ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті» коммерциялық емес акционерлік қоғамы

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

Қоныс Салтанат Қонысқызы

Cisco Packet Tracer-де кәсіпорын желісінің периметрін қорғауды модельдеу

ДИПЛОМДЫҚ ЖҰМЫС

6В06201– Телекоммуникациялар білім беру бағдарламасы

Алматы 2023

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті» коммерциялық емес акционерлік қоғамы

Автоматика және телекоммуникациялық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
техн.ғыл.кандидаты
_____ Е.Таштай
«___» _____ 2023 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы «Cisco Packet Tracer-де кәсіпорын желісінің периметрін қорғауды модельдеу »

6В06201 – Телекоммуникациялар мамандығы

Орындаған: С.Қоныс

Рецензент
Халықаралық ақпараттық
технологиялар университеті
т.ғ.к., кафедра меңгерушісі
_____ Бахтиярова Е.А
«___» _____ 2023 ж.

Ғылыми жетекші
_____ Марксұлы С. т.ғ.м
ЭТжГТ каф.аға оқытушысы
«__1__» ___06___ 2023 ж.

Алматы 2023

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті» коммерциялық емес акционерлік қоғамы

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

6В06201 Телекоммуникация

БЕКІТЕМІН
Кафедра меңгерушісі
_____ Е. Таштай
«___» _____ 2022 ж.

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы Қоныс Салтанат Қонысқызы

Тақырыбы: «Cisco Packet Tracer-де кәсіпорын желісінің периметрін қорғауды модельдеу»

Университет ректорының*«23»қараша 2022 ж. №408-П/Ө бұйрығымен бекітілген.*
Аяқталған жұмысты тапсыру мерзімі «30» сәуір 2023 ж.
Дипломдық жұмыстың бастапқы берілістері:
1) Корпоративтік желіні дамыту және кәсіпорын желісінің периметріндегі CISCO ASA SERIES құрылғысын желілік қауіп қатерден қорғау қауіпсіздігі;
2) Корпоративтік желіні құру үшін қажетті құрылғылардың сипаттамасы;
3) Желінің пайдалы өткізу қабілеттілігі 300 Мбит/с дейін және тарату пакетін жіберу;
4) CiscoFPR1120-ASA-K9 жабдығы негізінде CiscoPacketTracer жүйесінде жұмыс істейтін корпоративтік желі периметрі қорғанысын моделі.

Дипломдық жұмыста қарастырылатын мәселелер тізімі:
а) Корпоративтік желіні қорғаудың мәселелерін және олардың шешімдерін табу;
б) Корпоративтік желіні құруға арналған құрылғыларды таңдау;
в) Ортақ кілттермен жұмыс істеу үшін IPSecVPN хаттамаларының құралдарын талдау;
г) Корпоративтік желінің өткізу қабілетін және тарату пакетін жіберуді есептеу;

Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс):
Ұсынылатын негізгі әдебиеттер: *1)* "Network Perception," 2020. [Online]. Available: https://www. network-perception.com/np-view//
2) P. Wlazlo, K. Price, C. Veloz, A. Sahu, H. Huang, A. Goulart, K. Davis, and S. Zounouz, "A cyber topology model for the texas 2000 synthetic electric power grid," in 2019 Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm). IEEE, October, 2019.

дипломдық жұмысты (жобаны) дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
Диплом жұмысының тақырыбын талдау	04.01.2023 - 01.02.2023	Әдебиеттік шолу бойынша 2 беттік слайд
Теориялық ақпарат	01.02.2023 - 01.03.2023	Салыстырмалы талдаулар мен математикалық талдау бойынша 3-4 беттік слайд
Жабдықтар жұмысының есебі және жұмысты рәсімдеу	01.03.2023 - 30.05.2023	Құрылғылар немесе бағдарламалау бойынша зерттеуді ұсыну. 3-4 беттік слайд

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
Диплом жұмысының тақырыбын талдау	Марксұлы С, т.ғ.м ЭТжҒТ каф.аға оқытушысы	1.03.2023 ж.	
Теориялық ақпарат	Марксұлы С, т.ғ.м ЭТжҒТ каф.аға оқытушысы	30.03.2023 ж.	
Норма бақылау	Ақылжан П.Б. т.ғ,м ЭТжҒТ каф. ассистентті, т.ғ.м.	01.06.2023	

Ғылыми жетекшісі Марксұлы С.

Тапсырманы орындауға алған білім алушы Қоныс С.

Күні «22» желтоқсан 2022 ж.

МАЗМҰНЫ

АНДАТПА

Бітіру жобасы периметрді қорғауды ұйымдастыруға арналған "ASUE" компаниясының Корпоративтік желісінің адаптивті құрылғысы негізінде ішкі желіні сыртқы желіден қорғау мақсатында Cisco ASA series қорғау әсер ету, кіріс және шығыс қол жеткізуді бақылау, қауіпсіз ұйымның бас кеңсесі мен филиалдары арасындағы өзара іс-қимыл, сондай-ақ аутентификация, авторизация және практика жүйесін жетілдіру.

Желінің қауіпсіздігі мен негіздемесінің жалпы мәселелері қарастыру үшін Cisco ASA series құрылғысын таңдау.Жобада экономикалық сипаттағы мәселелер қарастырылған: тиімділік осы жобаны енгізу және оны іске асыру құны.

АННОТАЦИЯ

Дипломный проект основан на адаптивном устройстве корпоративной сети компании «ASUE» для организации охраны периметра, с целью защиты внутренней сети от внешней сети, совершенствования системы аутентификации, авторизации и практики.

Выбор устройства серии Cisco ASA для рассмотрения общих вопросов сетевой безопасности и обоснования.В проекте рассматриваются экономические вопросы: эффективность реализации данного проекта и стоимость его реализации.

ANNOTATION

The diploma project is based on the adaptive device of the ASUE corporate network for organizing perimeter security, in order to protect the internal network from the external network, improve the system of authentication, authorization and practice.

Choice of the Cisco ASA series device to consider general network security issues and justification. The project addresses economic issues: the effectiveness of the implementation of this project and the cost of its implementation.

In practice, CiscoPacketTracer assembled part of a large network consisting of routers connected in a ring topology, where an authorization server is connected to one of the routers. An aggregation network switch is connected to the routers, and access network switches are connected to it.

StaticNAT and dynamic NAT technologies were used to organize data transfer, VoIP-telephony was configured. Internet access to internal servers with media content on the network is also organized, authentication via PPPoE is organized.

КІРІСПЕ

Қазіргі таңда жаңашыл жергілікті желілер көлемі күрт көбеюі байқалды, бұл желілерді тұтынушылар саны және пайдалынушылығы желілер кеңейіп келеді. Қойылатын талаптар да өсуде берілетін трафикке, өткізу қабілеттілігіне, ұзақтығына (ауқымдылығына), ақпаратты қорғауға (деректерді беруге) және желіні әзірлеу мен өрістету құнына, сондай-ақ ақпараттың қауіпсіздігі мен жергілікті желінің құнына кез келген компанияны құру мен дамытудың маңызды стратегиялық факторына айналады.

Қазір ақпараттық көздерде ақпаратты қорғау жүйесін құру кезінде жүйелік тәсіл ұғымы жиі кездеседі. Бұл жүйелілік ұғымы тек тиісті қорғаныс механизмдерін құру ретінде қарастырылмайды, бірақ тұрақты болып табылады, өмірлік циклдің барлық кезеңдерінде жүзеге асырылатын тірі процесс ақпараттық жүйе.

Ақпаратты қорғауды арттыру және көбейту міндетінен басқа желінің магистральдық құрамдас бөлігінің өткізу қабілеттілігі өзекті болып табылады. Ақпараттық қол жетімділіктің міндеті, негізгі талаптары:

1) Корпоративтік желіні дамыту және кәсіпорын желісінің периметріндегі CISCO ASA SERIES құрылғысын желілік қауіп қатерден қорғау қауіпсіздігі;

2) Корпоративтік желіні құру үшін қажетті құрылғылардың сипаттамасы;

3) Желінің пайдалы өткізу қабілеттілігі 300 Мбит/с дейін және тарату пакетін жіберу;

4) CiscoFPR1120-ASA-K9 жабдығы негізінде CiscoPacketTracer жүйесінде жұмыс істейтін корпоративтік желі периметрі қорғанысын моделі.

