ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Кибернетика және ақпараттық технологиялар институты

«Киберқауіпсіздік, ақпаратты өңдеу және сақтау» кафедрасы

Қалмахан Ғалымжомарт Жұлдызұлы

«VPN технологиясын қолдана отырып, корпоративтік желіде деректерді беру қауіпсіздігін арттыру»

ДИПЛОМДЫҚ ЖҰМЫС

Мамандығы 5В100200 - Ақпараттық қауіпсіздік жүйелері

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Кибернетика және ақпараттық технологиялар институты

«Киберқауіпсіздік, ақпаратты өңдеу және сақтау» кафедрасы

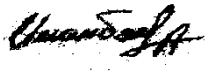
ҚОРҒАУҒА ЖІБЕРІЛДІ
КБОиХИ Кафедра меңгерушісі
тех.ғыл.канд, ассоц. профессор
_____ Н.А.Сейлова
“_____” _____20__ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы: “VPN технологиясын қолдана отырып, корпоративтік желіде деректерді беру қауіпсіздігін арттыру”

Мамандығы 5В100200 - Ақпараттық қауіпсіздік жүйелері

Орындаған  Қалмахан Ғ.Ж.

Ғылыми жетекші  т.ғ.к., лектор. Иманбаев А.Ж.

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Кибернетика және ақпараттық технологиялар институты

«Киберқауіпсіздік, ақпаратты өңдеу және сақтау» кафедрасы

БЕКІТЕМІН
КБОиХИ Кафедра меңгерушісі
тех.ғыл.канд, ассоц. профессор
_____ Н.А.Сейлова
“_____” _____20__ж.

Дипломдық жұмыс орындауға

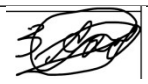
ТАПСЫРМА

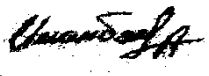
Білім алушы *Қалмахан Ғалымжомарт Жұлдызұлы*
Тақырыбы:VPN технологиясын қолдана отырып, корпоративтік желіде деректерді беру қауіпсіздігін арттыру.
Университет Ректорының *"27" 01 №762-б* бұйрығымен бекітілген
Аяқталған жұмысты тапсыру мерзімі *2020жылғы "15"мамыр*
Дипломдық жұмыстың бастапқы берілістері:VPN проблемалық аймағы,VPN протоколының әдістері, VPN құрылымы, VPN протоколдарын салыстыру.
Дипломдық жұмыста қарастырылатын мәселелер тізімі
a) Vpn желілерін іске асыру әдістері.
b) Корпоративтік желіге OpenVPN VPN-нін енгізу.
c) AnyConnect VPN Client арқылы SSL протоколын конфигурациялау.
d) Gns3 симуляторына желіні құру.
e) Anyconnect vpn-ді желіаралық экранға іске қосу.
Сызба материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс): *VPN протоколдары, RemoteAccess VPN корпоративтік желідегі топологиясы, салыстыру және ең қауіпсізін таңдау.*
Ұсынылатын негізгі әдебиет: 20 атаудан

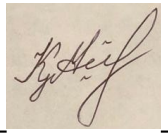
КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекші мен кеңесшілерге көрсету мерзімдері	Ескерту
VPN ҚҰРЫЛЫМЫ	01.03.2020 ж.	орындалды
GNS3 СИМУЛЯТОРЫНА ЖЕЛІНІ ҚҰРУ	03.04.2020 ж.	орындалды
ANYCONNECT VPN-ДІ ЖЕЛІАРАЛЫҚ ЭКРАНҒА ІСКЕ ҚОСУ	05.05.2020 ж.	орындалды

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

Бөлімдер атауы	Кеңесшілер, аты, әкесінің аты, тегі (ғылыми дәрежесі, атағы)	Қол қойылған күні	Қолы
Норма бақылау	магистр тех.ғыл, лектор Зиро А.	05.05.2020	

Ғылыми жетекші _____  _____ Иманбаев А.Ж.

Тапсырманы орындауға алған білім алушы ___  ___ Қалмахан Ғ.Ж.

Күні «27»_қаңтар_2020 ж.

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Қалмахан Ғ. Ж.

Название: VPN технологиясын қолдана отырып, корпоративтік желіде деректерді беруқауіпсіздігін арттыру»

Координатор: Азамат Иманбаев

Коэффициент подобия 1:3,1

Коэффициент подобия 2:1

Замена букв:8

Интервалы:0

Микропробелы:0

Белые знаки:0

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

☑ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

К заимствованию относятся стандартные определения и терминология, т.е. заимствования не обладают признаками плагиата……

……
……

Дата *Подпись заведующего кафедрой /*

начальника структурного подразделения

Окончательное решение в отношении допуска к защите, включая обоснование:

Работа является самостоятельной, имеющиеся незначительные заимствования являются добросовестными. Работа допускается к защите.

……
……
……
……
……
……
……
……

……

Дата

……
…

Подпись заведующего кафедрой / начальника структурного подразделени

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Қалмахан Ғ. Ж.

Название: VPN технологиясын қолдана отырып, корпоративтік желіде деректерді беруқауіпсіздігін арттыру»

Координатор: Азамат Иманбаев

Коэффициент подобия 1:3,1

Коэффициент подобия 2:1

Замена букв:8

Интервалы:0

Микропробелы:0

Белые знаки: 0

После анализа Отчета подобия констатирую следующее:

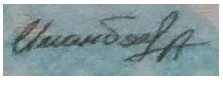
- ☑ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;
- ☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
- ☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

Заимствования объясняются использованием общепринятой терминологии, в которой часто используются не только отдельные слова, но и совокупность нескольких слов.

……
……

……



Иманбаев А. Ж.

Дата

Подпись Научного руководителя

АҢДАТПА

Бұл дипломдық жұмыс, VPN технологиясын қолдана отырып қазіргі заманғы корпоративті желілердің қауіпсіздік деңгейін талдауға арналған.

Түсініктеме А4 парағында жасалынған, 74 беттен, 2 кестеден, 76 суреттен, 1 диаграммадан және 19 пайдаланылған әдебиеттерден тұрады. Сонымен қатар кіріспеден, төрт тараудан және қорытындыдан тұрады.

Бірінші тарауда виртуалды жеке желінің құрылымы туралы жалпы ақпарат берілген. Екінші тарауда VPN желілерінің хаттамалары сипатталған. Бұл тарауда сынып диаграммалары, сынып сипаттамалары және кейбір әдістер берілген. Үшінші тарау VPN хаттаманы таңдауға арналған. Төртінші тарауда брандмауэрде AnyConnect VPN қолдануы сипатталған. Бірқатар тұжырымдар жасалды, қорытынды бөлімде OpenVPN-нің артықшылықтары мен кемшіліктері.

АННОТАЦИЯ

Данная дипломная работа посвящена анализу уровня защищенности современных корпоративных сетей с применением технологии VPN.

Пояснительная записка выполнена на листах А4, содержит 74 страниц, 2 таблиц, 76 рисунков, 1 диаграмма и 19 использованной литературы. Также включает в себя введение, четыре главы и заключение.

В первой главе приводится общая информация о структуре Virtual Private Network. Во второй главе описывается протоколы VPN сетей. В данной главе приведены диаграммы классов, описание классов и описание некоторых методов. Третья глава посвящена выбору протокола. В четвертой главе описывается реализация AnyConnect VPN на межсетевом экране. Сделано ряд выводов, плюсы и минусы OpenVPN в заключительной части.

ANNOTATION

This thesis is devoted to the analysis of the level of security of modern corporate networks using VPN technology.

The explanatory note is made on A4 sheets, contains 74 pages, 2 tables, 76 figures, 1 diagram and 19 references. It also includes an introduction, four chapters, and a conclusion.

The first Chapter provides General information about the structure of the Virtual Private Network. The second Chapter describes the VPN network protocols. This Chapter provides class diagrams, class descriptions, and descriptions of some methods. The third Chapter is devoted to the choice of Protocol. The fourth Chapter describes the implementation of AnyConnect VPN on the firewall. A number of conclusions are made, the pros and cons of OpenVPN in the final part.

ЖОСПАР

КІРІСПЕ	13
1 АНАЛИТИКАЛЫҚ БӨЛІМ (МӘСЕЛЕНІҢ ТҰЖЫРЫМЫ)	14
1.1 ДЕРЕКТЕРДІ БЕРУ КЕЗІНДЕГІ ҚАУІПТЕР	14
1.2 VPN АНЫҚТАМАСЫ	15
1.3 ІСКЕ АСЫРУ ДЕҢГЕЙЛЕРІ	15
1.4 VPN-НІҢ ЖІКТЕЛУІ	17
1.5 VPN ҚҰРЫЛЫМЫ	20
1.6 EXTRANET VPN КОРПОРАТИВ-АРАЛЫҚ ЖЕЛІСІ	20
1.7 VPN ЖЕЛІЛЕРІН ІСКЕ АСЫРУ ӘДІСТЕРІ	23
2 VPN ЖЕЛІЛЕРІНІҢ ХАТТАМАЛАРЫ	27
2.1 PPTP	27
2.2 L2TP/IPSEC	28
2.3 L2TP	29
2.4 IPSEC	30
2.5 OPENVPN (SSL)	31
2.6 MPLS	32
3 ТАҢДАЛМАЛЫ ХАТТАМА	34
3.1 ЖЫЛДАМДЫҚ	34
3.2 ҚАУЫПСІЗДІК	35
3.3 ОРНАТУ	36
3.4 САЛЫСТЫРУДЫҢ ҚОРТЫНДЫСЫ	36
4 VPN-ДІ ІСКЕ ҚОС	38
4.1 GNS3 СИМУЛЯТОРЫНА ЖЕЛІНІ ҚҰРУ	38
4.2 ANYCONNECT VPN-ДІ ЖЕЛІАРАЛЫҚ ЭКРАНҒА ІСКЕ ҚОСУ	39
ҚОРЫТЫНДЫ	73
ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ	74

КІРІСПЕ

Ғаламдық желі internet-тің қарқынды дамуына байланысты деректерді беру қауіпсіздігі мәселесі өзекті бола бастады. Өздеріңіз білетіндей, ғаламдық желі ол қауіпті орын. Деректерді көшіріп, басып алу қаупі және бұзу (ресурстарға заңсыз қол жеткізу) едәуір арта түсті. Сондықтан ресурстарға «әсер ету» саласының қарқынды дамуымен қатар, «қарсы әрекет» саласы дамуда.

Интернет арқылы ақпарат беру кезінде қорғаумақсаты жұмыс тапсырмаларын автоматтандыруға арналған технологиялық шешімдерді жүзеге асыру кез-келген компанияның алдында пайда болады.Интернет арқылы алмасудың негізгі жағдайлары:

- электрондық пошта;
- ұйымдастыру қызметкерінің web-порталына қол жеткізуі;
- ұйымдастыру қызметкерінің терминалдық серверге кол жеткізуі;
- үйым арасында файлдармен алмасу;
- бірлескен жоба жүргізу мақсатында ұйымдардың корпоративтік желілерінің бөліктерін бір желіге біріктіру;
- ұйымдастыру филиалдарының біртұтас желіге енуі.

Деректерді қауіпсіз алмастыруды құру үшінақпаратты қорғау хаттамалары жасалды және қорғау хаттамаларын іске асыратын бағдарламалық өнімдер шығарылды.

Ұйым желілерімәліметтерді берудің негізгі қауіпсіздік шаралары егжей-тегжейлі қарастырылатын VPN механизмімен қамтылады.

Менің жұмысымның негізгі бағыты – ұйымдастыру.Дипломдық жұмыстың зерттеу объектісі біздің ұйымдағы деректерді жіберу жүйесі болып табылады. Жұмыстың мақсаты – корпоративтік желідегі мәліметтер алмасудың қауіпсіздігін қамтамасыз ету.

Осы жұмыста шешілетін тапсырмалар:

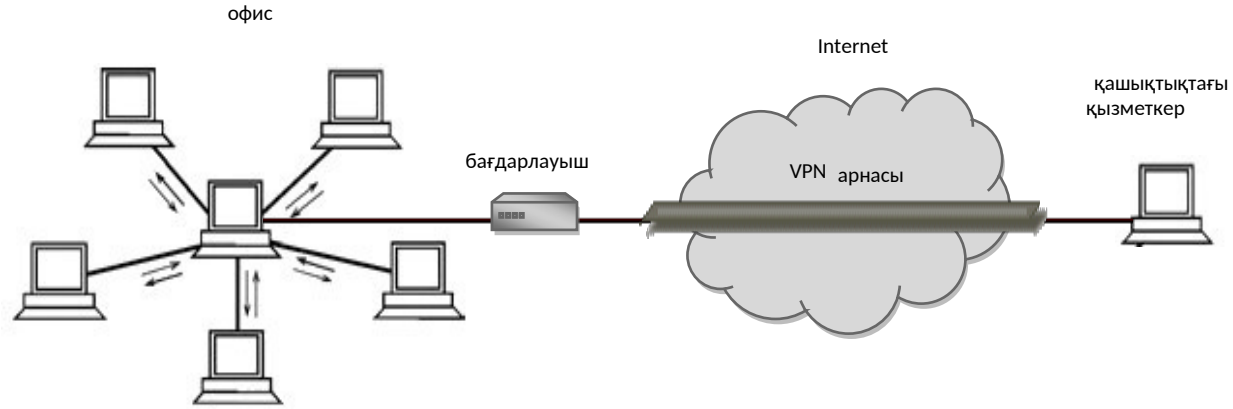
- VPN технологиялық шолу;
- VPN қосылымын құруға арналған хаттамаларға шолу;
- VPN негізгі хаттамаларын талдау;
- VPN қосылымын жүзеге асыру үшін хаттаманы таңдау;
- Деректерді қауіпсіз беруді жүзеге асыру.

Бұл жұмыс VPN-ді өз бетінше жөнге алу және қосылымдарды орындау үшін барлық қажетті ақпаратты қамтиды.

1 Аналитикалық бөлім (мәселенің тұжырымы)

Бізде қауіпсіз тарату арнасын ұйымдастыруы үшін ғаламторға қол жетімді шағын корпоративті желі бар, ол қашықтан жұмыс істейтін қызметкер мәліметтерімен алмасу үшін қажет.

Ұйым желісі арнайы сервер мен Интернетке кіретін клиенттің бес компьютерінен тұрады.Клиенттік машиналардың бірі VPN серверіне бөлінген (1.1 сурет).



1.1 сурет – Ұйым желісінің топологиясы

VPN анықтамасы қандай және оның не екендігі, қалай және қайда қолданылатындығы туралы алдын-ала мәлемет бере отырып, біз RemoteAccess VPN көмегімен қауіпсіз деректер алмасуды ұйымдастырамыз. Сонымен қатар, танымал корпоративтік желіге ең қолайлы VPN хаттамаларын талдап, біз таңдалған хаттамаларды қолдана отырып қосылуды жүзеге асырамыз.

1.1 Деректерді беру кезіндегі қауіптер

Корпоративтік желілерде деректерді беру кезінде көптеген қауіп-қатерлер туындайды.Қатерлер - бұл мүдделерге нұқсан келтіретін мүмкін болатын іс-әрекеттер, процестер, құбылыстар немесе оқиғалар.

Ақпараттық қауіпсіздікке қауіптер әртүрлі болуы мүмкін:

Қасақана әрекет ету арқылы:

- қасақана (диверсия және тыңшылық);
- кездейсоқ (табиғи апаттар, жүйенің бұзылуы).

Қауіптің көзін табу арқылы:

- сыртқы (қауіптің көздері жүйеден тыс);
- ішкі (қауіптің көздері жүйеде орналасқан).

Қауіптің мөлшері бойынша:

- жалпы (қауіпсіздік объектісіне толықтай зиян келтіру, айтарлықтай

зиян келтіру);
- жергілікті (қауіпсіздік құралының белгілі бір бөліктеріне зиян келтіретін);
- жеке (қауіпсіздік объектісі элементтерінің кейбір қасиеттеріне зиян келтіру).

Ақпараттық жүйеде әрекет ету деңгейі бойынша:
- белсенді (жүйенің құрылымы мен мазмұны өзгертілуі мүмкін);
- пассивті (жүйенің құрылымы мен мазмұны өзгермейді).

Қауіптер бөлінетін негізгі 3 топ, бұл:
- техногендік (техникалық құралдармен байланысты);
- антропогендік (субъектінің әрекетімен байланысты);
- табиғи (табиғи көздермен байланысты).

Деректерді беруде жиі кездесетін негізгі антропогендік қауіптерді қарастырайық:

1. Берілетін деректерді ұрлау;
2. Ақпаратты түрлендіру (ауыстыру);
3. Деректерді жою;
4. Қалыпты берілудің бұзылуы;
5. Желілік трафикті ұстап қалу (Сниффинг);
6. Ақпаратқа рұқсатсыз қол жеткізу, сондай-ақ заңсыз артықшылықтар алу (IP-спуфинг).

Желілер арасында қауіпсіз ақпарат алмасудың ақпараттық технологиясын қалыптастырудың қазіргі жағдайында виртуалды жеке желілердің (VPN) артықшылықтары сөзсіз.

1.2 VPN анықтамасы

VPN (VirtualPrivateNetwork) (ағылшын тілінен аударылған) виртуалды жеке желі – басқа желі арқылы бір немесе бірнеше желілік қосылыстар жасауға мүмкіндік беретін технологиялардың біріктірілген атауы. Бұл құрастырылған логикалық желіге сенім деңгейі криптографияны қолдану салдарынан негізгі желілерге деген сенім деңгейіне (аутентификация, шифрлеу, қайталануға қарсы құралдар, ашық кілттердің инфрақұрылымы және логикалық желі арқылы берілетін модификациялар) байланысты емес.

1.3 Іске асыру деңгейлері

OSI моделінің қандай да бір деңгейінде ақпаратты қорғау деп алдыңғы

деңгейде желілік пакеттердің әрбір келесі деңгейі инкапсулалданған кезде атауға болады. Басқаша айтқанда, қолданбалы қабат хаттамасының деректері (мысалы, HTTP) тасымалдау қабаты пакетінің ішінде болған кезде (мысалы, TCP), ал ол желілік қабат пакетінде (мысалы, IP), және бұл байланыс қабаты жақтауының ішінде (мысалы, Ethernet жақтауы) болғанда.

Желілік деңгейде ақпараттың қауіпсіздігін қамтамасыз ету үшін IP пакеттің барлық мазмұны шифрланады, атап айтқсақ TCP пакеті. Желілік қабатта бүкіл IP пакет шифрланады, содан кейін бұл шифрланған пакет инкапсуляцияланады. Бұл қосымша инкапсуляция ақпарат алмасуға қатысушылар желісінің топологиясын жасыруға көмектеседі.

Қауіпсіз арна (securechannel) – қауіпті желі арқылы деректерді қауіпсіз алмасу механизмі үшін қолданылатын жалпы атау. «Арна» сөзі ақпарат таратудың қауіпсіздігі пакеттік коммутацияланған желіде орналасқан барлық виртуалды канал бойында жұптық желілік тораптар (шлюздер немесе хосттар) арасында жүзеге асырылатындығын білдіреді.

Қауіпсіз деректер каналы OSI моделінің кейбір деңгейлерінде құрылған жүйелік құралдарды қолдану арқылы іске асырылады (ашық жүйелердің өзара әрекеттесу моделі) (1 кесте).

1 кесте – қауіпсіз арна хаттамасының деңгейлері

Қауіпсіз кіру хаттамасы	Қолданбалы	Қосымшаға әсеретіді
	Өкілдік	
	Сеансты	
	Тасымалдау	Қосымша түсінігі
	Желелік	
	Каналды	
	Физикалық	

VPN арналық деңгей. OSI моделінің деректерді байланыстыру қабатында қолданылатын VPN құралдары виртуалды «нүкте-нүкте» (дербес компьютерден ЛВС шлюзіне немесе маршрутизатордан маршрутизаторға) туннельдерін құруға және үшінші деңгейдегі (одан жоғары) әртүрлі трафик түрлерінің инкапсуляциясын қамтамасыз етеді.

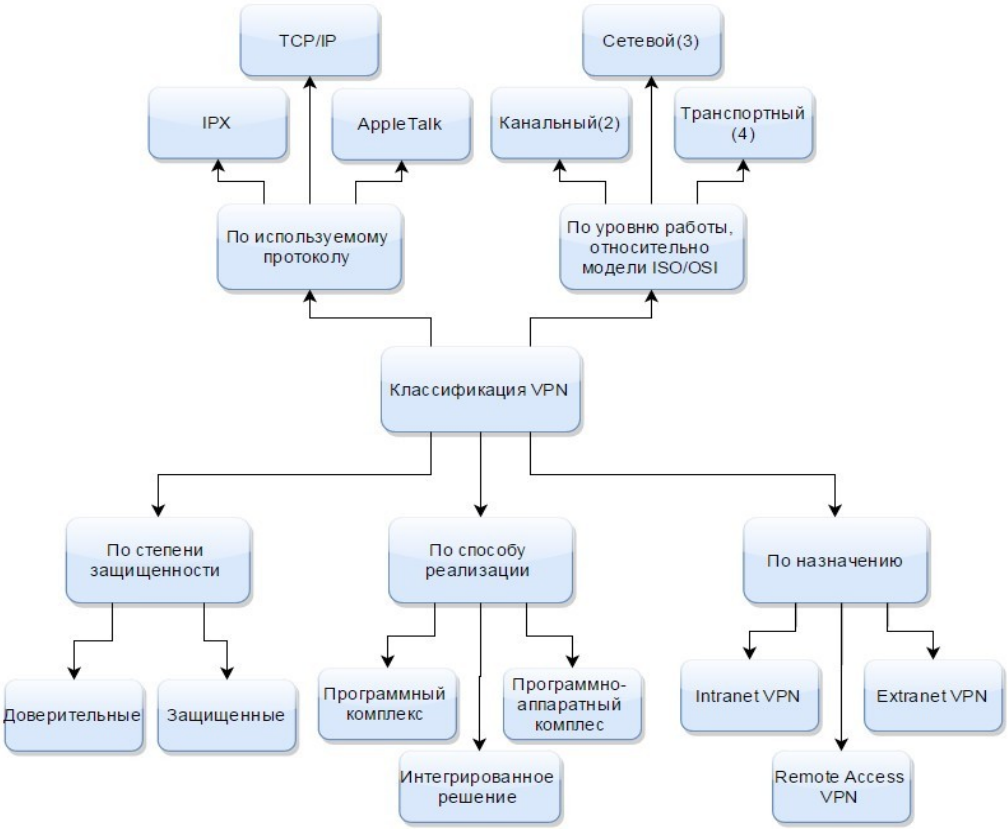
Бұл топқа Layer 2 Forwarding (L2F) және Point-to-Point Tunneling Protocol (PPTP) хаттамалары, сонымен қатар Microsoft және CiscoSystems әзірлеген Layer 2 TunnelingProtocol (L2TP) стандарттарын қолданатын VPN өнімдері кіреді.

VPN желілік деңгейі. VPN өнімдері IP-ға IP-ны инкапсуляциялайды. Осы деңгейдегі ең танымал хаттамалардың бірі IP Security (IPSec) протоколы болып табылады, ол IP-пакеттерді туннелдеуге, аутентификациялауға және шифрлауға арналған. IPSec протоколы Internet Engineering Task Force (IETF) консорциумымен стандартталған, пакеттерді шифрлау бойынша барлық үздік шешімдерді қамтиды және IPv6 протоколына міндетті компонент ретінде кіреді.

VPN тасымалдау деңгейі. Тасымалдау деңгейіндегі хаттамалар қолданбалы хаттамалар мен сервистерді ұсыну хаттамалары үшін айқын (FTP, HTTP, SMTP, POP3, NNTP және т.б.). Тасымалдау деңгейі логикалық байланыстарды орнатуға және осы қосылыстарды басқаруға жауап беретіндіктен, осы деңгейде қосылыстардың дұрыстығын тексеретін және басқа да қорғаныс функцияларын орындауды қамтамасыз ететін аралық бағдарламаларды қолдануға болады.

Тасымалдау деңгейі хаттамаларының арасында ең танымал SSL/TLS (Secure Socket Layer/Transport Layer Security) хаттамасы, etscape Communications фирмасымен әзірленген.

1.4 VPN-нің жіктелуі



1.2 сурет – VPN-нің жіктелуі

VPN жіктелуін бірнеше негізгі параметрлер бойынша жіктеуге болады (1.2сурет).

Іске асыру әдісі бойынша:

- Микробағдарлама негізінде.

VPN желісі құралдардың бағдарламалық-аппарттық кешені есебінен жүзеге асырылады. VPN құрудың бұл әдісі қауіпсіздік пен өнімділіктің жоғары дәрежесін қамтамасыз етеді.

- Бағдарламалық шешімге негізделген.

Бұл шешім VPN қосылымын жасауға мүмкіндік беретін арнайы бағдарламалық жасақтамасы бар дербес компьютердің көмегімен жүзеге асырылады.

- Интеграцияланған шешімге негізделген.

Мұнда VPN басқа тапсырмаларды қарастыратын, мысалы, брандмауэр құратын, қызмет көрсету сапасын және желілік трафикті қарастыратын кешенді ұйымдастырады.

Беру ортасының қорғалу дәрежесі бойынша:

- Қорғалған.

Виртуалды жеке желілердің танымал нұсқасы. Оның көмегімен сіз сенімсіз желіге, әдетте, Ғаламторға негізделген сенімді және қауіпсіз желіні жасай аласыз.

Қауіпсіз VPN мысалдары: IPSec, OpenVPN, GRE және PPTP.

- Сенімді.

Жеке меншік желілердің бұл әдісі деректер тасымалдаушысы сенімді

болғанда және үлкен желі шегінде виртуалды желі құру қажет болғанда қолданылады. Желінің сенімділігіне байланысты қауіпсіздік мәселесі маңызды емес.

Осындай VPN жіктеулерінің мысалдары: L2TP, MPLS.

Мақсаты бойынша:

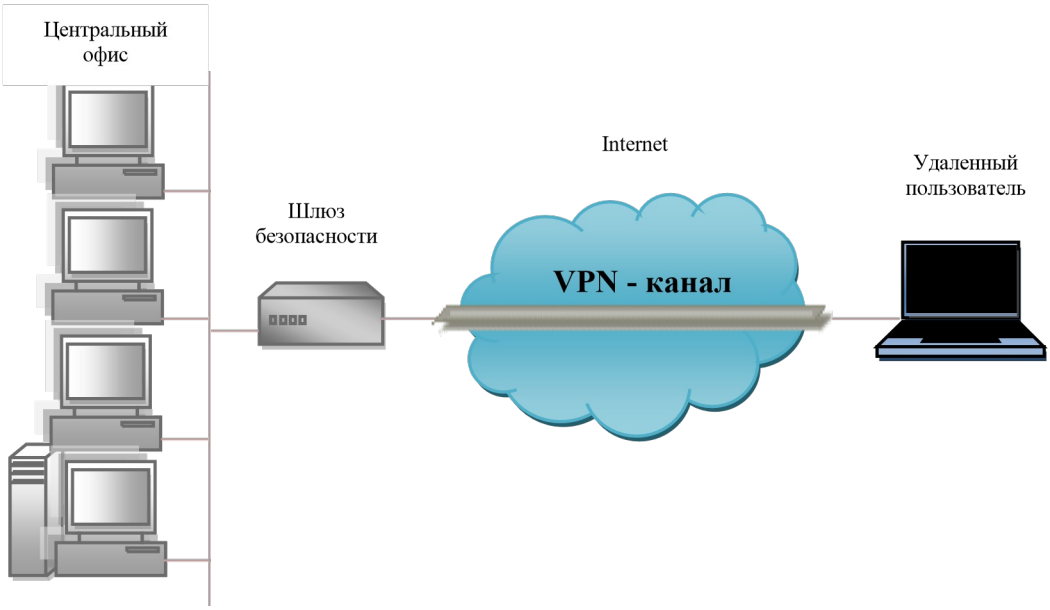
Виртуалды жеке желілердің бірнеше архитектуралық нұсқалары бар.

Виртуалды жеке желілердің негізгі түрлері:

- RemoteAccess VPN (vpn қашықтан қол жеткізу);
- Intranet VPN (ішкі корпоративтік VPN);
- Extranet VPN (корпоратив-аралық VPN).

Компанияның ақпараттық ресурстарына мобильді немесе қашықтағы қызметкерлеріне қауіпсіз қол жетімділікті қамтамасыз ету үшін VPN-ге қашықтықтан қол жеткізу құрылады (1.3 сурет).

Бұл нұсқаның мәні қызметкердің ғаламдық желіге жергілікті қол жеткізу нүктесімен байланыс орнатқандығында, кейін оның орындалуы Ғаламтор арқылы реттеледі.

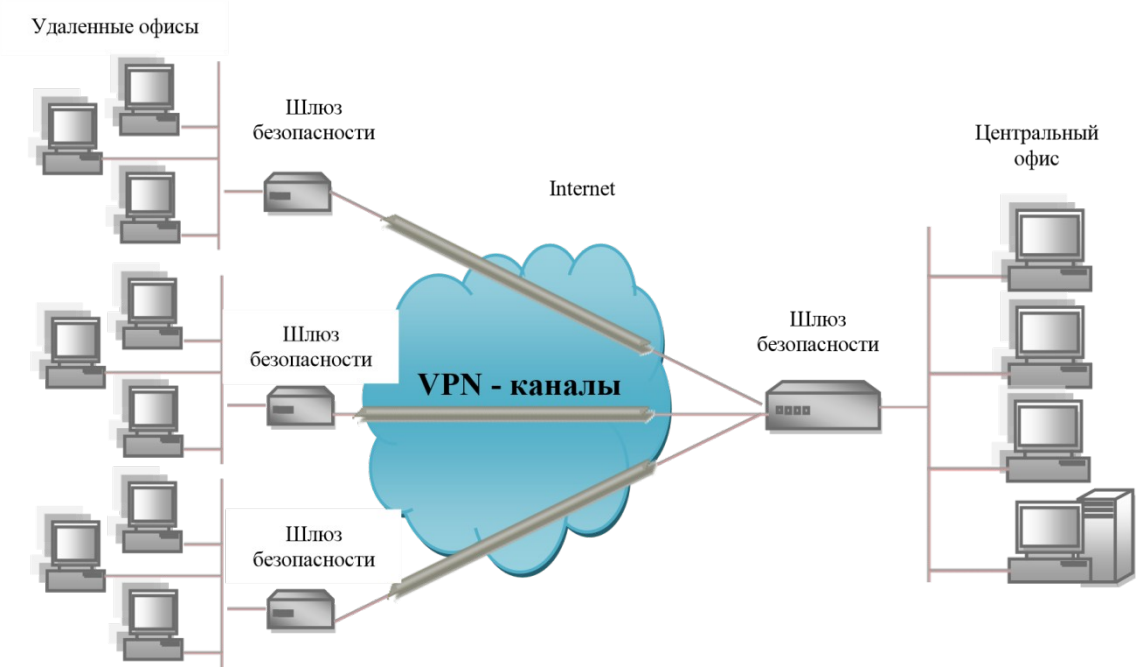


1.3 сурет – Қашықтан қол жетімді VPN

RemoteAccess VPN пайдалану кезінде айтарлықтай үнемдеу - бұл үлкен артықшылық.

VPN ішкі корпоративтік желілері бөлінген компанияның ішкі бөлімшелері арасында немесе корпоративтік байланыс желілерімен біріктірілген кәсіпорындар тобы арасында қауіпсіз қосылуды қамтамасыз ету үшін құрылады (1.4 сурет).

VPN ішкі корпоративтік желілері сервиспровайдерлер ұсынатын Internet немесе бөлінетін желілік инфрақұрылымдардың көмегімен құрылады.



1.4 сурет – Intranet VPN технологиясы арқылы желі тораптарын біріктіру

Корпоратив-аралық VPN (1.5 сурет) – бір ұйымның желісінен екінші

ұйымның желісіне тікелей қатынауды қамтамасыз ететін желілік технология. Технология іскерлік ынтымақтастық процесінде қолдау көрсетілетін өзара әрекеттестіктің сенімділігін арттырады. Корпоратив-аралық VPN пайдаланушылармен, тапсырыс берушілермен, жеткізушілермен, стратегиялық серіктестермен, ірі клиенттермен және басқалармен қауіпсіз ақпарат алмасуды ұйымдастыру үшін қолданылады.

1.5 VPN құрылымы

VPN «ішкі» және «сыртқы» желілерден тұрады. «Ішкі» желі – бұл басқарылатын желі, олардың бірнеше болуы мүмкін. Инкапсулирленген байланыс «сыртқы» желі арқылы өтеді (әдетте Ғаламтор қолданылады).

Қашықтағы пайдаланушы VPN-ге ішкі және жалпы (сыртқы) желіге қосылған қатынасу сервері арқылы қосылады.Қашықтағы пайдаланушыны қосылғанда немесе басқа қауіпсіз желіге қосылу кезінде қол жеткізу сервері процессаидентификацияланады, содан кейін процессааутенттеуден өтуді талап етеді. Екі процесс сәтті өткеннен кейін, қашықтағы пайдаланушыға немесе қашықтағы желіде жұмыс істеу үшін өкілеттілік беріледі, басқаша айтқанда, процессавторизация жүреді.

1.6 Extranet VPN корпоратив-аралық желісі

Extranet VPN желілері Intranet VPN-ге ұқсас. Олардың айырмашылығы ақпараттық қауіпсіздік мәселесі олар үшін анағұрлым өзекті.

Extranet VPN RemoteAccessVPN және IntranetVPN-дықолдану үшін хаттамалар мен архитектураларды қолдана отырып орналастырылады. Басты айырмашылық Extranet VPN пайдаланушыларына берілетін рұқсат олардың серіктесінің желісімен байланысты.

Желілік хаттаманың деңгейі және типі бойынша. IPX, TCP/IP және AppleTalk үшін VPN технологиясының орындалуы бар. Қазіргі уақытта VPN шешімдерінің жиынтығы TCP/IP хаттамасын қолдайды.

VPN желілік хаттамасының деңгейімен бөлу ISO/OSI анықтамалық моделінің деңгейлерімен арақатынас негізінде жүргізіледі.

OSI моделінің «жұмыс» деңгейінің белгісі бойынша. OSI моделінің «жұмыс» деңгейіне сәйкес VPN-ді бөлу үлкен қызығушылық туғызады, себебі іске асырылатын VPN функционалдығы және оның ұйымның ақпараттық жүйесінің қосымшаларымен, сондай-ақ таңдалған OSI деңгейінен қорғаудың басқа да құралдарымен үйлесімдігі барлығына дерлік байланысты.

OSI моделінің «жұмыс» деңгейі бойынша VPN жіктелуі

- Арналық – OSI моделінің (L2) арна деңгейінде желілер арасындағы байланысты қамтамасыз етеді. Мысалы, L2VPN MPLS арқылы жұмыс істейді, ал L2TP желілік деңгейде жұмыс істейді.

