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

Тюлюбекова Сания

VPN технологиясының көмегімен телекоммуникациялық жүйелердегі ақпаратты қорғау

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
«____» _____2019 ж.

Дипломдық жобаға

ТҮСІНІКТЕМЕЛІК ЖАЗБА

Тақырыбы: VPN технологиясының көмегімен телекоммуникациялық жүйелердегі ақпаратты қорғау

5В071900 – Радиотехника, электроника және телекоммуникация мамандығы

Орындаған: Тюлюбекова Сания

Рецензия беруші
ҚазҰАУ, ЭҮжА каф.
меңгерушісі, доктор PhD.,
қауымдастырылған профессор
_____ Ж.С. Шыныбай
«____» _____ 2019 ж.

Ғылыми жетекші
ЭТжҒТ каф PhD докторы,
сениор-лектор
_____ Қ.Н. Тайсариева
«___»_____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 ғарыш технологиялар кафедрасы

5В071900 – Радиотехника, электроника және телекоммуникациялар

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
тех.ғыл.канд, профессор
_____ Е.Таштай
«____» _____2019 ж.

Дипломдық жоба орындауға
ТАПСЫРМА

Білім алушы *Тюлюбекова Сания*
Тақырыбы *VPN технологиясының көмегімен телекоммуникациялық жүйелердегі ақпаратты қорғау*
Университет ректорының *“ 16 ” 10 № 1162-б бұйрығымен бекітілген*
Аяқталған жобаны тапсыру мерзімі “____”_____ 2019 жыл.
Жұмыстың бастапқы мәліметтері: VPN технологиясын қолдана отырып телекоммуникация жүйелерінде ақпаратты қорғау
Дипломдық жобада өңделетін сұрақтар, дипломдық жобаның қысқаша мазмұны:
а) Телекоммуникациялық жүйелерде ақпараттық қорғауды зерттеу
б) VPN фукнциясының стандарттық технологиялары түсінігі
в) Тораптық VPN технологиясының артықшылықтары
Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс)
Сызбалық материалдар 12 слайдпен көрсетілген
Ұсынылатын негізгі әдебиет 13 атау

дипломдық жұмысты (жобаны) дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
Телекоммуникациялық жүйелерде ақпараттық қорғауды зерттеу	8.02.2019	
Пайдаланушылық VPN артықшылықтары, әртүрлі деңгейдегі қорғалған арналар	22.03.2019	
Техникалық есептеулер	21.04.2019	

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		

Ғылыми жетекшісі _____ Қ.Н. Тайсариева
(қолы)

Тапсырманы орындауға алған білім алушы _____ С.Тюлюбекова

Күні “___” _____ 2019 ж.

АНДАТПА

Бітіру жұмысы PFsense программаны камтамасыздару негізге VPN технологиясын қолдана отырып телекоммуникация жүйелерінде ақпаратты қорғау мәселелерін зерттеуге арналған.

Технология желілеріндегі ақпаратты қорғауды ұйымдастыру үшін қолданылатын технологияға шолу қарастырылған, арнаны қолдану деңгейінің есептеулері мен алынған компьютерлер үшін ақпарат тарату жылдамдығы келтірілді.

АННОТАЦИЯ

Выпускная работа посвящена исследованию проблем защиты информации в телекоммуникационных системах используя технологию VPN на базе программного обеспечения PFsense

Рассмотрен обзор технологий применяемых для организации защиты информации сетей телекоммуникаций, произведены расчеты степени использования канала и скорости передачи информации для взятого числа компьютеров.

ANNOTATION

The final work is devoted to the study of problems of information protection in telecommunication systems using VPN technology based on the PFsense software

The review of the technologies used to organize the protection of information telecommunications networks, calculations of the degree of use of the channel and the speed of information transfer for the number of computers taken.

МАЗМҰНЫ

КІРІСПЕ

Бұл кезеңнің басты ерекшелігі – индустриалдық қоғамның ақпараттық қоғамға ауысуы болып табылады, мұнда ақпарат энергетикалық немесе материалдық ресурстармен салыстырғанда маңызды болып саналады.

Біз ақпараттық әлемде өмір сүреміз. Ақпараттарды меңгеру әр кезде анағұрлым толық, сонымен қатар үлкен көлемді ақпараттарға ие болған жаққа артықшылықтарын ұсынады, әсіресе, өзінің қарсыласы туралы ақпаратқа сәйкес болса. Бұл мемлекеттік, сондай-ақ, коммерциялық құпия, осыған сәйкес, бұл ақпаратты іздеу және оған қол жеткізу адам қоғамының ерте ғасырында, мемлекет пайда болғанда, олардың өзара арасында сауданың даму уақытымен сәйкес болып келеді [1].

Ақпарат – тұлға, оқиға, құбылыс, ұғым және үдерістер туралы, олардың ұсынылуына тәуелсіз мәліметтер болып табылады.

«Ақпарат» сөзі қазіргі кезде көп тараған және әртараптанған. Оны пайдаланбайтын саланы табу өте қиын. Үлкен көлемі бар ақпараттық ағындар адамзатты жаулап алады. Ғылымдық білімдердің көлемі, мысалға алсақ, мамандардың көлемі әр бес жыл уақыт сайын екі еселенеді.

Ақпаратты заңдастырылмаған қолжетімділік арқылы қорғау мәселесі бұрынғы кезде адамға қандай да бір себеп бойынша ақпаратарды ешкімге немесе кез-келген адамға таратуы керек болмаған кезде туындады. Адамзат қоғамы дамуы, жеке меншік пайда болуы, мемлекеттік міндет, билікке күрес сонымен бірге ары қарай адам әрекетінің артуымен ақпараттың бағасын арттырады. Иесіне саяси, материалдық, әскери жеңісті және т.б. алып келетін мәлімет құнды болып келеді.

Ақпаратты автоматты түрде енгізу, сақтау, өңдеу, шығарумен күрделі автоматты басқару жүйесі пайда болуымен байланысты ақпараттың қорғау мәселесі одан үлкен болады.

Мамандар мәліметтерді өңдеуде ақпаратта заңдастырылмаған қолжетімділіктің барлық мүмкін болатын тәсілін атайды: деректерді бақылауға, көшіруге және алмастыруға, жалған бағдарланы, пәрменді және хабарламаны енгізуге, осындай мақсатта желіге және байланыс арнасына қосылуға, жөндеуге және апатты бағдарламалар және құралдарды пайдалануға, зиянды электрмагнит сәулелену сигналдарын қабылдауға және ақпараттарды жинауға, аппаратураның ақаулықтары және істен шығуларын пайдалануға, бағдарламалардың қателіктерін, пайдаланушылардың қателіктерін пайдалануға және т.б. мүмкіндік береді. Бағдарламаларды бұзушыны тоқтатуға мәліметерді өңдеудің автоматты жүйесінде қосымшаның барлық мүмкін нүктелерін табу және оның жолына сай келетін қажетті тығыздықты кедергілерді орнатуы керек.

1 Телекоммуникациялық жүйелерде ақпараттық қорғауды зерттеу

1.1 Ақпаратты қорғау мәселелері

Ақпаратты қорғаудың және компьютерлік қауіпсіздіктің салаларында негізінен мәселенің үш тобы өзекті болып табылады:

1. ақпараттың құпиялылығын бұзу;
2. ақпараттың бүтіндігін бұзу;
3. ақпараттық-есептеуіштік жүйесінің жұмысқа қабілеттілігін азайту.

Жасалған зерттеулер және ізденістердің негізгі бағыты біздің елде, сонымен қатар шетелдерде қарастырылды:

- заңдастырылмаған әрекеттен (ЗӘ) қорғау мен ұжымдық пайдаланудың ақпараттық-есептеуіш жүйелеріндегі деректеріне шектелген қолжетімділік;
- пайдаланушылар және техникалық құралдарды сәйкестендіру мен анықтау (соның ішінде «сандық» қолтаңба);
- байланыс жүйесінде сонымен қатар деректі тарату жүйесінде теріс ақпараттардан қорғанысты қамтамасыздандыру;
- деректердің қауіпсіздігін қамтамасыз етудің стандарттарының (халықаралық, ұлттық, ұжымдық) сенімділігі және пайдалануының жоғарғы деңгейінің техникалық сондай-ақ, жүйелі бағдарламалық қамтамасыздығын құру;
- телекоммуникациялық желіде мәліметтерді қорғау;
- компьютердің қауіпсіздігінің құқықтық аспектісін дайындау.

Еліміздегі телекоммуникациялық инфрақұрылымының қарқынды дамуына және халықаралық желіге шығуына қарай, ең маңызды мәселе ретінде компьютерді вирустан қорғау қарастырылады. Желі вирустары (репликатор) логикаға ие, желінің пайдаланушыларына таратылуын қамтамасыздандыратын ерекше вирустың түрі болып саналады.

Соңғы кезде телекоммуникация жүйелеріндегі ақпараттардың қауіпсіздігін қамтамасыз ететін стандарттаудың тәсілдері және әдістері мәселесінде үлкен халықаралық белсенділікті көре аламыз.

Айта кететініміз, білім беруші телекоммуникациялық желілердегі ақпараттық қауіпсіздікпен қамтамасыз ету мәселесінің арналымы бар:

- Жетілдірілген нысанды технологиялардың тарату жүйесінде бірінші орында білім беру телекоммуникациясында пайдаланатыны анық. Ашық жүйеге ауысу үшін мүмкіндік тудыратын үлкен пайда анық белігілі. Бірақ олардың ішінде мәліметтердің қауіпсіздіктері ескерілмейді. Керісінше, мәліметтерді өңдеудің орталықтары өз қызметінің кейбіреуін оның субъектісінің жүйені бақылауына жұмсайды.

- Білім беру телекоммуникациясын дамыту (ББТ) интеллектуалды меншіктің құқықтық қорғаныстық мәселелерінің тоқтауына ұшыратады.

- Техникалық қызметкерлердің алдын-ала заңдастырылмаған әрекетінен қорғаудың мәселесі де аса маңызды мәселе болып саналады, олар ұжымдық ақпараттық жүйе немесе желілік сегменттер қызметінің толық немесе бөлшекті түрде тоқтатыуына алып келеді.

Қауіпсіз берілісті сонымен қатар мәліметтердің сақталуын қамтамасыз етуге желі аралық экранды пайдалануға рұқсат.

1.2 Желіаралық экрандар

Желіаралық экран (firewall) дегеніміз– ішкі желілерді сыртқы шабуылдан қорғау үшін қолжетімділікті басқаруға арналған құрылғы. Сыртқы және ішкі желілердің арасында орналасады. Дұрыс бапталған экран маңызды қорғаныс құралы болып есептелінеді. Бірақ, ол рұқсатталған байланыс арнасымен шабуыл орындау мүмкіндігі жоқ. Мысалы, сырттан веб-серверге қолжетімділік рұқсатын бергенде сонымен қатар әлсіз орын болғанда оның бағдарламалық қамтамасыз етілуінде желіаралық экран осы шабуылды ары қарай өткізеді, өйткені ашық веб-қосылыс серверлердің жұмысы үшін керек. Желіаралық экран іштегі пайдаланушыдан қорғамайды, өйткені олар жүйенің ішкі жағында орналасқан.

1.3 Желіаралық экрандардың түрлерін анықтау

Желіаралық экранның екі негізгі түрі бар: қолданбалы деңгейдегі желіаралық экран, пакеттік сүзгілі желіаралық экран. Олардың негізінде әртүрлі жұмыс принциптері кездеседі, алайда дұрыс баптаулар кезінде құралдардың екі түрі шектелген трафиктің бұғатталуымен сипатталатын қауіпсіздік қызметінің дұрыс орындалуын қамтамасыз етеді.

1.3.1 Қолданбалы деңгейдегі желіаралық экрандар

Қолданбалы деңгейдің желіаралық экраны, басқаша айтқанда прокси-экран ортақ тағайындалған операциялық жүйеге негізделген (Windows NT сонымен қатар Unix сияқты) немесе желіаралық экранның аппаратты платформаларына негізделген программалық пакет түрінде ұсынылады. Желіаралық экрандар бірнеше интерфейске ие болады, сонымен қатар өзі қосылған әр желіге тең болып келеді. Саясат ережесінің жиыны трафик бір желі арқылы екінші желіге қалай алмасатынын анықтайды. Егер де ережеде

трафик жіберілуіне нақты рұқсат жоқ болса, онда желіаралық экран пакетті қабылдай алмайды және жойып жібереді.

1.3.2 Пакеттік сүзгілеуі бар желіаралық экрандар

Пакеттік сүзгіс бар желіаралық экран ортақ тағайындалған операциялық жүйеге негізделген (Windows NT сонымен қатар Unix сияқты) немесе желіаралық экранның аппаратты платформасындағы бағдарламалық пакет түрінде болады. Желіаралық экран көптеген интерфейске ие болып келеді, ол өзі қосылған әр желіге тең болып келеді. Саясат ережелесінің жиыны трафик бір желі арқылы екінші желіге қалай алмасатындығын анықтайды. Егер ережеде трафик таралуына нақты рұқсат болмаса, желі аралық экран пакетті қабылдай алмайды және жояды [3].

1.4 Виртуалды жеке желілерді анықтау

Біз ғаламтордың көмегімен жалдамалы байланыстың арнасын қолданбай, бұрынғыдай трафик құпиялылығы үшін мүмкін болатын шараларды қолданып, ұйымдағы құпия мәліметтерді жіберуге тырысып көреміз. Біз өзіміздің трафикті жаһандық желінің өзге пайдаланушылары трафигінен ненің көмегімен ажырата аламыз? Бұл сұрақ жауабы шифрлау болып келеді.

Ғаламторда әр түрлі трафикті кездестіре аламыз. Мұндай трафиктің көп бөлігі ашық түрде таралады және бұл трафикті бақылайтын кез келген пайдаланушы оны міндетті түрде тани алады. Бұл пошталық сонымен қатар веб-трафикке қатысты болып келеді, сондай ақ telnet және FTP хаттамаларымен байланыс арнасына қатысы бар. Secure Shell (SSH) сонымен қатар Hypertext Transfer Protocol Secure (HTTPS) трафиктері шифрланатын трафиктер болып есептелінеді, оны пакетті бақылағыш пайдаланушы байқай алмайды. Сондай ақ, SSH және HTTPS трафиктері VPN желісінің виртуалдық бөлігін тудырмайды [5].

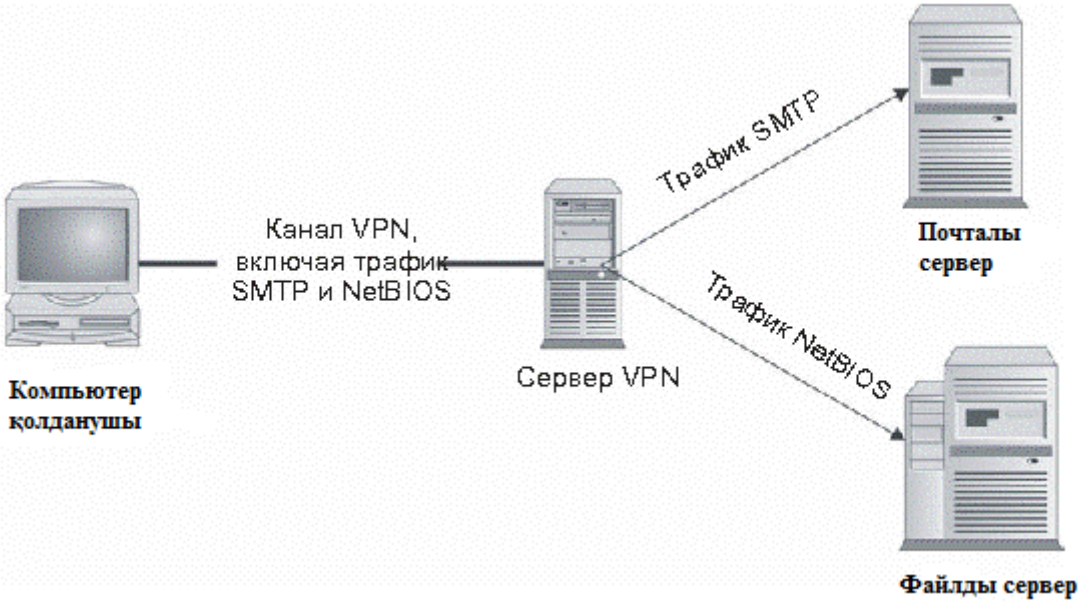
Виртуалды жеке желілердің бірнеше сипаттамасы бар:

- Трафик тыңдалудан қорғанысты қамтамасыз ету үшін шифрланады.
- Жойылған сайт сәйкестендірілуі іске асады.
- Виртуалдық жеке желілер бірнеше хаттамалардың қолдауларын қамтамасыздандырады.
- Қосылу тек екі абоненттің арасында байланыспен қамтамасыздандырады.

SSH сонымен қатар HTTPS бірнеше хаттаманы қолдай алмайтын болғандықтан, нақты виртуалды жеке желіге қатысты болып келеді. VPN-

пакеті ғаламторда әдеттегі трафиктың ағыны бойынша қосылады сонымен қатар бұл трафиктың қосылу нүктесі шықпаласымен есептелуіне қарай қолданыста болады.

Виртуалдық жеке желі түрлі хаттаманың қолдауымен,және қолданбалы деңгейде қамтамасыздандырады. Мәселен, алыстатылған пайдаланушы SMTP хаттамасын бір мезетте файлдық сервер арқылы қосылу үшін NetBIOS қолдану арқылы пошталы сервер мен байланыс жасау үшін қолданылады. Екі айтылған хаттамалар 1.1-суретте көрсетілген бойынша бірдей байланыс циклімен немесе VPN арнасымен жұмыс жасай алады.



Сурет 1.1 - Виртуалды жеке желілердің хаттамалары

VPN 2 нақты нысандарды қосады, сонымен қатар солайша екі абоненттің арасында бір арнаны түзеді. VPN әр шықпалы нүктелері басқа шықпалы нүктесі бар бірнеше VPN қосылыстарын қолдай алады, бірақ нүктелердің әрбірі басқаларымен салыстырғанда бөлек болып келеді, сонымен қатар трафик шифрлау бойынша бөлінеді [6].

Виртуалды жеке желі ережелерге сай болып келеді, және екіге бөлінеді: пайдаланушылық VPN, тораптық VPN. Екеуінің арасындағы басты айырмашылық әрбір трафикті бөлу әдісі емес, пайдалану әдісінде болып табылады.

1.5 VPN фукнциясының стандарттық технологиялары түсінігі

VPN желісінің негізгі құрамдас бөліктері:

- VPN серверлері.
- Шифрлаудың алгоритмі.

- Сәйкестендіру жүйелері.
- VPN хаттама.

Дипломдық жұмыста VPN технологиясын пайдаланып телекоммуникация жүйесінде мәліметті қорғау мәселесі қарастырылған. Мұндай компоненттер қауіпсіздік, өнімділік және өзара іс-қимыл жасау қабілетіне сәйкестігін жүзеге асырады. VPN архитектурасының қаншалықты дұрыс іске асырылғанына байланысты талаптарды анықтаудың дұрыстығына байланысты болады.

Жүйені әзірлеу кезінде сапардағы қызметкерлердің орналасқан жеріне байланысты қосымша талаптарды (өзге ұйымдағы немесе қонақ үй нөміріндегі тораптарды) ескеру, сондай-ақ VPN арқылы жұмыс жасайтын қызметтің түрлерін ескеру өте маңызды болып табылады.

2 Виртуалды жеке желілерді анықтау

Біз ұйымға құпия деректерді ғаламтор арқылы жалға берілетін байланыс арналарын пайдаланбай және трафик құпиялылығы үшін мүмкін болатын барлық шараларды пайдалана отырып беруге тырысамыз. Біз өз трафигін басқа жаһандық желі пайдаланушыларының трафигінен қалай ажыратамыз? Бұл сұраққа жауап шифрлау болып есептелінеді.

