желі арналары бойынша ақпарат алмасудың өсу жылдамдығы қандай жағдайда көпір/маршрутизатор өнімділігінің айтарлықтай өсуіне әкелмейді. Есептеу үшін бастапқы деректер:

- станциялар саны-500;
- бір станциядан транзакциялар (кадрлар) саны-700.

Жұмыс режимі тәулік бойы (24 сағат). Ең үлкен жүктеме сағатына берілетін кадрлардың барлық санынан 20% беріледі. Кадр өлшемі 80 байт.

Hub арқылы сағат жиыны Гаусс бөлу кезінде өтеді:

$$N = 700 \cdot 500 \cdot 0.2 = 70000 \text{ кадр.}$$

Қалыпты бөлу кезінде:

$$N = 700 \cdot 500 / 24 = 14583{,}3 \text{ кадра.}$$

Кадрлардың түсу жылдамдығы (яғни бөлумен алынған сандарды 3600 кезінде Гаусстық бөлу:

$70000 / 3600 = 19{,}44$ кадр секунд шамасында.

Қалыпты бөлу кезінде:

$14583{,}3 / 3600 = 4{,}05$ кадр секунд шамасында.

Қызмет көрсету жылдамдығын есептеу үшін жаһандық желі жұмысының белгілі бір жылдамдығының мәнімен белгіленуі керек. Бастапқы жақындау ретінде ғаламдық желі бойынша ақпарат алмасу жылдамдығы, өйткені барлық есептеулер басқа жылдамдық мәніне оңай қайталанады. Бір кадрдың ұзындығы 80 байт болатын бір кадрды жіберу үшін қажетті уақыт 0,01 секунд құрайды. Қызмет көрсетудің күтілетін уақыты 0,01 с тең, сонда қызмет көрсетудің орташа жылдамдығы (күтілетін қызмет көрсету уақытына кері шама) 100

кадрды құрайды. Сонымен қатар, қызмет көрсету жылдамдығы кадрлардың түсу жылдамдығынан жоғары, яғни бұл арна кіріс трафигін игереді. Бір арналы бір фазалы жүйеде қызмет көрсету құрылғысының техникалық мүмкіндіктерін пайдалану деңгейін (Р) тапсырыстардың орташа түсу жылдамдығын қызмет көрсетудің орташа жылдамдығына бөле отырып анықтауға болады. Гаусстық бөлу кезінде:

$$P = 19,44/100 = 0,1944 = 19,44\%.$$

Қалыпты бөлу кезінде:

$$P = 4,05/100 = 0,0405 = 4,05\%.$$

Қызмет көрсететін құрылғыны пайдалану дәрежесін біле отырып, қазіргі уақытта тапсырыстардың болмауы ықтималдығын анықтау оңай. Біз P0 ретінде белгілеген бұл ықтималдық минус арнаны пайдалану дәрежесіне тең (P0 = 1 - P). Гаусстық бөлу кезінде:

$$P0 = 1 - 0,1944 = 0,8066 = 80,66\%.$$

Қалыпты бөлу кезінде:

$$P0 = 1 - 0,0405 = 0,9595 = 95,95\%.$$

Қызмет көрсету құрылғысының пайдалану деңгейіне қатысты кейбір мәліметтерді алып, кадрлардың кезектерде қалай жиналғанын және осы кезектерге байланысты кідірістер бір жергілікті желіден екіншісіне кадр жіберу процесіне қалай әсер ететінін анықтаймыз. Жүйеде нысандардың орташа саны (unit) әдетте L, ал кезекте нысандардың орташа саны-Lq деп белгіленеді. Бір арналы бір фазалы жүйе үшін L орта Қызмет көрсету жылдамдығы мен тапсырыстардың түсу жылдамдығы арасындағы айырмашылыққа бөлінген тапсырыстардың орташа түсу жылдамдығына тең болады. Гаусстық бөлу кезінде:

$$L = 19,44 / (100 – 19,44) = 0,2414.$$

Қалыпты бөлу кезінде:

$$L = 4,05 / (100 – 4,05) = 0,0422.$$

Осылайша, маршрутизатор мен байланыс желісінің буферінде кез келген уақытта бір кадрдың 4 - 24% - дан сәл артық болады. Анықтау үшін орташа саны объектілерді кезек (Lq), перемножим пайдалану дәрежесі қызмет көрсету құрылғылары (Р) нысандар саны (L). Гаусстық бөлу кезінде:

