ӨЗБЕКСТАН БАЙЛАНЫС ҲӘМ ИНФОРМАЦИЯЛАСТЫРЫЎ АГЕНТЛИГИ

ТАШКЕНТ ИНФОРМАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРЫ УНИВЕРСИТЕТИ НӨКИС ФИЛИАЛЫ

ИНФОРМАТИКА ҲӘМ ИНФОРМАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР КАФЕДРАСЫ

Информациялық технологиялар факультетиниң

информациялық сервис бағдарының

4-курс студенти Асқаров Баҳадырдың

ПИТКЕРИЎ ҚӘНИГЕЛИК ЖУМЫСЫ

Темасы: Сыпатлы хызмет көрсетиўши байланыс тармағында мағлыўматларды қорғаў

Илимий басшысы:_____ Ахымбетов А.

Кафедра баслығы:_____ Бурханов Ш.А.

НӨКИС - 2012 ж.

Мазмуны

КИРИСИЎ

Информация ҳәм оны қайта ислеў технологиясы кәрханаларды эффектив басқарыўда ҳәм олардың искерлигинде айрықша әҳмийетке ийе. Компьютерлер кәрханалардың ҳәр қыйлы тараўларында қолланыла баслағаннан соң кәрханаларда бул компьютерлерди байланыстырып ҳәр қыйлы бөлимлердиң жумысының эффективлигин асырыў талабы келип шықты. Бирақ бул байланыс исенимли ҳәм қорғалған болыўы керек.

Internet технологияларының күнделикли турмысымызда кең түрде қолланылыўы кәрханалар ҳәм банклердиң коммерциялық ҳәм басқарыў мағлыўматларын узатыў ушын Internet каналларынан пайдаланыў қызығыўшылығы артты. Бирақ Internet тармағының дүзилиў принципи зыян келтириўши адамларға мағлыўматларды урлаў ҳәм мағлыўматларды өзгертиўге имканият жаратып береди. TCP/IP протоколы тийкарында дүзилген корпоратив ҳәм ведомоствалық тармақлар сыртқы ҳүжимнен кепилленбеген.

Тармақ ҳүжимлеринен сақлаў ушын ҳәм ашық тармақларды бизнес ҳәм банк тараўларында актив ҳәм қәўипсиз пайдаланыў ушын 1990-жыллардың басында виртуаль жеке тармақлар VPN (Virtual Private Network) пайда болды. «Виртуаль» сөзи VPN терминине бундай түрдеги байланысыў ўақтынша екенлигин аңлатады.

Виртуаль жеке тунеллердиң техникалық әмелге асырылыўының тарийхы еки бағдар бойынша алып барылды:

- бир тармақ ишиндеги еки түйини арасында басқа пайдаланыўшылардан ажыратылған жалғаныўлар бирикпесин (frame relay яки ATM) виртуаль каналларды шөлкемлестириў мехнизмин қолланыў арқалы қурыў;

- тунеллеў технологиясын қолланыў арқалы тармақтың еки түйини арасында виртуаль IP-туннелди қурыў.

Виртуаль жеке тармақларды қурыўдың биринши замангөй технологиясы бул кадрларды трансляциялаў хызмети (frame relay) болып табылады. Бирақ frame relay тармағы мобил пайдаланыўшылар талабын қанаатландыра алмады ҳәм кәрханалар модемли байланыстан пайдаланыўға мәжбур болды. Бул өз гезегинде мобил байланыс ҳәм аралықтан кириўге талаптың өсиўи менен сезилерли машқалаға айланды.[7]

Улыўмалық (қорғалмаған) тармақ арқалы түйинлерди байланыстырыўшы тармақ сервислери пайда болғаннан соң, Internet тийкарында виртуаль жеке тармақлар (қорғалған) VPN бул мәселелердиң шешими ретинде қолланылды. Бул шешим алдынғыларынан арзан есапланады. Енди жер шарының қәлеген жеринен, Internet тармағына жалғанған инсан банк пенен байланыса алады. Internet тармағының ашық, қорғалмағанлығынан VPN тармағында VPN хостлары арасында мағлыўматларды узатыўда мағлыўматларды қорғаў қураллары киритилген.

Бул питкериў қәнигелик жумысында сыпатлы хызмет көрсетиўши байланыс тармағында мағлыўматларды қорғаў мәселеси қарастырылады. Питкериў қәнигелик жумысы кирисиў бөлиминен, төрт параграфтан, жуўмақлаў бөлиминен ҳәм пайдаланылған әдебиятлар дизиминен ибарат.

Питкериў қәнигелик жумысы келеси мазмунға ийе:

Питкериў қәнигелик жумысының биринши параграфында виртуаль, қорғалған VPN тармақларды қурыўдың концепциясы қарап өтилген.

Питкериў қәнигелик жумысының екинши параграфында қәўипсизликти шөлкемлестириўдиң улыўма сиясаты мәселелери келтирилген.

Питкериў қәнигелик жумысының үшинши параграфында OPENVPN программалық тәмийнлеўи тийкарында виртуаль жеке тармағын жаратыўға мысал келтирилген.

Питкериў қәнигелик жумысының төртинши параграфында VPN клиентлерин сазлаў ҳаққында айтып өтилген.

Питкериў қәнигелик жумысының жуўмақлаў бөлиминде жумыста алынған нәтийжелердиң жуўмағы жазылған.

§1. ВИРТУАЛЬ, ҚОРҒАЛҒАН VPN ТАРМАҚЛАРДЫ ҚУРЫЎДЫҢ КОНЦЕПЦИЯСЫ

VPN виртуаль тармақларды қурыў концепциясы тийкарының мәниси жеткиликли әпиўайы: егерде глобал тармақта бир-бири менен мағлыўмат алмасыўы зәрүр болған еки түйин бар болса, онда бул еки түйин арасында мағлыўматлардың конфиденциаллығын ҳәм пүтинлигин сақлаўшы виртуаль қорғалған тунелди қурыў керек. Бул виртуаль тунелге мүмкин болған сыртқы актив ҳәм пассив бақлаўшылар кире алмаўы керек.

Банклер бундай тунеллерди қурыў арқалы биринширен жеткиликли қаржыны үнемлейди, себеби бул жағдайда банк қымбат ажыратылған каналларды қурыў яки арендалаўдан азат етиледи. Буның орнына өзлеринде бар Internet каналарынан пайдаланады. Ҳәзирги күнде бундай каналлар ажыратылған линиялардан тезлиги ҳәм исенимлилиги бойынша дерлик парықланбайды.

1.1.VPN тармағының тийкарғы түсиниклери ҳәм функциялары

Корпоратив локал тармақты ашық глобал тармаққа жалғағанымызда қәўипсизликтиң келеси тийкарғы еки түрдеги қәўиплери жүзеге келеди:

- Корпоратив локал тармақтың ишки ресурсларына рухсатсыз сырттан кириў ҳәм ишки мағлыўматларға қәўип туўдырыў;

- корпоратив мағлыўматларды ашық қорғалмаған тармақ бойынша узатыўда жолда рухсатсыз урланыўы яки өзгериўи;

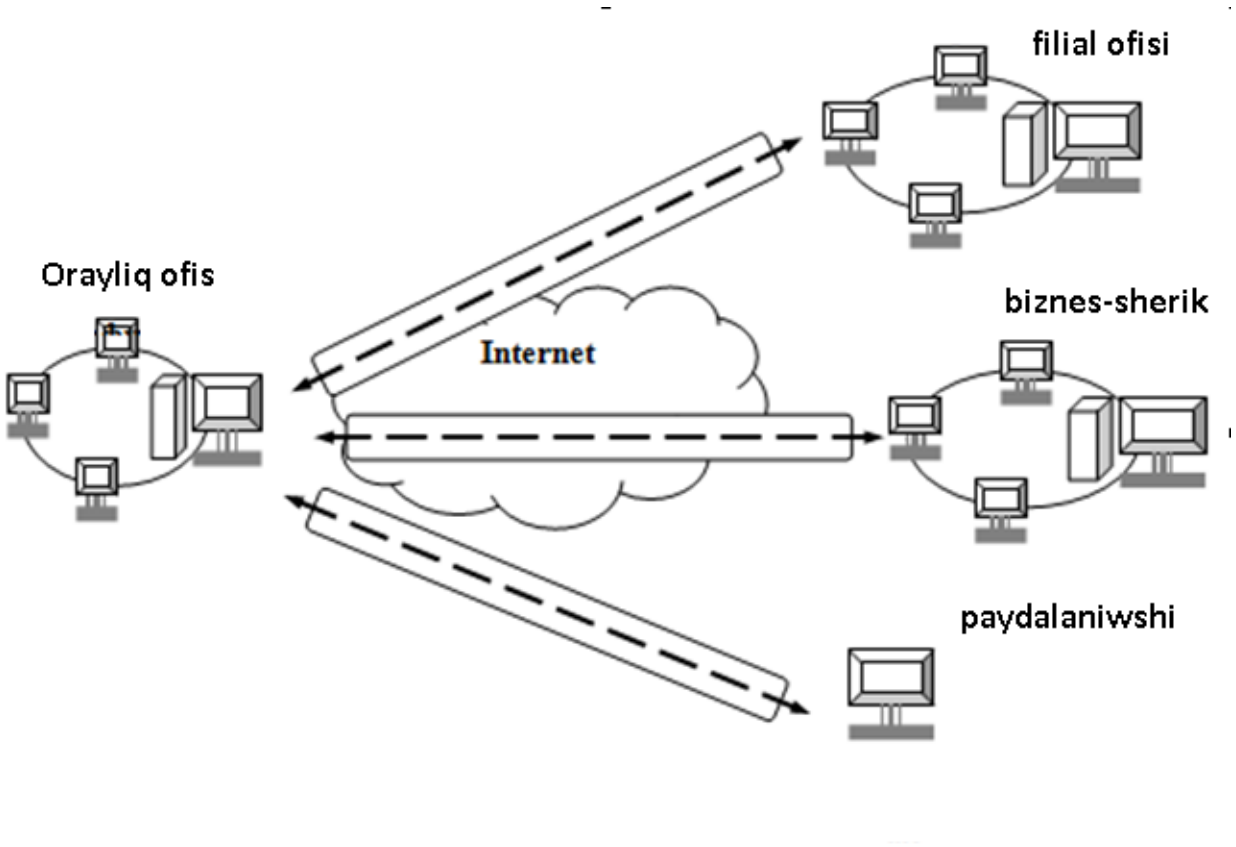
Локал тармақлардың ҳәм жеке компьютердиң ашық қорғалмаған тармақта, атап айтқанда Internet тармағында мағлыўматлар алмасыўының қәўипсизлигин тәмийинлеў келеси мәселелерди эффектив шешиў арқалы әмелге асырылады:

- ашық байланыс каналларына жалғанған локал тармақлар ҳәм жеке компьютерлерге сыртқы орталықтан рухсатсыз кириў ҳәм әмеллерди орынлаўдан қорғаў;

- мағлыўматларды ашық қорғалмаған байланыс каналлары бойынша узатыў процессинде қәўипсизлигин тәмийинлеў;

Ашық байланыс каналларына жалғанған локал тармақлар ҳәм жеке компьютерлерге сыртқы орталықтан рухсатсыз кириўден сақлаў ушын еки тәреплеме өтиўши пакетлер ағымын филтрлеў арқалы қәўипсизликти тәмийнлеўши тармақлар аралық экранлар (firewalls) қолланылады. Тармақлар аралық экранлар еки ашық ҳәм локал тармақтың бир-бирине жалғанған жеринде жайласады. Ашық байланыс каналына жалғанған жеке компьютерди қорғаў ушын тармақлар аралық экранның программасы орнатылады ҳәм персонал деп аталады. [2]

Мағлыўматларды ашық қорғалмаған байланыс каналлары бойынша узатыў процессинде қәўипсизлигин тәмийинлеў виртуаль қорғалған VPN тармақларды қолланыўға тийкарланады. Виртуаль қорғалған VPN тармағы деп ашық қорғалмаған тармақ арқалы локал тармақлар ҳәм жеке компьютерлердиң мағлыўмат алмасыў қәўипсизлигин тәмийинлеўши жалғыз виртуаль корпоратив тармағына бирлесиўине айтамыз. Виртуаль корпоратив тармақ VPN виртуаль қорғалған каналларды қурыў арқалы дүзиледи. Бул виртуаль қорғалған байланыс каналларды VPN тунеллери деп аталады. VPN тармағы VPN тунеллери жәрдеминде орайлық офисти, филиаллар офисин, бизнес-шериклер офисин ҳәм аралықтағы пайдаланыўшыларды байланысытырыўды ҳәм Internet арқалы мағлыўматларды қәўипсиз узатыў мүмкиншилигин береди (сүўрет. 1.1).