Дипломдық жобада компаниялардың ақпараттық жүйесін қорғауға мүмкіндік беретін заманауи Cisco ASA series жабдықтары негізінде желінің периметрін қорғау жүйесі жасалды. Жобаның негізгі міндеті экономикалық тиімділікті бағалау және ақпараттық құрылымды қорғаудың жолға қойылған тетігін құру арқылы сыртқы қатерлерден ақпарат пен ақпараттық көздердің қауіпсіздігін қамтамасыз ету. Дипломдық жоба Cisco ASA series аппараттық конфигурациясының негізгі мәселелерін қарастырады.

1 Корпоративтік желі

Корпоративтік желі-негізгі мақсаты осы ұйымның тиімді ішкі және сыртқы жұмысын құру болып табылатын кез келген ұйымның құрылымдық желісі. Бұл іс жүзінде ғаламдық желінің әсерінен жергілікті желілердің өзара байланысты жиынтығы. Бұл желіні пайдаланушылар тек осы ұйымның қызметкерлері болып табылады.

1.1 Корпоративтік желінің қауіпсіздігі

Корпоративтік желінің қауіпсіздік жүйелерін әзірлеу кезінде қауіптер өрісінің динамикасы және олардан болуы мүмкін залал, сондай-ақ оған шабуылдарды бейтараптандыру үшін желі құрылымындағы қорғаныс механизмдерін пайдаланудың қарқындылық дәрежесінің қажеттілігі бағаланадыКорпоративтік желіні тестілеуден кейін вирустық шабуылдарды болжау, зиянды кодты зерттеу және оны жою бойынша бірқатар алдын алу шаралары жүзеге асырылады.

1.2 Желі қауіпсіздігіне қауіп төндіретін мәселелер

1.2.1 Желіні қорғау қажеттілігі

Ғаламторды тарату қалай ойлайтынымызды тез өзгертеді және бизнес жүргізу, оқу, өмір сүру және демалу керек екендіінде. Ғаламдық бизнес жетекшілерә XXI ғасырда өз ұжымының өміршеңдігі мен бәсекеге қабілеттілігі арттыру үшін ғаламтордың алар орнын рөлі сөзсіз мойындайды. Қолданушылар мен соңғы пайдаланушылар байланыс пен электрондық бәсекенің нақты қорғалған құралдарына иемденгісы келеді. Өкінішке орай, Ғаламтор бастапқыда ашық ғаламторға негізделген қарапайымдылығын қамтамасыз ететін стандарттар қорғаудың кейбір негізгі компоненттерін жіберіп алды, мысалы, қашықтан қол жеткізуді басқару, байланыс құпиясы және қызмет көрсетудегі кедергілерден қорғау. Ғаламтордағы коммуникацияларды қорғау пайдалылығын барлық желілерді қорғау технологиялардың жылдам дамуына негіз болды.

Хакерлі әдістердің пайда болуынан қорғанысты бұзу қаупінің тұрақты өсуі жағдайында кәсіптің әлсіздігін әлсірету үшін қорғаныс құралдары мен түрлеріне қарай жүзеге асыруға және жетілдіруге болатындығы туралы қорқынышты мәселе іскер топтардың алдында тұр. Желілік қауіпсіздік мәселесінің барлығына сәйкес шешімін ұсыну қиын, өйткені жергілікті желі үшін оқумекемелер бір ғана шешім, ал ғаламдық желі үшін тиімді болуы мүмкін- мүлдем басқа. Кейбір қорғаныс шешімдері шағын бизнес үшін жақсы,бірақ олар үлкен ұйымдар үшін қолайсыз болып шығады еңбек

сыйымдылығы, тым жоғары шығындар немесе шамадан тыс уақыт шығындары,мұндай шешімдерді үлкен желілерде іске асыру үшін қажет.

Қазіргі таңғы кәсіптің басында тұрған қорғалыс себебі жеткілікті шешімдердің барлық спектрін қарастырылуы және анығын таңдау міндетіне дейін азаяды. Бүгінгі кезде көптеген технологиялар мен қорғаныс жабдықтары ұсынылады. Желіні қорғауды жүзеге асырудың қиындығы мынада тиісті қорғаныс технологиясы жоқ, және сіздің бизнесіңіздің белгілі бір желісі мен талаптарына сәйкес келетін және тиісті жеткізуші ұсынатын қорғаныс жабдықтарын қолдау мен қорғау шығындары аз болатын көптеген шешімдерді қарастыруда.

Желілік инженер желілік орта үшін тиісті қорғаныс жиынтығын таңдағаннан кейін, осының бәрін тиісті кәсіпорын шеңберінде біріктіретін және бүгінгі жағдайда біртұтас және келісілген қорғаныс саясатын жүзеге асыруды қамтамасыз ететін құралдар қажет болады бұл өте қиын бизнес.

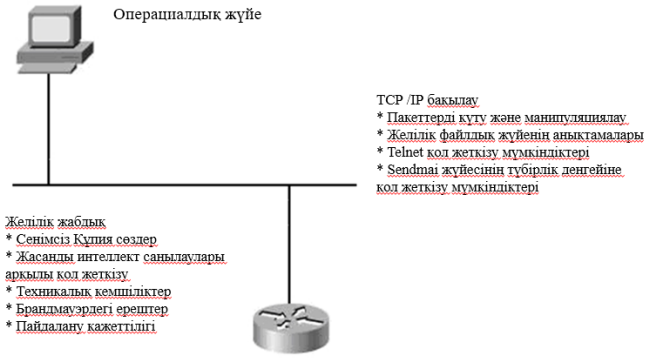
1.2.2 Қорғаныс проблемаларының пайда болу себептері

Ішкі желіге кіру, қашықтан қол жеткізу және ғаламторға кіру бүгінде кеңінен қолданылады. Бірақ бұл белгілі бір тәуекелді тудырады және бірқатар қауіпсіздік мәселелерін тудырады. Әлемде бар адамдар бар белгілі кемшіліктерді пайдалану үшін жеткілікті біліктілік және кейде материалдық қызығушылық қорғауды, үнемі жаңаларын ашу және пайдалану. Желіні қорғау қаупінің кем дегенде үш негізгі пайда болу себебі бар:

- Технологиялық кемшіліктер. Әрбір желі мен әрбір компьютерлік технологияның өзіндік қорғаныс мәселелері бар.
- Конфигурацияның кемшіліктері. Тіпті ең сенімді қорғаныс технологиясы дұрыс енгізілмеуі немесе пайдаланылмауы мүмкін, нәтижесінде қорғаныс проблемалары пайда болуы мүмкін.
- Қорғау саясатының кемшіліктері. Жарамсыз немесе дұрыс жүзеге асырылмаған қорғаныс саясаты тіпті ең жақсы желілік қорғаныс технологиясын осал етуі мүмкін.

1.2.3 Технологиялық кемшіліктер

Компьютерлік және желілік технологиялардың қорғаудың ішкі проблемалары бар. TCP/IP операциялық жүйелеріне тән кемшіліктерді қарастырыңыз және желілік жабдықты. (1.1-сурет).



1.1-сурет – Желілік және компьютерлік қорғаудың технологиялық кемшіліктерікомпоненттері

1.2.4 TCP/IP кемшіліктері

TCP/IP хаттамасы желіні жеңілдету мақсатында ашық стандарт ретінде жасалған. Осы протоколға негізделген оның функциялары, құралдары мен утилиталары да ашық коммуникацияларды қолдауға арналған. TCP/IP және онымен байланысты қызметтерді сипаттайтын кейбір кемшіліктерді қарастырайық.

