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

Досаханов Даулет Нұрланұлы

«IP-желілерде мәліметтерді берудің қауіпсіз арнасын ұйымдастыру әдістері мен тәсілдерін талдау»

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: “ IP-желілерде мәліметтерді берудің қауіпсіз арнасын ұйымдастыру әдістері мен тәсілдерін талдау ”

Мамандығы 5В100200 - Ақпараттық қауіпсіздік жүйелері

Орындаған Досаханов Д.Н.

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 *Досахаов Даулет Нұрланұлы*
Тақырыбы: IP-желілерде мәліметтерді берудің қауіпсіз арнасын ұйымдастыру әдістері мен тәсілдерін талдау.
Университет Ректорының *" 27 " 01 № 762-б* бұйрығымен бекітілген
Аяқталған жұмысты тапсыру мерзімі *2020 жылғы " 15 " мамыр*
Дипломдық жұмыстың бастапқы берілістері: VPN проблемалық аймағы, VPN туннельдік протоколының әдістері, site-to-site vpn теңшеу, салыстыру және ұсыныстар.
Дипломдық жұмыста қарастырылатын мәселелер тізімі
a) Протоколдар мен site-to-site VPN-ның құру тәсілдерін зерттеу.
b) Әр түрлі туннель протоколдарын қолдану арқылы site-to-site VPN-ды конфигурациялау.
c) Site-to-site VPN-де деректерді беру кезінде жылдамдықты тексеру.
d) Деректер қауіпсіздігін талдау.
e) Site-to-site VPN әдісін таңдау үшін ұсыныстарды әзірлеу.
Сызба материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс): *VPN туннелдік протоколдары, site-to-site VPN корпоративтік желідегі топологиясы, салыстыру және рекомендация.*
Ұсынылатын негізгі әдебиет:12 атаудан

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: Досаханов Д.Н.

Название: IP-желілерде мәліметтерді берудің қауіпсіз арнасын ұйымдастыру әдістері мен тәсілдерін талдау

Координатор: Азамат Иманбаев

Коэффициент подобия 1:0,5

Коэффициент подобия 2:0

Замена букв:81

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 подразделения*

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: Досаханов Д.Н.

Название: IP-желілерде мәліметтерді берудің қауіпсіз арнасын ұйымдастыру әдістері мен тәсілдерін талдау

Координатор: Азамат Иманбаев

Коэффициент подобия 1:0,5

Коэффициент подобия 2:0

Замена букв:81

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

18 мая 2020г — Иманбаев А.Ж

Дата — *Подпись Научного руководителя*

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекші мен кеңесшілерге көрсету мерзімдері	Ескерту
Виртуалды жеке желі	12.04.2020 ж.	Жасалынды
VPN туннелдік протоколының әдістері	19.04.2020 ж.	Жасалынды
Симуляциялық ортаны таңдауу және site-to-site VPN теңшеу	26.04.2020 ж.	жасалынды
VPN салыстыру және ұсыныстар	15.04.2020 ж.	жасалынды

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	тех.ғыл, лектор Зиро А.	01.05.2020 ж.	

Ғылыми жетекші _____ Иманбаев А.Ж.

Тапсырманы орындауға алған білім алушы _____ Досаханов Д.Н.

Күні «27»_қаңтар_2020 ж.

АҢДАТПА

Бұл дипломдық жұмыс WAN арқылы хосттар site-to-site VPN қосылу кезінде, деректерді қауіпсіз арнасының тарату әдістері мен тәсілдерін зерттеуге арналған.

Түсініктеме А4 парағында жасалынған, 43 парақ, 7 кесте, 49 сурет және 12 пайдаланылған әдебиет көздерінен тұрады. Сонымен қатар кіріспеден, төрт тараудан және қорытындыдан тұрады.

Бірінші тарауда виртуалды жеке желі туралы жалпы ақпарат берілген. Екінші тарауда VPN туннельдеу протоколының әдістері сипатталған. Бұл тарауда сынып диаграммалары, сынып сипаттамалары және кейбір әдістер берілген. Үшінші тарау симуляциялық ортасын таңдауға және site-to-site VPN теңшеуге арналған. Төртінші тарауда VPN салыстыру мен ұсыныстар сипатталған. Қорытынды бөлімде, VPN туннельдік протоколдарының жақсы және жағымсыз жақтарына бірқатар тұжырымдар жасалды.

АННОТАЦИЯ

Данная дипломная работа посвящена исследованию анализа методов и подходов защищенного канала передачи данных в site-to-site VPN-соединения между хостами через WAN.

Пояснительная записка выполнена на листах А4, содержит 43 страниц, 7 таблицы, 49 рисунков и 12 источников использованной литературы. Также включает в себя введение, четыре главы и заключение.

В первой главе приводится общая информация о виртуальной частной сети. Во второй главе описываются методы протокола туннелирования VPN. В данной главе приведены диаграммы классов, описание классов и описание некоторых методов. Третья глава посвящена выбору среды симуляции и настройка site-to-site VPN. В четвертой главе описываются сравнения и рекомендации VPN. Сделаны ряд выводов, плюсы и минусы протоколов туннелирования VPN в заключительной части.

ANNOTATION

Диссертациялар WAN арқылы хосттар арасындағы VPN-сайттан сайтқа қосылу кезінде қауіпсіз деректер арнасының әдістері мен тәсілдерін талдауды зерттеуге арналған.

Түсініктеме А4 парағында жасалынған, 43 парақ, 7 кесте, 49 сурет және 12 пайдаланылған әдебиет көздерінен тұрады. Сонымен қатар кіріспеден, төрт тараудан және қорытындыдан тұрады.

Бірінші тарауда виртуалды жеке желі туралы жалпы ақпарат берілген. Екінші тарауда VPN туннель протоколының әдістері сипатталған. Бұл тарауда сынып диаграммалары, сынып сипаттамалары және кейбір әдістер берілген. Үшінші тарау модельдеу ортасын таңдауға және сайттан сайтқа VPN орнатуға арналған. Төртінші тарауда VPN салыстыру мен ұсыныстар сипатталған. Бірқатар тұжырымдар жасалды, VPN туннельдік хаттамаларының жақсы және жағымсыз жақтары қорытынды бөлімде.

МАЗМҰНЫ

КІРІСПЕ 9
1 Виртуалды жеке желі 10
1.1 VPN дегеніміз не? 10
1.2 VPN топологиясы 11
1.2.1 VPN түрлері 12
1.2.2 Виртуалды жеке желінің артықшылықтары: 16
1.3 VPN қауіпсіздігінің жалпы ақпараты 17
1.3.1 VPN деректер қауіпсіздігін қалай қамтамасыз етеді? 17
1.4 VPN-ге бағытталған негізгі талаптар 18
1.5 Өнімділік және экономикалық пайда 19
1.5.1. VPN компанияға келесі жолдармен пайдасын береді 20
1.6 Қызмет көрсету сапасы (QOS) 21
1.7 VPN болашағы 21
2 VPN туннелдік протоколының әдістері 24
2.1 IPSEC (IP Security Protocol) 24
2.1.1. Трафик қауіпсіздігінің қауіпсіздік протоколдары 24
2.1.2 Жұмыс режимдері 25
2.1.3 Кілттермен алмасу және басқару 25
2.2 PPTP (Point-to-Point Tunneling Protocol) 26
2.3 L2TP (Layer 2 Tunneling Protocol) 27
2.4 SSL / TLS (Transport Layer Security & Secure Sockets Layer) 28
3 Симуляциялық ортаны таңдау және site-to-site VPN теңшеу 30
3.1 Желілік эмуляторларды салыстыру 30
3.1.1 GNS3 30
3.1.2 Cisco Packet Tracer 31
3.1.3 Cisco VIRL 31
3.1 Желіні құру ортасын салыстыру нәтижелері 32
3.2 Корпоративтік желінің схемасының құрылуы 33
3.2.1 PPTP 34
3.2.2 L2TP / IPsec 35
3.2.3 IKEv2/IPsec 39
3.2.4 SSL VPN 42
4 VPN салыстыру және ұсыныстар 46
4.1 Орнату 46
4.2 Қауіпсіздік 46
4.2.1 PPTP 47
4.2.2 L2TP / IPsec 47

4.2.3 IKEv2 / IPsec 47
4.2.4 SSL / TLS 48
4.3 Жылдамдық 48
4.3.1 PPTP 48
4.3.2 L2TP / IPsec 48
4.3.3 IKEv2 / IPsec 49
4.3.4 SSL 49
4.4 Ұсыныс 49
ҚОРЫТЫНДЫ 50
ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ 51

КІРІСПЕ

Жұмыстың өзектілігі. Бүгінгі таңда, пандемия кезінде барлық адамдар VPN қызметтерін пайдаланады, ал қызметкерлер немесе іскери компаниялар сыртқы желілерден ішкі желілерге үнемі қол жеткізе алатын кезде қауіпсіздік басты факторға айналады.

Бұл жобаны шешуге қажетті мәселесі - хакерлерден қорғану және Wan арқылы site-to-site VPN қолданатын күні сенімді қорғаныс алу.

Зерттеу мақсаты. Бұл жобаның негізгі мақсаты WAN арқылы хосттар site-to-site VPN қосылу кезінде деректерді қауіпсіз арнасының таратудың әдістері мен тәсілдерін талдау, компанияларға бірнеше хосттарды қоғамдық желі арқылы құпия түрде қосуға көмектесу, осылайша WAN арқылы хосттар арасында қауіпсіз VPN қосылымын жасау.

Егер компанияда бір жеке желіде қосылғысы келетін бір немесе бірнеше филиал болса, олар VPN интранет құра алады. Бұл лизингтік қызмет көрсетумен салыстырғанда арзан шешім.

Бұл жұмыстың практикалық мақсаты - site-to-site VPN-ды WAN арқылы қалай қолдануға болатындығын талдау. VPN әр түрлі құрылғыларда жүзеге асырылуы мүмкін болғандықтан, біз әртүрлі конфигурациялармен, соның ішінде маршрутизаторлар арасындағы VPN-мен тәжірибе жасаймыз.

Зерттеу әдісі:

1) ПРОТОКОЛДАР мен site-to-site VPN-ның құру тәсілдерін зерттеу.

2) Әр түрлі туннель протоколдарын қолдану арқылы site-to-site VPN-ды конфигурациялау.

3) Site-to-site VPN-де деректерді беру кезінде жылдамдықты тексеру.

4) Деректер қауіпсіздігін талдау.

5) Site-to-site VPN әдісін таңдау үшін ұсыныстарды әзірлеу.

Зерттеу аймағы. Жоба WAN арқылы хосттар site-to-site VPN әдісімен қосылу кезінде әдістері мен тәсілдерін талдау, шифрлау, туннельдеу және жоғары сапалы күзет қызметін қоса, егжей-тегжей қарастырады. Жоба GNS3 бағдарламасын қолдана отырып әзірленеді. Бұл жобада біз қолданатын жабдық - бұл маршрутизатор, коммутатор, GNS3 компьютерлері және көмекші.

Жобаның құны. Бұл жобаның маңыздылығы бизнес-компаниялардың шығындарын азайту және ғаламдық желі арқылы қауіпсіз VPN-желіден «site-to-site» желісіне қол жеткізу және хакерлер шабуылына толықтай төзімді корпоративтік желіні құру болып табылады.

1 Виртуалды жеке желі

Шолу. Бұл тарауда біз виртуалды жеке желінің (VPN) не екенін, VPN технологияларын, VPN типтерін, VPN компоненттерін және VPN қауіпсіздігы туралы жалпы ойларын бағалаймыз. Содан кейін біз өнімділік пен үнемділік, қызмет көрсету сапасы (QOS) мен VPN болашағын талқылаймыз.

1.1 VPN дегеніміз не?

VPN - бұл жалпыға ортақ желі инфрақұрылымы арқылы қауіпсіз қосылысты құру құралы. VPN ақпараттың құпиялылығы қамтамасыз ету үшін шифрлауды және аутентификацияны қолданады. Бұл деректердің тұтастығы туралы алаңдамай, көптеген орындар арасында деректер мен ресурстарды алмасуға болатындығын білдіреді. Жалғыз, деректерді беру үшін жалпыға қол жетімді желіні пайдалану VPN технологиясының артықшылығы болып табылады.

VPN мақсаты - қауіпсіз емес Ғаламтор арқылы пайдаланушы деректеріне кіру қауіпсіздігін беру. Бұл компанияларға Ғаламторды корпоративті желілер үшін виртуалды тірек ретінде пайдалануға мүмкіндік береді, бұл оларға корпоративті кеңсе мен филиал немесе Ғаламтор арқылы қашықтағы кеңселер арасында қауіпсіз виртуалды байланыс құруға мүмкіндік береді. VPN-нің экономикалық пайдасы корпорацияларға жеке WAN желілерінен Ғаламторға негізделген VPN-ге көбірек деректерді тасымалдауға себеп болды.

Бұрын VPN термині жалпыға қол жетімді телефон желісі (PSTN) сияқты қашықтан қосылу қызметтерімен байланысты болды, бірақ VPN ақыры IP негізіндегі деректер желісімен байланыса бастады. Бұрын IP негізіндегі желілік ұйымдар көп уақытты және ресурстарды көп жұмсады, қазіргі кезде Интранет деп аталатын күрделі жеке желілерді құру. Бұл желілер қашықтықтан пайдаланушыларды қостыру үшін қымбат жалдамалы желі, Frame Relay және ATM көмегімен орнатылды. Шағын сайттар мен қашықтағы мобильді жұмысшылар үшін компаниялар өз желілеріне қашықтан қол жеткізу серверлерімен немесе ISDN-мен толықтырды.

Жалға алынған желілерге қол жеткізе алмаған шағын және орта компаниялар төмен жылдамдықтағы коммутация қызметін пайдаланды. Ғаламтор қол жетімді болып, өткізу қабілеті өскен сайын компаниялар өздерінің интранеттерін желіге орналастыра бастады және ішкі және сыртқы пайдаланушыларды қосу үшін экстранет деп аталатын элементтерді құра бастады. Алайда, Ғаламторды қаншалықты үнемді және тез қолдануға болатындығына қарамастан, маңызды мәселелердің бірі - қауіпсіздік.

Заманауи VPN шешімдері арнайы туннель протоколдары мен шифрлаудың күрделі процедураларын қолдану арқылы қауіпсіздік факторын жеңеді, мәліметтердің тұтастығы мен құпиялылығына қол жеткізіледі, ал жаңа қосылым арнайы нүкте-нүкте байланысы сияқты көрінетін жағдай жасайды. Бұл

операциялар жалпыға ортақ желіде орындалатындықтан, VPN-ды енгізу, жеке немесе жалға алынған қызметтерге қарағанда едәуір арзан болуы мүмкін. Ертерек VPN-ді қолдану үлкен тәжірибені қажет етсе де, технология кез-келген деңгейдегі компаниялар үшін қарапайым және қол жетімді шешім болатын деңгейге жетті.

Виртуалды. Виртуалды сөзі шынайы емес немесе басқа күйде болу мағынасын білдіреді. VPN-де екі немесе одан да көп құрылғылар арасындағы жеке байланыс жалпы Ғаламтор арқылы қол жеткізіледі. Сондықтан байланыс практикалық болып табылады, бірақ физикалық емес.

Жеке. Жеке дегеніміз - көпшіліктен бір нәрсе жасырын ұстау. Екі құрылғы бір-бірімен қоғамдық ортада байланыс орнатса да, бұл байланысты үзетін немесе олар кез келген деректерімен алмасқанда, деректерді ұрлайтын үшінші жағы жоқ.

Желі. Желі екі немесе одан да көп құрылғылардан тұрады, олар кабельдер мен сымдар арқылы бір-бірімен еркін және электронды байланыс жасай алады. VPN - бұл желі. Ол ұзақ қашықтыққа ақпаратты тиімді және нәтижелі жеткізе алады.