Сүўрет 1.1- VPN виртуаль қорғалған тармағы

VPN тунели ашық қорғалмаған тармақ арқалы виртуаль тармақтың криптографиялық қорғалған пакетлер узатылыўшы жалғаныў болып есапланады. VPN тунели бойынша узатылыў процессиндеги мағлыўматлардың қәўипсизлиги келеси функцияларды орынлаўға тийкарланады:

- мағлыўмат алмасыўшы тәреплердиң аутентификациясы;
- узатылыўшы мағлыўматлардың криптографиялық жабылыўы (шифрлаў);
- жеткизилип берилиўши мағлыўматтың исенимлилигин ҳәм пүтинлигин тексериў;

Бул функциялар ушын өз-ара байланысыў зәрүр. Оларды әмелге асырғанда мағлыўматларды криптографиялық қорғаў методлар қолланылады. Бундай системаның эффективлигине симметриялық ҳәм асимметриялық криптографиялық системаларды биргеликте қолланыў есабынан ерисиледи.

VPN қурылмалары тәрепинен жаратылған VPN тунеллери қорғалған ажыратылған линия қәсийетлерине ийе болады. VPN қурылмалары виртуаль жеке тармақларында VPN-клиент, VPN-сервер яки қәўипсизлик шлюзи ретинде қолланылыўы мүмкин.[5]

VPN-клиент – бул жеке компьютер базасында орынланыўшы программалық яки аппаратлық-программалық комплекс болып табылады. Екинши VPN-клиент пенен, VPN-сервер яки VPN қәўипсизлик шлюзи менен мағлыўмат алмасыўы ушын оның тармақлық программалық тәмийинлениўи шифрлаўды, трафикти аудентификациялаўды орынлаў ушын өзгертиледи. Әдетте VPN-клиентиниң программалық тәмийинлениўи Windows, Linux яки UNIX операциялық системасының қурамына қосымша ретинде киритиледи.

VPN-сервер – бул сервер ўазыйпасын атқарыўшы компьютерде орнатылған программалық яки аппаратлық-программалық комплекс болып табылады. VPN-сервер серверди сыртқы тармақлардан рухсатсыз кириўден сақлайды, локал тармақ сегментиндеги ҳәм жеке компьютерлер арасында қорғалған жалғаныўларды шөлкемлестиреди. VPN-сервер мобил пайдаланыўшылар менен қорғалған жалғаныўды шөлкемлестириў мүмкиншилигине ийе.

VPN қәўипсизлик шлюзи (security gateway) – бул еки тармаққа жалғаныўшы, көплеген хостлар ушын шифрлаў ҳәм аудентификациялаў функцияларын атқарыўшы тармақ қурылмасы. VPN қәўипсизлик шлюзи ишки корпоратив тармағына арналған барлық трафик VPN қәўипсизлик шлюзинен өтетуғындай етип жайластырылады. VPN қәўипсизлик шлюзиниң жалғаныўы шлюз артындағы пайдаланыўшылар ушын мөлдир. VPN қәўипсизлик шлюзиниң адреси кириўши тунелленiўши пакеттиң сыртқы адреси сыяқлы, ал пакеттиң ишки адресине шлюз артындағы конкрет хосттың адреси жазылады. VPN қәўипсизлик шлюзи жеке программалық шешим сыяқлы, жеке аппаратлық қурылма сыяқлы, сондай-ақ маршрутизатор яки қосымша функциялар менен толтырылған тармақлар аралық экран сыяқлы әмелге асырылыўы мүмкин. [1]

1.2.VPN тармақларының классификациясы

Ҳәзириг ўақытта VPN виртуаль қорғалған жеке тармақларды қурыў технологиялары ири компанияларды (банклер, ведомствалар, мәмлекетлик структуралар) көбирек қызықтырады. Себеби VPN-технологиялары компания офислери арасында ҳәм жеке жумыс станциясы ҳәм серверлери арасында қорғалған тунелди шөлкемлестириў мүмкиншилигин береди. Бунда конкрет жумыс станциясы қорғалған ресурсларға Internet тиң қайсы провайдери жәрдеминде жалғаныўы әҳмийетли емес. Қапталдан бақлаўшы ушын мазмунын оқып болмайтуғын әдеттеги IP-пакет ағымын көреди. [3]

VPN классификациясының ҳәр қыйлы вариантлары бар. Классификацияның келеси үш белгиси қолланылады:

- OSI моделиниң жумыс дәрежеси;
- VPN ниң техникалық шешиминиң архитектурасы;
- VPN ди техникалық әмелге асырыў усылы.

1.3.OSI моделиниң жумыс дәрежеси бойынша классификациялаў

Ашық қорғалмаған тармақ бойнша мағлыўматларды қәўипсиз узатыў технологияларды улыўма қорғалған канал (secure channel) деп атайды. «Канал» термини пакетлерди коммутациялаў тармағында дүзилген қандайда виртуаль жол бойлап мағлыўматларды қорғаў тек тармақтың еки түйини (хостлар яки шлюзлер) ушын тәмийинлениўин аңлатады. Қорғалған каналды OSI моделиниң ҳәр қыйлы дәрежелеринде әмелге асырылған системалық қураллар жәрдеминде қурыў мүмкин.(Кесте 1.1).

OSI моделиниң жумыс дәрежеси бойынша VPN ди классификациялаў әҳмийетли себеби таңланған OSI моделиниң жумыс дәрежесинен қурылыўшы VPN тармағының искерлиги ҳәм корпоратив информациялық

тармақтың программалары ҳәм басқада қорғаўшы қураллары менен сәйкеслиги ғәрезли болады.

Кесте 1.1 – Қорғалған канал протоколларының дәрежелери

<table>
<tr><td rowspan="7">Қорғалған канал протоколлары</td><td>Әмелий</td><td rowspan="3">Программаларға тәсир етеди</td></tr>
<tr><td>Ўәкиллик</td></tr>
<tr><td>Сеанслы</td></tr>
<tr><td>Транспортлы</td><td></td></tr>
<tr><td>Тармақлық</td><td rowspan="3">Программалар ушын мөлдир</td></tr>
<tr><td>Каналлы</td></tr>
<tr><td>Физикалық</td></tr>
</table>

OSI моделиниң жумыс дәрежеси бойынша келеси VPN топарларын ажыратамыз:

- канал дәрежесиндеги VPN;
- тармақ дәрежесиндеги VPN;
- сеанс дәрежесиндеги VPN.

VPN OSI моделиниң жеткиликли төмен дәрежелеринде дүзиледи. Буның себеби әпиўайы: қорғалған каналдың қураллары қаншелли төмен дәрежеде әмелге асырылса, оларды программалар ушын мөлдир етиў соншелли аңсат болады. Тармақ ҳәм канал дәрежелеринде программалардың протоколлардан ғәрезлилиги пүткиллей жоғалады. Сонлықтан пайдаланыўшы ушын универсал мөлдир қорғаўды қурыў тек моделдиң төмен дәрежелеринде мүмкин. Бирақ бунда екинши машқала жүзеге келеди – қорғаў протоколының конкрет тармақ технологиясынан ғәрезлилиги. Егерде мағлыўматларды қорғаў ушын жоқары дәрежелердиң биринде (әмелий яки сеанслы) протокол қолланылса, онда қорғаўдың бундай усылы мағлыўматларды тасыў ушын қандай тармақ (IP яки IPX, Ethernet яки ATM) қолланылыўынан ғәрезсиз болады. Бунда бир жағынан программалар қорғаўдың конкрет протоколынан ғәрезли болып қалады, яғный мөлдир емес.

Қорғалған канал ең жоқарғы әмелий дәрежеде және бир кемшиликке ийе – ҳәрекет етиў области шекленген. Протокол белгиленген тармақ хызметин қорғайды – файллы гипертекстли яки почта. Мәселен S/MIME протоколы тек электрон почта хабарларын қорғайды. Сонлықтан ҳәр бир хызмет ушын сәйкес қорғаўшы протоклды ислеп шығыў зәрүр. [3]

1.4.Техникалық шешим архитектурасы бойынша классификациялаў

Техникалық шешиминиң архитектурасы бойынша виртуаль жеке тармақлардың тийкарғы үш түрин ажыратамыз:

- корпоратив тармақ ишиндеги VPN;
- аралықтан кириўши VPN;
- корпоратив тармақлар аралық VPN;

Корпоратив тармақ ишиндеги VPN тармақлары (Intranet VPN) бир корпоратив тармаққа бириккен кәрхана ишиндеги бөлимлер арасында яки кәрханалар топары арасында қорғалған мағлыўмат алмасыўды тәмийинлеў ушын арналған.

Аралықтан кириўши виртуаль жеке VPN тармақлары (Remote Access VPN) корпоратив информациялық ресурсларға компанияның мобил яки аралықтағы (home-office) хызметкерлериниң қорғалған мағлыўмат алмасыўды тәмийинлеў ушын арналған.

Корпоратив тармақлар аралық VPN тармақлары (Extranet VPN) стратегиялық бизнес-шериклер, ири буйыртпашылар, пайдаланыўшылар, клиентлер ҳ.т.б. менен менен қорғалған мағлыўмат алмасыўды тәмийинлеў ушын арналған. Extranet VPN бир компания тармағынан екинши компания тармағына туўры байланысты тәмийинлйди.

1.5. Техникалық әмелге асырыў усылы бойынша классификациялаў

VPN ди техникалық әмелге асырыў усылы бойынша келеси VPN топарларын ажыратамыз:

- маршрутизаторлар тийкарындағы VPN;

- тармақлар аралық экран тийкарындағы VPN;

- программалық шешимлер тийкарындағы VPN;

- арнаўлы қәнигелестирилген қурамында шифропроцессорға ийе аппаратлық қурылмалар тийкарындағы VPN

Маршрутизаторлар тийкарындағы VPN. VPN ди бундай етип қурыў усылы маршрутизаторларды қорғалған каналларды қурыў ушын пайдаланыўды усынады. Локал тармақтан шығыўшы барлық мағлыўмат маршрутизатор арқалы өтетуғын болғанлықтан, оған шифрлаў мәселесин жүклеўимизге болады. Маршрутизаторлар тийкарындағы VPN ди қурыўшы қурылмаға мысал ретинде Cisco Systems компаниясының қурылмаларын келтирсек болады.

Тармақлар аралық экран тийкарындағы VPN. Көпшилик тармақлар аралық экранлар тунеллеў ҳәм шифрлаў функцияларын қоллайды. Бундай - тармақлар аралық экранға мысал ретинде Check Point Software Technologies компаниясының Fire Wall-1 программасын келтирсек болады. Жеке компьютер базасындағы тармақлар аралық экранларды пайдаланғанда бундай шешим салыстырмалы киши мағлыўматларды узатыў көлемине ийе киши тармақлар ушын туўры келиўин умытпаўымыз керек.

Программалық шешимлер тийкарындағы VPN. Программалық усыл менен әмелге асырылған VPN-өнимлер өнимдарлық көз-қарасынан арнаўлы қәнигелестирилген қурылмалардан артта. Бирақ VPN-тармағын шөлкемлестириў ушын жеткилики қуўатлылыққа ийе. Аралықтан кириў жағдайында зәрүр өткериў уқыплылығына талабы онша үлкен емес. Сонлықтан аралықтан кириў ушын программалық шешимлер қолай болып есапланады.