- IP, TCP және UDP пакеттерінің тақырыптарында кемшіліктер бар, сонымен қатар жіберушіні анықтау мүмкін болмайтындай олардың мазмұнын жасырын оқу, өзгерту және ұстап алу мүмкіндігі бар.
- Желілік файлдық жүйе (NTFS) NFS пайдаланушы хосттарына аутентификацияны қамтамасыз етпей және байланыс сеанстары үшін кездейсоқ UDP порт нөмірлерін пайдаланбай рұқсатсыз кіруге мүмкіндік береді, бұл протоколға пайдаланушының қол жеткізуін нақты шектемейді.
- Telnet пайдаланушы үшін қуатты құрал болып табылатын әртүрлі Интернет утилиталары мен қызметтеріне қол жеткізу мүмкіндігін береді. Қауіпсіздігі жеткіліксіз деп саналатын қызметтермен интерактивті сөйлесуді бастау үшін шабуылдаушылар Telnet қызметін пайдалана алады және порт нөмірін хост атымен немесе IP мекенжайымен бірге көрсете алады.
- UNIX sendmail демоны операциялық жүйенің түбірлік деңгейіне қол жеткізуге мүмкіндік береді, бұл қажет емес және жеткізуге мүмкіндік береді. Sendmail — Unix жүйесінде электрондық поштамен алмасуға арналған бағдарлама. Оның қауіпсіздік мәселелерінің ұзақ тарихы бар. Мұнда олардың кейбіреулері бар:
- Шабуыл жасаушылар жалған электрондық пошта хабарларын жіберу үшін sendmail ішіне тиісті пәрмендерді енгізу арқылы UNIX жүйесінің түбірлік деңгейіне қол жеткізе алады.

- Sendmail қайтарылған нұсқа нөмірі және жалған хабарламалар арқылы бағдарлама жұмыс істейтін операциялық жүйенің түрін анықтауға мүмкіндік береді. Бұл ақпаратты белгілі бір операциялық жүйедегі осалдықтарға шабуыл жасау үшін пайдалануға болады.
- Sendmail берілген домендік атқа жататын хосттарды анықтау үшін пайдаланылуы мүмкін.
- Sendmail поштаны рұқсат етілмеген мекенжайларға жіберу үшін пайдаланылуы мүмкін. Барлық операциялық жүйелер
- Олардың кемшіліктері бар және олардың әрқайсысында қауіпсіздік мәселелері бар. Linux, UNIX, Microsoft Windows 2000, Windows NT, Windows 98, Windows 95 және IBM OS/2 белгілі және құжатталған кемшіліктерге ие. Сондай-ақ, желілік жабдықтың өзіндік қауіпсіздік кемшіліктері бар, оларды да анықтау және жою қажет.

Бұл кемшіліктерді жою үшін тиісті шараларды қабылдау талап етіледі. Мұндай әлсіздіктердің мысалдары әлсіз құпия сөзді қорғауды, аутентификация құралдарының жоқтығын, маршруттау протоколдарындағы қауіпсіздік мәселелерін және табуға болатын желіаралық қалқандардың осалдықтарын қамтиды. Көптеген желілік жабдық өндірушілері операциялық жүйеге бағдарламалық немесе аппараттық жаңартулар арқылы анықталған қауіпсіздік кемшіліктерін дереу түзетеді. Осалдықтар рұқсат етілмеген пайдаланушыларға кіру кезінде рұқсатсыз кіруге немесе артықшылықтарды көтеруге мүмкіндік береді. Бұл аппараттық немесе бағдарламалық құралдың ақауларына байланысты болуы мүмкін.

Олқылықтар рұқсат етілмеген пайдаланушыларға рұқсатсыз кіруге немесе жүйеге кіру артықшылықтарын арттыруға мүмкіндік береді. Мұның себебі аппараттық құралдардың немесе бағдарламалық жасақтаманың ақауы болуы мүмкін.

1.3 Конфигурацияның кемшіліктері

1.2-суретте көрсетілген конфигурациямен байланысты кемшіліктер бар, олар техникалық аспектілерге қатысты. Бұл кемшіліктер мәселені шешу үшін пайдаланылатын желілік жабдықтың дұрыс конфигурацияланбауына байланысты туындайды. Конфигурацияның кемшіліктері белгілі болса, оларды ең аз шығынмен оңай түзетуге болатынын ескеру маңызды.

1.2-сурет – Дұрыс конфигурацияланбау немесе жабдықты дұрыс пайдаланбау салдарынан туындайтын қорғаныс мәселелері

Конфигурацияның кемшіліктерінің кейбір мысалдары:

Бастапқы қондырғылармен қамтамасыз етілген қорғаныс жеткіліксіз.Көптеген өнімдердің бастапқы қондырғылары қорғаныс жүйесіндегі кемшіліктерді ашық қалдырады. Пайдаланушылар фирмамен кеңесу керек-өндіруші немесе пайдаланушылар қауымдастығы қандай бастапқы параметрлер қорғаныстың әлсіздігін тудыратыны және оларды қалай өзгерту керектігі туралы.

Желілік жабдықтың дұрыс конфигурациясы. Жабдықтың дұрыс конфигурациясы елеулі қорғаныс мәселелерін тудыруы мүмкін. Мысалы, кіру тізімдерінің, маршруттау протоколдарының немесе SNMP топтық жолдарының дұрыс емес құрылымы қорғаныс жүйесіндегі кең олқылықтарды ашуы мүмкін.

Қорғалмаған пайдаланушы тіркелгілері. Егер пайдаланушы тіркелгісі туралы ақпарат желі арқылы ашық түрде берілсе, бұл шабуылдаушыларға пайдаланушы имен мен құпия сөздерді пайдалануға мүмкіндік береді.

Тым қарапайым құпия сөздерді қолданатын пайдаланушы тіркелгілері. Бұл кең таралған мәселе пайдаланушылардың шектеулі жиыннан оңай болжанатын құпия сөздерді таңдауынан туындайтын опциялар. Мысалы, NetWare, UNIX және Windows NT жүйелерінде guest пайдаланушы аты мен guest құпия сөзі бар есептік жазбалар болуы мүмкін.

Интернет қызметтерін дұрыс конфигурациялау. Жалпы мәселе-Java және JavaScript-ті web шолғышында қолдану, Бұл зиянды Java апплеттерін енгізу шабуылдарының мүмкіндіктерін ашады. Желілік жабдық немесе компьютердің операциялық жүйесі желіге қашықтан қол жеткізуге мүмкіндік беретін қорғалмаған TCP/IP қызметтерін пайдалануға мүмкіндік береді.

1.4 Желілік қауіпсіздік қатерлерінің түрлері

Қауіпсіздікке төнетін қауіптердің ауқымы соншалықты кең, сондықтан оларды толық жіктеуге және олардан қорғаудың тамаша жүйесін жасауға мүмкіндік жоқ. Желінің қауіпсіздігіне қауіп төндіретін ең көп таралған түрлерін қарастырыңыз.

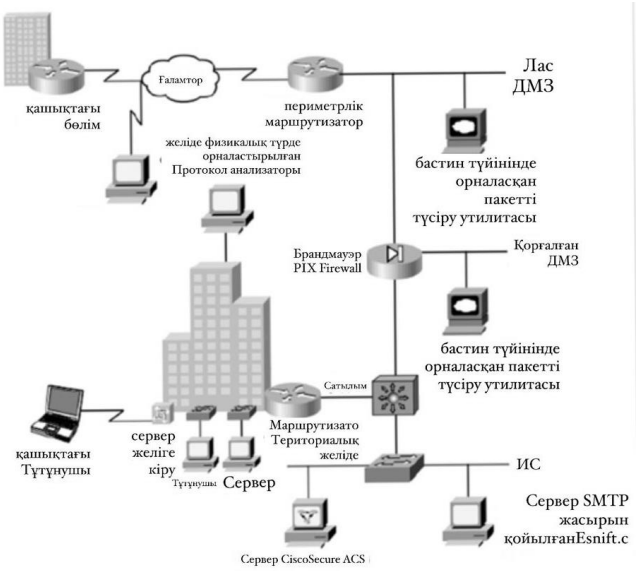
Желіде орын алуы мүмкін қажетсіз әрекеттер бар:

- Рұқсат етілмеген қол жеткізу.
- Құлыптау қызметі.
- Деректердің бұрмалануы.