Қарапайым сөзбен айтқанда, VPN, виртуалды жеке желі, жалпыға ортақ желі жолдарын пайдаланатын, бірақ жеке желілердің қауіпсіздігі мен қорғалуын қолдайтын желі ретінде айтылады.

1.2 VPN топологиясы

Келесіде, біз VPN қалай жұмыс істейтінін қарастырамыз:

VPN қолдана бастау үшін сізге Ғаламтор қосылымы қажет; Ғаламтор байланысы Ғаламтор-провайдерден жалға алынады және үй пайдаланушылары үшін телефон байланысы арқылы қосылудан бизнес үшін жылдам қосылыстарға дейін қосуға болады. Содан кейін, арнайы жасалынған маршрутизатор немесе коммутатор Ғаламторға кірудің әр тізбегін VPN желісіне қосылу үшін бір-бірімен қосылады.

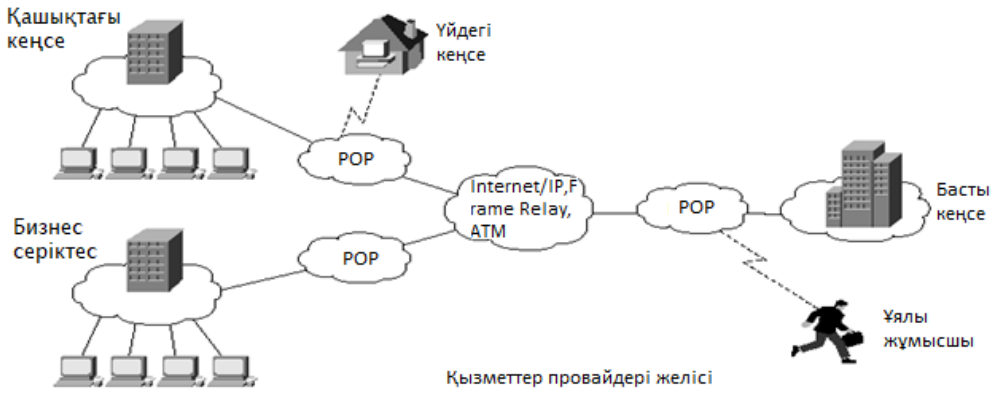
VPN құрылғылары Ғаламтортағі негізгі бағыттау және коммутация инфрақұрылымын жасыратын IP пакеттерінде жіберушілерге мәліметтерін инкапсулялауға мүмкіндік беретін туннельдер арқылы PVC (тұрақты виртуалды тізбек - жалға алынған сызыққа ұқсас виртуалды схема) жасайды. жіберушілер мен алушылардан.

Жіберетін құрылғыдағы VPN құрылғысы шығыс пакетті немесе жақтауды қабылдайды және оны VPN туннелі бойынша Ғаламтор арқылы қабылдаушы жаққа өту үшін инкапсуляциялайды. VPN көмегімен пакетті жылжыту процесі пайдаланушылар үшін де, Ғаламтор-провайдерлер үшін де, жалпы Ғаламтор үшін де ашық. Пакет қабылдау аяғына жеткенде, басқа құрылғы VPN жақтауын алып тастап, түпнұсқалық пакетті тағайындалған желіге жеткізеді.

VPNдер OSI моделінің 2 деңгейінде немесе 3 деңгейінде жұмыс істейді (ашық жүйенің өзара байланысы). 2-қабат VPN Ethernet сияқты 2-қабатты

жақтауды қолданады, ал 3-қабатта IP сияқты 3-қабатты пакеттер қолданылады. Layer 3 VPN 3-ші қабаттан басталады, онда кіріс Layer 2 жақтауын түсіріп, тағайындалған жерге жаңа Layer 2 жақтауын жасайды. Layer 2 VPN құру үшін Ғаламтор арқылы ең көп қолданылатын екі протоколдар: Layer 2 Tunneling Protocol (L2TP) және Point-to-Point Tunneling Protocol (PPTP).

Жақында жасалған көп протоколды жапсырмаларды ауыстыру (MPLS) деп аталатын протокол тек Layer 3 VPN-де қолданылады (1 -суретті қараңыз)



1.2-сурет: Анықталған VPN

1.2.1 VPN түрлері

Қазіргі уақытта VPN үш түрі бар:

- VPN қашықтықтан қол жетімділік (RA).
- VPN сайттан сайтқа (site-to-site).
- Динамикалық көп нүктелі VPN (DM).

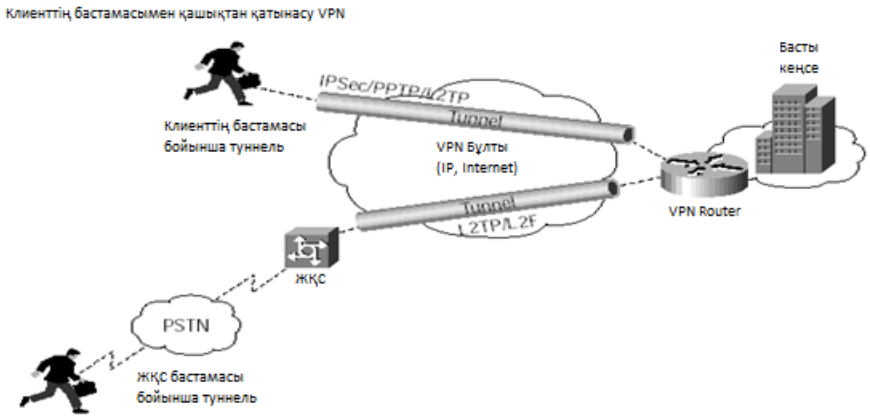
Қашықтан қол жеткізу. Қашықтан қол жетімділік VPN үйден немесе саяхаттаушыларға қашықтан орналасқан орталық LAN-ға қол жеткізуді қажет ететіндерге арналған. Олар провайдердің нөмірін теріп, Ғаламтор арқылы жергілікті желіге қосылады. Бұл орталық жергілікті желідегі VPN шлюзі арасындағы VPN трафикті шифрлайтын және шешетін қашықтағы пайдаланушының ноутбукіне немесе дербес компьютеріне клиенттік бағдарламаны орнату арқылы мүмкін болды.

Қашықтан қол жетімділік VPN ұялы пайдаланушыларға Ғаламтор-провайдер ұсынған инфрақұрылымды пайдаланып, ұйымның серверіне қосылуға мүмкіндік береді. Қашықтан қол жеткізу VPN пайдаланушыларға корпоративті интранеттерге немесе экстранеттерге кез келген жерде және кез келген уақытта қосылуға мүмкіндік береді. Пайдаланушылар ұйым желісіндегі барлық ресурстарға, ұйымда болған сияқты қол жеткізе алады. Пайдаланушы кәдімгі ескі телефон қызметтерін (POTS), интеграцияланған қызметтері (ISDN) бар сандық желі, сандық абоненттік желі (DSL) және т.б. қолдана отырып, VPN қолдайтын жергілікті Ғаламтор-провайдермен байланысады. Ғаламтор-провайдердегі VPN құрылғысы пайдаланушының логинін қабылдайды. содан

кейін ұйымның кеңсесінде VPN құрылғысына туннель орнатып, пакеттерді Ғаламтор арқылы жіберуді бастайды.

Қашықтан қол жетімділік VPN келесі артықшылықтарды ұсынады:

- Модем мен терминал серверінің жабдықталуына байланысты шығындардың азаюы.
- Үлкен ауқымдылығы және жаңа пайдаланушыларды қосудың қарапайымдылығы.
- Халықаралық телефон қоңырауларының құнын арзандату үшін 800-ге дейін ұлттық телефон нөмірі ұйымның модемдеріне қосылу қажет емес.



Сурет 1.3 Қашықтан қол жетімді VPN-мен

Site-to-site VPN. Желілік VPN желілері ұйымның (немесе ұйымдардың) географиялық бөлінген сайттары (мысалы, бас кеңсе мен филиалдар) арасында байланыс орнатуға мүмкіндік береді. Site-to-site VPN-ның екі түрі бар:

VPN Интранет. Бір ұйымның сайттары арасында қосылуға рұқсат беріңіз. Интранеттер ұйымның орналасқан жерін байланыстырады. Бұл орындар бас кеңселерден филиалдарға дейін, қашықтағы қызметкердің үйіне дейін. Көбінесе бұл қосылым электрондық пошталарға, бағдарламалар мен файлдарды бөлісуге қолданылады. Frame Relay, ATM және MPLS бұл тапсырмаларды орындағанымен, әрбір кемшіліктер қосылысты шектейді.

Үй пайдаланушыларын қосудың құны Ғаламторға қосылу технологияларына, мысалы, DSL немесе кабельге қарағанда өте жоғары. Осыған байланысты, ұйымдар өз желілерін Ғаламторке жылжытады, бұл арзан және оларды құру үшін IPSEC қолданады.

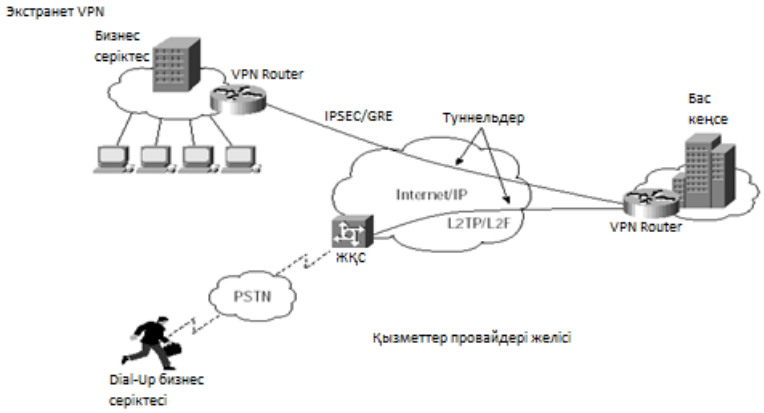
VPN интранетінің артықшылықтары мыналарды қамтиды:

- WAN өткізу қабілеттілігінің төмендеуі, WAN өткізу қабілетін тиімді пайдалану.
- Икемді топологиялар.
- Өткізу қабілеттілігін бақылауды қолдана отырып, кептелістің алдын алу.

VPN Extranet. Іскери компаниялар немесе бизнес сияқты ұйымдар мен оның клиенттері арасында байланыс орнатуға мүмкіндік беріңіз. Экстранеттер - бұл екі немесе одан да көп ұйымдар арасындағы қауіпсіз байланыс. Экстранеттің жалпы қолданысына жеткізу тізбегін басқару, серіктестік және жазылым

қызметтері кіреді. Қосылу құны, кідірістер және қол жетімділікке байланысты бұл кәсіпорындарға бұрынғы технологияларды қолдану қиын болуы мүмкін.

IPSEC негізіндегі VPN желілері экстранетке қосылуға өте ыңғайлы. IPSEC-пен жұмыс істейтін құрылғылар Ғаламтор желісіне тез және арзан орнатылуы мүмкін.

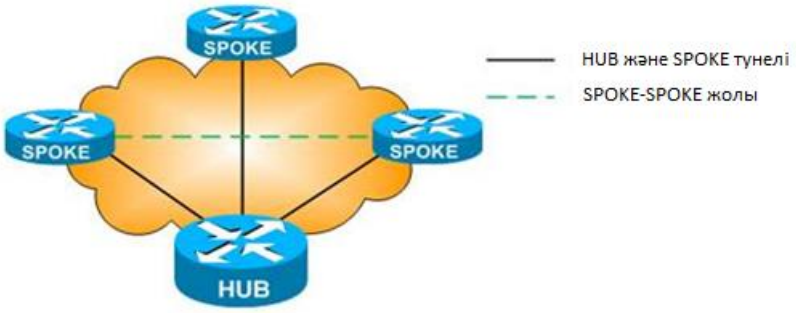


Сурет 1.4 VPN Extranet

Динамикалық көп нүктелі виртуалды жеке желі. Динамикалық көп нүктелі виртуалды жеке желі (DMVPN) - бұл виртуалды жеке желі (VPN) ұйымының сервері немесе маршрутизаторы арқылы трафикті өткізбестен сайттар арасында мәліметтер алмасатын қауіпсіз желі.

VPN әдеттегідей әр қашықтағы сайтты бас кеңсеге қосады; DMVPN негізінен VPN тор топологиясын жасайды. Бұл дегеніміз, әр сайт (сөйлеген) қай жерде орналасқанына қарамастан, барлық басқа сайттармен тікелей байланыса алады.

DMVPN қызметі VPN маршрутизаторлары мен брандмауэр хабтарында жұмыс істейді. Әр қашықтағы сайтта қол жетімді ресурстарға қол жетімділікті қамтамасыз ететін компанияның бас кеңсесінің VPN құрылғысына (концентраторына) қосылу үшін теңшелген маршрутизатор бар. Бір-бірімен мәлімет алмасу үшін екі сәуле қажет болғанда - мысалы, VoIP телефон қоңырауы үшін - пучка хабпен байланысады, екінші жағы туралы қажетті ақпаратты алады және тікелей олардың арасында динамикалық IPSEC VPN туннелін жасайды.



1.5-сурет. Динамикалық көп нүктелі VPN желілік диаграммасы

Бір-бірден тікелей орналастыру дәстүрлі VPN-ге қарағанда бірнеше артықшылықтарды ұсынады:

- Қашықтағы тораптар арасындағы трафик хабтан өтпеуі керек (VPN негізгі маршрутизаторы).
- DMVPN орналастыру хабтың өткізу қабілеттілігінің қосымша талаптарын болдырмайды.
- DMVPN желінің қосымша кідірістерін болдырмайды.
- DMVPN желілері WAN өткізу қабілетін сақтайды.
- Олар VPN схемаларының құнын төмендетеді.

DMVPN қондырғыларына әкімшілік жүктемені азайтуға және сайттар арасындағы сенімді динамикалық байланысты қамтамасыз етуге арналған IPSEC шифрлауды бағыттайтын GRE туннелі және Next Hop Resolution Protocol (NHRP) сияқты механизмдер кіреді. Әрбір компанияның артықшылығы - DMVPN мүмкіндігін пайдалану, ғаламдық желі шығындарын азайтуға және өткізу қабілеті мен сенімділікті арттыруға көмектеседі.

Multiprotocol Label Switching (MPLS) затбелгі алмасу құрылымын қолданады. Бұл гибридтік архитектура, бұл желілік қабатты бағыттауды және пакеттік коммутация құрылымдарын, сонымен қатар сілтеме қабаттарының схемалары мен ағынды коммутацияны қолдануды біріктіруге тырысады. MPLS маршрутизаторлар арасындағы көліктік инфрақұрылымды жасау арқылы жұмыс істейді, сонымен қатар ол байланысқан қабат пен қабат 2-де әртүрлі коммутация орталарын ауыстыру үшін тең-теңімен VPN моделі ретінде жұмыс істей алады, пакеттер MPLS-ке кірген кезде оған жергілікті этикетка және шығыс интерфейс туралы шешімге негізделген. жергілікті экспедиция.

Бағыттау туралы шешім кіріс белгіге негізделген, онда келесі интерфейс пен келесі ауысудың белгісі анықталады. MPLS іздеу пакетін әр пакетке арналған соңғы жолды құру үшін пайдаланады.

Пакеттік аутентификация рұқсаты жоқ пайдаланушыларға деректерді көруге, ұстамауға немесе өзгертуге жол бермейді. Пакеттік аутентификация оның тұтастығын қамтамасыз ету үшін тақырып пакетіне IP пакетіне қолданылады. Қабылдаушы тарап пакетті қабылдаған кезде тиісті буманың тақырыбын тексеріп, пакетте қандай да бір қателіктер бар-жоғын тексеруі керек.

Пайдаланушының аутентификациясы авторланған және рұқсат етілмеген пайдаланушыларды анықтау үшін қолданылады. Кәсіпорын желісінен ресурстарға қол жеткізуге тырысатын пайдаланушылардың жеке басын растау қажет. Пайдаланушының аутентификациясы қол жетімділік деңгейлерін де анықтайды; пайдаланушылар деректерді алады немесе қарайды және кәсіпорынның ресурстарының белгілі бір аймақтарына рұқсат береді.