Ғаламторда кез-келген түрдегі трафикті табааламыз. Бұл трафиктің көпшілігі ашық түрде таралады және бұл трафикті бақылайтын әр пайдаланушы оны тануы мүмкін. Бұл пошта және веб-трафиктерге, сондай-ақ telnet және FTP хаттамалары арқылы байланыс арналарына жатады. Secure Shell (SSH) сонымен қатар Hypertext Transfer Protocol Secure (HTTPS) трафигі шифрланған трафик болып есептелінеді және пакетті бақылайтын пайдаланушыны көре алмайды. Сондай-ақ, SSH және HTTPS трафигі VPN желісінің виртуалды бөлігін жасамайды.

Виртуалдық жеке желілердің бірнеше сипаттамалары бар:

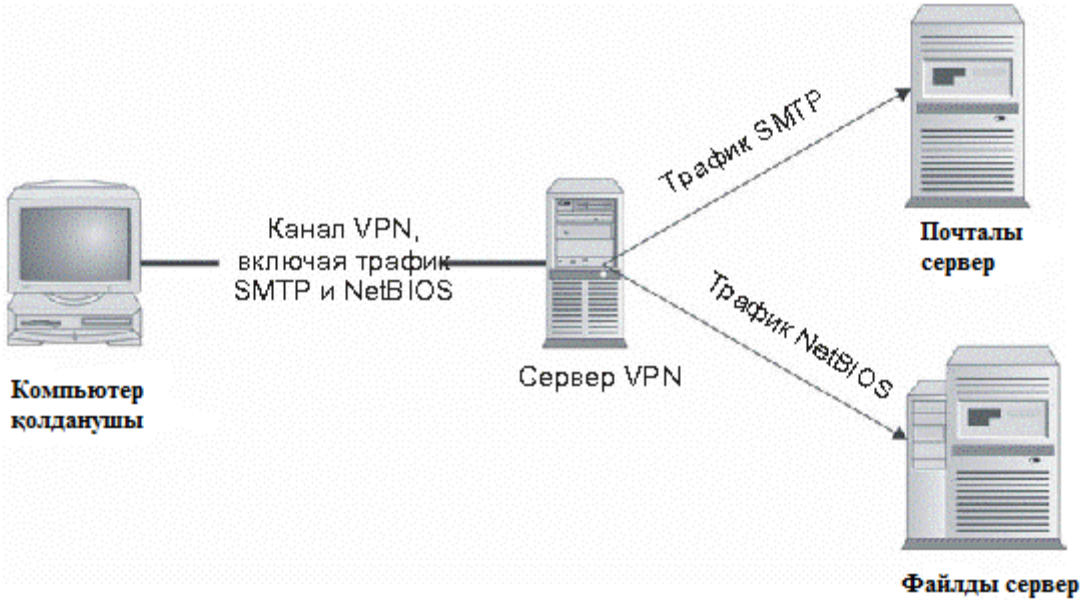
- Трафикті тыңдаудан қорғауды қамтамасыз ету үшін шифрланады.
- Қашықтағы сайтты сәйкестендіру жүзеге асырылады.
- Виртуалдық жеке желілер көптеген хаттамаларды қолдауды қамтамасыз етеді.
- Қосылу тек 2 нақты абоненттің арасында байланыспен қамтамасыздандырады.

SSH және HTTPS бірнеше хаттаманы қолдай алмайды, сол себепті олар белгілі бір виртуалды жеке желіге қолданылады. VPN-пакеттер интернеттегі әдеттегі трафиктың ағынына қосылады және трафиктың қосылу нүктесінің шығысы бойынша есептеледі.

VPN әр сипаттамасын нақты сипаттамаларын қарастырайық. Жоғарыда айтылғандай, VPN трафигі тыңдаудан қорғау үшін шифрланады. Шифрлау өзектілігі жойылғанға дейін берілетін ақпараттың құпиялылығын сақтауға жеткілікті қуатты болуы тиіс. Пароль 30 күнге әрекет ету уақытына ие (парольдерді өзгерту саясаты әр бір 30 күн сайын қарастырылды); бірақ парольдер көптеген уақыт бойы өз құндылығын ешқашан жоғалтпайды. Осыған сай шифрлеу алгоритмі сонымен қатар VPN-ды бірнеше жыл бойы пайдалану трафикті рұқсатсыз шифрлеудің алдын алады.

Екінші сипаттама қашықтағы сайтты сәйкестендіруді жүзеге асырумен сипатталады. Осы сипаттама орталық серверде бірнеше пайдаланушыларды сәйкестендіруді немесе VPN қосатын 2 тораптарды сәйкестендіруді талап етеді. Қолданылатын сәйкестендіру тетігі саясатпен бақыланады. Саясат пайдаланушыларды екі параметрі бойынша немесе динамикалы парольдерді пайдалана отырып сәйкестендіруді көздеуі мүмкін. Өзара сәйкестендіру кезінде екі сайтта да ортақ құпияларды ұсыну талап етіледі (құпия ретінде екі сайтқа бұрыннан анық ақпарат алынады) немесе сандық сертификаттар талап етіледі.

Виртуалдық жеке желі әр түрлі хаттаманы, әсіресе қолданбалы деңгейлі хаттамаларды қолдауды қамтамасыз етеді. Мысалы, қашықтағы пайдаланушы файлдық сервермен бір уақытта қосылуы үшін NetBIOS арқылы пошта серверімен байланыс үшін SMTP хаттамасын пайдаланады. Көрсетілген екі хаттама 2.1-суреттегідей бірдей байланыс циклімен немесе VPN арнасымен жұмыс істеуге болады.



Сурет 2.1 - Виртуалды жеке желілер көптеген хаттамаларға ие

VPN екі нысандарды біріктіреді, сонымен қатар ол арқылы екі абоненттің арасындабір арнаны орнатады. VPN әр шықпалы нүктесі екінші шықпалы нүктесі бар көптеген VPN қосылыстарын қолдай алады, бірақ нүктенің әрқайсысы басқасымен салыстырғанда бөлек болып келеді, және трафиктер шифрлаумен бөлінеді.

Виртуалды жеке желілер әдетте екі түрге бөлінеді: VPN пайдаланушысы және торапты VPN. Желідегі трафикті бөлудің әрбір тәсілінде, олардың арасындағы айырмашылықты әдістерде пайдалану көзделеді.

2.1 Пайдаланушылық виртуалды жеке желілерді анықтау

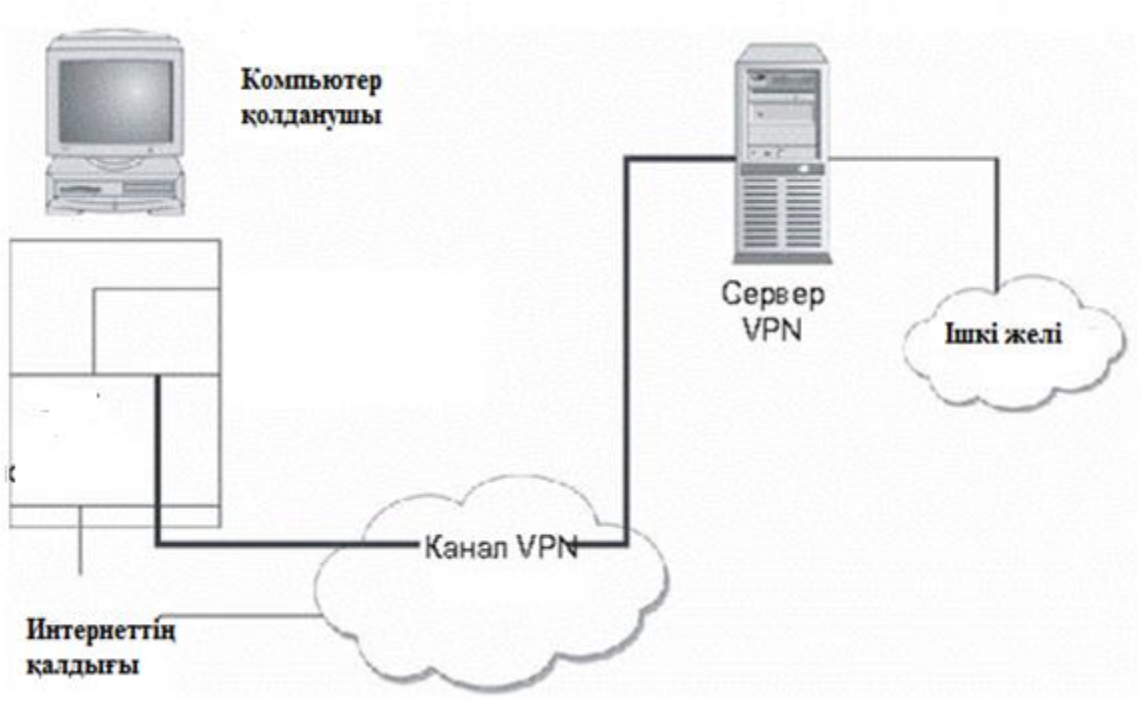
Пайдаланушы VPN жеке қолдану жүйесі мен желі немесе ұйым торабы арасында құрылған виртуалдық жеке желілерді көрсетеді. Көптеген жағдайларда пайдаланушы VPN жолға шыққанда немесе үйде жұмыс істейтін қызметкерлер пайдаланады. VPN сервер ұйымның желіаралық экран немесе жеке VPN сервері болуы мүмкін. Пайдаланушы жергілікті қызмет жеткізушілеріне телефон арқылы, DSL арнасы немесе кабельдік модем

арқылы интернетке қосылады және ұйымның VPN-байланысын интернет арқылы анықтайды.

Ұйымның торабы пайдаланушы көмегімен сәйкестендіру деректерін сұратады, егер сәйкестендіру сәтті орындалса, пайдаланушыға ұйымның ішкі желісіне қатынауды іске асыруға мүмкіндік тудырады, өйткені пайдаланушы желі ішінде және іс жүзінде желі ішінде болады. Желілік байланыс жылдамдығы пайдаланушының интернетке қосылу жылдамдығымен шектелуі мүмкін.

Қолданушылық VPN ұйымға қашықтағы пайдаланушылардың жүйемен файлға кіруін шектеуге мүмкіндік жасайды. Бұл шектеу ұйым саясатына негізделуі тиіс және VPN өнімінің мүмкіндігіне тығыз байланысты.

Бұл кезде пайдаланушы VPN-ұйымның ішкі желісімен байланысы бар, ол сондай-ақ интернетке қосыла алады немесе әдеттегі интернет пайдаланушысы сияқты басқа функцияларды орындай алады. VPN желісі 2.2 суретте көрсетілген бойынша, пайдаланушының компьютеріндегі басқа да жеке қолданбаларды қолдайды.



Сурет 2.2 - Пайдаланушылық VPN баптаулары

2.2 Пайдаланушылық VPN артықшылықтары

Пайдаланушы VPN екі маңызды артықшылықтары бар:

- Сапарда жүрген қызметкерлер серверлермен қосылу үшін жоғары бағамен қалааралық және халықаралық телефон қоңырауларын қажетсіз кез келген мезетте электрондық пошта, файлдар және кіші жүйеге қол жеткізе алады.

- Үйде жұмыс істейтін қызметкер жоғары бағаның бөлінген арналарын жалға алмай, ұйым қызметкерлері сияқты желі қызметтеріне қол жеткізе алады.

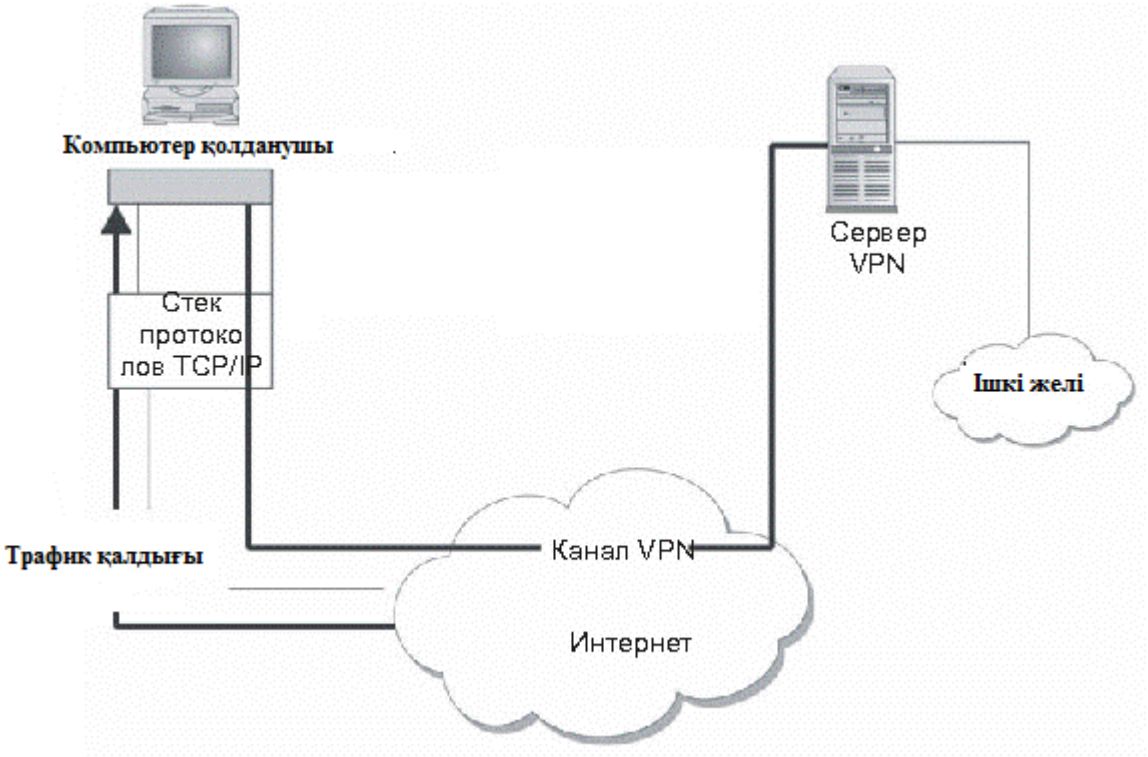
Бұл екі артықшылық ақша үнемдеу санына жазылуы мүмкін. Үнемдеу халықаралық және қалааралық қосылыстарды, жалға алынған байланыс арналарын қолданудан бас тартумен немесе қызметкердің кіріс телефон қоңырауын қабылдайтын серверлердің әкімшіліктік міндетін орындауымен өзара байланысты. Үй пайдаланушыларында DSL немесе кабельді модемді пайдалану 56 Кбит/с жылдамдықпен телефон байланысын пайдаланған кезде қол жетімді болуы мүмкін. Бірнеше қонақ үй нөмірі желіге қосылу мүмкіндігімен жабдықталады, сол үшін іссапарға жіберілетін пайдаланушылар үшін желіге қосылатын жоғары жылдамдықты қолжетімділіктің барлық шарттары жасалады.

2.3 Пайдаланушылық VPN байланысты мәселелер

VPN пайдаланушылық қолдану ұйымның шығынын азайтуы мүмкін, бірақ VPN пайдаланушылық барлық мүмкін проблемаларды шешу болып табылмайды. Оларды пайдалану кезінде қауіпсіздікпен, іске асыру мәселелерімен байланысты елеулі қауіп туындайды, оларды ескеру керек.

VPN пайдаланғанда, пайдаланушы пайдаланатын ең үлкен қауіпсіздік мәселесі интернеттің барлық басқа сайттармен байланысын қарастырады. Ережеге сәйкес, VPN бағдарламалық жасақтамасы пайдаланушының компьютеріндегі трафик vpn бойынша таралуы мүмкін немесе оны басқа сайтқа ашық түрде жіберу қажет екенін анықтайды. Егер пайдаланушының компьютерінде "үш есімді" пайдалану арқылы шабуыл жасалса, онда кез келген сыртқы рұқсатсыз пайдаланушы қызметкердің компьютерін ұйымның ішкі желісіне қосу үшін пайдаланады, ол 2.3-суретте бейнеленген. Бұл түрдегі шабуылдар өте қиын, бірақ нақты болады.

VPN пайдаланушы басқаратын, сонымен қатар ішкі жүйемен байланысты мәселелерді қажет етеді. Кейбір кезде VPN қолданушылары пайдаланушы идентификаторларына немесе Windows NT немесе Windows 2000 доменіндегі пайдаланушы басқарудың орталықтандырылған жүйесіне байланысты. Бұл функция пайдаланушыны басқаруды оңтайлы етеді, бірақ әкімшіге бұрынғыдай мұқият сақтау және қашықтан VPN-қол жеткізу қандай пайдаланушыларға қажет екенін бақылау қажет.



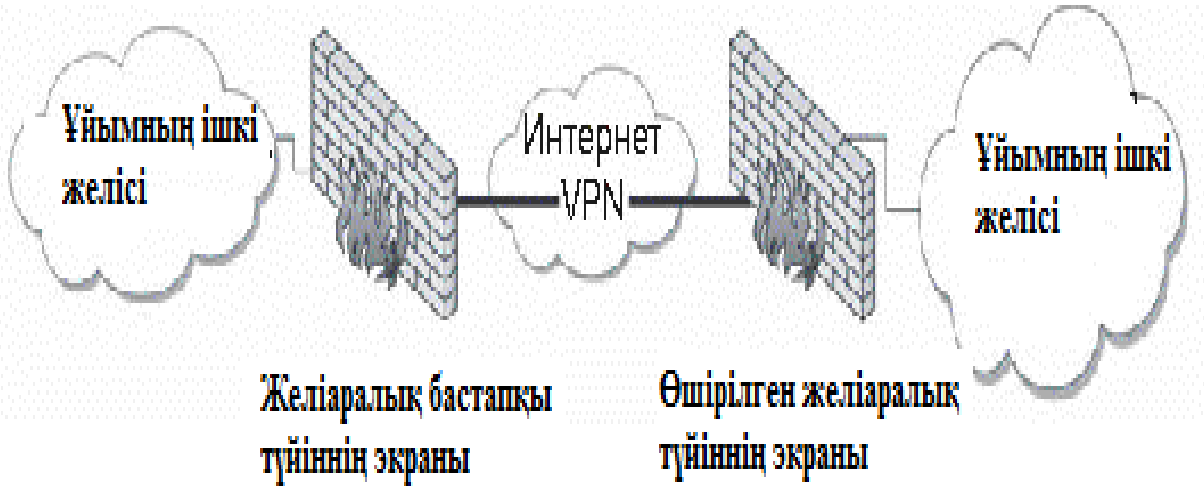
Сурет 2.3 - Ұйымның ішкі желісіне кіру үшін «троя атын» пайдалану

2.4 VPN тораптық желілерін анықтау

Тораптық жеке желілер қашықтағы тораптарға қосу немесе жоғары бағалаудың нақты арналарын қолданбай, ұйым қызметіне қатысты ақпарат алмасуды жүзеге асыру үшін қажетті екі түрлі ұйымдар арасында қосылуды жүзеге асырады. Әдетте, VPN бір желі аралық экран немесе 2.4 суретте көрсетілгендей шекаралы бағдарды басқа балама құрылғымен қосады.

Қосылысты анықтауға бір торап трафикті өзге торапқа таратуды жүзеге асырады. Нәтижесінде VPN қосылымының қарама-қарсы екі түйінінде VPN болады. Екі шығыс тораптарын қосу параметрлері тораптардың түріне байланысты анықталады. Екі сайт да бір-бірін құпиялық ортамен немесе ашық кілт сертификатымен сәйкестендіреді. Кейбір ұйымдар VPN желісін жалға алынған арналар үшін қосымша арналар ретінде пайдаланады.

Осы баптаумен жұмыс істегенде бағдардың дұрыс құрылуын қамтамасыздандыру қажет. Сондай ақ, VPN үшін пайдаланылатын физикалық байланыс арналары міндетті түрде жалға алынған қосылыстардан ерекшеленуі тиіс. Физикалық байланыс арнасы екі бірдей қосылу арқылы жүзеге асырылуы мүмкін, соның нәтижесінде артықшылықтың керекті деңгейі қамтамасыз етілмейді.