$$Lq = 0{,}2414 \cdot 19{,}44 = 0{,}0469.$$

Қалыпты бөлу кезінде:

$$Lq = 0{,}0422 \cdot 4{,}05 = 0{,}00171.$$

Кесте 3.5 - WAN өткізу қабілетін түрлендіру

Атауы	Формула	Тиісті мәндері					
Жылдамдығы, (кбит/с)		19,1	31	63	1128	266	522
Кадр беру уақыты, с		0,043	0,03	0,02	0,004	0,003	0,002
Қызмет көрсетудің орташа жылдамдығы.		40	50	150	200	350	700
Арнаны пайдалану дәрежесі	P	0,638	0,398	0,1945	0,087	0,058	0,014
Жүйеде кадрлардың болмауы ықтималдығы	P0 = 1 - P	0,341	0,621	0,806	0,901	0,952	0,976
Объектілердің орташа саны (барлығы)	L	1,841	0,637	0,242	0,106	0,052	0,025
Кезектердегі объектілердің орташа саны	Lq = L · P	1,194	0,2347	0,036	0,020	0,001	0,0005
Толық күту уақыты	W	0,095	0,031	0,011	0,005	0,002	0,002
Кезекте күту уақыты	Wq = W·P	0,0615	0,0126	0,0025	0,0004	0,0002	3,1E-05

Объектінің жүйеде болуының орташа уақытын (W) және кезекте күтудің орташа уақытын (Wq) есептеуге мүмкіндік береді. Жүйеде болудың орташа уақыты қызмет көрсету жылдамдығы мен тапсырыстардың түсу жылдамдығы арасындағы кері айырмашылық болып табылады. Бұл жағдайда әрбір кадр жүйеде орта есеппен өткізетінін табамыз. Гаусстық бөлу кезінде:

$$W = 1/(100 - 19{,}44) = 0{,}0124\text{с}.$$

Қалыпты бөлу кезінде:

$$W = 1 / (100 - 4,05) = 0,0104c.$$

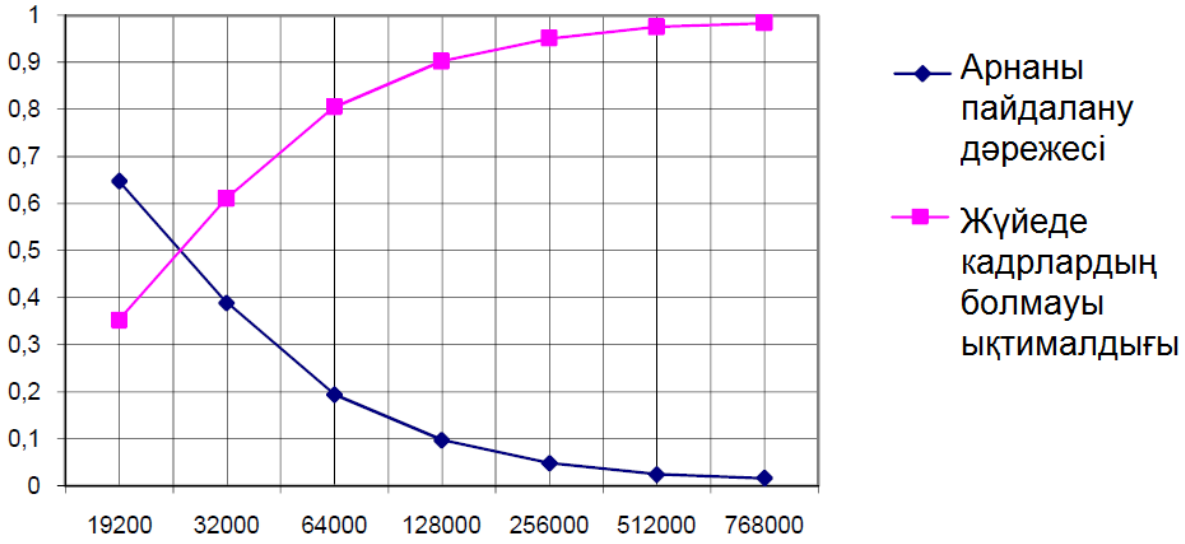
Жүйеде кезек күту уақытын сипаттауға болады. Wq жүйеде қызмет көрсету құрылғысының пайдалану дәрежесіне тең күту уақытын құрайды. Осылайша, Гаусстық бөлу кезінде:

$$Wq = 0,0124 \cdot 0,1944 = 0,00241c.$$

Қалыпты бөлу кезінде:

$$Wq = 0,0104 \cdot 0,0405 = 0,00042c.$$

3.6-суретте жүйеде кадрлардың болмау ықтималдығы және арнаны пайдалану дәрежесі көрсетілген.



Сурет 3.4 - Кадрлардың болмауы ықтималдығының тәуелділігі жүйесі

Өткізу қабілетінің өсуіне қарай күту уақытының ұтысының заңды азаюы әртүрлі өткізу қабілеті бар арналар үшін жаһандық желінің өнімділігін салыстыру кезінде әсіресе жақсы көрінеді. Байланыс арнасының өткізу қабілеті төртінші деңгейден жоғары (128000 бит/с) ұлғайған кезде жүйеде кадрлардың болмау ықтималдығы іс жүзінде өспейді.

Бұл ретте кезекте күту уақыты 0,000538 сек, ал байланыс арнасы бойынша беру уақыты бір жаққа – 0,005 сек құрайды. Арнаны пайдалану дәрежесі 90%, ал жүйеде кадрлардың болмауы ықтималдығы 10%. Бұл жағдайда маршрутизатор алмасу буферінде кез келген уақытта бір кадрдың

0,5% болады.

3.6-кестеде жаһандық желінің өткізу қабілетінің өзгеруі кезіндегі есептер көрсетілген.

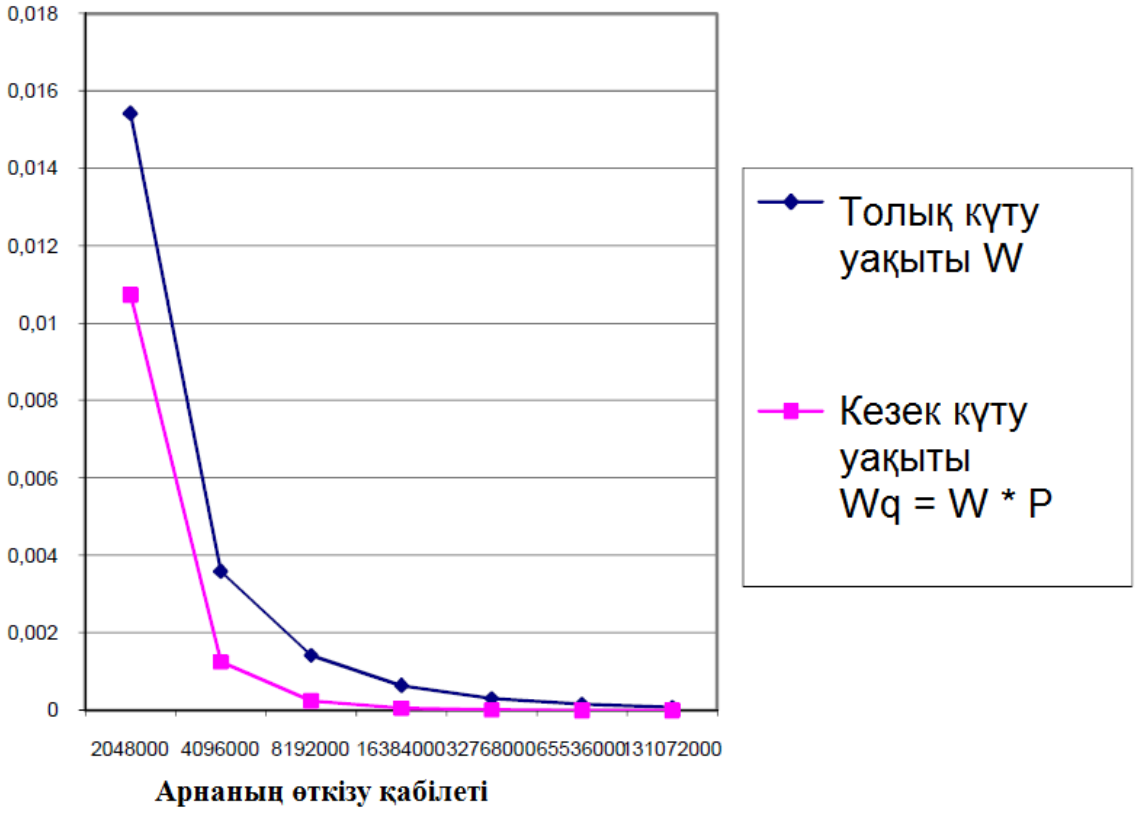
Кесте 3.6 - Жаһандық желінің өткізу қабілеті