2. Кіруді анықтайтын брандмауэрлар. Брандмауэрлар желілік трафиктің параметрлерін бақылайды және кәсіпорындарды рұқсатсыз кіруден қорғайды. Ұйым мен Ғаламтор арасындағы әрбір желі қосылымында брандмауэр бар желіні жобалауы керек. Желіаралық қалқанның жиі қолданылатын екі түрі пакеттік деңгейдегі брандмауэр және қолданылу деңгейіндегі брандмауэр.

Пакеттік деңгейдегі брандмауэр желі арқылы өтуге тырысатын әр пакеттің бастапқы және тағайындалған мекен-жайларын тексереді. Пакеттік деңгейдегі брандмауэр пайдаланушыға ұйымның желісіне кіруге және одан шығуға мүмкіндік береді, егер пайдаланушының тиісті көзі мен тағайындалған мекен-жайы бар қолайлы пакеті болса ғана. Пакет TCP порт идентификаторы және IP мекенжайы арқылы жеке тексеріледі, осылайша пакеттің қайда бара жатқанын біледі. Пакеттік деңгейдегі брандмауэрдің кемшілігі - пакеттің мазмұнын немесе оның берілу себептерін тексермеуі және өшірілмеген ресурстар барлық қолданушылар үшін қол жетімді.

Бағдарлама деңгейіндегі брандмауэр ұйым желісі мен Ғаламтор арасындағы басты компьютер ретінде әрекет етеді. Ұйымның желісіне қол жеткізгісі келетін пайдаланушылар алдымен бағдарлама деңгейіндегі брандмауэрге кіріп, өздері уәкілеттік берілген ақпаратқа қол жеткізуге рұқсат беруі керек. Брандмауэрді қолданба деңгейінде қолданудың артықшылықтары: пайдаланушылардың кіру деңгейі мен ресурстарды авторизациялау деңгейін бақылау. Тек рұқсат етілген ресурстар қол жетімді. Керісінше, Ғаламтор арқылы кіру кезінде пайдаланушы қосымша парольдер жиынтығын есте сақтауға мәжбүр болады.

3. Менеджмент. Менеджмент - қауіпсіздік саясатын басқару, қол жеткізуге рұқсаттар және VPN трафигін басқару компанияны басқаруға икемді болуы керек, кейбір компаниялар VPN-дің барлық орналастырылуы мен күнделікті жұмысын басқаруды жөн көреді, ал басқалары оны үшінші тараптың провайдерлеріне беруді жөн көреді. Келесі бөлімде біз кәсіпорындардың өнімді VPN-ден қалай пайда таба алатындығын, сондай-ақ VPN-ді іске асыру құны тұрғысынан қарастырамыз.

1.2.2 Виртуалды жеке желінің артықшылықтары:

- VPN барлық алынған дерек пакеттерін олардың сенімді көзден алынғанын тексеріп, аутентификациялайды. Шифрлау деректердің құпия болуын қамтамасыз етеді.
- Көптеген VPN Ғаламтор арқылы қосылады, сондықтан шалғайдағы пайдаланушы орталық LANдан өте үлкен қашықтықта болса да, қоңыраулардың құны аз болады.
- Орталық жерде бірнеше телефон желілері мен модем банктері қажет емес.
- Жалпы телекоммуникациялық инфрақұрылымды қысқарту, өйткені Ғаламтор-провайдер желінің көп бөлігін қамтамасыз етеді.
- басқару, техникалық қызмет көрсету және техникалық қолдау шығындарының қысқаруы.
- Модемдік пулдарды және жеке желілік инфрақұрылымды жою арқылы желілік топологияны жеңілдетеді.
- VPN функционалдығы кейбір АТ жабдықтарында бар.

- VPN қол жетімді өткізу қабілеттілігін арттыру және клиенттің қосымша бағдарламалық жасақтамасын лицензиялау арқылы оңай кеңейтіледі.

1.3 VPN қауіпсіздігінің жалпы ақпараты

Төменде VPN қолдану үшін жалпы қауіпсіздік ұсыныстары берілген:

1. VPN қосылымдарын брандмауэрді қолдану арқылы жақсартуға болады.
2. Шабуылдарды тиімді бақылау үшін IDS / IPS (басып кіруді анықтау / алдын-алу жүйесі) қолдану ұсынылады.
3. Қандай да бір вирустың / құрттың таралуын болдырмау үшін қашықтағы клиенттер мен желілік серверлерде антивирустық бағдарламалық қамтамасыздандыру орнатылуы керек.
4. Қарапайым немесе аутентификациясы жоқ қамтамасыз етілмеген немесе басқарылмайтын жүйелерге ішкі желіге VPN қосылыстарын орнатуға рұқсат етілмейді.
5. Тіркеу және аудит функциялары желілік қосылыстарды, әсіресе кез-келген рұқсатсыз кіру әрекеттерін тіркеу үшін қамтамасыз етілуі керек. Журналды үнемі қарау керек.
6. Оқыту желілік / қауіпсіздік әкімшілері мен қолдау персоналына, сондай-ақ алыстағы пайдаланушыларға ұсынылуы керек.
7. VPN-ді енгізу және оны пайдалану кезінде озық тәжірибелер мен қауіпсіздік саясатының сақталуын қамтамасыз ету.
8. VPN және желілік қолдауды дұрыс пайдалану бойынша қауіпсіздік саясаттары мен нұсқаулықтары VPN пайдалануды бақылау және басқару үшін жауапты тараптарға қол жетімді болуы керек.
9. Ішкі желіні қорғау үшін VPN кіру нүктесін периметрлік желіге (DMZ) қою ұсынылады.
10. VPN қосылымы кезінде Ғаламторға немесе кез-келген басқа қауіпті желіге бір уақытта қол жеткізу үшін бөлек туннельді қолданбау ұсынылады. Егер бөлінген туннель қолданылса, қауіпті желілердің ықтимал шабуылдарының алдын алу үшін брандмауэр мен IDS пайдаланылуы керек.

1.3.1 VPN деректер қауіпсіздігін қалай қамтамасыз етеді?

TCP / IP қауіпсіздікті қамтамасыз ету үшін жасалмаған, сондықтан VPN желілері қосылыстың әр түрі үшін ең жақсы қауіпсіздік шешімін ұсыну үшін IP протоколдары мен жүйелерінің үйлесімін пайдаланады. Кейбір протоколдар деректер пакеттерін шифрлайды, ал басқа протоколдар пакетті беру кезінде қорғайды. Мұнда VPN деректердің қауіпсіздігін қамтамасыз ету үшін пайдаланатын ең танымал протоколдар мен жүйелер:

PPTP (Point-to-Point Tunneling Protocol) қосылыстар үшін виртуалды туннель жасайды, L2TP (Layer 2 Tunneling Protocol) және L2F (Layer 2 Forwarding) бірге VPN-ге қашықтан қол жеткізу үшін қолданылады.

1) IPSEC (Internet Security Protocol) тіркелген VPN шешімдері үшін жиі қолданылатын қауіпсіздік опциясына айналады. Әрбір деректер пакеті шифрланған және түпнұсқалығын растайтын мөрге ие, оның шыққан жерін растайды. Бұл IPSEC-ті өте қауіпсіз нұсқаға айналдырады. IPSEC екі жолмен жұмыс істейді:

- Тасымалдау режимінде пакеттің пайдалы жүктемесінің бір бөлігі ғана шифрланған. (Пайдалы жүктеме нақты мәліметтерден тұрады.)

- «Туннель режимінде» бүкіл пакет, оның ішінде тақырып, шифрланған. (Тақырыпта бастапқы және тағайындалған IP мекен-жайы болады.)

2) Хакерлер алушыға пакеттерді олар тағайындалған жерге жетпестен бұрын ұстау және өзгерту арқылы алдау үшін тырысып емес, пакеттерді жіберушінің шынайы екендігін растайтын аутентификация жүйесі.

3) PKE (ашық кілттерді шифрлау) PKE-ны VPN-мен қолдануға болады. Шифрлау кодтарын қолмен енгізудің орнына, Ғаламтор арқылы кілттермен алмасу (IKE) үлкен желілерде пайдалы болатын кілттерді автоматты түрде алмастыруға мүмкіндік береді. Берілу кезінде деректерді қорғаудың көптеген әдістері бар. Көптеген VPN шешімдері деректердің қауіпсіздігін қамтамасыз ету үшін шифрлауды немесе аутентификацияны қолданады. Қауіпсіздік жоғарылаған сайын әр пакетті өңдеуге және жинауға қажет уақыт артады.

Ғаламторды қарау кезінде әдеттегі VPN шифрлау 20 пайызды құрайды; VPN арқылы жұмыс істейтін басқа қолданушылар қосымша шығындарды едәуір арттыра алады. Бұл мәселені шешу үшін кейбір VPN жүйелері желінің жұмысын жақсарту үшін деректерді жібермес бұрын қысады.

1.4 VPN-ге бағытталған негізгі талаптар

Әдетте, қашықтағы желі үшін шешім қолдану кезінде кәсіпорын корпоративтік ресурстар мен ақпаратқа басқарылатын қол жетімділікті қамтамасыз етуі керек. Шешім роумингке немесе қашықтағы клиенттерге жергілікті желі ресурстарына қосылуға мүмкіндік беруі керек, ал шешім қашықтағы кеңселерге ресурстар мен ақпарат алмасу үшін бір-бірімен байланысуға мүмкіндік беруі керек (маршрутизаторлар арасындағы байланыс). Сонымен қатар, шешім Ғаламтор арқылы өтетін кезде құпиялылық пен тұтастықты қамтамасыз етуі керек.

- **Кеңейту мүмкіндігі**: сіздің бизнесіңіздің өсуіне байланысты шешіміңізді кеңейтуге және жүк көтергіштерін жаңарту қажеттілігін болдырмауға мүмкіндік береді.

- **Өнімділік**: VPN деректерді кіріс желісінің жылдамдығына немесе ең баяу сызықтың жылдамдығына жақын өңдеуі керек.

- **Сенімділік**: VPN кез-келген уақытта қол жетімді болуы керек, сенімділік қызмет көрсетудің шектеулі үзілісімен істен шыққан құрылғыларды автоматты түрде қалпына келтіретін резервтік функцияларды қамтуы керек.

- **Пайдаланудың қарапайымдылығы**: VPN қолдану өте оңай және соңғы пайдаланушыларға түсінікті болуы керек.

- **Басқарудың қарапайымдылығы**: Басқару платформасында қауіпсіздік саясатын әзірлеудің қарапайым тәсілі, осы саясатты таратудың қарапайым тәсілі және көптеген құрылғыларды бір уақытта басқарудың оңай жолы болуы керек.

- **Үйлесімділік**: VPN жабдығы салалық стандарттар мен хаттамаларға сәйкес болуы керек.

- **Протоколдық қолдау**: Кем дегенде келесі хаттамаларға қолдау көрсетілуі керек. IPSEC, PPTP, L2TP және RADIUS.

- **Қызмет деңгейінің келісімі** (**SLA**): байланыстырылған орындар үшін тұрақты өткізу қабілеттілігін және қызмет көрсетуді қамтамасыз ету үшін қызмет провайдеріңізбен келісіңіз.

- **Толық интеграция**: VPN шешімі қосымша қызмет ретінде ұйымның желілік жүйесіне біріктірілуі керек. Пайдаланушы аутентификациясында талап пайдаланушыны анықтау болып табылады. Мекенжайды басқару клиенттің компьютерлік мекен-жайларын құпия сақтау үшін қолданылады.

Деректерді сығымдау көбінесе үлкен көлемдегі мәліметтер үшін қолданылады. Деректерді шифрлауды басқару деректерді қауіпсіз алмасу үшін қолданылады. Кілттерді басқару шифрлау және шифрлау үшін пайдаланылатын кілтті тиімді басқарады. Пайдаланушының аутентификациясының бөлігі ретінде EAP пайдаланушының жеке басын куәландыру үшін қолданылады.

1.5 Өнімділік және экономикалық пайда

Өнімділік тұрғысынан, VPN ұзақ жолға түсті. Бұрын қауіпсіздік пен басқару мәселелері ұтқырлықтың артықшылықтарын жасырған. Шағын ұйымдар жолда жұмыс істейтін қызметкерлерге ақпараттық қолдау көрсетуге байланысты қосымша уақыт пен шығындарды ескеруі керек. Ірі компаниялар, мобильді жұмысшыларды желіге қашықтан қол жетімділікпен қамтамасыз ету, хакерлерге кездейсоқ корпоративтік ақпараттық ресурстарға қол жеткізуге мүмкіндік беретіндігіне алаңдаулы.

Бірақ жеке цифрлық көмекшілер (ұялы телефондар) және ұялы телефондар сияқты соңғы қолданушы технологиялар қызметкерлер үшін ұтқырлықты тартымды еткендіктен, алдыңғы бөлімде көргеніміздей, желілік технологиядағы технологиялық жетістіктер IT мәселелерін шешуге көмектесті. Технологияның осы жетістіктерімен өнімділік жақсарады. VPN компаниялары барған сайын маңызды бола түсуде, өйткені компанияларға мобильді қызметкерлер корпоративті жергілікті желіге қосыла алатындай жалпыға қол жетімді Ғаламтор арқылы үнемді, уақытша, қауіпсіз байланыс арналарын құруға мүмкіндік береді.

1.5.1. VPN компанияға келесі жолдармен пайдасын береді

- Географиялық қосылысты кеңейтеді - VPN қашықтағы қызметкерлерді орталық ресурстармен байланыстырады, бұл жаһандық операцияларды конфигурациялауды жеңілдетеді.

- Ғаламтор қауіпсіздігін жақсартады - кең жолақты Ғаламтор қосылымы желіні хакерлік шабуылдардан осал етеді. Көптеген VPN шешімдеріне желінің қауіпсіздігінің түрлі қауіптеріне қарсы тұру үшін қорғаныс және антивирустық қарап шығу сияқты қосымша қауіпсіздік шаралары кіреді.

- Масштабтау оңай - VPN компанияларға Ғаламтор-провайдерлердің ішінен қашықтан қатынау инфрақұрылымын пайдалануға мүмкіндік береді. Осылайша, компаниялар айтарлықтай инфрақұрылымсыз іс жүзінде шексіз қуаттылықты қоса алады.

Қашықтағы пайдаланушыларды Ғаламтор желісі арқылы компанияның желісіне қосудың арзан әдісі болса да, VPN енгізу қымбатқа түседі. Типтік шығындардың кейбіріне аппараттық құрал, ISP-дің ай сайынғы ақысы, желіні жаңарту және соңғы пайдаланушыларды қолдау кіреді. Бұл шығындар стандартты емес, олар көптеген факторларға, соның ішінде мөлшеріне немесе корпорацияға, қашықтағы пайдаланушылардың санына, қолданыстағы желілік жүйелердің түріне және Ғаламтор-провайдердің қайнар көздеріне байланысты өзгеріп отырады.

Шешім қабылдауға келгенде, IT-менеджерлер немесе басшылар бұл шығындарды ескеруі керек. Сонымен қатар, шешім қабылдаушылар VPN шешімін сайтта жасауды немесе оны үшінші тарап қызмет провайдеріне беру керек пе, соны шешуі керек.

Бұл тақырыпқа бірнеше тәсілдер бар.

Үйді сатуда компаниялар қажеттіліктері үшін тек өздері шешеді деп шешеді. Бұл компаниялар жеке тоннельдер мен құрылғыларды бір-бірлеп орнатуды жөн көреді, және бұл құрылғаннан кейін компанияның бақылау және қызмет көрсету үшін өзінің IT-қызметкерлері болуы мүмкін.