Программалық шешимлер тийкарындағы VPN ниң жетискенлиги: пайдаланыў ушын қолайлы ҳәм бейимлесиўшеңлиги, сондай-ақ баҳасының арзанлығы. [3]

Арнаўлы қәнигелестирилген қурамында шифропроцессорға ийе аппаратлық қурылмалар тийкарындағы VPN. Арнаўлы қәнигелестирилген қурамында шифропроцессорға ийе аппаратлық қурылмалар тийкарындағы VPN ниң тийкарғы жетимкенлиги олардың өнимдарлылығы болып табылады. Бундай өнимдарлылық арнаўлы қәнигелестирилген қурамында шифропроцессорға ийе аппаратлық қурылмалар тийкарындағы VPN – системаларында шифрлаў арнаўлы қәнигелестирилген микросхемалар тийкарында алып барылыўы менен түсиндириледи. Арнаўлы қәнигелестирилген қурамында шифропроцессорға ийе аппаратлық қурылмалар қәўипсизликтиң жоқары дәрежесин тәмийинлейди, лекин олар жүдә қымбат турады.

§2. ҚӘЎИПСИЗЛИКТИ ШӨЛКЕМЛЕСТИРИЎДИҢ УЛЫЎМА СИЯСАТЫ

2.1.Корпоратив тармақлардағы мағлыўматларды қорғаў стратегиялары

Мағлыўматлара қәўипти қәлеген шахс, объект яки әмелге асырылыўы нәтийжесинде локал есаплаў тармағына үлкен зыян келтириўи мүмкин болған ўақыя туўдырыўы мүмкин. Қәўип зыян келтириў мақсетинде алдын ала жобаластырылған яки есаплаўлардағы қәтелер яки файллардың тосынанлы өшип кетиў нәтийжесиндеги тосынанлы болыўы мүмкин. Қәўип тәбийий қубылыс болыўы да мүмкин. Мәселен суў тасып кетиў, жасын, дүбелей ҳ.т.б.

Локал есаплаў тармағының әззи жерлери қәўипли жерлер саналады. Мәселен локал есаплаў тармағына әпиўайы паролди анықлаған бөтен инсан тәрепинен кириўи ҳәм тармақ ресурсларынан пайдаланыўы мүмкин. Бул жерде әззи жер ретинде пайдаланыўшы тәрепинен әпиўайы етип қойылған парол болып табылады. Локал есаплаў тармағының әззи жерлерин азайтыў яки шеклеў локал есаплаў тармағына қәўипти азайтады яки улыўма сапластырады. Мәселен пайдаланыўшылар ушын қурамалы паролди ойлап табыўға жәрдем бериўши қурал пайдаланыўшылар әпиўайы паролден пайдаланыў итималлығын кемитеди ҳәм нәтийжеде локла есаплаў тармағына қәўипти азайтады.

Қорғаў хызмети локал есаплаў тармағын конкрет қәўиптен қорғаўшы механизмлер ҳәм шөлкемлестириў қағыйдалары бирикпесинен турады. Мәселен аутентификациялаў ҳәм идентификациялаў хызмети пайдаланыўшыны идентификациялаўды ҳәм өзиниң идентификаторының ҳақыйқый екенлигин тастыйықлаўды талап ете отырып, локал есапаў тармағын авторизацияланбаған кириўден сақлайды. Қорғаў қуралын қураўшы механизмлер, процедуралар ҳ.т. басқалар қаншелли исенимли болса, қорғаў қуралыда соншелли исенимли болады.

Әмелията пайдаланылатуғын қорғаў механизмлериниң көпшилиги криптография усылларына тийкарланған. Шифрлаў ёки шифрлаўға жақын болған мағлыўматты өзгертиўлер мағлыўматларды қорғаў усыллары есапланады. [6]

2.1.1.Қорғаныўдың бузылыўы

Компьютер системаси яки тармағы қәўипсизлигин бузыўға урынысларды, компьютер системасын мағлыўматларды тәмийинлеўши объект сыпатында қараў арқалы классификациялаў мүмкин. Улыўма жағдайда қандайда бир деректен (мәселен, файл яки яд бөлими) мағлыўмат ағымының адресатқа (мәселен, басқа файл яки тиккелей пайдаланыўшы) узатылыўы бақланады. Усы көз-қарастан төмендеги ҳүжимлерди ажыратыў мүмкин:

- Үзиў;
- Услап алыў;
- Түрлендириў;
- Қәлбекилестириў.

Үзиў. Система ресурсы жоқ қылынады, мағлыўматтан пайдаланыў бузылады. Бундай бузылыўларға мысал ретинде үскененің истен шығыўы, байланыс линиясының үзилиўи яки файлларды басқарыўшы системаның бузылыўын көрсетиў мүмкин.

Услап алыў. Ресурстан рухсат етилмеген пайдаланыўға жол ашылады. Нәтийжеде мағлыўматтың сырлылығы (конфиденциаллығы) бузылады. Бундай пайдаланыўшылар физикалық шахс, программа яки компьютер болыўы мүмкин. Бундай бузылыўларға мысал ретинде мағлыўматларды услап алыў мақсетинде байланыс кабелине жалғаныў ҳәм файллардан яки программалардан нызамсыз копиялаўды көрсетиў мүмкин.

Түрлендириў. Ресурстан тек нызамсыз пайдаланыўға жол қойылмастан, ресурс бузыўшы тәрепинен өзгертириледи. Нәтийжеде мағлыўматтың пүтинлиги бузылады. Бундай бузылыўларға мысал ретинде файлдағы мағлыўматлар мазмунының өзгериўин, программаның ўазыйпалары ҳәм

характеристкаларын өзгертиў мақсетинде оны модификациялаўды, тармақ арқалы узатылыўшы мағлыўматлар мазмунын өзгертиўлерди ҳ.т.б. көрсетиў мүмкин.

2.2.VPN ВИРТУАЛЬ ЖЕКЕ ТАРМАҒЫНА ҲҮЖИМЛЕР

2.2.1.Криптографиялық алгоритмлерге ҳүжимлер

Ҳәзирги ўақытта барлық алгоритмлерди шәртли еки категорияға бөлиўимиз мүмкин: белгили ҳәм сырлы. Белгили алгоритмлерге DES, TripleDES, RSA, AES ҳәм ГОСТ 28147-89 алгоритмлери киреди. Бул алгорритмлер қәнигелерге бурыннан белгили. Қәнигелер олардың күшли ҳәм әззи тәреплерин жақсы биледи.

Криптоалгоритмлерге ҳүжим түрлери жүдә көп. Олардың ең әпиўайысы тек шифрланған текстке ҳүжим. Бунда криптоаналитик тек шифрланған текстке ийе болады ҳәм символлардың статистикалық бөлистирилиўин анализлеў ҳәм басқада методларды қолланып шифрланған текстти оқыўға ҳәрекет қылады. Қәлеген алгоритм бундай ҳүжимнен қорғаўы керек. Қурамалырақ ҳүжимлерге белгили шифрланбаған текстке ийе болған ҳүжим. Бул жағдайда криптоаналитикке берилген текстиң бир фрагменти белгили. Мәселен бул ҳүжжетиң стандарт басланыўы яки тамамланыўы болыўы мүмкин: «Конфиденциал», «Ҳүрметили», «Ҳүрмет пенен». Бунанда қурамалырақ ҳүжим түрлери бар, мәселен дифференциал криптоанализ. Ҳәзирги күнде кең тарқалған алгоритмлердиң көпшилиги бундай ҳүжимлерге қарсы тура алады. [5]

Сырлы патентленген яки уникал алгоритмди пайдаланыў оптимал шешим бола алмайды. Өткен мың жыллықта дәлилленгениндей криптографиялық алгоритмниң турақлылығы оның сырлылығы менен емес ал гилти менен анықланады. Сонлықтан криптографиялық алгоритмди жәмийеттен қанша жасырсақ оның исенимлилигине соншелли гүман туўдырылады.

2.2.2.Криптографиялық гилтлерге ҳүжим

Жоқарыда айтып өткен ҳүжимлердиң екеўиде ҳәзирги ўақытта пайдаланылыўшы криптографиялық алгоритмлер алдында дерлик күшсиз. Себеби криптоаналитик текстти оқыў ушын мүмкин болған барлық гилтлерди тексериўине туўра келеди. Сонлықтан жеткиликли узынлықтағы гилтке ийе криптографиялық алгоритмди таңлаў үлкен әҳмийетке ийе. 2.1-кестесинде криптоаналитик симметриялық алгоритлерди (DES, AES, ГОСТ 28147-89) дешифрлаў ушын мүмкин болған барлық криптографиялық гилтлерди тексериўге сарпланатуғын ўақыт келтирилген. Бул кестеден көринип турғанындай ГОСТ 28147-89 алгоритмин 256 гилт узынлығында жақын келешекте «бузыў» мүмкин емес, ал қалғанларын салыстырмалы «бузыў» аңсат.

Кесте-2.1. Мүмкин болған барлық криптографиялық гилтлерди тексериўге сарпланатуғын ўақыт

Криптоаналитик категориясы	**Технология**	**Сарпланатуғын ўақыт**	
		40 бит	**56 бит**
Жеке хакер	Жеке компьютер	1 ҳәпте	Мүмкин емес
Хакер топарлары	FPGA технологиясы	5 саат	38 жыл
Киши фирмалар	FPGA технологиясы	12 минут	18 ай
Ири фирмалар	FPGA технологиясы	24 секунд	19 күн
	ASIC технологиясы	18 секунд	3 күн
Ири корпорациялар	FPGA технологиясы	7 секунд	13 саат
	ASIC технологиясы	0,005 секунд	6 минут

Асимметриялық алгоритмлер үлкен узынлықтағы гилтлерди пайдаланады. 2.2-кестесинде мағлыўматлардың қәўипсизлигин тәмийинлеў

дәрежеси бойынша бир-бирине сәйкес симметриялық ҳәм асимметриялық гилтлердиң узынлықлары келтирилген.

Кесте-2.2. Симметриялық ҳәм асимметриялық алгоритмлердиң гилтлердиң узынлықлары

Симметриялық алгоритм ушын гилт узынлығы	Асимметриялық алгоритм ушын гилт узынлығы
56 бит	385 бит
64 бит	512 бит
80 бит	768 бит
112 бит	1792 бит
128 бит	2304 бит

Гилт узынлығы қорғалыўшы мағлыўмат қаншелли сырлы сақланыўы кереклигинен ғәрезли болады. Егерде бул бирне неше жыллар даўамында сақланыўы керек болған жеке мағлыўматлар яки бизнес-проектлер болса онда гилт узынлығы оларды қорғаў ушын үлкен болыўы керек. Егерде бул оператив мағлыўмат болса мәселен акциялар кодировкалары яки әкерий тактикалық план ҳаққында мағлыўмат болса, онда бул мағлыўмат бир неше сааттан яки минуттан кейин өзиниң актуаллығын жоғалтатуғынлығын есапқа алып гилт узынлығын онша үлкен емес етип алыўға болады.

Душпанның криптоаналитиклери баллистикалық ракета берилген ноқатқа 8 минуттан кейин барып түсетуғынлығы ҳаққында хабарды 10 минуттан кейин дешифрлады. Бундай мағлыўматтың актуаллығы дерлик нолге тең.

2.2.3.VPN протоклларына ҳүжим

Ҳәзирги ўақытта VPN виртуаль жеке тармағын жаратыў ушын бир қатар протоколлар қолланылады: IPSec, PPTP, L2TP ҳәм т.б. Бул протоколар мағлыўматларды шифрламайды олар тек шифрлаў алгоритмлери қалай пайдаланылыўын ҳәм VPN ди қурыў ушын зәрүр болған бир қатар шәртлерди (пүтинликти қадағалаў, абонентлерди аудентификациялаў)

анықлайды. Қәўипсизлик тараўындағы бир қатар қәнигелер бул протоколларды қәўипсизлик көз-қарасынан анализледи ҳәм әззи жерлерин таба алмады. Анықланғанлары я пайдаланыўшылардың дурыс емес эксплутациясы нәтийжесинде яки ислеп шығарыўшылар тәрепинен бул кемшиликлер сапластырылған. Бирақ бәри бир VPN де пайдаланылыўшы протоколлардың әззи жерлери теориялық жақтан жоғалмайды.