Бұл қауіп санаттары желінің осалдықтарын көрсетеді және біреуге тиісті желі нысандарына қарсы дұшпандық әрекеттер жасауға мүмкіндік береді. Бұл әрекеттер орындалатын компьютердің белгілі бір сипаттамалары бар. Бұл жағдайда дұшпандық әрекет сценарийлер немесе бағдарламалар арқылы осалдықты пайдалануға бағытталған арнайы процедура болып табылады. Мұндай әрекеттердің мақсаты қолда бар ақпаратты жинау (барлау), заңды пайдаланушыға қызмет көрсету жүйесін бұғаттау, объектілер мен деректерге рұқсатсыз қол жеткізу немесе деректерді бұрмалау болуы мүмкін

1.4.1 Барлау

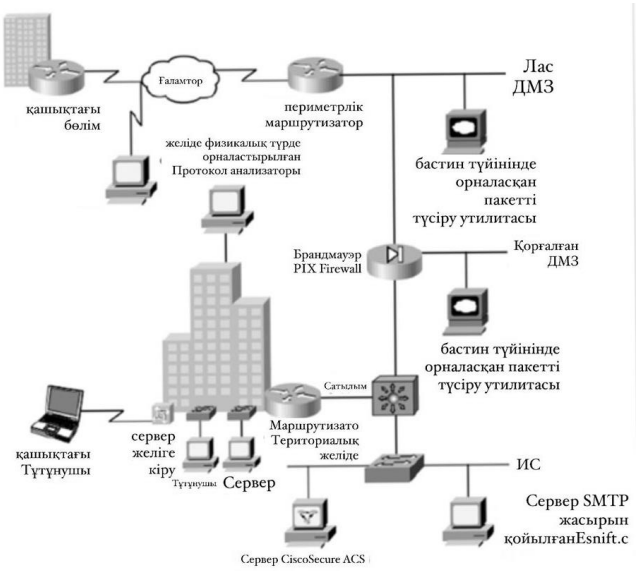
Барлау-бұл желінің құрылымын рұқсатсыз анықтау, оның картасын құру және жүйелерді, қызметтерді және желінің осалдық нүктелерін бақылау. Оған желілік трафикті бақылау да кіреді. Барлау белсенді немесе пассивті болуы мүмкін. Барлау шабуылдарынан алынған ақпаратты сол желіде басқа типтегі шабуылдар жасау үшін немесе маңызды деректерді ұрлау үшін пайдалануға болады. Барлау шабуылдары мақсаттарды анықтау, хабарламаларды ұстау және ақпаратты ұрлау түрінде болуы мүмкін. 1.3-суретте кәсіпорын желісінің қай нүктелерінде барлау шабуылдарын жүргізуге тырысуға болатындығы көрсетілген.



1.3-сурет — Барлау шабуылдарын жүргізу нүктелері

1.4.2 Құлыптау қызметі

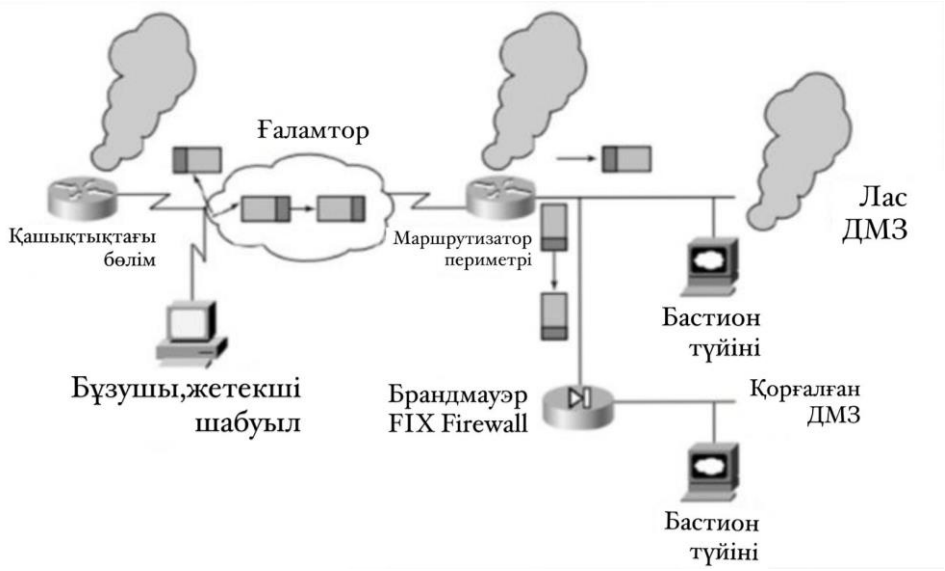
Желідегі компьютерлерге немесе желілік құрылғыларға рұқсатсыз қашықтан қол жеткізу шабуылдаушының әрекеті болуы мүмкін. Мұндай хакерлердің негізгі мақсаты мақсатты компьютерде түбірлік артықшылықтарды (UNIX жүйелерінде) немесе әкімшілік құқықтарды (Windows жүйесінде) алу болып табылады. Бұл оларға мақсатты жүйені көбірек басқаруға немесе желідегі басқа компьютерлерге қол жеткізуге мүмкіндік береді..



1.4-сурет — негізгілері көрсетілген бұзушы мүмкін болатын желі нүктелері рұқсатсыз қол жеткізу.

1.4.3 Қызметті бұғаттау

Бұған қоса, бұғаттау қызметтері жүйенің осалдығын тексеру әдісі ретінде, сондай-ақ рұқсатсыз кіру іздерін бүркемелеу үшін келесі шабуылдарға дейінгі қадам ретінде пайдаланылуы мүмкін. IP протоколы сервистік блоктау шабуылдарына айтарлықтай осалдықты ұсынады және мұндай шабуылдардың көптеген түрлері бар. Қызметтерді бұғаттау - бұл вандализмнің бір түрі, оны орындау салыстырмалы түрде оңай. Қызметті блоктау шабуылдары периметрлік маршрутизаторға, негізгі хостқа немесе брандмауэрге қарсы бағытталуы мүмкін. Қызметті блоктау шабуылдары периметрлік маршрутизаторға, Бастион түйініне немесе брандмауэрге қарсы бағытталады.



1.5-сурет — сервисті бұғаттау шабуылдарын жүргізу нүктелері

Қызметті блоктау шабуылдары болуы мүмкін орындар

1.4.4 Деректердің бүлінуі

Шабуылдаушы байланыс арнасы арқылы берілетін деректерді ұстап, өзгерте және қайта жасай алады. Деректердің бүлінуі, сонымен қатар жалғандық ретінде белгілі, IP мекенжайын өзгертуі, сеансты қабылдау үшін хабарларды қайта жіберу, маршруттау параметрлерін өзгерту және жіберілген хабарлардың мазмұнын өзгерту мүмкін. Деректерді бұрмалау сонымен қатар веб-вандализмді, соның ішінде веб-беттердің мазмұнын өзгертуді қамтуы мүмкін. Деректер ағып кету шабуылдары IP протоколдарымен, қатысты

қызметтермен және қолданбалармен байланысты осалдықтарды пайдалана алады. Деректер ағып кету шабуылдары, сондай-ақ ортадағы адам шабуылдары ретінде белгілі, әдетте TCP/IP сеансындағы екі түйін арасындағы деректер байланысы желісін пайдалануға негізделген және осалдықтарды пайдалана алады.

2 Cisco ASA Series қауіпсіздік құралына шолу

2.1 Cisco ASA сериясының мүмкіндіктері

Cisco ASA сериясы интернетте жұмыс істеу қызметтерін және адаптивті қауіпсіздікті қамтамасыз ететін қолдану оңай шешім болып табылады

SSL және IPSec қолдайтын VPN,бірыңғай байланыс қауіпсіздігі (дауыстық және бейне деректерін беру) және икемді модульдік отбасылық қауіпсіз өнім. Cisco өзін-өзі қорғау желісінің негізгі құрамдас бөлігі ретінде әзірленген Cisco ASA series құрылғылары Бизнестің тұтастығына теріс әсер етпес бұрын шабуылдардың таралуын тоқтататын зияткерлік қауіп-қатерден қорғауды және қауіпсіз байланыс қызметтерін ұсынады.Cisco ASA series құрылғылары барлық масштабтағы желілерді қорғауға арналған және ұйымдарға бір уақытта орналастыру мен пайдалану шығындарын азайтуға мүмкіндік береді,кешенді көп деңгейлі қауіпсіздікті қамтамасыз етеді.