Аутсорсингті енгізу - компаниялар ауқымды болса немесе өздерінің VPN-ді толығымен жүзеге асыру үшін IT-кадрлары болмаса, аутсорсингті таңдай алады. Компания үшінші тарап провайдерлерін тартқан кезде, қызмет провайдері әдетте компания атынан VPN жобалайды және басқарады.

Орта жерді пайдалану - Кейбір компаниялар қызмет провайдерінің VPN құрғанын қалайды, бірақ олардың AT-қызметкерлері туннель трафигі сияқты мүмкіндіктерді басқарады. Іске асырудың бұл түрі компания мен провайдер арасындағы ымыраға келу болып табылады.

Іске асырғаннан кейін компания өзінің соңғы пайдаланушыларына тиісті қолдауды қамтамасыз етуі керек. Бұл жерде қызмет көрсету сапасы келеді.

1.6 Қызмет көрсету сапасы (QOS)

Кең таралған VPN пайдаланушылары әдетте желінің топологиясына, трафикті өңдейтін қауіпсіздік / шифрлаудың немесе брандмауэрдің жоғары деңгейіне мән бермейді. Олар желіні жасаушыларда IPSEC немесе GRE туннельдерінің болуы маңызды емес. Оларды қызықтыратын нәрсе неғұрлым іргелі нәрсе, мысалы, кідірістердің қабылдау деңгейлері әртүрлі. Пайдаланушы файлды жіберуді аяқтау үшін бірнеше қосымша уақытты өткізгісі келеді, бірақ сол пайдаланушы дерекқорға кіру немесе IP деректер желісі арқылы дауыстық қоңырау шалу кезінде мұндай кідірістерге төзімділік аз болады.

QOS (қызмет көрсету сапасы) сіздің миссияңыз үшін сыни трафикті қамтамасыз етуге бағытталған. Өткізу қабілеті шектеулі және түрлі қосымшалар, бейнеконференциядан бастап ERP дерекқорын іздеуге дейінгі нақты әлемде QOS барлық ресурстардың жетіспейтіндігіне ұмтылуы керек, барлық қосымшалардың бірлесіп жұмыс істей алатындығын және жұмысының қолайлы деңгейімен жұмыс жасауын қамтамасыз ететін маңызды құралға айналады.

Қызмет көрсету сапасы (QOS) кез-келген VPN қызметінің негізгі компоненті болып табылады. MPLS / BGP VPN-де Q3 L3 бар мүмкіндіктері белгіленген пакеттерге тақырыптағы «эксперименталды» биттерді немесе ATM магистраль ретінде пайдаланылған кезде, ATM QOS мүмкіндіктерін қолдана отырып қолданыла алады. Қарастырылып отырған трафикті жобалау MPLS / BGP VPN-ге де қатысты. Трафик дизайнын тіпті егер қаласаңыз, белгілі бір жұп сайттар арасында QOS сипаттамалары бар LSP-ларды құру үшін пайдалануға болады. Егер MPLS / BGP VPN бірнеше SP құраса, сипатталған архитектура пайдалы болуы мүмкін.

1.7 VPN болашағы

Кәсіпорындардың көбі желіге қол жеткізудің жоғарырақ деңгейін талап ететіндіктен, бизнес жеке желілік ортадан жаңа кәсіпорын моделіне көшеді, онда кәсіпорынның барлық желісі бойынша ақпарат таратылады. Осылайша, жақын арада олардың желісінің кеңеюі және виртуалды жеке желілерді (VPN) құрудың негізі ретінде Ғаламторды қолданудың артықшылықтарын нақты пайдалану. VPN қауіпсіз және үнемді ортада ақпаратқа қол жетімділік қажеттілігін қанағаттандыру үшін жасалған.

Көптеген провайдерлердің VPN үшін өзара әрекеттесуі қазіргі желілік ортада бизнестің сәттілік сипатына, мердігерлер мен компанияға арналған корпоративті желілерді кеңейту қажеттілігіне, сондай-ақ компанияның желісіндегі әр түрлі жабдықтарға байланысты өте маңызды. VPN технологиясы Ғаламторға қауіпсіз, арзан қашықтықтан қол жетімділікті және филиалдық қосылысты қамтамасыз етуге көмектесетін Microsoft Windows амалдық жүйесіне енген.

Болашақ интеграцияланған VPN-лерден тұрады, бұл VPN индустриясы өзінің ерекше қасиеттерін жақсартатындығына байланысты, бұл тұтынушыларға басқа тұтынушылармен тиімді қарым-қатынас жасай алады. Сондықтан, VPN компанияның бүкіл аумағында көптеген сайттардың деректер желісін құрады, бұл әр құрылғыға желінің кез келген нүктесінен ерекше мекен-жай алуға мүмкіндік береді. Бұл орталық ресурстарға кез-келген ұйымның веб-сайтынан немесе бүкіл әлемдегі Ғаламторға қосылған жерден қол жеткізуге болатындығын білдіреді. Жүздеген шалғай сайттарды орталық желіге қосумен байланысты техникалық мәселелер өте кең.

Бұл көбінесе өте қымбат тығыздығы жоғары магистральды маршрутизаторларды немесе қымбат Frame Relay қызметтерін пайдалануды қамтиды. Бұл жүйелерді сирек күту оңай және көбінесе арнайы дағдыларды қажет етеді. Сонымен қатар, бұл интражелі мен экстранеттің өз уәделерін орындау қабілетіне байланысты. Біріншіден, VPN компаниялары VPN қызметіндегі үнемдеуді қарастыруы керек. Жалпы алғанда, қызметтердің бағасы неғұрлым арзан болса, компаниялар неғұрлым көп өнім алады немесе нарықта олардың қажеттілігі артады. Осылайша, олар жоғары кіріс алады, содан кейін әлдеқайда жақсы VPN-ді дамытуға көп ақша жұмсайды.

VPN қызмет жеткізушілері клиенттердің іскери операциялары үшін құнды желілік қызметтерді ұсыну арқылы клиенттердің адалдығын қалыптастырады. Бұл жаңа клиенттерді тартуға мүмкіндік береді, өйткені компаниялар кешегі деректерді беру стратегиясынан қазіргі кездегі неғұрлым жан-жақты шешімдерге көшеді.

Бірнеше сайтты қамтитын VPN қашықтан қатынау бағдарламалық шешіміне қарағанда көбірек мүмкіндіктерге ие болуы керек. Кейбір негізгі ерекшеліктері:

- **AAA** - аутентификация (пайдаланушы кім), авторизация (пайдаланушы не істей алады) және бухгалтерлік есеп (пайдаланушы іс жүзінде не істейтінін жазу).

- **Қауіпсіздік** - кем дегенде 128 биттік деректерді шифрлау мүмкіндігі бар сайттар арасындағы жолды жоспарлауды қолдау.

- **Масштабталу** - жаңа талаптарға бейімделу үшін қосымша пайдаланушылар мен өткізу қабілеттілігін оңай қосуға болады.

- **Қызметтер** - қызметтердің сапасы, оның ішінде өткізу қабілеттілігін басқару және трафиктің қалыптасуы бітелудің алдын алу үшін маңызды.

- **Менеджмент** - пайдаланушының белсенділігі, пайдаланушылық саясатты басқару және жалпы VPN мониторингі туралы есептер. Бұрын өздерінің байланыс қажеттіліктерін басқарған компаниялар өз желілерін жаһандық деңгейде құруға, жетілдіруге және басқаруға көмектесіп, қызмет провайдерлерімен бірлесе жұмыс істейді. Бұл үздіксіз өсуге, кірісті арттыруға және қызмет жеткізушілері мен абоненттер үшін үлкен жетістіктерге жол ашады. Бұрын қызмет жеткізушілер жалға алынған желілер мен реле релесі сияқты төменгі деңгейдегі көліктерге назар аударатын еті. Қазіргі уақытта қызмет жеткізушілері виртуалды жеке VPN арқылы желінің қажеттіліктерін

қанағаттандыру үшін іскери тұтынушылармен жұмыс жасауда. VPN - болашақ қызметтердің көзі. Дұрыс іске асырылған кезде, олар капиталды шығындарды азайта отырып, желінің жұмысын жеңілдетеді. Көптеген компаниялар үшін бастапқы нүкте әр түрлі жұмыс топтарына тиімді және ыңғайлы түрде қосылу болып табылады. Сол жерден қызмет провайдерлері қосымша технологияны ұсыну үшін негіз болып табылатын технологияға әсер ете алады, мысалы, хостинг, бейнеконференция және пакеттік телефония.

VPN технологиясы (виртуалды жеке желі) Ғаламтор арқылы берілетін ақпаратты қорғаудың жолын ұсынады, бұл пайдаланушыларға Ғаламтор сияқты қауіпті желі арқылы ішкі желіге, ресурстарға, мәліметтер мен байланысқа қауіпсіз қол жетімділік үшін виртуалды жеке «туннель» құруға мүмкіндік береді.

Бұл тарауда VPN және VPN негізгі технологияларына шолу жасалады. Біз виртуалды жеке желіні енгізу кезінде ескерілуі мүмкін қауіпсіздік қауіптері мен қауіпсіздік мәселелерін талқылаймыз.

2 VPN туннелдік протоколының әдістері

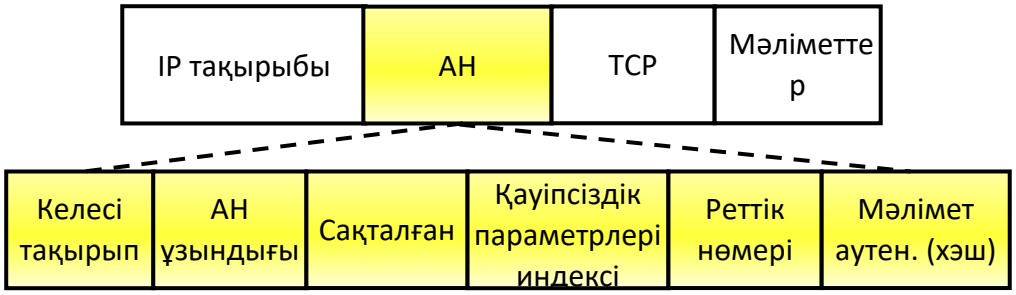
2.1 IPSEC (IP Security Protocol)

IPSEC протоколын IETF (Internet Engineering Task Force) ақпараттық қауіпсіздікті қамтамасыз ету үшін OSI-дің үшінші деңгейінде Ғаламтор сияқты көпшілікке қол жетімді қорғалмаған IP желісі арқылы жасады. IPSEC жүйеге талап етілетін қызмет үшін пайдаланылатын қауіпсіздік протоколдарын, алгоритмдерін және құпия кілттерін таңдауға және келісуге мүмкіндік береді. IPSEC деректерді рұқсатсыз қарау мен өзгертуден қорғау үшін негізгі аутентификацияны, деректердің тұтастығын және шифрлау қызметтерін ұсынады. Ол екі қауіпсіздік протоколын, AH (түпнұсқалық растама тақырыбы) және ESP (Encapsulated Security Payload), қажетті қызметтер үшін пайдаланады. Алайда, IPSEC тек IP пакеттерін жіберумен шектеледі.

2.1.1 Трафик қауіпсіздігінің қауіпсіздік протоколдары

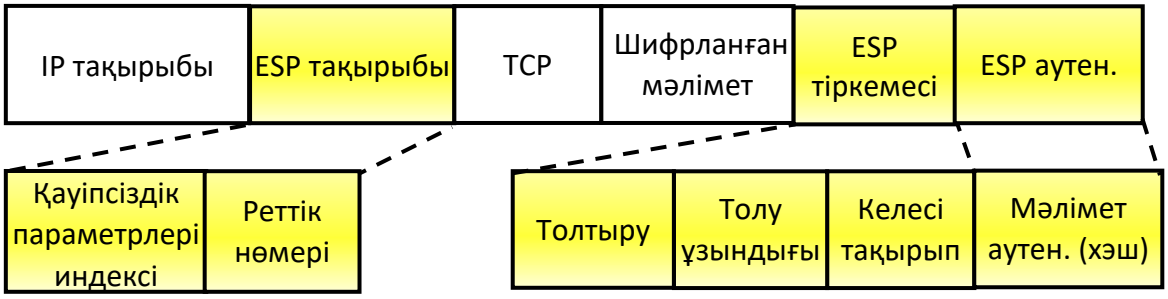
IPSEC қауіпсіздік қызметтерін ұсыну үшін AH және ESP протоколдарын қолданады:

1. AH протоколы (Authentication Header) түпнұсқалық көзін тексереді және IP пакет тұтастығын қамтамасыз етеді, бірақ онда шифрлау жоқ. IP пакетіне қосылған AH тақырыбы деректердің хэшін, сериялық нөмірін және т.б., сонымен бірге жіберушіні тексеруге, деректердің тұтастығын қамтамасыз етуге және қайталану шабуылдарын болдырмауға қолданылатын ақпаратты қамтиды.



2.1-сурет. AH протоколы

2. ESP (Encapsulated Security Payload) протоколы аутентификация мен тұтастықтың көзіне қосымша деректердің құпиялылығын қамтамасыз етеді. Деректердің құпиялылығын қамтамасыз ету үшін ESP 3DES сияқты симметриялық шифрлау алгоритмдерін қолданады. Алгоритм өзара әрекеттесетін түйіндер үшін бірдей болуы керек. ESP сонымен қатар тек шифрлауды немесе түпнұсқалықты тексеру конфигурацияларды қолдайды. Алайда, 2007 жылы жүргізілген зерттеулер ESP-ны тек шифрлау үшін пайдаланатын кез-келген RFC-ке сәйкес келетін IPSEC-тің зақымдалуы мүмкін екенін көрсетті.



2.2-сурет. ESP протоколы

2.1.2 Жұмыс режимдері

Әрбір қауіпсіздік протоколы екі жұмыс режимін қолдайды: туннель режимі және тасымалдау режимі. Туннель режимі әр пакеттің тақырыптары мен деректерін шифрлайды және / немесе аутентификациялайды, ал тасымалдау режимі тек деректерді шифрлайды және / немесе аутентификациялайды.

1. Туннель режимі. Мұнда бүкіл пакет қорғалған. Бастапқы адресі көрсетілген бастапқы IP пакет жаңа IP пакетіне салынып, AH және ESP жаңа пакетке қолданылады. Жаңа IP тақырыбы туннельдің соңғы нүктесін көрсетеді. Пакетті алғаннан кейін туннельдің соңғы нүктесі мазмұнын дешифрлайды, содан кейін бастапқы пакет желінің соңғы орнына жіберіледі.

2. Көлік режимі (хост хост). Мұнда AH және ESP тақырыптары бастапқы IP пакеттің деректеріне қолданылады. Режим деректерді шифрлайды және / немесе аутентификациялайды, бірақ IP тақырыбын емес. Қосылған есептік шығындар тоннель режимінде талап етілетіннен аз. Дегенмен, соңғы мекен-жайы мен бастапқы мекен-жайы анықталуы мүмкін. Шабуылшылар осы тақырып түріндегі тақырып туралы ақпарат негізінде трафикке талдау жасай алады. Әдетте хосттар арасындағы байланыс үшін ғана қолданылады.

2.1.3 Кілттермен алмасу және басқару

IPSEC Ғаламтор арқылы кілттерді басқарудың екі түрін қолдайды: автоматты және қолмен басқару.

1. Автоматты кілттерді басқару. IKE (Internet Key Exchange) - IPSEC протоколдарды, алгоритмдер мен кілттерді айқындау және келісу және екі тараптың түпнұсқалығын растау үшін пайдаланатын әдепкі протокол. Бұл кеңінен таралған масштабты VPN жаюы мен жүзеге асырылуы үшін пайдалы.

IKEv2 протоколы 2005 жылы шығарылды. Ол IKEv1 протоколының көптеген мүмкіндіктерін сақтайды, сонымен қатар икемділікті қамтамасыз етеді. Ол IKEv1 протоколының көптеген мүмкіндіктерін сақтайды, сонымен қатар NAT желіні айналып өтуді және икемділікті қамтамасыз етеді.