2.2.4.Исленбелерге ҳүжим

Бул түрдеги ҳүжим хакерлер тәрепинен кең қолланылады. Буның себеби ҳүжимди әмелге асырыў ушын математика тараўында кең түсиникке ийе болыў шәрт емес. Тек маман программашы яки инсанның әззи жерлерин билиў талап етиледи. Ҳүжим етиўине жол қойып бериўши дурыс емес исленбелерге мысаллар:

- Шифрлаўдың жабық гилти компьютердиң қатты дискинде сақланады. Ал бул компьютерден пайдаланыўды ҳәш ким қадағаламайды.

- Оператив ядтағы криптографиялық гилт пайдаланылып болынғаннан соң өширилмейди.

- Сеанслық гилтлердиң қәўипсизлиги тәмийинленген, ал тийкарғы гилтлердиң қәўипсизлигине жеткиликли итибар қаратылмаған.

- VPN программалық комплексиниң пүтинлиги қадағаланбайды. Бул жаман ойдағы инсанның шифрлаўға яки тармақ арқалы алынатуғын пакетлердиң пүтинлигине жуўап беретуғын программалық тәмийинлеўди өзгертиўине мүмкиншилик туўдырады.

Төменде конкрет анықланған дурыс емес исленбелер келтириледи:

- PPTP ны әмелге асырыўда әззилик. Windows NT операциялық системасында, WatchGuard Firebox II тармақлар аралық экранында, Cisco ҳәм BinTec маршрутизаторларда «Хызмет көрсетиўден бас тартыў» жағдайына алып келеди.

- OpenBSD операциялық системасында AH/ESP (IPSec тиң арнаўлы режимлери) пакетлериниң дурыс емес ислеўи нәтийжесинде «Хызмет көрсетиўден бас тартыў» жағдайына алып келди.

- Windows 2000 операциялық системасында IPSec ушын IKE гилтлери менен алмасыў протоколында әззилик анықланды.

Сондай-ақ VPN ди қураўшы тек программалық тәмийинлеўге емес ал аппаратлық элементлерге де ҳүжим жасалады. Мәселен Touch Memory таблеткаларына, смарт-карталарға ҳәм басқада криптографиялық гилтлерди тасыўшыларға.

2.2.5.VPN қурылмаларына ҳүжим

Көпшилик жағдайларда VPN алдыннан бар қурылып турған тармақ қурылмалары базасында жаратылады. Әдетте маршрутизаторлар (мәселен, Cisco 1720) яки аппаратлы-программалық тармақлар аралық экранлар (мәселен, Nokia IP Security Solutions платформасы базасындағы CheckPoint VPN-1). Сондай-ақ қәнигелестирилген VPN ди жаратыў қурылмаларыда пайдаланылады (мәселен, «Континент-К»). Бул қурылмалар TCP/IP стегин қоллаўынан оларға «хызмет көрсетиўден бас тартыў» (DOS-ҳүжим) ҳүжимин жасаў "отказ в обслуживании" (DOS-атака) мүмкин. Буның нәтийжесинде қурылманың өзиниң жумысы ҳәм оның жәрдеминде қорғалыўшы тармақтың ҳәм түйинлердиң өз-ара жумысы ўақтынша бузылады. [1]

2.2.6.Операциялық системаларға ҳүжим

Көпшилик жағдайда VPN программалық қураллар жәрдеминде жаратылады. Ҳәм VPN ди жаратыўшы программалық қураллар операциялық системаның қурамына киргизилген болады. Ал бул хакерлер тәрепинен жийи қолланылады. Себеби VPN ниң қаншелли исенимли қорғалғаны менен операциялық системаның әззи жерлери арқалы системаға кириў VPN ниң

барлық қорғаў механизмлерин жоққа шығарады. Бул әсиресе Microsoft операциялық системаларына тийисли.

2.2.7.Пайдаланыўшыларға ҳүжим

Ақырғы пайаланыўшы VPN элементи болып есапланатуғынлығын ҳәм оғанда басқа элементлер қатарында ҳүжим жасаў мүмкин екенлигин естен шығармаў керек. Пайдаланыўшы билмеген ҳалда сырлы гилтлер сақланған USB флешка яки басқа мағлыўмат тасыўшыны бөтен адамға бериўи яки жоғалтып алыўы мүмкин ҳәм бул ҳаққында зәрүр ўақытқа шекем хабар бермеўи мүмкин.

Айрым системаларда пайдаланыўшылар өзлери ушын өзи шифрлаў ушын гилтлерди жаратыўы мүмкин. Гилтти генерациялаў пайдаланыўшы таңлаған паролге тийкарланады. Пайдаланыўшылардың қурамалы парольди таңлаў фантазиясы жүдә төмен. Сонлықтан олар әдетте ядта жақсы сақланатуғын сөз яки гәплерди таңлайды, ал бул болса хакерлер тәрепинен аңсат табылады.

§3. OPENVPN ТИЙКАРЫНДА ВИРТУАЛЬ ЖЕКЕ ТАРМАҒЫН ЖАРАТЫЎ

Мәселениң қойылыўы

Компанияның Интернетке жалғанған бирнеше офислери арасында виртуаль жеке тармақты жаратыў талап етиледи.

3.1.OpenVPN технологиясы ҳаққында улыўма түсиниклер

OpenVPN – бул SSL/TLS протоколын яки бөлистирилген гилтлерди пайдаланып клиент/сервер VPN ҳәм site-to-site VPN тармақларын қурыў ушын пайдаланылатуғын ашық кодлы қурал болып табылады. OpenVPN Интернет сыяқлы ашық қорғалмаған тармақта бир TCP/UDP порт арқалы мағлыўматларды узатыў ушын қәўипсиз туннел хызметин атқарады. OpenVPN дерлик қәлеген платформаға орнатылыўы мүмкин. Атап айтқанда: Linux, Windows 2000/XP/Vista/7, OpenBSD, FreeBSD, NetBSD, Mac OS X ҳәм Solaris.

Linux системалары 2.4 яки оннан үлкен болған ядрода ислеўи керек. Конфигурациялаў принципи барлық платформалар ушын бирдей. OpenVPN клиент/сервер архитектурасын пайдаланады. OpenVPN VPN тармағының барлық түйинлерине орнатылған болыўы зәрүр. Бунда бир түйин сервер хызметин ал қалғанлары клиент хызметин атқарады. OpenVPN TCP яки UDP тунелин жаратады ҳәм усы туннел бойынша мағлыўматлар өткенинде шифрланады. OpenVPN ушын стандарт порт - UDP 1194, бирақ қәлеген басқа TCP яки UDP портты пайдалыныўы мүмкин. OpenVPN серверинде 2.0. версиясынан баслап бир порттың өзин бир неше туннеллер ушын пайдаланыў мүмкин. Статикалық гилтлерди пайдаланғанда VPN шлюзлер бир гилтти мағлыўматларды шифрлаў ҳәм дешифрлаў ушын пайдаланады. Бул жағдайда сазлаў жүдә әпиўайы болып, бирақ гилтти жөнетиў ҳәм қәўипсизлиги машқаласы жүзеге келеди. Егерде кимде-ким бул гилтке ийе болса, онда ол мағлыўматларды дешифрлаўы мүмкин. Бул машқаладан қутылыў ушын Ашық Гилтлер Инфраструктурасынан (PKI) пайдаланыўымыз

керек. Бунда ҳәр бир түйин еки гилтке ийе болады: ҳәммеге белгили ашық гилт ҳәм тек ийесинде болатуғын жабық гилт. Бундай структураны шифрланған мағлыўматларды жөнетиўден алдын VPN түйинлерин аутентификациялаўшы OpenVPN қурамына кириўши OpenSSL пайдаланады. Төмендеги 4.1-кестесинде еки OpenVPN режимлериниң салыстырылыўы келтирилген

Кесте-3.1. OpenVPN режимлериниң салыстырылыўы: бөлистирилген гилтлер ҳәм SSL

OpenVPN режими	**Бөлистирилген гилтлер**	**SSL**
Шифрлаў:	Симметриялық	Асимметриялық/ Симметриялық
Әмелге асырыў:	Аңсат	Қурамалы
Тезлик:	Тез	әстен
Процессордың жүклениўи:	Киши	Жоқары
Гилтлер менен алмасыў:	Аўа	Яқ
Гилтлерди жаңалаў:	Яқ	Аўа
Түйинлерди аутентификациялаў:	Яқ	Аўа

3.1.1.Secure Sockets Layers

Secure Sockets Layer (SSL) – бул Интернет тармағы арқалы мағлыўматларды қәўипсиз узатыў мүмкиншилигин бериўши криптографиялық протокол. Оны қолланғанда сервер ҳәм клиент арасында қорғалған жалғаныў жаратылады. SSL дәслеп Netscape Communications компаниясы тәрепинен ислеп шығылды. Еки версиясы ислеп шығарылады v2 (1994) ҳәм v3 (1995). 2001 жылы IETFсатып алады ҳәм патентти жаңалайды. Соңғылығында SSL 3.0 протоколы тийкарында TLS деп аталған RFC 2246 стандарты ислеп шығарылды ҳәм қабылланды. Узатыўшы ҳәм

қабыллаўшының исенимлилигин тастыйықлаў ушын ашық гилтли шифрлаўды пайдаланады. Қәўипсиз хэш-функциялар ҳәм корректлеўши кодларды пайдаланыў есабынан мағлыўматларды исенимли узатылыўын қоллайды.

SSL еки дәрежеден ибарат. Көпдәрежели транспорт протоколының төмен дәрежесинде (мәселен, TCP) ол жазыў протоколы болып есапланады ҳәм ҳәр қыйлы протоколларды (SSL POP3, IMAP, XMPP, SMTP ҳәм HTTP сыяқлы протоколлар менен биргеликте жумыс ислейди) инкапсуляциялаў (яғный пакетти таярлаў) ушын қолланылады. Ҳәр бир инкапсуляцияланған протокол ушын ол сервер ҳәм клиент бир-бирине өзлериниң ҳақыйқыйлығын тастыйықлай алатуғын, шифрлаў алгоритмлерин орынлай алатуғын ҳәм әмелий программаның протоколы мағлыўматларды узатыў ҳәм қабыллаўдан алдын криптографиялық гилтлер менен алмаса алатуғын жағдайды жаратып береди.

SSL протоколы менен қорғалған веб-бетлерди ашыў ушын URL ға әдеттеги http префикисиниң орнына https префикси қолланылады. Бул SSL-жалғаныўдың қолланылыўын аңлатды. https протоколы бойынша жалғаныўдың стандарт порты - 443

SSL еки тийкарғы мәселени орынлайды:

- Ашық Гилтлер Инфраструктурасы (PKI) қуралларын пайдаланып сервер ҳәм клиентти аутентификациялайды

- клиент ҳәм сервер арасында мағлыўматларды алмасыў ушын шифрланған байланысты жаратады

SSL/TLS тиң жумыс этабы:

- SSL Handshake – мағлыўматларды узатыў ушын шифрлаў методы анықланады.

- SSL Change Cipher Spec – усы сессия ушын клиент ҳәм сервер арасында гилтти жаратыў ҳәм узатыў.

- SSL Alert – клиент ҳәм серверге қәтелер ҳаққында SSL хабарын жеткериў.

- SSL Record – мағлыўматларды узатыў.