2.1-сурет — Cisco ASA series қорғаныс құрылғысы

Техникалық тұрғыдан ASA series жүйесі PIX 500 Firewall, ids 4200 Sensor және VPN 3000 Concentrator сияқты Cisco өнімдерінің отбасыларында бар қуатты қауіпсіздік құралдарына сүйенеді.Cisco ASA Series Adaptive Threat Defence жалпы атауымен белгілі бейімделген қауіптен қорғау механизмдерін ұсынады. Бұған белгісіз қауіптерден қорғау құралдары (Anti-X), бизнесті қорғау әдістері кіреді-қолданбалар (Application Security) және желіні бақылау және қорғау технологиялары(Network Containment and Control) кәсіпорынның барлық маңызды ресурстарын санкцияланбаған әрекеттердің кең ауқымынан бірыңғай және толық қорғауға кепілдік береді. Қауіпсіздік оқиғаларын корреляциялаудың ішкі жүйесін қамтитын бір құрылғыда тұтынушылар желіні көптеген белгісіз қауіптерден (компьютерлік құрттар мен вирустармен күресу үшін) және шпиондық бағдарламалар мен жарнамалық бағдарламалардан қорғайды,трафикті талдау, хакерлердің белсенділігін анықтау құралдары және шабуылдың алдын алу, сондай-ақ қызмет көрсетуден бас тарту (DoS) шабуылының алдын алу құралдары.

2.1.1 Брандмауэр қорғаныс құралдары

Cisco ASA Series қол жетімділікті басқара отырып кеңейтілген қолданбалы брандмауэр қызметтерін ұсынады сәйкестендіру, қызмет көрсетуден бас тарту шабуылдарынан қорғау және нарықта сыналған Cisco PIX қорғаныс құрылғысының технологиясы негізінде жасалған бірқатар қосымша қызметтер. ASA қорғаныс құрылғысы-сенімді қорғауды қамтамасыз етеді байланыс күйін бақылау арқылы корпоративтік желілер, және жоғары өнімділігін көрсетеді. Ол ішкі желі архитектурасын сыртқы бақылаушыдан толығымен жасырып, кең қорғаныс мүмкіндіктерін ұсынады және басқару функцияларын орындай отырып, корпоративтік желі мен Интернет арасындағы "шекарашы" қызметін атқарады.

Корпоративтік желіні басып кіруден қорғау үздіксіз жүзеге асырылуы тиіс. Корпоративтік желінің" сақтаушылары " қаражатты пайдалануы керек, Интернет желісімен желілік қосылыстардың қауіпсіздігіне кепілдік беру. Бұл ASA адаптивті қорғаныс құрылғысының күші. Кейбір желілік инженерлер мамандандырылған қорғаныс құрылғыларының орнына өздеріне қолданады желілер тиісті пайдалануға негізделген шешімдер маршрутизаторлардың функционалдығы. Бағдарламалық жасақтаманы (және кейде аппараттық элементтерді) жаңартқаннан кейінмаршрутизаторлар брандмауэр функцияларын орындай алады.Бұл шешім мамандандырылған брандмауэрлер екендігімен негізделген тым қымбат және орнату қиын.Бірақ маршрутизаторлар пакеттік маршруттар туралы ақпаратты өңдеуге арналған, олар үшін емес байланыстарды басқаратын брандмауэр функцияларын орындау.Сондықтан нақты уақыт режимінде жұмыс істейтін интрузияны анықтау жүйесін құру үшін маршрутизатордың мүмкіндіктері жеткіліксіз болып шығады.

Өте күрделі маршрутизаторлар кейбіреулерін орындай аладыкіру тізімдері, сүзгілер және т. б. арқылы брандмауэр функциялары"ақылды" конфигурация параметрлері. Алдымен бұл болуы мүмкін өте тиімді, бірақ мұндай шешім көп күш жұмсауды қажет етеді көру басқару және шектеулі масштабтау мүмкіндіктері бар.

Маршрутизаторға негізделген қорғаныс құралдарын қолданатын компаниялар олардың "кездейсоқ хакерлерге" қарсы тиімділігін атап өтеді, бірақ технология дамыған сайын хакерлер техникалық оқуды бастадыәдебиет және жаңа ақпаратты электронды түрде тез тарату пошта, веб-түйіндер және" байланыс бөлмелері " (chat room). Көптеген желілік қорғаныс сарапшылары үшін желілік шабуыл құралдарын дамытудағы соңғы оқиғалардан хабардар болу үшін белгілі хакерлер топтарының веб-тораптарына үнемі бару ережеге айналды.

1. Cisco ASA жүйесіне ендірілген операциялық жүйе UNIX негізіндегі немесе Windows негізіндегі болуы мүмкін.

2. Енгізілген, қауіпсіз Cisco ASA операциялық жүйесі қауіпсіздік мәселелеріне қарамастан нақты уақыттағы басқаруды қамтамасыз етеді. ASA операциялық жүйесі желілік шабуылдан қорғау контекстінде арнайы жетілдірілген және қауіпсіздік мақсаттарын ескере отырып жасалған.

3. ASA (Adaptive Security Algorithm) қолданылады.

4. ASA алгоритмі қосылымдардың сипаттамаларын жазады, бұл ақпаратты кестеде сақтайды және «сеанс күйінің» қосылым орнатылған кездегі өзгеріссіз қалатынын растау үшін кіріс және шығыс пакеттерді пайдаланады. Ол өзгерістер анықталғанша трафиктің кідіріссіз берілуін тексеру және қамтамасыз ету үшін қолданылады. Егер сәйкессіздік табылса, деректерді беру тоқтатылады.

5. Қосылым сұрауынан кейін ASA алгоритмі ақпаратты жазу үшін бастапқы және тағайындалған IP мекенжайларын, бастапқы порттарды және TCP реттік нөмірлерін пайдаланады.

6. Шифрланған қолтаңба болашақта сәйкес хостты анықтау үшін сұрау алынған интерфейс негізінде жасалады. Қолтаңба қосылымның қызмет ету мерзімі ішінде ғана жарамды және қосылым жабылғаннан кейін жарамсыз болады. Кейбір жағдайларда әрбір жаңа қосылым сұрауы хост үшін жаңа қолтаңбаны жасайды.

7. Шабуыл жасаушылар ASA қауіпсіздік құрылғысы арқылы өтіп, Node ASA ішкі желісіне кіру үшін алгоритм жұмысына еліктеу керек. Олар ASA қосылым дерекқорының жазбаларына сәйкес «кездейсоқ» TCP реттік нөмірлерімен, сәйкес IP мекенжайларымен және порт нөмірлерімен нақты уақытта толық пакеттерді жасауы керек. Бұл хакердің желіге ену әрекеттерін дереу тоқтату және тарту мен таңдау үшін күрделірек нысаналарды жасау қажет.ASA алгоритмінің артықшылықтары:

8. Қосылымы және күй ақпараты ASA алгоритмдер кестесіндегі деректерге сәйкес келмейтін пакеттер ASA арқылы өткізілмейді.

9. Шығыс кіру тізімдерінде тыйым салынғандарды қоспағанда, барлық шығыс қосылымдар мен күйлерге рұқсат етіледі. Кіріс қосылымына немесе күйге бастаушы немесе клиент тағайындалған орынға немесе серверге қарағанда қауіпсіз интерфейсі болғанда рұқсат етіледі. Ішкі интерфейс әрқашан ең жоғары қауіпсіздік деңгейіне ие, ал сыртқы интерфейс әрқашан ең төменгі деңгейге ие. Қосымша интерфейстер үшін (мысалы, DMZ) ішкі және сыртқы интерфейстер арасындағы қауіпсіздік деңгейлерін анықтауға болады.

10. Кіріс қосылымдар мен күйлер саясатта анық рұқсат етілмесе, қабылданбайды. Кіріс қосылымына немесе күйге бастаушы немесе клиент тағайындалған орынға немесе серверге қарағанда қауіпсіз интерфейсі төмен болғанда рұқсат етіледі. Әрбір тарату мекенжайы үшін кез келген хосттан немесе желіден көрсетілген хостқа хабар тарату арқылы кіруге мүмкіндік беретін бірнеше ерекшеліктер болуы мүмкін.

11. Осы құқықтарды айналып өту әрекетіжурналдар қабылданбайды және сәйкес хабарлама syslog серверіне жіберіледі.

12. "Conduit Permit ICMP" пәрменін немесе кіру тізімін пайдалану арқылы арнайы рұқсат етілгендерден басқа барлық ICMP пакеттері қабылданбайды.