Сурет 2.4 - Ғаламтор арқылы өтетін VPN торап аралық қосылысы

2.5 Тораптық VPN артықшылықтары

Пайдаланушы VPN сияқты, торапты VPN негізгі артықшылығы үнемді пайдалану болып табылады. Бір-бірінен алыс шағын ұйымдар бір-бірімен қашықтағы екі кеңсені біріктіретін жеке виртуалды желі құрады. Оларды пайдалану кезінде қауіпсіздікпен, есептеу үшін қажетті іске асыру мәселелерімен байланысты қауіп туындайды.

Пайдаланушы VPN пайдаланушыларның жүйелер мен файлдарға кіруін шектейді. Бұл шектеу ұйым саясатына негізделуі тиіс және VPN өнімінің мүмкіндігіне байланысты болып келеді.

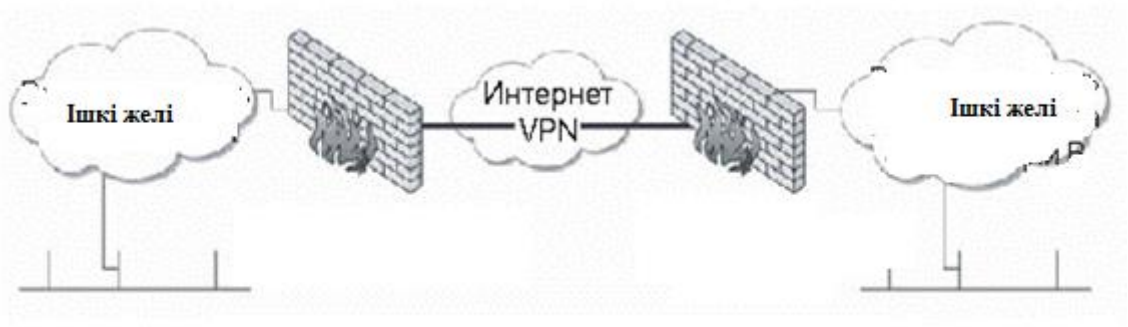
2.6 Тораптық VPN байланысты мәселелер

Торапты VPN жаңа алыстатылған тораптарды не тіпті алыстатылған ұйымды қосу көмегімен ұйым қауіпсіздік периметрін ұлғайтады. Егер қашықтағы тораптың қауіпсіздігінің деңгейі аз болса, VPN сыншыл ойлаушыға орталық тораптарға қол жеткізуге және ұйымның басқа да ішкі жүйесіне қол жеткізуге мүмкіндік жасайды. Осыған сай ұйымдарның толықтай қауіпсіздігі үшін қатаң саясатты қолдану және аудит функцияларын жүзеге асыру қажет. Қолданылатын желіде VPN

бағдарламалық қамтамасыз ету трафик VPN көмегімен таратылуы немесе басқа сайтқа ашық түрде жіберілуі тиіс екенін анықтайды.

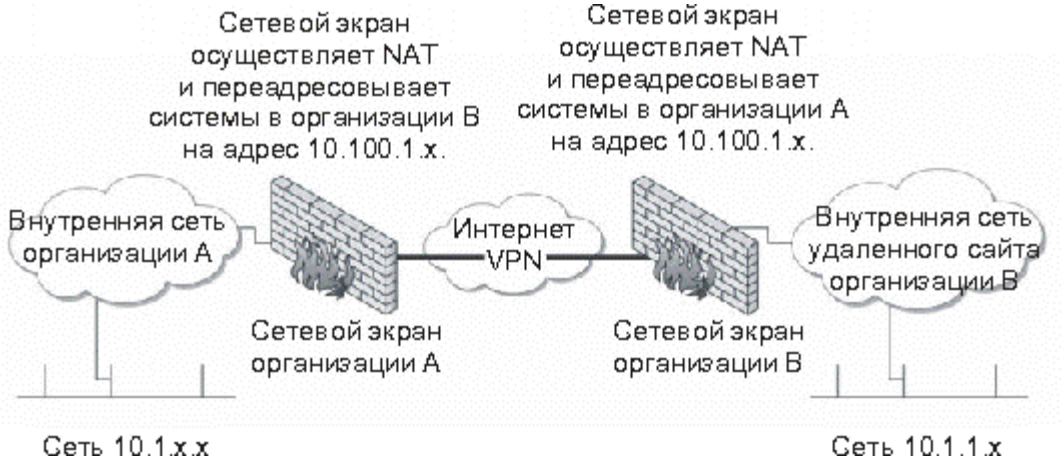
Тораптық VPN идентификациясы қауіпсіздікті қамтамасыз етудің маңызды шарты болып табылады. Әртүрлі өндірушілер өнімді сатуды шектеу, аспекті, лицензиялау және бағдарлама бойынша ұсыныстарды шектеу сияқты мәселелерге байланысты түрлі алгоритмдер бойынша ұсыныстарды қарастырады. Пайдаланушылық VPN ұқсас VPN-сервері VPN-трафикті шифрлеуді және дешифрлеуді жүзеге асыруы тиіс. Егер трафик деңгейі үлкен болса, VPN сервері жүктеледі. Көптеген жағдайларда бұл желіаралық экран VPN сервері болған кезде кездеседі.

Адресацияға байланысты мәселені ойластыру керек. Бұл жағдайда, егер сіз тораптық VPN ұйым ішінде пайдалансаңыз, онда барлық тораптарды адрестеу схемасы қажет. Бұл кезде адресация қандай да қиындықтар әкеледі. Егер VPN екі түрлі ұйымдарды қосу үшін қолданса, онда адресацияға қатысты барлық келіспеушіліктер туралы шешім қабылдау керек. 2.5 суретте туындаған даулы жағдай бейнеленді. Бұл ретте екі ұйым бірдей мекенжай кеңістігін пайдаланады (10.1.1.X желі).



Сурет 2.5 - Тораптық VPN адрестелумен байланысты келіспеушіліктерді тудыруы мүмкін

Бір-бірімен адрестеу схемасы келіспеушілік болатыны белілі, бағдарлану жұмыс жасамайды. Бұл кезде VPN-ның әрбір жағы желілік мекенжайды жіберуді және басқа ұйымдардың жүйесін өзінің жеке адресация сұлбасына бағыттауды орындауы тиіс, ол 2.6 суретте сипатталған.



Сурет 2.6 – Тораптық VPN адрестелу келіспеушіліктерінің алдын алу үшін NAT пайдаланады

2.6.1 VPN фукнциясының стандарттық технологиялары түсінігі

VPNжелісінің төртмаңыздықұрамдас бөліктері:

- VPN сервер.
- Шифрлаудың алгоритмі.
- Сәйкестендіру жүйелері.
- VPN хаттама.

Аталған құрамдас бөліктер қауіпсіздік бойынша талаптар, өнімділік және өзара әрекеттесік қабілеттілігі бойынша сәйкестікті жүзеге асырады. VPN архитектурасы қаншалықты дұрыс жүзеге асырылғаны талаптардың дұрыс анықталуына байланысты болады.

Талаптарды анықтау мынадай аспектілерден тұруы тиіс.

- Ақпаратты қорғауды қамтамасыз ету үшін қажетті уақыт саны.
- Пайдаланушылардың бір мезгілдегі қосылыстар саны.
- Пайдаланушыларды қосудың күтілетін түрі (үйде немесе сапарда жұмыс істейтін қызметкерлер).
- Қашықтағы серверлік қосылыстар саны.
- Қосылу қажет болатын VPN желісінің түрі.
- Қашықтағы тораптардағы кіріс және шығыс трафигінің күтілетін көлемі.
- Қауіпсіздік параметрлерін анықтайтын қауіпсіздіктің саясаты.

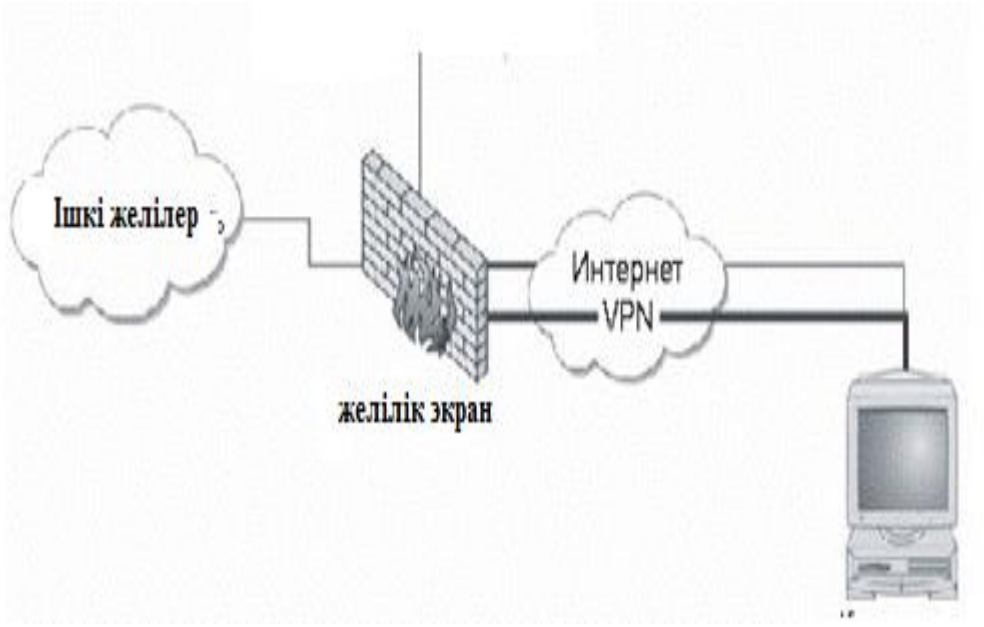
Олардың негізінде көптеген жұмыс принциптері бар, бірақ дұрыс баптағанда құралдың екі түрі шектеулі трафикті бұғаттаумен сипатталатын қауіпсіздіктің қызметінің дұрыс болуын қамтамасыздандырады.

2.7 VPN сервері

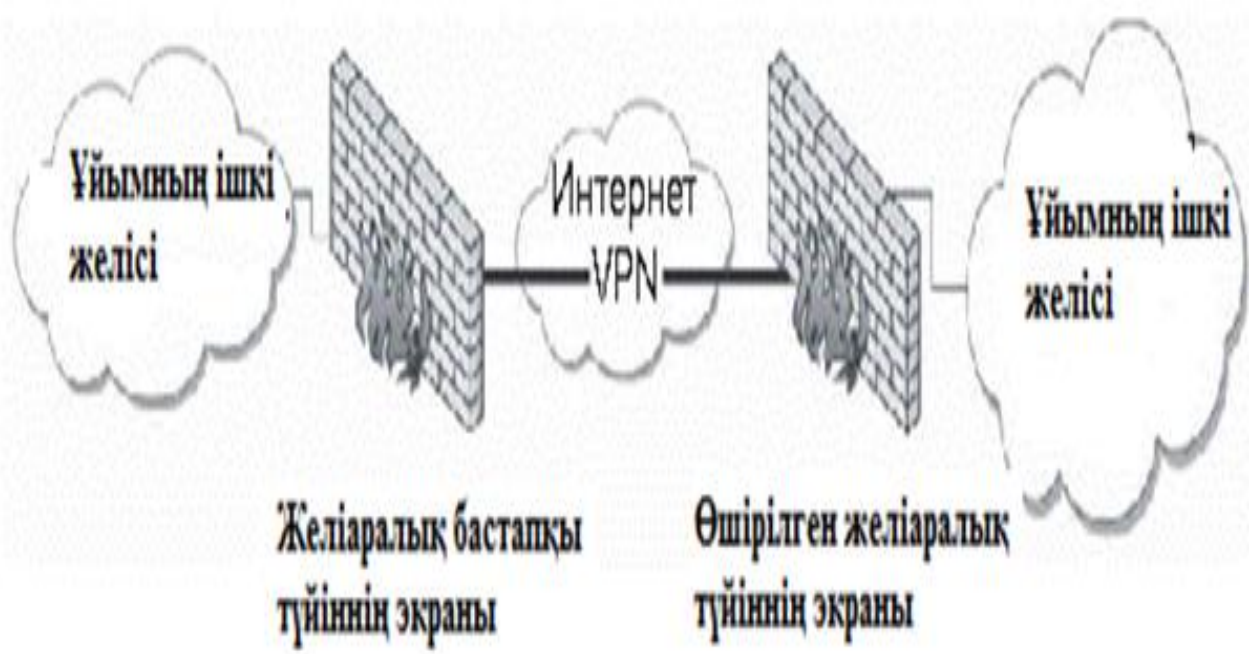
VPN сервері VPN шығыс байланыс торабының рөлінде берілетін компьютер ретінде сипатталады. Бұл сервердің күтілетін жүктемені қолдау үшін жеткілікті сипаттамалары болуы тиіс. Көптеген VPN бағдарламалық жасақтама өндірушілері VPN-қосылыстар санына қарамастан процессордың өнімділігі мен жадыны баптау туралы нұсқаулықты ұсынуы тиіс.

Күтілетін жүктемені қамтамасыз ету үшін көптеген VPN серверлерін құру керек болуы мүмкін. Бұл кезде күтілетін VPN қосылымы жүйе ішіндеаз уақыт ішіндетаралуы тиіс.

VPN-сервері желіде орналасады. Ол 2.7-суретте бейнеленгендей желіаралық экран не шекаралық бағдарлауыш та болуы мүмкін. Балама ретінде сервер жеке жүйе ретінде қарастырылуы мүмкін. Мұндай жағдайда сервер 2.8 суретте көрсетілген белгілеген демилитаризацияланған жерде (DMZ) орналасуы тиіс. Нақтырақ айтсақVPN демилитаризацияланған аймақ тек VPN серверінен тұруы тиіс және DMZ интернеттен жойылуы тиіс. Бұл VPN-сервері авторизацияланған пайдаланушыға ішкі жүйеге қолжетімділікті ұсынып, тиісінше, сенімді пайдаланбайтын адамдар арасында ғана орын алатын жоғары сенімділік объектісі ретінде қарастырылуы тиіс. Желіаралық экран және VPN трафик ережелері, таралу аймағы және милитаризацияланған қызметкерлер тек қана жиынтықтармен қорғалады.



Сурет 2.7 - Желіаралық экран VPN-сервер болып табылатын VPN желісінің архитектурасы



Сурет 2.8 - Жеке VPN сервері үшін VPN желісінің архитектурасы

2.8 Шифрлау алгоритмі

VPN қолданатын шифрлаудың алгоритмі стандартты ең қуатты шифрлау алгоритмі болуы тиіс. Негізінен VPN құру кезінде барлық стандартты қуатты алгоритимдер тиімді қолданылады. Әр түрлі өндіруші компаниялар өнімді сатуды шектеумен, аспектілер, лицензиялау және бағдарлама бойынша ұсыныстышектеуге байланысты әр түрлі алгоритмдерге ұсыныстарды қарастырады. VPN программалық пакетін алып, маманның пікірін тыңдау керек сонымен қатар өндірушілер шифрлеудің қуатты алгоритмдерін қолданады.

Қате іске асырылған жүйе шифрлаудың ең қуатты алгоритмін пайдасыз ете алады. VPN көмегіменберілетін ақпаратқа қол жеткізу үшін қастықойлау міндеттері:

– барлық қосылу сеанстарын қамту, яғни тыңдау құрылғысы барлық VPN трафигімен берілуі тиіс;

– үлкен есептеуіш қуатты және үлкен көлемді уақытты ауыр күш пен трафикті шифрлеу арқылы кілтті алу үшін пайдалану.

2.9 Сәйкестендіру жүйесі

Архитектураның үшінші буыны ретінде VPN сәйкестендіру жүйесі қаралатын болады. VPN сәйкестендіру жүйелері екі фактордан тұрады. Пайдаланушыларды сәйкестендіру олар білетін ақпарат арқылы немесе жеке басын білетін тұлғаны пайдалана отырып жүргізіледі. Пайдаланушы VPN қолданғанда бірінші екі нұсқаға ұсыныс қарастырылуы тиіс.

Сәйкестендіру құралының оң құрылымы түрінде сәйкестендірілген нөмірмен немесе парольмен байланысты смарт-карталар қарастырылады. Бағдарламалық жасақтаманы өндірушілер ұйымдарға ережеге сәйкес таңдалған бірнеше сәйкестендіру жүйелерін ұсынады.

2.10 VPN хаттамасы

VPN хаттамасы, сондай-ақ басқа да ұйымдармен ғаламторда әрекет ететін және жүйенің қорғау деңгейін анықтайды. Егер қарастырылып отырған ұйым VPN-ды тек ішкі деректер алмасуға пайдаланса, өзара іс-қимыл туралы мәселені жауапсіз қалдыра алады. Бірақ, егер де ұйым басқа ұйымдармен байланысқа VPN пайдаланса, онда өз хаттамасын пайдалану мүмкін емес болады. VPN хаттамасы жүйенің жалпы қауіпсіздігінің деңгейіне ықпалын көрсетеді. Бұл VPN протоколы екі шығыс түйіндерінің арасында шифрлау кілтімен алмасуға қолданылады. Егер бұл тарату қорғалған болмаса, онда қолтық асты кілтін алуға және VPN барлық артықшылығы бар трафик оқуға болады.

Қосылған кезде стандартты хаттамаларды пайдалану ұсынады. Қазіргі кезде IPSec VPN үшін стандартты хаттама болып есептелінеді.

2.11 IPSec хаттамалары. AH, ESP И IKE арқылы қорғалған арнаны ұйымдастыру

InternetProtocolSecurity (IPSec) стандартында Internet-жүйе деп аталады. Шын мәнінде, IPSec-қазіргі кезде толық ядросы бар ашық стандарттардың біріккен жиынтығы, және ол жаңа хаттамалармен, алгоритмдермен және функциялармен айтарлықтай оңай толықтырылуы мүмкін.

IPSec хаттамасының негізгі мақсаты — IP желілері бойынша деректерді қауіпсіз беруді қамтамасыз ету. IPSec пайдалануға мүмкіндік береді:

- тұтастық, яғни деректерді таратқанда сығылған, жойылған немесе ауыстырылған болмауы тиіс;
- сәйкестік, яғни деректер жіберушіге берілетін болады, ол кім екенін растайды;
- құпиялылық, яғни ақпарат рұқсат етілмеген ұсыныстың алдын алу түрінде жіберіледі.

(Классикалық анықтамаға сәйкес, деректер қауіпсіздік түсінігі тағы талап–қарастырылып отырған контексте оларды жеткізу кепілдігі ретінде қарастырылуы мүмкін деректердің қол жетімділігін анықтайды. IPSec хаттамасы TCP транспортты деңгей хаттамасын қалдырып, бұл міндетті орындай алмайды).

2.12 Әртүрлі деңгейдегі қорғалған арналар

IPSec жалпы қол жетімді (қорғалмаған) желі бойынша деректерді берудің ең кең тараған және ең қауіпсіз технологияларының бірі болып табылады. Бұл технология үшін ортақ ат-қорғалған арна (secure channel) қолданылады. «Арна» термині деректерді қорғау желінің екі торабы (хост пен шлюз) арасында бірнеше виртуалды желілер бойынша желіге қосылған пакеттерді коммутациялаумен қамтамасыз етіледі.

<table>
<tr><td rowspan="6">Қорғалған қолжетімділік хаттамалары</td><td>Қолданбалы</td><td rowspan="3">Қосымшаларға әсер етеді, желілік технологияға тәуелді емес</td></tr>
<tr><td>Көріністік</td></tr>
<tr><td>Сеанстық</td></tr>
<tr><td>Транспорттық</td><td></td></tr>
<tr><td>Желілік</td><td rowspan="3">Қосымшалар үшін анық, желілік технологияға тәуелді</td></tr>
<tr><td>Арналық</td></tr>
<tr><td>Табиғи</td></tr>
</table>

Сурет 2.9 - Қорғалған арнаның хаттамалар деңгейі

2.9-суретте қорғалған арна көрсетілген OSI моделінің әртүрлі деңгейінде іске асырылған жүйелі құралдармен құруға болады. Егер қызметтерді қорғау үшін жоғары деңгейдегі (қолданбалы, көріністік не сеанстық) сипаттамалар пайдаланылса, онда қандай қорғаныс әдісі (IP немесе IPX, Ethernet немесе ATM) деректерді тарату үшін пайдалануға байланысты емес, ол бір жағынан, ал жойылған қосымшалар осы уақытта нақты қорғаныс хаттамасына тәуелді, яғни қосымшалар үшін мұндай хаттамалар айқын болып саналмайды.