IKE сонымен қатар сандық сертификаттарды қолдануды қолдайды. Пайдаланушылар алдымен сандық қолтаңба кілтімен деректерге қол қою арқылы

аутентификация жасайды. Содан кейін басқа соңғы нүкте қолды тексереді. IKE екі нысанның арасында сенімді қорғалған туннель жасайды, содан кейін екі субъект арасындағы қауіпсіздік қауымдастығымен (SA) келісіп, кілттерін ауыстырады. SA - бұл бірдеңгейлі түйіндердің келіссөздер кезінде қызметтерді және трафикті қорғау тетіктерін анықтау үшін қолданылатын параметрлер жиынтығы. Бұл параметрлерге алгоритм идентификаторлары, режимдер, кілттер және т.б жатады. IKE сонымен қатар байланысушы компаниялар арасында кілттерді қадағалап, оларды жаңартады. IKE кілттердің пайда болуын, SA құруды және басқаруды және аутентификация процедураларын анықтау үшін ISAKMP (Ғаламтор қауіпсіздігі қауымдастығы және кілттерді басқару протоколы) және Oakley сияқты протоколдарды қолданады.

IPSEC VPN шлюзі қашықтағы пайдаланушыны аутентификациялау үшін IKE-мен жұмыс жасайтын бірнеше аутентификация әдістері бар, соның ішінде гибридтік аутентификация, кеңейтілген аутентификация (Xauth), криптографиялық кілттерге (CRACK) сұрау / жауап аутентификациясы және сандық сертификаттар. Бұл қол жеткізуді басқару процесін жақсарту үшін үшінші тараптың аутентификациясының қосымша қызметтерін пайдалануға мүмкіндік береді.

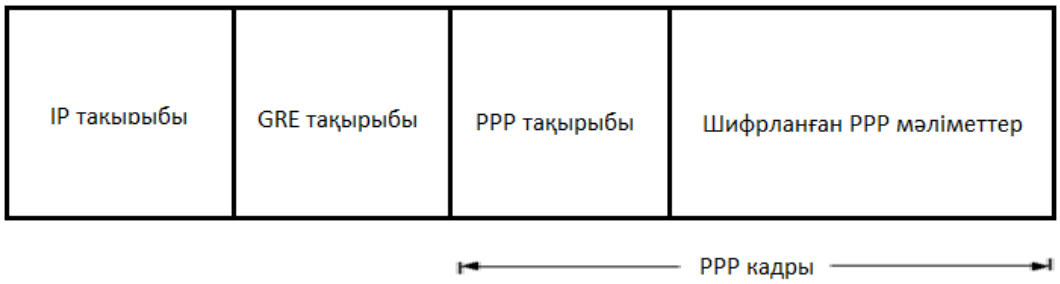
2. Қолды кілттерді басқару. Жеке кілттер мен қауіпсіздік ассоциациялары қосылымды орнатпас бұрын екі VPN байланыс торабында қолмен реттеледі. Қауіпсіздік қызметтерінің құпия кілтін тек жіберуші мен алушы ғана біледі. Егер аутентификация деректері дұрыс болса, алушы хабарлама жіберушіден келгенін және оның өзгермегенін біледі. Бұл тәсілді кішігірім статикалық ортада қолдануға болады, бірақ ол жақсы таралмайды. Қауіпсіз байланыс үшін барлық кілттерді бірдеңгейлі беттермен алдын-ала бөлісу керек. Егер кілттер бұзылса, басқа адам пайдаланушыны еліктей алады және VPN-ге қосыла алады.

2.2 PPTP (Point-to-Point Tunneling Protocol)

PPTP (Point-to-Point Tunneling Protocol) - бұл PPP (Point-to-Point Protocol) үстіне салынған OSI протоколының екінші қабаты. PPP - Ғаламторға қосылу үшін пайдаланылатын көп протоколды қашықтан қол жеткізу протоколы. Қашықтағы пайдаланушылар өздерінің жергілікті Ғаламтор-провайдерін бірінші рет теру арқылы PPTP арқылы жеке желіге қол жеткізе алады. PPTP әр қашықтағы клиент үшін виртуалды желі құра отырып, толық желіге қосылады. PPTP IP-желі арқылы TCP / IP протоколдарымен (мысалы, IP, IPX немесе NetBEUI) PPP сеансын өткізуге мүмкіндік береді. PPTP ақпараттық жоба ретінде RFC 2637-де құжатталған.

PPP қосылымдары үшін қолданылатын аутентификация механизмі PPTP VPN қосылымдарында қолданылады. Оларға EAP (кеңейтілген аутентификация протоколы, MSCHAP (Microsoft қоңыраудың аутентификациялау протоколы), CHAP, SPAP (Shiva парольді аутентификациялау протоколы) және PAP (парольді аутентификациялау протоколы) кіреді. Шифрлау үшін PPP

мәліметтерін MPPE көмегімен әрі қарай шифрлауға болады (Microsoft Point Encryption), арна шифрлауына арналған RSA RC4 стандартына (40/56/128 бит) негізделген. Капсуланған PPTP 2.3-суретте көрсетілген.



2.3-сурет. Капсулаланған PPTP

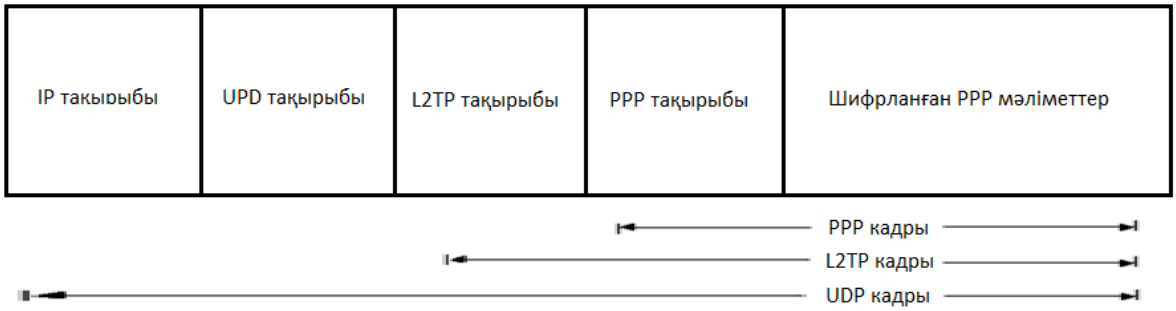
PPTP деректерін туннельдеу бірнеше инкапсуляция деңгейлері арқылы жүреді. PPTP GRE (General Routing Encapsulation) өзгертілген нұсқасын қолдана отырып, Ғаламтор немесе жеке интранет сияқты IP желісі арқылы берілетін туннельді деректер ретінде PPP кадрларын инкапсуляциялайды. GRE ағынды басқарумен және PPP пакеттерін беруге арналған бітелумен жабдықталған инсультталған қызметті ұсынады. Инкапсуланған PPP кадрларындағы мәліметтер шифрлануы мүмкін (және / немесе қысылу). Алынған деректер GRE және PPP-де инкапсулденген, содан кейін PPTP клиенті мен PPTP сервері үшін сәйкес көзі мен тағайындалған IP мекен-жайлары бар IP тақырыбында инкапсуляцияланады. Тунельдендірілген PPTP деректерін алғаннан кейін, PPTP сервері IP, GRE және PPP тақырыптарын өңдейді және жояды, содан кейін PPP деректерінің шифрын ашады.

2.3 L2TP (Layer 2 Tunneling Protocol)

L2TP (Layer 2 Tunneling Protocol) - бұл Microsoft PPTP (Point-to-Point Tunneling Protocol) және Cisco L2F (Layer 2 Forwarding) жиынтығы. L2TP IP, X.25, Frame Relay немесе ATM желілері арқылы жіберілуі керек PPP (нүкте-нүкте протоколы) кадрларын инкапсуляциялау үшін туннельді протокол ретінде пайдаланылуы мүмкін. Бір туннель арқылы бірнеше рет қосылуға рұқсат етіледі. PPTP және L2F сияқты, L2TP OSI екінші деңгейінде жұмыс істейді. Layer 2 VPN протоколдары мәліметтерді PPP шеңберлерінде инкапсулаттайды және IP емес протоколдарды IP желілері арқылы жіберуге қабілетті. L2TP стандартты жол ретінде RFC 3931-де құжатталған.

L2TP қосылымдары EAP, CHAP, MS-CHAP, PAP және SPAP сияқты PPP қосылымдарымен бірдей аутентификации механизмдерін қолданады. L2TP туннелі инкапсуляцияның бірнеше деңгейлері арқылы жүреді. PPP деректері PPP тақырыбында және L2TP тақырыбында жинақталады. Капсулаланған L2TP пакеті қосымша UDP тақырыбына 1701-ге орнатылған бастапқы және тағайындау порттармен оралған. Соңғы пакет VPN клиентінің және VPN

серверінің бастапқы және тағайындалған IP мекен-жайларын қамтитын IP тақырыбымен оқшауланған. Капсуланған L2TP 2.4-суретте көрсетілген.



2.4-сурет. Капсулаланған L2TP

L2TP беретін құпиялылықтың болмауына байланысты ол көбінесе IPSEC-пен бірге қолданылады және L2TP / IPSEC деп аталады. L2TP IPSEC арқылы жұмыс істеген кезде қауіпсіздік қызметтері IPSEC, AH және ESP арқылы қамтамасыз етіледі. Барлық басқару элементтері мен L2TP деректері IPSEC жүйесіне арналған бірыңғай IP деректер пакеттері түрінде көрсетіледі.

2.4 SSL / TLS (Transport Layer Security & Secure Sockets Layer)

SSL / TLS - бұл 443 TCP портын қолданатын тасымалдау қабаты протоколы. SSL протоколын IETF анықтайды және 3.1 нұсқасынан басқа SSL нұсқасы жоқ. TLS 1.0 және TLS 1.1 - TLS стандартталған екінші нұсқасымен, ал TLS 1.0 - SSL 3.1 нұсқасымен бірдей.

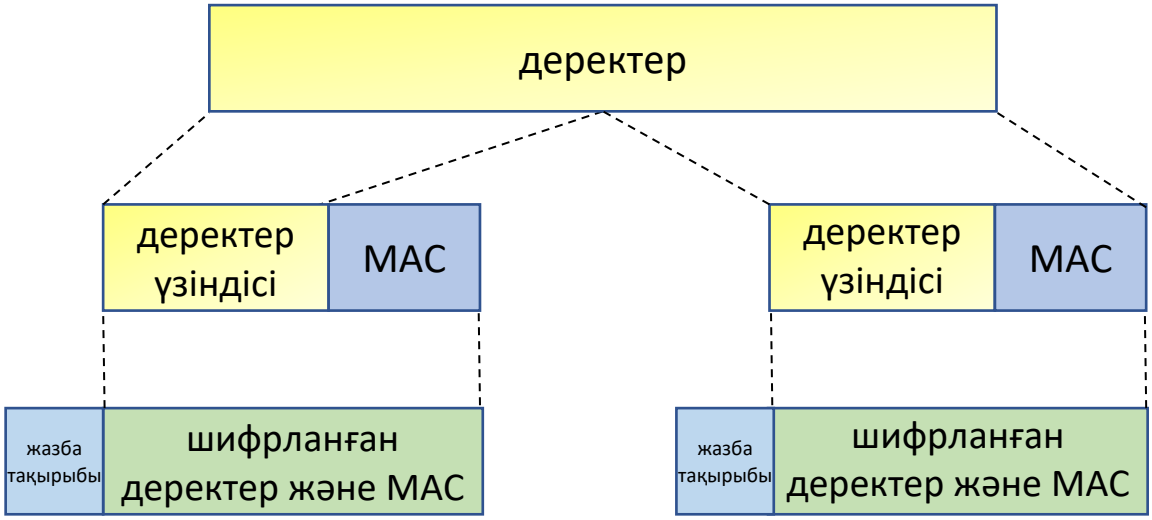
SSL / TLS бірқатар криптографиялық мүмкіндіктерді, соның ішінде құпиялылықты, тұтастықты және сандық қолтаңбаларды ұсынады. Екі өзара әрекеттесуші тарап криптографиялық функцияларға келісетін IPSEC-тен айырмашылығы, SSL / TLS мәліметтер алмасу кезінде клиент пен сервер қолданатын криптографиялық функциялардың жиынтығын анықтау үшін шифрлық жинағы қолданады.

SSL VPN шлюзі қолданушыға өзінің браузері арқылы сенімді сервермен байланысып тұрғандығын тексере алатындай сенімді сертефикат органы (CA) қол қойған SSL сервер куәлігін қолданып веб-пайдаланушыға өзін-өзі растауы мүмкін. Іс жүзінде кейбір SSL VPN өздігінен қол қойылған сандық сертификатты қолдана алады, ол әдетте көптеген веб-браузерлерге сенбейді. Бұл жағдайда пайдаланушыға SSL VPN сервер сертификатын пайдаланушыға арналған сенімді сертефикаттардың тізіміне қосу немесе сертефикатка сенім білдіру үшін «иә» деп қабылдау қажет болуы мүмкін.

SSL VPN-дің капсулануы, келесі тәсілімен жүзеге асырылады.

SSL VPN-де қосымшалар туралы мәліметтер блоктарда қабылданады. Хабарды аутентификациялау коды (MAC) блоктармен бекітілген, ол төмендегі

2.5-суретте көрсетілгендей капсулаланған деп аталатын нысанға енеді. Жазба ұзындығы 5 байттан тұрады.



2.5-сурет. Капсулаланған SSL

3 Симуляциялық ортаны таңдау және site-to-site VPN теңшеу

Бұл тарауда әр түрлі протоколдарды қолдана отырып желілік модельдеу орталары мен site-to-site VPN теңшеуі талданады.

3.1 Желілік эмуляторларды салыстыру

Көбінесе қай бағдарламалық жасақтама ең жақсы екендігі туралы сұрақтар туындайды. Бұл белгілі бір артықшылықтар беретін және кейбір кемшіліктері бар барлық шешімдердің жеке қалауына байланысты.

Желілерді зерттеу және тестілеу үшін бүгінгі таңда көптеген танымал бағдарламалық жасақтама бар, мысалы:

- GNS3.
- Cisco Packet Tracer.
- Cisco VIRL.
- және басқалары.

3.1.1 GNS3

GNS3 – ашық күйіндегі коды бар, тегін бағдарламалық жасақтама.

Артықшылықтары:

- Тегін бағдарламалық жасақтама.
- Ашық күйіндегі коды бар, тегін бағдарламалық жасақтама.
- Ай сайынғы немесе жылдық лицензиялық төлемдер жоқ.
- Қолдау көрсетілетін құрылғылар санында ешқандай шектеулер жоқ (жалғыз шектеулер - сіздің жабдықтарыңыз: процессор және жад).
- Қосылудың бірнеше нұсқаларын қолдайды (Etherswitch NM-ESW16 модулі, IOU / IOL Layer 2 кескіні, VIRL IOSvL2):
- Барлық VIRL кескіндері қолдайды (IOSv, IOSvL2, IOS-XRv, CSR1000v, NX-OSv, ASAv).
- Мультивендорлық орталарды қолдайды.
- Гипервизорларсыз немесе онсыз қосуға болады.
- Ақысыз және ақылы гипервизорларды қолдайды (Virtualbox, VMware жұмыс станциясы, VMware ойнатқышы, ESXi, Fusion).
- Жүктеуге болатын, ақысыз, алдын-ала конфигурацияланған және оңтайландырылған құрылғылар оңай орналастыруға болады.
- Linux қолдауымен қосымша виртуализация бағдарламалық жасақтамасын қажет етпиді.
- Бірнеше жеткізушілердің бағдарламалық жасақтамасы еркін қол жетімді.
- Үлкен және белсенді қоғамдастық (800000-нан астам мүше).