Тікелей аутентификация (cut-through proxy). Жүйе Cisco ASA қорғаныс құрылғысының аутентификациясы арқылы қолданушы деңгейінде бастапқы тексеруді орындайды (сияқты пайдаланушыны tacacs+ немесе RADIUS типті қорғаныс дерекқоры сервері анықтағаннан кейін, Cisco ASA қорғаныс құрылғысы пайдаланушыға қауіпсіздік саясатына сәйкес рұқсат береді және сұралған байланысты ашады. Берілген қосылым үшін кейінгі трафик қолданба деңгейінде аутентификацияланбайды, бірақ күйді сақтау үшін ASA алгоритмі тек TCP/IP сеансын тексереді (бұл жүйе жылдам желі деңгейінде жұмыс істейді), бұл өнімділікті айтарлықтай жақсартады.Прокси сервермен стандартты аутентификацияны пайдалану қолданбаның қалай жұмыс істейтініне байланысты және транзакцияны өңдеуді баяулатуы мүмкін. Қолданбалы деңгейдің жылдамдығы толығымен негізгі компьютерге байланысты және процессордың жылдамдығымен шектеледі.

Протоколдар мен қолданбаларға шолу (қолданбаны тексеру). Ұйымдар пайдаланатын кейбір хаттамалар мен қолданбаларды желіаралық қалқандар, әсіресе порттармен (HTTP, ESMTP, FTP және H.323 сияқты) динамикалық түрде келісетіндер бұғаттауы мүмкін. Сондықтан жақсы брандмауэр OSI желілік деңгейіндегі пакеттерді тексеріп, осы протоколдар мен қолданбалардың талаптарына сәйкес келуі керек.

Хаттамалар мен өтінімдерді тексеру (Application Inspection). Ұйымдар пайдаланатын кейбір хаттамалар мен қолданбаларды брандмауэрлер бұғаттауы мүмкін, әсіресе порттарды динамикалық түрде келісетіндер (мысалы, HTTP, ESMTP, FTP және H.323). Сондықтан, жақсы брандмауэр тексеруі тиіс пакеттер OSI желілік деңгейінің үстінде және астында және осы протоколдар мен қолданбалардың талаптарына сәйкес болуы керек.

Рұқсат етілген клиент/сервер қосылымдары үшін динамикалық бөлінген порттарды немесе IP мекенжайларын қауіпсіз ашады және жабады

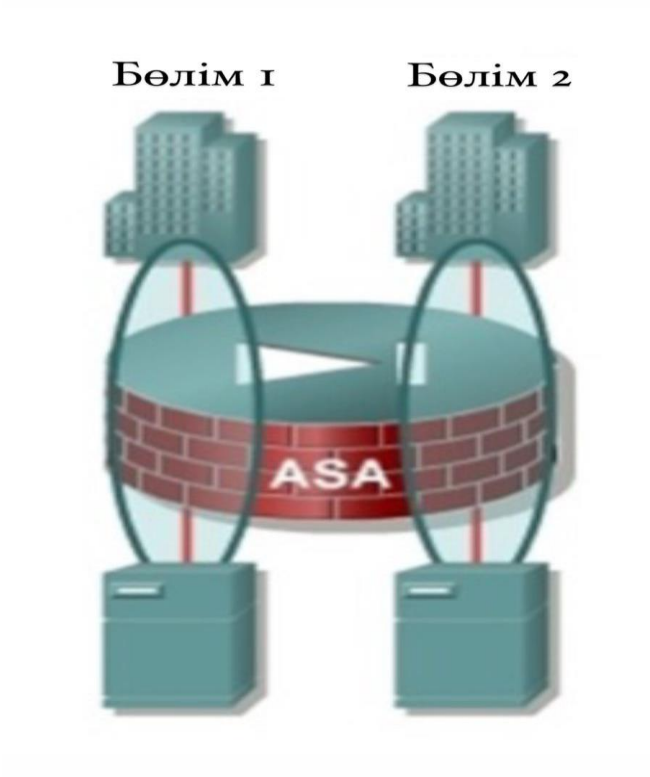
Хаттамалар мен қосымшаларды тексеру (Applications Inspection).Ұйымдар қолданатын кейбір хаттамалар мен қосымшаларбрандмауэр арқылы бұғатталуы мүмкін. Әсіресепорттар туралы динамикалық түрде келісетін хаттамалар (HTTP, ESMTP,FTP және H. 323). Сондықтан жақсы брандмауэр тексеруі керекпакеттер OSI моделінің желілік деңгейінен жоғары және келесі талаптарды орындаңыз хаттамалар немесе қосымшалар: Хаттамалар мен қосымшаларды тексеру (Applications Inspection).Ұйымдар қолданатын кейбір хаттамалар мен қосымшалар брандмауэр арқылы бұғатталуы мүмкін. Әсіресе порттар туралы динамикалық түрде келісетін хаттамалар (HTTP, ESMTP,FTP және H. 323). Сондықтан жақсы брандмауэр тексеруі керек пакеттер OSI моделінің желілік деңгейінен жоғары және келесі талаптарды орындаңыз хаттамалар немесе қосымшалар:

- динамикалық бөлінген порттарды қауіпсіз ашады және жабады немесе рұқсат етілген клиент-сервер қосылымдары үшін IP мекенжайлары;
- IP пакетінде желілік мекен-жай трансляциясын (NAT) қолданады;

- пакет ішіндегі порт трансляциясын (PAT) пайдаланады;
- пакеттерді дұрыс емес (зиянды)тексереді қолданбаларды пайдалану.

Cisco ASA дәл осы талаптарды қанағаттандырады және мүмкіндік береді ашық қорғалған байланыс бірқатар хаттамалар мен қосымшалар үшін.

Виртуалды брандмауэр (Security Contexts). Жетінші нұсқадан Cisco ASA операциялық жүйесі виртуалды технологияны қолдайды брандмауэрлер (Security Contexts) (2.2-сурет).



2.2-сурет — Виртуалды брандмауэр

Бұл бір физикалық құрылғыда бірнеше нәрсені анықтауға мүмкіндік береді әрқайсысы жұмыс істей алатын жеке брандмауэрлер дербес-өзінің конфигурациясымен, логикалық интерфейстерімен, саясатыменқауіпсіздік, маршруттау кестесі және басқару. Алайда, бұл функционалдылық лицензияланған және барлық құрылғы үлгілерінде қол жетімді емес қорғау.

Ақауларға төзімділікті қолдау (Failover). Cisco ASA қолдайды екі құрылғы бірдей болған кезде ақауларға төзімділік конфигурациясы (Failover) қорғаныс жұпта конфигурацияланған, біреуі белсенді, екіншісі резервтік. Тек белсенді құрылғы өзінің функционалдығын орындайды, ал резервтік тек мониторинг жүргізеді және белсенді брандмауэрді ауыстыруға дайын, егер ол бұл сәтсіздікке әкеледі. Бағдарламалық жасақтаманың жетінші нұсқасынан бастап қолдау көрсетіледі конфигурация белсенді / белсенді, екі құрылғы да өңдей алады трафик. Бұл конфигурация виртуалды желіаралық қолдауды қажет етеді экрандар (security contexts). Әр құрылғыда екі конфигурация бар виртуалды брандмауэр. Әдетте, әрбір физикалық құрылғыда бір белсенді және

бір күту режиміндегі виртуалды желіаралық қалқан болады. Бір құрылғы істен шыққан жағдайда, сақтық көшірме виртуалды брандмауэр басқа құрылғыда қосылады және барлық трафикті өңдейді. Сондай-ақ, белсенді құрылғыларды бұрыннан бар қосылымдарды жоғалтпай өшіруге болатын күйді динамикалық ауыстыруды конфигурациялауға болады.

Cisco ASA жетінші шығарылымы желі мекенжайын өзгертпей OSI үлгісінің жетінші деңгейіне дейін желіні қорғауды қамтамасыз ететін мөлдір желіаралық қалқан режимінде (көпір режимі) жұмыс істеу мүмкіндігін береді. Бұл қорғаныс құрылғысын бар желіге енгізуге мүмкіндік береді.

ASDM (Adaptive Security Device Manager) — құрылғы интерфейсінің пәрмен жолын пайдаланбай құрылғыны орнатуға және басқаруға көмектесетін графикалық қабық ASDM (Adaptive Security Device Manager) - графикалық қабық,құрылғыны орнатуға және басқаруға көмектесу үшін жасалған,құрылғының командалық қабығын (CLI) білместен.

2.1.2 AIP-SSM модулі

Маңызды желілік активтеріңізді кеңейтілген шабуылдардан қорғаңыз интрузияның алдын алу жүйесінің (IPS) толыққанды қызметтері. Cisco ASA Series тиімді, жоғары өнімділікті қамтамасыз етеді,қазіргі заманғы қауіп-қатерден қорғау, соның ішінде қосымшалардың осалдығы және операциялық жүйе, бағытталған шабуылдар, құрттар, вирустар және басқа формадағы зиянды бағдарламалар.