3.1.2.Берилген мағлыўматлар

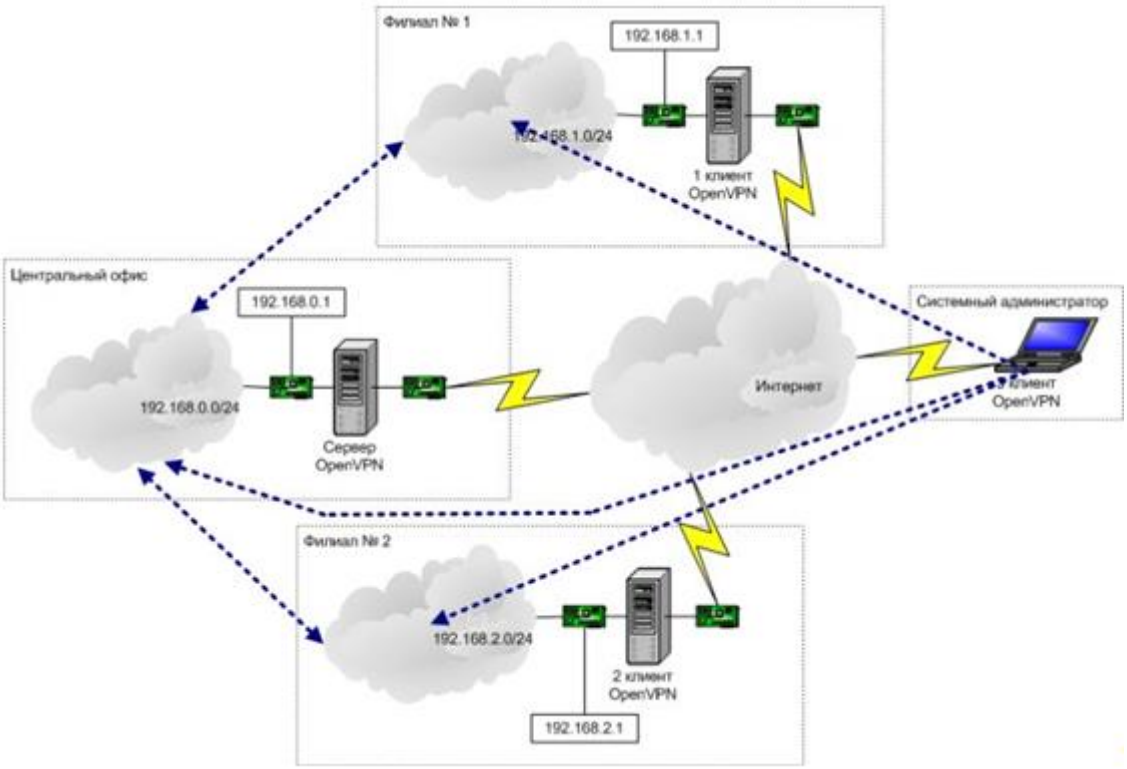
FreeBSD операциялық системасы орнатылған серверге ийемиз. Бул сервер арқалы орайлық офистиң локал тармағы Интернетке жалғанған. Усы серверде OpenVPN серверин жаратамыз. Интернетке FreeBSD (булар OpenVPN клиентлери болады) операциялық системасы орнатылған сервер арқалы жалғанған еки филиалға ийемиз. Windows XP операциялық системасы орнатылған системалы администратор компьютерине (булда OpenVPN клиенти болады) ийемиз. Орайлық офистиң локал тармағы 192.168.0.0/24 адресине; № 1 филиалдың локал тармағы - 192.168.1.0/24 адресине; № 2 филиалдың локал тармағы - 192.168.2.0/24 адресине ийе.

Тармақтың шөлкемлесиўиниң графикалық схемасы 3.1-сүўретте келтирилген.

Point-To-Multi-Point (бир сервер ҳәм бирнеше клиентлер) топологиясында, трафикти шифрлаў ушын TLS/SSL ди пайдаланыўшы ҳәм төмендеги маршрутизациялаў сиясатын тәмийинлеўши routed (яғный массалық трафикти өткизбейтуғын) түриндеги виртуаль тармақты жаратыў талап етиледи:

- орайлық офистиң локал тармағынан еки филиалдың локал тармағында жайласқан компьютерлерге кириў мүмкин;

- филиал локал тармағынан орайлық офистиң локал тармағында жайласқан компьютерлерге кириў мүмкин;



Сүўрет 3.1 – Интернетке жалғанған компания офиси ҳәм филиаллары арасында виртуаль тармақты қурыў схемасы

Бул мәселени әмелге асырыўда OpenSSL пакети ҳәм OpenVPN портының ең соңғы версиясы пайдаланылды.

3.2.OpenVPN серверин орнатыў

OpenVPN серверин орнатыўдан алдын ядроның конфигурация файлына `pseudo-device tun` қатарын киритиў керек. Егерде бундай қатар болмаса ядроны қайтадан жыйнаў ҳәм системаны қайтадан иске түсириў керек. Бунна кейин OpenVPN ди портлардан орнатамыз:

```
cd /usr/ports/security/openvpn
make install
```

OpenVPN серверинің конфигурация файллары `/usr/local/etc/openvpn` каталогында жайласады.

Бул каталогты ҳәм барлық зәрүр ишки каталогларды жаратыў ушын келеси командалар избе-излигин орынлаўымыз керек:

```
mkdir /usr/local/etc/openvpn
```

```
cd /usr/local/etc/openvpn
mkdir ccd
mkdir certs
mkdir crl
mkdir keys
mkdir private
mkdir req
chmod 700 keys private
echo "01" > serial
touch index.txt
```

бул командалар избе-излиги `/usr/local/etc/openvpn`; каталогин жаратады, оның ишинде жайласқан каталогларды жаратады: `ccd` (аралықтағы клиентлер конфигурациясы), `certs` (клиентлер ҳәм серверлердиң сертификатлары), `crl` (сертификатлардың пикир дизими), `keys` (клиентлер ҳәм сервердиң жабық гилтлери), `private` (өзи имзаланыўшы исенимли сертификаттың жабық гилти (CA)), `req` (сертификатларғ сораўлар); каталогларына рухсатты шеклейди `keys` и `private`; сертификатлар мағлыўматлар базасын жаратады (`serial` ҳәм `index.txt` файллары).

3.2.1.OpenSSL конфигурация файллары

Әдетте OpenSSL `/etc/ssl/openssl.cnf` файл конфигурациясын пайдаланады. Бирақ OpenSSL бөтен конфигурация файлын `/usr/local/etc/openvpn` каталогында жаратыў усыныс етиледи. Бул файл `openssl.cnf` аты менен атамаланыўы ҳәм келеси мазмунға ийе болыўы тийис:

```
[ ca ]
default_ca = CA_default
[ CA_default ]
dir = /usr/local/etc/openvpn
```

```
crl_dir = $dir/crl
database = $dir/index.txt
new_certs_dir = $dir/certs
certificate = $dir/CA_cert.pem
serial = $dir/serial
crl = $dir/crl/crl.pem
private_key = $dir/private/CA_key.pem
RANDFILE = $dir/private/.rand
default_days = 3650
default_crl_days = 365
default_md = md5
unique_subject = yes
policy = policy_any
x509_extensions = user_extensions
[ policy_any ]
organizationName = match
organizationalUnitName = optional
commonName = supplied
[ req ]
default_bits = 2048
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
x509_extensions = CA_extensions
[ req_distinguished_name ]
organizationName = Organization Name (must match CA)
organizationName_default = Company
organizationalUnitName = Location Name
commonName = Common User or Org Name
commonName_max = 64
[ user_extensions ]
basicConstraints = CA:FALSE
[ CA_extensions ]
basicConstraints = CA:TRUE
default_days = 3650
[ server ]
basicConstraints = CA:FALSE
nsCertType = server
```

3.3.Өзи имзаланыўшы исенимли сертификатты жаратыў

Өзи имзаланыўшы исенимли сертификатты (Certification Authority, CA) ҳәм оның ушын жабық гилтти жаратыў ушын төмендеги команданы /usr/local/etc/openvpn каталогында жайласқан ҳалда бериў керек:

```
openssl req -new -nodes -x509 -keyout
private/CA_key.pem -out CA_cert.pem -days 3650
```

req командасы OpenSSL ди сертификат жаратыўға мәжбүрлейди. Бул жерде:

-new – жаңа сертификатқа сораўды жаратады;

-nodes – жабық гилт шифрланбайды;

-x509 (-new менен бирге) - өзи имзаланыўшы сертификатты (Certification Authority, CA) жаратады;

-keyout – жабық гилттиң жайласқан орнын көрсетеди;

-out - өзи имзаланыўшы сертификаттың жайласқан орнын көрсетеди;

-days – сертификаттың ҳәрекет етиў ўақтын көрсетеди (365410 күн, шама менен он жылға тең).

Командаларды орынлаў процессинде экранға Country Name, State or Province Name; Locality Name; Organization Name; Organizational Unit Name; Common Name; Email Address параметрлери мәнислерин киритиў ҳаққында сораў шығарылады. Ең әҳмийетли параметр Common Name параметри. Бизиң жағдаймызда оның мәниси сервердиң FQDN-аты менен сәйкес келиўи керек. Өзи имзаланыўшы сертификатты ҳәм жабық гилтти генерациялаўдың нәтийжесин көриў ушын келеси команданы /usr/local/etc/openvpn каталогында жайласқан ҳалда бериледи:

```
openssl x509 -noout -text -in CA_cert.pem (сертификат)
openssl rsa -noout -text -in private/CA_key.pem (гилт)
```

3.4. Сервер сертификатын жаратыў

Сервер сертификатын жаратыўдан алдын сервер сертификаты ҳәм сервердиң жабық гилтине сораўды жаратыўымыз керек. Бул ушын /usr/local/etc/openvpn каталогында жайласып келеси команданы киритемиз:

```
openssl req -new -nodes -keyout keys/server.pem -
out req/server.pem
```

Команданың орынланыў процессинде сораўларға және бир мәртебе жуўап бериў керек. Жуўаплар жоқарыда кириткен жуўапларға сәйкес келиўи керек. Қосымша берилген «A challenge password []:» ҳәм «An optional company name []:» сораўларын жуўапсыз қалдырамыз («Enter» ди басамыз). Сервер сертификаты ҳәм сервердиң жабық гилтине сораўдың генерациялаўдың нәтийжесин көриў ушын /usr/local/etc/openvpn каталогында жайласып келеси командаларды киритемиз:

```
openssl req -noout -text -in req/server.pem (серт)
openssl rsa -noout -text -in keys/server.pem (гилт)
```

Сервер сертификатын жаратыў ушын сервер сертификатына сораўды өзи имзаланыўшы исенимли сертификат (CA) пенен имзалаў талап етиледи. Бул ушын /usr/local/etc/openvpn каталогында жайласып келеси команданы киритемиз:

```
openssl ca -batch -config openssl.cnf -extensions
server -out certs/server.pem -infiles req/server.pem
```

ca командасы OpenSSL ди сертификатқа сораўды имзалаўға мәжбүрлейди. Ол келеси опцияларға ийе:

`-config` OpenSSL конфигурация файлының жайласқан орнын көрсетеди;

`-extensions` – OpenSSL конфигурация файлының генерацияланыўшы сертификаттың қосымша параметрлери жайласқан секциясын көрсетеди;

`-out` – генерацияланыўшы сертифкаттың қайсы жерге жаратылыўын көрсетеди;

`-infiles` – сертификаттың сораўының жайласқан орнын көрсетеди;

`-batch` – қосымша сораўларға жуўап бериўден азат етеди.

Команданың орынланыў процессинде «Sign the certificate? [y/n]:» сораўы бериледи. Оған у деп жуўап бериў керек ҳәм буннан соң сертификатты генерациялаў басланады ҳәм сертификатлар жайласқан мағлыўматлар базасы (index.txt ҳәм serial файллары) жаңаланады. Генерациялаў нәтийжесин көриў ушын келеси команданы /usr/local/etc/openvpn каталогында жайласқан ҳалда киритемиз:

```
openssl x509 -noout -text -in certs/server.pem
```

§4. VPN КЛИЕНТЛЕРИН САЗЛАЎ

4.1. Диффи-Хэлман параметрлери файлын жаратыў

Клиенттиң сервер менен байланысыўында мағлыўматлардың исенимлирек қәўипсизлигин тәмийинлеўге арналған Диффи-Хэлман параметрлери файлын жаратыў ушын /usr/local/etc/openvpn каталогында жайласып келеси команданы киритемиз:

```
openssl dhparam -out dh2048.pem 2048
```

dhparam командасы OpenSSL ге Диффи-Хэлман параметрлери файлын жаратыўға буйрық береди, 2048 саны битлердеги разрядлықты анықлайды. Бул команда жүдә күшли компьютерлерде де жеткиликли әстен орынланады.