Кемшіліктері:

- Cisco кескіндерін пайдаланушы қамтамасыз етуі керек (Cisco.com сайтынан жүктеу немесе VIRL лицензиясын сатып алу немесе жеке құрылғыдан көшірме жасау керек).
- Автономдық пакет емес, бірақ жергілікті бағдарламалық жасақтаманы (GUI) орнатуды қажет етеді.
- Компьютеріңіздің параметрлері мен шектеулері GNS3-ке жергілікті орнатуға байланысты әсер етуі мүмкін (брандмауэр және қауіпсіздік параметрлері, ноутбуктің компанияның саясаты және т.б.).

3.1.2 Cisco Packet Tracer

Cisco Packet Tracer - бұл Cisco желілерін имитациялайтын Cisco Академиясының студенттеріне арналған ресми өнім. Ол Cisco жабдығын эмуляцияламайды және Cisco немесе басқа сатушылардан алынған нақты кескіндерді қолдамайды.

Артықшылықтары:

- Теңшеулеу қарапайым.
- Cisco маршрутизаторын, коммутаторды және компьютерді модельдеуді қолдайды.
- CCNA зерттеуіне жеткілікті.
- Бірнеше құрылғылар мен протоколдарды имитациялайды (маршрутизаторлар, коммутаторлар, сымсыз, RADIUS және т.б.).
- Тегін (Cisco NetAcad сайтында тіркелуді қажет етеді).

Кемшіліктері:

- Кодтың түпнұсқасы - ашық код емес.
- Тек Cisco құрылғыларын модельдейді (нақты Cisco кескіндері жұмыс істемейді).
- Көп сатушыдан қолдау жоқ.
- Нақты физикалық құрылғылармен біріктіру мүмкін емес.
- Сіз тек әзірлеушілер енгізген IOS командаларын қолдана аласыз. Packet Tracer-де модельделген платформада қол жетімді барлық командалар бола бермейді.

3.1.3 Cisco VIRL

Cisco тағы бір ресми қолдау көрсетілетін желіні - Cisco Virtual Internet Routing Lab (VIRL) модельдеу платформасын құрды. Бұл Cisco Packet Tracer-мен салыстырғанда әлдеқайда күшті шешім және сізге нақты желілерді оқып үйренуге ғана емес, сонымен бірге модельдеуге де мүмкіндік береді.

Cisco VIRL - бұл GNS3-тен анағұрлым жақын өнім, бұл желі инженерлеріне Cisco технологиясы туралы білуден басқа, нақты желілерді модельдеуге мүмкіндік береді.

Артықшылықтары:

- Cisco маршрутизаторын, коммутаторды, брандмауэрді және компьютерді модельдеуді қолдайды (IOSv, IOSvL2, ASAv).
- CCNA, CCNP және CCIE зерттеулеріне жарамды.
- Cisco Firewall (ASAv) қолдайды.
- Көптеген хаттамалар мен функцияларға қолдау көрсетіледі: RPVST +, Etherchannel, Port Security, MPLS, VRF және басқалары.
- Cisco IOS (15.X) соңғы нұсқаларына қолдау көрсетіледі.

Кемшіліктері:

- Тегін емес бағдарламалық жасақтама. Personal Edition VIRL-ға тіркелу үшін жылына $ 199.99 төлейсіз.
- Құрылғылары шектеулі. Персоналдық нұсқада сіз бір топология үшін 20 Cisco түйіндерімен шектелесіз.
- VIRL-ді теңшеу және орнату қиын болуы мүмкін.
- Ресурсі көп (жедел жад пен процессордың көп мөлшерін қажет етеді).
- Виртуализация бағдарламасын талап етеді (VMware Workstation Player / Pro, Fusion немесе ESXi).
- VirtualBox қолдамайды.
- Көп сатушыдан қолдау жоқ - тек Cisco желілік құрылғыларына қолдау көрсетіледі.

3.1 Желіні құру ортасын салыстыру нәтижелері

3.1 кестеде бағдарламалық жасақтаманың (БЖ) салыстыру нәтижесі көрсетілген.

Кесте 3.1 – БЖ салыстыру нәтижелері

	GNS3	**Packet Tracer**	**VIRL**
Баға	Тегін	Тегін	Тегін
Теңшеу	Қарапайым	Қарапайым	Қиын
Ашық күйдегі код	Бар	Жоқ	Бар
Жүйелік ресурстарға қойылатын талаптар	Жоғары	Төмен	Жоғары
Бағдарламалық жасақтаманың жылдамдығы	Төмен, қателер мен жалтырақтар пайда болады	Жоғары	Орташа
Cisco img, Juniper немесе QEMU қолдау	Бар	Тек Cisco img бар	Бар

3.1-кестенің жалғасы

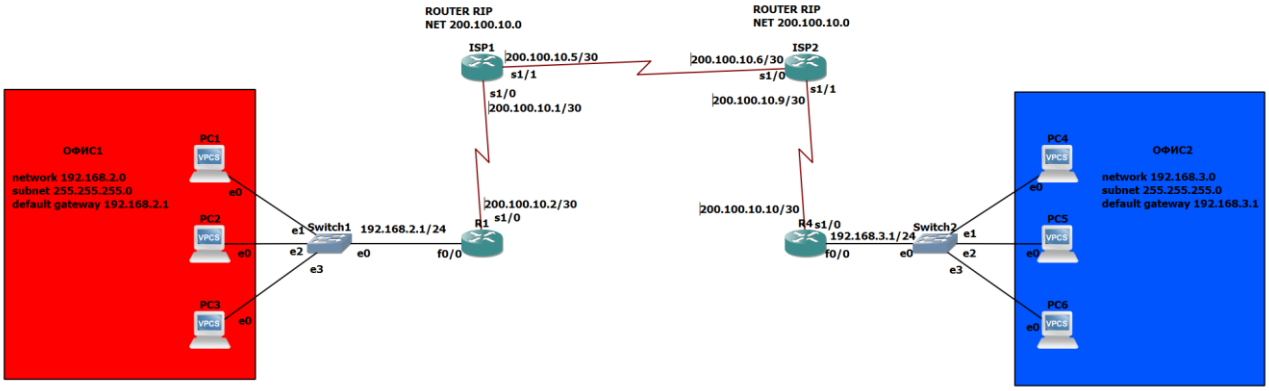
	GNS3	Packet Tracer	VIRL
Windows, Linux ОЖ қолдану	Бар	Бар	Бар
VM қолдауы	Ақысыз және ақылы гипервизорларды қолдайды.	Қолдамайды	Виртуализация үшін бағдарламалық жасақтама қажет етеді. VirtualBox-ты қолдамайды

Жоғарыда аталған бағдарламалық жасақтаманың ішінен таңдау GNS3-ке түсті, себебі:

1. Оқшауланған құрылғылардың толық функционалдығы бар, яғни (мысалы, маршрутизаторлардың барлық қызметі қол жетімді болады).
2. Гетерогенді желілерді құру мүмкіндігі бар, яғни біз тек Cisco құрылғыларының ғана емес, сонымен қатар Juniper, Mirotik, Checkpoint схемасын жинай аламыз.
3. Толыққанды жұмыс станциялары мен серверлерді желіге қосу, яғни ОЖ-мен толыққанды компьютерді қосуға болады.
4. Тегін пайдалануға болады.

3.2 Корпоративтік желінің схемасының құрылуы

VPN желісін PPTP, L2TP / IPsec, IKEv2 / IPsec, SSL протоколдарын қолдана отырып жасамас бұрын, сізге VPN құратын корпоративті желі схемасын реализациялау қажет. Топология 3.1-суреттегі тәсілімен көрсетілкен:



3.1-сурет. Топология site-to-site VPN

Бізде екі офис бар - ISP, R2 және R3 маршрутизаторларымен байланысқан, оларды кеңсе әкімшілері басқара алмайтын 1-ші кеңсе (192.168.2.0/24), 2-ші офис (192.168.3.0/24) бар.

Site-to-site VPN енгізу R1 және R4 маршрутизаторларының көмегімен жүзеге асырылады.

IP адресі және бағыттауы теңшеуленген. Бағыттау динамикалық бағыттау протоколының көмегімен құрылған RIP.

3.2.1 PPTP

PPTP қосылымын келесі қадамдармен теңшей бастадым:

1-кадам. Жаңа командаларды ұсыну үшін жаңа модельді іске қостым. Әдепкі бойынша локалды дерекқор үшін PPP аутентификациясын орнаттым. Клиенттік компьютерге авторизацияны ұсындым, егер қолданушы аутентификациядан сәтті өткен болса, авторизацияны автоматты түрде өтеді(3.2.1-сурет):

```
R1(config)#aaa new-model
R1(config)#aaa authentication ppp default local
R1(config)#aaa authorization network default if-authenticated
```

3.2.1-сурет – 1 кадам

2-кадам. Ішкі желіге қосылу кезінде VPN клиенттерінің пайдалануы үшін жергілікті IP мекенжайлар пулын жаздым(3.2.2-сурет):

```
R1(config)#ip local pool PPTP-VPN-POOL 192.168.2.1 192.168.2.10
%IP address 192.168.2.1 is already defined as a^\bda^\ate2^QLeB*$`EI^TeW^FHeB*$Int.
R1(config)#
```

3.2.2-сурет – 2 кадам

3-кадам. VPDN-ді іске қостым, өйткені VPDN (Virtual Private Dialup Network) жалпы инфрақұрылымды пайдаланып жеке желіге қашықтан қол жеткізуді кеңейтеді. Қашықтағы пайдаланушыдан ISP желісі арқылы жеке желіге Layer 2 және жоғары деңгейдегі желілік қосылыстарды кеңейту үшін VPDN-де Layer 2-гі туннельдеу технологиялары қолданылады (L2F, L2TP және PPTP)(3.2.3-сурет):

```
R1(config)#vpdn enable
```

3.2.3-сурет – 3 кадам

4-кадам. VPN тобы үшін VPDN тобының конфигурациясын енгіздім. VPDN тобын конфигурацияладым. Біздің PPTP VPN кіріс байланыстарымызды осылай анықтадым. Сонымен қатар PPTP-ге қолданыстағы протоколын және қосымша параметрлері бар виртуалды шаблонын көрсеттім(3.2.4-сурет):

```
R1(config)#vpdn-group VPN
R1(config-vpdn)#accept-dialin
R1(config-vpdn-acc-in)#
R1(config-vpdn-acc-in)#protocol pptp
R1(config-vpdn-acc-in)#virtual-template 1
```

3.2.4-сурет – 4 кадам

5-кадам. Роутерге қосылу кезінде VPN клиенттері пайдаланатын виртуалды интерфейсті теңшедім. PPTP VPN клиенттері роутердегі жергілікті локалмен анықталған пулдағы IP мекенжайды пайдаланады. Әрі қарай, PPP туннеліне арналған 128-биттік MPPE шифрлауды және орнаттым. содан кейін MS-CHAP-V2 протоколын аутентификациясын қолдандым(3.2.5-сурет):

```
R1(config)#interface virtual-template 1
R1(config-if)#ip unnumbered FastEthernet0/0
R1(config-if)#peer default ip address pool PPTP-VPN-POOL
R1(config-if)#no keepalive
R1(config-if)#ppp encrypt mppe 128
R1(config-if)#ppp authentication ms-chap-v2
R1(config-if)#encapsulation ppp
```

3.2.5-сурет – 5 кадам

6-кадам. PC1-ден PC4-ке қосылуды тексердім(3.2.6-сурет):

```
PC1> ping 192.168.3.2
84 bytes from 192.168.3.2 icmp_seq=1 ttl=60 time=83.605 ms
84 bytes from 192.168.3.2 icmp_seq=2 ttl=60 time=79.713 ms
84 bytes from 192.168.3.2 icmp_seq=3 ttl=60 time=78.191 ms
84 bytes from 192.168.3.2 icmp_seq=4 ttl=60 time=79.800 ms
84 bytes from 192.168.3.2 icmp_seq=5 ttl=60 time=85.588 ms

PC1> tracer 192.168.3.2
trace to 192.168.3.2, 8 hops max, press Ctrl+C to stop
 1   192.168.2.1   119.794 ms  6.052 ms  10.292 ms
 2   200.100.10.1   669.345 ms  30.705 ms  20.527 ms
 3   200.100.10.6   660.456 ms  30.623 ms  32.558 ms
 4   200.100.10.10   151.934 ms  51.549 ms  43.662 ms
 5     *  *  *
 6   *192.168.3.2   80.864 ms (ICMP type:3, code:3, Destination port unreachable)
```

3.2.6-сурет – 6 кадам

7-кадам. Нәтижесі 3.2.1 кестеде көрсетілген:

Кесте 3.2.1 – PPTP нәтижесі

Орнату	Қарапайым
Шифрлау	mppe 128
Аутентификация	ms-chap-v2
Жылдамдығы max	15-20 mbit

3.2.2 L2TP / IPsec

Енді L2TP / IPsec туннелдік протоколының қосылымын теңшей бастаймыз:

1-кадам. Жаңа командаларды ұсыну үшін жаңа модельді іске қостым. Онда, локалды дерекқор үшін PPP аутентификациясын орнаттым. Клиенттік

компьютерге авторизацияны ұсындым, егер қолданушы аутентификациядан сәтті өткен болса, авторизацияны автоматты түрде өтеді(3.2.8-сурет):

```
R1(config)#aaa new-model
R1(config)#aaa authentication ppp default local
R1(config)#aaa authorization network default if-authenticated
```

3.2.8-сурет – 1 кадам

2-кадам. Жалпы инфрақұрылымды пайдаланып жеке желіге қашықтан қол жеткізуді кеңейту үшін VPDN-ді іске қостым(3.2.9-сурет):

```
R1(config)#vpdn enable
```

3.2.9-сурет – 2 кадам

3-кадам. Ішкі желіге қосылу кезінде VPN клиенттерінің пайдалануы үшін жергілікті IP мекенжайлар пулын жаздым(3.2.10-сурет):

```
R1(config)#ip local pool PPTP-VPN-POOL 192.168.2.1 192.168.2.10
%IP address 192.168.2.1 is already defined as a^\bda^\ate2^QLeB*$`EI^TeW^FHeB*$Int.
```

3.2.10-сурет – 3 кадам

4-кадам. VPN тобы үшін VPDN тобының конфигурациясын енгіздім. Қашықтан қол жетімділік қосылымдары үшін VPDN тобын конфигурацияладым. Сонымен қатар L2TP-ге қолданыстағы протоколын және қосымша параметрлері бар виртуалды шаблонын көрсеттім(3.2.11-сурет):

```
R1(config)# vpdn-group L2TP-GROUP
R1(config-vpdn)#accept-dialin
R1(config-vpdn-acc-in)#protocol l2tp
R1(config-vpdn-acc-in)#virtual-template 1
R1(config-vpdn-acc-in)#ex
R1(config-vpdn)#
```

3.2.11-сурет – 4 кадам

5-кадам. Роутерге қосылу кезінде VPN клиенттері пайдаланатын виртуалды интерфейсті теңшедім. L2TP VPN клиенттері роутердегі жергілікті локалмен анықталған пулдағы IP мекенжайды пайдаланады. Әрі қарай, PPP туннеліне арналған аутентификацияны орнаттым. Ол ушін, MS-CHAP-V2 протоколын аутентификациясын қолдандым(3.2.12-сурет):

```
R1(config-vpdn)#interface Virtual-Template1
R1(config-if)#peer default ip address pool L2TP-POOL
R1(config-if)#ppp authentication ms-chap-v2
AAA: Warning, authentication list "default" is not defined for PPP.
```

3.2.12-сурет – 5 кадам

6-кадам. Қауіпсіздікті күшейту үшін IPsec протоколын бірге қолдандым. Ол үшін IKE саясатын жасадым. Мұнда аутентификация әдісін, хэш алгоритмін,