Атауы	Форм.	Тиісті мәндері						
Желінің бір абонентке орналасуы, сағ		1	1	1	1	1	1	1
Кодтар, дыбыстар, жылдамдығы кбит / с		19,8	19,8	19,8	19,8	19,8	19,8	19,8
Тәулігіне 1 абоненттік трафик, Мбит		71,28	71,28	71,28	71,28	71,28	71,28	71,28
Орташа кадр ұзындығы, кбит		1,2	1,2	1,2	1,2	1,2	1,2	1,2
Бір абоненттен кадрлар саны, 10^3		59,4	59,4	59,4	59,4	59,4	59,4	59,4
Абонент саны		18	18	18	18	18	18	18
Кадрлардың саны х 10^3		1059,2	1059,2	1059,2	1059,2	1059,2	1059,2	1059,2
Қоңыраулардың жалпы санының пайызы, %		50	50	50	50	50	50	50
Тұрақты кадрлардың жылдамдығы		148,5	147,5	148,5	148,5	158,5	168,5	158,5
Желі жылдамдығы (Мбит/с)		2,048	4,086	8,292	16,394	32,76	65,63	131,07
Кадр беру уақыты, мс		4,68	2,34	1,16	0,59	0,28	0,15	7,3E-02
Қызмет көрсетудің орташа жылдамдығы		213,3	426,66	853,43	1706,7	3414,3	6825,6	13653,
Арнаны пайдалану дәрежесі	P	0,69	0,36	0,17	0,086	0,04	0,01	0,01
Жүйеде кадрлардың болмауы ықтималдығы	P0=1-P	0,304	0,652	0,826	0,914	0,957	0,979	0,988

Кесте 3.6-ның жалғасы

Объектілердің орташа саны (барлығы)	L	2,28	0,524	0,21	0,08	0,045	0,023	0,012
Кезектердегі орташа саны	Lq=L·P	1,58	0,18	0,027	0,008	0,002	0,0005	0,0002
Толық уақытша күту, мс	W	15,41	3,59	1,21	0,65	0,31	0,16	7,4E-02

3.5-суретте толық күту уақыты және кезек күту уақыты көрсетілген.



Сурет 3.5 - Толық күту уақыты және кезек күту уақыты

Сурет 3.6 - Арнаны Р және P_0 пайдалану дәрежесі

Бұл жағдайда кезек күту уақыты 10,7367 мсек құрайды, ал бір жаққа байланыс арнасы бойынша беру уақыты 4,68 мсек. Арнаны пайдалану дәрежесі 70%, ал жүйеде кадрлардың болмауы ықтималдығы 30%.

3.3 VPN желісінің өнімділігін талдау

Желі өнімділігі-бұл өте маңызды параметр және оны азайтатын кез-келген құралдарға, кез-келген ұйымда күдік бар. VPN-құрылғы арқылы өтетін трафикті өңдеуге байланысты қосымша кідірістер енгізетін VPN құру құралдары да ерекшелік болып табылмайды. Трафикті криптографиялық өңдеу кезінде туындайтын барлық кідірістерді үш түрге бөлуге болады:

- VPN-құрылғылар арасында қорғалған қосылысты орнату кезіндегі кідірістер;
- қорғалатын деректерді шифрлау және шифрлеу, сондай-ақ олардың бүтіндігін бақылау үшін қажетті түрлендірулермен байланысты кідірістер;
- берілетін пакеттерге жаңа тақырып қосумен байланысты кідірістер.