- Желілік – OSIмоделініңжелілікдеңгейінде (L3) желілерді байланыстырады. Мысалдар: IPSEC, IPIP.

- Тасымалдаушы – желілерді осьтік модельдің көлік қабаты (L4) арқылы байланыстырады. Мысалдар: SSH туннелі, OPENVPN.

VPN құрылысы. VPN құрудың әртүрлі шешімдері бар. Шешім таңдау үшін VPN құру құралдарының өнімділігін ескеру қажет.Тәжірибе көрсеткендей, VPN құру үшін арнайы жабдықты қолданған дұрыс, алайда қаражат шектеулі болса, онда бағдарламалық жасақтаманың опциясын ғана пайдалануға болады.

Төменде VPN құрудың бірнеше нұсқалары келтірілген.

Маршрутизаторлар негізіндегі VPN. VPN құрудың келесі мүмкіндігі – қауіпсіз арналарды құру үшін маршрутизаторларды пайдалану.Жергілікті желіден шығатын барлық ақпарат маршрутизатор арқылы жүреді, сондықтан шифрлау тапсырмаларын осы маршрутизаторға сеніп тапсырған жөн.

VPN құру үшін маршрутизаторларда жабдық үлгісі ретінде CiscoSystems компаниясының жабдығы қызмет ете алады. Ciscointegratedservicesrouters (ISR) 1700 сериялы маршрутизаторлары, 1800, 2600XM, 3700 аумақтық бөлімшелері бар үлкен компаниялар үшін де, шағын кеңселер үшін де қолайлы.Cisco маршрутизаторлары IPSec, L2TP, SSL, MPLS, GRE және L2F өткізілетін ақпаратты жай шифрлаумен қатар, Cisco басқа VPN мүмкіндіктерін қолдайды, мысалы, кілт алмасу және туннельді аутентификация.

Брандмауэр базасындағы VPN. Брандмауэр өндірушілерінің көпшілігі деректерді шифрлауды және туннельдеуді жүзеге асырады. Ұқсас өнімдер брандмауэр арқылы өтетін трафик шифрланатын етіп жасалынған. Брандмауэрдің бағдарламалық жасақтамасына шифрлау модулі қосылады. Бұл шешім кемшілігі – брандмауэр жұмыс істейтін аппараттық қамтамасыз ету өнімділігіне тәуелділік болып табылады.

Брандмауэр базасындағы VPN үлгісі ретінде ENTENSYS ресейлік компаниясының usergateproxy&Firewall 6.0 VPN GOST деп атап айтсақ болады, онда толыққанды VPN-сервер іске асырылған.

Бағдарламалық қамтамасыз ету базасындағы VPN. VPN құру тәсілдері бағдарламалық шешімдер болып табылады.Мұндай шешімдерді іске асыру барсында арнайы бөлінген компьютерде жұмыс істейтін және көптеген жағдайларда proxy-сервер ретінде әрекет ететін мамандандырылған бағдарламалық қамтамасыз ету қолданылады.

Бағдарламалық жасақтама шешімімен орындалған VPN өнімдері

мамандандырылған құрылғыларға қарағанда төмен, бірақ VPN желілерін іске қосу үшін жеткілікті қуатқа ие.

Қазіргі уақытта PPTP, L2TP, PPPoE сияқты әртүрлі VPN хаттамаларын қолдайтын VPN серверлерінің көптеген бағдарламалық қамтамасыз етілулері бар.

Мұндай шешімнің мысалы – VPN құруға арналған LogMeIn-тің Hamachi бағдарламалық жасақтамасы. Архитектура – Hamachi екі түйіні өзара аутентификациядан кейін және сеанстың кілті туралы келісімнен кейін бір-бірімен байланысады. Трафик тікелей бір нүктеден екінші нүктеге бағытталған, сервер арқылы жіберілуі керек трафик ақырғы нүктелерде шифрланған және қорғалған. Hamachi IPsec, PPTP және 256-биттік SSL шифрлауды пайдаланып, жеке желілер арқылы сенімді қорғаныс байланысын қолданады.

Бағдарламалық жасақтама өнімдерінің айқын артықшылығы ол икемділік және пайдаланудың қарапайымдылығы, сонымен қатар салыстырмалы түрде арзан бағасы.

Аппараттық құралдар базасындағы VPN. VPN шлюзі – бірнеше желіге қосылған желілік құрылғы, оның артында бірнеше хост үшін шифрлау және аутентификация функцияларын орындайды.

Бөлінген аппараттық VPN шлюздер құны басқа барлық мүмкін көрсеткіштер бойынша көшбасшы.Мұндай VPN-нің басты артықшылығы – олардың жоғары өнімділігі, себебі жылдамдық шифрлау арнайы микросхемалармен жүзеге асырылады. Арнайы VPN құрылғылары жоғары қауіпсіздік деңгейін қамтамасыз етеді.

Аппараттық шешімдердің есептеу қуаты өте жоғары, бірақ әрдайым талап етілмейді, сондықтан бағдарламалық шешімдер, әсіресе стандартты шешімдер осындай үлкен танымалдыққа ие болды.

Желілік операциялық жүйелер базасындағыVPN. Желілік операциялық жүйе базасында VPN құру стандартты құралдардың көмегімен жүзеге асырылады.Қарастыру үшін Microsoft WindowsServer 2012 R2 жүйесін алайық. VPN қосылымдарының қауіпсіздігін арттыру үшін L2TP/IPsec сандық сертификаттар мен екі факторлы аутентификацияны қолдана отырып негізгі хаттама ретінде қолданылады. Байланыс орнатпас бұрын, түйіндер сертификаттың немесе алдын-ала берілген кілттің негізінде бір-бірінің түпнұсқалығын тексереді, содан кейін қосылуды жалғастырады.

Сертификаттың аутентификациясы PKI желісінің инфрақұрылымын қажет етеді, ол болмаған жағдайда, аутентификацияны алдын ала кілт бойынша пайдалануға болады.

Алдын-ала кілт аутентификациясы сертификатқа негізделген аутентификацияға қарағанда сенімді емес. Уақытша кілт клиентте VPN қосылымын құру кезінде бір рет көрсетіледі және пайдаланушыға белгісіз болуы мүмкін (орнатуды әкімші жасайды). Егер қашықтан кіру серверіндегі алдын-ала кілт өзгерсе, бірде-бір VPN клиенті жаңа қызмет профилін алғанға

және орнатқанға дейін алдын-ала кілт арқылы серверге кіре алмайды.

Бұл шешім Windows корпоративті операциялық жүйе ретінде пайдаланатын компаниялар үшін өте ұтымды. Мұндай шешімнің құны басқа шешімдердің құнынан едәуір төмен екендігіне назар аудару керек.

1.7 VPN желілерін іске асыру әдістері

Виртуалды жеке желіні іске асыру 3 әдістен құрылады:

- Туннелдеу;
- Аутентификациялау;
- Шифрлеу.

Туннельдеу (инкапсуляция) – бұл негізгі желілік хаттаманы екінші желілік хаттамаға ендіру.Инкапсуляция VPN құрудың басты тәсілі болып табылады.

VPN технологиялары кешені деректерді атауымен туннелдеуді жүзеге асырады,ол транзиттік желі бойынша осы деректерді жіберу үшін маршруттау ақпаратын сақтайды.

Туннельдеу процесіне үш хаттама іске асырылады:

1. тасымалданатын;
2. тасымалдаушы;
3. инкапсуляция хаттамасы.

Біріккен желілердің хаттамасы – тасымалданатын, ал транзиттік желінің хаттамасы – тасымалдаушы. Туннельдік протоколды қолдана отырып, тасымалданған хаттаманың пакеттері тасымалдаушы протокол пакеттерінің деректер өрісіне «жасырын» болады. Пакеттер - «жолаушылар» транзиттік желі арқылы беру кезінде өзгеріссіз қалады.

Туннельдеу туннельдің екі ұшының арасында деректердің берілуін жасайды, осылайша қабылдағыш пен деректер көзі олардың арасында орналасқан барлық желілік инфрақұрылымды жасырады.

Туннельге кірер кезде туннельдің тасымалдау құралы пайдаланылған желілік хаттаманың пакеттерін алады және ешқандай өзгеріссіз оларды шығуға әкеледі. Туннель екі желілік торапты, олар жұмыс істейтін бағдарламалық жасақтама бірдей желіге қосылатындай етіп қосуға жеткілікті. Дегенмен, бұл шын мәнінде деректер ашық жалпыға қол жетімді көптеген аралық тораптар (маршрутизаторлар) арқылы өтетінін есте ұстаған жөн.

Бұндай жағдай екі мәселеге әкеледі. Біріншісі, туннель арқылы берілген ақпарат шабуылдаушыларға қол жеткізе алады. Сондай-ақ, шабуылдаушылар туннель арқылы жіберілген деректерді қабылдаушы олардың сенімді немесе сенімді еместігін тексере алмайтындай етіп өзгертуге мүмкіндік жасайды. Жоғарыда айтылғандарды ескере отырып, туннель өзінің таза түрінде онлайн-компьютерлік ойындарға жарамды және одан әлдеқайда маңызды нәрсе талап ете алмайды.Бұл проблемалар ақпаратты қорғаудың заманауи

криптографиялық құралдарының көмегімен шешіледі. Туннельден өту кезінде деректер пакетіне рұқсатсыз өзгертулердің енуіне жол бермеу үшін электрондық цифрлық қолтаңба (ЭЦҚ) әдісі қолданылады.Әдістің барлық мәні әрбір берілген пакетке асимметриялық криптографиялық алгоритмге сәйкес құрылған және пакеттің ішкі мазмұны мен жіберушінің ЭЦҚ құпия кілті үшін қосымша ақпарат блогы қосылатындығында. Ақпараттары бар бұл блок пакеттің электрондық цифрлық қолтаңбасы болып табылады, оның көмегімен мәліметтер алушының аутентификациясы болып табылады, ол үшін жіберушінің ЭЦҚ ашық кілті белгілі.

VPN туннель бойынша берілетін хабарламалар пакеттерінің қорғалуына әсер етпейді. Дегенмен инкапсуляцияның арқасында капсулаланған пакеттерді толығымен шифрлауға болады. Инкапсуляцияланатын пакеттердің құпиялылығы оларды криптографиялық жабу, яғни шифрлау жолымен, ал тұтастығы мен түпнұсқалылығы – цифрлық қолтаңбаны қалыптастыру жолымен қамтамасыз етіледі.

Аутентификация. VPN байланысы үшін аутентификацияның үш нұсқасын қарастырайық:

1. PPP хаттамасы бойынша пайдаланушы деңгейінде тексеру.

VPN қосылымын құруға арналған VPN сервері PPP қолданып пайдаланушы деңгейінде қосылымды орнататын VPN клиентінің түпнұсқалығын тексереді. Ол VPN клиентінде қажетті авторизация бар-жоғын тексереді. Екі жақты аутентификация кезінде VPN клиенті VPN серверін де аутентификациялайды. Бұл VPN серверлерін бейнелейтін компьютерлерден қорғауды қамтамасыз етеді.

2. IKE хаттамасы бойынша компьютер деңгейінде тексеру.

Алдын ала кілтпен немесе IPsec VPN-клиент және VPN-сервер компьютерлерінің сертификаттарымен алмасу үшін IKE хаттамасын қауіпсіздікті салыстыру үшін қолданады. VPN-клиент және VRN-сервер барлық жағдайларда компьютер деңгейінде бір-бірінің түпнұсқалығын тексеруді орындайды. Бұл ретте компьютер сертификаты бойынша шынайылығын тексеру ұсынылады. Бұл әдіс қауіпсіз деп саналады. Компьютер деңгейінде түпнұсқалығын тексеру тек L2TP / IPSec қосылымдары үшін орындалады.

3. Деректер көзін тексеру және деректердің тұтастығын қамтамасыз ету.

Деректері VPN қосылымына дәл солай жіберілгеніне және беру кезінде олардың сыртқы көрінісі өзгермегеніне көз жеткізу үшін, мәліметтерді шифрлауды тексеру кестесі де бар. Ол тек жіберуші мен қабылдағышқа белгілі шифрлау кілтіне негізделген. Берілген деректердің тұтастығын және деректер көзінің түпнұсқалығын тексеру тек L2TP/IPSec қосылымдары үшін жүзеге асырылады.

VPN-нің негізгі қызметі ақпараттың қауіпсіз берілуін құру болып табылады. VPN клиенттерінен VPN серверіне мәліметтер Ғаламтор арқылы

жіберіледі.Бұл сервер клиенттің компьютерінен алыс орналасуы мүмкін, және деректер компания желісіне бүкіл жол бойы провайдерлердің массалық жабдығын сатып алады.ректердің оқылмағанына немесе өзгертілмегеніне көз жеткізу үшін түпнұсқалық растама мен шифрлаудың әртүрлі әдістері қолданылады.

IPSec-пен өзара әрекеттескен кезде L2TP хаттамысы PPP базасында түпнұсқалықты тексерудің стандартты әдістерін қолданады, мысалы:

- MSCHAP (1 және 2 нұсқалар);
- EAP;
- SPAP;
- CHAP;
- PAP.

Жалпы хаттамалар Microsoft Challenge Handshake Authentication Protocol 2-нұсқасы және Transport Layer Security (EAP-TLS), олар бір-бірінің аутентификациясын жүзеге асырады, басқаша айтқанда, VPN клиенті мен сервер бір-бірін анықтайды.

PPTP деректерді қорғайды, бірақ IPSec және L2TP сенімдірек. L2TP Ipsec «компьютер» және «пайдаланушы» деңгейлерінде аутентификацияны жүзеге асырады, сонымен қатар деректерді шифрлауды жүзеге асырады.

Сервер мен клиенттің аутентификациясының бастапқы кезеңінде L2TP және IPSec екеуі сертификаттау қызметінен алынған жергілікті сертификаттарды қолданады.Сервер мен клиент сертификаттармен алмасады және ESP SA (security association) қорғалған байланысын қалыптастырады. L2TP хаттамасын IPSec-пен бірге компьютердің аутентификациясы тәртібі аяқталғаннан кейін, пайдаланушы тарапынан аутентификация жүзеге асырылады. Мұны істеу үшін сіз кез-келген хаттаманы, мысалы, қолданушы аты мен құпия сөзді жабық түрде жіберетін PAP-ті қолдана аласыз. Бұл салыстырмалы түрде қауіпсіз, себебі L2TP IPsec көмегімен бүкіл сессияны шифрлайды. Дегенмен, MSCHAP көмегімен пайдаланушының түпнұсқалығын растауды енгізу компьютер мен пайдаланушының түпнұсқалығын растау үшін шифрлау кілттерінің барлық түрлерін қолдану қауіпсіздікті арттыруға көмектеседі.

1993 жылы BlowFish айнымалы кілті бар 64 биттік шифр алгоритмі жасалды. BlowFish алгоритмінің ерекшелігі – DESалгоритмінен айырмашылығы криптографиялық беріктіктің жоғары деңгейі (оның ішінде 448 битке дейін ауыспалы кілттерді пайдалану арқылы), шифрлаудың жоғары жылдамдығы (шифрлаудың жылдамдығы (ауыстыру кестелерінің пайда болуына байланысты) және оны кез келген мақсатта еркін пайдалану мүмкіндігі.

Қазір ұзындығы 128 биттен кем кілтті пайдалана отырып VPN – шифрлауды табу мүмкін емес. Ұсынылған OpenVPN-шешімдерде кілттер тіпті 2048 бит болады.

Бүгінгі таңда AES – ең кең таралған симметриялық шифрлау

алгоритмдерінің бірі. AES (AdvancedEncryptionStandard) - симметриялық блокты шифрлау алгоритмі (блоктың өлшемі 128bit, 128/192/256 биттік кілт). Бұл алгоритм жеткілікті жақсы талданған және қазіргі уақытта кеңінен қолданылады.

Сонымен қатар Шифрлаудың бірнеше әдісі де қолданыста, олар:

- MPPE шифрлау хаттамасы (MicrosoftPoint-to-PointEncryption тек MSCHAP-пен үйлесімді (1 және 2-нұсқалар) және ұзындығы 40, 56 немесе 128 битті кілттермен жұмыс жасауды қолдайды);
- EAP-TLS (клиент пен сервер арасындағы параметрлерді келісу кезінде шифрлау кілтінің ұзындығын автоматты түрде таңдай алады).

Сонымен, туннельдеу, шифрлау және аутентификация жеке (жергілікті) желінің жұмысын іске асыра отырып, екі нүкте арасында жалпыға қол жетімді желі арқылы мәліметтерді қауіпсіз жіберуді қамтамасыз етеді. Басқаша айтқанда, виртуалды жеке желі осы «тізбектен» құрылған.

2 VPN желілерінің хаттамалары

Корпоративтік желілерде қауіпсіз деректер алмасуды қамтамасыз ету үшін виртуалды жеке желілердің әртүрлі хаттамалары қолданылады. Олардың өзіндік кемшіліктері мен артықшылықтары бар. Енді әрбір хаттаманы жеке талдауға кірісейік.

Хаттама – бұл екі және одан да көп тараптарды жүзеге асыратын іс-қимыл тәртібі болып табылады. Бұл белгілі бір міндеттерді шешу үшін жасалған әрекет тәртібі.

VPN желілері әдетте internet желісі бойынша пайдаланылатын байланыс желісі арқылы деректерді инкапсуляциялау хаттамаларын қолдана отырып құрылады. Туннелдеу хаттамалары деректерді шифрлауды қамтамасыз етеді, сондай-ақ, пайдаланушылар арасында деректердің тасымалын жүзеге асырады.Қазіргі таңда VPN желілерін құру үшін келесі деңгей хаттамалары қолданысқа алынған:

- Арналық;
- Желілік;
- Тасымалдаушы.

Арналық деңгейде тунельдеу хаттамаларымен қатар аутентификация мен авторизацияны пайдаланатын PPTP және L2TP сияқты туннельдеу хаттамалары қолданылады.

2.1 PPTP

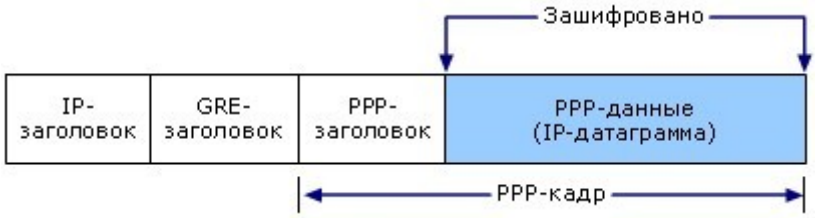
Point-to-point tunneling protocol – нүкте-нүкте типті тунельдік хаттамасы компьютерге стандартты, қауіпті емес желіде арнайы туннель құру арқылы сервермен қауіпсіз байланыс орнатуға мүмкіндік береді.

VPN – хаттама қауіпсіздікке арналған аутентификацияның әртүрлі әдістеріне негізделген (ең көп таралғаны MS-CHAP v.2). PPTP – бұл ұзақ уақыт аралығына VPN енгізуге арналған стандартты хаттама. Хаттама барлық дерлік құрылғыларда және амалдық жүйелерде VPN қолдайтын стандартты хаттама түрінде орындалуы мүмкін. Бұл сізге қосымша бағдарламалық жасақтаманы орнатпай-ақ пайдалануға мүмкіндік береді.

Бұл хаттаманың тағы бір артықшылығы есептеу үшін аз ресурстарды пайдаланады, яғни оның жылдамдығы жоғары. PPTP ескірген екі нүктелік PPP байланыс хаттамасына арқа сүйейді. Әдетте ол екі желі торабының арасында тікелей байланыс жасау үшін қолданылады; шифрлауды, деректерді қысуды және байланысты аутентификациялауды қамтамасыз етеді. Сондықтан PPP тәжірибеде PPTP қосылу сессиясының байланыс протоколы болып қала береді.

PPTP хаттамасының инкапсуляциясы PPP кадрын желі арқылы жіберу үшін IP датаграммаларына орналастырады (2.1 сурет). PPTP туннельді басқару

хаттамасы үшін TCP қосылымын пайдаланады.Мұнда туннельделген деректер PPP кадрларын инкапсулирлеу үшін GRE хаттамасының өзгертілген нұсқасы қолданылады. Сервер мен клиент туннель жасағаннан кейін қызметтік пакеттермен алмасады. PPP-кадрдың қажетті деректері бір уақытта кішірейтілген, шифрланған немесе ауысқан болуы мүмкін.



2.1 сурет – IP датаграммасы бар PPTP-пакеттің құрылымы

Жіберуден бұрын деректерді туннелдеу екі кезеңді қамтиды:

- PPP ақпараттық бөлімі қалыптасады. OSI қолданбалы қабатындағы деректер арнаға жіберіледі.
- Алынған деректер OSI моделі бойынша жоғарыға және жоғарғы деңгейдегі хаттамалармен инкапсуляцияланады.

Екінші өту кезеңінде деректер тасымалдау деңгейіне дейін жеткізіледі. Бірақ бұл үшін OSI арналық деңгейі жауап беретіндіктен, ақпарат тағайындау пунктіне жіберілуі мүмкін емес. Осыған орай, PPTP пакеттік жүктеме өрісін шифрлайды және PPP-ге тиесілі екінші деңгейлі тапсырмаларды қабылдайды, яғни PPP тақырыбын қосады және PPTP пакетімен аяқталады.

PPP жақтауы MPPE шифрлау алгоритмін қолдана отырып, MS-CHAP протоколының 2 – нұсқалық немесе EAP-TLS көмегімен аутентификация кезінде жасалған шифрлау кілттерін қолданып шифрланады.

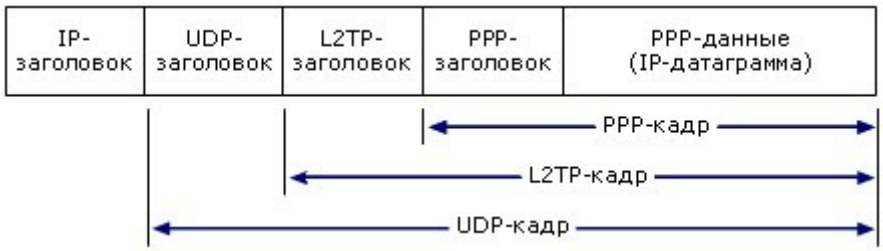
PPTP әдетте 128 биттік шифрлаумен қолданылады, дегенмен бірқатар осалдылықтар табылды. MS-CHAP v.2 аутентификация хаттамасының осалдығы олардың ішіндегі ең қауіптіі болып табылады.Осы осалдықты пайдаланып PPTP-ны екі күнде бұзуға болады.

2.2 L2TP/Ipsec

Екінші деңгейлі туннельдік хаттама (Layer 2 TunnelingProtocol) – бұл VPN хаттамасы, құпиялылықты және ол арқылы өтетін трафикті шифрлауды қамтамасыз етпейді. Сондықтан IPsec шифрлау протоколы әдетте құпиялылық пен қауіпсіздікті қамтамасыз ету үшін іске қосылады.

L2TP/IPsec пакеттік инкапсуляциясы келесі екі деңгейде жүзеге асырылады:

- Бірінші деңгей (L2TP инкапсуляциясы);
- L2TP және UDP тақырыптары PPP жақтауы құрамына енеді (IP датаграммаларына) (2.2 сурет).



2.2 сурет – IP датаграммасы бар L2TP-пакетінің құрылымы

Екінші деңгей (L2TP инкапсуляциясы).

Алынған L2TP хабарлама IPsec түпнұсқалық растама тақырыбымен және ESP жабу хаттамасымен толықтырылады. Ол хабарламаның түпнұсқалығын, тұтастығын және соңғы IP тақырыбын қамтамасыз етеді (2.3 сурет).

IP тақырыбында VPN серверіне және VPN клиентіне сәйкес келетін бастапқы және тағайындалған IP-мекенжайлары болады.

2.3 сурет – Ipsec ESP хаттмасы арқылы L2TP трафигін шифрлау

2.3 L2TP

L2TP L2F (Layer 2 Forwarding) және PPTP хаттамаларының қосылуы есесінде пайда болды. PPTP туннель арқылы PPP пакеттерін, L2F PPP және SLIP пакеттерін жіберуге мүмкіндік береді. Көпшіліктің пікірінше, L2TP хаттамасы L2FP және PTP-тің ең жақсысын өзіне айналдырды.

L2TP Microsoft корпорациясы UDP пакеттерін PPP шифрланған пакеттерін сақтайтын бақылау хабарламалары ретінде пайдаланады.Ол туннельді басқару үшін де, деректерді беру үшін де бірдей хабарлама форматын қолданады.Пакеттердің реттілігін бақылау сенімді жеткізу кепілдігін береді.

L2TP және PPTP функционалдық мүмкіндіктері әр түрлі.PPTP тек IP желілерінде ғана қолданылады және туннельді қалыптастыру және пайдалану үшін оған бөлек TCP қосылымы қажет.L2TP тек IP желілерінде ғана қолданылмайды.L2TP IPSec-пен бірге PPTP-ге қарағанда қауіпсіздік деңгейлерін қамтамасыз етеді және компанияның маңызды мәліметтерінің

100% қауіпсіздігіне кепілдік береді.

2.4 IPSec

IPSec (Internet Protocol Security) – күшті шифрлау алгоритмдерімен VPN арнасының қауіпсіздігін қамтамасыз ететін стандарт. IPSec хаттамасы желілік деңгейде қорғауды қамтамасыз етіп, IPSec стандартын тек бір-бірімен байланысқан құрылғылардан ғана қолдауды талап ете отырып, Ғаламтор хаттамасына арналған қауіпсіздік негіздерін құрады.

SecurityAssociation (SA) – «Қауіпсіз қауымдастық» термині IPSec технологиясын пайдаланатын тұлғалардың өзара әрекет ету әдісін білдіреді. Қауіпсіз қауымдастық бір-біріне берілетін деректерді қорғау үшін IPSec қолданатын тараптардың келісімі аясында жұмыс жасайды.

Бұл келісім төмендегі параметрлерді реттейді:

- кілттермен алмасу тәртібі;
- жіберушінің және алушының IP-мекенжайлары;
- криптографиялық алгоритм;
- аутентификация алгоритмі;
- кілттердің қызмет ету мерзімі;
- кілттердің өлшемдері.

IPSec мынандай стэк-хаттамаларды құрайды: AH, ESP, IKE (2.4 сурет).

2.4 сурет – IPSec стек-хаттамаларының архитектурасы

Жоғарғы деңгейде IPSec ядросын құрайтын үш хаттама бар:

1. *IKE* (InternetKeyExchange) – виртуалды арна параметрлерін келісу және кілттерді басқару хаттамасы. Ол қолданылатын шифрлау алгоритмдерін келісуді қоса алғанда, қорғалған арнаны инициалдау тәсілін анықтайды.

Сондай-ақ, ол қауіпсіз қосылу шегінде құпия кілттерді алмасу және басқару рәсімдерін анықтайды;

2. *AH* (Authenticationheader) – аутентификациялайтын тақырып хаттамасы. Ол деректерді жіберушінің аутентификациясын, қабылдау аяқталғаннан кейін олардың тұтастығы мен түпнұсқалығын тексеруді жүзеге асырады, сонымен қатар бірдей хабарламаларды енгізуден қорғайды;

3. *ESP* (EncapsulatingSecurityPayload) - мазмұнды қорғаудың инкапсуляциялық хаттамасы. Ол криптографиялық жасыруды, аутентификацияны және деректердің тұтастығын жүзеге асырады, сонымен қатар қайталанатын хабарламалардың енуінен қорғайды.

AH және ESP хаттамаларын кез келгенін жеке немесе басқасымен бірге де қолдануға болады. AH және ESP хаттамаларының көрсетілген функциялары ішінен бұл хаттамалардың мүмкіндіктері ішінара қабаттасатыны анық.

IPSec архитектурасының **орташа деңгейі** IKE хаттамасында қолданылатын параметрлерді келісу және кілттерді басқару алгоритмдерін ұйымдастырады. Ол сонымен қатар ESP мазмұнын және аутентификацияның түпнұсқалық растамасын AH мазмұнын инкапсуляциялық қауіпсіздік хаттамаларында қолданылатын шифрлау және аутентификация алгоритмдерін қалыптастырады.

IPSec архитектурасының **төменгі деңгейі** Domain of Interpretation (DOI) деп аталады – интерпретация домені. DOI интерпретациясының доменін ESP және AH хаттамалары модульдік құрылымға ие болғандықтан қолданылады. Бізге барлық қолданылатын және жаңадан енгізілген хаттамалар мен алгоритмдердің ортақ жұмысын қамтамасыз ететін модуль қажет. Бұл DOI интерпретациясының міндетіне жүктелген. DOI интерпретациясының домені IPSec-те қолданылатын протоколдар мен алгоритмдер, олардың параметрлері, протокол идентификаторлары және т.б. мәліметтер базасы ретінде ақпаратты қамтиды. Осылайша, IPSec архитектурасында DOI басты базасының рөлін атқарады.

2.5 OpenVPN (SSL)

OpenVPN – бұл жаңа технологиялық ашық код. Сенімді VPN шешімін ұсынудың әртүрлі технологияларымен бірге SSLv3/TLSv1 хаттамаларын және OpenSSL кітапханасын пайдаланады. OpenVPN-нің басты артықшылығының бірі параметрлердің икемділігі. Бұл хаттама кез-келген портта, атап айтқанда 443 TCP портында конфигурацияланған. Бұл қалыпты HTTPS бойынша OpenVPN ішіндегі трафикті жасыруға мүмкіндік береді, сондықтан оған кіруді шектеу қиынға соғады.

OpenVPN-нің тағы бір артықшылығы ол криптографиялық қорғау үшін қолданылатын OpenSSL кітапханаларының көптеген криптографиялық алгоритмдерді (мысалы, Blowfish, AES, CAST-128, 3DES, Camelia және басқалары) қолдауы. VPN провайдерлері қолданатын ең танымал алгоритмдері

– Blowfish және AES. Екеуі де қауіпсіз деп саналады, дегенмен жаңа AES технологиясы Blowfish сияқты 64 биттік емес, 128 биттік блок өлшеміне ие. Бұл үлкен файлдармен (1ГБ-тан көп) AES жақсы жұмыс атқарады. OpenVPN жылдамдығы қолданылатын шифрлау алгоритміне байланысты.

OpenVPN операциялық жүйелердің стандартты мүмкіндіктеріне кірмейді, бұл хаттамағабейтарап бағдарламалық жасақтамалар арқылы қолдау көрсетіледі. Көп уақыттан бері iOS пен Android жүйелерінде OpenVPN-ді «root» көмегінсіз пайдалану мүмкін болмады, қазіргі уақытта бұл мәселені шешетінөзге қосымшалар бар.

OpenVPN-нің тағы бір мәселесі оның икемділігінде. Бұл параметрді ыңғайсыз жағдайға түсіруі мүмкін. Мысалы, OpenVPN типтік бағдарламалық жасақтамасын қолданған кезде (мысалы, Windows үшін OpenVPN стандартты клиенті) клиентті жүктеп алып, орнату керек, содан кейін қосымша конфигурация файлдарын жүктеу және орнату қажет. Әр түрлі VPN провайдерлері бұл мәселені алдын-ала теңшелген VPN клиенттерінің көмегімен шешеді.

2.6 MPLS

MPLS (Multiprotocollabelswitching) – көп хаттамалыды таңбаларды коммутациялау – жоғары жылдамдықты телекоммуникациялық желідегі мәліметтерді бір желінің торабынан екіншісіне беру үшін тегтерді қолданатын технология.

MPLS ол масштабталатын және басқа хаттамаларға тәуелсіз деректерге беру механизмі.MPLS ұйымдастырылған желідегі деректер пакеттеріне таңба қойылады. Белгіленген белгінің мәні бойынша (деректер пакетін өзі ашудың қажеті жоқ) деректер пакетін одан әрі екінші желілік торапқа жіберу туралы шешім қабылданады. Осының арқасында сіз кез-келген деректерді беру хаттамаларымен жұмыс істеп, жіберу желісіне тәуелді емес виртуалды арнаны іске асыра аласыз.

MPLS OSI моделінің арналық және үшінші желілік қабаттары арасындағы деңгейінде жұмыс істейді, сондықтан оны әдетте арналық-желі қабатының хаттамасы деп атайды. Ол коммутацияланған желілердің клиенттеріжәне пакеттік коммутацияланған желілер үшін әмбебап деректермен қамтамасыз ету мақсатында құрылған. MPLS көмегімен әркелкі трафик түрін жіберуге болады: ATM, SONET, IP-пакеттері мен Ethernet кадрлары.

VPN-ді арналық деңгейінде ұйымдастыру айтарлықтай шектеулі, әдетте провайдер домен шеңберінде әрекет ету аймағы бар.

Желілік деңгейде (IP деңгейі) шифрлауды және деректердің құпиялығын, сондай-ақ абоненттің аутентификациясын жүзеге асыратын IPSec хаттамалары қолданылады. IPSec хаттамасын қолдану корпоративтік желіге тең физикалық қосылуға толыққанды қол жеткізуге мүмкіндік береді.VPN құру үшін әр клиенттің IPSec енгізетін бағдарламалық жасақтамасы болуы керек.

SSTP (Secure Socket Tunneling Protocol) – сокеттердің қауіпсіз туннелдеу хаттамасы. Бұл HTTPS және TCP 443 портын PPTP және L2TP/IPsec трафигін бұғаттай алатын брандмауэрлер мен веб-прокси арқылы тарату үшін пайдаланатын хаттама.

SSTP инкапсуляциясы. Желі арқылы жіберу үшін, SSTP IP-диаграммалардағы PPP кадрларын инкапсуляциялайды.SSTP протоколы TCP байланысын (порт 443) туннелді басқару және PPP деректер кадрларын тасымалдау үшін пайдаланады.

SSTP шифрлау. SSTP хабарламасы HTTPS SSL арнасының көмегімен шифрланады.

SSTP клиент VPN байланысын орнатуға тырысқан кезде SSTP серверімен екі жақты HTTPS қосылымын орнатады. Хаттама пакеттері осы HTTPS деңгейінде пайдалы деректер түрінде беріледі.

SSTP Windows-ке салынғандықтан, OpenVPN-ге қарағанда пайдалану оңайырақ және тұрақты. HTTPS бөлек хаттама емес. Бұл HTTP хаттамада шифрланған SSL және TLS тасымалдау механизмдері қосылады. Шифрлау құралдары мен тексерілген сервер сертификатын пайдаланған кезде протокол желілік қосылымды тыңдауға негізделген шабуылдардан қорғайды.