шифрлау алгоритмін, Diffie-Hellman тобының идентификаторын, уақыт мәнін, кілт қауіпсіздігін беру мәнін көрсеттім(3.2.13-сурет):

```
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#hash sha
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#ex
R1(config)#
R1(config)#crypto isakmp key security address 200.100.10.10 255.255.255.252
A pre-shared key for address mask 200.100.10.10 255.255.255.252 already exist
s!
```

3.2.13-сурет – 6 кадам

7-кадам. IPsec саясатын жасадым, ол үшін трафикті қалай қорғауды анықтайтын түрлендіру жиынтығын теңшедім. Енді динамикалық қатынау тізімдерін бердім(3.2.14-сурет):

```
R1(config)#crypto ipsec transform-set R1set esp-des esp-md5-hmac
R1(cfg-crypto-trans)#mode transport
R1(cfg-crypto-trans)#$t ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#
```

3.2.14-сурет – 7 кадам

8-кадам. Крипто картаны жасадым. Ол үшін криптографиялық картаға кіру тізімін тағайындадым. IPsec арқылы қорғалған трафикті қайта бағыттауға болатын бірдеңгейлі түйінің көрсеттім. Осы криптографиялық картаға қандай түрлендірулер жиынтығы рұқсат етілгенін көрсеттім. Басымдық реті бойынша бірнеше түрлендірулер жиынтығын енгізуге болады (біріншісі жоғары басымдылық). Сіз криптографиялық картада 6-ға дейін түрлендіру жиынтығын көрсете аласыз(3.2.15-сурет):

```
R1(config)#
R1(config)#crypto map R1map 10 ipsec-isakmp
R1(config-crypto-map)#set peer 200.100.10.10
R1(config-crypto-map)#set transform-set R1set
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit
R1(config)#interface serial 1/0
R1(config-if)#crypto map R1map
```

3.2.15-сурет – 8 кадам

9-кадам. Әдепкі маршрутты тіркедім(3.2.16-сурет):

```
R1(config)#ip route 0.0.0.0 0.0.0.0 200.100.10.1
```

3.2.16-сурет – 9 кадам

10-кадам. R1-ге түзету командасын бердім(3.2.17-сурет):

```
R1(config)#end
R1#debug crypto ipsec
Crypto IPSEC debugging is on
R1#
*Mar  1 00:26:06.955: %SYS-5-CONFIG_I: Configured from console by admin on console
R1#debug crypto isakmp
Crypto ISAKMP debugging is on
R1#
```

3.2.17-сурет – 10 кадам

11-кадам. PC1-ден PC4-ке қосылуды тексердім(3.2.18-сурет):

```
PC1> ping 192.168.3.2
84 bytes from 192.168.3.2 icmp_seq=1 ttl=62 time=62.066 ms
84 bytes from 192.168.3.2 icmp_seq=2 ttl=62 time=80.176 ms
84 bytes from 192.168.3.2 icmp_seq=3 ttl=62 time=505.987 ms
84 bytes from 192.168.3.2 icmp_seq=4 ttl=62 time=173.312 ms
84 bytes from 192.168.3.2 icmp_seq=5 ttl=62 time=63.812 ms
```

3.2.18-сурет – 11 кадам

12-кадам. Құрастырылған ISAKMP(3.2.19-сурет):

```
R1#show crypto isakmp key
Keyring              Hostname/Address                  Preshared Key

default              200.100.10.10  [255.255.255.252]   security
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               3600 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
R1#show crypto isakmp peers

R1#show crypto isakmp profile

R1#
*Mar  1 00:52:02.475: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 200.100.10.2, remote= 200.100.10.10,
    local_proxy= 192.168.2.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0x88F26740(2297587520), conn_id= 0, keysize= 0, flags= 0x400E
*Mar  1 00:52:02.479: ISAKMP: received ke message (1/1)
*Mar  1 00:52:02.483: ISAKMP:(0:0:N/A:0): SA request profile is (NULL)
*Mar  1 00:52:02.483: ISAKMP: Created a peer struct for 200.100.10.10, peer port 500
*Mar  1 00:52:02.483: ISAKMP: New peer created peer = 0x659F14A8 peer_handle = 0x80000002
*Mar  1 00:52:02.483: ISAKMP: Locking peer struct 0x659F14A8, IKE refcount 1 for isakmp_initiator
*Mar  1 00:52:02.487: ISAKMP: local port 500, remote port 500
*Mar  1 00:52:02.487: ISAKMP: set new node 0 to QM_IDLE
R1#r  1 00:52:02.487: insert sa successfully sa = 660F81B8
*Mar  1 00:52:02.487: ISAKMP:(0:0:N/A:0):Can not start Aggressive mode, trying Main mode.
```

3.2.19-сурет – 12 кадам

13-кадам. Құрастырылған IPsec(3.2.20-сурет):

```
R1#show crypto ipsec policy
No policy exists


R1#show crypto ipsec transform-set
Transform set R1set: { esp-des esp-md5-hmac  }
   will negotiate = { Transport,  },


R1#show crypto ipsec client
% Incomplete command.

R1#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: R1map, local addr 200.100.10.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 200.100.10.10 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 200.100.10.2, remote crypto endpt.: 200.100.10.10
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:
```

3.2.20-сурет – 13 кадам

14-кадам. Нәтижесі 3.2.2 кестеде көрсетілген:

Кесте 3.2.2 – L2TP / IPsec нәтижесі

Орнату	Қарапайым
Шифрлау алгоритмі	3des
Аутентификация әдісі	ms-chap-v2, pre-share
Хэш мәні	Sha
Diffie Hellman идентификатор тобы	group 2
Орташа жылдамдық	30-40 mbit

3.2.3 IKEv2/IPsec

IKEv2/IPsec туннелдік протоколының теңшей бастаймыз:

1-кадам. IKE саясатын жасадым. Мұнда басымдылықты, аутентификацияның әдісін, хэш алгоритмін, шифрлау алгоритмін, Diffie-Hellman тобының идентификаторын, уақыт мәнін, кілт қауіпсіздігін беру мәнін көрсеттім(3.2.21-сурет):

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#hash md5
R1(config-isakmp)#encryption des
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#$mp key security address 200.100.10.10 255.255.255.252
```

3.2.21-сурет – 1 кадам

2-кадам. IPsec саясатын жасадым, ол үшін трафикті қалай қорғауды анықтайтын түрлендіру жиынтығын теңшедім(3.2.22-сурет):

```
R1(config)#crypto ipsec transform-set R1set esp-des esp-md5-hmac
```

3.2.22-сурет – 2 кадам

3-кадам. Қорғалған трафикті анықтау үшін кіру тізімін жасадым. Ол ушін Енді динамикалық қатынау тізімдерін бердім(3.2.23-сурет):

```
R1(cfg-crypto-trans)#$t ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
```

3.2.23-сурет – 3 кадам

4-кадам. Крипто картаны жасадым. Ол үшін криптографиялық картаға кіру тізімін тағайындадым. IPsec арқылы қорғалған трафикті қайта бағыттауға болатын бірдеңгейлі түйінің көрсеттім. Осы криптографиялық картаға қандай түрлендірулер жиынтығы рұқсат етілгенін көрсеттім. Басымдық реті бойынша бірнеше түрлендірулер жиынтығын енгізуге болады (біріншісі жоғары басымдылық). Сіз криптографиялық картада 6-ға дейін түрлендіру жиынтығын көрсете аласыз(3.2.24-сурет):

```
R1(config)#crypto map R1map 10 ipsec-isakmp
R1(config-crypto-map)#set peer 200.100.10.10
R1(config-crypto-map)#set transform-set R1set
R1(config-crypto-map)#match address 101
```

3.2.24-сурет – 4 кадам

5-кадам. Крипто карта жұмыс істейтін сыртқы портты көрсеттім(3.2.25-сурет):

```
R1(config)#interface serial 1/0
R1(config-if)#crypto map R1map
```

3.2.25-сурет – 5 кадам

6-кадам. Әдепкі маршрутты тіркедім(3.2.26-сурет):

```
R1(config)#ip route 0.0.0.0 0.0.0.0 200.100.10.1
```

3.2.26-сурет – 6 кадам

7-кадам. R1-ге түзету командасын бердім(3.2.27-сурет):

```
R1(config)#end
R1#
*May 17 22:04:09.115: %SYS-5-CONFIG_I: Configured from console by console
R1#debug crypto ipsec
Crypto IPSEC debugging is on
R1#debug crypto isakmp
Crypto ISAKMP debugging is on
```

3.2.27-сурет – 7 кадам

8-кадам. PC1-ден PC4-ке қосылуды тексердім(3.2.28-сурет):

```
PC1> ping 192.168.3.2
84 bytes from 200.100.10.10 icmp_seq=1 ttl=252 time=52.274 ms
84 bytes from 200.100.10.10 icmp_seq=2 ttl=252 time=47.014 ms
84 bytes from 200.100.10.10 icmp_seq=3 ttl=252 time=61.844 ms
84 bytes from 200.100.10.10 icmp_seq=4 ttl=252 time=57.954 ms
84 bytes from 200.100.10.10 icmp_seq=5 ttl=252 time=48.988 ms
```

3.2.28-сурет – 8 кадам

9-кадам. Құрастырылған ISAKMP-ны көрдім(3.2.29-сурет):

```
R1#ping 192.168.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#ping 192.168.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/220/624 ms
R1#
R1#show crypto isakmp
% Incomplete command.

R1#show crypto isakmp ?
  key      Show ISAKMP preshared keys
  peers    Show ISAKMP peer structures
  policy   Show ISAKMP protection suite policy
  profile  Show ISAKMP profiles
  sa       Show ISAKMP Security Associations

R1#show crypto isakmp key
Keyring              Hostname/Address                  Preshared Key

default              200.100.10.10  [255.255.255.252]   security
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               3600 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

3.2.29-сурет – 9 кадам

10-кадам. Құрастырылған IPsec-ты көрдім(3.2.30-сурет):

```
R1#show crypto ipsec security-association
Security association lifetime: 4608000 kilobytes/3600 seconds

R1#show crypto ipsec transform-set
Transform set hoset: { esp-des esp-md5-hmac  }
   will negotiate = { Tunnel,  },

Transform set R1SET: { esp-des esp-md5-hmac  }
   will negotiate = { Tunnel,  },
```

3.2.30-сурет – 10 кадам

11-кадам. Құрастырылған Crypto map-ты show crypto map командасы теріп көрдім(3.2.31-сурет):

```
R1#show crypto map
Crypto Map "R1MAP" 10 ipsec-isakmp
        Peer = 200.100.10.10
        Extended IP access list 101
            access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
        Current peer: 200.100.10.10
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                R1SET,
        }
        Interfaces using crypto map R1MAP:
                FastEthernet0/1
```

3.2.31-сурет – 11 кадам

12-кадам. Нәтижесі 3.2.3 кестеде көрсетілген:

Кесте 3.2.3 – IKEv2/IPsec нәтижесі

Орнату	Қарапайым
Шифрлау алгоритмі	Des
Аутентификация әдісі	pre-share
Хэш мәні	message digest 5
Diffie Hellman идентификатор тобы	group 2
Орташа жылдамдық	60-70 mbit

3.2.4 SSL VPN

1-кадам. Жаңа командаларды ұсыну үшін жаңа модельді іске қостым. Әдепкі бойынша локалды дерекқор үшін PPP аутентификациясын орнаттым(3.2.32-сурет):

```
R4(config)#aaa new-model
R4(config)#aaa authentication login SSLVPN local
```

3.2.32-сурет – 1 кадам

2-кадам. Өзі қол қойған сертификатты тіркедім(3.2.33-сурет):

```
R4(config)#crypto pki trustpoint TEST
R4(ca-trustpoint)#enrollment term pem
R4(ca-trustpoint)#subject-name CN=TEST
R4(ca-trustpoint)#revocation-check none
R4(ca-trustpoint)#rsakeypair TEST
R4(ca-trustpoint)#ex
R4(config)#
R4(config)#crypto pki enroll TEST
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=TEST
% The subject name in the certificate will include: R4
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [no]: n
Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIH9MIGoAgEAMCIxDTALBgNVBAMTBFRFU1QxETAPBgkqhkiG9w0BCQIWAlI0MFww
DQYJKoZIhvcNAQEBBQADSwAwSAJBAM3mDgA6sVbx+dbemiA+djNbEEnsB1Wx5G2R
h75jII35En1PZIZjgqo+ABmuVbbRO027qNTs4MSTar4dWtf0aNECAwEAAaAhMB8G
CSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb3DQEBBAUAA0EA
sofr/gkwfwrwaPp5SK0wLtbL211SCUDk/x1z3jAyKIoiWqNVipN9/G2rL0IwfwV/
28CGOMlNLDYvg8+pAzom4g==
-----END CERTIFICATE REQUEST-----
```

3.2.33-сурет – 2 кадам

3-кадам. Егер өздігінен қол қойылған enroll сертификат өтпегесін, онда біз өздігінен қол қойылған self-signer сертификатын тіркедім(3.2.34-сурет):

```
R4(config)#crypto pki certificate chain TEST
R4(config-cert-chain)#certificate ?
  WORD         Certificate serial number
  ca           CA certificate
  ra-encrypt   RA encryption certificate
  ra-general   RA general purpose certificate
  ra-sign      RA signing certificate
  rollover     Shadow rollover certificate
  self-signed  Self-signed certificate

R4(config-cert-chain)#certificate ?
  WORD         Certificate serial number
  ca           CA certificate
  ra-encrypt   RA encryption certificate
  ra-general   RA general purpose certificate
  ra-sign      RA signing certificate
  rollover     Shadow rollover certificate
  self-signed  Self-signed certificate

R4(config-cert-chain)#certificate self-signed 01 ?
  WORD  file specification
  <cr>

R4(config-cert-chain)#certificate self-signed 01 nvram:IOS-Self-Sig#2.cer
R4(config-cert-chain)#
*May 18 03:13:32.978: % Multiple self signed certificates in config
    certificate for trust point TEST ignored

R4(config-cert-chain)#ex
```

3.2.34-сурет – 3 кадам

4-кадам. HTTP және HTTPS серверіне рұқсат бердім(3.2.35-сурет):

```
R4(config)#ip http server
R4(config)#ip http secure-server
Failed to generate persistent self-signed certificate.
    Secure server will use temporary self-signed certificate.
```

3.2.35-сурет – 4 кадам

5-кадам. Webvpn gateway-ді теңшедім. IP интерфейсі пәрмені үшін интерфейстің орнына, тікелей 200.100.10.10 IP адресімен, порт 443 пәрменімен көрсеттім, Сонымен қатар, шифрлау алгоритімі мен траспойнт тесті қостым(3.2.36-сурет):

```
R4(config)#webvpn gateway GATE
R4(config-webvpn-gateway)#ip address 200.100.10.10 port 443
R4(config-webvpn-gateway)#http-redirect port 80
R4(config-webvpn-gateway)#ssl encryption 3des-sha1
R4(config-webvpn-gateway)#ssl trustpoint TEST
```

3.2.36-сурет – 5 кадам

6-кадам. Әрі қарай біз webvpn деп аталатын context өз gateway қостым, онда біз бұрын жасалған түпнұсқалық тізімді, сонымен қатар браузер арқылы порталға кірген кездегі сәлемдемені көрсеттім(3.2.37-сурет):

```
R4(config-webvpn-gateway)#webvpn context SSL
R4(config-webvpn-context)#ssl authenticate verify all
R4(config-webvpn-url)#url-list "URL List"
R4(config-webvpn-url)#heading "Login Pages"
R4(config-webvpn-url)#$ome Page" url-value "http://10.10.10.10&#8221;"
```