4.2.Клиент сертификатларын жаратыў

Клиент сертификатларын ҳәм жабық гилтлерин жаратыўға сораўларды жаратыў, сертификатларды ҳәм сертификатларды генерациялаўды имзалаў, сондай-ақ сертификатларға сораўларды, сертификатларды ҳәм жабық гилтлерди көриў процедурасы серверде орынланған процедура сыяқлы алып барылады. Сертификатларға сораўлар, жабық гилтлер ҳәм сертификатлар сәйкес келеси шаблондағы атларға ийе болыўы керек: `req/RClient` сертификатларға сораўлар, `keys/KClient` жабық гилтлер ушын ҳәм `certs/CClient` сертификатлар ушын. `Client` сөзи клиент аты менен алмастырылады. Бул ат сәйкес клиент ушын сертификатқа сораўды генерациялаў ўақтында киритилген `Common Name` параметри мәнисине қатаң сәйкес келиўи керек. Бир неше клиентлерде `Common Name` параметрлериниң мәнислериниң қайталаныўы сервер конфигурациясы тәрепинен анықланады.

`Client` клиенти ушын сертификатқа ҳәм жабық гилтине сораўды генерациялаў ушын ҳәм сертификатқа сораўды имзалаў, сертификатты

генерациялаў ушын /usr/local/etc/openvpn каталогында жайласқан ҳалда келеси команданы киритемиз:

```
openssl req -new -nodes -keyout keys/KClient.pem -out req/RClient.pem
openssl ca -batch -config openssl.cnf -out certs/CClient.pem -infiles req/RClient.pem
```

Сертификатқа, жабық гилтке генерацияланған сораўды ҳәм Client клиенти ушын генерацияланған сертификатты көриў ушын /usr/local/etc/openvpn каталогында жайласқан ҳалда келеси команданы киритемиз:

```
openssl req -noout -text -in req/RClient.pem
openssl rsa -noout -text -in keys/KClient.pem
openssl x509 -noout -text -in certs/CClient.pem
```

Бул этапта қарастырылып атырғын жағдай ушын сертификатқа сораўдан / жабық гилттен / сертификаттан қуралған үш топарды жаратыўымыз керек. Олардың атлары сәйкес Rclient1 / Kclient1 / Cclient1, Rclient2 / Kclient2 / Cclient2 ҳәм Rclient3 / Kclient3 / Cclient3 №1 филиал ушын (Common Name - client1), №2 филиал ушын (Common Name - client2) ҳәм системалы администратор ушын (Common Name - client3).

4.2.1. Сертификатлардың пикирлери дизимин жаратыў

Сертификатлардың пикирлери дизимин жаратыў ушын /usr/local/etc/openvpn каталогында жайласқан ҳалда келеси команданы киритемиз:

```
openssl ca -config openssl.cnf -gencrl -out crl/crl.pem
```

-gencrl гилти менен ca командасы OpenSSL ди сертификатлардың пикир дизимин жаратыўға мәжбүрлейди. Ол келеси опцияларға ийе:

`config` – OpenSSL конфигурация файлының жайласқан орнын көрсетеди;

`out` – сертификатлардың пикир дизимин қайсы жерге жаратылыўын көрсетеди;

Бул команда бос сертификатлардың пикир дизимин жаратады. `Client` клиентиниң сертификатының пикирин жаратыў ушын /usr/local/etc/openvpn каталогында жайласқан ҳалда келеси команданы киритемиз:

```
openssl ca -config openssl.cnf -revoke
certs/CClient.pem
```

-revoke гилти менен ca командасы OpenSSL ди берилген сертификаттың пикирин жаратыўға мәжбүрлейди. config опциясы OpenSSL конфигурация файлының жайласқан орнын көрсетеди. Сертификатлардың пикирлери дизимин көриў ушын келеси команданы киритемиз:

```
openssl crl -noout -text -in crl/crl.pem
```

4.3.HMAC статикалық гилтин жаратыў

DoS-ҳүжимлерден ҳәм UDP-портлардың флудингинен қорғаўды тәмийинлеўши HMAC статикалық гилтин жаратыў ушын келеси команданы киритемиз: `openvpn --genkey --secret ta.key`

4.3.1.Сервердиң конфигурация файлы

Әдеттеги жағдайда OpenVPN сервериниң конфигурация файлы `/usr/local/etc/openvpn` каталогында жайласыўшы `openvpn.conf` файлында жайласады. который должен находится в папке

/usr/local/etc/openvpn. Қарастырып атырған жағдаймызда конфигурация файлы төмендеги көриниске ийе болады:

```
dev tun
local <Внешний IP-адрес сервера>
port 1194
proto udp
server 10.0.0.0 255.255.255.0
push "route 10.0.0.0 255.255.255.0"
route 192.168.1.0 255.255.255.0
route 192.168.2.0 255.255.255.0
client-config-dir ccd
client-to-client
tls-server
dh /usr/local/etc/openvpn/dh2048.pem
ca /usr/local/etc/openvpn/CA_cert.pem
cert /usr/local/etc/openvpn/certs/server.pem
key /usr/local/etc/openvpn/keys/server.pem
crl-verify /usr/local/etc/openvpn/crl/crl.pem
tls-auth /usr/local/etc/openvpn/ta.key 0
comp-lzo
keepalive 10 120
tun-mtu 1500
mssfix 1450
persist-key
persist-tun
user openvpn
group openvpn
verb 3
```

Бул берилген файлда сервер параметрлериниң келеси мәнислери берилген:

dev – OpenVPN интерфейси;

local ҳәм port - OpenVPN қабыл қылатуғын кириўши байланыслардың IP-адреси ҳәм порты;

proto - протокол (бизиң жағдайымызда UDP);

`server` – жеке виртуаль тармақ ушын ажыратылған ҳәм клиентлер арасында автомат түрде бөлистирилиўши IP-адресслер жыйындысы;

`push` – клиентке жөнетилиўши ҳәм клиент тәрепинен орынланыўшы OpenVPN командасы (бизиң жағдайымызда "`route 10.0.0.0 255.255.255.0`" клиент тәрепинде виртуаль жеке тармағына маршрутты қосады);

`route` – сервер тәрепинде локал тармақларға маршрутларды қосады;

`client-config-dir` – клиентлердиң конфигурациялық файллары сақланыўшы каталог;

`client-to-client` – клиентлерге бир-бирин «көриўге» рухсат етиў (сәйкес маршрутизация қағыйдалары киритилгенде);

`tls-server` – TLS ти қоллаўдыиске түсириў;

`dh` – Диффи-Хэлман параметрлери файлының жайласқан орны;

`ca` – өзи имзаланыўшы исенимли сертификаттың (CA) жайласқан орны;

`cert` – сервер сертификатының жайласқан орны;

`key` – сервердиң жабық гилтиниң жайласқан орны;

`crl-verify` – сертификатлардың пикирлери дизими жайласқан орны;

`tls-auth` – HMAC статикалық гилтиниң жайласқан орны;

`comp-lzo` – трафиктиң LZO-компрессиясының пайдаланылыўы;

`keeplive` – жалғаныўдың тәмийинлениўи (бизиң жағдайымызда ҳәр бир 10 секундтан пинг жөнетиледи ҳәм жуўап пакетлери еки минут даўамында келмесе сервер тәрепинендe, клиент тәрепинендe жалғаныў жабылады (үзиледи)) ;

`tun-mtu` ҳәм `mssfix` – туннел бойынша мағлыўматларды узатыў параметрлери;

`user` ҳәм `group` – OpenVPN иске түсирилгенде қайсы пайдаланыўшы ҳәм қайсы топардың атынан жумыс ислеўин анықлайды (OpenVPN root тәрепинен иске түсириледи);

`verb` – OpenVPN тәрепинен `/var/log/messages` ке хабарлардың анықластырыў дәрежеси.

4.3.2.Клиентлердиң конфигурация файллары

Клиентлердиң конфигурация файллары текстли файллар болып, қурамында клиентлердиң жалғаныў ўақтында сервер тәрепинен орынланыўшы командалар избе-излигинен турады. Клиентлердиң конфигурация файллары атлары клиентлердиң Common Name параметрине сәйкес келиўи керек, яғный бул параметр мәниси client1 болса онда сервер client1 файлына жазылған командаларды орынлайды ҳ.т.б.

Клиентлердиң конфигурация файллары /usr/local/etc/openvpn/ccd каталогында жайласады. Бизиң қарастырып атырған проектимиз ушын үш клиентлердиң конфигурация файлларын жаратыўымыз керек:

```
cd /usr/local/etc/openvpn/ccd
touch client1 client2 client3
```

client1 файлы еки командадан турады: клиентке орайлық офистиң локал тармағына маршрутты қосыўшы ҳәм клиенттиң артында жайласқан локал тармақтың адресин анықлаўшы:

```
push "route 192.168.0.0 255.255.255.0"
iroute 192.168.1.0 255.255.255.0
```

client2 файлы client1 файлына уқсас:

```
push "route 192.168.0.0 255.255.255.0"
iroute 192.168.2.0 255.255.255.0
```

client3 файлы клиентке орайлық офистиң локал тармағына ҳәм еки филиалдың локал тармақларына маршрутларды қосыўшы командалардан турыўы керек:

```
push "route 192.168.0.0 255.255.255.0"
push "route 192.168.1.0 255.255.255.0"
push "route 192.168.2.0 255.255.255.0"
```

4.4.Сервердиң автомат түрде иске түсирилиўи

OpenVPN серверин операциялық система жүкленгенде автомат иске түсириў ушын `openvpn_enable="YES"` қатарын `/etc/rc.conf` файлына киритиў керек.

4.4.1.Брэндмауэрлерди сазлаў

OpenVPN сервериниң коррект жумыс ислеўи ушын брэндмауэрлердиң сазлаўларына келеси өзгерислерди киритиўимиз керек:

- OpenVPN интерфейси арқалы қәлеген трафиктиң өтиўине рухсат етиў;

- OpenVPN сервериниң сыртқы адресине UDP-трафигиниң (порт 1194) өтиўине рухсат етиў;

- қәлеген трафиктиң виртуаль жеке тармақтан локал тармаққа өтиўине рухсат етиў;

- қәлеген трафиктиң локал тармақтан виртуаль жеке тармаққа өтиўине рухсат етиў;

- қәлеген трафиктиң №1 филиалдың локал тармағынан локал тармаққа өтиўине рухсат етиў;

- қәлеген трафиктиң локал тармақтан №1 филиалдың локал тармағына өтиўине рухсат етиў;

- қәлеген трафиктиң №2 филиалдың локал тармағынан локал тармаққа өтиўине рухсат етиў;

- қәлеген трафиктиң локал тармақтан №2 филиалдың локал тармағына өтиўине рухсат етиў;

ipfw ушын келеси қағыйдаларды киритемиз:

```
/sbin/ipfw -q add pass ip from any to any via ${vif}
/sbin/ipfw -q add pass udp from any to ${oip} 1194 in
via ${oif}
```

```
/sbin/ipfw -q add pass ip from ${vnet} to ${inet} out
via ${iif}
/sbin/ipfw -q add pass ip from ${inet} to ${vnet} in
via ${iif}
/sbin/ipfw -q add pass ip from 192.168.1.0/24 to
${inet} out via ${iif}
/sbin/ipfw -q add pass ip from ${inet} to
192.168.1.0/24 in via ${iif}
/sbin/ipfw -q add pass ip from 192.168.2.0/24 to
${inet} out via ${iif}
/sbin/ipfw -q add pass ip from ${inet} to
192.168.2.0/24 in via ${iif}
```

shell өзгериўшилери келеси мәнислерге ийе:

`oip` – сервердиң сыртқы IP-адреси,

`inet` – локал тармақ адреси (бизиң жағдаймызда - 192.168.0.0/24),

`vnet` – виртуаль жеке тармақ адреси (бизиң жағдаймызда - 10.0.0.0/24),

`iif` – сервердиң ишки интерфейсиниң аты (мәселен, `rl1`),

`oif` - сервердиң сыртқы интерфейсиниң аты (мәселен, `rl0`),

`vif` - OpenVPN интерфейсиниң аты (мәселен, `tun0`).