VPN құрудың ең көп таралған нұсқаларын іске асыру желі абоненттері арасында емес, тек VPN-құрылғылар арасында қорғалған қосылуларды орнатуды көздейді. Қолданылатын алгоритмдердің криптографиялық тұрақтылығын есепке ала отырып, кілтті ауыстыру ұзақ уақыт аралығы арқылы мүмкін. Сондықтан VPN құру құралдарын пайдалану кезінде бірінші типті кідірістер деректермен алмасу іс жүзінде әсер етпейді. Бұл тезис 128 бит (Triple DES, ГОСТ 28147-89 және т.б.) кем емес кілттерді пайдаланатын тұрақты шифрлау алгоритмдеріне қатысты. Бұрынғы DES стандартын пайдаланатын

құрылғылар желі жұмысына белгілі бір кідірістер енгізе алады [12].

Екінші типтегі кідірістер жоғары жылдамдықты арналар арқылы (10 Мбит/сек бастап) деректерді беру кезінде ғана рөл атқара бастайды. Барлық қалған жағдайларда таңдалған шифрлеу алгоритмдерін бағдарламалық немесе аппараттық іске асырудың жылдам әрекеті және тұтастықты бақылау әдетте өте үлкен және «пакетті шифрлеу - пакетті желіге беру» және «пакетті желіден қабылдау - пакетті шифрлеу» (шифрлеу) уақыты осы пакетті желіге беру үшін қажетті уақыттан едәуір аз.

Негізгі мәселе VPN-құрылғы арқылы өтетін әрбір пакетке қосымша тақырып қосумен байланысты. Мысалы, қашықтағы станциялар мен орталық пункт арасындағы нақты уақыт ауқымында деректерді алмасуды жүзеге асыратын диспетчерлік басқару жүйесін қарастырайық. Берілетін деректер көлемі үлкен емес-25 Байттан артық емес. Бұл салыстырмалы өлшемде банк саласында (төлем тапсырмалары) және IP-телефонияда беріледі. Берілетін деректердің қарқындылығы

- Секундына 50-100 айнымалы. Желі арасындағы өзара іс-қимыл өткізу қабілеті 64 кбит/сек арналар арқылы жүзеге асырылады.

Бір айнымалы процестің мәні бар бума 25 байттың ұзындығына ие (айнымалы аты-16 байт, айнымалы мәні-8 байт, қызметтік тақырып

- 1 байт). IP протоколы пакеттің ұзындығына тағы 24 байт қосады (IP - пакеттің тақырыбы). Frame Relay LMI арналарын тарату ортасы ретінде пайдаланғанда тағы 10 байт FR-тақырып қосылады. Барлығы:

$$L_{всего} = L_{имя} + L_{знач.} + L_{сл.заг.} = 16+8+1+24 = 59 \text{ байт} = 472 \text{ бит}.$$

Осылайша, 10 секунд ішінде ауыспалы процестің 750 мәнін беру үшін (секундына 75 пакет) Өткізу жолағы қажет:

$$ПП = 75 \cdot 472 = 34,5 \text{ Кбит/с}.$$

Алынған мән 64 кбит/сек өткізу қабілетінің бар шектеулеріне сәйкес келетінін көрсетеді. VPN құру құралдарын қосу кезінде желіні қалай ұстап тұратынын қарастырайық. Бірінші мысал-SKIP протоколының тәртібі негізінде қаражат. 59 байтқа қосымша тақырып 112 байт қосылады (МЕМСТ 28148-89 үшін).

$$L_{по\ сети} = L_{всего} + L_{доп.} = 59+112 = 171 \text{ байт } (1368 \text{ бит}).$$

$$ПП = 75 \cdot 1368 = 102,6 \text{ Кбит/с}.$$

Яғни қолда бар байланыс арнасының максималды өткізу қабілеттілігінен 60% - ға артық.

IPSec протоколы және жоғарыда көрсетілген параметрлер үшін өткізу қабілеті 6% - ға (67,8 кбит/сек) артатын болады. Бұл жағдайда алгоритм үшін

қосымша тақырып ГОСТ 28147-89 54 байтты құрайды. Сонымен қатар, әртүрлі өндірушілердің құрылғыларында әрбір пакетке қосылатын қосымша тақырып бар болғаны 36 байтты (немесе 26 - жұмыс режиміне байланысты) құрайды, бұл өткізу қабілетінің ешқандай төмендеуіне әкелмейді (тиісінше 57 кбит/сек және 51 кбит/сек).