3 ТАҢДАЛМАЛЫ ХАТТАМА

Біздің ұйымымызға ең қолайлы қосылымды таңдау үшін ең көп таралған VPN хаттамасын қарастырып, салыстырайық. Қашықтағы пайдаланушыда ұйымға қосуды жүзеге асыру тәуелдігі туындайды. Әрбір хаттаманың артықшылықтары мен кемшіліктері бар, олар қосылысты құру үшін белгілі бір хаттаманы таңдауда шешуші болуы мүмкін.

Негізгі VPN хаттамаларын қарастырайық. Олар: L2TP/IPSEC, PPTP және OpenVPN. Зерттелетін және талданатын негізгі өлшемдер – қауіпсіздік, жылдамдық, орнатудың қарапайымдылығы. Айырмашылығын білу мақсатында бірнеше тәжірибелік сынақтар қолдансақ олады.

3.1 Жылдамдық

Біз әрбір хаттаманың жылдамдығын тексеру мақсатында ElephantVPN көмегімен ЕС серверіне байланыс жасадық. Бізде 100 Мбит/с Ғаламтор бар, дегенмен тәжірибеде әдетте 40-50 Мбит VPN-сіз беріледі. Speedtest желісіне қосылудың параметрлерін анықтауға арналған бағдарламаны қолдана отырып, біз барлық хаттамалар бойынша бірнеше өлшеулер жүргіземіз, әр протоколға тән жылдамдықты көреміз және жылдамдықтың айырмашылығы туралы түсінік аламыз.

Бұл жағдайда барлық сынақтар Алматы қаласында өткізілді (3.1 – 3.4 сурет)

VPN қосылымсыз(3.1 сурет):

3.1 сурет – VPN қосылымсыз жылдамдық

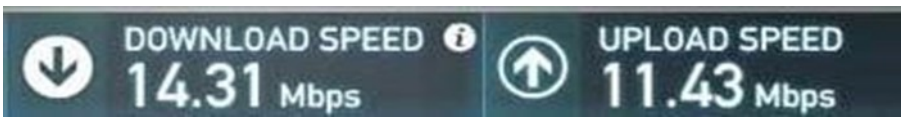
PPTP-мен VPN байланысы (3.2 сурет):

3.2 сурет – PPTP-мен VPN қосылымының жылдамдығы

L2TP (IPSEC) арқылы VPN қосылымы (3.3 сурет):

3.3 сурет – L2TP/IPSec көмегімен VPN қосылу жылдамдығы

OpenVPN-мен VPN байланысы (3.4 сурет):



3.4 сурет – OpenVPN-мен VPN қосылу жылдамдығы

Көріп отырғанымыздай, PPTP ең жоғары жылдамдықты көрсетті, L2TP – төмен, ал OpenVPN – ең төмен.

3.2 Қауыпсіздік

Бұрын берілген жылдамдық ол қауіпсіздік пен жылдамдық арасындағы ымыраға негізделген. Біздің байқағанымыздай, OpenVPN ең төмені болды және ең қауіпсіз болуы әбден мүмкін.VPN сервері деректерді тезірек шешеді, соның арқасында біз өткізу қабілетін жоғары жылдамдықпен аламыз.

«Анағұрлым қауіпсіз» және «қауіпсіз емес» деген сөздердің мағыналары нені білдіретінің қарастырайық? PPTP 128 биттік кілтпен ақпаратты шифрлайтын MPPE қысу хаттамасымен жұмыс істейді. Сондықтан деректер шифрланған түрде болады және бұл көптеген кездейсоқ шабуылдардан қорғайды. Алайда, PPTP-тің осал тұсы - пайдаланушы аты мен құпия сөздің шифрланбаған түрде серверге берілуі, сондықтан шабуылдаушы хабарламаларды «тыңдау» кезінде кілтті тауып, жіберілген деректердің шифрын шеше алады.

L2TP, әдетте, қандай да бір себептермен MPPE хаттамасына қатысты ең қауіпсіз болып табылатын IPSec қауіпсіздік хаттамасымен бірге қолданылады. Олардың бірі деректерді шифрлау үшін Pre-SharedKey бағдарламасын қолданады. Бұл кілт Ғаламтор арқылы берілмейді. Осылайша, шифрланған деректерді «тыңдайтын» шабуылдаушы, егер ол қандай да бір электрондық поштаға немесе компьютерге кіріп, Pre-SharedKey-ны ұрлап алмаса, біздің компьютерден шығатын мәліметтерді шифрлай алмайды.

OpenVPN SSL шифрлауға негізделген. Бұл хаттама сонымен қатар «HTTPS»-тен басталатын веб-сайттарға кірген кезде деректердің қауіпсіздігін қамтамасыз ету үшін қолданылады. Іс жүзінде, OpenVPN деректерді HTTPS сайттары сияқты бірдей порт арқылы жібереді. Сондықтан, провайдер үшін OpenVPN-ді блоктау қиын, өйткені егер HTTPS портын блоктаса, олар Интернеттегі көптеген маңызды және пайдалы сайттарды қоса блоктайды. OpenVPN серверіне қосылу үшін бізге бірқатар сертификаттар қажет. Сертификат - бұл біздің кілтіміздің жартысы. Кілттің екінші жартысы серверде, және шифрды ашу үшін бізде толық кілт болуы қажет. Осылайша, деректерді тек сервер ғана шеше алады. Сондықтан, OpenVPN біз қарастыратын негізгі хаттамалардың ең қауіпсізі болып табылады. Егер шабуылдаушы біздің мәліметтерімізді ұстап алып, сіздің компьютеріңізге кіріп, куәлігіңізді ұрлап алса да, ол сіздің компьютеріңізден шифрды шеше алмайды, өйткені

шабуылшыда кілттің екінші бөлігі жоқ.

3.3 Орнату

Орнату жылдамдығы мен қарапайымдылығын талдау үшін әрбір нақты хаттама үшін VPN провайдерінен не талап етілетінін анықтау қажет (кесте 2).

Кесте 2

PPTP	L2TP (IPSEC)	OpenVPN,
- Пайдаланушының аты; - Құпия сөз; - Сервер мекенжайы.	- Пайдаланушының аты; - Құпия сөз; - Сервер мекенжайы; - Ортақ кілт	- Сертификат файлдары (crt, key, ca); - OpenVPN конфигурационды қ файлдар (сервер мекенжайын анықтайтын файл)

L2TP (IPSEC) және PPTP үшін параметрлер өте ұқсас. Оған VPN қосылымының әдеттегі құрылуы кіреді. Алайда, L2TP орнату кезінде алдын-ала ортақ кілтті немесе алдын-ала жасалған сертификаттарды енгізу үшін қосымша қадам қосылады.

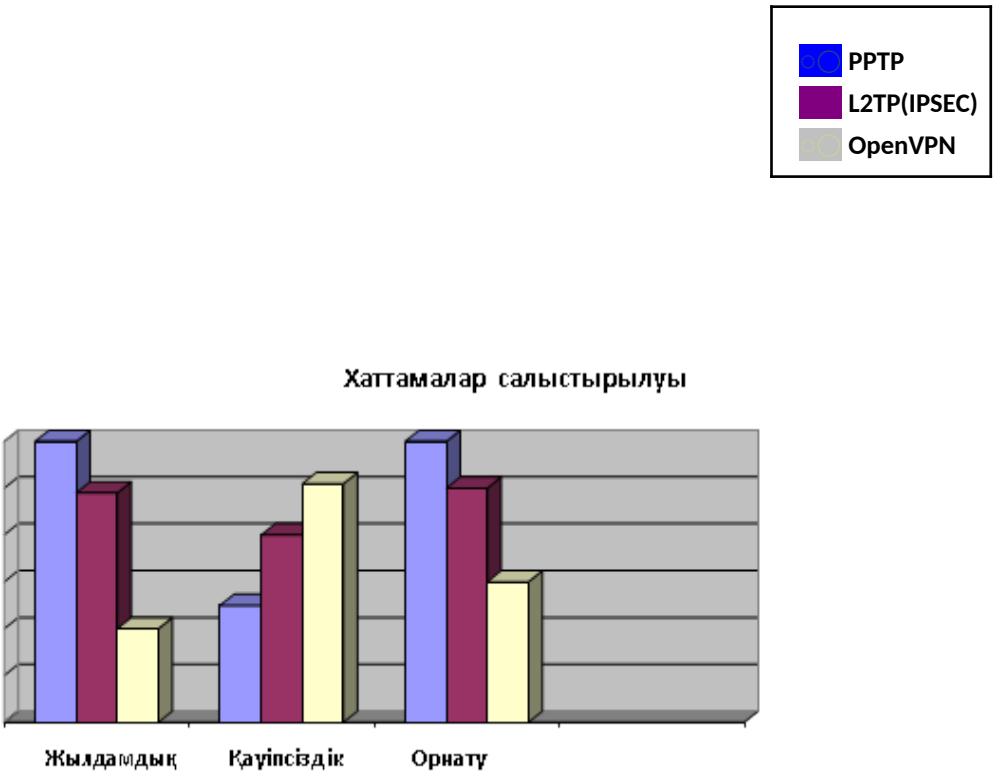
OpenVPN орнату әр түрлі, бірақ әлдеқайда қиын емес.Біріншіден, көптеген операциялық жүйелер PPTP және L2TP қосылыстарына қолдау көрсетсе, OpenVPN – бұл компьютерге жүктеліп, орнатылуы керек қосымша бағдарлама.Біздің VPN жеткізуші төрт файлды ұсынған. Біз файлдарды көшіріп, оларды компьютердегі сәйкес OpenVPN конфигурация каталогына қоюымыз керек.

OpenVPN іске қосылғаннан жағдайда, біз жаңа қосылымды құру опциясын көреміз. Ең дұрысы, орнату қиын болмауы керек, бірақ негізгі механизм күрделірек және операциялық жүйенің бөлігі болмағандықтан, көп нәрсе істен шығуы мүмкін және әдетте OpenVPN орнату біраз уақытты алады. Windows-де әкімші ретінде OpenVPN іске қосып, файлдардың дұрыс каталогқа көшірілгеніне көз жеткізу керек. Сіз қосылуға тырысқанда, OpenVPN орындалады және оның әрекеттер журналын көрсетеді. Егер сізде байланысқа қатысты күрделі мәселер болса, қателерді жою үшін алдымен осы журналға қарау керек.

3.4 Салыстырудың қортындысы

Қорытындылай келе, біз OpenVPN қажеттіліктеріне арналған хаттаманы

таңдадық. Егер біз жоғары жылдамдықты қажет ететін болсақ немесе берілетін деректерді қорғау қажеттілігі болмаса, онда PPTP хаттамасын таңдаймыз.L2TP (IPSEC) жылдамдықты жақсы атқарады, бірақ OpenVPN қауіпсіздігі айтарлықтай жоғары. Сондықтан, қауіпсіз қосылымды ұйымдастыру үшін бізге OpenVPN шешімі қолайлы.



3.5 сурет – Хаттамалар салыстырылуы

Диаграммадан (3.5-сурет) PPTP қауіпсіз емес екенін көрсек болады, сондықтан оны пайдаланудан аулақ болған абзал. Орнатудың қарапайымдылығы мен үйлесімділігі тартымды болғанымен, L2TP/IPsec бірдей артықшылықтарға ие және қауіпсіз болып табылады.

L2TP/IPsec жақсы VPN шешімі болды, бірақ OpenVPN сияқты жақсы емес. OpenVPN – барлық операциялық жүйелерде үшінші тарап бағдарламалық жасақтамасының қажеттілігіне қарамастан, ең жақсы VPN шешімі. Бұл сенімді, жылдам және қауіпсіз хаттама, бірақ ол басқа хаттамаларға қарағанда біршама күш жұмсауды қажет етеді.

SSTP OpenVPN артықшылықтарының көпшілігін ұсынады, бірақ тек Windows жүйесінде. Бұл ОЖ-ге жақсы интеграцияланған дегенді білдіреді, бірақ VPN провайдерлері оны әлсіз қолдайды.

Көптеген пайдаланушылар жұмыс үстеліндегі компьютерлерде OpenVPN қолдана алады, сондай-ақ оны мобильді құрылғылардағы L2TP/IPsec-пен толықтыра алулары әбден мүмкін.

4 VPN-ді іске қос

Іс жүзінде виртуалды жеке желіні енгізу әдетте ол келесі түрде көрінеді. VPN сервері компания кеңсесінің жергілікті желісіне орнатылды. Клиенттің VPN бағдарламалық жасақтамасын пайдаланып, қашықтағы қызметкер серверге қосылым орнатады. VPN қосылымын орнатудың бірінші кезеңі – ол қызметкерлерді аутентификациялау. Егер тіркелінген деректер расталса, келесі кезең басталады - сервер мен клиент арасындағы байланысты қамтамасыз етудің егжей-тегжейлері келісіледі. Содан кейін сервер мен клиент арасында ақпарат алмасуға мүмкіндік беретін VPN қосылымы жасалады, яғни кез-келген деректер пакеті шифрлау/дешифрлау және тұтастықты тексеру арқылы өтеді – деректердің аутентификациясы.

VPN сервері үшін Windows 10 Pro жүйесіндегі машиналардың бірі бөлінді.

VPN протоколдарын талдау негізінде біз қарастырылған ұйым үшін OpenVPN протоколы қауіпсіз байланысымызды қанағаттандыратын оңтайлы шешім болып табылады деп тұжырымдаймыз. Біз оның орындалуын толығырақ қарастырамыз.

4.1 GNS3 симуляторына желіні құру

Graphical Network Simulator 3 – бұл желі мамандарының мүмкіндіктерін кеңейтетін бағдарламалық жасақтама болғандықтан, желіні осы бағдарламалық жасақтамада жасауды ұйғардық.

Бұл бағдарламаның бірнеше артықшылықтары мен ерекшеліктері бар. Ресми веб-сайттан ақысыз қол жетімді. GNS3 күрделі желілерді модельдеу үшін қолданылады. Бұл Cisco емтихандарына дайындалуға, CCNA, CCNP, CCIP, CCIE, JNCIA, JNCIS, JNCIE сияқты сертификаттар алуға өте ыңғайлы. Сонымен қатар, бұл бағдарламалық жасақтаманы нақты физикалық құрылғыларға конфигурациялау және кейіннен орнату үшін пайдалануға болады.

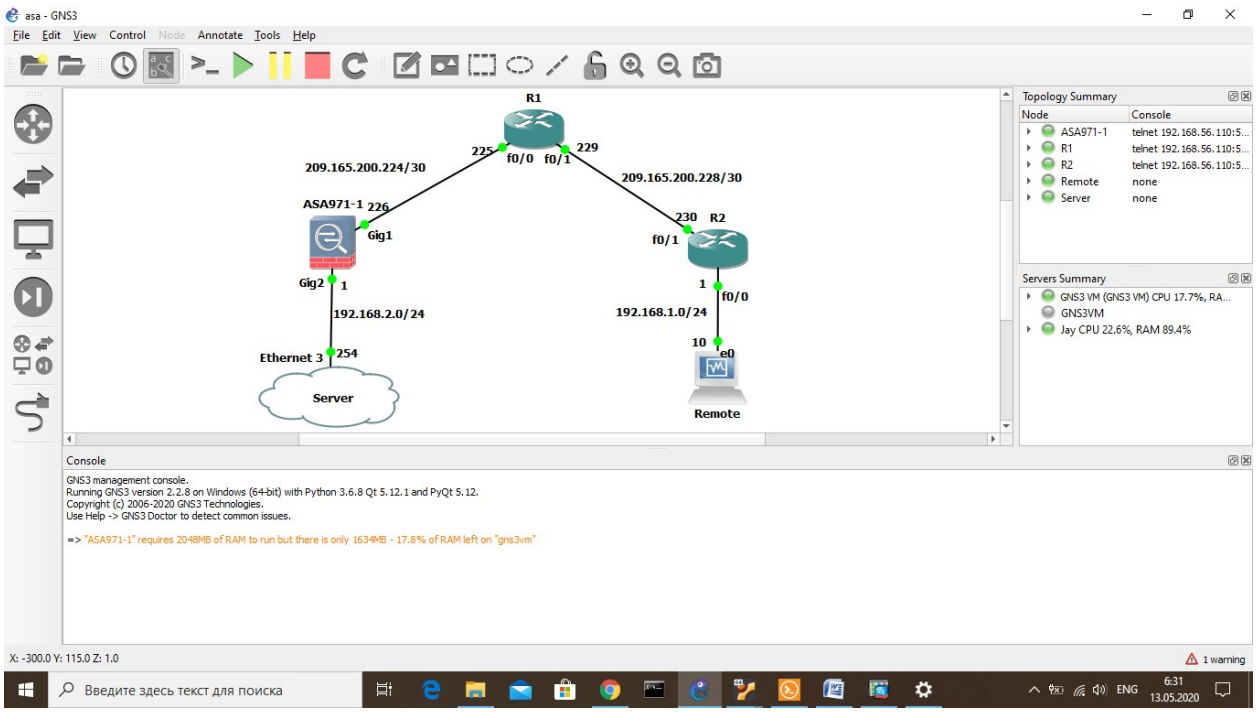
Бұл өнімнің жалпы артықшылықтары мен ерекшеліктері мыналарды қамтиды:

- Жоғары сапалы күрделі топологияларды құру мүмкіндігі
- Көптеген Cisco IOS роутерларын (IPS, PIX және ASA брандмауэрлері, JUNOS) эмуляциясы
- Ethernet, ATM және Frame Relay коммутаторларын модельдеу
- Модельделген желіні нақты желіге қосу

4.2 AnyConnect VPN-ді желіаралық экранға іске қосу

Сертификаттың көмегімен қашықтағы пайдаланушыларды ішкі желіге қосу үшін AnyConnect қосымшасын пайдаланып OpenVPN серверін енгізу.

Қашықтан қол жеткізу желісінің топологиясы Серверден (сервер рөлінде бұл Windows 10 pro бар жеке компьютер), қашықтағы пайдаланушы (Windows 10 Home виртуалды машина), Cisco ASA брандмауэрі және роутердан тұрады (4.1 суретті қараңыз).

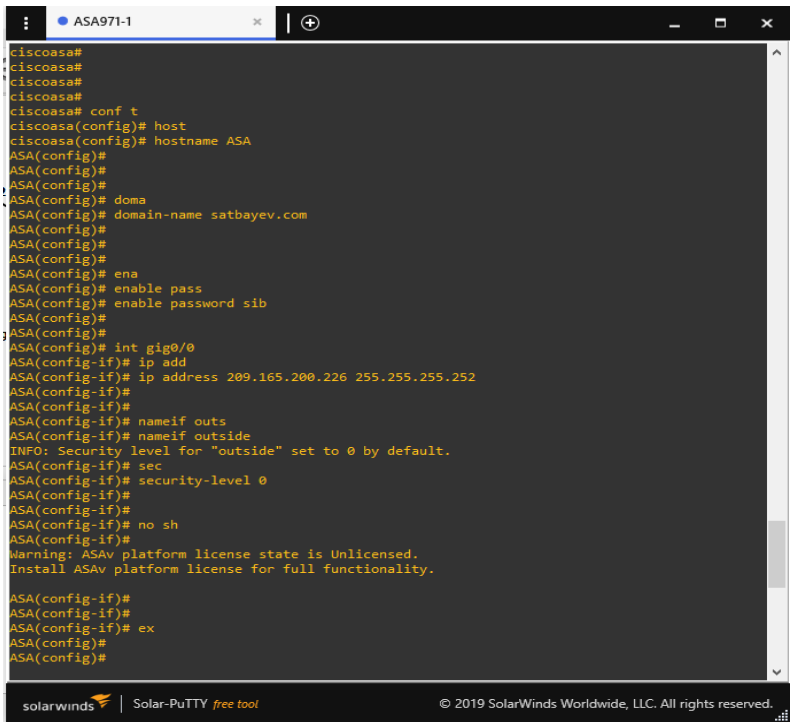


4.1 сурет – Қашықтан қол жеткізу желісінің топологиясы

Ең алдымен берілген тополияның бастапқы баптауларын орындап шықтық, яғни топологияға байланысты интерфейстерге IP адрес баптауларын орындау, NAT баптауларын R2 роутерине енгізіп, әдепкі маршрутқа Internet-тің мекен-жайын енгіздік. NAT үшін сыртқы интерфейс – fa0/1, ал ішкі интерфейс – fa0/0 болып табылады.

Брандмауэрдың архитектуралық ерекшелігі және ASA жұмысының принципі IP-адресімен қатар, ASA-дағы әр интерфейстің атауы мен қауіпсіздік деңгейі берілген. Ішкі желі үшін және сыртқы желі үшін екі бекітілген атаулар бар, бұл атауды орнатқаннан кейін қауіпсіздік деңгейі автоматты түрде осы интерфейске тағайындалады, оның ішкі (inside) интерфейсі үшін 100, ал сырты (outside) интерфейсі үшін 0 (нөл) болып табылады. Қауіпсіздік деңгейі 100 дегеніміз - бұл сенімді желі, ал 0 (нөл) – сенімді емес желі.

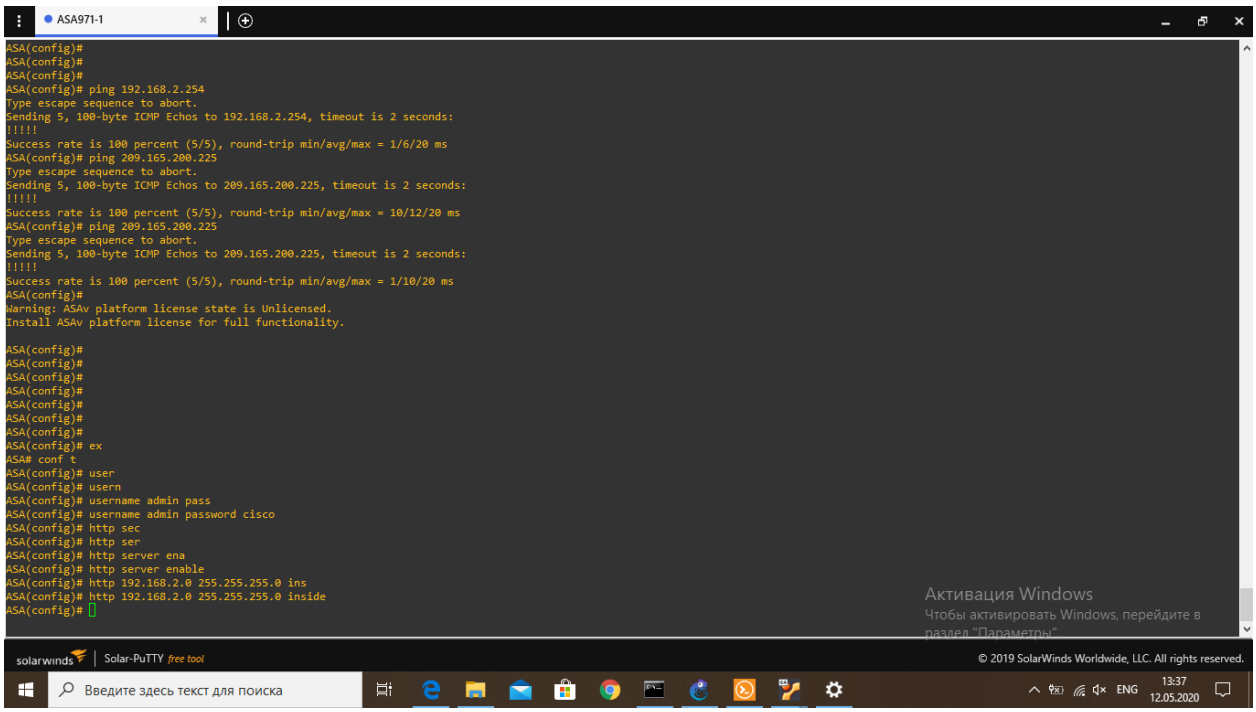
Бастапқыда осы схемаға сәйкес интерфейстерге IP-мекен-жайларды конфигурациялауымыз керек, интерфейс атауын, қауіпсіздік деңгейін және олар үшін IP-мекен-жайларды тіркеуіміз керек, және қашықтан кіру үшін бізге домен атауы қажет (4.2 суретті қараңыз).



4.2 сурет – ASA-ның бастапқы баптаулары

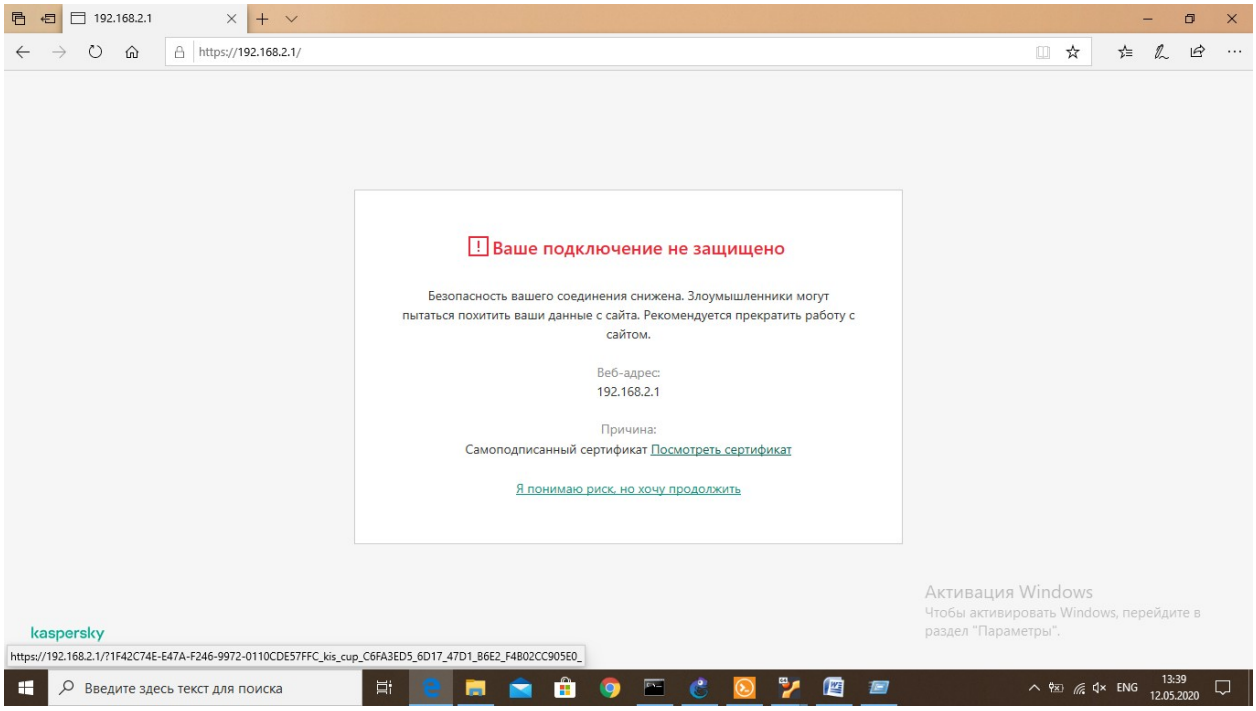
ASA-ға R1 маршрутизаторының IP-мекен-жайы бойынша әдепке сәйкес маршрутты орнаттық, содан кейін 192.168.2.0 диапазоны бар ішкі желісі ASA-ның сыртқы интерфейсінің IP-адресімен интернет желісіне ақ IP адресімен жүре алатындай етіп мекен-жай аудармасын теңшейміз. Әдетте, Asa icmp протоколын кез келген бағытта бұғаттайды, сондықтан серверден Интернетке «ping» командасын орындауға тырыссаңыз, ол жұмыс істемейді. Icmp инспекция протоколын қоссақ, серверден интернетке деректер оңай өтеді, бірақ егер біреу интернеттен сервер ресурстарын іздеуге тырысса, ол бұғатталады.

Қашықтықтан пайдаланушы Cisco-ға «https» арқылы қашықтықтан қол жетімді болу үшін артықшылықты (привилегированный) пайдаланушыны құрды. «Https» арқылы, яғни графикалық интерфейс арқылы қатынауды конфигурациялау үшін келесі әрекеттерді орындау керек (4.3-суретті қараңыз).



4.3 сурет – ASA-ға қол жеткізуге арналған параметрлері

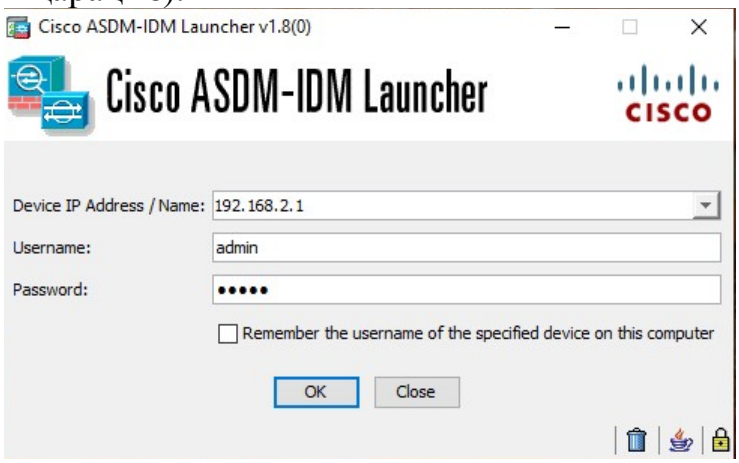
Сервер арқылы Asa-ға қосылу үшін браузерде « https » арқылы ASA-ның мекен-жайын көрсетеміз (https://192.168.2.1), куәлік көпшілікке жүктелмегендіктен ерекшелік жасаймыз және ASDM жүктемесін жасадық (4.4-суретті қараңыз).



4.4 сурет – Серверден Асаға қатынас

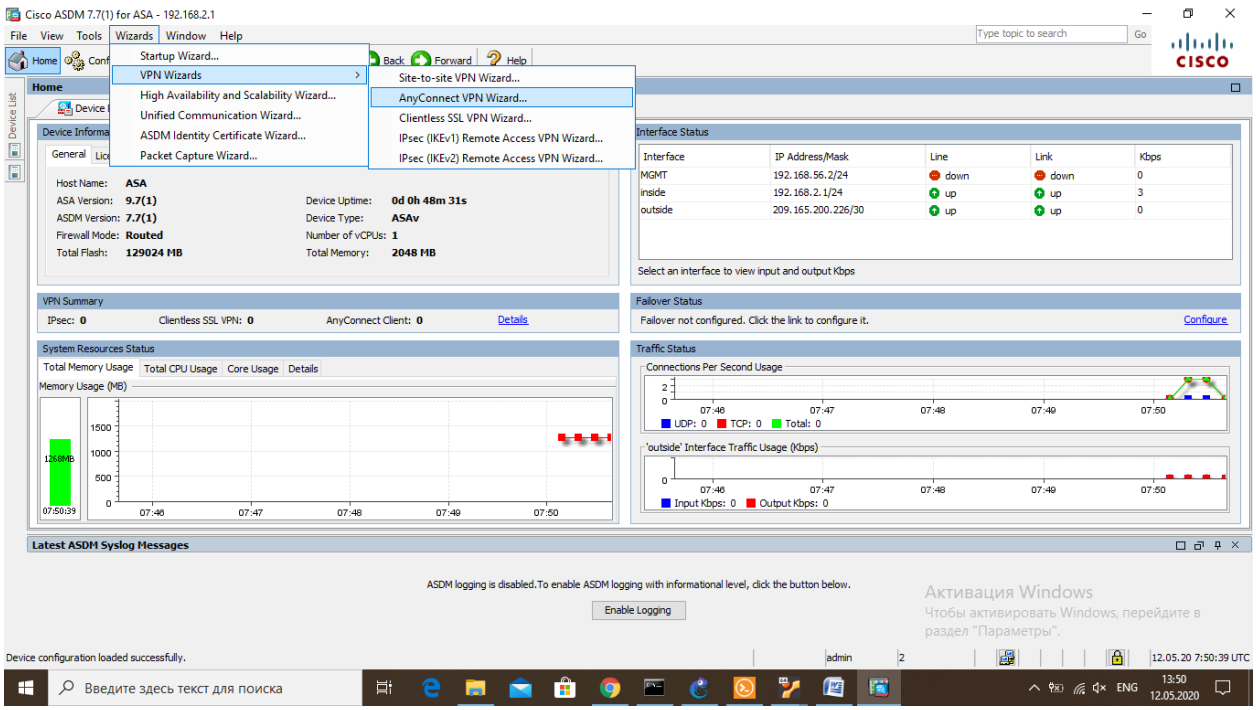
ASDM-ның жүктемесі аяқталған соң автоматты түрде іске қосылды, енді ASA-ны конфигурациялау үшін мекен-жайын, атын мен құпия сөзді

көрсеттік (4.5-суретті қараңыз).



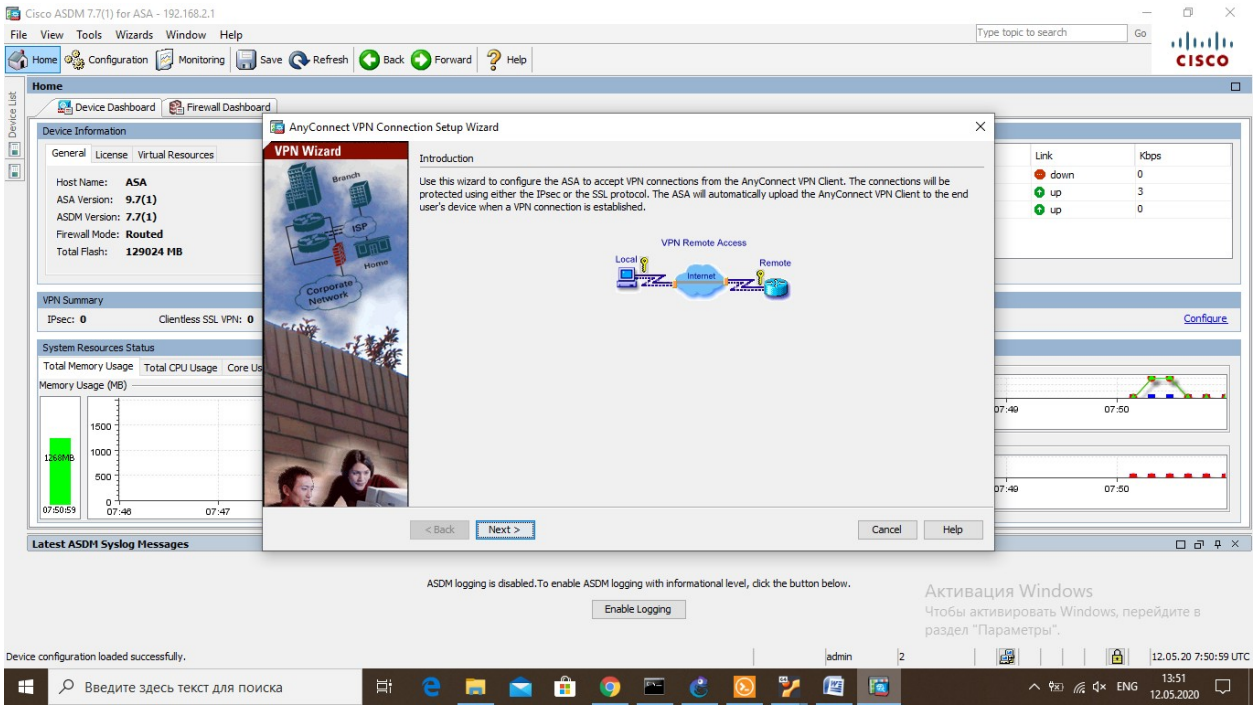
4.5 сурет – ASA-ға кіру аутентификациясы

Пайда болған терезе арқылы біздің AneConnect VPN-ді конфигурациясын жүзеге асырдық, ол үшін жаңа терезеде «Wizards» қойындысына өтіп, «AnyConnect VPN» таңдадық (4.6 суретті қараңыз).