Арнаның қорғалу деңгейі пайдалану үшін пайдаланылғанына байланысты, ол шектеулі әрекет аймағы бар. Хаттама тек толық белгілі бір қызметті-файлдық, гипермәтіндік немесе пошта қызметін қорғайды. Мысалы, S/MIME ХАТТАМАСЫ тек электрондық пошта хабарын қорғайды. Сондықтан әр бір қызметке хаттаманың тиісті нұсқасын дайындау керек.

Secure Socket Layer (SSL) сонымен қатар оның жаңа ашық іске асырушысы Transport Layer Security (TLS) басқа деңгейде жұмыс істейтін, қорғаныс арналарының аса танымал хаттама болды. Хаттама деңгейін төмендету оны әмбебап қорғаныс құралы етеді. Енді кез келген қосымшалар,

қолданбалы деңгейдегі хаттамалар, кез келген және бірыңғай қорғаныс хаттамаларын пайдалану. Алайда, қолданба бұрынғысынша жазылуға тиіс – оларда қорғалған арна протоколының функциялары анық қоңыраулары орнатылуы тиіс.

Арнаның қорғау құралдары төмен іске асса, оларды қосымша мен қосымша хаттамаға мөлдірлету қиын емес. Желілік сонымен қатар арналық деңгейде қорғау хаттамасынан қосымша тәуелділігі толық жойылады. Алайдамұнда біз нақты желілік технологиялардан қорғау хаттамасы тәуелділігі басқа мәселемен қақтығысамыз. Шынымен, ірі құрамды желі әрі бөлігінде, жалпы айтқанда, әртүрлі арналы хаттамапайдаланылады, сол үшін арналық деңгей бірыңғай хаттама арқылыбұл гетерогенді ортаға қорғалған арнаны орындау мүмкін емес.

Мысалы, арналы деңгейде жұмыс істейтін қорғалған Point-to-Point Tunneling Protocol (PPTP) арнасының протоколын қарастырайық. Ол "нүкте-нүкте" байланысты кеңінен пайдаланатын PPP стандарттарында негізделген, мысалы, айтылған желілермен жұмыс істеу кезінде.

PPTP хаттама қолданбалы деңгейдің қызметі және жүргізу үшін қорғаныс құралдары мөлдірлігін қамтамасыздандырмай, сондай ақ желілік деңгей қабылданатын хаттамаға тәуелді болмайды: көбіне, PPTP хаттама IPX, DECnet не NetBEUI хаттамасының негізінде жұмыс істейтін, желіде және IP желісінде пакеттітарата алады. Бірақ, PPP барлық желіде пайдаланбайтындықтан (көптеген жергілікті желілер арналық деңгейде Ethernet протоколы жұмыс істейді, ал жаһандық - ATM, frame relay протоколдары), онда PPTP әмбебап құрылғы болып саналмайды.

Желілік деңгейде жұмыс істейтін IPSec хаттама ымыралы болып есептелінеді. Бір жағынан, ол қолданба үшін мөлдір, ал екінші жағынан-ол барлық желіде жұмыс істей алады, өйткені ол кең тараған IP протоколына негізделген: қазіргі кезде әлемдегі компьютерлердің тек 1% - ы IP-ді қолдамайды, тұтастай алғанда, қалған 99% оны жалғыз хаттама ретінде немесе бірнеше хаттамалардың бірі ретінде пайдаланады.

2.13 IPSec хаттамалары арасында функциялардың таралуы

IPSec ядро 3 хаттамадан құрылады: идентификация хаттамасы (Authenti-cation Header, AH), шифрлаудың хаттамасы (Encapsulation Security Payload, ESP) және кілттерді алмасу хаттамасы (Internet Key Exchange, IKE). Қорғалған арна қолдау функциялары келесі хаттама арасында қолданылады:

- AH хаттамасы сәйкес деректердің толықтығына кепілдік бере алады
- ESP хаттамасы құпиялыққа кепілдік беріп, берілетін деректерді шифрлайды, бірақ ол сондай-ақ деректерді сәйкестендіруді және толықтығын қолдай алады;

– IKE хаттамасы деректерді идентификациялау және шифрлау хаттамасының жұмысына керекті құпия кілттер арнасы соңғы нүктесін автоматты түрде ұсынудың қосымша мәселесін шешеді.

Құрылымның қысқаша сипаттамасындағыдай, AH сонымен қатар ESP хаттамасының функциялары біртіндеп жабылады. AH хаттамасы тек деректердің сәйкестендірілуіне және толықтығына ғана жауап береді, ESP хаттамасы қуатты, өйткені деректерді шифрлеуге, сондай-ақ AH хаттамасының функцияларын орындауға болады (бірақ біз байқағанындай, идентификация мен толықтық бірнеше қысқартулармен қамтамасыз етіледі). ESP хаттамасы шифрлау және сәйкестендіру/толық функцияларын кез келген комбинацияларда, яғни функциялардың басқа да топтарын немесе тек шифрлауды қолдай алады.

IPSec деректерін шифрлау үшін құпия кодты қолданатын шифрлеудің кез келген симметриялы алгоритм пайдалануы мүмкін. Шифрлау тәсілдерінің бірінде деректерді толық және сәйкестендіруді қамтамасыз ету үшін – дайджест функция (digest function) немесе хэш функция (hash function) деп аталатын бір бағытты функция (one-way function) арқылы шифрлау.

Шифрланған деректер белгілі бір аз байттан тұратын дайджест-шаманың негізінде беріледі. Дайджест IP-пакеттегі шығыс хаттарымен бірге жіберіледі. Алушы дайджесті қалыптастыру үшін қандай да бір шифрлеудің бағыттаушы функциясы қолданылатынын біле отырып, оны бастапқы хабарламаларды пайдаланып қайта есептейді. Егер алынған және есептелген дайджестердің шамасы сәйкес келсе, онда бұл пакеттің құрамы беру кезінде қандай да бір өзгерістерге ұшырамағанын білдіреді. Бұл дайджест бастапқы хабарламаларды қалпына келтіруге мүмкіндік бермейді, сондықтан қорғау үшін пайдалануға болмайды, бірақ деректердің толықтығын тексеруге мүмкіндік береді.

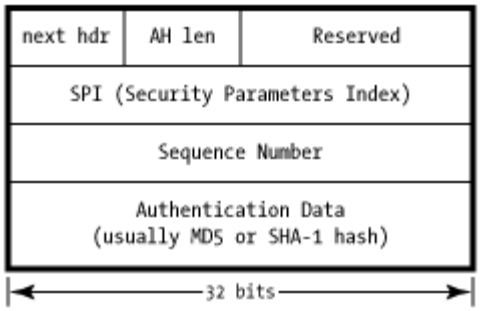
Дайджейст бастапқы хаттарға бақылау сомасы болып табылады. Алайда айтарлықтай айырмашылық бар. Бақылау сомасын пайдалану - бұл сенімсіз байланыс желілері бойынша жіберілетін хаттардың толықтығын тексеру құралы және ол ақыл-ойдың нашар әрекеттерімен күреске бағытталмаған. Негізінен, жіберілетін пакетте бақылау сомасының болуы зиянкестерге бақылау сомасының жаңа мәнін қосып, бастапқы хатты тасымалдауға кедергі келтірмейді. Дейджейсті есептеу кезінде бақылау сомасына қарағанда құпия код пайдаланылады. Егер дейджейсті алу кезінде тек жіберушіге және алушыға белгілі параметрлері бар бір бағытты функция (онда пароль бар) пайдаланса, онда бастапқы хат кез келген модификациясы дереу анықталады.

AH және ESP екі хаттамасы арасында қорғау функцияларын бөлу шифрлау жолымен деректердің құпиялылығын қамтамасыз ету экспорт және/немесе импорт құралдарын шектеуде көптеген елде пайдаланылатын тәжірибеге негізделген. Осы еі хаттамаларының әр қайсысы дербес және басқалармен бір мезгілде пайдаланылуы мүмкін, сондықтан мұндай жағдайларда, яғни шифрлау қолданыста шектеулерден пайдаланылуы мүмкін емес болғандықтан, жүйені тек қана AH хаттамамен қою керек.

Тек АН хаттама арқылыдеректерді қорғау көпжағдайда жеткіліксіз болып кетеді, өйткені бұл кезде қабылдаушы жақ деректер дәл өзі күтелетін түйін арқылы жіберілгеніне, сонымен қатар жібергендежеткендігіне сенімді болып келеді. Рұқсаты жоқ қаралымдардан деректерді қолдану бойынша АН хаттама оларды қорғамайды, себебі оны шифрлемейді. Деректердің шифрленуіне, олардың толықтығыжәне сәйкестендірілгенін тексеретін, ESP хаттамасын пайдалану керек.

2.13.1 АН хаттамасы

Authentication Header (АН) құпиялылықты қамтамасыз ету үшін ғана емес, IP-трафикті сәйкестендіру үшін де қолданылады. Яғни, хаттама деректерін қолдана отырып, біз пакеттің құрамы беру процесінде өзгермегеніне және егер бұл өзгерістер орын алса (көбінесе – пакетті шығару) көз жеткізе аламыз. АН хаттамасының формасы 2.10 суретте бейнеленген.



Сурет 2.10 –АН атауының пішіні

Төменде АН әр өрісінің атауы түсіндірілетін түрі көрсетілген:

nexthdr – пайдалы жүктеменің атауы өрісінен соң болатын ақпаратты сәйкестендіреді

AHlen – АН ұзындық 32-биттік сөздегі атау (2х сөздердің есептелуі RFC 1883 көрсетілген)

Reserverd – болашақтағы қажеттіліктерге кейінге қалған, нөлдік шамаға иелену

Security Parameters Index – SPD бұл байланыстың қауіпсіздігінің параметрлерінің 32-биттік сәйкестендірілуі

SequenceNumber – пакеттің жалғану шабуылын болдырмау үшін қызмет жасайтын, бірқалыпты ұлғаятын шама.

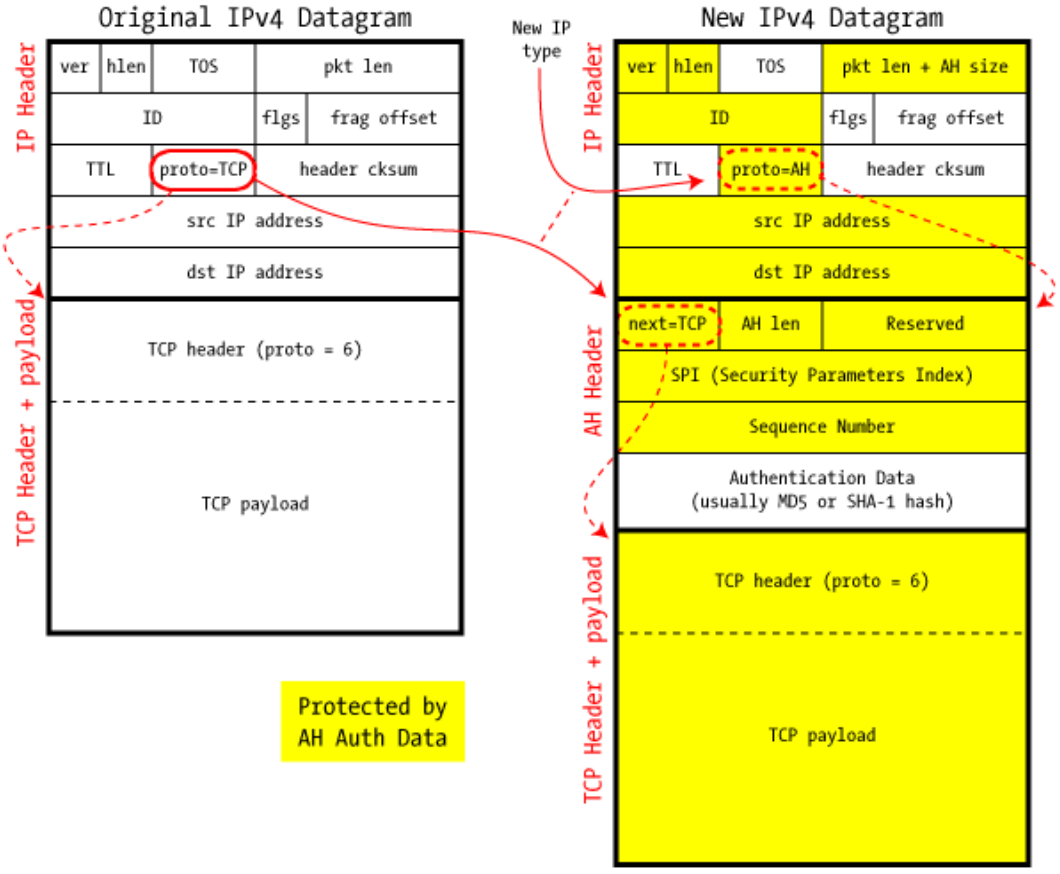
Authentication Data – ICV (Integrity Check Value) – стандартты IP-атауының көптеген өрісін қосатын, пакеттер бойынша саналатын шама.

Алушы бұл пакетті есептейді және де егер шамалар сәйкес болса, пакет сәйкес болып есептелінеді.

Соңғы шама алгоритмін есептеу туралы ол кейінірек айтады. AH протоколын қолданудың екі мүмкін нұсқасы: transport mode (тасымалдау режимі) сонымен қатар tunnel mode (туннель режимі). Олардың бәрінтолық қарастырайық.

2.13.2 Transport mode

Екі пайдаланушы арасындағы байланысты қорғау үшін end-to-end пайдаланады. Бұл режимде IP-пакеті тек жай ғана өзгереді-пайдалы жүктеменің өрісі мен IP арасында, AH аты қойылады:



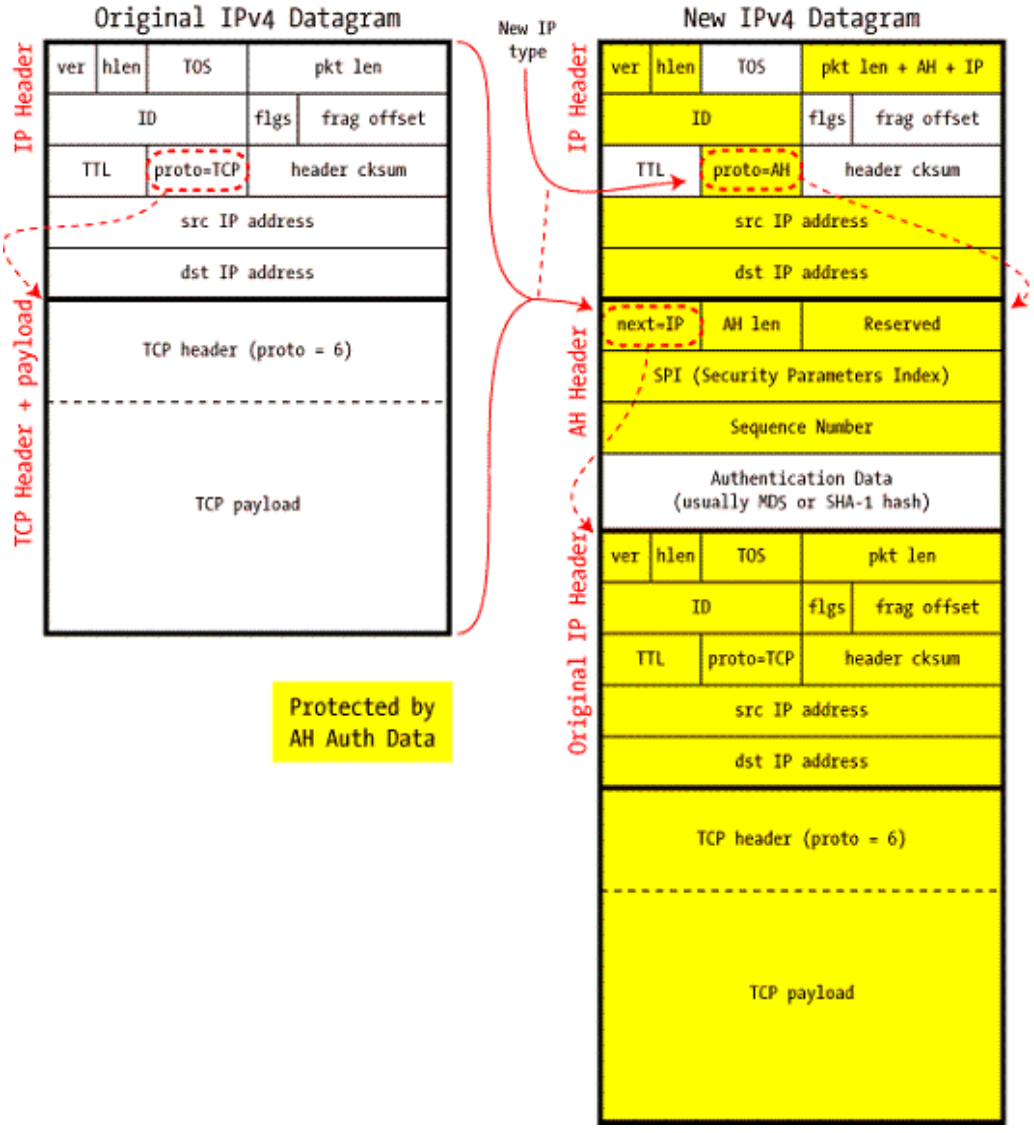
Сурет 2.11 – Тасымалдаушы режімдегі AH

IP-пакетті AH-атауда қосудан басқа protocol өрісі шамасы өзгереді: AH идентификаторы көрсетіледі, ал бұрын сақталған шама nexthdr өрісіне ауыстырылады. Пакетті сәтті сәйкестендірген кезде AH атауын таңдау және хаттама идентификаторын ауыстыру жүргізіледі.

2.11 суретте көрсетілгендей, ICV есептеуінің алгоритмі желіде қолдану жүрісі бойынша рұқсатталғантүрде өзгере алады(мысалы TTL өрісі).

2.13.3 Tunnel mode

Туннельдік режим барлық халыққа таныс виртуалдық жеке желінің (VPN) сервисіне қызмет етуі бойынша жақын, мұндаалғашқы IP-пакеттер толық жаңаға капсуланады және желі арқылы беріледі. Тағайындалудың орнында кері процесс болады. Толық капсулдану IP-адресіне салынған пакетте, сыртта көрсетілгеннен ерекшеленуге мүмкіндік жасайды, сонымен қатар туннель функциясын жүзеге асырады.



Сурет 2.12 – Туннельді режімдегі AH

2.12- суретте көрсетілгендей, туннельдік режимді қолдану IP-пакеттің алғашқы өрісін: сонда тасымалдаушы режимді қолдану кезінде алынып тасталғанды қосып, сәйкестендіруге мүмкіндік тудырады.

Тасымалдаушы режим көбіне екі соңғы пайдаланушылардың арасында байланыс қорғаған ұйым үшін пайдаланады, сол кезде туннельдік режим,

виртуалдық жеке желі сервистерін іске асыруға мүмкіндік жасайды, бағдарлауыштар арасында байланысты ұйымдастыру үшін қолданылады.