3.4 Оптикалық талшықтың негізгі сипаттамаларын есептеу

ОК сапасы Өлшеудің жалпы қабылданған әдістерін пайдалана отырып тексеріледі. ӨЖ параметрлеріне және тиісті өлшеу әдістеріне стандарттар орнату қажет. Еуропалық деңгейде осындай стандарттарды әзірлеу үшін CENELEC Электрондық компоненттер жөніндегі комитеттің 28 жұмыс тобы, дүниежүзілік деңгейде - 86 Халықаралық электротехникалық комиссияның техникалық комитеті жауап береді. Талшықты жарық таратқыштың ең маңызды жалпыланған параметрі апертура болып табылады. Оптикалық ось пен оптикалық конустың арасындағы бұрыш, ол толық ішкі шағылысу шарты орындалады.

N2 қабықшасының сыну көрсеткішін есептейміз, кабельдің оптикалық сипаттамаларына сүйене отырып, na = 0,13 сандық апертура

Бұл белгілі:

$$NA = \sqrt{n_1^2 - n_2^2}, \tag{3.15}$$

мұндағы, $1n_1$ – жүректің сыну көрсеткіші, 1,4681. сонда,

$$n_2 = \sqrt{n_1^2 - NA^2} \tag{3.16}$$

$$n_2 = \sqrt{1.4681^2 - 0.13^2} = \sqrt{2.1553 - 0.0169} = 1.4623$$

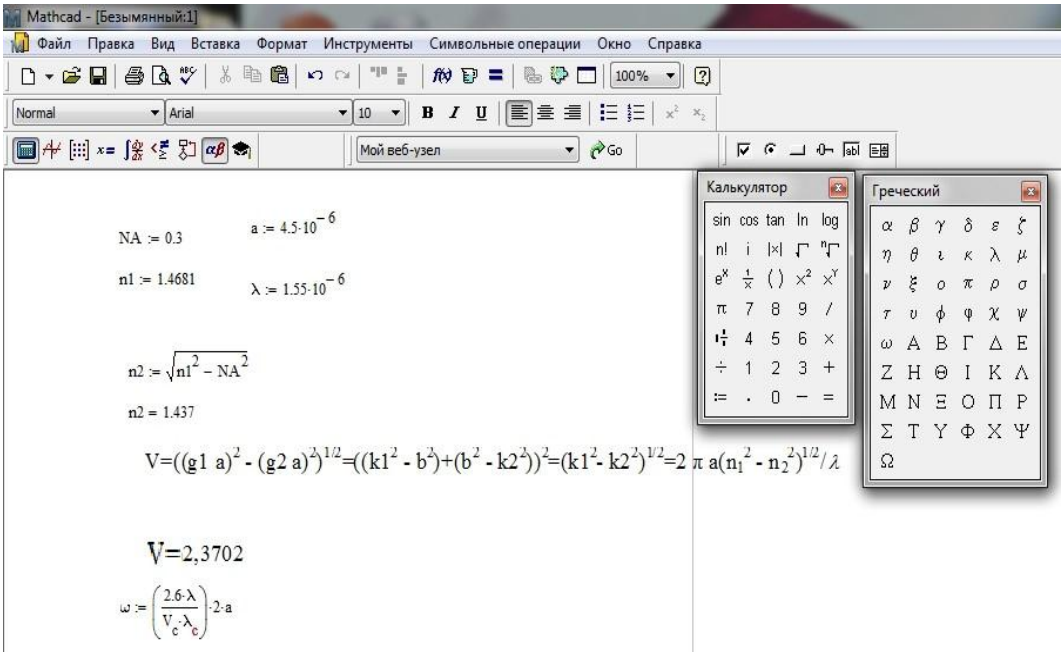
Ол өзегі (g1 a) мен қабығы (g2 a) үшін цилиндрлік функциялардың аргументтерін жинақтаумен алынады):

$$V = ((g1\ a)^2 - (g2\ a)^2)^{1/2} = ((k1^2 - b^2) + (b^2 - k2^2))^2 = (k1^2 - k2^2)^{1/2} = 2\ \pi\ a\ (n_1^2 - n_2^2)^{1/2}/\lambda \tag{3.17}$$