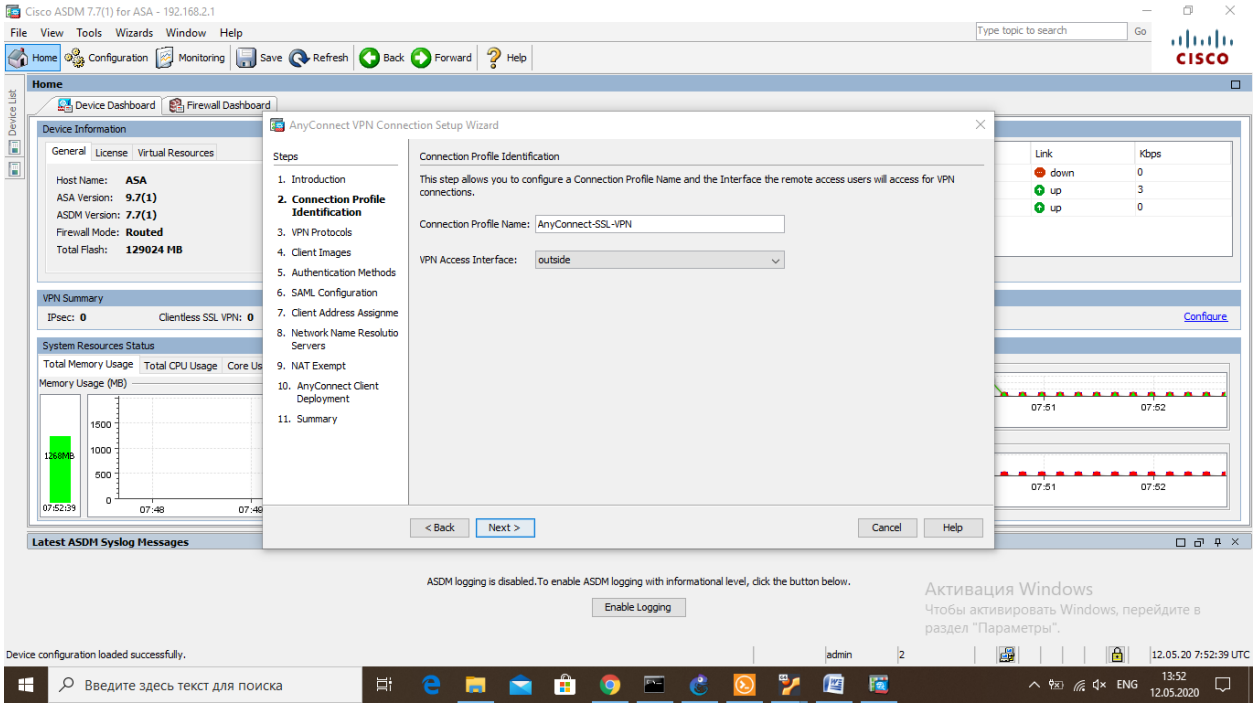
4.6 сурет – AnyConnect VPN орнату

ASA конфигурациясы туралы келісім (4.7 суретті қараңыз).



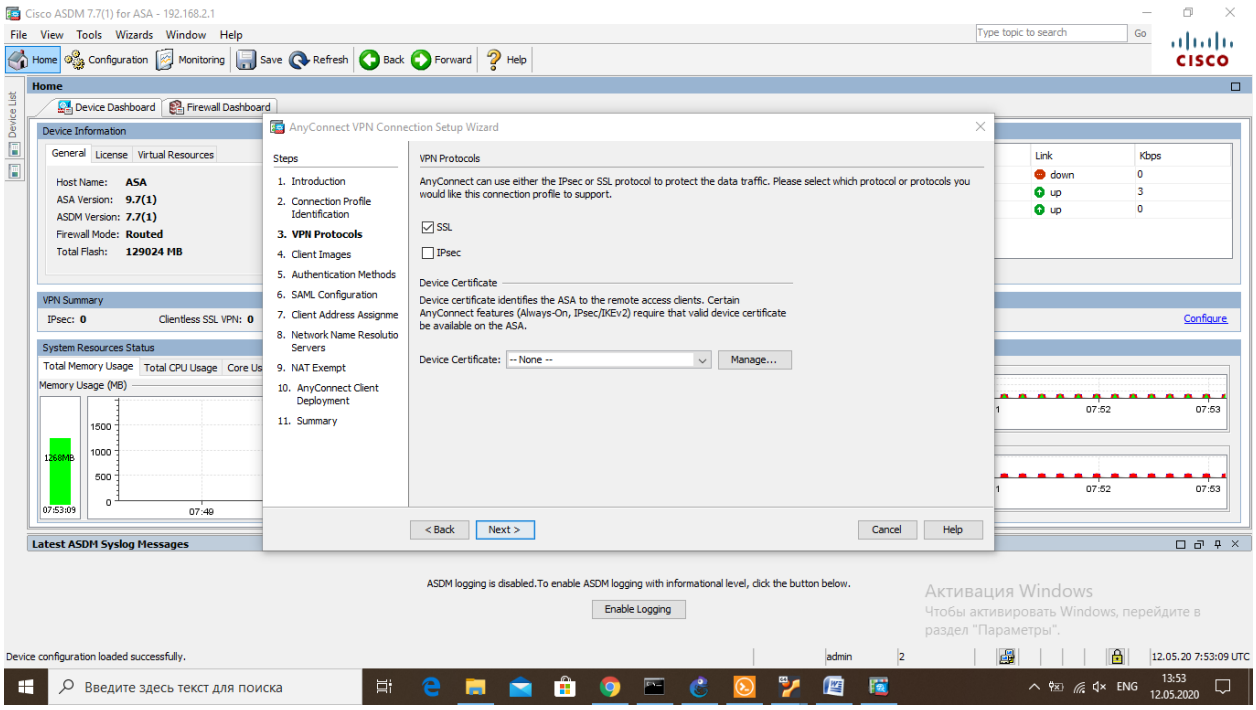
4.7 сурет – AnyConnect VPN көмегімен ASA-ны баптау

Келесі терезеде конфигурацияның 10 қадамын көрдік те, екінші қадамда қосылуға арналған профильді енгіздік (4.8-суретті қараңыз).



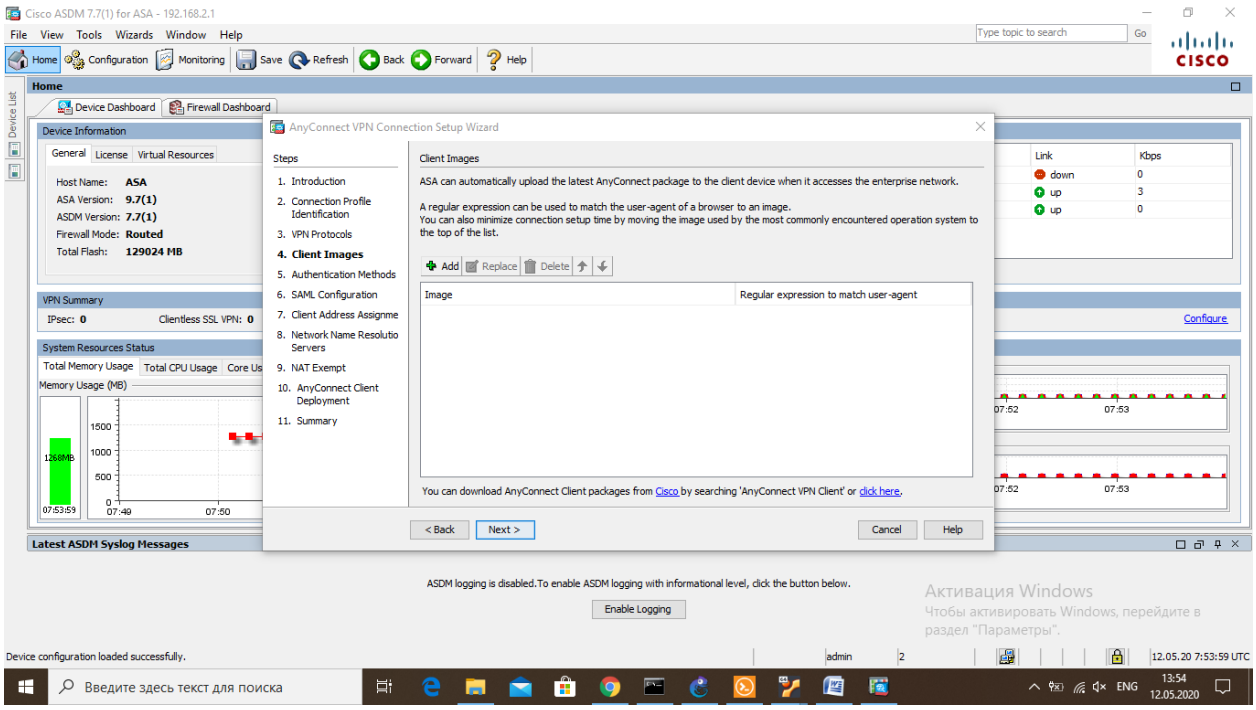
4.8 сурет – Екінші қадам, қосылатын профильді енгізу

Үшінші қадамда қандай протоколдар қолданатынымызды анықтадық, біздің жағдайда ол SSL протоколы, ол сертификатты қажет етеді, сондықтан өз қол қойылған сертификаттың өзін көрсеттік (4.9 суретті қараңыз).



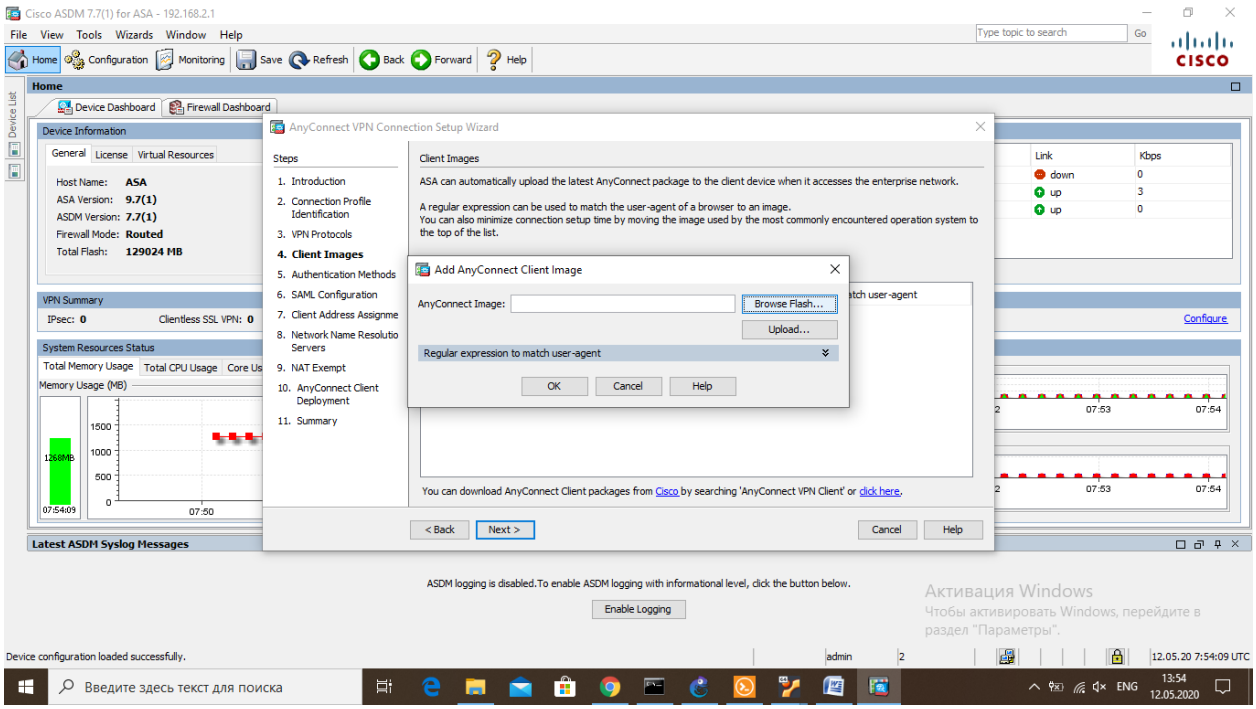
4.9 сурет – Протоколды таңдау

Келесі қадамда .pkg форматта VPN Client кескінін қостық (4.10 суретті қараңыз).

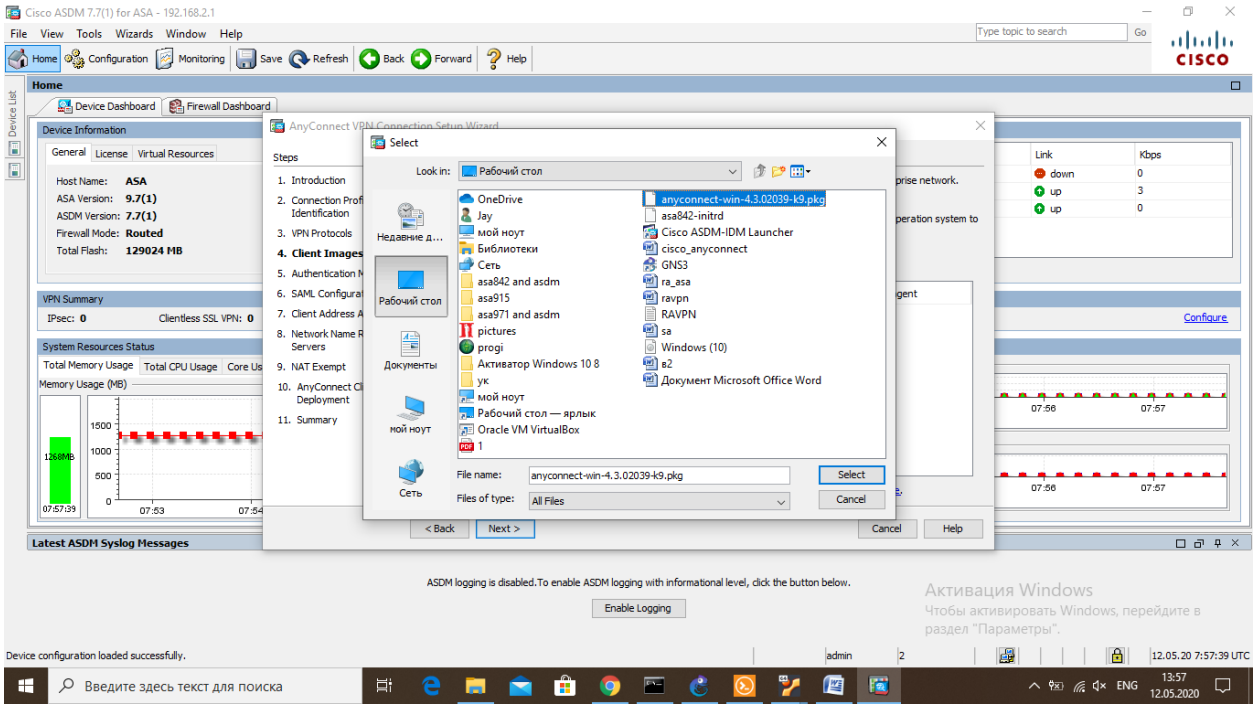


4.10-сурет – VPN клиенттік кескінін қосу

Пайда болған терезеде VPN Client кескінін көрсеттік (4.11-4.12 суретін қараңыз).

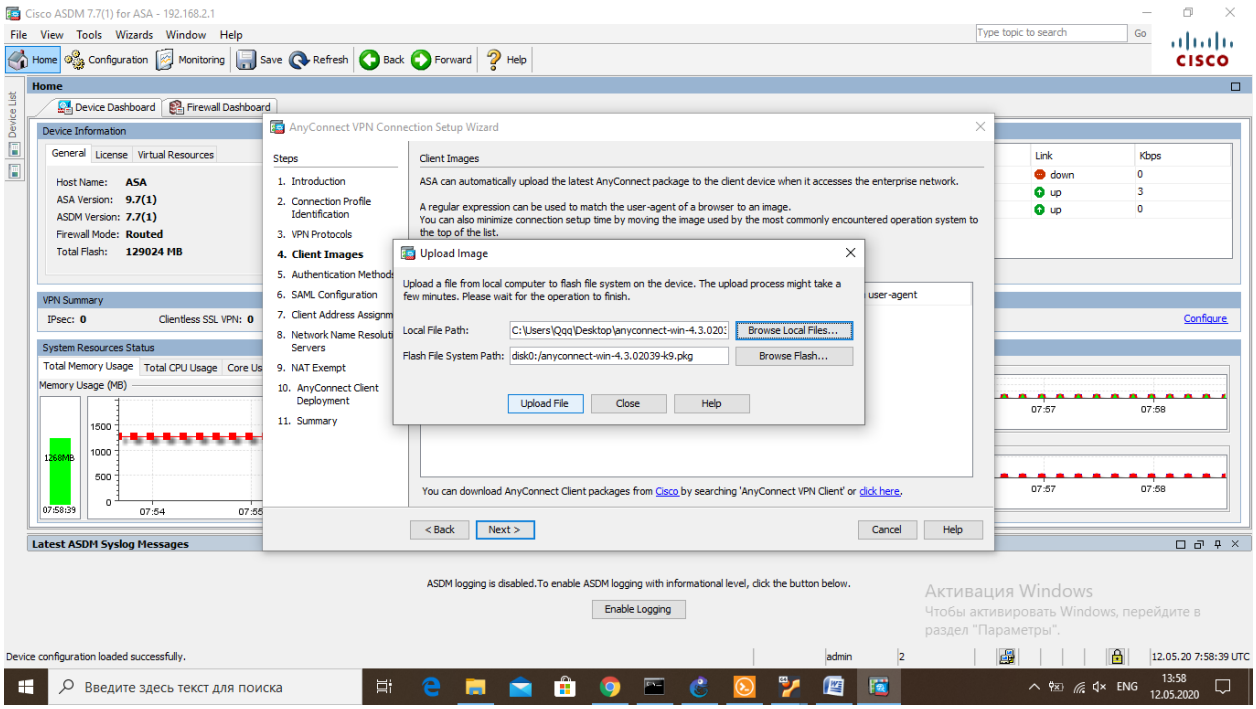


4 .11 сурет – Файлды ашу



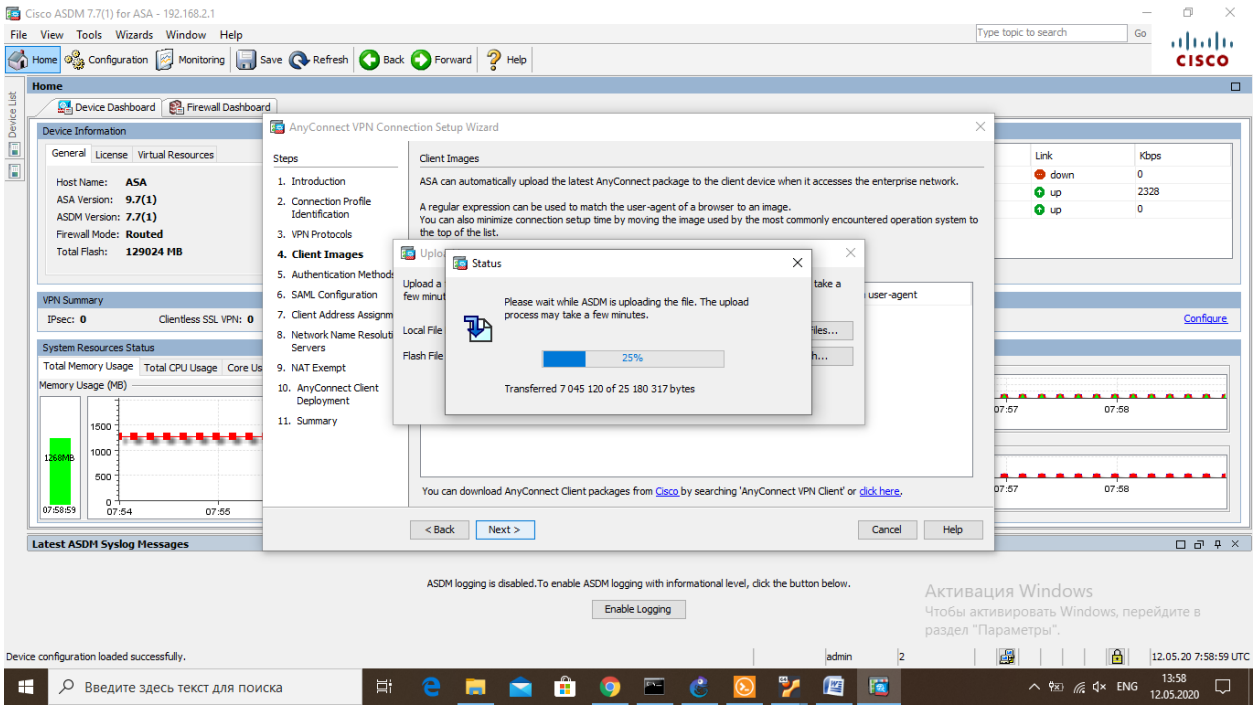
4 .12 сурет – VPN Client кескінін таңдау

Көрсетілген кескінді «Upload» батырмасы арқылы жүктеу керек (4.13-суретті қараңыз).

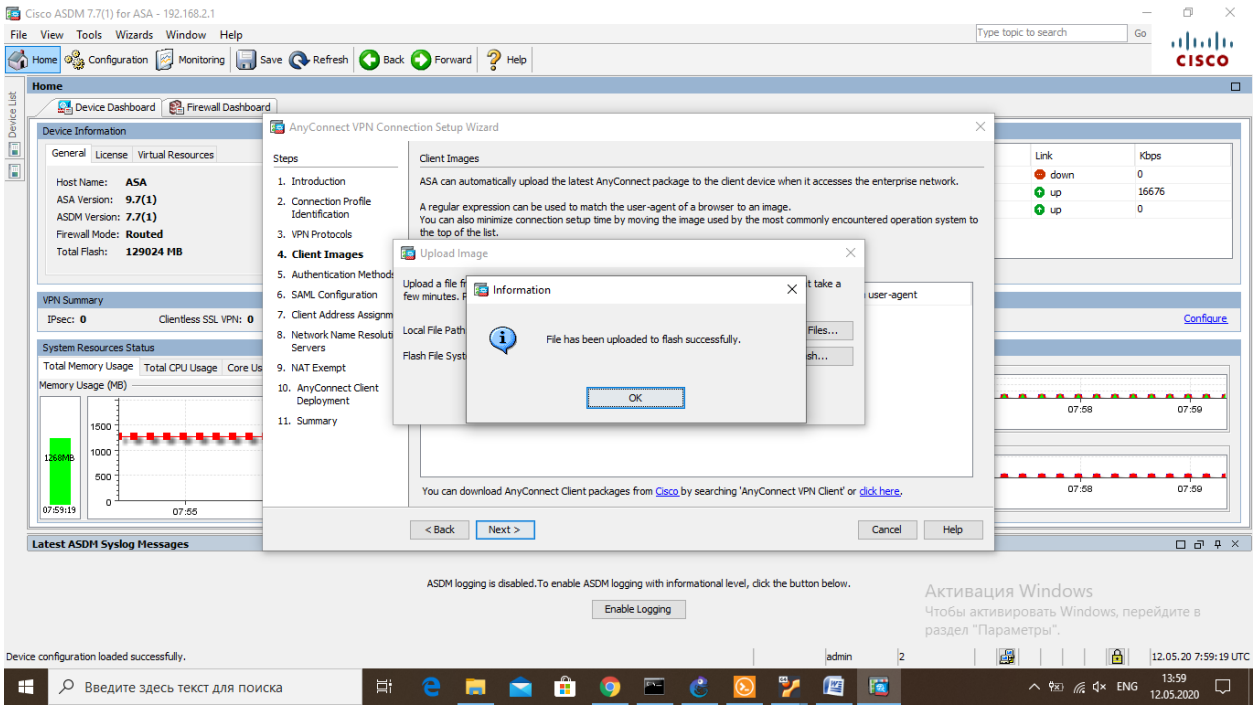


4.13 сурет – VPN клиентінің кескінін жүктеңіз

Осыдан кейін кішігірім жүктеме жізеге асып, сәтті қосылудың нәтижесін байкадық (4.14-4.15 суретті қараңыз).

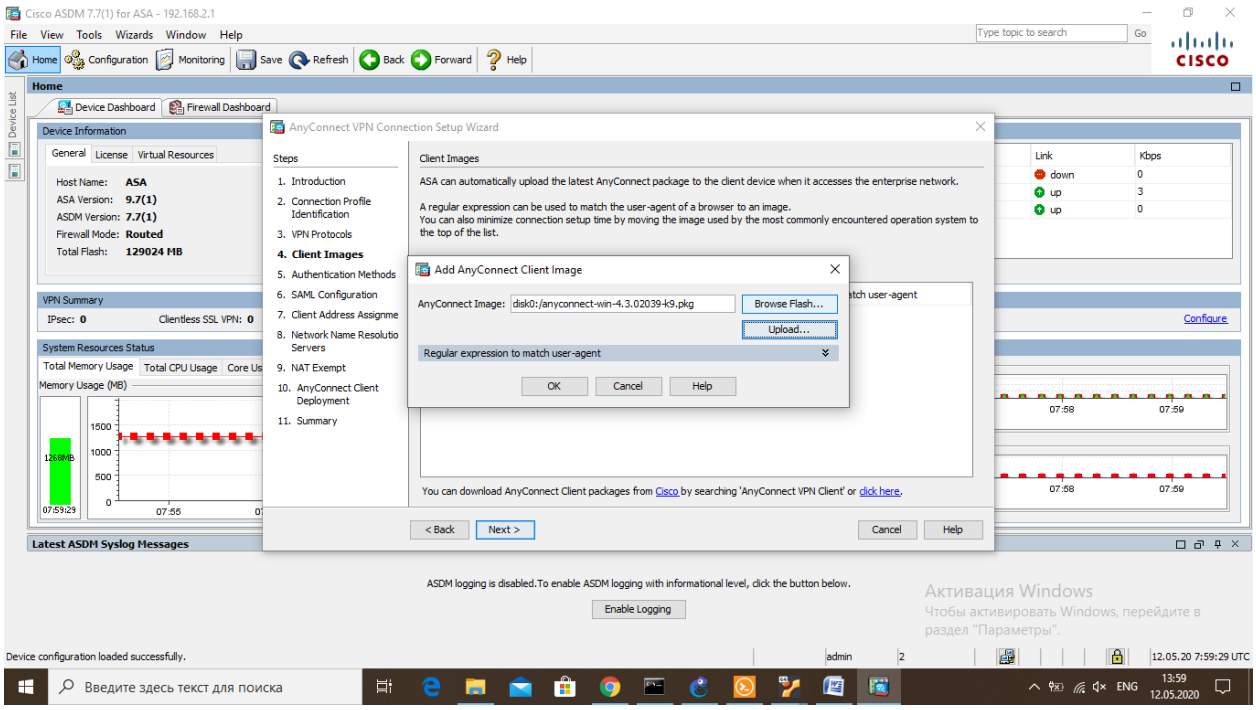


4.14 сурет – VPN клиентінің кескінін жүктеу

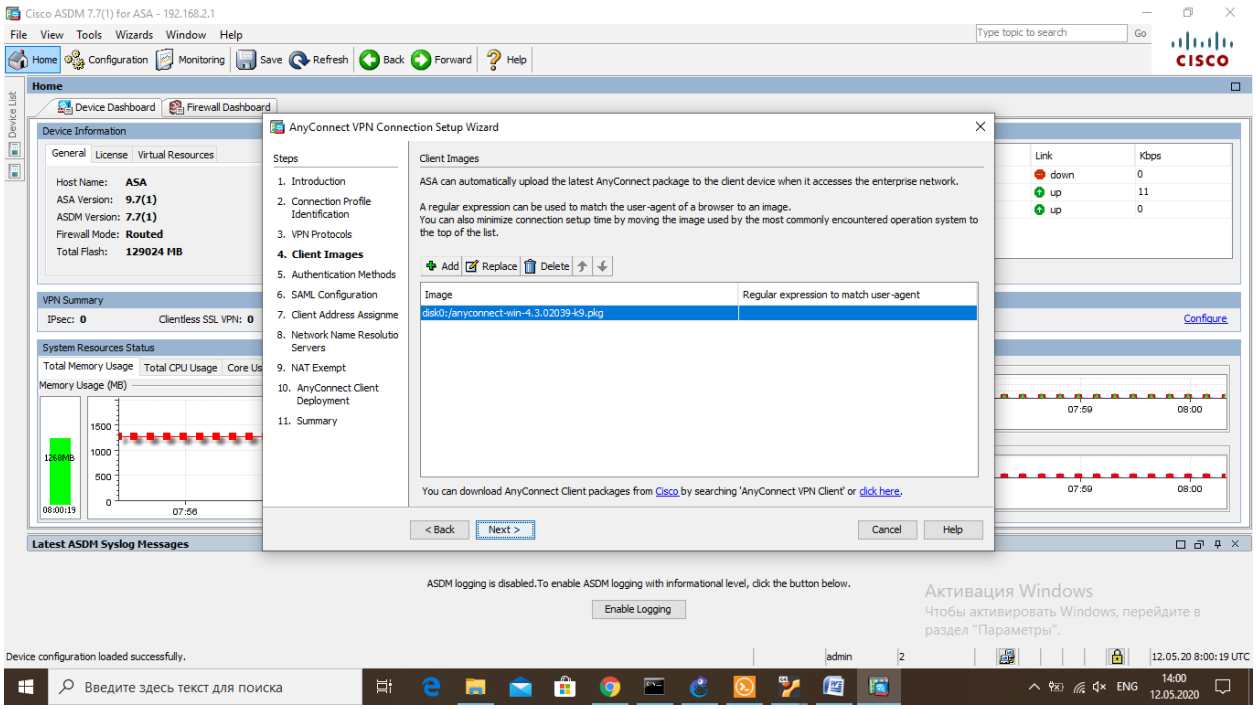


4.15 сурет – Кескіннің сәтті қосылуы

Жүктелген кескін автоматты түрде жүктеліп, кескіннің қосылғандығын көрдік (4.16-4.17 суретті қараңыз).

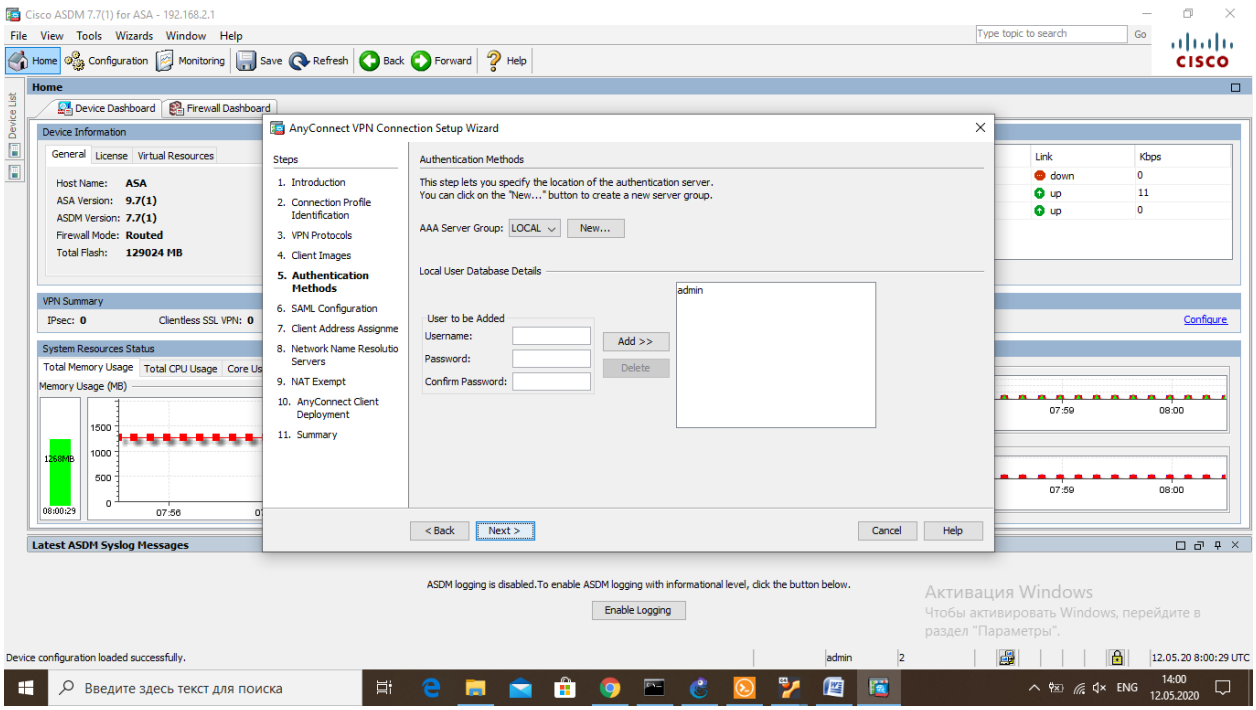


4.16 сурет – Жүктелген кескін

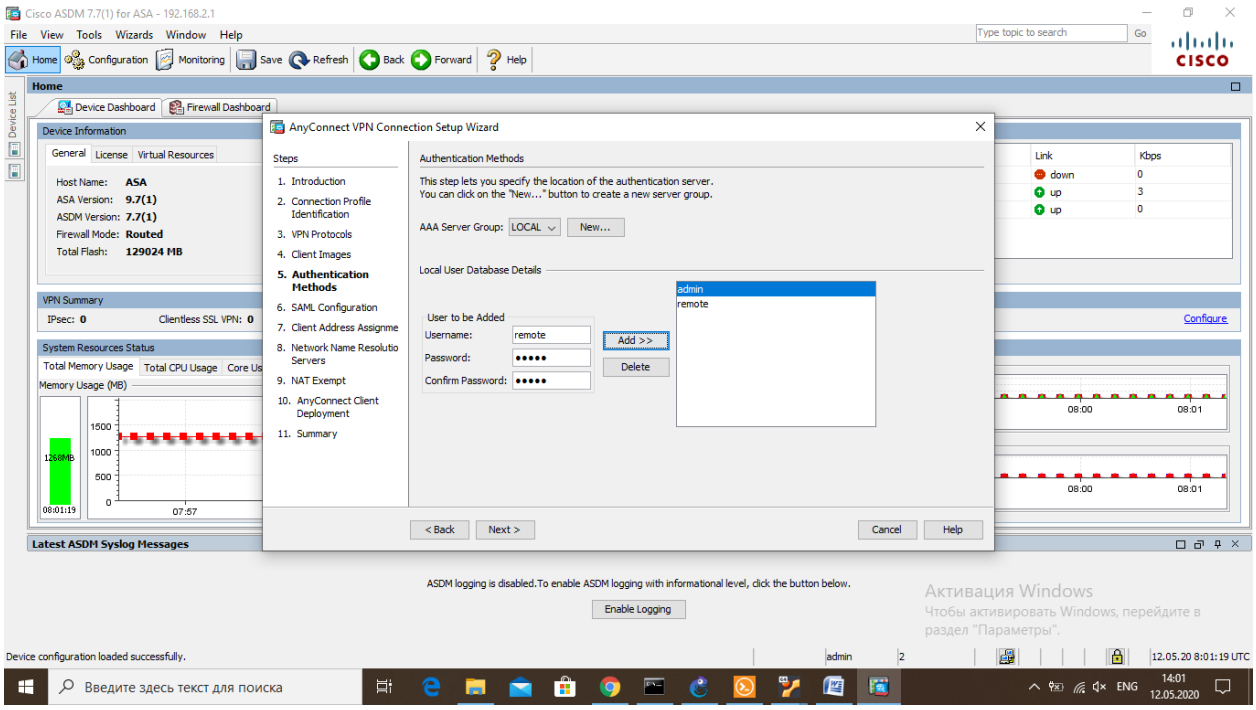


4.17 сурет – Қосылған кескін

Бесінші қадамда аутентификация әдістерін таңдау. Біріншіден, жергілікті аутентификация мұнда ASA-дағы жергілікті пайдаланушы базасына негізделіп пайдаланылады және осы кезеңде жаңа пайдаланушыны жасадық (4.18-4.19-суретті қараңыз).