3 Сәйкестендіру алгоритмдері

AH атауында, MD5 немесе SHA-1 хэштілеудің стандартты криптографиялық алгоритмдерінің негізінде есептеуге болатын, ICV шамалары болады. Бақылаушы суммаларды тікелей есептеудің алгоритмдерін жүзеге асырудың орнына, бұл жағдайда Hashed Message Authentication Code (HMAC) есептеу амалы қолданылады, ол өзіне құпия кілттердің пайдаланылуын, ICV қайта есептелуімен шабуыл мүмкіндігін болдырмас үшін қолданылады. Бұл жерде тек сәйкестендірудің қысқаша есептеу сұлбасын келтіреміз:

HMAC есептері үшін хэш-функция (оны H ретінде белгілейік) және құпия кілт K қажет болады. H процедураның көмегімен хэштегтеленетін, хэш-функция болып табылады, сәйкесінше бірізді мәліметтер блогында қолданылады. B байттарда осындай блоктардың ұзындығын, ал блоктардың ұзындығын хэштілеу нәтижесінде алынған –L ретінде белгілейміз. Содан кейін, қосымша «құпиялы» шамаларды енгіземіз

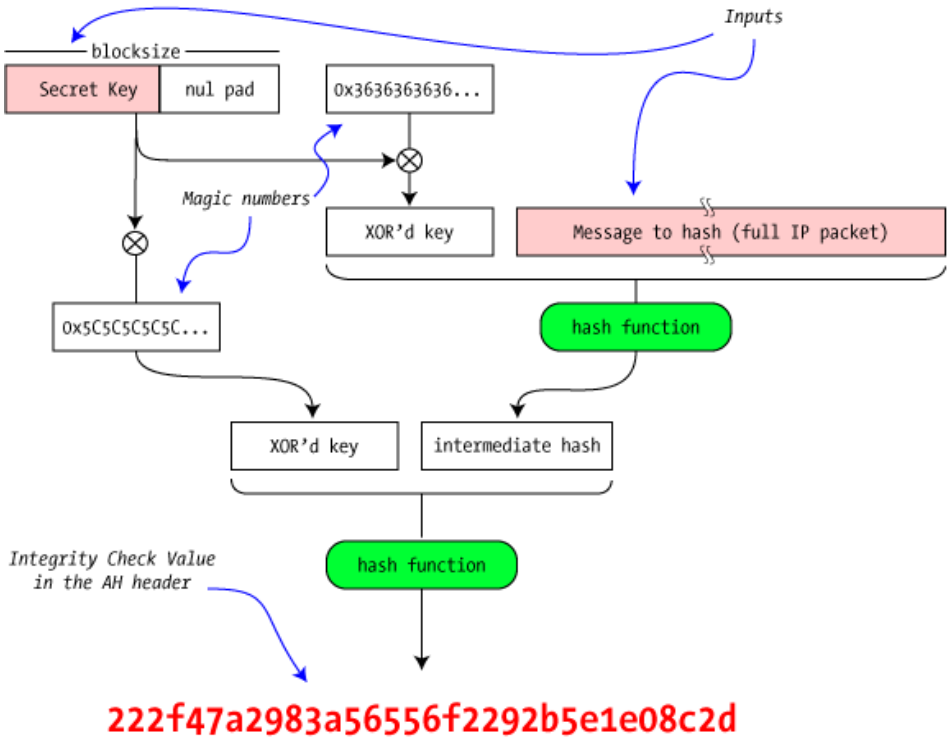
ipad = байт 0x36, B рет қайталанған

opad = байт 0x5C, B рет қайталанған

'text' ретінде көрсетілген, пайдаланушылық мәліметтерден HMAC есетеу үшін келесідей операцияларды орындау керек:

ICV = H (K XOR opad, H (K XOR ipad, text))

ICVесептеудің бұл сұлбасы мына суретте көрсетілген:



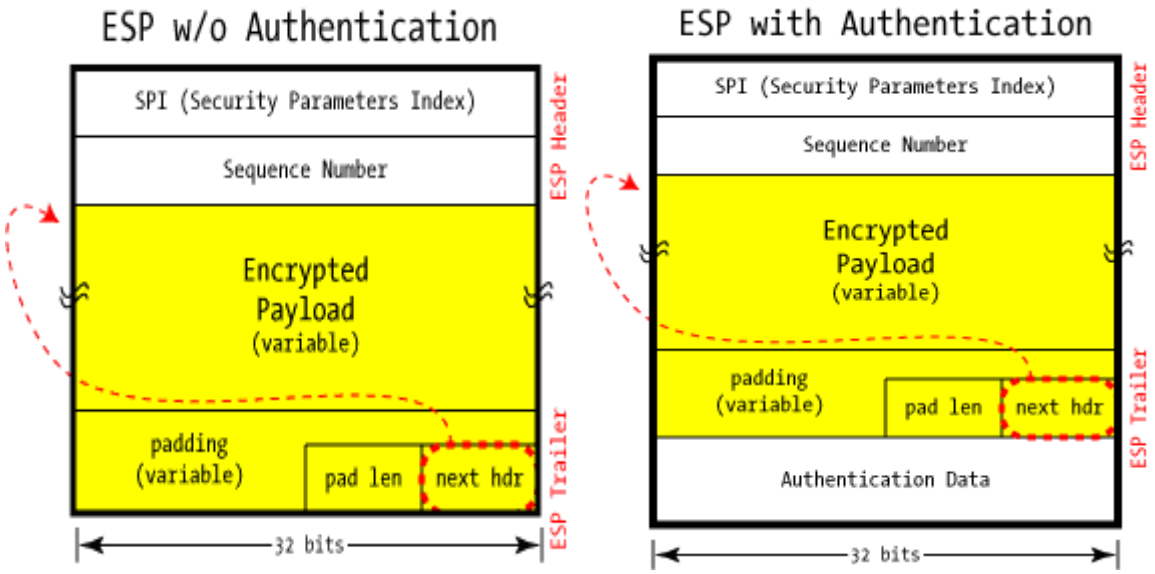
Сурет 3.1 –HMAC

Еске салатын жағдай, IPsec белгіленген алгоритмдердің пайдалануын болжайды, тек ақпараттардың алмасуына қатысатын, олардың екі жақтан келісімдері қажет. Сондықтан сәйкестендірудің басқа қызметтері үшін мүмкіндіктер сақталады.

3.1 ESP хаттамасы

ESP (Encapsulating Security Payload) – жіберіліетін ақпараттардың құпиялылығын сақтау үшін шифрлеу алгоритмін пайдаланатын хаттама, сондықтан ол күрделірек. ESP стандартты жүзеге асырылуында, мәліметтердің шифрленуі үшін DES қолданылады. Бұл алгоритмде қолданылатын құпия сөздің ұзындығы 56 бит, сондықтан ол бүгінгі стандарттар бойынша жеткілікті берік болып табылады. Осы мәселеге орай көптеген өндірушілер өздерінің имплеметацияларында 3DES-ке, ал кейбіреулері AES-ке өтті.

ESPның AH басты айырмашылығы, ESP шифрленген мәліметтерді қапшықтандырады, яғни өзіне атаулар мен аяқтағыштарды қосады. ESP негізіг қызметі рұқсат етілмеген көрілімнен трафиктің қорғалуы, сол уақытта сәйкестендіру салдарынан қорғаныс өзгерісі опционды болып табылады. Бірақ ESP тек пайдалы жүктемені және ESP атауы сәйкестендіреді, сол уақытта стандартты IP-атауда көптеген өрістерді AH сәйкестендіреді. Суретте әртүрлі опциондармен ESP-пакеттің екі пішіні көрсетілген: таритің сәйкестендірілуінсіз және сәйкестендірілуімен



Сурет 3.2-– ESP

SPI және Sequense Number, nexthdr өрістері AH өрісіне ұқсас сәйкес келетін, шамаларға ие.

Encrypted Payload – жоғарғы деңгейлер хаттамасының шифрленген мәліметтері (TCP, UDPжәне т.б.)

padding – мәліметтер блогының ұзындығын түзулеу үшін қызмет ететін өріс

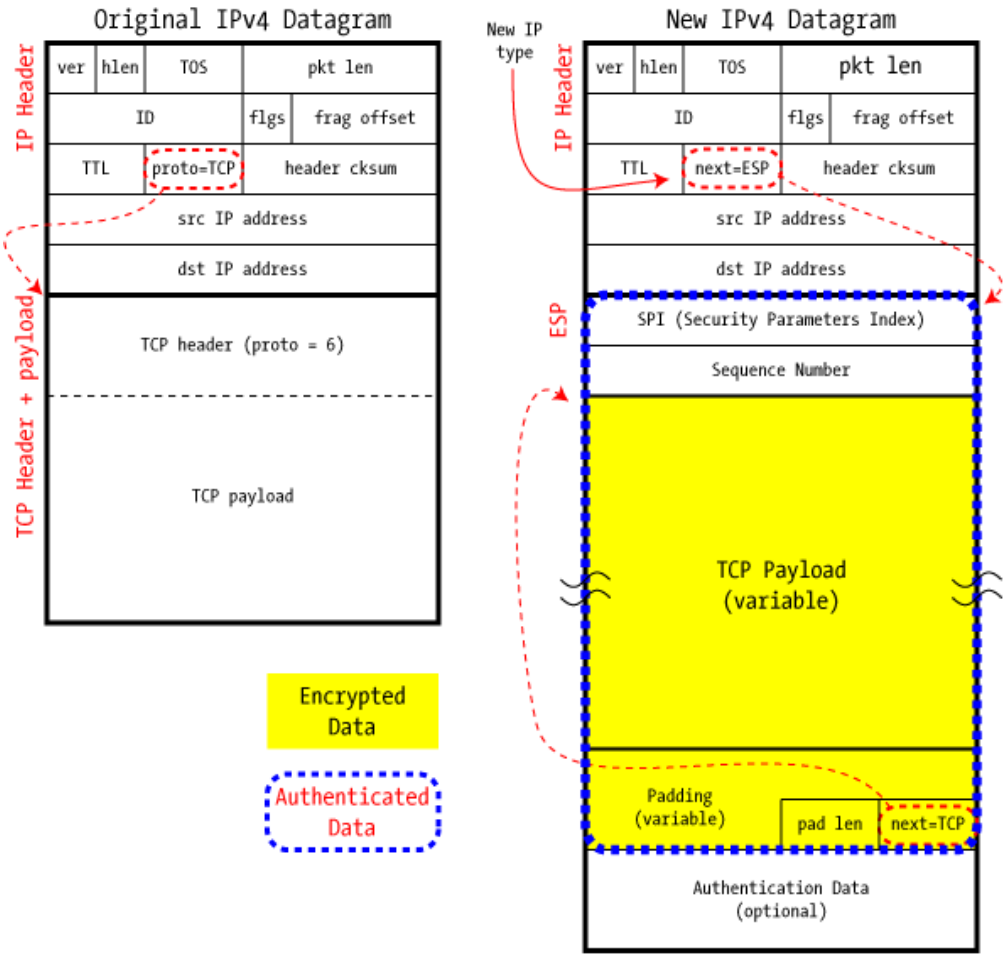
pad len –padding өрісінің ұзынидығы

ESP, AH секілді, тунелльді сияқты тасымалдаушы режімде де жұмыс жасай алады.

ESP қызмет жасауының екі режімін бөлек қарастырамыз.

3.2 Transport mode

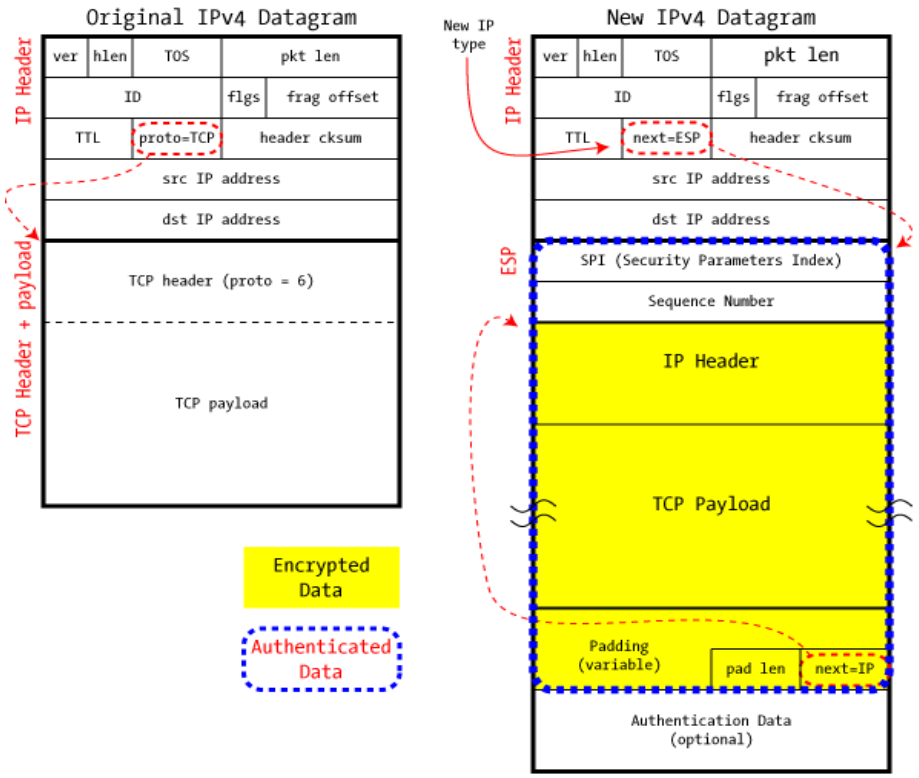
ESP тасымалдаушы режімде қызмет көрсетуі негізінде AH тасымалдаушы режімге ұқсас, тек мына айырмашылық бар, яғни мәліметтер шифрленеді, және оларға қажеттілік кезінде ақтауыштар қосылады:



Сурет 3.3 – ESP transport mode

3.3 Tunnelmode

АН туннельді режімге ұқсас:



Сурет 3.4 – ESP tunnelmode

ESPжәнеАНрежімдерінің тағы бір айырмашылығы мынаған негізделген, яғни АНда шеттен бақылаушы қандай режімнің қолданылғанын үнемі айта алады: егер next hdr = IP – туннельді болса, басқа жағдайларда – тасымалдаушы. ESPте шеттен бақылаушы пакеттердің өңделу режімін анықтай алмайды, себебі next hdr шифрленетін өрістердің қатарына жатады.

3. 4 Қауіпсіз қауымдастық

Мәліметтердің берілісін қорғау бойынша АН және ESP хаттамалары өздерінің жұмыстарын орындау алуы үшін, IKE хаттамасы екі соңғы нүктелер арасында, IPSec стандартында «қауіпсіз қауымдастық» (Security Association, SA) деген атауға ие, логикалық байланысты орнатады. SA орнату өзара сәйкестендіруден басталады, себебі егер де барлық мәліметтер басқамен берілсе немесе басқамен қабылданса, қауіпсіздік шаралары міндетін жоғалтады. SA келесіде таңдалынатын параметрлері, АН немесе ESP екі хаттамасының қайсысы, мәліметтерді қорғау үшін, қандай қызметтер хаттаманы орындайтынын анықтайды: мысалы, тек сәйкестендірілуді немесе толықтылықты тексеру ма, немесе сонымен қатар, жалған қойылымдардан

қорғаныстыма. Қауіпсіз қауымдастықтың аса маңызды параметрі криптографиялық материял болып табылады, яғни AH және ESP хаттамаларының жұмысы кезінде қолданылатын, құпия кілттер.

IPSec жүйесі қауіпсіз қауымдастықтың қолмен орнату амалын қолдануға рұқсат береді, онда әкімшілік құпия кілттерді қоскқанда, қауымдастықтың келісілген параметрлерін олардың қолдауы үшін, әрбір соңғы тұйінді конфигурациялайды.

AH немесе ESP хаттамасы орнатылған SA логикалық байланыстың аясында жұмыс істейді, оның көмегімен таңдалынған параметрлерді пайдаланумен жіберілетін мәліметтердің қажет етілген қорғанысы жүзеге асырылады.

Қауіпсіз қауымдастықтың параметрлері қорғалған арнаның екі соңғы нүктелерін орнату керек. Сондықтан IKE хаттамасының SA орнатудың автоматты процедурасын пайдалану кезінде, арнаның іртүрлі жақтарында жұмыс жасайтындар, келісімді үдерістің жолы кезіндегі параметрлерді таңдайды, оған ұқсастары, алмасу жылдамдығының екі жақ үшін де макисмалды қолайлысын анықтайды. AH және ESP хаттамаларымен шешілетін, әрбір міндеттер үшін сәйкестендіру мен шифрлеудің бірнеше сұлбалары ұсынылады – бұл IPSec өте икемді құрал жасайды. (Байқағанымыздай, сәйкестендірілу мәселесін шешу үшін дайджест қабылдау функциясын таңдау мәліметтерді ширлеу үшін алгоримтді таңдауға еш әсер етпейді.)

IPsec стандартты нұсқасында үйлесімділікті қамтамасыз ету үшін кейбір міндетті «құрал-саймандық» жиынтықтар анықталған: көбінесе, мәліметтердің сәйкестендірілуі үшін SHA-1 немесе MD5 бір жақты шифрлеудің бір функциясы пайдаланылуы мүмкін, ал шифрлеу алгоритмінің саны міндетті түрде DES кіреді. Сонымен қатар IPSec қосатын, өнімді өндірушілер, шифрлеу мен сәйкестендірудің басқа алгоритмдерінің есебінен хаттаманы кеңейту керек, олар оны сәтті жасауда. Мысалы, IPSec көптеген жүзеге асырушылары Triple DES атақты алгоритмін, сонымен қатар салыстырмалы жаңа — Blowfish, Cast, CDMF, Idea, RC5 қолдайды.

IPSec стандарттары Internet хосттары арқылы барлық өзара әрекеттесетін трафиктердің берілісі үшін SA бір қауымдастығын шлюздерге пайлануға мүмкіндік береді, сонымен осы мақсат үшін SA еркін санын құра алады, мысалы әрбір TCP байланысқа біреуі беріледі. SA қауіпсіз қауымдастық өзімен IPSec логикалық байланысты ұсынады, сондықтан мәліметтердің екі жақты ауысым кезінде SA екі қауымдастықты ұсынады.

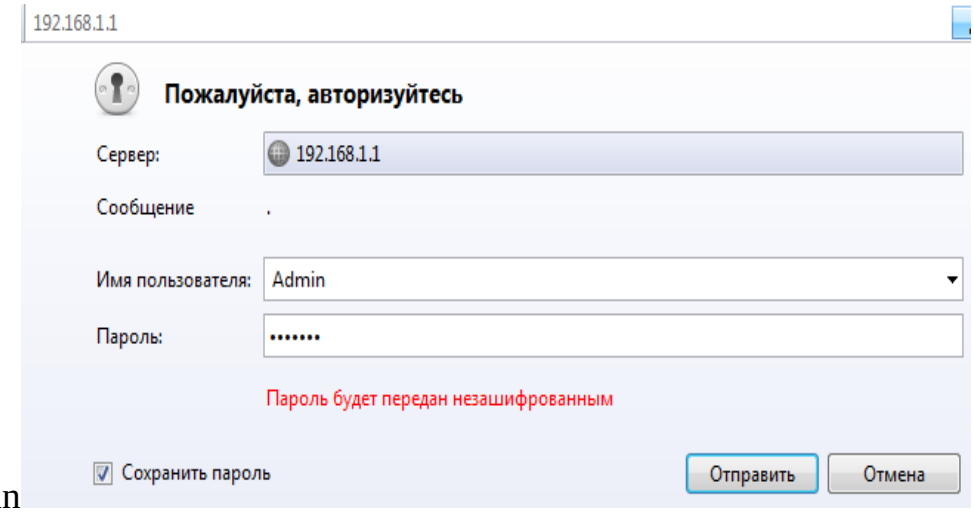
3.4.1 IPsec хаттамасында жеке виртуалды желіні құру

Жұмыстың мақсаты: PFsense бағдарламалық қамтамасыз етудің көмегімен тұтынушы-тұтынушы байланысы үшін VPNIPsec туннелін құру.