3.2.37-сурет – 6 кадам

7-кадам. Policy group теңшедім, ішінде webvpn context конфигурациясында топтан қандай клиенттердің трафиктің туннельге оралатынын көрсететін саясат тобын жасадым. Маршруттау үшін клиенттерде осы екі желінің жазбалары ғана пайда болады, бұл трафиктің шифрланған туннельге өтетіндігін көрсетеді және күту уақыты мен күту уақыты сеансы мәнін орнаттым, пайдаланушылардың ең көп санын көрсеттім және gateway іске қостым (3.2.38-сурет):

```
R4(config-webvpn-url)#policy group SSLVPN
R4(config-webvpn-group)#url-list "URL List"
R4(config-webvpn-group)#banner "Login Successful"
R4(config-webvpn-group)#hide-url-bar
R4(config-webvpn-group)#mask-urls
R4(config-webvpn-group)#timeout idle 300
R4(config-webvpn-group)#timeout session 3600
R4(config-webvpn-group)#default-group-policy SSLVPN
R4(config-webvpn-context)#gateway GATE
R4(config-webvpn-context)#max-users 50
R4(config-webvpn-context)#inservice
```

3.2.38-сурет – 8 кадам

9-кадам. Қосылуды тексердім(3.2.39-сурет):

```
PC1> ping 192.168.3.1
84 bytes from 192.168.3.1 icmp_seq=1 ttl=252 time=65.878 ms
84 bytes from 192.168.3.1 icmp_seq=2 ttl=252 time=73.486 ms
84 bytes from 192.168.3.1 icmp_seq=3 ttl=252 time=67.679 ms
84 bytes from 192.168.3.1 icmp_seq=4 ttl=252 time=71.577 ms
84 bytes from 192.168.3.1 icmp_seq=5 ttl=252 time=61.078 ms
```

3.2.39-сурет – 9 кадам

10-кадам. Құрастырылған ssl webvpn теңшесі(3.2.40-сурет):

```
R1    R4
crypto pki trustpoint TEST
 enrollment terminal pem
 subject-name CN=TEST
 revocation-check crl
 rsakeypair TEST
!
!
crypto pki certificate chain TEST
 certificate self-signed 01
        quit
username admin secret 5 $1$Lfxe$w6P6.AyInOkBmMoZGkpYE/
archive
 log config
  hidekeys
!
!
webvpn gateway SSLVPNGW
 ip address 192.168.3.1 port 443
 ssl trustpoint TEST
 inservice
!
webvpn gateway GATE
 ip address 200.100.10.10 port 443
 ssl encryption 3des-sha1
 ssl trustpoint TEST
 inservice
!
webvpn context SSL
 ssl authenticate verify all
!
 url-list "URL List"
   heading "Login Pages"
   url-text "R4 Router Home Page" url-value "http://10.10.10.10&#8221;"
!
!
 policy group SSLVPN
   url-list "URL List"
   banner "login Successful"
   hide-url-bar
   mask-urls
   timeout idle 300
   timeout session 3600
 default-group-policy SSLVPN
 gateway GATE
 max-users 50
 inservice
!
end

R4(config)#
solarwinds | Solar-PuTTY free tool
```

3.2.40-сурет – 10 кадам

11-кадам. Нәтижесі 3.2.4 кестеде көрсетілген:

Кесте 3.2.4 – SSL нәтижесі

Установка	Средний
Алгоритм шифрования	3des
Самоподписанный сертификата	self-signer
Хэш значения	sha1
Средняя скорость	6-10 mbit

4 VPN салыстыру және ұсыныстар

Тестілеуден өтіп, әрбір туннельдік протоколдарын талдай отырып, енді біз аталған туннельдік протоколдарының ішінен ең жақсы нұсқаны таңдау үшін оларды салыстырамыз.

4.1 Орнату

Орнатудың қарапайымдылығы әр қызметкер үшін басты артықшылық болып табылады, өйткені бағдарламалық жасақтаманы орнатудың қарапайымдылығы үлкен стратегияларды және қауіпсіздік саясатын тиімді құралға айналдыруға мүмкіншілік береді, бұл басқарудың айқындылығын арттыруға және басқару шешімдерін кепілдендірілген іске асыру тетігін алуға мүмкіндік береді.

GNS3 эмуляторында әр туннельдік протоколды орындау кезінде практикалық қиындықтар болған жоқ. Алайда, SSL VPN-ді теңшеу кезінде серверде сертификатқа қол қою кезінде қиын болды.

4.1-кестеде VPN орнату нәтижесі көрсетілген.

Кесте 4.1 – VPN-ды орнату нәтижесі

Туннельдік протокол	**Орнату деңгейі**
PPTP	Ең қарапайымы
L2TP / IPSEC	Қарапайым
IKEV2 / IPSEC	Қарапайым
SSL	Орташа

4.2 Қауіпсіздік

Пайдаланушы деректерінің қауіпсіздігін қамтамасыз ету - «site-to-site» кіру сценарийлерін пайдалану кезінде әрбір VPN алдында тұрған басты міндет болып саналады. Деректер Ғаламтор секілді қауіпті қоғамдық желілер арқылы берілсе, көптеген компаниялар үшін қауіпсіздік маңызды басымдыққа айналады. Пайдаланушылар VPN шешімін жобалау кезінде, жасалу керек алғашқы нұсқалардың бірі - нақтылы туннельдеу протоколына байланысты.

Қазіргі таңда, VPN туннельдеу протоколының қауіпсіздігін зерделеу және қорытындылау, ең негізгі мәселенің бірі.

PPTP, L2TP / IPsec, IKEv2 / IPsec, SSL сияқты туннельдік протоколдардың қауіпсіздігін зерделеу барысында келесі тұжырымдар жасалды.

4.2.1 PPTP

PPTP деректерді шифрлау үшін негізінен 128 биттік MMPE (Microsoft Point-to-Point Encryption) пайдаланады, бұл өте қауіпті. Ол корпорацияларға немесе коммерциялық мақсатта пайдалануға ұсынылмайды. Оны әлі де жаңа амалдық жүйелерде (Windows 10 қоса) табуға болатынына қарамастан, VPN протоколдары арасында PPTP ескірген болып саналады. Бұл құпиялылықты бірінші орынға қоятын пайдаланушыларға арналмаған, өйткені оның көптеген кемшіліктері бар.

Сонымен қатар, PPTP эусплойт тарихына ие, өйткені ол MS-CHAP v2-ні 128 биттік AES-ке дейін қолданды. Нәтижесінде, протокол әрине бақыланады, себебі бұндай шифрлауды NSA оңай бұза алады. Өкінішке орай, MS-CAP v2 әлі де пайдаланылуда.

Аутентификация туралы сөз болғанда тек сервер аты, пайдаланушы аты және пароль қажет.

4.2.2 L2TP / IPsec

L2TP шифрлауды және құпиялылықты қорғауды қамтамасыз етуге бекітілген функциялары жоқ. Мұндай функциялар жеке шифрлау протоколымен қорғалған, ал L2TP үшін ең көп таралған - IPsec (Internet Protocol Security), ол IPv4 желісі арқылы берілетін деректерді шифрлай алады. Сондықтан L2TP туннельмен қамтамасыз етеді, ал IPsec қауіпсіздікке қамқорлық жасайды.

IPsec - бірнеше шифрлау режимдерін қолданатын VPN протоколдарының бірі. Ол 128 биттік AES, 256 биттік AES және 3DES қолдайды. Олар қауіпсіздіктің жоғары деңгейін ұсынады, бірақ тек аутендификацияның дұрыс түрімен ғана орындалады (ешнәрсе ашық емес).

Көптеген жағдайларда L2TP / IPsec аутентификациясы ортақ кілттер, ашық кілттер немесе сертификаттар көмегімен жүзеге асырылады, бірақ одан да басқа әдістер бар. Аутентификацияның бұл түрі протоколды орнатуды жеңілдетеді, сондықтан ешқандай кодтау шеберлікті қажет етпейді.

4.2.3 IKEv2 / IPsec

PPT2P және L2TP / IPsec-пен салыстырғанда, IKEv2 / IPsec 128 биттік AES, 192 биттік AES және 256 биттік AES шифрлауды қолдана отырып, қауіпсіздікті жақсартады.

Аутентификация туралы сөз болғанда, IKEv2 X.509 алдын ала ортақ пайдаланылатын кілттерді немесе сертификаттарды қолданады, бұл конфигурацияны жеңілдетеді. Ол сонымен қатар әрбір қосылған компания үшін қауіпсіздік саясатын жасайды және қолдайды.

4.2.4 SSL / TLS

SSL-де қауіпсіздік кемшілігі бар, оның орнына TLS туннельдік протоколдарының жаңа жаңартылған нұсқасы ретінде келді. Бұл дерлік бірдей нәрсе, өйткені TLS - бұл SSL жаңартылған нұсқасы және оның атауын алады. Сондықтан, қауіпсіздікті қамтамасыз ету үшін TLS туннельдік протоколын таңдау керек.

TLS архитектурасы оңай сіңіріледі. Ол екі деңгейден тұратын екі бағытты қорғауды қамтамасыз етеді: біреуі қосылымның жеке және тұрақты екендігіне көз жеткізу үшін (TLS жазу протоколы), ал екіншісі берілуге дейін деректерді шифрлау үшін (TLS қол қою протоколы), сондықтан қауіпсіздікті қамтамасыз ету үшін TLS туннельдік протоколын таңдау керек.

Шифрлауға келер болсақ, TLS E2EE (тіке шифрлау) қолданады, бұл мәліметтер басқа тараптардан, соның ішінде Ғаламтор-провайдерлерден және хакерлерден қорғалатындығына байланысты қауіпсіздіктің жоғары деңгейін қамтамасыз етеді.

Аутентификацияны алдын-ала ортақ кілттер немесе симметриялық шифрлау үшін сандық сертификаттар көмегімен жүзеге асыруға болады.

4.3 Жылдамдық

VPN қызметі пайдаланушының қауіпсіздігі мен анонимділігін ғана емес, сонымен қатар кез-келген VPN қызметінің маңызды аспектілерінің бірі қосылу жылдамдығы болып табылады. Сонымен қатар, VPN жылдамдығы, оның жұмысының көптеген факторлар әсер етеді.

VPN жылдамдығын бір түпнұсқа хосттан екінші соңғы хостқа сынау кезінде ол келесі нәтиже берді:

4.3.1 PPTP

PPTP құпиялылықтың төмен деңгейіне және тұрақты Ғаламтор байланыстарына байланысты оның жылдамдығы өте тұрақты. PPTP Netflix, BBC iPlayer және Amazon Prime сияқты желідегі ағындарға қол жетімділік үшін тамаша таңдау. Қауіпсіздікпен алаңдамаған кезде, процессор қуаты шектеулі ескі компьютерлерде, әсіресе роутерлерде де қолдануға болады.

4.3.2 L2TP / IPsec

L2TP / IPsec барлық VPN-дің ең нашар жылдамдығына ие, өйткені UDP (ядро негізіндегі жеделдету) арқасында жақсы Ғаламтор жылдамдығы қамтамасыз етіледі. Сонымен бірге, мәліметтердің инкапсуляциясы, процессордың көбірек өңдеу қуатын қажет ететіндігіне байланысты жылдамдық төмендейді.

4.3.3 IKEv2 / IPsec

IKEv2 / IPsec барлық VPN ішіндегі ең жоғары жылдамдыққа ие. Бұл екі тапсырма бөлек орындалғандықтан, бұл желінің жұмысына әсер етпейді,

сондықтан да жоғары жылдамдыққа әкеледі.

4.3.4 SSL

SSL-де жақсы жылдамдық бар, бірақ процессордың жоғары қуатына байланысты, бұл, әдетте, жылдамдық пен өнімділіктің төмендеуіне әкеледі. Дегенмен, бұл үшін SSL үдеткіштерін пайдалану немесе трафиктің басымдықтарын орнату сияқты жолдарымен шешуге болады.

4.4 Ұсыныс

VPN туннелдеу протолдарының нәтижесі 4.4-кестеде көрсетілген. VPN қолдана отырып, IKEv2 / IPSEC ұсынамын, өйткені қауіпсіздік үшін IKEv2 / IPSEC қауіпсіз болып табылады, бірақ IPSEC-тің кемшіліктері байланысты өзіндік кемшіліктерге ие. Site-to-site VPN-де деректерді беру жылдамдығына байланысты ең жоғары жылдамдыққа ие. Ал орнату қарапайым, қосымша дағдылар қажет етпейді.

Кесте 4.4 – VPN туннельдеу протолдарының салыстыру нәтижесі

	PPTP	**L2TP/IPSEC**	**IKEv2/IPSEC**	**SSL**
Орнату	Орнату қарапайым	Орнату қарапайым	Орнату қарапайым	Орнату орташа
Қауіпсіздік	Қауіпсіздік өте төмен, бұл тізімдегі ең нашары	PPTP-ден гөрі қауіпсіздігі орташа	PPTP және L2TP / IPSEC қарағанда қауіпсіздігі жақсы	PPTP және L2TP / IPSEC қарағанда қауіпсіздігі жақсы
Жылдамдық	Үлкен жылдамдық-қа ие, бірақ IKEv2 / IPsec қарағанда баяу	Орташа жылдамдық екі рет капсуляциялау себебінен PPTP-ден нашар	Тамаша жылдамды қ, осы тізімдегі ең жақсы.	Жылдамдық-тың төмендеуі
Тұрақтылық	Өте тұрақты	Тұрақты	Өте тұрақты	Тұрақты

ҚОРЫТЫНДЫ

VPN Ғаламтор сияқты қауіпсіз қоғамдық желілер арқылы қауіпсіз, жеке, ішкі желіге қол жеткізуді қамтамасыз етеді. Бұл жұмыста VPN-нің бірқатар туннельдеу протоколдарын, практикалық тұрғыда салыстыра отырып, IKEv2 / IPsec туннельдеу протоколы тиімді екенін түсіндік.

IKEv2 / IPSec - бұл ең жылдам және қауіпсіз VPN протоколы. Бұл VPN қауіпсіз байланысын, байланыс жоғалғанда немесе сіз желілерді ауыстырған кезде де қолдана алады. Оның негізгі қолданылуы ұялы желілерге арналған.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Imam Riadi. Analysis of Security Virtual Private Network (VPN) Using OpenVPN / Yogyakarta. 2019. – б.59-65.

2 Configure Cisco Router for Remote Access PPTP VPN Connections // Сайттағы электрондық нұсқа https://aaronwalrath.wordpress.com/2008/05/12/configure-cisco-router-for-remote-access-pptp-vpn-connections/

3 SSL VPN Clientless & Thin Client Configuration // Сайттағы электрондық нұсқа https://cjnetworks.wordpress.com/tag/ssl-vpn-in-gns3/

4 Getting Started with GNS3 // Сайттағы электрондық нұсқа https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html

5 Configure a Site to Site VPN in Cisco Routers Using GNS3 // Сайттағы электрондық нұсқа https://www.chennaicisco.com/2013/11/configure-site-to-site-vpn-in-cisco.html

6 PPTP Router Configuration // Сайттағы электрондық нұсқа https://www.cisco.com/c/en/us/support/docs/ip/point-to-point-tunneling-protocol-pptp/29781-pptp-ios.html

7 How to Identify Affected Products // Сайттағы электрондық нұсқа https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/215118-ios-self-signed-certificate-expiration-o.html

8 VPN Protocols Breakdown: PPTP, L2TP/IPsec, IKEv2/IPsec, OpenVPN, and Others // How to Identify Affected Products // Сайттағы электрондық нұсқа https://www.findyourvpn.com/vpn-protocols/

9 Phil Benn. Site to Site Virtual Private Networks (VPNs): Good Practice Guidelines / West Yorkshire. 2006. – б.5-13.

10 Tiamiyu A. Osuolale. TRUSTED ROUTING VS. VPN FOR SECURED DATA TRANSFER OVER IP-NETWORKS/ INTERNET / Saint Petersburg. 2018. – б.63-69.

11 Zeeshan Ashraf. Virtual Private Networks in Theory and Practice / German. 2018 – б.10-21, 44-72, 161-169.

12 The Government of Special Administrative. VPN SECURITY / the Hong Kong. 2008. – б.8-14.