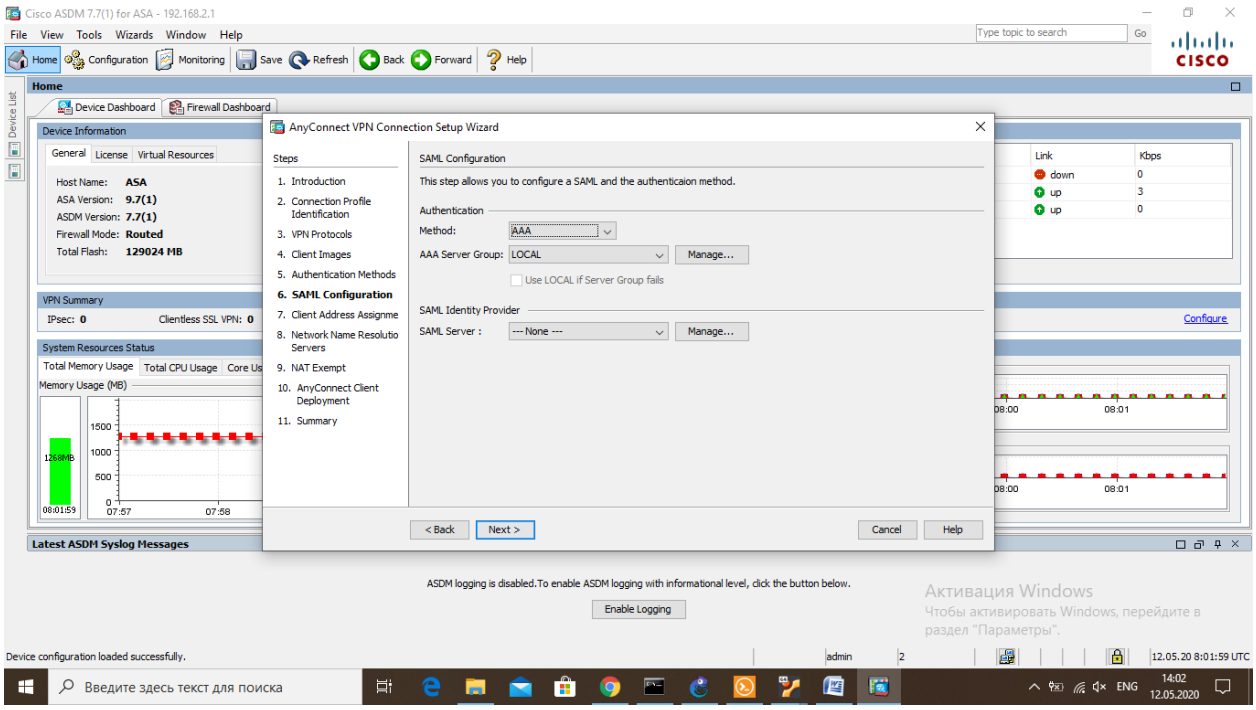


4.18 сурет – Аутентификация әдісі



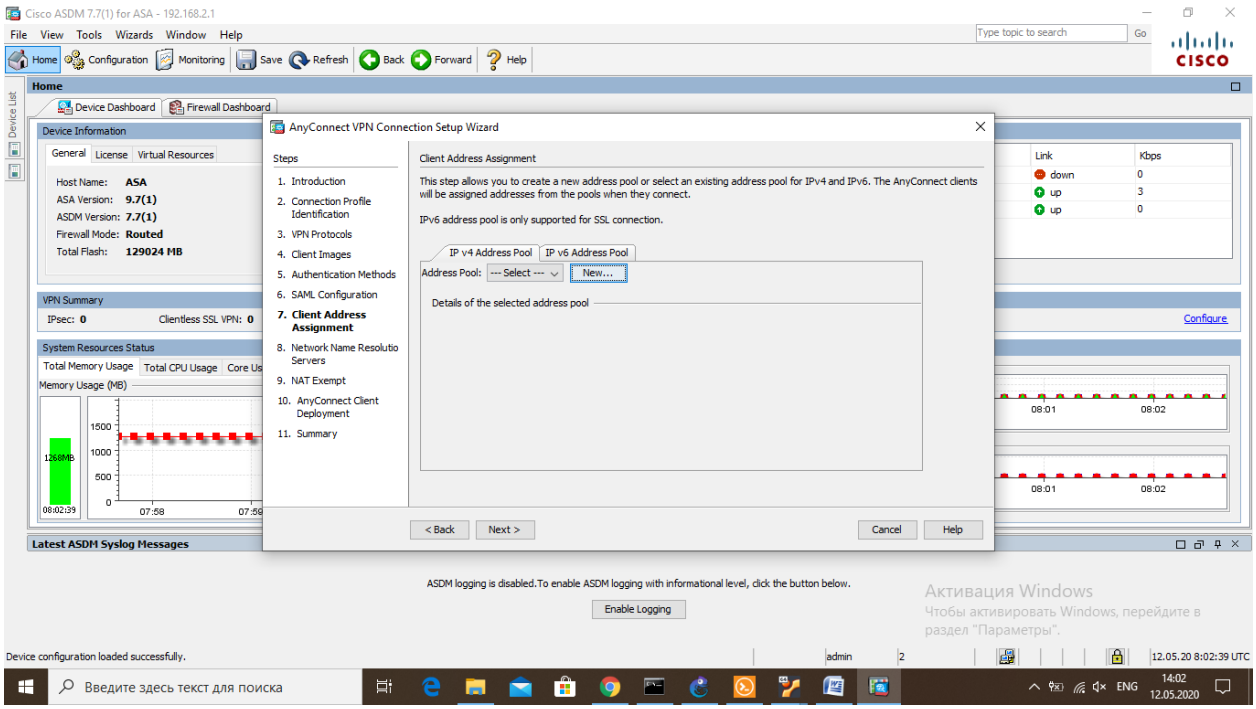
4.19 сурет – Жаңа пайдаланушыны қосу

SAML конфигурациясы әдепкі жағдайда қалдырамыз (4.20 суретті қараңыз).

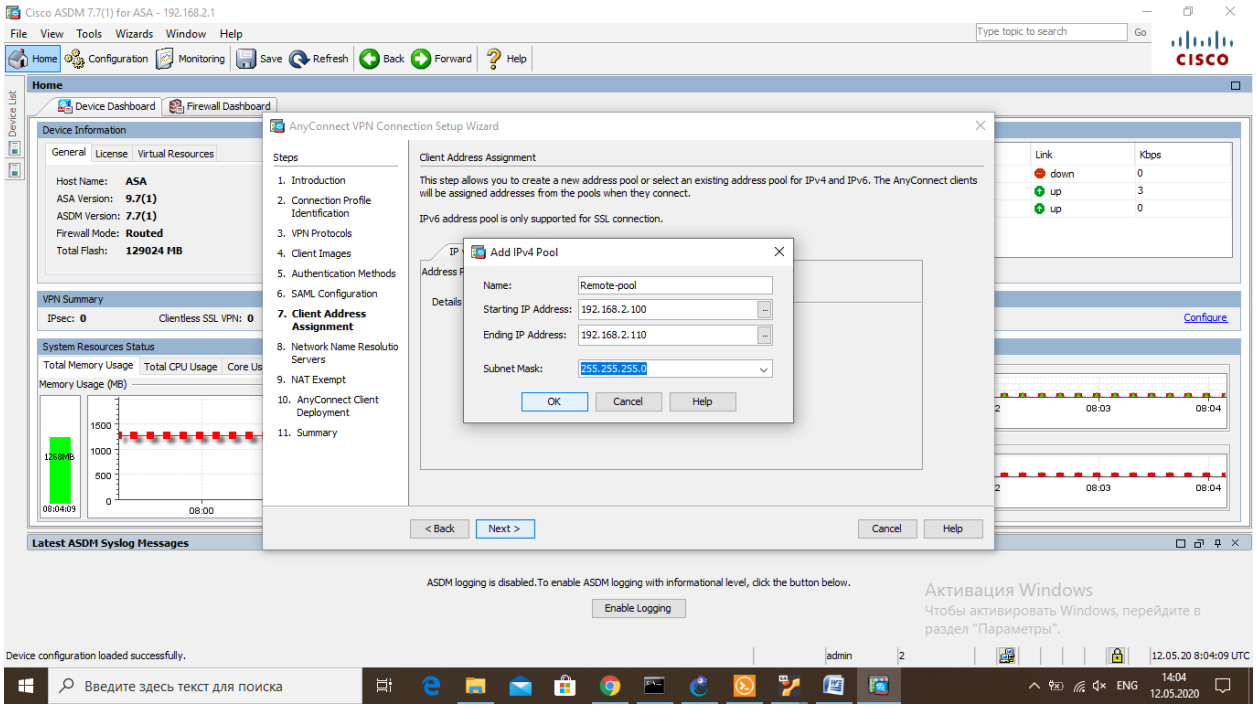


4.20 сурет – SAML конфигурациясы

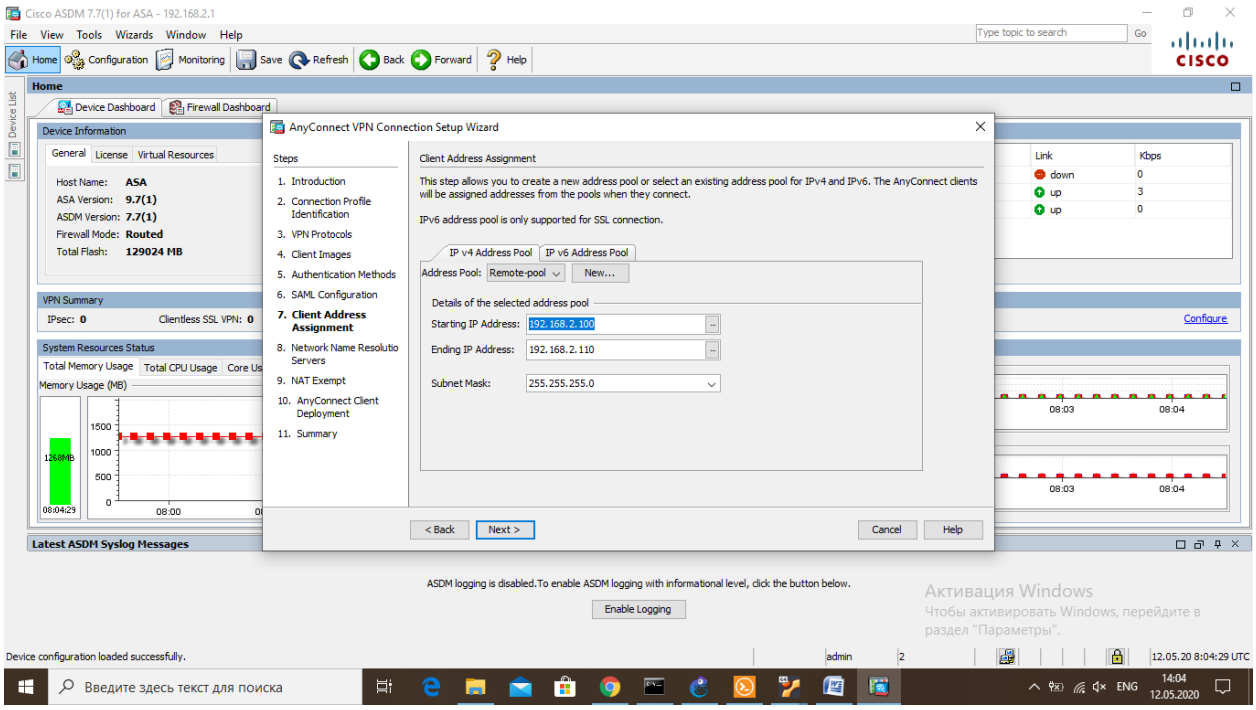
Бұл қадамда Pool – IP мекен-жайларды енгіздік, олар тұтынушыларға беріледі (4.21-4.23 суретті қараңыз).



4.21 сурет – Pool-IP мекенжайларын қосу

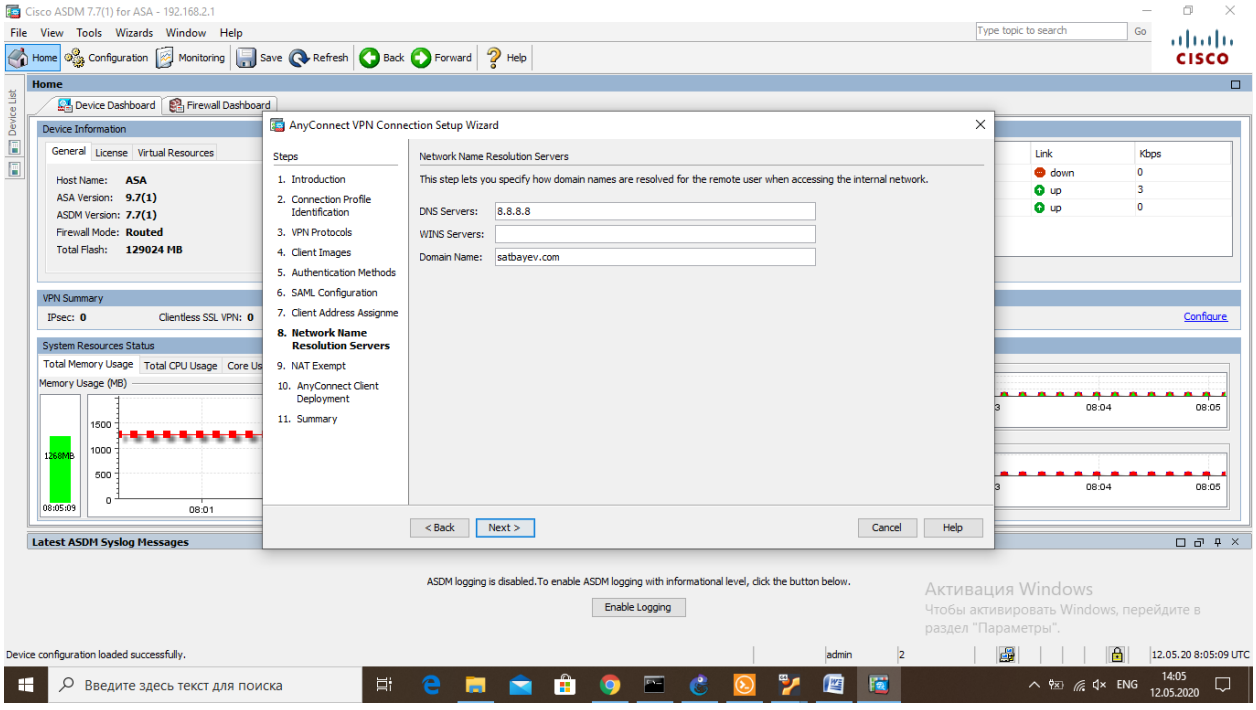


4 .22 сурет – IP мекенжайларының атауы мен аралығын енгіздік



4.23 сурет – Берілген IP мекенжайлары

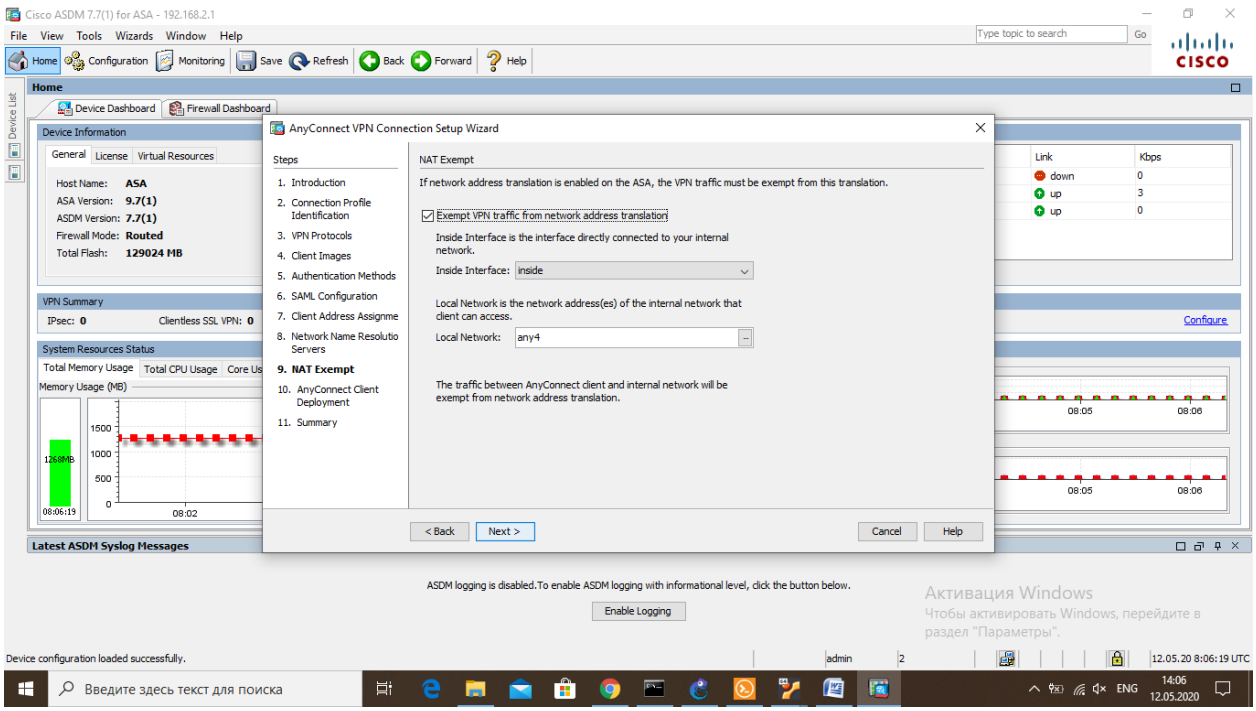
Сегізінші қадам, домен атауын және DNS серверін орнату, мұнда тек DNS серверін белгіледік, өйткені ASA қондырғысында домендік атауды көрсеткен болатынбыз (4.24 суретті қараңыз).



4.24 сурет – DNS серверін көрсетіңіз

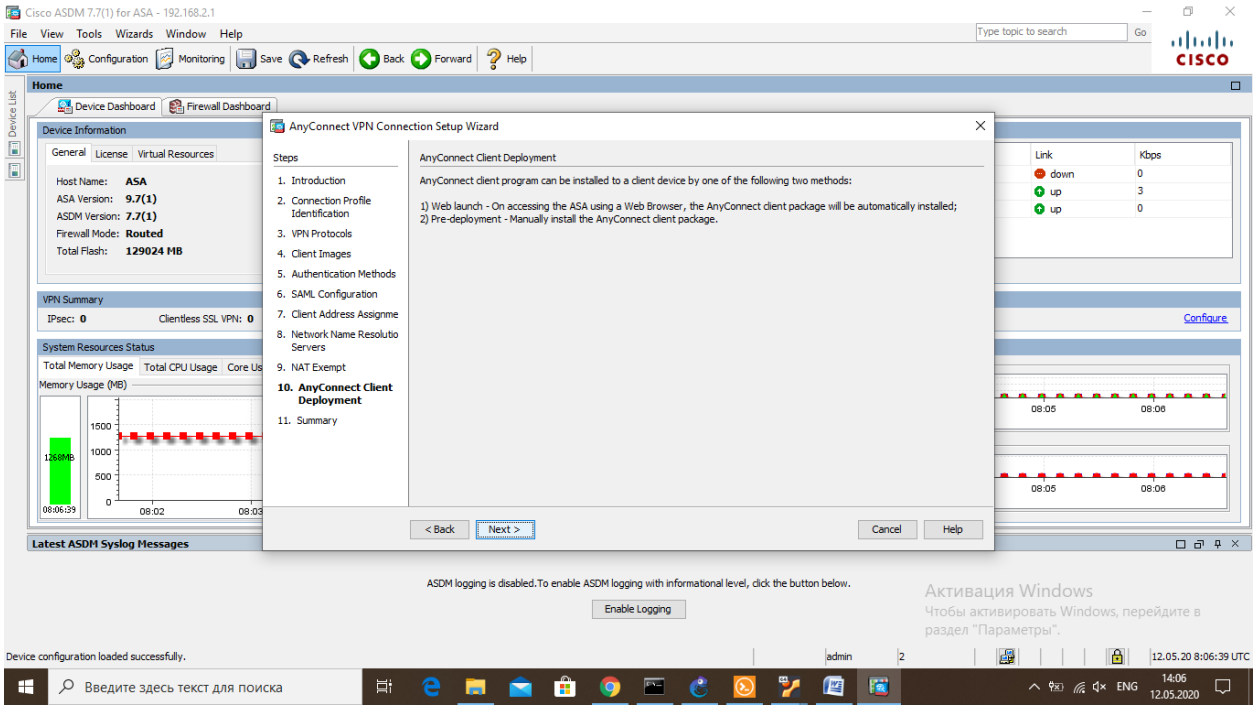
Тоғызыншы қадамда NAT-тан ерекшелік жасау үшін құсбелгіні салыңыз, бұл аппараттық LAN-нан пакеттер қашықтағы пайдаланушының AnyConnect клиентіне оралған кезде, олар таратылмайтындай етіп оралуы үшін қажет,

әйтпесе сіз бір жақты байланыс аласыз. «Inside» интерфейсіндегі барлық IP мекенжайлар олар AnyConnect VPN Client үшін аудармадан шығарылады (4.25 суретті қараңыз).



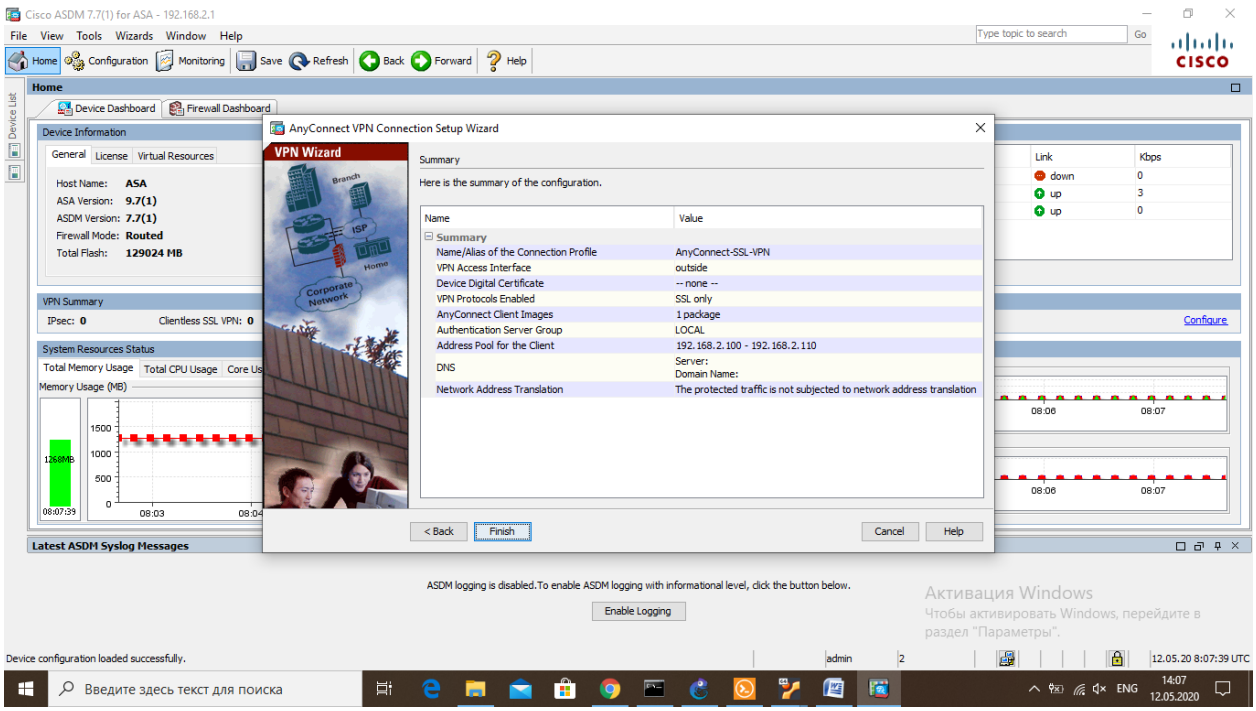
4.25 сурет – NAT ережесінен ерекшелік

Әдепкі бойынша, егер «https» арқылы ASA-ға қосылатын болса, AnyConnect VPN Client-тін орнатуға мүмкіндік береді. Осыдан кейін ол сізге автоматты түрде AnyConnect VPN Client-ті орнатуды SSL веб-браузер арқылы жүктеуді ұсынады (4.26-суретті қараңыз).



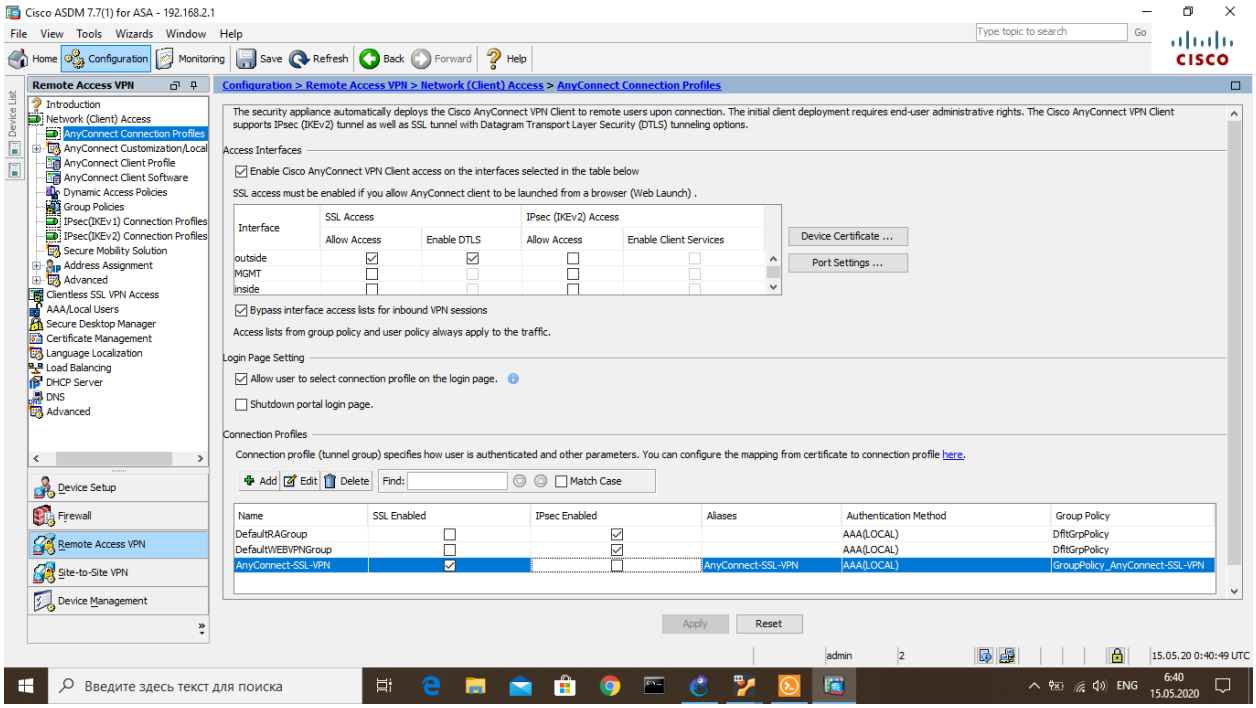
4.26 сурет – AnyConnect VPN клиентін жүктеуге келісім

Соңғы қадам – AnyConnect VPN баптаулары дұрыс екеніне көз жеткізіп «Finish» батырмасын бастық (сурет 4.27 қараңыз).



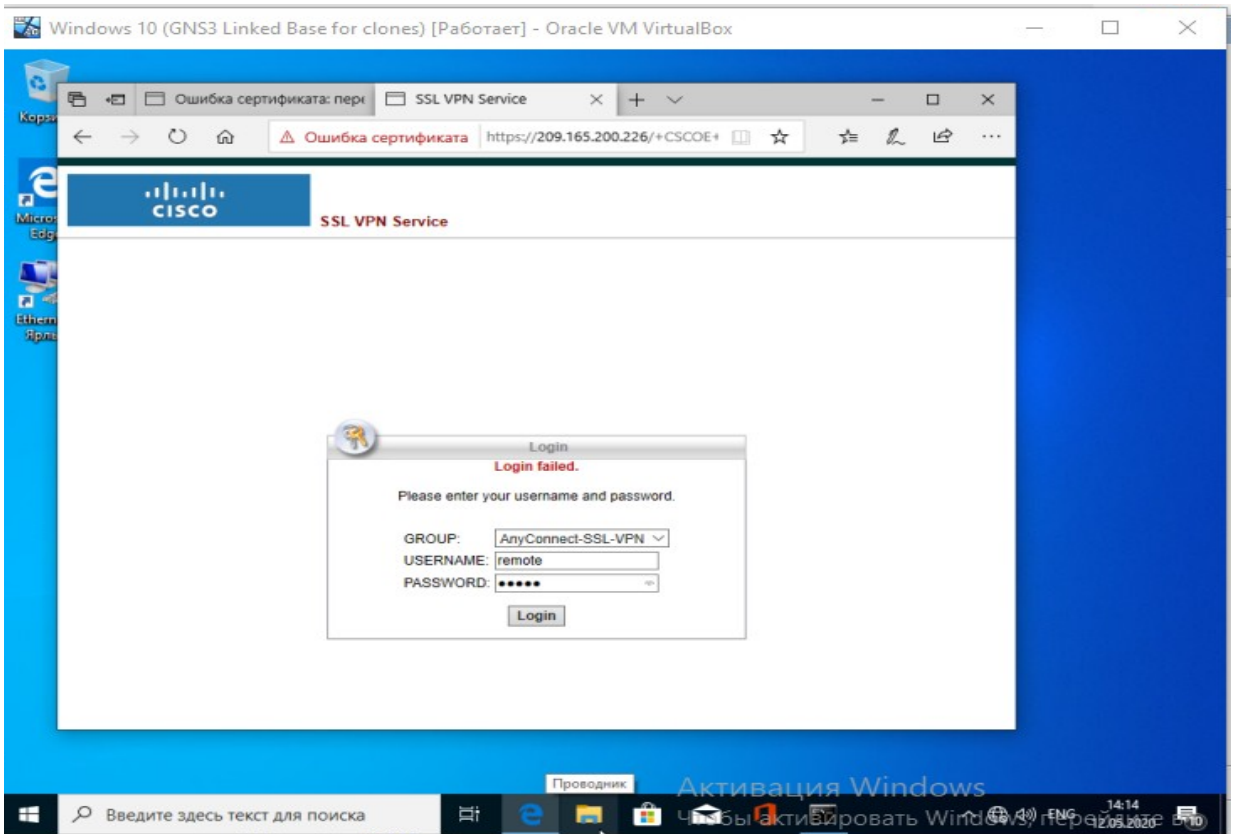
4.27 сурет – AnyConnect VPN-нің соңғы қадамы

Негізгі конфигурация мәзірі, құрылған AnyConnect VPN көрдік (сурет 4.28 қараңыз).