2.3-сурет — AIP-SSM модулі

2.1.3 SSL және IPSec қолдайтын VPN

Желіні қорғалған, икемді қашықтан кеңейтіңіз аралық өтініштерсіз қол жеткізу. Cisco ASA озық VPN шешімі Series порталдың бірегей функционалдығын ұсынады, жоқ клиенттік бағдарламалық жасақтаманы (clientless) пайдалануды талап етеді, және 5000-ға арналған платформааралық толыққанды туннель клиенттерді бір құрылғыдағы SSL немесе IPsec протоколы бойынша бір мезгілде қосады, әлемдік деңгейдегі брандмауэр қызметтерімен қорғалады және т.б.

ASA series жүйесі трафиктің құпиялылығын қамтамасыз ететін механизмдер жиынтығын ұсынады. Олар IPSec және SSL протоколдарын пайдалануға негізделген және бейімделген қауіп-қатерден қорғау

технологияларымен біріктірілген. Cisco ASA series құрылғыларында IPSec және SSL VPN біріктіру оларға кез келген vpn қолдану сценарийіне, соның ішінде нүкте-нүкте конфигурацияларына, кәсіпорын желісіне қашықтан қол жеткізуге және қол жеткізуге оңай бейімделуге мүмкіндік береді серіктес желісіне немесе экстранет желісіне. Бір құрылғы арқылы және басқарылатын инфрақұрылымды жоғары қорғаныспен қамтамасыз етуге болады кез келген пайдаланушы үшін желіге қашықтан қол жеткізу, ол қай жерде болса да. Cisco ASA series құрылғылары қолданыстағы Cisco vpn3000 Concentrator кластерлерімен біріктіре алады, бұл тұтынушыларға ең көп енгізу арқылы қолда бар VPN құрылымдарын пайдалануға мүмкіндік береді қазіргі заманғы VPN және қауіпсіздік қызметтері.

2.1.4 Модуль CSC-SSM

Cisco ASA Series мазмұн қауіпсіздігі және қауіпсіздік қызметтерін басқару модулін ұсынады-CSC-SSM (Content Security and Control Security services Module). Ол вирустармен және шпиондық бағдарламалармен күресу,спам және фишингтік шабуылдармен күресу, URL мекенжайларын блоктау және сүзу, сондай-ақ ықтимал қауіпті немесе жұмыс істемейтін материалдарға қол жеткізуді болдырмайтын мазмұнды сүзу сияқты Anti-x қызметтерінің толық жиынтығын қолдайды. Модуль Интернет шлюзі ретінде жұмыс істейді және ішкі желілік ресурстарды Интернет арқылы таралатын зиянды бағдарламалар мен хакерлік шабуылдардан қорғайды, бұл операциялық шығындарды азайтуға, ақаулықтарды азайтуға және қызметкерлердің өнімділігін жақсартуға көмектеседі.

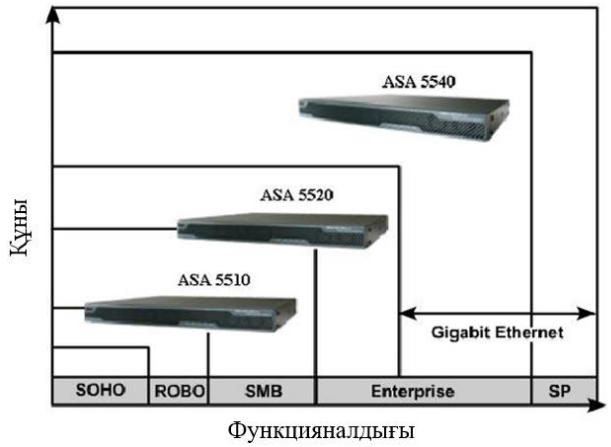
2.2 Cisco ASA сериясының үлгілері

Cisco ASA сериясының үлгілері әртүрлі конфигурациялар үшін сенімділікті қамтамасыз ететін жаңартылатын етіп жасалған. Қазіргі уақытта үш ASA үлгісі қол жетімді.

Cisco ASA 5510 бюджет пен өнімділік талаптарына сәйкес келетін сенімді қосылымды ұсынады. Бұл бастапқы деңгейдегі жергілікті желі үшін қорғауды қажет ететін шағын және орта бизнес үшін тамаша таңдау.

Cisco ASA 5520 ASA 5510 қарағанда сенімдірек желілік қауіпсіздік платформасын қамтамасыз етеді. Қосымша интерфейстерді, Gigabit Ethernet немесе бір мезгілде қосылымдарды қолдау қажет болса, ASA 5520 қолайлы таңдау болуы мүмкін, asa 5520 моделі қолайлы болуы мүмкін. Бұл модель бүкіл кәсіпорын деңгейінде қорғауды қажет ететін компаниялар желілеріндегі жүктемені оңай жеңе алады (2.4-сурет).

Cisco ASA 5540 моделі. Ірі кәсіпорындар үшін қауіпсіздік қызметтерін қамтамасыз етеді.



2.4-сурет — функционалдылықтың ASA өнімдерінің құнына тәуелділігі

Барлық модельдер адаптивті тексеру модульдері (2.5-Сурет) және шабуылдардың алдын алу (AIP-SSM) және мазмұн қауіпсіздігін қамтамасыз ету (CSC-SSM) сияқты басқа қорғаныс қызметтерін қосуға мүмкіндік береді.

2.5-сурет — SSM ұясы

Икемді архитектурасы бар Cisco ASA отбасы сенімді қауіпсіздікті және динамикалық қауіп ортасында жаңа шабуылдарға оңай бейімделу мүмкіндігін қамтамасыз етеді. ASA қауіпсіздік құрылғыларының сипаттамалары 1-кестеде көрсетілген.

Кесте 2.1-Cisco ASA series модельдерінің сипаттамалары

Өнімділік МСЭ, Мбит/с	Дейін 300	Дейін 450	Дейін 650
Өнімділік шабуылдарды тойтару, Мбит/с	150 с AIP SSM-10 300 с AIP SSM-20	225 с AIP-SSM-10 375 с AIP-SSM-20 450 с AIP-SSM-40	500 с AIP-SSM-20 650 с AIP-SSM-40
Өнімділік VPN, Мбит/с	До 170	До 225	До 325
Бір уақытта сан қолдау көрсетілетін сессиялар	32 000/64 000*	130 000	280 000
IPSec туннельдерінің саны VPN	50/150*	300/750*	500/2000*/5000***
SSL туннельдерінің саны VPN	50/150*	300/750*	500/1250*/2500***
Виртуалды МСЭ	0	2/10**	2/50***
Ақауларға төзімділік	Active/Standby*	Active/Active және Active/Standby	Active/Active және Active/Standby
Кластерлеу және VPN теңгерімі	Жоқ	Ия	Ия
Қолдау физикалық интерфейстер	3 Fast Ethernet + 1 порт басқару/5 Fast Ethernet*	4 Gigabit Ethernet + 1 Fast Ethernet	4 Gigabit Ethernet + 1 Fast Ethernet
Қолдау логикалық интерфейстер VLAN 802.1q	0/10*	25	100
* 5510 Security Plus, 5520 vpn Plus және 5540 vpn plus лицензиялары бар тиісінше; ** қосымша лицензиямен (базалық жиынтықта - 2); *** 5540 vpn Premium лицензиясымен.			

ASA алдыңғы панелінде (2.6 және 2.7-сурет) келесі жарықдиодты индикаторлар бар:

1 Power-таза жасыл құрылғы қосулы екенін көрсетеді.

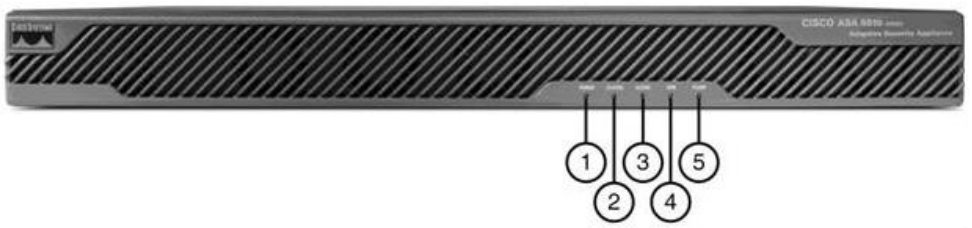
2 Status -Жасыл жыпылықтау жүйенің жүктеліп жатқанын және қуат қосылымын тексеру жүргізіліп жатқанын көрсетеді. таза жасыл мынаны көрсетеді жүйелік сынақтар өтіп, жүйе жұмыс істейді. Таза кәріптас жүйелік сынақтардың сәтсіз болғанын көрсетеді.