PFsense көмегімен байланыс баптауы

Алғашқыда компьютерде WEB браузер бағдарламасының көмегімен PFsense бағдарламасында қуаттаймыз:

1. IP: 192.168.1.1;
2. Пайдаланушы аты: Admin;
3. Құпия
4. сөз:

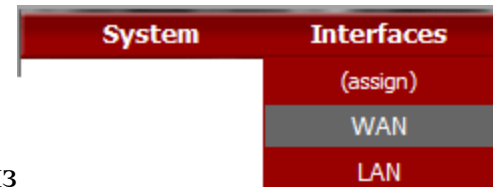


Admin

Қаттандырғаннан кейін PFsenseбағдарламасының негізгі жұмыстық терезесі қосылады. Себебі біздің желіде PFsense 2 сервері онда барлық параметрлердің баптаулары екі сервер үшін де екі рет болады.

PFsense бірінші серверінің баптауы

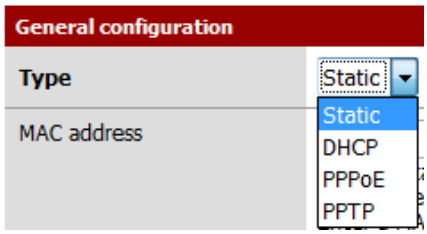
Жұмыс терезесінде WAN баптау параметрлерінің Interfaces кіреміз.



Interfaces-→ WAN бөлімін таңдаймыз

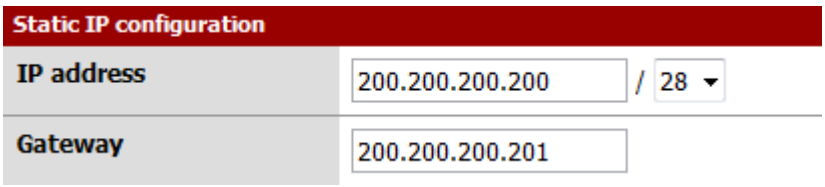
Бұл бөлімді ашу кезінде кейбір баптауларды жүргізе бастаймыз

Type-→Static

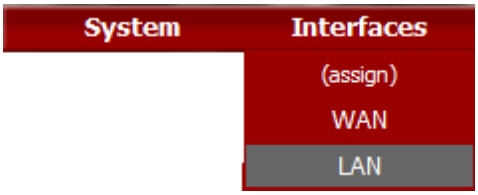


Static IP configuration:IP address 200.200.200.200/28

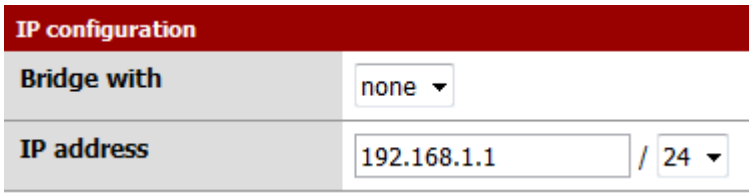
Gateway 200.200.200.201



Содан кейін дәл осындай баптауды жүргіземіз, тек LANжағынан Interfaces-→LAN

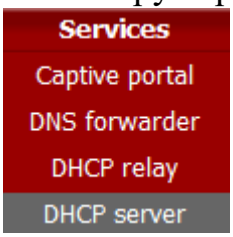


Содан кейін Ipconfiguration IPадрессті және LAN жағынан қосымша желінің маскасын береміз.



LANжелісінде IPдербестендірілу автоматты түрде беріледі. Біздің жағдайда IPsec туннелін құру үшін DHCP servera өшіру керек. IP дербестендірілу белгілі бір RANGE автоматты түрде берілмеуі үшін. DHCP серверін өшіру үшін DHCP server бөліміне кіру керек.

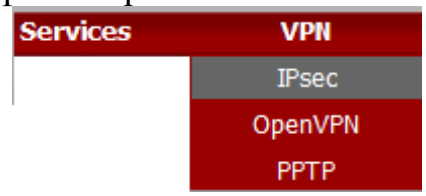
Services-→DHCP server



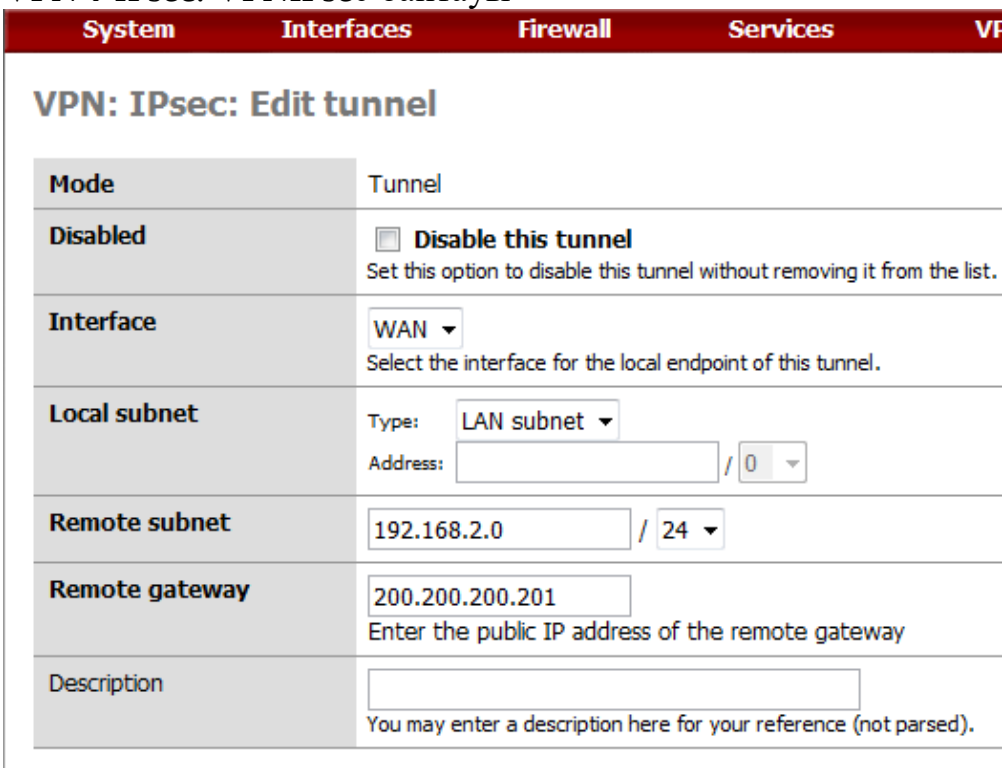
Сақтауды жүргіземіз (SAVE) → LAN және WAN параметрлері сәтті тұрғызылды.

IPsec туннелін құрудың келесі қадамы VPN IPsec бөлімінің параметрлерін баптау болып табылады.

Жұмыс терезесінен VPN→IPsec таңдаймыз



VPN→IPsec. VPNIPsec баптауы



MODE бағанында --→Tunnel әдепкі қалпы бойынша.

Interface-→WANWANжәне LAN қосымша желілері міндетті түрде әртүрлі болуы керек WAN-→/28,алLAN-→/24

Жергілікті желінің түрі қажетті зертханалық жұмыс бойынша таңдалынады, біздің жағдайда --→LAN subnet.

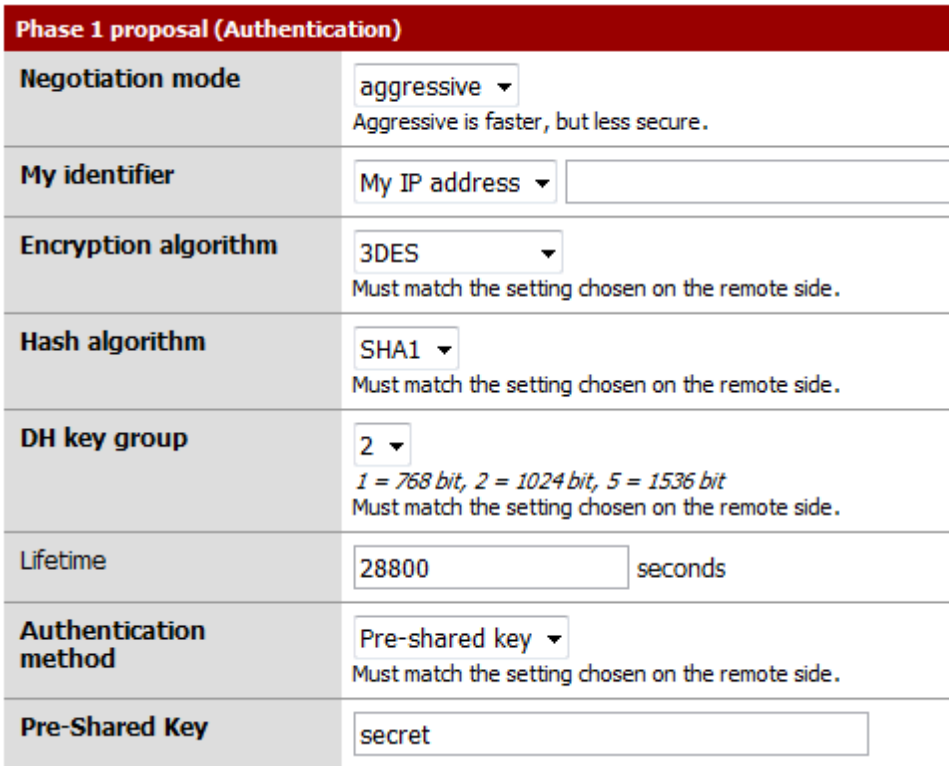
Қашықтықтағы желінің IP address: Remote subnet 192.168.2.0 /24 Қосымша желінің маскасы -→/24

Қашықтықтағы шлюз:Remote gateway 200.200.200.201

Шлюз-үшінші деңгей құралы

Description бағаны әдеттегі қалпы бойынша.

Phase 1(Authentication)-Сәйкестендіру



IPsec үшін бағдарламада Negotiation mode 2 түрде болуы мүмкін. (Aggressive және Main). Біздің жағдайда-→Aggressive.

Бұл режим Main режиміне қарағанда жылдам, бірақ қауіпсіздігі төмен.

My identifier→My Ip address. яғни IP адресті алу автоматты түрде жүреді.

Encryptionalgorithm→3DES.

Хэштеу алгоритмі Hashalgotithm-→SHA1.

Dhkey group→2(Диффи-Хеллмана).

Lifetime еркін таңдалынады, біздің жағдайда →28800 seconds

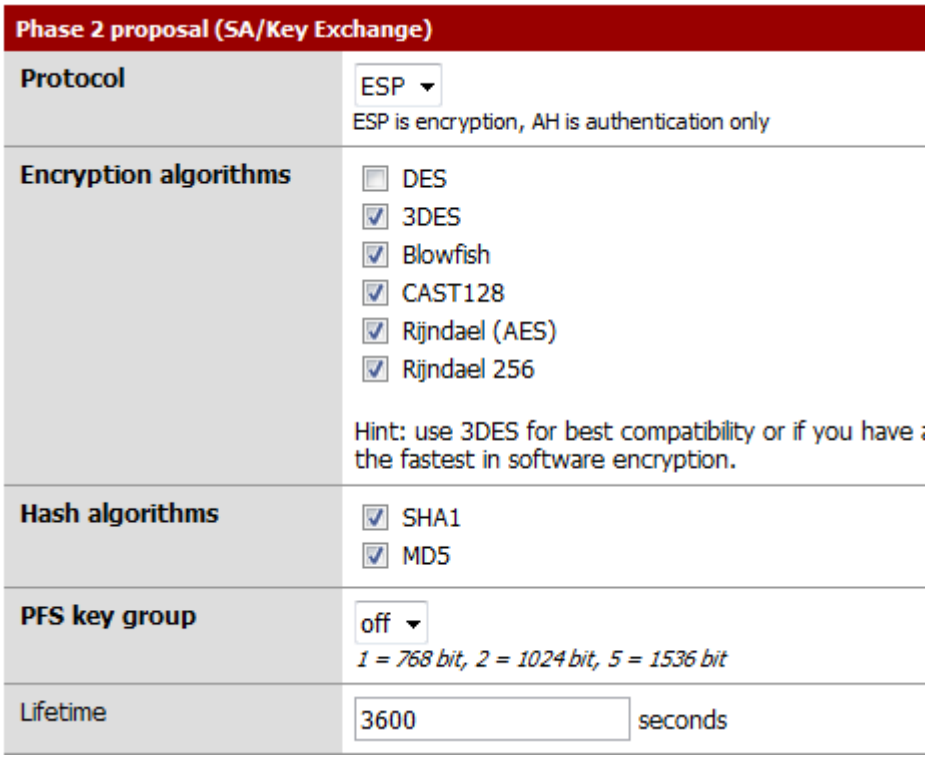
Сәйкестендірілу амалы –жалпы кілт. Authentication mode→Pre-shared key.

Pre-shared key өзі еркін енгізіледі (мәтіндік сөз)----Pre-shared key-→secret

Біздің жағдайда сертификаттау VP NIPsec үшін әдепкі қалпы бойынша белгіленбейді.

PFsense екі сервері үшін PHASE1(Authentication) баптауы туннельді құру үшін міндетті түрде бірдей болуы керек.

PHASE 2(SA,Key Exchange)



Protocol→ESP.(сәйкестендіруді және берілістерді жүргізеді – осымен АН хаттамасы тиімді)

Encryption algorithms→біз үшін барлық мүмкін болатын түрлерді белгілейміз. Сұранысты кім бірінші жасайтын сервистен, сол шифрлеу түрін Encryption algorithms оған ұсынылған тізімнен таңдайды. Ол Pfsense2 сервері үшін Encryption algorithms 2 тізімінен шифрлеудің белгілену түрімен кездейсоқтық жолмен таңдайды.

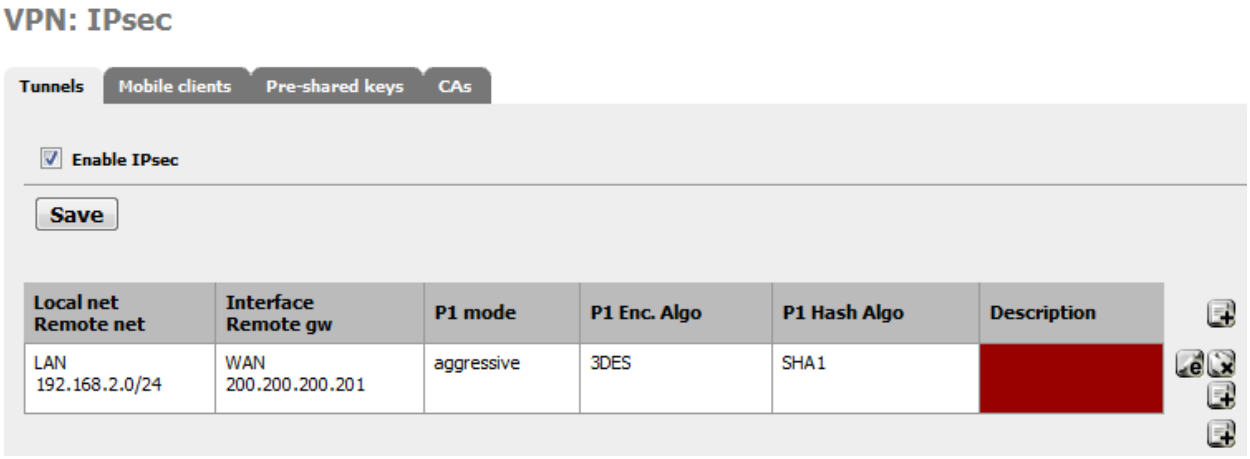
Hash algorithms→SHA1 и MD5.

PFSkey group→off

Lifetime→3600 seconds.

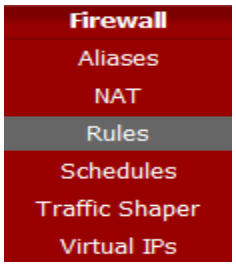
Баптауларды аяқтағаннан кейін олардың сақталуын орындаймыз →SAVE

Параметрлерді сақтағаннан кейін біз жүргізген барлық баптаулардың терезесі көрсетіледі.

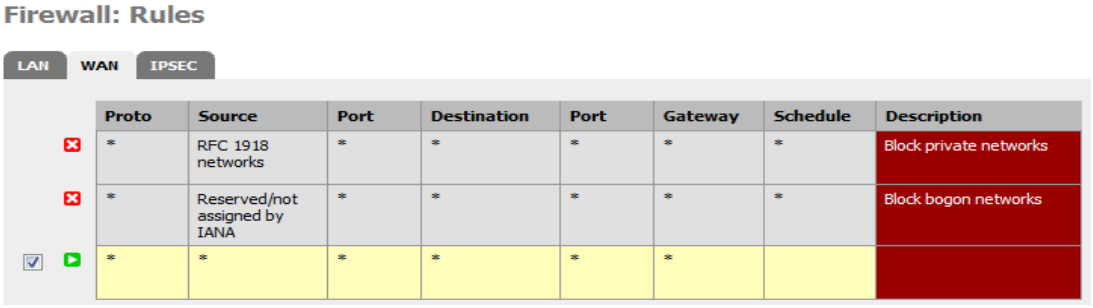


Содан кейін Firewall түріне PFsense келтіреміз..

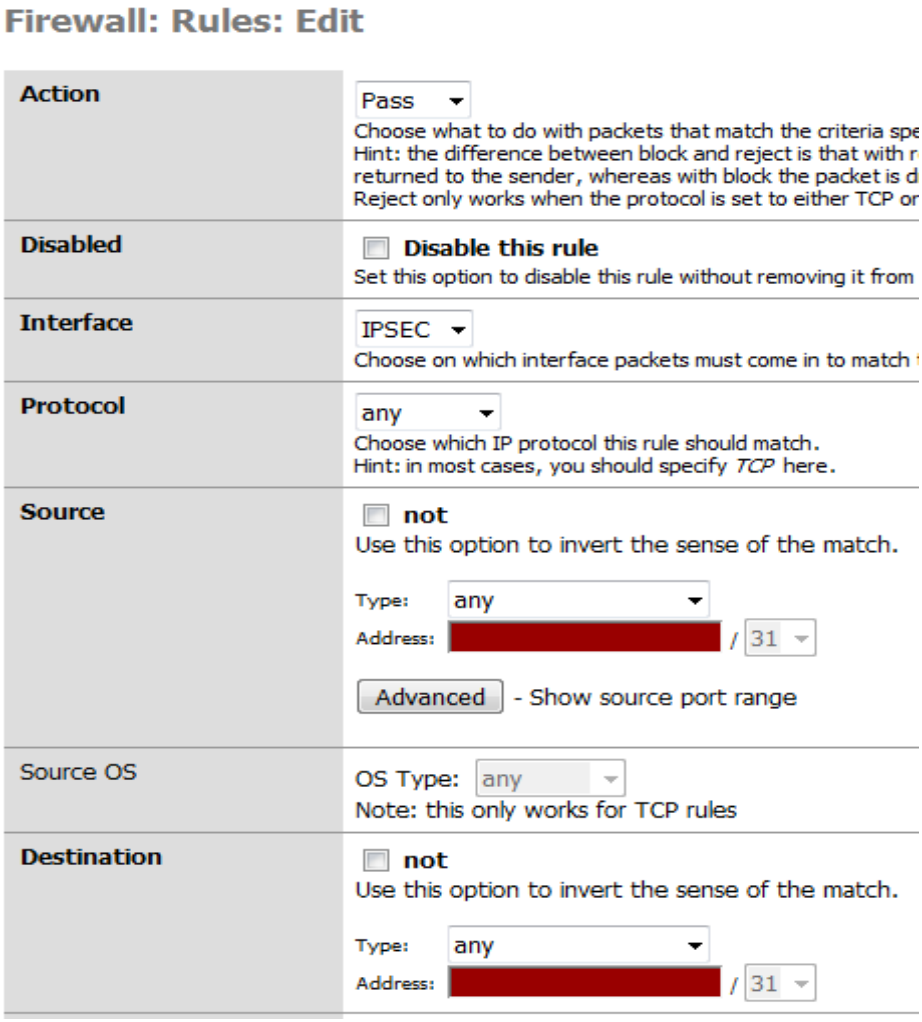
Біздің PFsense бағдарламамызда Firewall6 түрі бар. Бізге Rules таңдау керек Firewall → Rules.