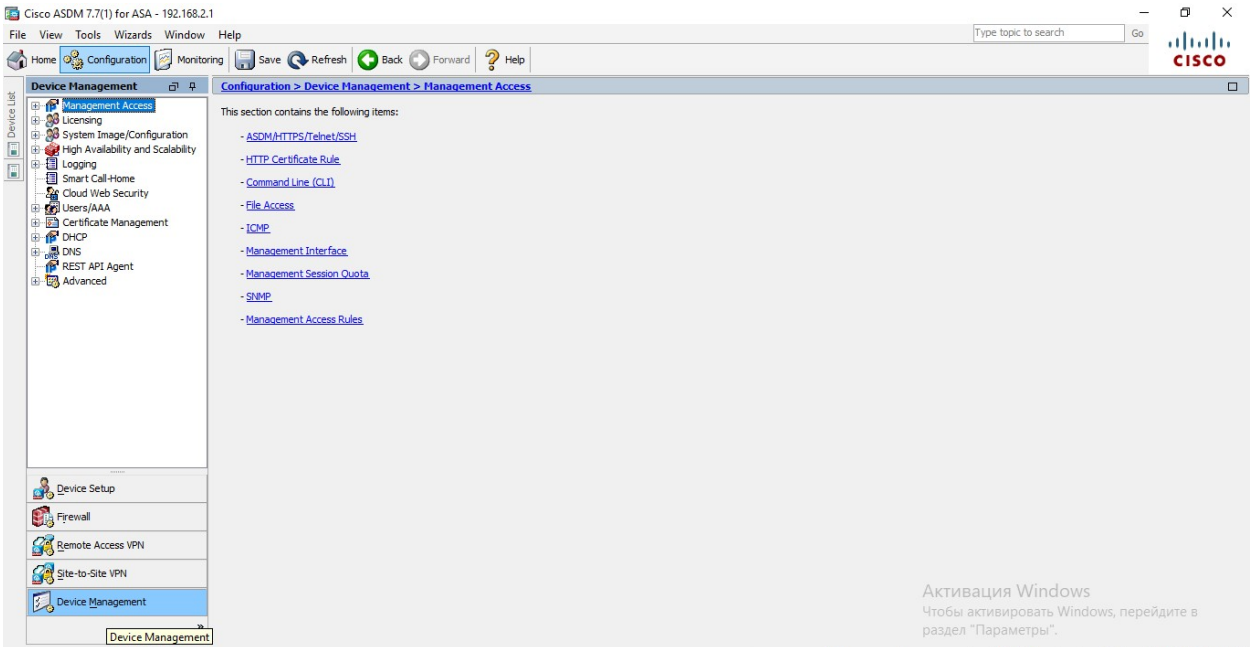
4.28 сурет – Негізгі конфигурация мәзірі

Енді қашықтағы пайдаланушы арқылы ASA-ға қосылуға тырысамыз, ол аутентификация әдістерін сұрауда, яғни топты, логин мен құпия сөзді, бәрін дұрыс енгізгенімен, бірақ аутентификация әдістерінен отпегініміз жайлы хабар берді (сурет 4.29 қараңыз).

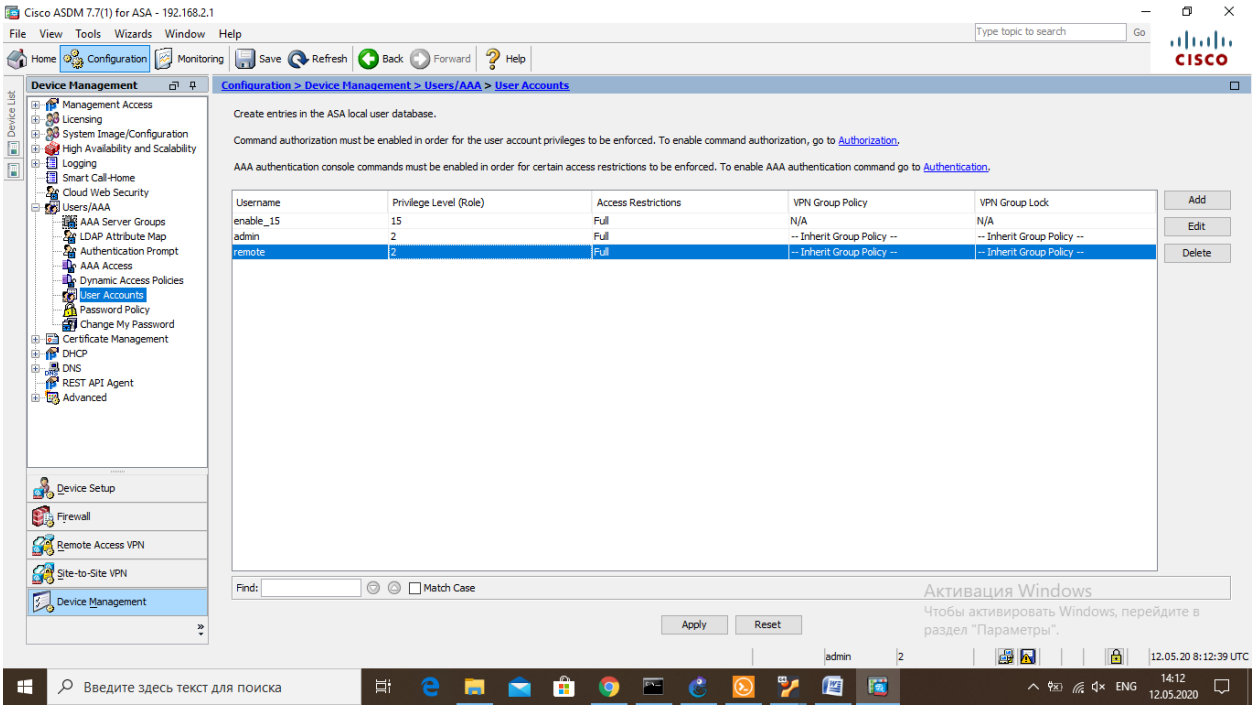


4.29 сурет – Аутентификация әдісі

Қоолданушының түпнұсқалығын растау үшін, ASA-дағы тағы бір баптауларды орындауымыз керек, ол үшін «Configuration» қойындысын басып, «Device Management» тармақтарына мәзірін тандап, «User accounts» тармағына кіріп, керек қолданушыны тандап «Edit» батырмасымен баптаулар жасадық (4.30-4.31 суретті қараңыз).

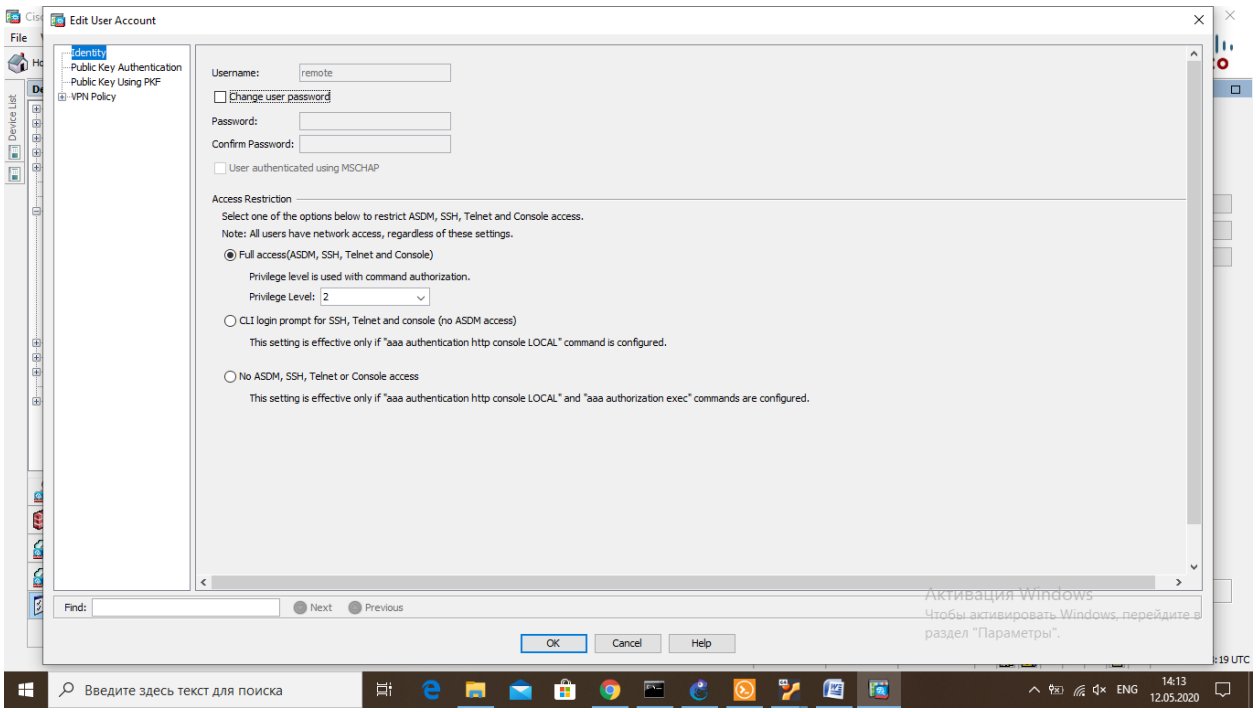


4.30 сурет – Пайдаланушыға арналған ASA параметрлері

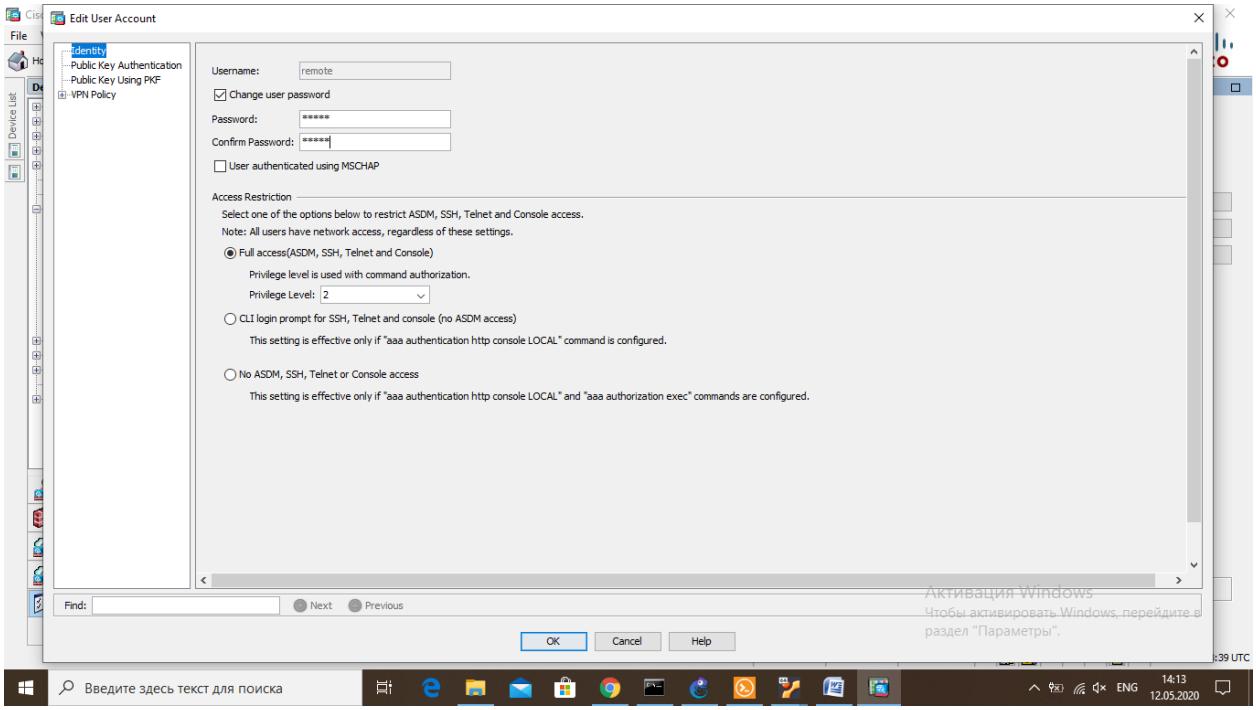


Сурет 4. 31 – Пайдаланушыға арналған ASA параметрлері

Пайдаланушы параметрлерінде құпия сөздің орны бос екендігін көріп, енді құпия сөзді енгізу үшін пайдаланушы құпия сөзін өзгертуге құсбелгі қойып, қашықтағы пайдаланушының құпия сөзін енгіздік (4.32-4.33 суретті қараңыз).

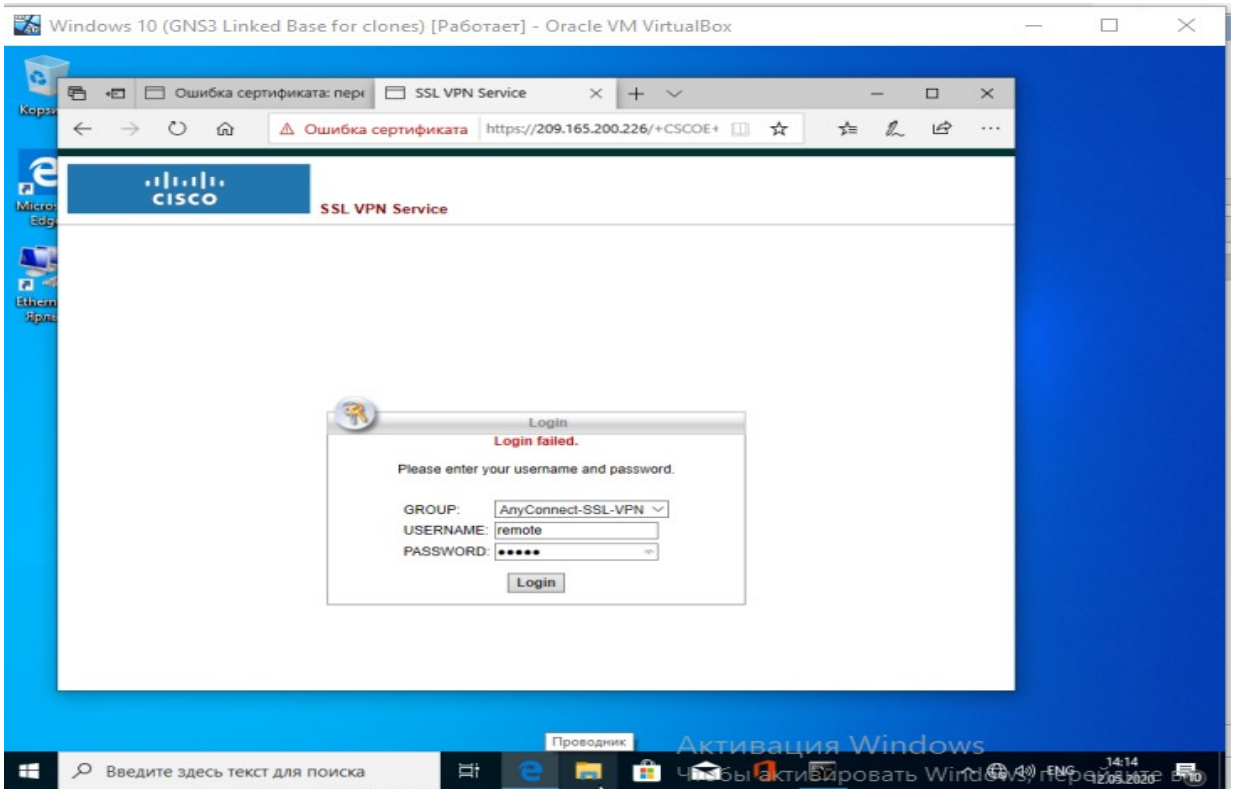


Сурет 4.32 – Қашықтағы пайдаланушының баптаулары



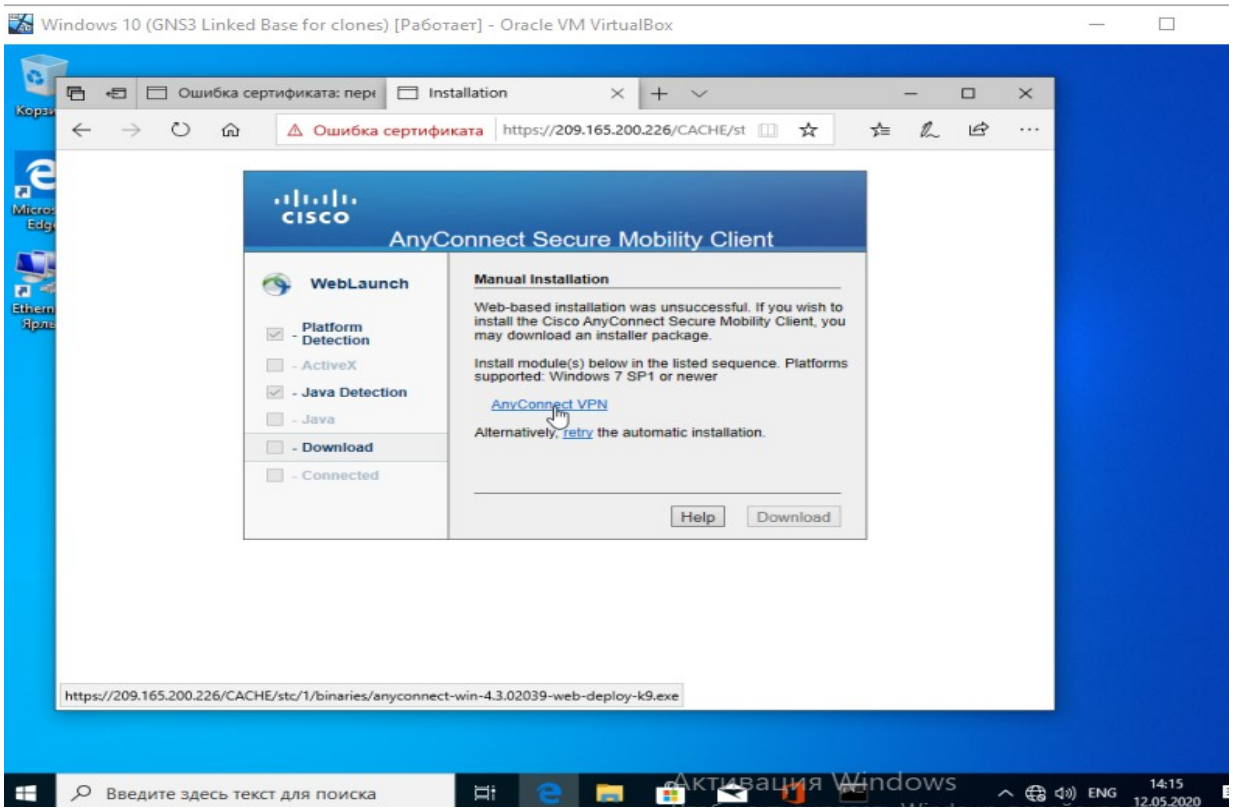
Сурет 4.33 – Қашықтағы пайдаланушының баптаулары

Енді қашықтағы пайдаланушының әрекеттін қайталап, топты, аты мен құпия сөзді енгіздік (4.34 суретті қараңыз).



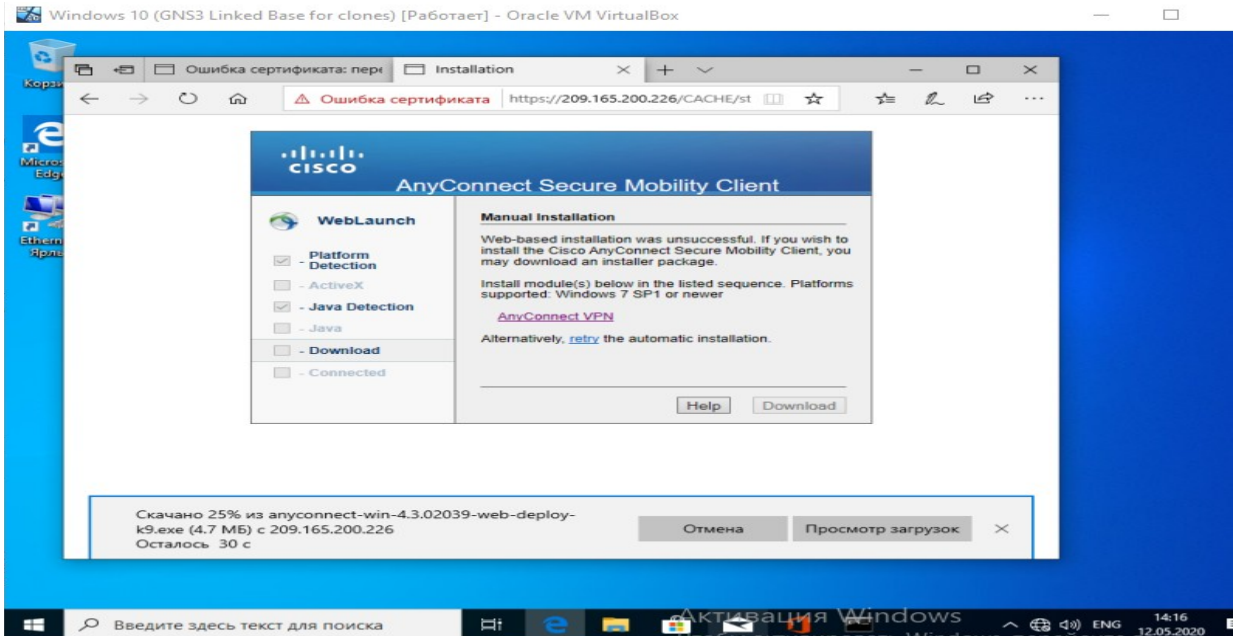
4.34 сурет – Қашықтағы пайдаланушының аутентификациясы

Осыдан кейін ASA бізге AnyConnect VPN Client бағдарламалық жасақтамасын жүктеуді ұсынады (4.35-суретті қараңыз).

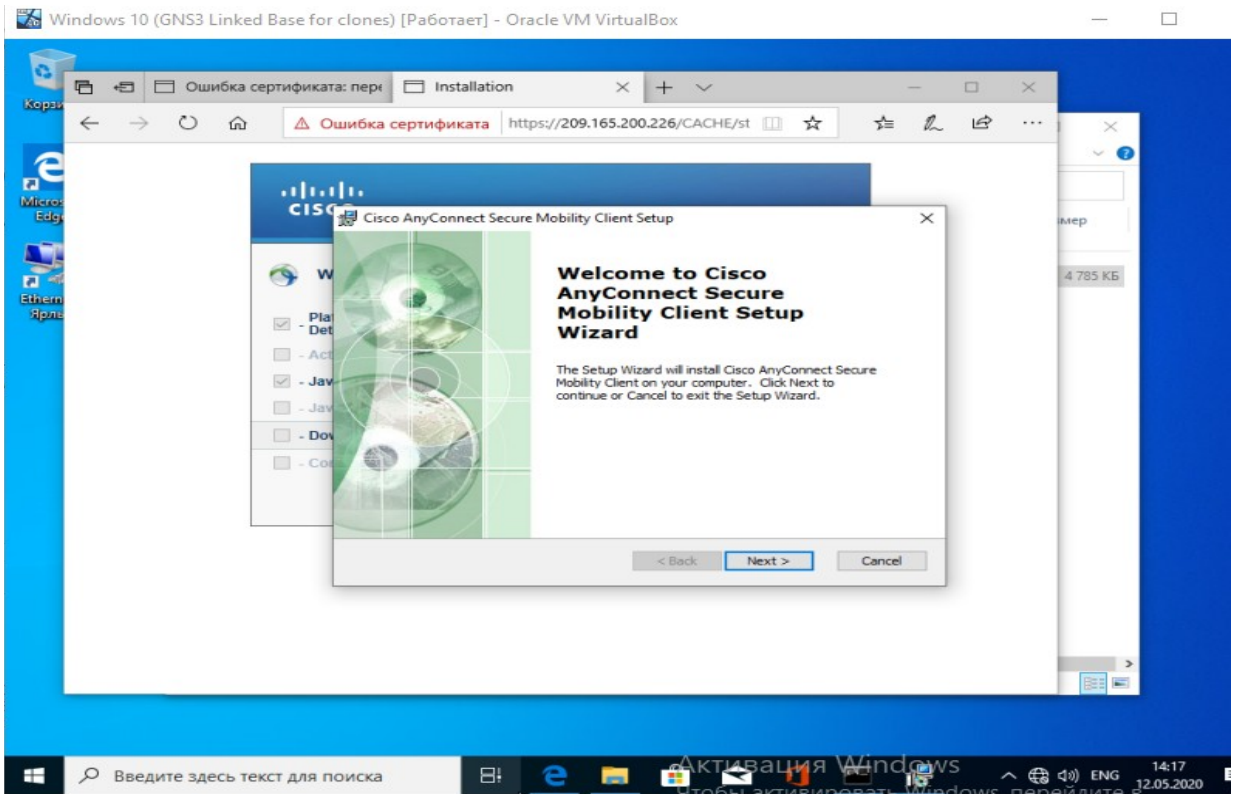


4.35 сурет – AnyConnect VPN Client бағдарламалық жасақтамасын жүктеу

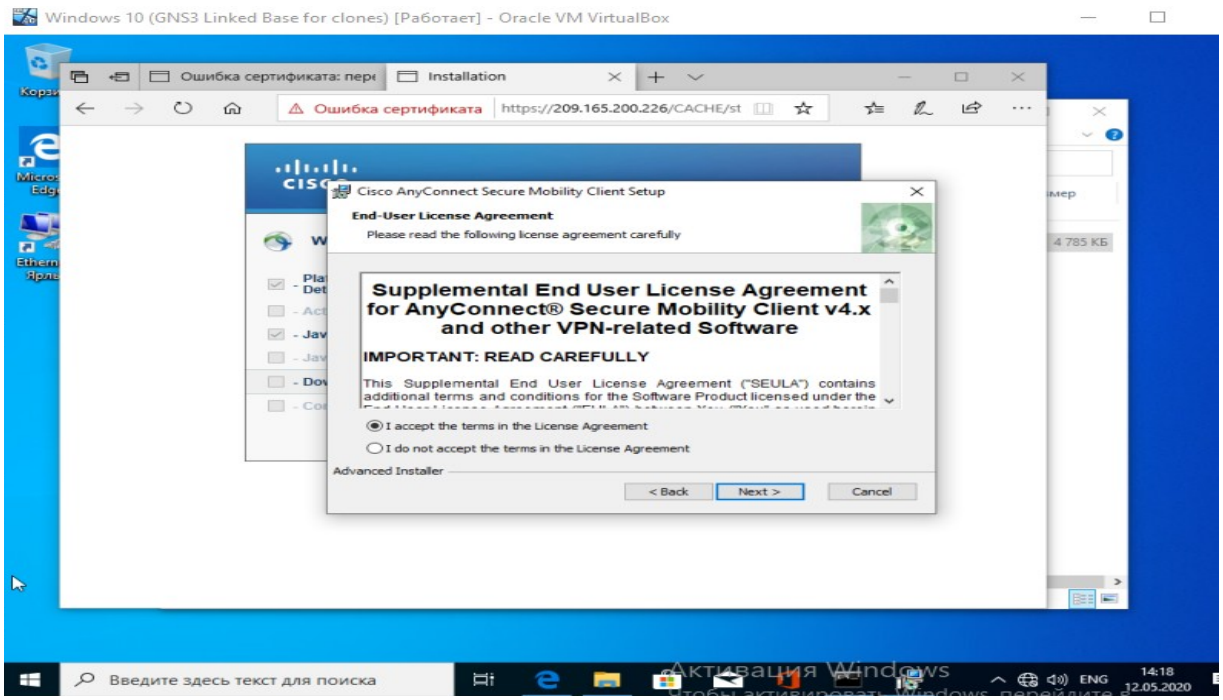
Бағдарламалық жасақтаманы жүктеу процесі орындалды (4.36-4.40 суретті қараңыз).



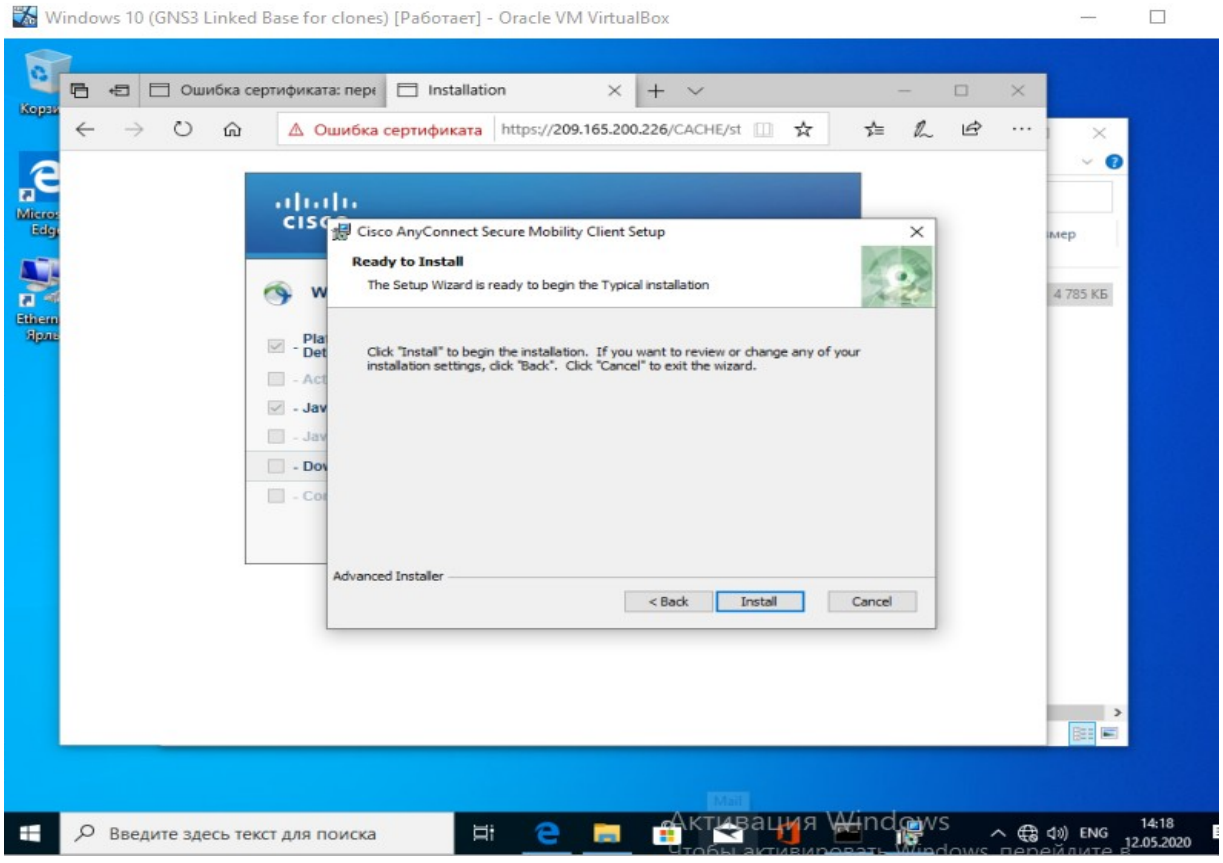
4.36-сурет – AnyConnect VPN Client бағдарламалық жасақтамасын жүктеу



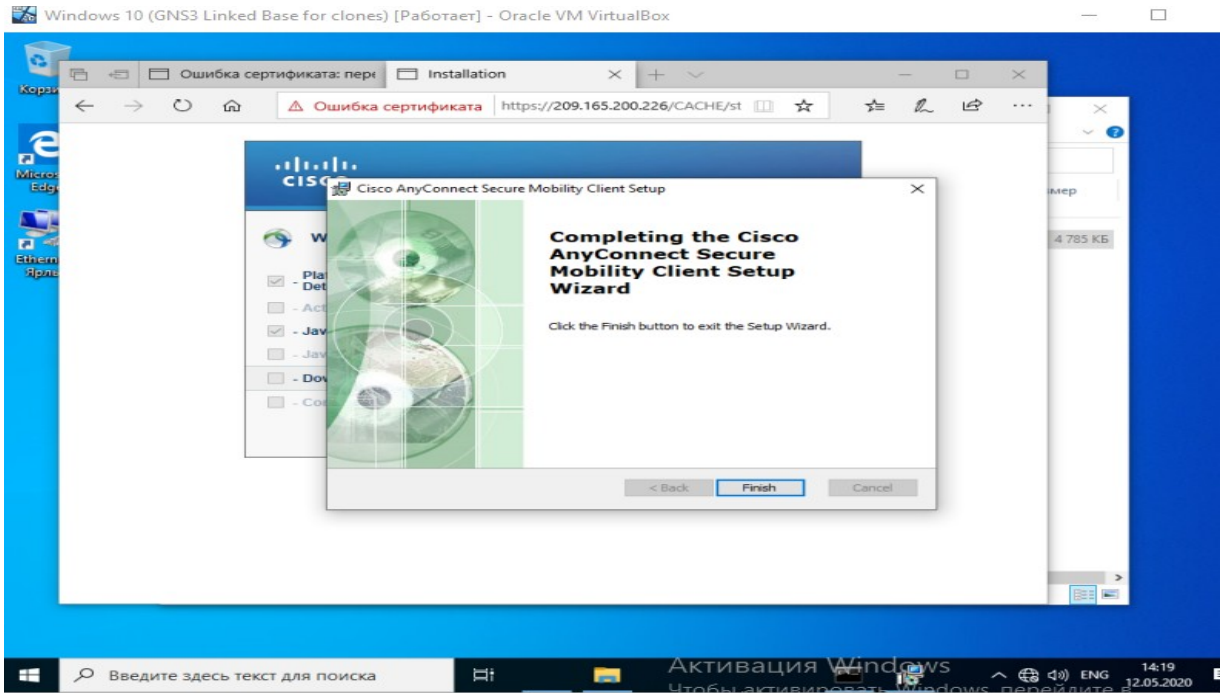
4.37 сурет – БЖ жүктеу процесі



4.38 сурет – БЖ-ның лицензиясымен келісу

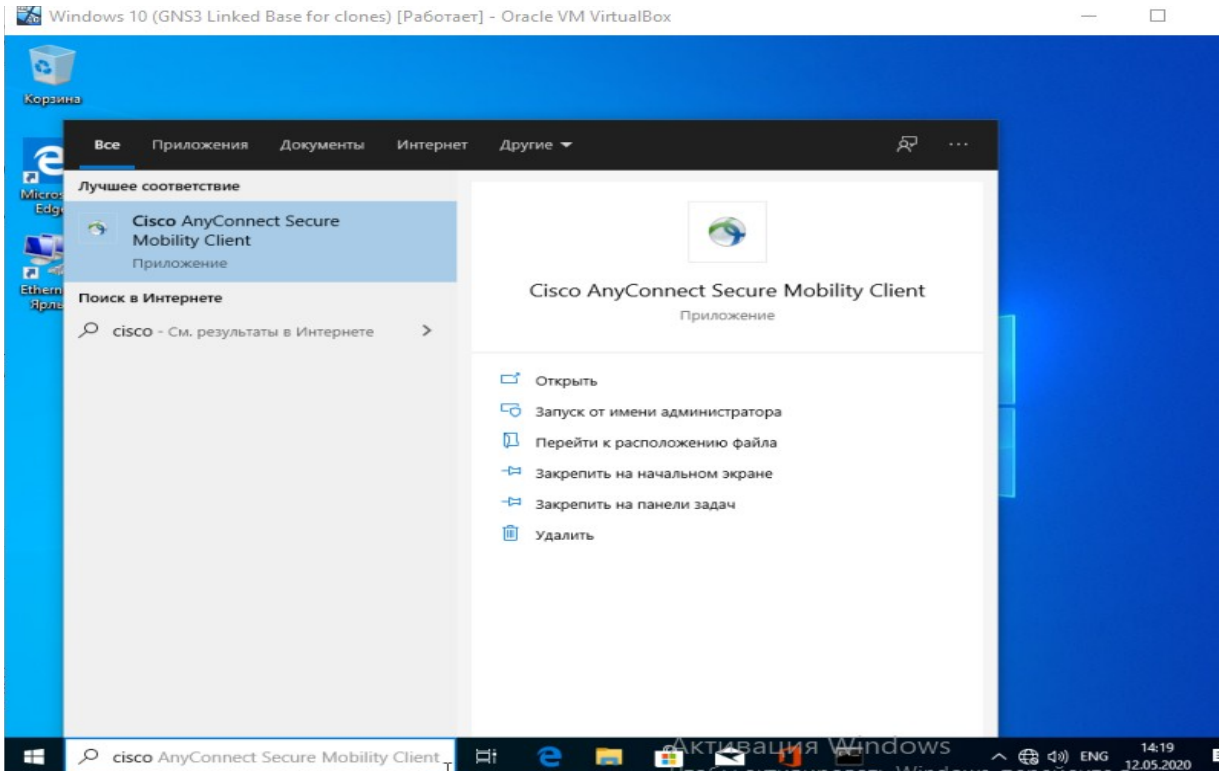


4.39 сурет – БЖ жүктеу процесі



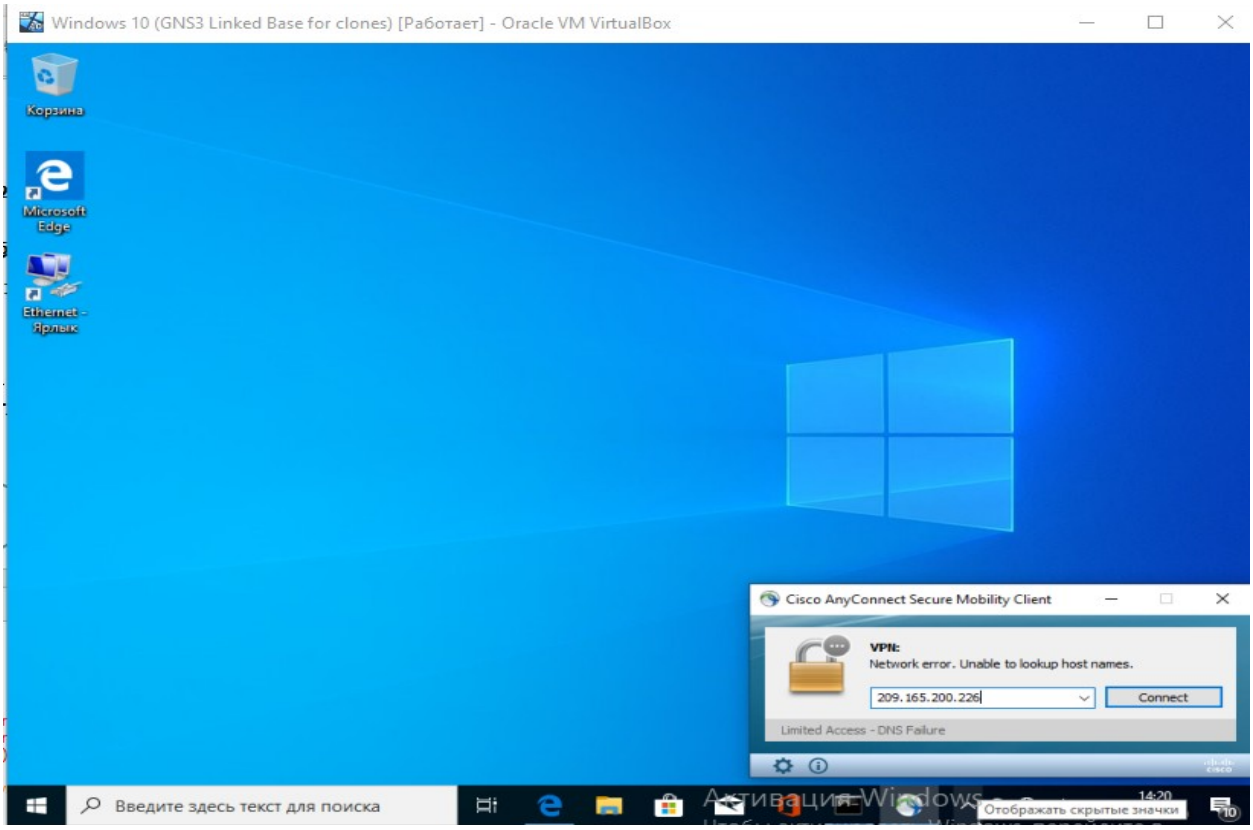
4.40 сурет – БЖ жүктеу процесі аяқталды

Біз «Cisco AnyConnect Secure Mobility Client» бағдарламасын іске қосамыз (4.31 суретті қараңыз).