мұндағы а қабық өзегінің радиусы, а = 4,5 мкм;

n_1 - 1-өзектің сыну көрсеткіші, n_1=1,4681; n_2 -қабықтың сыну көрсеткіші, n_2=1,4623.

$$V = 2 \cdot 3.14 \cdot 4{,}5 \cdot 10^{-6} \cdot 0.13 / (1.55 \cdot 10^{-6}) = 2{,}3702$$



3.7 - Сурет. Mathcad бағдарламасындағы есептеулер

DF өткізу қабілеті өшумен қатар ТОБЖ маңызды параметрі болып табылады. Ол жарық өткізгішпен өткізілетін жиіліктер жолағын және сәйкесінше оптикалық кабель арқылы таратуға болатын ақпараттың көлемін анықтайды. Қабылдағыш құрылғысының кіруіне сигналдың бұрмалануымен байланысты айтарлықтай шектеулер бар. Бұл құбылыс дисперсия деп аталады және жарық өткізгіште әртүрлі мод тарату уақытының айырмашылығымен және сыну көрсеткішінің жиіліктік тәуелділігінің болуымен байланысты.

ҚОРЫТЫНДЫ

Дипломдық жобада Қазақстан аумағында орналасқан кез-келген мекемелердің филиалдары үшін корпоративтік байланыс желісін іске асыру схемасы ұсынылған (Алматы, Астана, Атырау қалаларында 3 нүкте).

Желі жер үсті арналары бойынша құрылады. Қазіргі уақытта ірі компаниялар телекоммуникация операторлары оптикалық талшық бойынша ұсынатын қызметті алуды қалайды. Серверлік клиенттен салынған оптикалық кабель оптикалық конвертер арқылы ДКП торабына қосылады. Техникалық бөлімде осы қосылымды іске асыру үшін сипаттамалар есебі және оптикалық кабельді таңдау жүргізілді. Жобада талданып қойылатын талаптар әзірлейтін желісінің құрылымы, жалпы ұйымдастыру сұлбалары құрастырылды. Жобада тұтынушының корпоративтік желісіне қосылу үшін қажетті барлық заманауи талаптарға жауап беретін жабдық таңдалынды.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР

1. С. В. Запечников, Н. Г. Милославская, А.И. Толстой. Основы построения виртуальных частных сетей. – М: Горячая линия – Телеком, 2003.

2. Лукацкий А.В. Неизвестная VPN. – М.:Компьютер – Пресс . – 2001.

3. Сериков И. Виртуальные частные сети PC Magazine RE. – 1999.

4. Мясковский Г.М. «Системы производственной радиосвязи»: Справочник - М: Связь 1980г.

5.Л.Г. Мордухович, А.П.Степанов. Системы Радиосвязи. Курсовое проектирование. Учебное пособие. Москва «Радио и связь» 1987 г.

6. А.С. Немировский, Е.В. Рыжков. Системы связи и радиорелейные линии. Москва «Связь» 1980 г.

7. В.В. Марков. Радиорелейная связь, М.: Связь,1979

8. Бутусов М.М., Верник С.М., Галкин С.Л., Гомзин В.Н., Машковец Б.М., Щелкунов К.Н. Волоконно-оптические системы передачи. – М.: Радио и связь, 1992.

9. Скляров О.К. Современные волоконно-оптические системы передачи, аппаратура и элементы. – М.: СОЛОН-Р, 2001.

10. Кемельбеков Б.Ж., Мышкин В.Ф., Хан В.А. Волоконно-оптические кабели. М., 1999.

11. Гроднев И.И. Волоконно – оптические линии связи: учебное пособие для высших учебных заведений. – М.: Радио и связь 1990.

12. Убайдуллаев Р.Р. Волоконно оптические сети. – М.: Радио и связь 1998.

13Алибаева С.А. Методические указания по дипломному проектированию (для студентов всех форм обучения направления 652400 – Радиоэлектроника и телекоммуникации). – Алматы: , 2001. - 17 с.