Rules бөлімі ашылғаннан кейін IPsec бізге қажетті бөлігін белгілейміз.



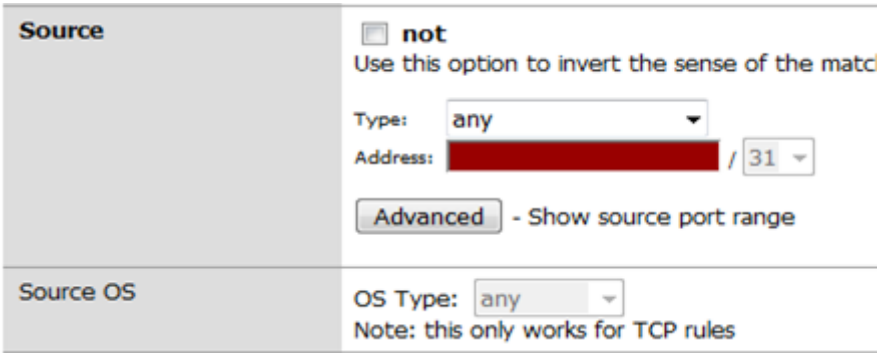
Бізге IPsec баптаулары қажет.Сондықтан  басамыз және VPN IPsec баптауын жүргіземіз.



Firewall rules по IPsec бойынша Firewall rules барлық бағаналар әдепкі қалпы бойынша толтырылған. Бізге Destination ,Source,Source OS,Protocol бағаналарын дұрыстау қажет.

В графу Destination бағанына жіберіліс кімге тиесілі болса соған енгізіледі. Онда біз қабылдаушының Ip address адресін енгізбейміз. Біз Destination→Any белгілейміз, яғни кез келген IP address автоматты алады.

Осындай баптауларды Source,Source OS бағанына енгіземіз.

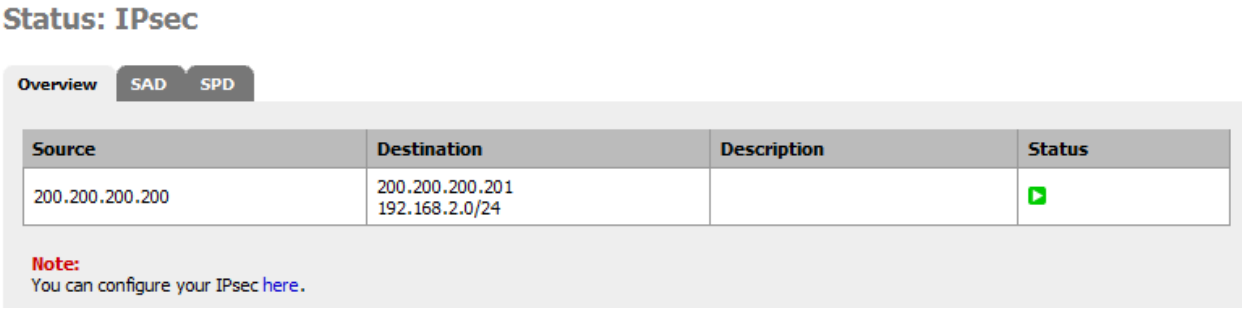


Source-→Any и Source OS→Any.

Protocol-→Any.Біздің жағдайда ProtocolTCPретінде толтырылған. Бізге берілістің хаттама түріне тәуелсіз өткені қажет.

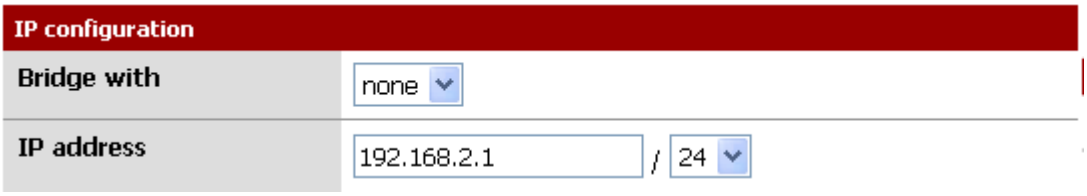
Баптауларды қайтадан сақтаймыз Firewall Rules -→Save.Осындай баптауды Firewall →Rules→ WAN үшін жүргіземіз.

IPsec туннелің статусын тексеру үшін біз STATUS-→IPsec бөліміне кіреміз.



PFsense бірінші сервері үшін VPNIP sec параметрінің баптауы аяқталды.
PFsense екінші сервері үшін VPN IPsec туннелінің параметрлерін баптауға кірісеміз.
Interfaces WAN және LAN үшін IP configuration ұқсас баптауларын жүргіземіз .
Interfaces→WAN
Type→static
Static IP configuration IP address 200.200.200.201/28
Gateway
200.200.200.200

Interfaces→LAN IP address 192.168.2.1/24

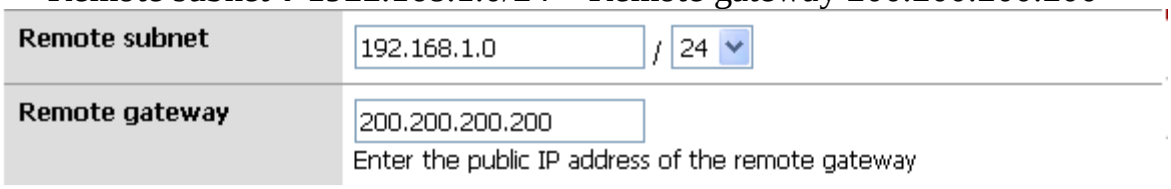


Сосын VPNIPsec параметрлерінің баптаулары

VPN→IPsec

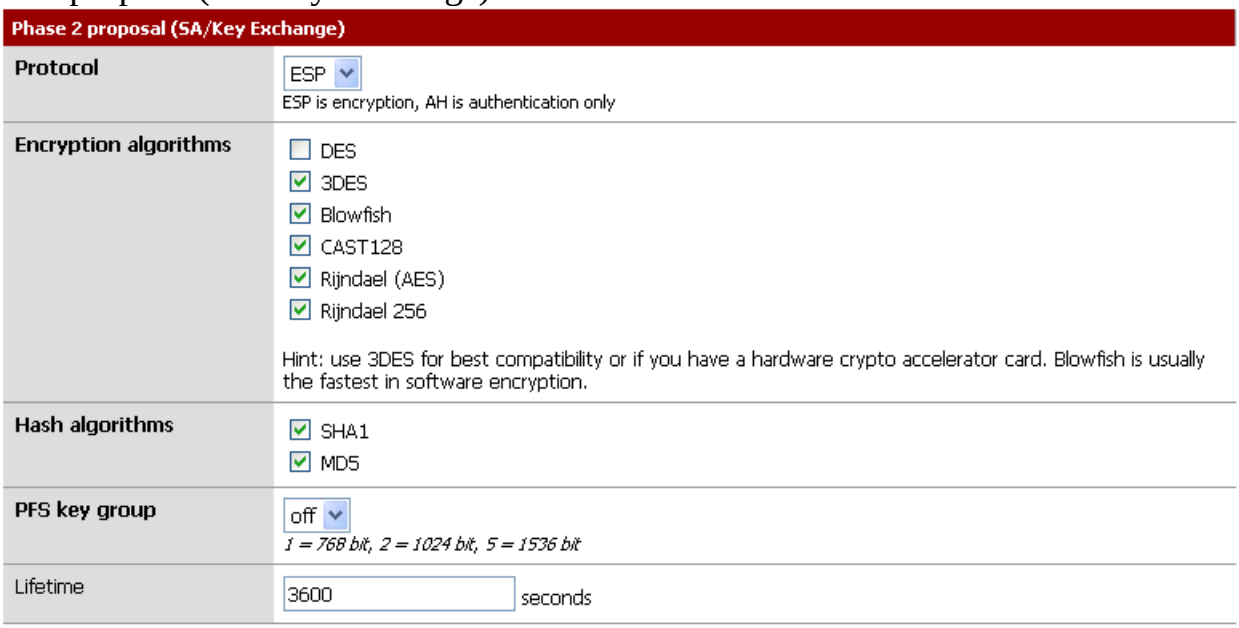
IPsec:Edittunnel→бұл параметрлердің баптаулары PFsenseсерверінің баптауларына ұқсас болады. Тек Remote subnet және Remote gateway бағандары өзгереді.

Remote subnet→1922.168.1.0/24 Remote gateway 200.200.200.200

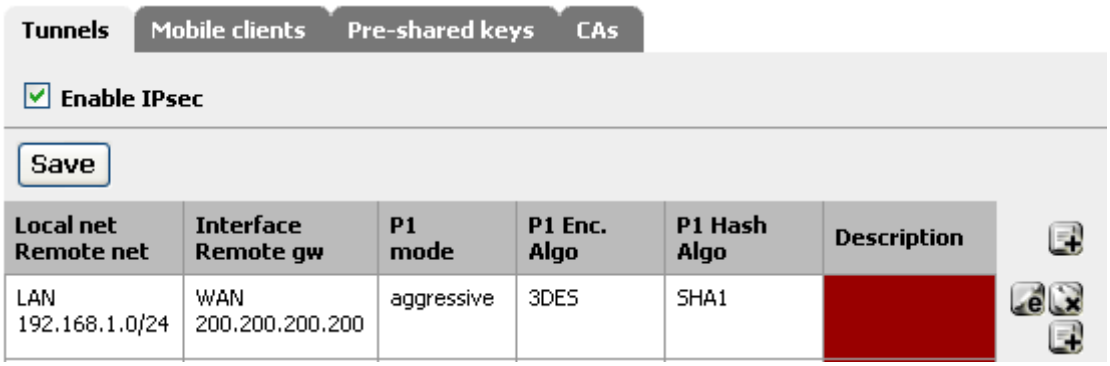


Екінші сервердің Phase 1 proposal (Authentication) параметрлерінің баптауы айтылып кеткендей VPNIPsec туннелін құру үшін PFsense бірінші сервердің сәйкестендірілу баптауларымен тура келуі керек.

Phase 2 proposal(SA Key exchange)



IPsec туннелінің статусы.

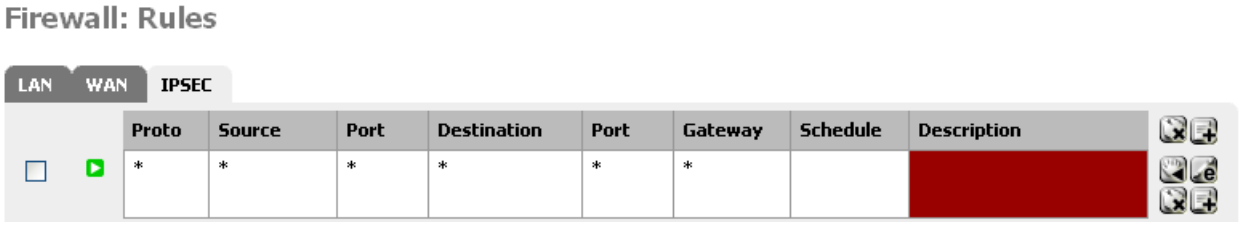


PFsense екінші сервердің Firewall(для WANи IPsec) параметрлерінің баптауы Pfsense бірінші сервердің баптауларына ұқсас болып келеді.

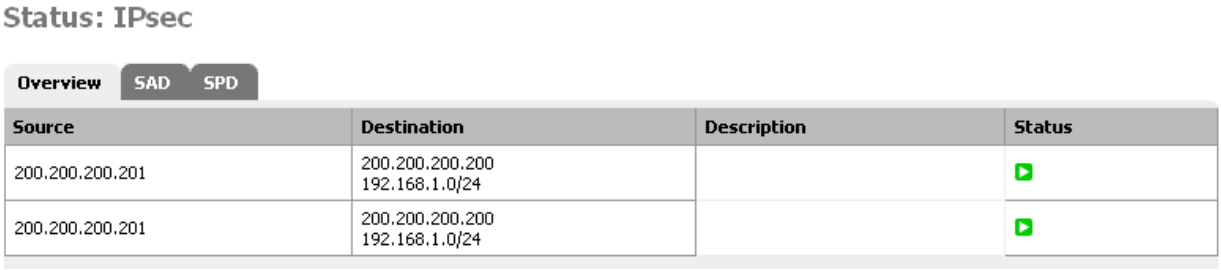
Firewall→Rules

Protocol→any Source→any Source OS→any Destinantion→any

Status Firewall Rules для IPsec

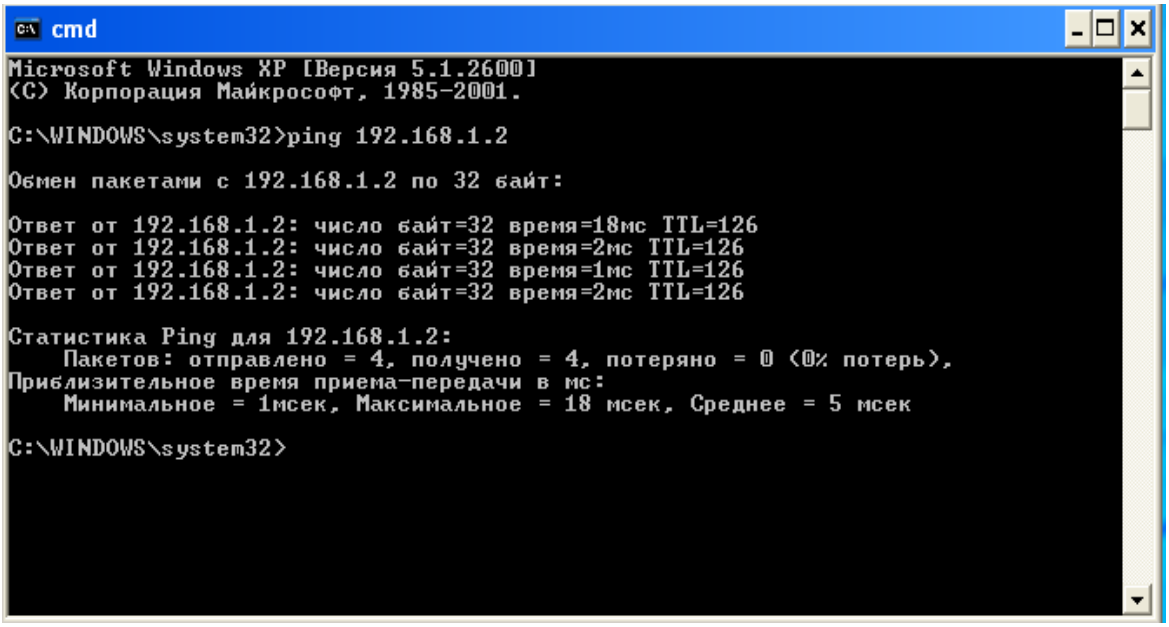


Status IPsec tunnel Overview



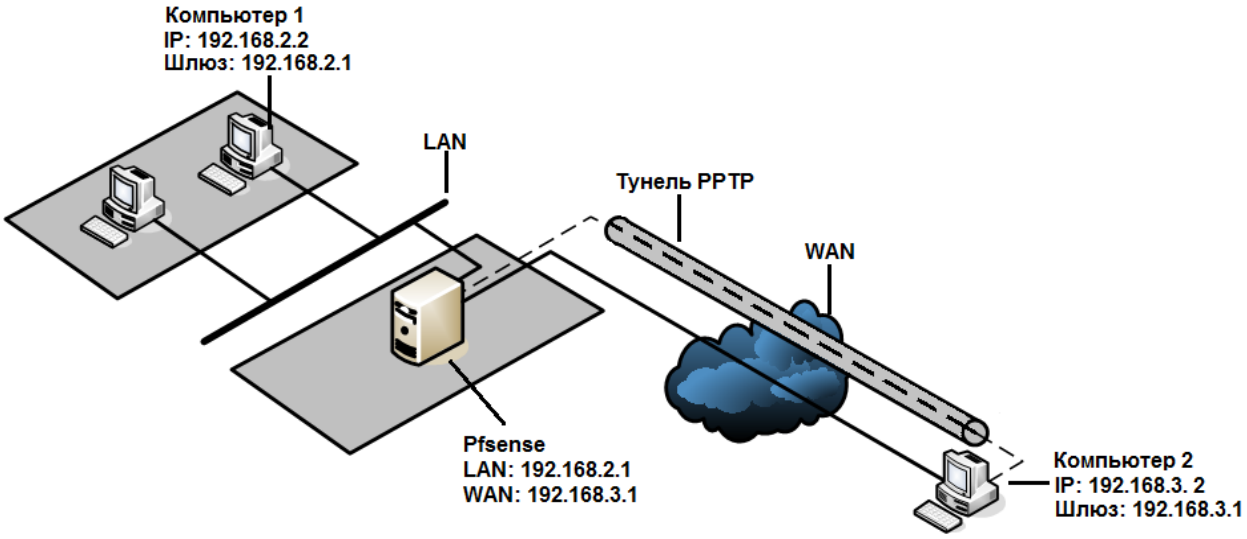
PFsense екінші сервері үшін VPNIPsec параметрлерінің баптауы аяқталды.

Құрылған VPNIPsec туннеліне тексеру жүргіземіз. Тексеру ping функциясының көмегімен болады. Бір тұтынушы екіншіге сұраныс жасайды.



VPNIPsec туннелі сәтті құрылды

PFsense операциялық жүйесін пайдаланумен PPTP хаттамасында виртуалды жеке желіні құру

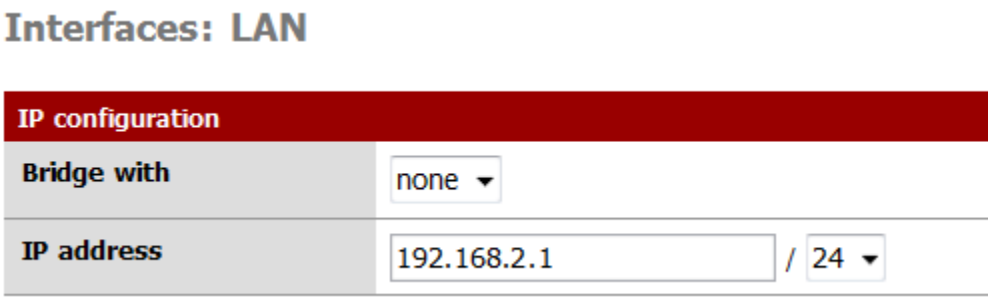


Сурет 3.5 – PPTP хаттамасында туннельді құру

Жұмыстың мақсаты: 3.5- суретте көрсетілгендей, 1,2 компьютерлерінің арасында PPTP хаттамасы негізінде туннельді құру .

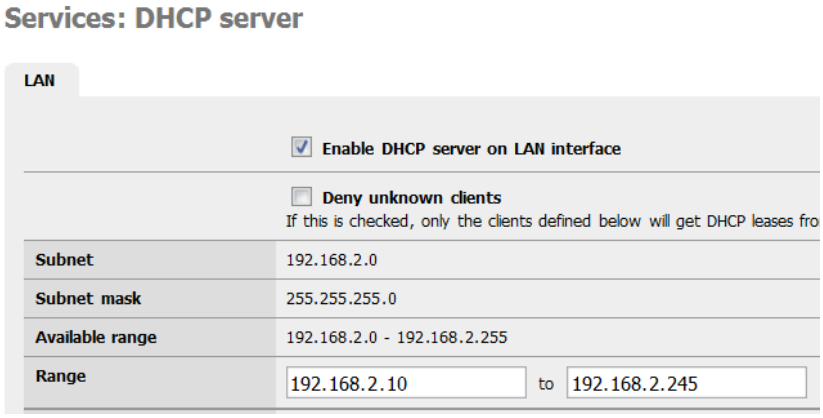
LAN және WAN желісінің баптауы

Алдымен LAN ішкі желісін құрып аламыз. Interfaces шығатын мәзірге кіріп және онда LAN өосымша пунктін таңдау керек. Ашылған терезеде, «IP address» сөзіне қарама-қарсы IP адресті және сіз нұсқа бойынша таңдаған қосымша желіні енгіземіз. Біздің жағдайда бұл 192.168.2.1.