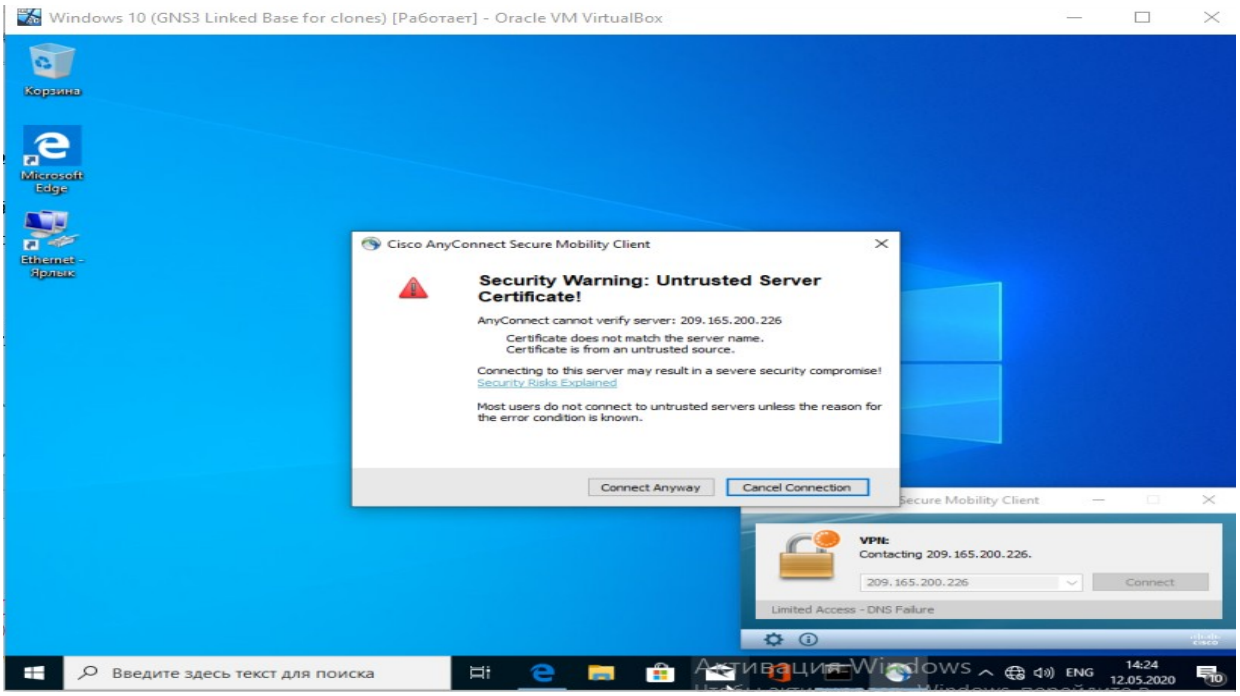
4.41сурет – бағдарламалық жасақтаманы қосу

Бағдарламалық жасақтаманы іске қосқаннан кейін, байланыс үшін ASA мекенжайын енгізу керек (4.32-суретті қараңыз).



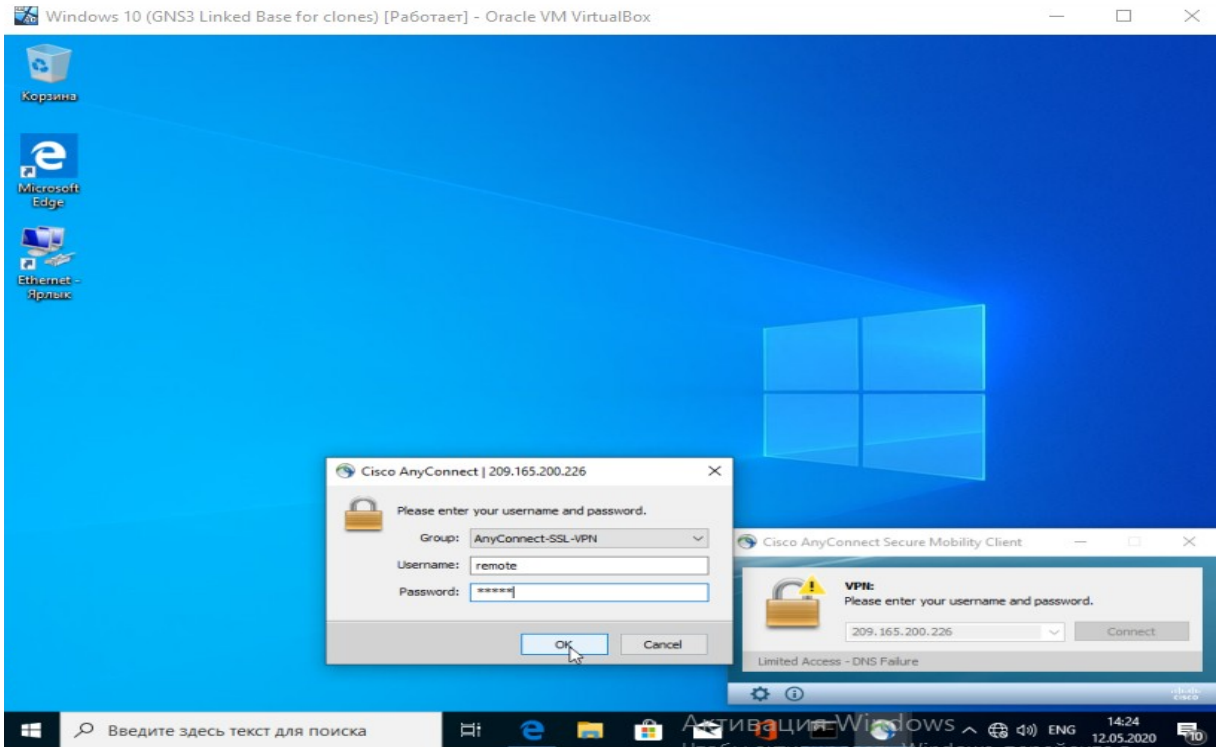
4.42 сурет – Қашықтағы пайдаланушыны ASA-ға қосу

Өз-өзіміз қол қойған куәлікті көрсеткендіктен, ұрысу үстінде, біз кез-келген жағдайда қосылу опциясын таңдаймыз (4.33- суретті қараңыз).



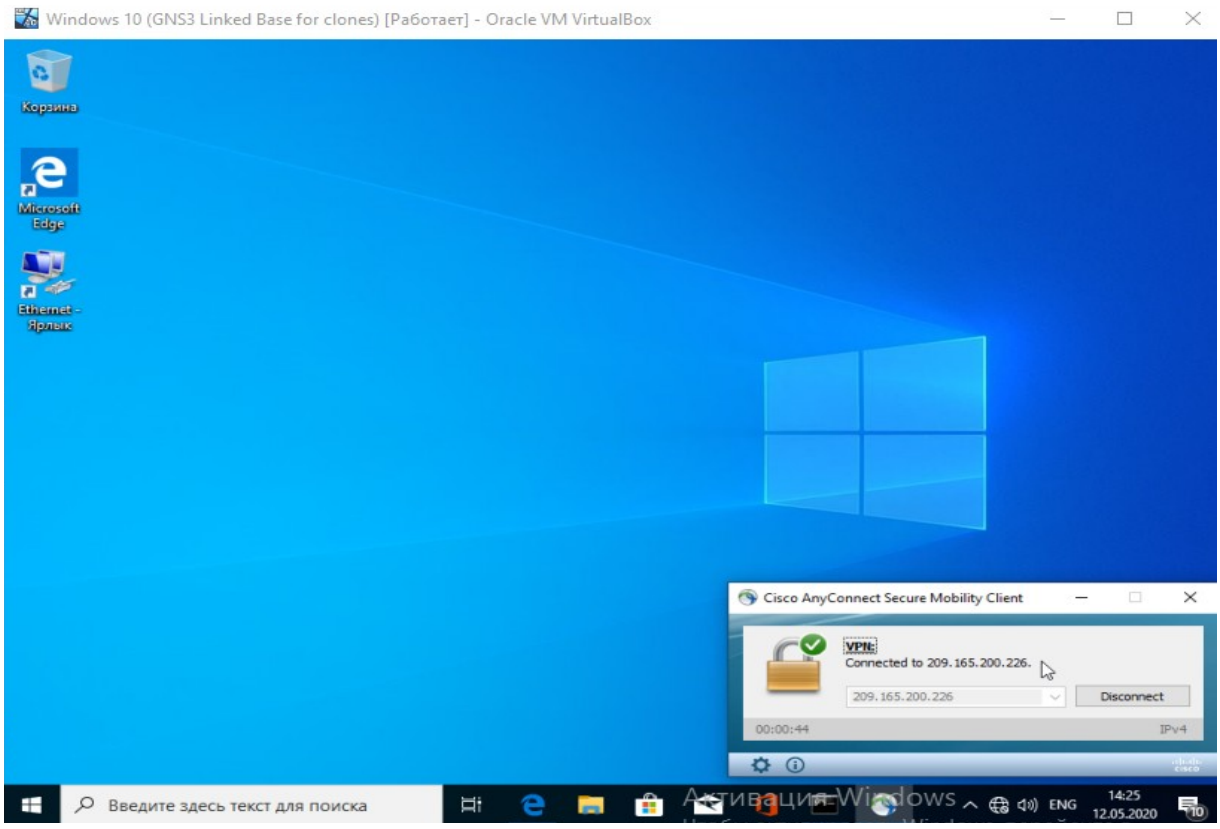
4.43 сурет – Кез-келген жағдайда байланыс

Байланысқан кезде бізден пайдаланушының тобын, аты мен құпия сөзін енгізуді сұрады (4.44 суретті қараңыз).



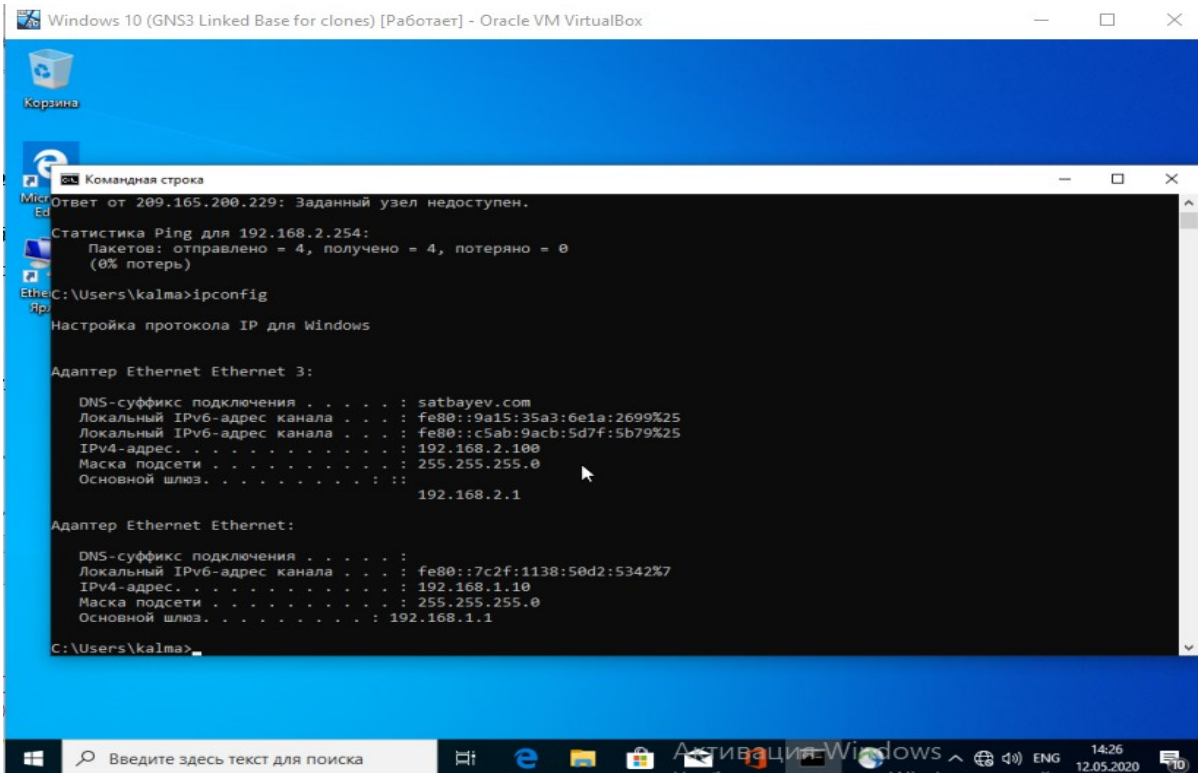
4.44 сурет – Аутентификация әдісі

Қашықтықтан қосылуды пайдалуны барлық деректерді енгізіп, байланыс жасады (4.45 суретті қараңыз).



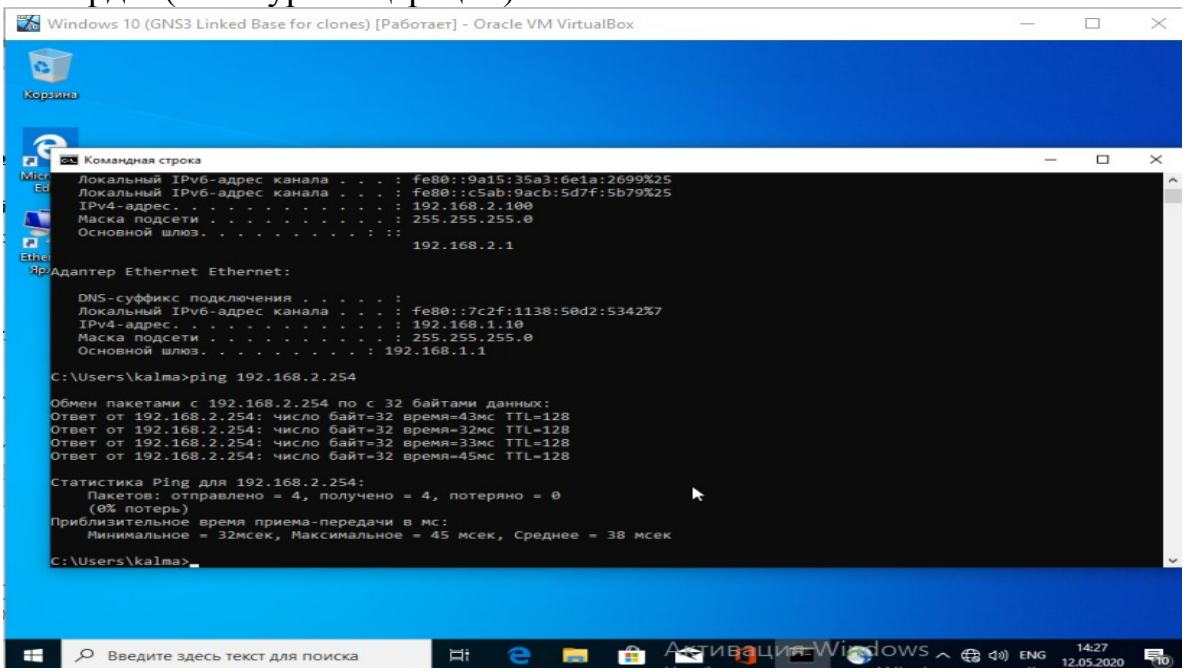
4.45 сурет – Қосылым сәтті өтті

Қосылғаннан кейін бағдарламалық жасақтамамыздың қай Pool-IP мекенжайын бергенін тексердік (4.46 суретті қараңыз).



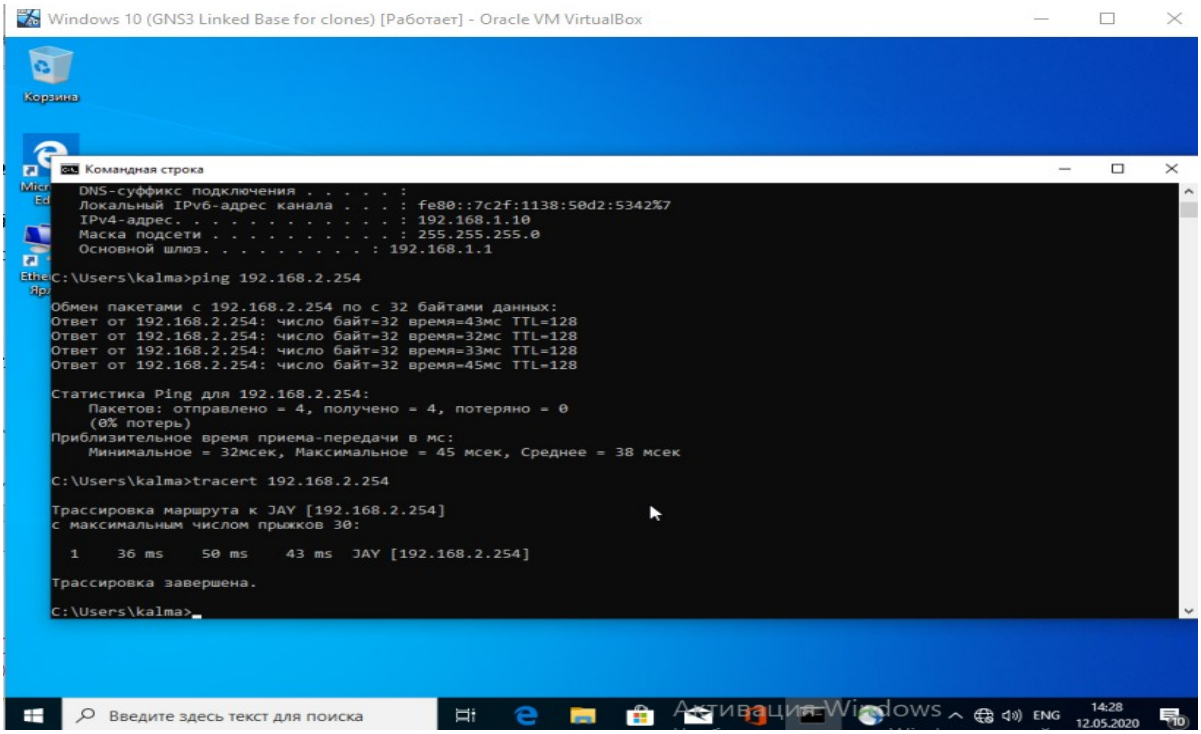
4.46 сурет – IP мекенжайын тексеру

Содан кейін «ping» командасымен біздің сервермен байланыс бар-жоғын тексердік (4.47 суретті қараңыз).



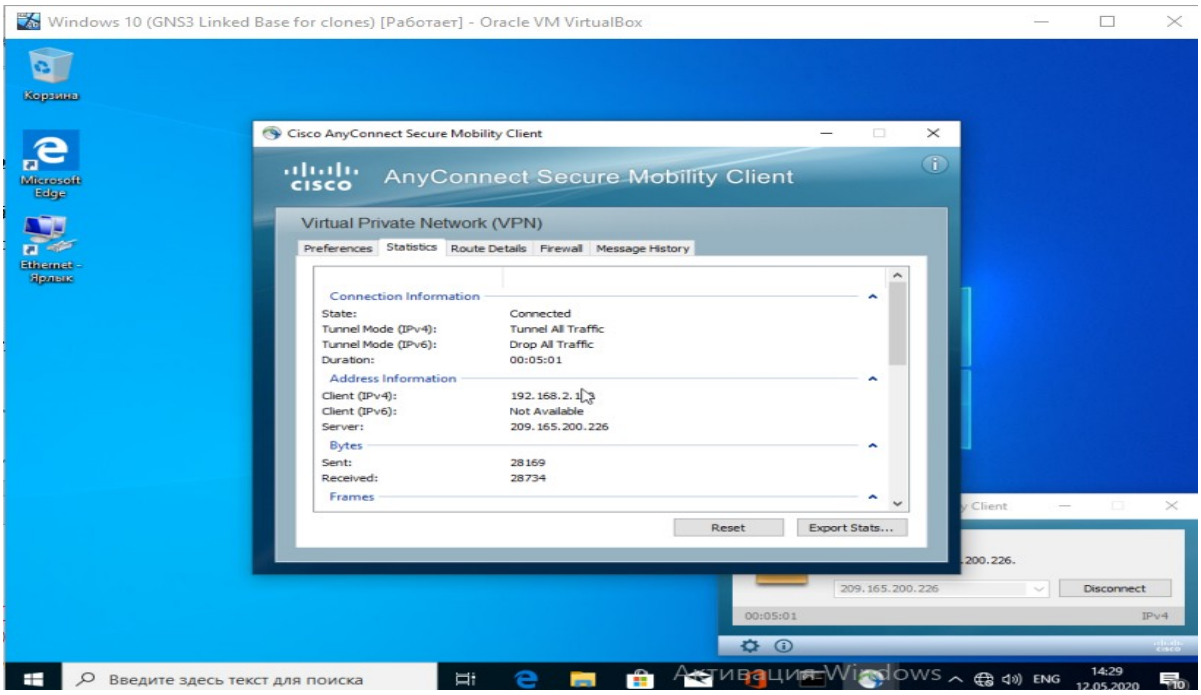
4.47 сурет – Сервермен байланысты тексеру

Осыдан кейін маршруттың ізін «tracert» пәрменін пайдаланып тексердік (4.48 суретті қараңыз).



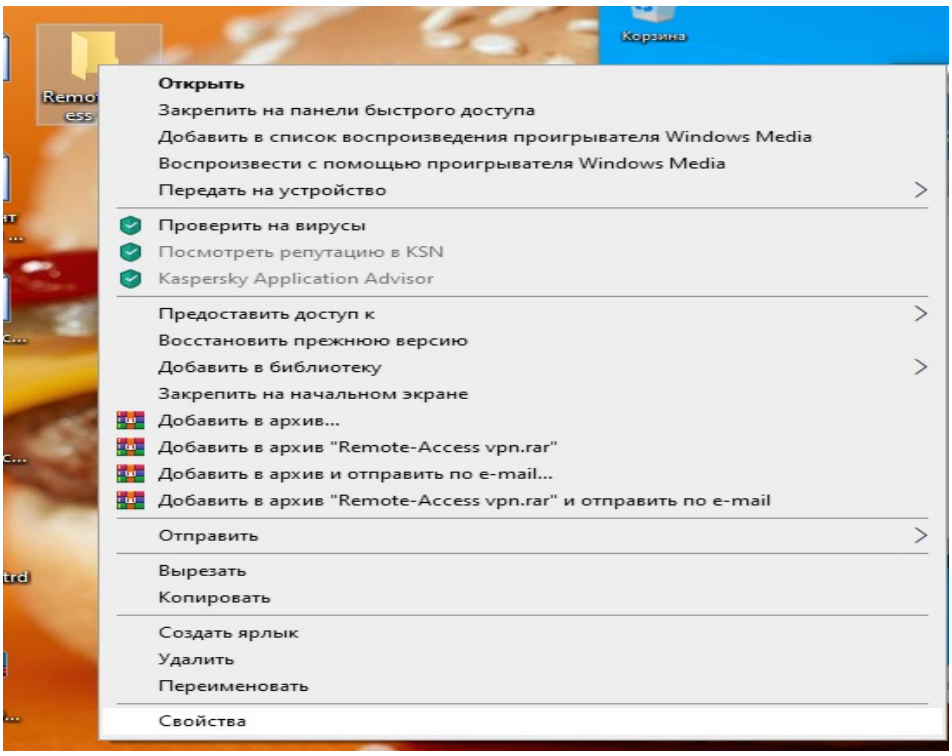
4.48 сурет – Тағайындалған серверге бағыттың ізін тексеру

AnyConnect VPN бағдарламалық жасақтамасының параметрлерін қарастырдық. (4.49- суретті қараңыз).



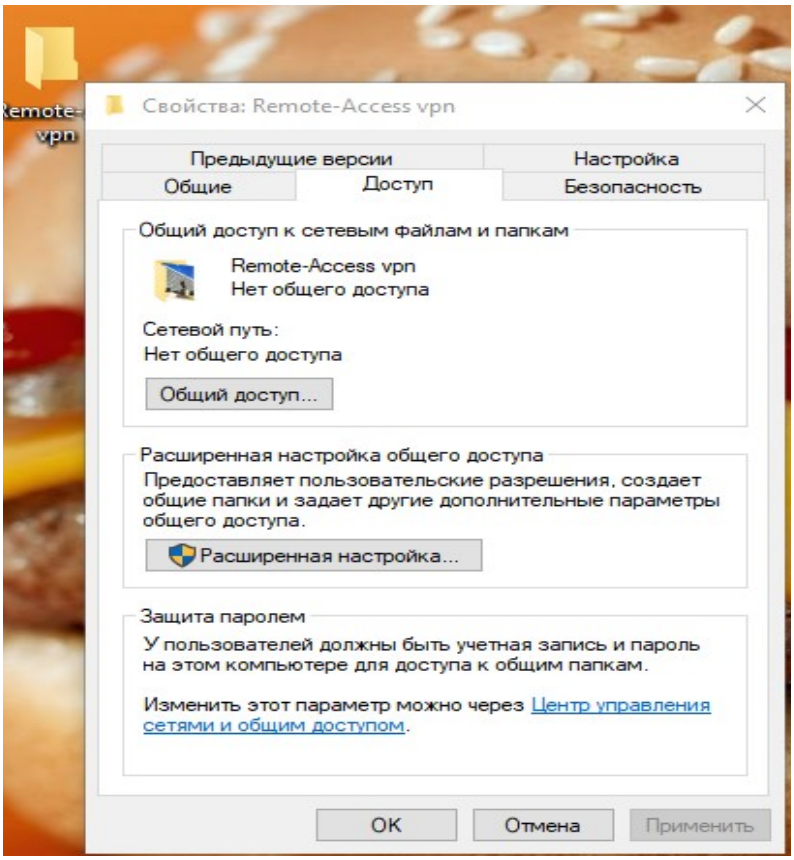
4.49-сурет – БЖ параметрлерін қарау

Енді қашықтықтан пайдаланушы үшін керек деректерді ашу баптауларын қарадық, ол үшін «Свойства» батырмасын бастық (4.50-суретті қараңыз).



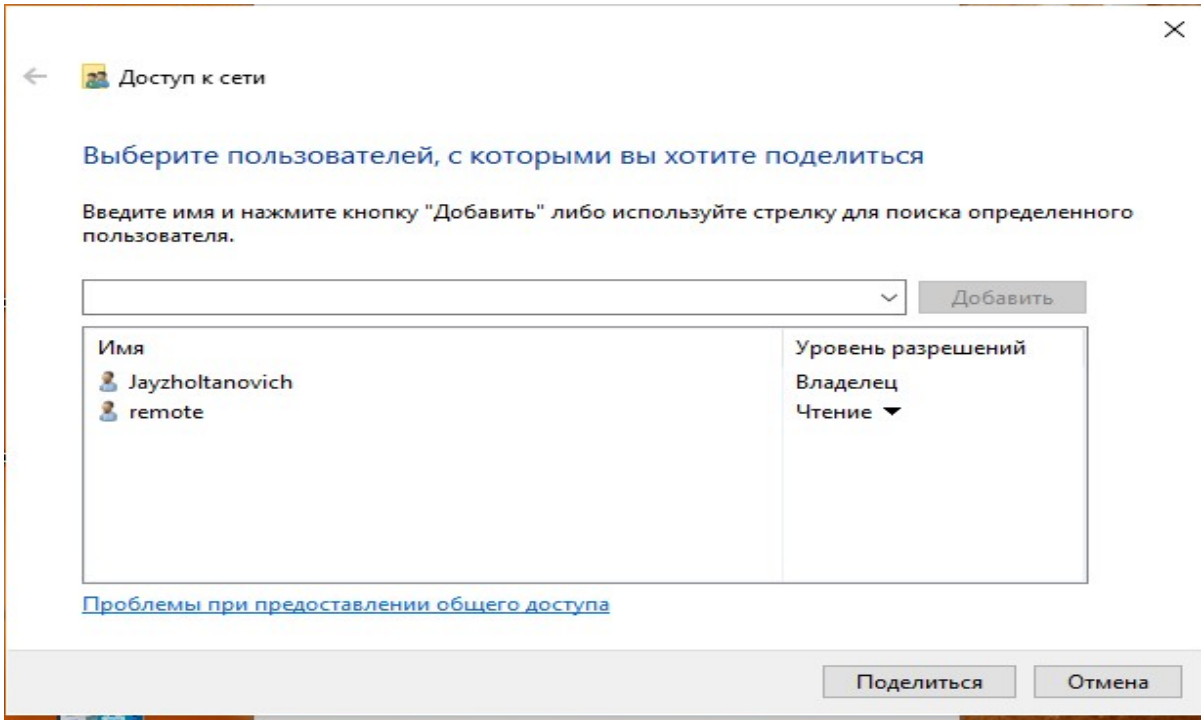
4.50 сурет – Қашықтағы пайдаланушының баптаулары

Құрылымдағы «Доступ» бөліміне өтіп, ортақ қол жеткізу элементін таңдаңыз (4.51 суретті қараңыз).



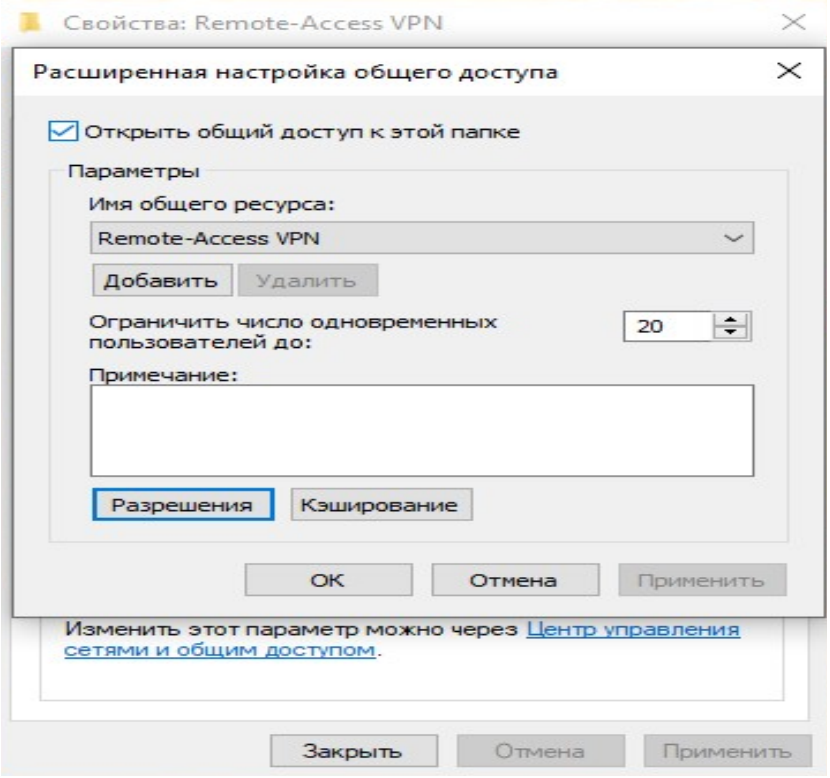
4.51-сурет – Ортақ пайдалану баптаулары

Біздің қашықтағы пайдаланушыны қосып және деректерді бөлістік (452 суретті қараңыз).