Клиент брандмауэрлерин сазлаў усыған уқсас алып барылады. Қағыйдалар бесинши қағыйдадан баслап, шөлкемлестирилген маршрутизация сиясатынан ғәрезли болады. Бизиң жағдайымызда ipfw қағыйдалары `client1` клиенти (енди shell өзгериўшиси `inet` client1 клиентиниң локал тармағының адресин анықлайды - 192.168.1.0/24) ушын келеси көриниске ийе болады:

```
/sbin/ipfw -q add pass ip from any to any via ${vif}
/sbin/ipfw -q add pass udp from any to ${oip} 1194 in
via ${oif}
```

```
/sbin/ipfw -q add pass ip from ${vnet} to ${inet} out
via ${iif}
/sbin/ipfw -q add pass ip from ${inet} to ${vnet} in
via ${iif}
/sbin/ipfw -q add pass ip from 192.168.0.0/24 to
${inet} out via ${iif}
/sbin/ipfw -q add pass ip from ${inet} to
192.168.0.0/24 in via ${iif}
```

`client2` клиенти ушын ipfw қағыйдалары `client2` клиенти қағыйдаларынан парықланбайды (енди shell өзгериўшиси `inet` client2 клиентиниң локал тармағының адресин анықлайды - 192.168.2.0/24).

4.4.2.Гилтлик файлларды клиентке узатыў

Файлларды клиентке узатыў ушын жақсысы исенимли мағлыўмат тасыўшыдан (диск яки флешка) пайдаланған мақул. Бирақ бул ушын ҳеш қашан Интернет тармағынан пайдаланыўға болмайды. `Client` клиентине зәрүр файлларды дискетаға копиялаў ушын келеси командалар избе-излигин орынлаў керек:

```
mount -t msdos /dev/fd0 /mnt
cd /usr/local/etc/openvpn
cp certs/CClient.pem /mnt
cp keys/KClient.pem /mnt
cp CA_cert.pem /mnt
cp ta.key /mnt
umount /mnt
```

Бул командалар дискетаны `/mnt` каталогына жалғап, соң клиент сертификатын, клиенттиң жабық гилтин, өзи имзаланыўшы исеним

сертификатын (CA) ҳәм HMAC статикалық гилтин дискетаға копиялайды. Буларды орынлап болғаннан кейин дискетаны ажыратады.

4.4.3.VPN Клиентиниң программалық тәмийинлениўи

Егерде клиентке UNIX системасы орнатылған болса онда программалық тәмийнлеўди орнатыў северге орнатқан сыяқлы алып барылады ҳәм сол портқа орнатылады. Windows системасы менен жумыс ислегенде клиент программалық тәмийинлениўиниң еки варианты бар: OpenVPN ҳәм OpenVPN GUI. Биринши вариант барқулла жалғанған жағдайына мақул келеди (OpenVPN Windows тиң хызмети сыяқлы орнатылады), екиншиси корпоратив тармаққа периодлы жалғаныўшы мобил клиентлер ушын. Еки жағдайда да конфигурация файлы бирдей форматқа ийе боады. Windows-клиентлерди пайдаланған жағдайында конфигурация файлларында бир бэкслэштиң орнына қос бэкслэшти пайдаланыў керек.

4.4.4.Клиент программалық тәмийинлениўиниң конфигурация файлы

OpenVPN клиентиниң конфигурация файлы openvpn.conf файлында сақланады. Егерде биз UNIX-клиент пенен жумыс алып барсақ онда ол /usr/local/etc/openvpn катлогында жайласады, ал егерде Windows-клиенти менен жумыс алып барсақ онда егерде OpenVPN (OpenVPN GUI) ди орнатқан пайтында басқа жол көрсетилмеген болса C:\Program Files\OpenVPN\config\ каталогында .ovpn кеңейтпеси менен жайласады.

client3 клиентиниң конфигурация файлын қарастырамыз. Бул клиент Windows XP операциялық системасын ноутбукке орнатқан. OpenVPN клиенти әдеттеги жол бойынша орнатылған. Алдын дискетаға көширилген гилтлик файллар P: дискинде OpenVPN каталогында сақланады. Қарастырып атырған жағдайымызда OpenVPN клиентиниң конфигурация файлы келеси көриниске ийе болады:

```
client
```

```
dev tun
proto udp
remote <IP-адрес сервера OpenVPN>
tls-client <FQDN сервера OpenVPN>
tls-remote
ca "P:\OpenVPN\CA_cert.pem"
cert "P:\OpenVPN\Cclient3.pem"
key "P:\OpenVPN\Kclient3.pem"
tls-auth "P:\OpenVPN\ta.key" 1
ns-cert-type server
comp-lzo
tun-mtu 1500
mssfix 1450
verb 3
```

Бул файлда OpenVPN клиентиниң келеси параметрлериниң мәнислери берилген:

`client` – бул файл OpenVPN клиентиниң конфигурация файлы екенлигин аңлатыўдың қысқаша варианты;

`dev` – OpenVPN қурылмасы;

`proto` – протокол (бизиң жағдайымызда UDP);

`remote` – OpenVPN сервериниң IP-адреси;

`tls-client` – TLS ти қоллаўды қосыў;

`ca` –өзи имзаланыўшы исенимли сертификаттың (CA) жайласқан орны;

`cert` – клиент сертификатының жайласқан орны;

`key` – клиенттиң жабық гилтиниң жайласқан орны;;

`tls-auth` – HMAC статикалық гилтиниң жайласқан орны;

Бул жаратылған виртуаль жеке тармағы жәрдеминде Windows ОС ның Remote Administrator ҳәм Terminal Services хызметлери ҳәм Unix ОС ның FTP, NFS, SSH ҳәм Telnet хызметлери жумыс алып барыўы мүмкин.

ЖУЎМАҚЛАЎ

VPN (Virtual Private Network – виртуаль жеке тармақ) – логикалық тармақ болып, өзинен жоқарыдағы екинши тармақ, мәселен Internet тийкарында қурылады. Бул тармақта улыўма коммуникацияда қәўипсиз болмаған тармақ протоколларынан пайдаланылыўына қарамай, шифрлаўдан пайдаланған ҳалда, мағлыўмат алмасыўда бөтенлерге жабық болған каналларды пайда етеди. VPN кәрханалардың бир неше офислери арасында қадағаланбайтуғын каналлардан пайдаланған ҳалда жалғыз тармаққа бирлестириў имканиятын береди.

Өз нәўбетинде, VPN бөлек тармақ қәсийетлерин өзине алған, лекин бул тармақ улыўма пайдаланыў тармағы арқалы әмелге асырылады. Туннеллестириў методы жәрдеминде мағлыўматлар пакети улыўма пайдаланыў тармағы арқалы әпиўайы еки түйинли байланысыўдағы сыяқлы трансляцияланады.

Қаралып атырған питкериў қәнигелик жумысында сыпатлы хызмет көрсетиўши байланыс тармағында мағлыўматларды қорғаў менен танысылады ҳәм OPENVPN тийкарында виртуаль жеке тармағын жаратыўға ерисилди.

Жумыстың нәтийжелери ретинде төмендегилерди көрсетиўге болады:

- Виртуаль, қорғалған VPN тармақларды қурыўдың концепциясы көрип шығылды;
- Қәўипсизликти шөлкемлестириўдиң улыўма сиясаты үйренилди;
- OPENVPN тийкарында виртуаль жеке тармағы жаратылды;

Питкериў қәнигелик жумысы нәтийжесин виртуаль жеке тармақларды қурыўда методикалық қолланба ретинде пайдаланыўға болады деп есаплаймыз.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЯТЛАР ДИЗИМИ

1. Галатенко В.А. «Информационная безопасность» // Открытые системы. - 2006. - № 1. - С. 38-43.
2. Зима В.М., Молдовян А.А., Молдовян Н.А. «Безопасность глобальных сетевых технологий.» - СПб.: БХВ-Петербург, 2007.
3. Кульгин М. «Технологии корпоративных сетей» // - СПБ. : Питер, 2008, 704 с.
4. Норман Р. «Выбираем протокол VPN» // Windows 2000 Magazine. - 2007. - №7.
5. Олифер В. «Новые технологии и оборудование IP-сетей» // - СПб.: БХВ-Петербург. - 2006.
6. Петренко С.А. Реорганизация корпоративных систем безопасности // Конфидент. - 2007. - № 2.
7. Саливан К. «Прогресс технологии VPN» // PCWEEK/RE, №2
8. Стивен Б. «Виртуальные частные сети» // издательство «Лори» , 2007, 504 с.
9. «Типовые решения по применению средств VPN для защиты информационных ресурсов» / ООО «Конфидент». - СПб., 2006.
10. Фратто М. «Секреты виртуальных частных сетей» // Сети и системы связи, №3
11. http://acy-books.ru
12. http://intuit.ru

ҚОСЫМША

OpenVPN жалғаныўын орнатыў ҳәм сазлаў

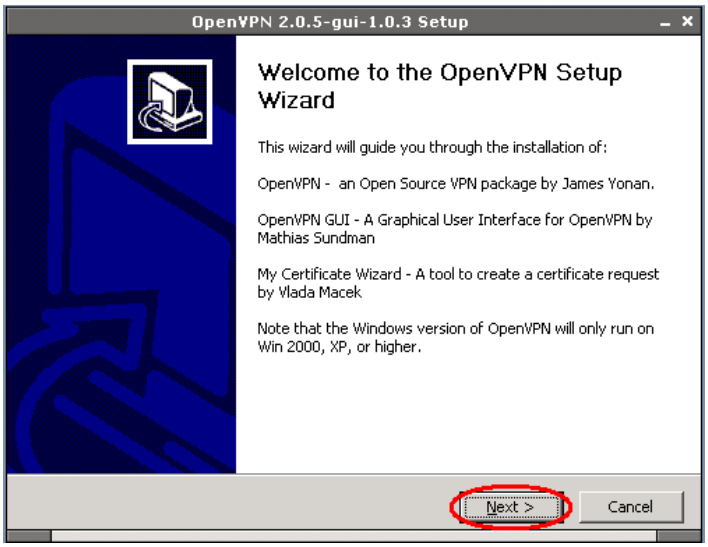
OpenVPN 2.0.9 + OpenVPN GUI 1.0.3 программаны төмендеги адрес бойынша жүклеп аламыз [1.1 Мб]:

http://openvpn.se/files/install_packages/openvpn-2.0.9-gui-1.0.3-install.exe

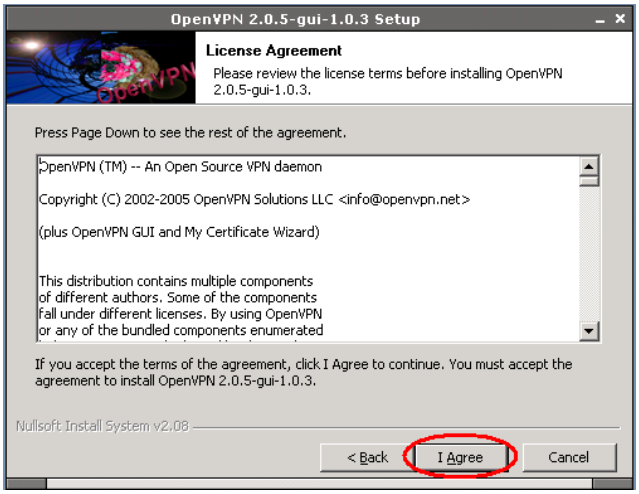
Егер сизде Windows Vista ОС сы болса, онда OpenVPN 2.1 талап етиледи.