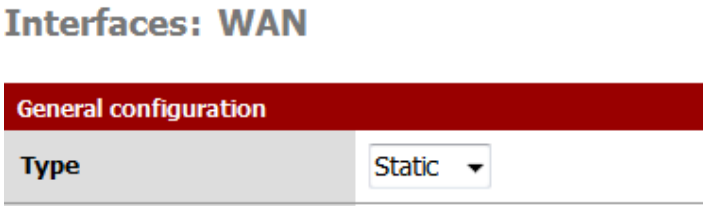
Сурет 3.6 – Шығатын Interfaces мәзірі: LAN

Бізге DHCPсерверін өшіру керек. Өткен жұмыста біз бұны pfsense ерверінен бастап жасағанбыз, енді веб-интерфейстің көмегімен жасаймыз. Шығатын Services мәзірге кіріп DHCP server қосымша пунктін таңдайміз және «Enable DHCP server on LAN interface» пунктінен белгіні алып тастаймыз. Өздеріңіз байқағандай біз берген диапазон (192.168.2.10 до 192.168.2.245) активті болмады.



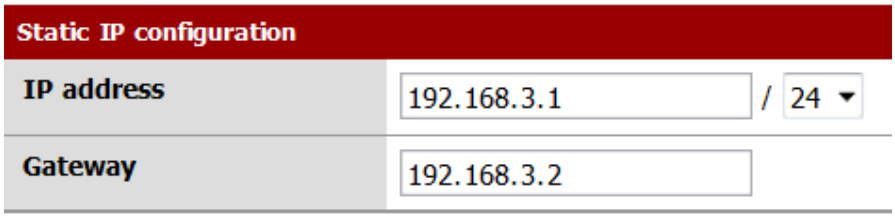
Сурет 3.7– Шығатын Services мәзірі: DHCP server

Содан кейін WANсыртқы желіні құрамыз. Шығатын Interfaces мәзіріне керу керек және WAN қосымша пунктін таңдаймыз. Ашылған терезеде, «Type» сөзіне қарама-қарсы қосылыс типін таңдаймыз. Біздің зертханалық жұмыс үшін «Static» типін таңдаймыз. Онда біз IP адресті және қосымша желіні өзіміз анықтай аламыз.



Сурет 3.8 – Шығатын Interfaces мәзірі: WAN

«Static» қосылыс типін таңдау кезінде «Static» бөлімі белсенді болады.



Сурет 3.9- –Static IP configuration бөлімі

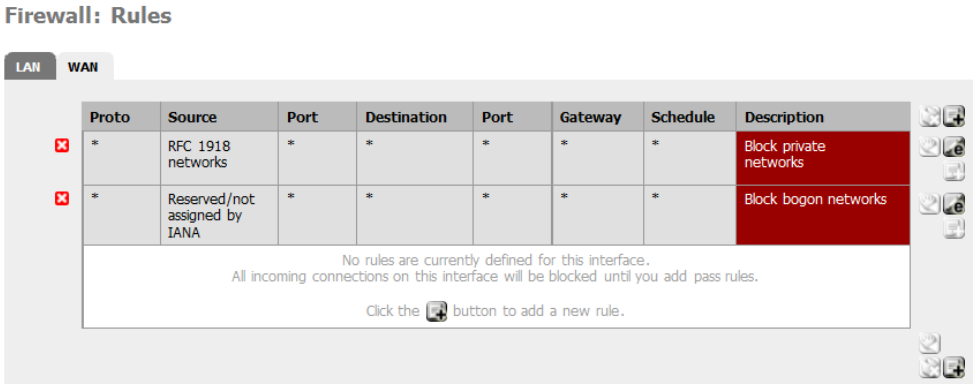
IP адрес және қосымша желінің нөмерін нұсқа бойынша таңдаймыз. Желі қосылған шлюздің IP адресін анықтауымыз керек. Адрес юір желіде жатуы керек.

Мысал үшін WAN желісінің IP адрес: 192.168.3.1;

Ал қашықтықтағы компьютердікі 2: 192.168.3.2.

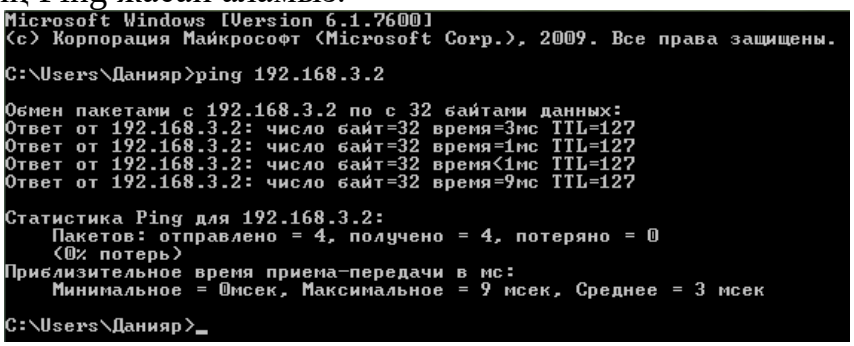
Біз LAN және WANIP адресін анықтады. Енді компьютерлер арасында Ping жүргіземіз. Өздеріңіз көріп тұрғандай Ping өтпейді. Бұл pfsense-те Firewall орнатылмағандықтан.

Бұл үшін шығатын Firewall мәзіріне кіру керек және Rules қосымша пунктін таңдау керек. WAN бапталмаған, баптау үшін WAN кіріңіз.



Сурет 3.10 – шығатын Firewall мәзірі: Rules

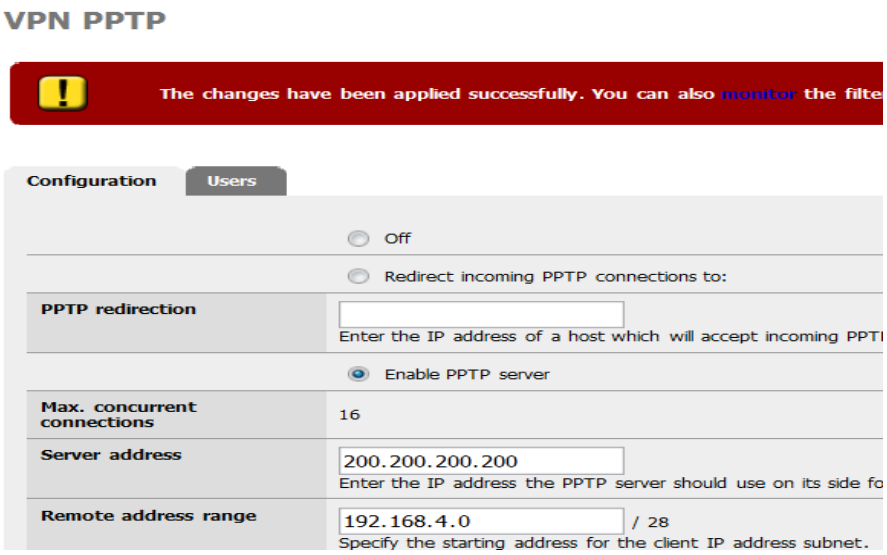
 батырмасын басып біз WANжелісіне жаңа ережелерді береміз. Бұл жерде WAN желісі үшін ережелерді беруге болады. Алдымен ең бастысы хаттама типін өзгерту керек,Protocol TCP-ны any-ге. Any таңдап, біз барлыө хаттамаларға сервер арқылы LANжелісіне өтуге рұқсат береміз. Содан кейін «Save» басамыз. Енді біз 2 компьютер көмегімен 1 компьютердің Ping жасай аламыз.



Сурет 3.11 –1 компьютердің көмегімен 2 компьютердің Ping

PPTP (pfsense) серверін баптаймыз.

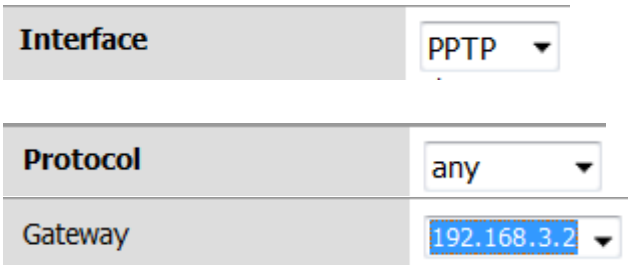
PPTP (pfsense) серверін құру үшін шығатын VPN мәзіріне кіру керек және PPTP қосымша пунктін таңдау керек.



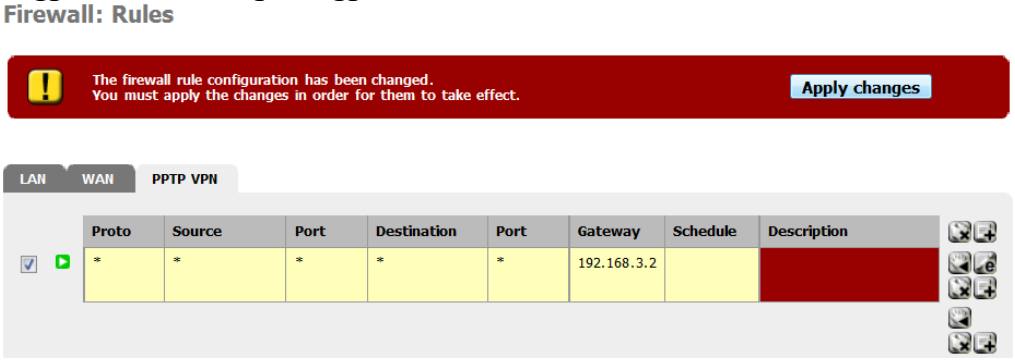
Сурет 3.12- – Шығатын VPN мәзірі: PPTP

Создаем сервер PPTP пометив пункт «Enable PPTP server» пунктін белгілеп PPTP серверін құрамыз және IPсерверін 200.200.200.200 береміз. PPTP хаттамасында VPN құрылған кезде, серверге қосылғандардың барлығы жаңа желіде жұмыс істейді, яғни туннель құрылады. Жаңа желіні құру үшін IP желінің «Remote address range» сөзін протиге жазу керек. Біздің жағдайда бұл 192.168.4.0. Мұнда PPTP серверінің адресі және туннель бір желіде жатпауы керек. «ОК» басып, біз қабылданған баптауларға келісеміз. Енді желінің құрылуы үшін «Rules» ережесін беру керек. Бұл үшін шығатын Firewall мәзіріне кіру керек және Rules қосымша пунктіні таңдаймыз. PPTP VPN үшін ережелерді құрамыз. Бұл үшін батырмасын басамыз. Баптаулар келесідей жүргізіледі:

1. Interface → PPTP.
2. Protocol → any.
3. Gateway →



«Save» содан кейін «Apply changes» басамыз. Енді біз PPTP қосылысының ережесі құрылғанын көріп тұрмыз.



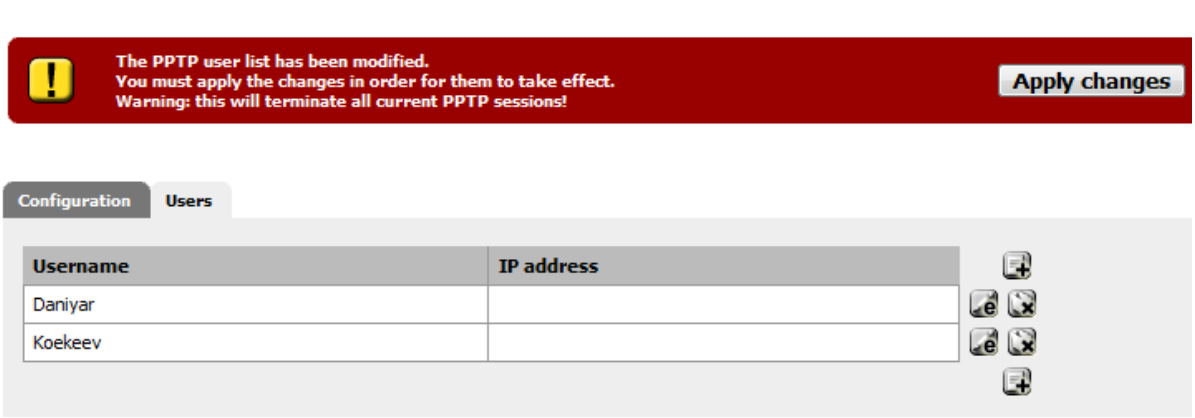
Сурет 3.13 – PPTP VPN үшін ережелер

Енді пайдаланушыларды қосамыз. Бұл үшін шығатын VPN мәзіріне кіреміз және PPTP қосымша желісін таңдаймыз. Ол жерден «Users» пунктін басамыз. Біз 192.168.4.0 желісінде жататын 16 пайдаланушыны қоса аламыз. Яғни IP адрестер 192.168.4.0 тен 192.168.4.15 дейін автоматты түрде тағайындалатын боладыу Алдымен 2 пайдаланушыны, компьютер 1 және компьютер 2 қосуға болады. Барлық әрекеттер төменде көрсетілген:

1. VPN → PPTP → Users

2. батырмасын басамыз және жаңа пайдаланушыны қосамыз және пайдаланушының аты мен құпия сөзін енгіземіз. Мысалы:Username: Daniyar; Password: Daniyar.

Сосын «Save» және содан кейін «Apply changes» басамыз.



Сурет 3.14 – Пункт «Users»

Сонымен минимум 2 пайдаланушыны құру керек, аты мен құпия сөзді өзіңіз таңдайсыз.

Пайдаланушы бөлімінің баптаулары.

1 компьютерді баптау үшін келесідей әрекеттерді жасау керек:

1. Сетевое окружения → Свойства подключения по локальной сети → Свойства Протокол Интернет (TCP/IP) Свойства.
2. IP-адрес енгіземіз: 192.168.2.2;
3. Қосымша желі маскасы: 255.255.255.0;
4. Негізгі шлюз: 192.168.2.1.

Сосын VPN PPTP қосылысты баптаймыз. Ол үшін:

1. Сетевое окружения → Свойства → создания нового подключения → Подключить к сети на рабочем месте → подключения к виртуальной частной сети.
2. Ұйымның атауын енгізу керек. Мысалы:KAZNTU1;

3. «Не набирать номер для предварительного подключения» дегенді таңдау керек;

4. Енді VPN-сервердің амауын немесе адресін көрсету өажет. Бізде IP адрес 192.168.2.1, яғни компьютердің шлюзі.

5. KAZNTU1 басып пайдаланушы атын және құпия сөзді енгіземіз. Мысал 12 суретте көрсетілген.

Енді 2 компьютерді баптауымыз керек:

1. Сетевое окружения → Свойства → подключения по локальной → сети Свойства → Протокол Интернет (TCP/IP) → Свойства.
2. IP-адресті енгіземіз: 192.168.3.2;
3. Қосымша желі маскасы: 255.255.255.0;
4. Негізгі шлюз: 192.168.3.1.

Содан кейін VPNPPTPқосылысын баптаймыз. Ол үшін:

1. Сетевое окружения → Свойства создания нового → подключения Подключить к сети на рабочем месте подключения к виртуальной частной сети.
2. Ұйым атын енгізу керек. Мысалы: KAZNTU2;
3. «Не набирать номер для предварительного подключения» таңдау керек;
4. Енді VPN-сервердің атын немесе адресін көрсету керек. БіздеIPадрес 192.168.3.1, яғни компьютер шлюзі.
5. KAZNTU2басамыз және пайдаланушы атын және құпия сөзді енгіземіз.

Енді 1 және 2 компьютерлері арасында Pingтест жүргіземіз. Маңызды: 1 және 2 компьютерлердің IP адресі басқа болады. IP адресін білу үшін, 1 компьютері үшін «KAZNTU1», 2 компьютер үшін «KAZNTU2» VPN қосылысының мағлұматтарының күйіне кіру керек.

ҚОРЫТЫНДЫ

Бұл жұмыста біз VPN технологиясын қолдана отырып телекоммуникация жүйелерінде ақпаратты қорғау мәселелерін қарастырдық. Біз технология жұмысының принципін дайындадық.

VPN технологиясы қайта қолданылады және оның хаттамаларымен т.б. VPN технологиясы мынада, яғни қашықтықтағы қолжетімділіктің ұйымдары телефон желісі арқылы емес, Интернет арқылы жасалынуында, ол анағұрлым арзан және жақсы. VPN технологиясының кемшілігі, VPN тқрғызылу құралдары анықтаудың және шабуылдарды бұғыттаудың толыққанды құралдары болып табылмайды. Олар рұқсат етілмеген әрекеттердің қатарын алдын алуы мүмкін, бірақ корпоративті желіге ену үшін барлық мүмкіндіктерін қолдана алмайды. Бірақ бұған қарамастан VPN бұл технологиясы үлкен дамуларға ие болды.

Internet-те ақпарттарды қорғау мәселесі қойылады, және тиімділіктің сол немесе басқа деңгейімен, TCP/IP туыстығы хаттамасының негізінде желінің пайда болу мезетінен шешіледі.

Қорғаныс технологиясының эволюциясында үш негізгі бағытты белгілеуге болады. Біріншісі – желіні белгілі бір қорғаныс құралына имплементациялайтын, стандарттарды дайындау. Мыал ретінде IP security option және TCP/I туыстығы хаттамасының нұсқаларын айтуға болады. Екінші бағыт – желі аралық экрандардың (firewalls) мәдениеті, қосымша желілерге қолжетімділікті реттеу үшін ертеден қолданылуда. Үшіншісі, аса сәнді және белсенді дамушы бағыт – виртуалды қорғалған желілердің технологиясы (VPN, virtual private network, немесе intranet).

Соңғы жылдары бақылып келе жатқан Internet және соған байланысқан коммерциялыұ жобалардың атақтылық деңгейінің өсуі TCP/IP-желісінде ақпаратты қорғаудың жаңа технологиясы, жаңа буынының дамуына түрті ретінде қызмет көрсетті. Сонымен, ертеректе Internet-те қорғаныстың басты мақсаты хакерлік шабуылдардан қорларды сақтау болса, онда қазіргі уақытта коммерциялық ақпаратты сақтау актуалды мәселе болып келуді.

ҚОЛДАНЫЛҒАН ӘДЕБИЕТТЕР

1. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. - М.: 2001. - 368 с.
2. Кульгин М. Технологии корпоративных сетей. Энциклопедия. - СПб.: Питер, 2000. -704 с
3. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. - СПб.: Питер, 2001. - 672 с.
4. Романец Ю. В.. Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. - М: Радио и связь, 2002. −328 с.
5. Продукты для виртуальных частных сетей [Электронный документ] - http://www.citforum.ru/nets/articles/vpn_tab.shtml
6. Анита Карве Реальные виртуальные возможности // LAN. - 1999.- № 7-8 http://www.osp.ru/lan/1999/07-08/107.htm
7. IPSec - протокол защиты сетевого трафика на IP-уровне [Электронный документ] / Станислав Коротыгин. - http://www.ixbt.com/comm/ipsecure.shtml
8. VPN и IPSec на пальцах [Электронный документ] / Dru Lavigne. - http://www.nestor.minsk.by/sr/2005/03/050315.html
9. В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. - М.: «Вильямс», 2002. - С. 432.
10. Сергей Петренко Защищенная виртуальная частная сеть: современный взгляд на защиту конфиденциальных данных // Мир Internet. - 2001. - № 2
11. Дюсебаев М. К. БЖД. Дипломное проектирование. Методические указания (для студентов всех специальностей ФРТС), Алматы, АИЭС, 2003.
12. Экономика связи: Учебник для вузов. - Под ред. О.С. Срапионова. – М.: Радио и связь,1992. − 354 с.
13. Н.П. Резникова Маркетинг в телекоммуникациях. – М.: Эко–Трендз, 1998. − 351 с.