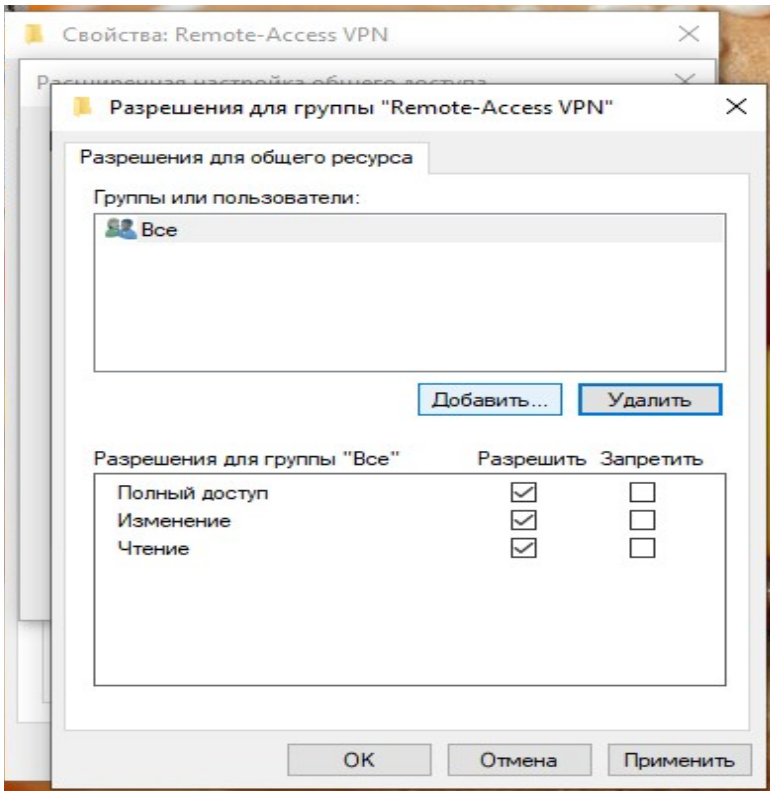
4.52 сурет – Қашықтағы пайдаланушы

Осыдан кейін кеңейтілген баптаулар бөліміне өтіп, осы пайдаланушы үшін рұқсаттылықты теңшедік (4.53 суретті қараңыз).



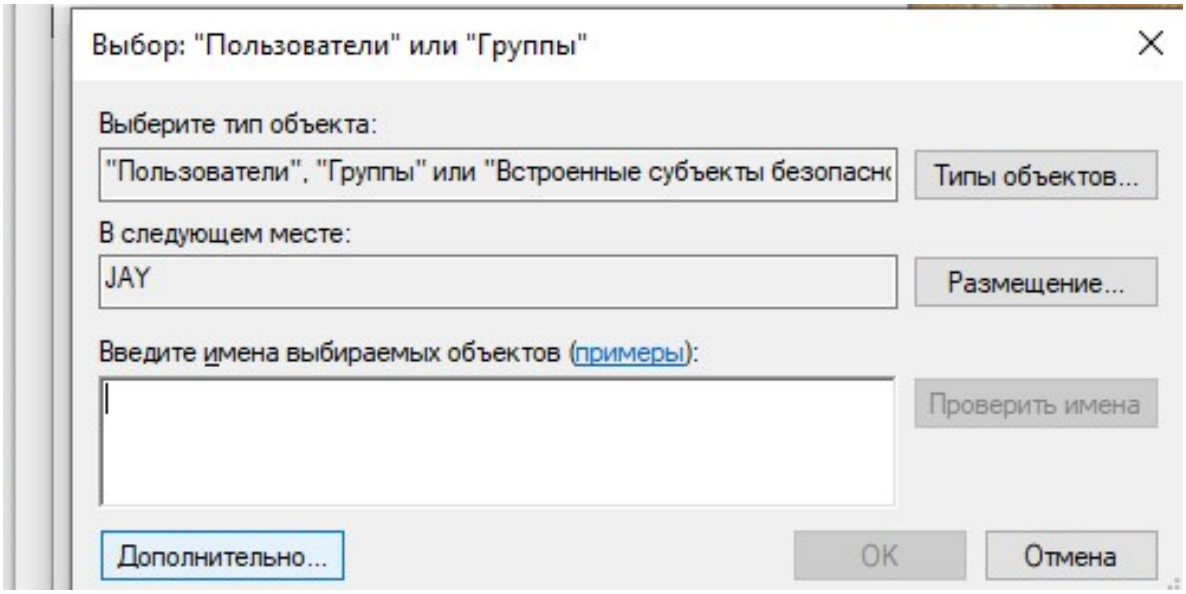
4.53 сурет – Қашықтағы пайдаланушыға рұқсатты теңшеу

Қашықтағы пайдаланушының кіру құқықтарын теңшедік, рұқсат ету және тыйым салу, бұл үшін қашықтағы пайдаланушыны қостық (4.54 суретті қараңыз).

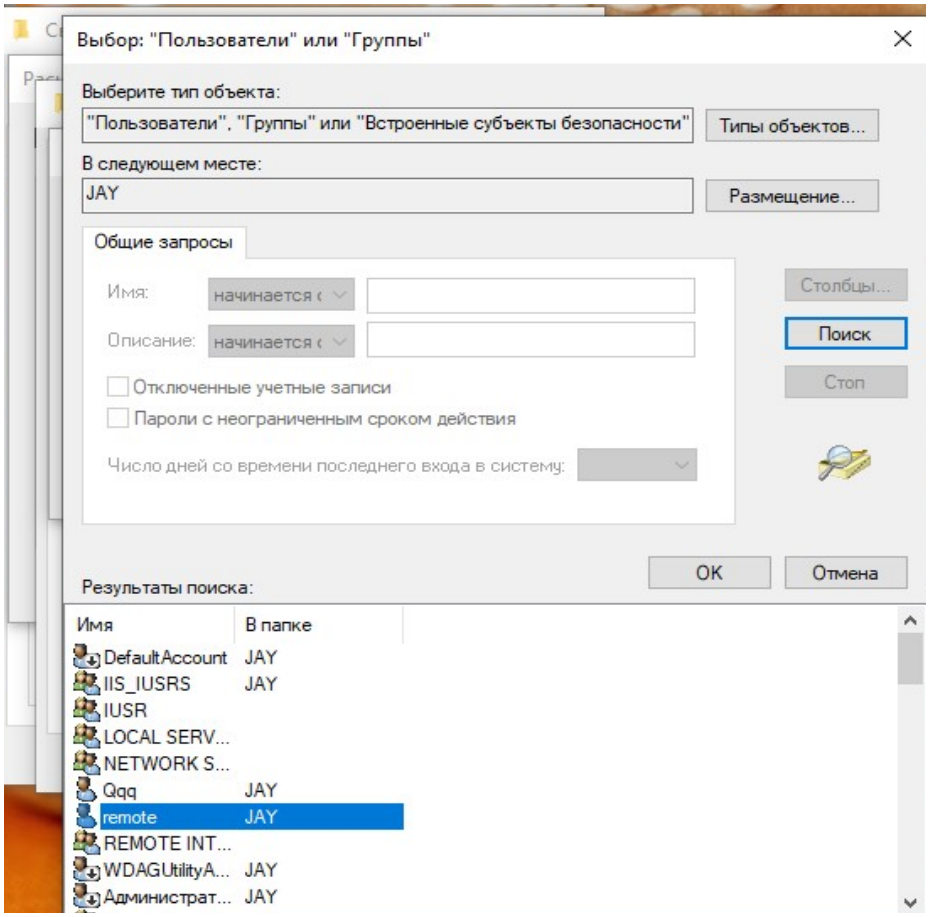


4.54 сурет – Қашықтағы пайдаланушыны қосу

Қашықтағы пайдаланушыны қосу үшін «Кеңейтілген» қойындысына және «Іздеу» тармағына өтіп, пайдаланушымызды таңдадық (суретті 4.55-4.56 қараңыз).

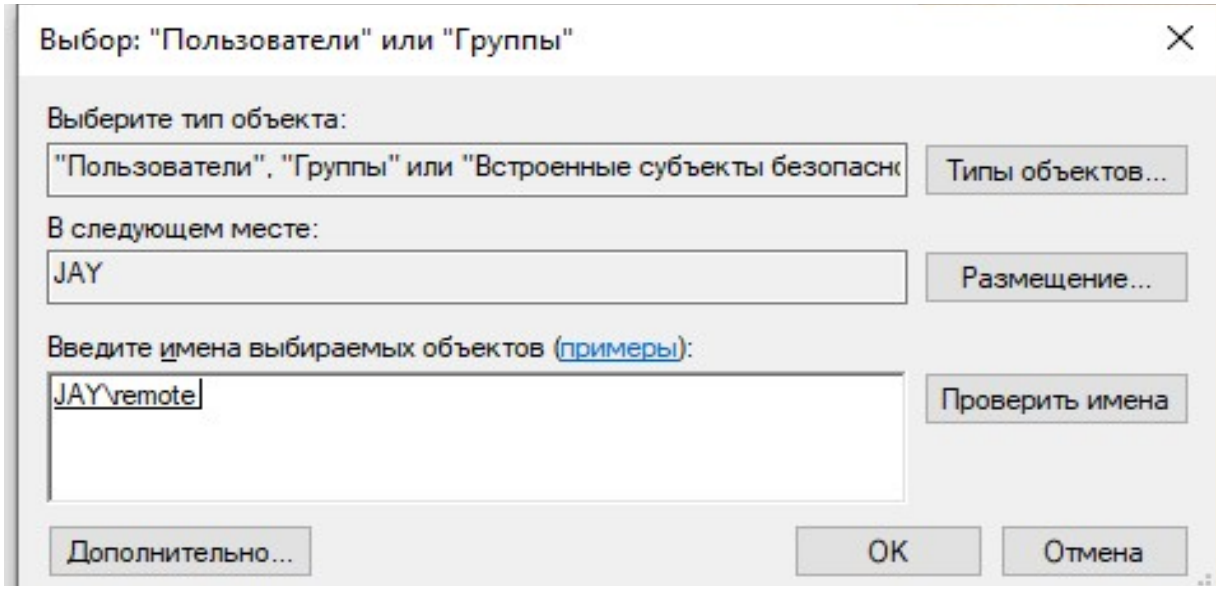


4.55-сурет – Қашықтағы пайдаланушыны қосу



4.56 сурет – Қашықтан пайдаланушыларды таңдау

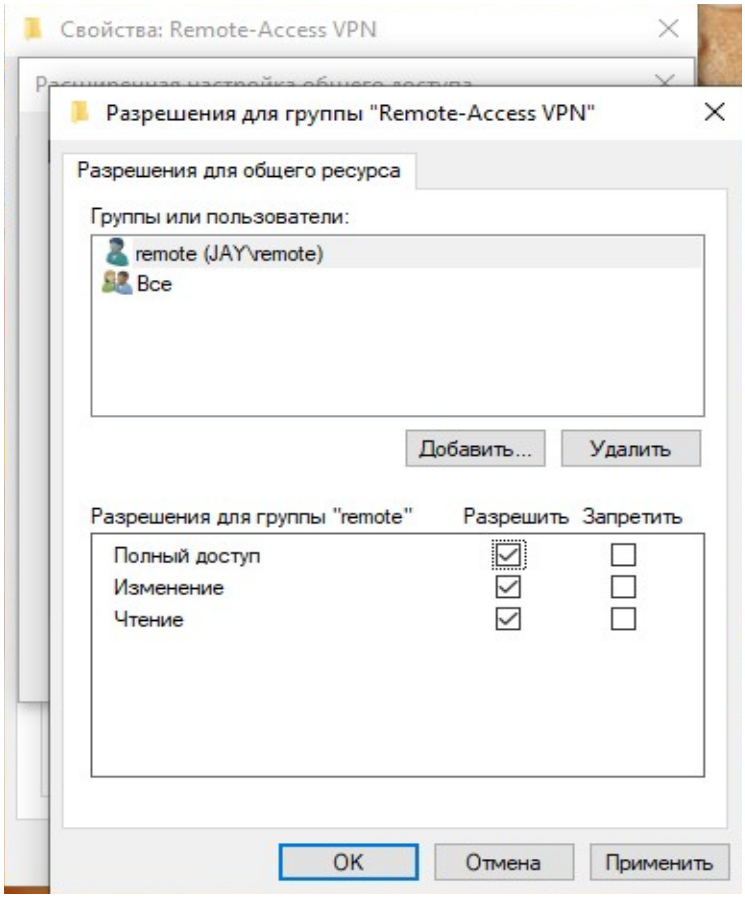
Осы қадамдардан кейін біз қашықтағы пайдаланушыны қостық (4.57- суретті қараңыз).



Сурет 4.57 – Қашықтағы пайдаланушыны қосу

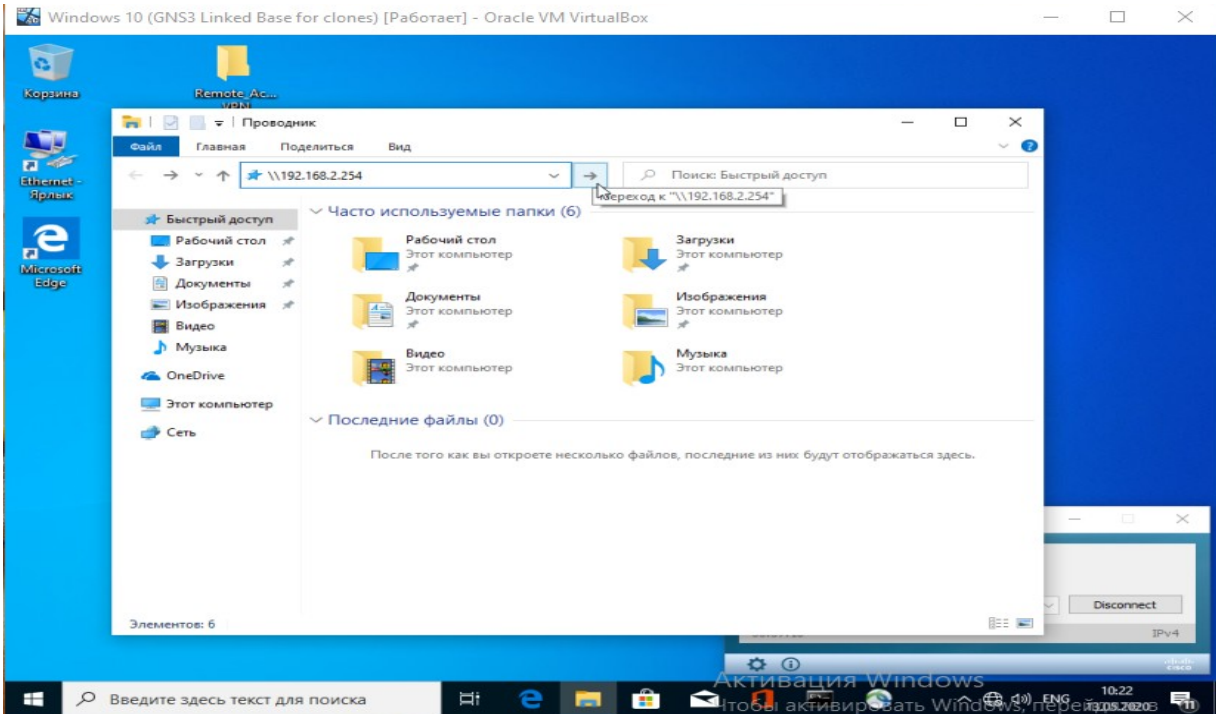
Енді осы қашықтағы пайдаланушы үшін кіру құқығын көрсеттік

(4.58 суретті қараңыз).



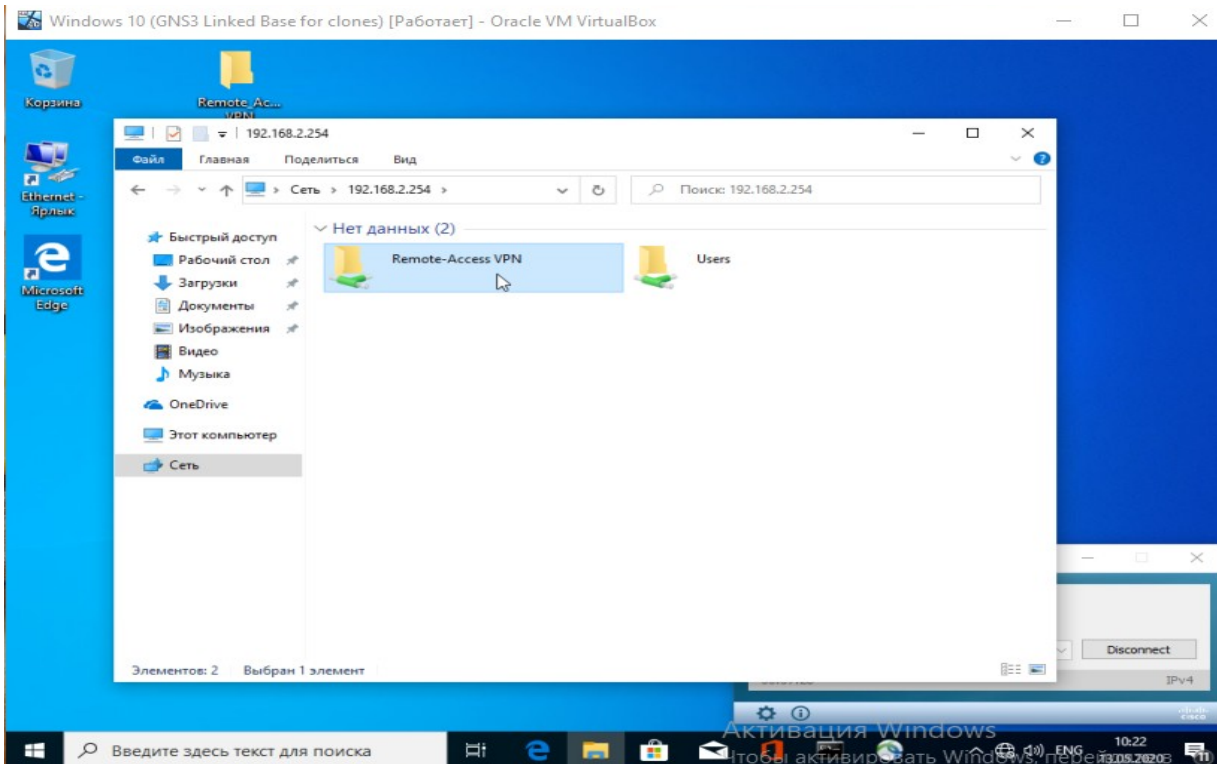
Сурет 4.58 – Қашықтағы пайдаланушыға қол жеткізу құқығын көрсету

Енді қашықтағы пайдаланушы серверге қосылды (4.59- суретті қараңыз).



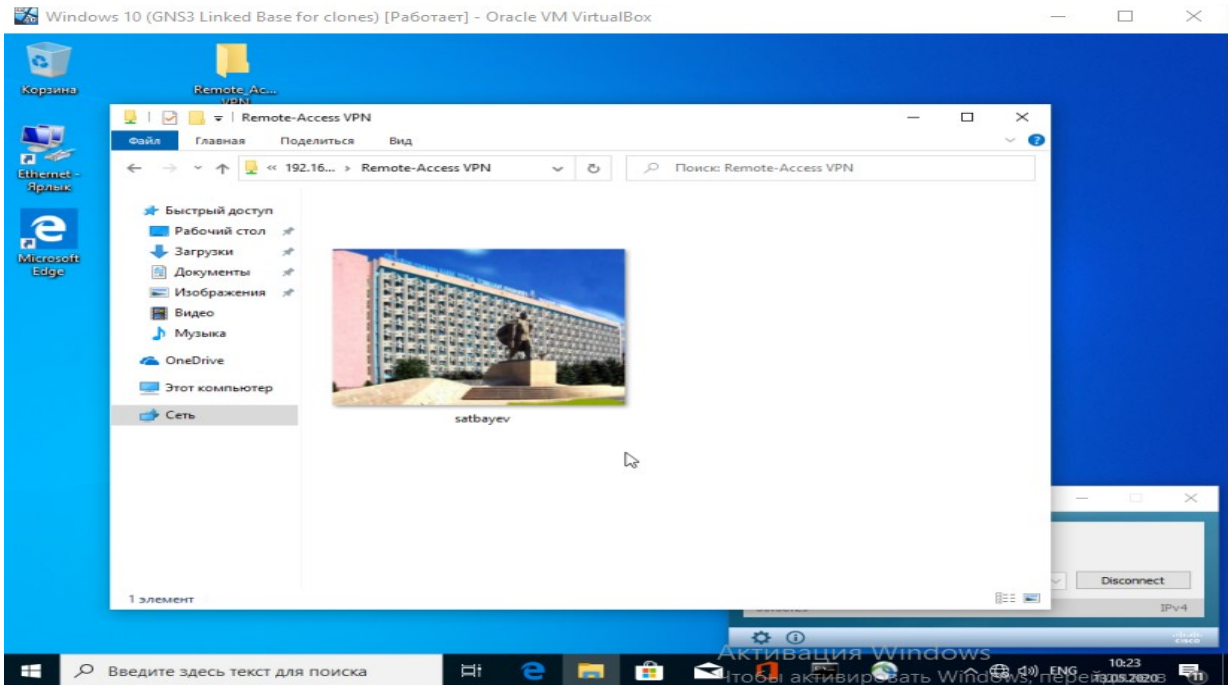
4.59-сурет – Қашықтағы пайдаланушы серверге қосылуы

Көріп отырғаныңыздай, қашықтағы пайдаланушыға керек деректер қол жетімді (4.60-суретті қараңыз).

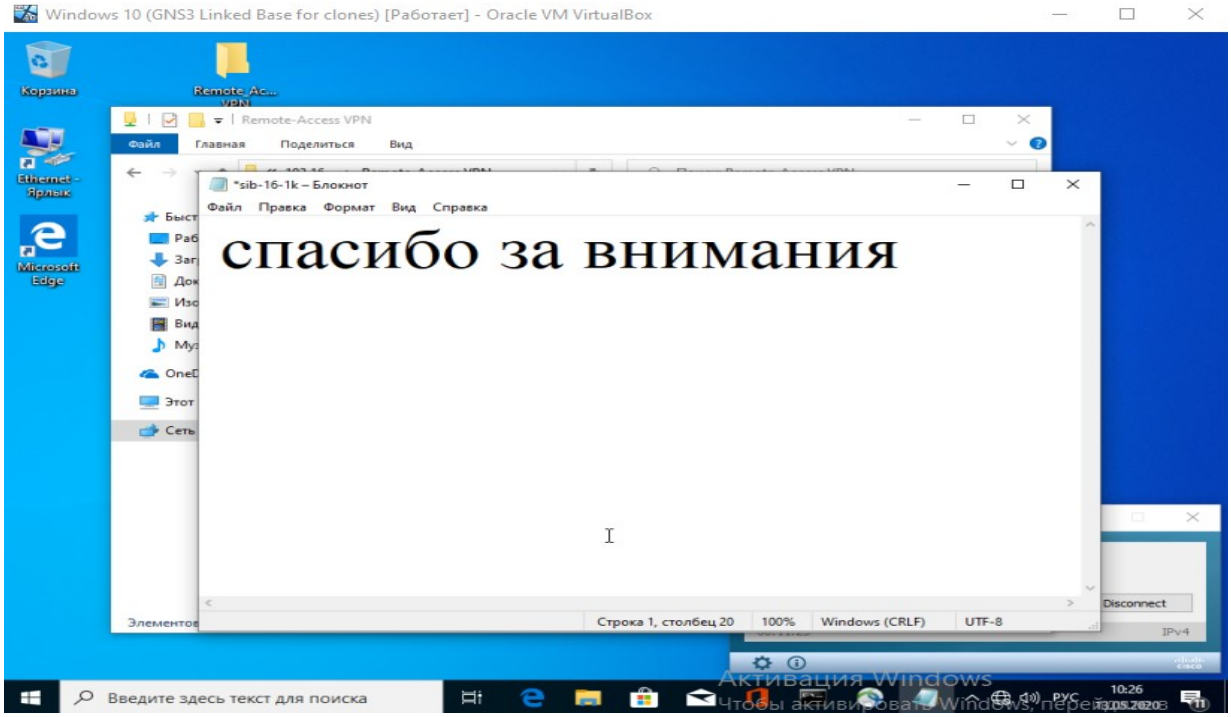


Сурет 4.60 – Қашықтағы пайдаланушы үшін қол жетімді қалталар

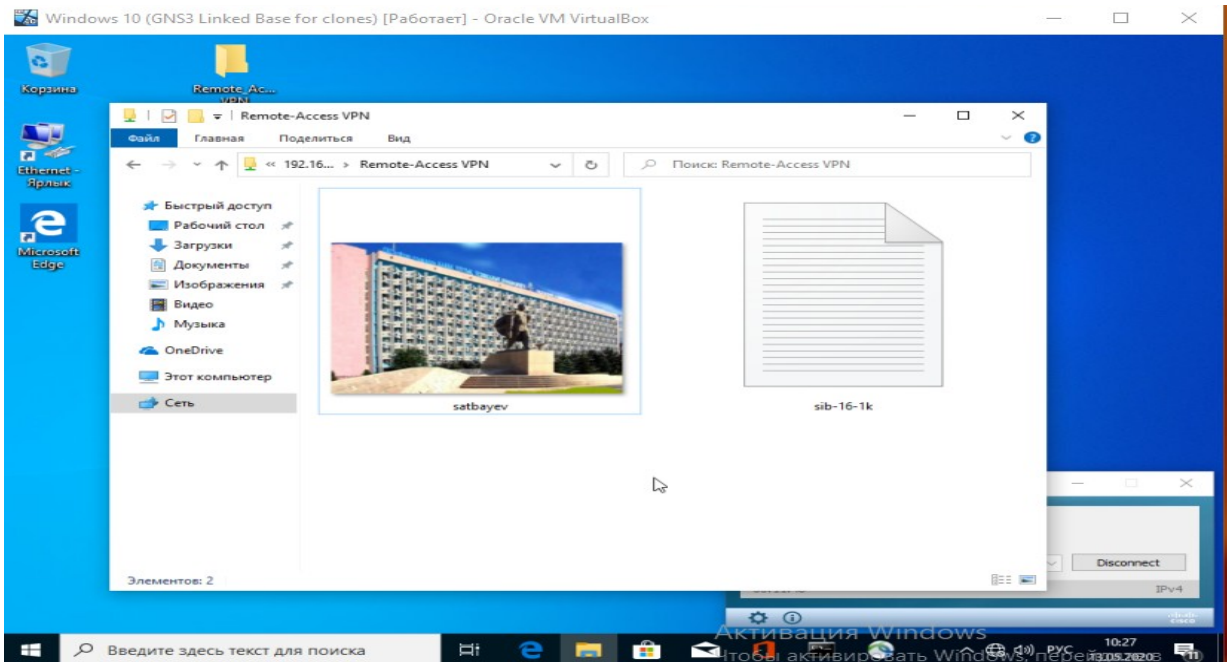
Қашықтағы қолданушы серверге толық қол жеткізді, қолданышу осы қалтаны оқып, өңдей алады, тексеру үшін мәтіндік құжатты қосып, оны сақтап , сақталған құжат серверде көрсетілетінін тексереміз (4.61-4.64 суретті қараңыз).



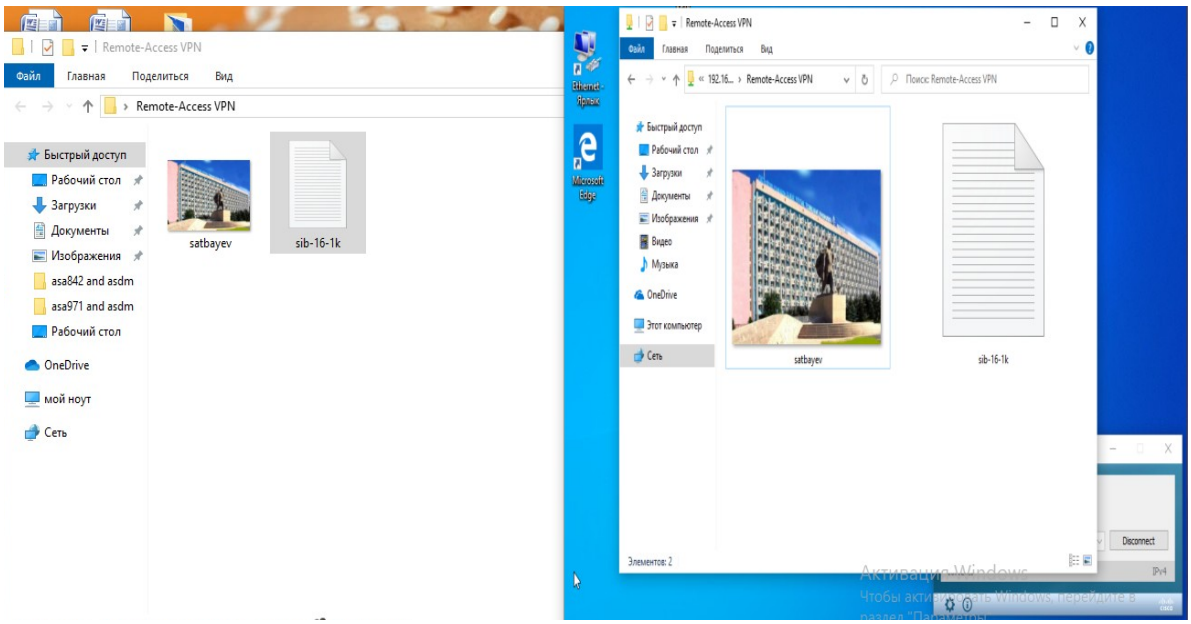
4.61 сурет – Қашықтағы пайдаланушы үшін қол жетімді қалта



4.62 сурет – «sib-16-1k»атауымен сынақ құжатын қосу



4.63 сурет – осы құжатты сақтау



4.64 сурет – Серверде тексеру

ҚОРЫТЫНДЫ

Осылайша, біздің офис пен қашықтан жұмыс істейтін қызметкер арасында қауіпсіз ақпарат беру ұйымдастырылды. Мұны VPN технологиясының көмегімен жасауға болады, ол қашықтағы қызметкер мен кеңсе арасындағы қауіпсіздік туннелін қамтамасыз етеді, қосылудың екі «нүктесін» түпнұсқалығын растайды, сондай-ақ жіберілген деректерді шифрлайды. VPN технологиясының арқасында берілетін ақпарат деректерді беру кезінде туындайтын негізгі қауіптерден, атап айтқанда ақпаратты ұрлау, өзгерту, жою, рұқсат етілмеген мәліметтерге қол жеткізу және берілетін ақпаратқа рұқсатсыз кіруден қорғады.

OpenVPN VPN қосылым протоколы ретінде пайдаланылды, өйткені ол қауіпсіздікті қамтамасыз етеді. VPN енгізу GNS3 бағдарламалық жасақтамасының көмегімен және брандмауэрде AnyConnect VPN қолдану арқылы жүзеге асырылды. Көптеген жылдар бойы Cisco AnyConnect тек орыс тіліне лайықтандырылып қоймай, сонымен қатар SSL және IPSec протоколдарының бірін қолдана отырып, корпоративті инфрақұрылымға қашықтан қол жетімділіктің көптеген функциялары мен мүмкіндіктерімен байытылды. Бұл жұмыста сертификатты пайдаланып қашықтағы пайдаланушыларды ішкі желіге қосу үшін OpenVPN ендіруді қолдану қауіпсіз екенін анықтадық. Сондықтан, бұл әдіс деректермен қауіпсіз алмасу үшін біздің корпоративтік желімізде қолданылды. Берілген тапсырманы дұрыс орындадық деп санауға болады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Петренко С.А. Курбатов В.А. Политики безопасности компании при работе в интернет: Руководство, 2011;
2. Кульгин М. Технологии корпоративных сетей: Энциклопедия. — СПб.: Питер, 2000;
3. Блинов А.М. Информационная безопасность часть 1: Учебное пособие - СПбГУЭФ, 2010;
4. Файльнер М. Виртуальные частные сети нового поколения LAN: Журнал сетевых решений. - М.: №11, 2005;
5. Тимофеев П. А. Романец Ю. В. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. — М:Радио и связь, 2002;
6. Александр Барсков. Говорим WAN, подразумеваем VPN: «Журнал сетевых решений/LAN», № 06, 2010;
7. Олифер Н. А. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. — СПб.: Питер, 2001;
8. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. — М.: КУДИЦ-ОБРАЗ, 2001;
9. В. С. Горбатов, О. Ю. Полянская. Основы технологии PKI, 2011;
10. Сафонова В.Г. Гумбург Б.Ю. IT: вчера, сегодня, завтра: Материалы IV научно-исследовательской конференции студентов и аспирантов Института водного транспорта: Перспективы развития протоколов виртуальной частной сети, их сравнение и анализ, Санкт-Петербург, 2016. - С. 250-254;
11. Dave Kosiur. Building & Managing Virtual Private Networks-Издательство**:**Wiley, 1998;
12. Snader J.C. VPNs Illustrated: Tunnels, VPNs, and IPsec, 2005;
13. Файльнер М. Виртуальные частные сети нового поколения LAN: Журнал сетевых решений, - М.: №11, 2005;
14. Лукацкий А. Неизвестная VPN, Компьютер Пресс.-М.: №10, 2001;
15. Норманн Р. Выбираем протокол VPN: Windows IT Pro. - М.: №7, 200;
16. Петренко С. Защищенная виртуальная частная сеть: Современный взгляд на защиту конфиденциальных данных. Мир Internet. - М.: №2, 2001;
17. Қауіпсіз желілерді құруға арналған VPN шешімдері // электрондық нұсқасы мына сайтында http://ypn.ru/342/vpn-solutions-for-secured-networking;
18. VPN-ның тунельдік протоколы // электрондық нұсқасы мына сайтында https://technet.microsoft.com/ru-ru/library/cc771298(v=ws.10).aspx;
19. OSI моделінің әртүрлі деңгейлеріндегі қорғаныс // электрондық нұсқасы мына сайтында http://www.cryptocom.ru/solutions/vpn.html.