http://openvpn.net/release/openvpn-2.1_rc7-install.exe

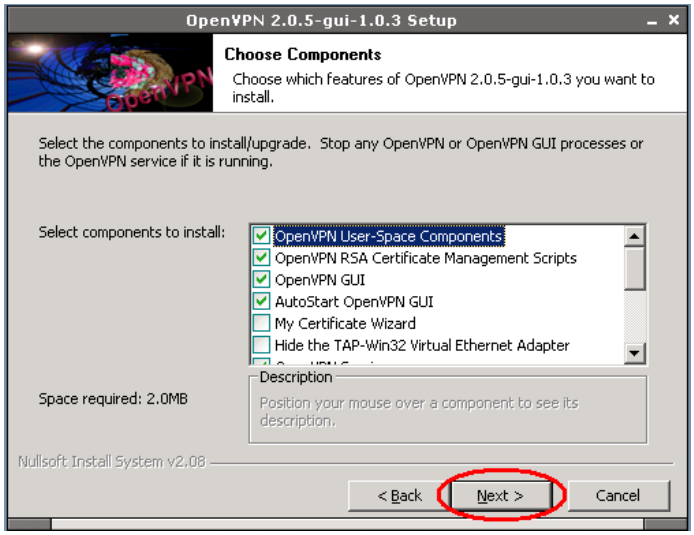
1. Гилт ҳәм сазлаў файлын алыў.
2. Openvpn-2.0.9-gui-1.0.3-install.exe программасын иске түсиремиз
3. Пайда болған дилог айнада "Next" кнопкасын басамыз



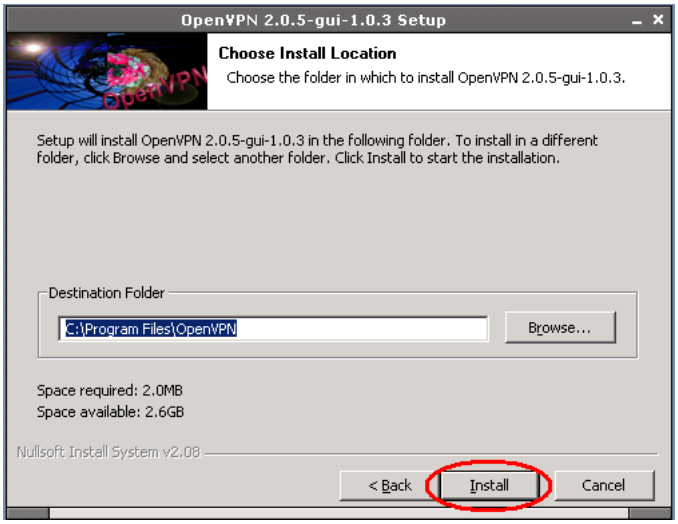
4. Лицензиалық келисиўди дыққат пенен оқыймыз. Егер сиз разы болсаңыз "I Agree", кери жағдайда "Cancel" кнопкасын басып орнатыўды тоқтатасыз.



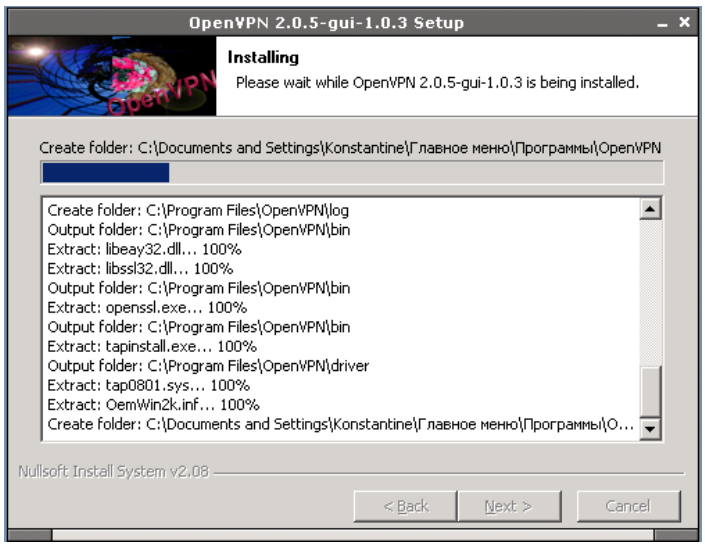
5. Орнатылыўшы компонентлер дизиминде ҳеш нәрсе өзгертилмейди



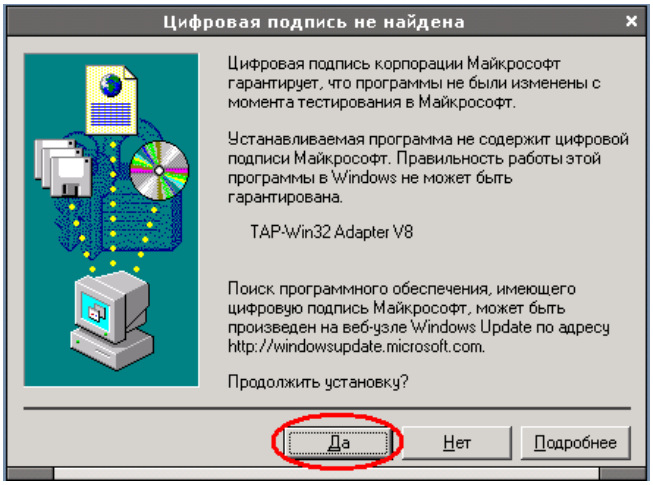
6. "Destination Folder" текстли майданшасына программа орнатылыўы керек каталог көрсетиледи ҳәм "Install" кнопкасы басылады



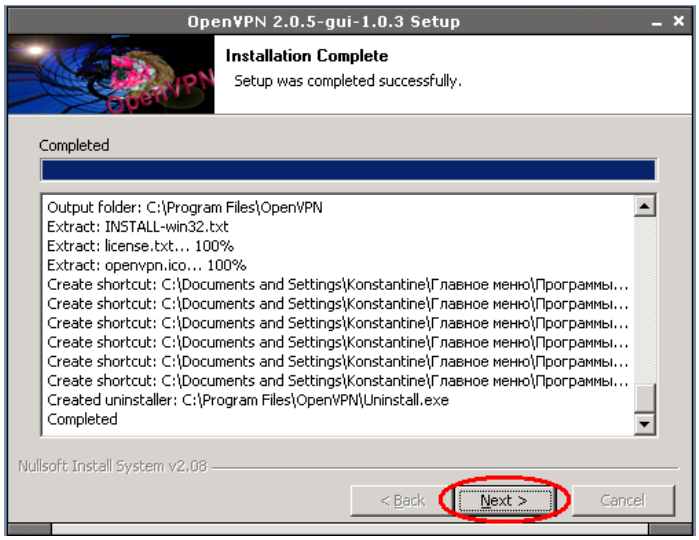
OpenVPN файлларын орнатыў процесси



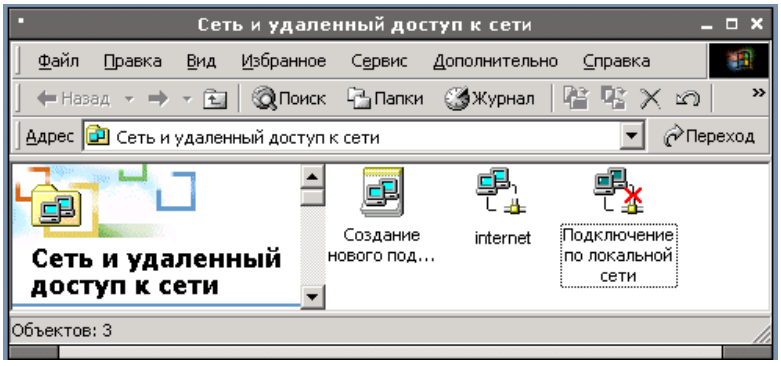
OpenVPN файлларын орнатыў процессинде Майкрософт тың цифрлы имзасына ийе емес виртуал қурылма драйвери орнатылады.



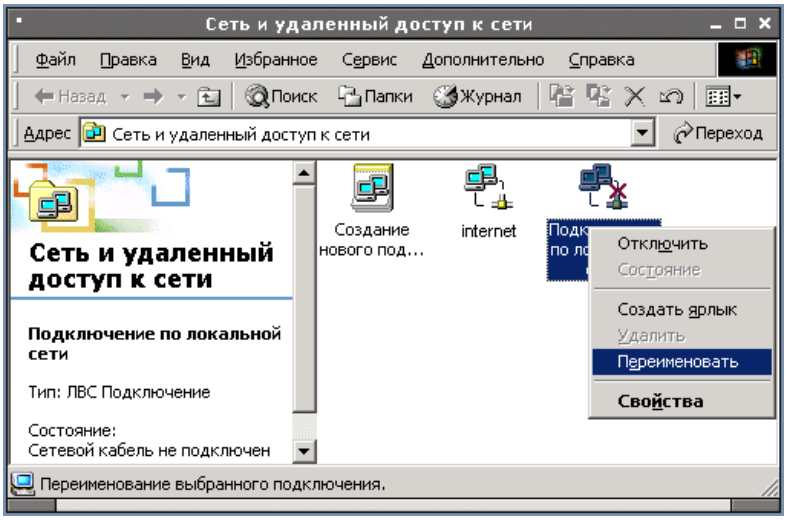
OpenVPN файлларын орнатыў тамамланғаннан соң "Next" басылады.

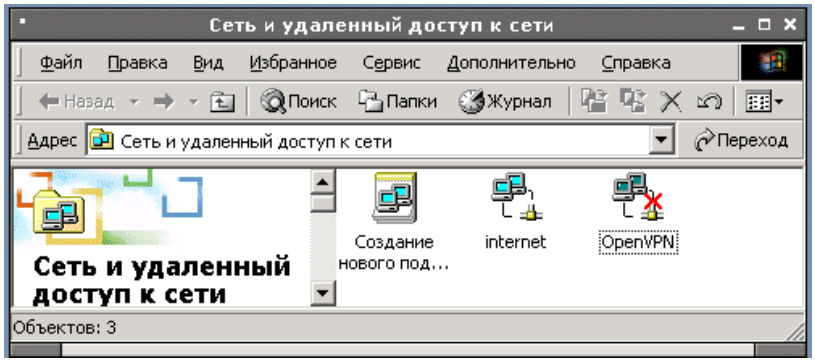


"Сеть и удалённый доступ к сети" папкасына киремиз

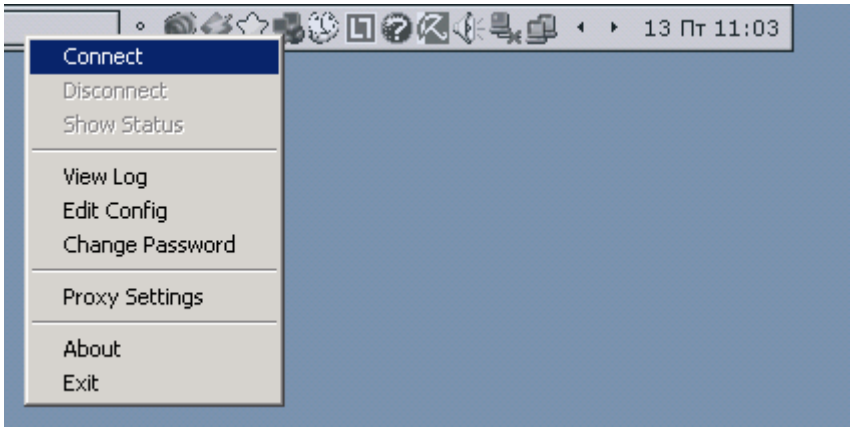


Жаңа жалғаныўды "OpenVPN" ге қайта атамалаймыз.





OpenVPN ниң сазлаўлар папкасын ашамыз. Бул ушын "Пуск" >> "Программы" >> "OpenVPN" >> "OpenVPN configuration file directory". Бул папкаға гилт ҳәм сазлаўлар файлын жайластырамыз. OpenVPN ди жалғаймыз.



OpenVPN Connection айнасында жалғаныў адымлары көрсетиледи. Жалғаныўды үзгенимизде айна жабылады