3 Active-жасыл жыпылықтау желінің белсенді екенін көрсетеді.

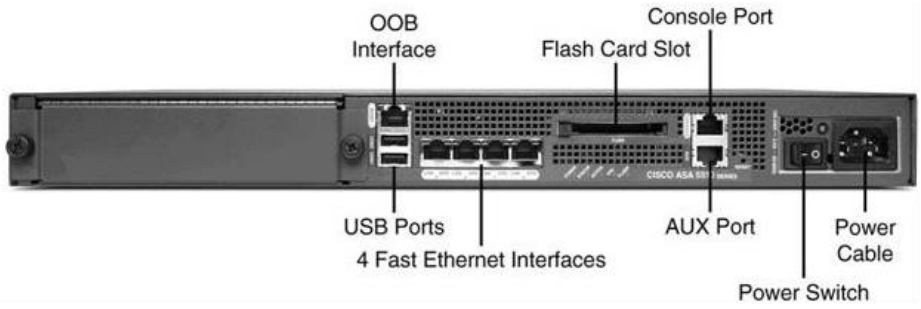
4 VPN-қатты жасыл бір немесе одан да көп екенін көрсетеді VPN туннельдер

белсенді.

5 Flash-қатты жасыл жады бар Flash картасына екенін көрсетеді өтініш.



2.6-сурет — Cisco ASA 5510 моделінің алдыңғы панелі



2.7-сурет — Cisco ASA 5510 моделінің артқы панелі

Барлық модельдер one-rack unit (1RU) дизайнын ұсынады.Сыртқы орналастыру интерфейстерді қоспағанда бірдей.

3 Бірлескен корпоративтік желіні ұйымдастыру

Әрбір бөлімшенің жергілікті корпоративтік желілері бір-бірімен тірек (көлік) желісімен байланысты. Компанияның кеңселері мен кеңселері әртүрлі қалалар мен елдерде болған кезде ауқымды ұйымда қолданыстағы Ғаламдық деректер желілері, атап айтқанда Интернет желілері тірек желілері ретінде пайдаланылуы мүмкін. Деректердің негізгі алмасуы жергілікті желілерде жүзеге асырылады, ал тірек желі ұйымның әртүрлі кеңселерінде алынған жобалық нәтижелерді келісуге арналған. Бұған желінің иерархиялық құрылымы ықпал етеді, осылайша деректер арналарындағы трафикті азайтады. Деректерді беру арнасы бөлімшелер арасында деректер алмасу үшін байланыс желісі рөліндегі тірек көлік желісін, деректерді қабылдау-берудің соңғы аппаратурасын, деректерді беру маршрутындағы коммутациялық жабдықты қамтиды.

Cisco ASA Series сонымен қатар қауіпсіздік мүмкіндіктерінің бай жиынтығын қамтиды,Threat-protected vpn (виртуалды жеке желілер) деп аталды қауіп-қатерден қорғау). Бұған соңғы желілік құрылғыларды қорғау, құралдар кіреді қауіп-қатерге қарсы күрес, қолданбаларға арналған МСЭ және кіруді басқару қызметтері,vpn қосылымдары мен пайдаланушы деректерін желіден қорғайтын құрттар, вирустар, тыңшылық бағдарламалар және хакерлік шабуылдар. Жаңа мүмкіндіктер күйлерді ескере отырып SSL VPN авариялық алу бизнестің үздіксіздігі және жалпы еңбек өнімділігін арттырады.

Cisco ASA series 7.1 нұсқасының көмегімен әрбір ASA series құрылғысы бір уақытта 5000 SSL VPN сеансын қолдайды. Осылайша, кез-келген көлемдегі ұйымдар өздерінің мобильді және қашықтағы қызметкерлеріне Жер шарының кез-келген жерінен қосымшалар мен желілік ресурстарға оңай және қауіпсіз қол жетімділікті қамтамасыз ете алады. Кіріктірілген vpn жүктемені теңестіру мүмкіндіктері және IPSec VPN-дің толық ауқымды функционалдығы виртуалды жеке желілерді қорғауға және бір уақытта ондаған мың пайдаланушыларға қолдау көрсетуге қажетті аппараттық құрылғылардың санын азайтуға мүмкіндік береді. Сонымен қатар, IPSec, клиенттік және клиенттік емес SSL режимдері, қашықтан қол жеткізу, сайттар арасындағы байланыс және экстранет сияқты әртүрлі типтегі VPN мүмкіндіктерін қолдау үшін қажет VPN платформаларының саны азаяды.[4]

ASA series 7.1-де SSL VPN желілерінде мазмұнды жеткізу механизмі жетілдірілген. Java компоненттерін, ActiveX және күрделі конструкцияларды қамтитын веб-беттерге арналған қуатты веб-мазмұнды түрлендіру мүмкіндіктері пайда болды HTML және JavaScript. Қолданба өнімділігін оңтайландыру, қолдау түрлі браузерлер және теңшелетін пайдаланушы порталы ұйымдар үшін қашықтан және мобильді қызметкерлерге корпоративтік

ресурстарға ыңғайлы қол жеткізуді қамтамасыз ету мүмкіндіктерін одан әрі кеңейтеді.

Интеграцияланған қызметтерге арналған Cisco маршрутизаторлары (800, 1800, 2800 және 3800 сериялары) және Cisco 7200 және Cisco 7301 маршрутизаторлары SSL VPN-ді қолдайды, бұл тұтынушыларға осы платформаға негізделген қауіпсіз маршруттау жүйесін құруға мүмкіндік береді. Іске асырылған SSL VPN қызметтері Cisco маршрутизаторларында клиенттік емес 150-ге дейін қолдайды және шағын және орта бизнестің қажеттіліктерін қанағаттандыратын SSL VPN клиенттік сессиялары. Клиенттік емес қатынас-бұл Citrix сияқты жиі қолданылатын желілік қосымшаларға қол жеткізудің сенімді қорғалған тәсілі және Outlook. SSL VPN клиенттік қызметтері кез-келген іскери қосымшалар үшін қорғалған кіру арналарын ұсынады. Олар IPSec технологиясын толықтырады VPN және қазіргі заманғы Cisco IOS қауіпсіздік қызметтері (ХЭО, IPS және т.б.), оңай енгізілуімен және қол жетімділігімен ерекшеленеді. Жаңа SSL қызметтерінің пайда болуы Cisco интеграцияланған қызмет маршрутизаторларындағы VPN желілік инфрақұрылымның өтелу мерзімін және тұтынушының операциялық шығындарын айтарлықтай қысқартады.[7]

Барлық Cisco SSL VPN платформалары Cisco Secure Desktop функциясын іске асырады, ол желіге қосылуға тырысатын әрбір құрылғының қауіпсіздік жүйесінің күйін автоматты түрде тексереді және деректерді қорғайды. Ол үшін құпия деректерді қорғайтын және компьютерді "тазартатын ""қауіпсіз Виртуалды машина" жасалады байланыс сеансы аяқталғаннан кейін ("тазарту" процесінде сессияның барлық іздері өшіріледі, оның барысында құпия сипаттағы деректер пайдаланылды).

3.1 "ASUE"корпоративтік желісінің периметрін қорғау

3.1.1 "ASUE"компаниясының жалпы сипаттамасы

Cisco Packet Tracer телекоммуникация желілерін және желілік жабдықтарды зерттеуде, сонымен қатар жоғары оқу орындарында зертханалық жұмыстар бойынша сабақтарды өткізу үшін ұсынылады.

Cisco Packet Tracer негізгі мүмкіндіктері:

1. Достық графикалық интерфейс (GUI) желіні ұйымдастыруды, құрылғының жұмыс істеу принциптерін жақсырақ түсінуге ықпал етеді.

2. CCNA күрделілік деңгейінде кез келген көлемдегі желілерді құру үшін логикалық топологияны модельдеу мүмкіндігі.

3. Нақты уақытта модельдеу.

4. Модельдеу режимі.

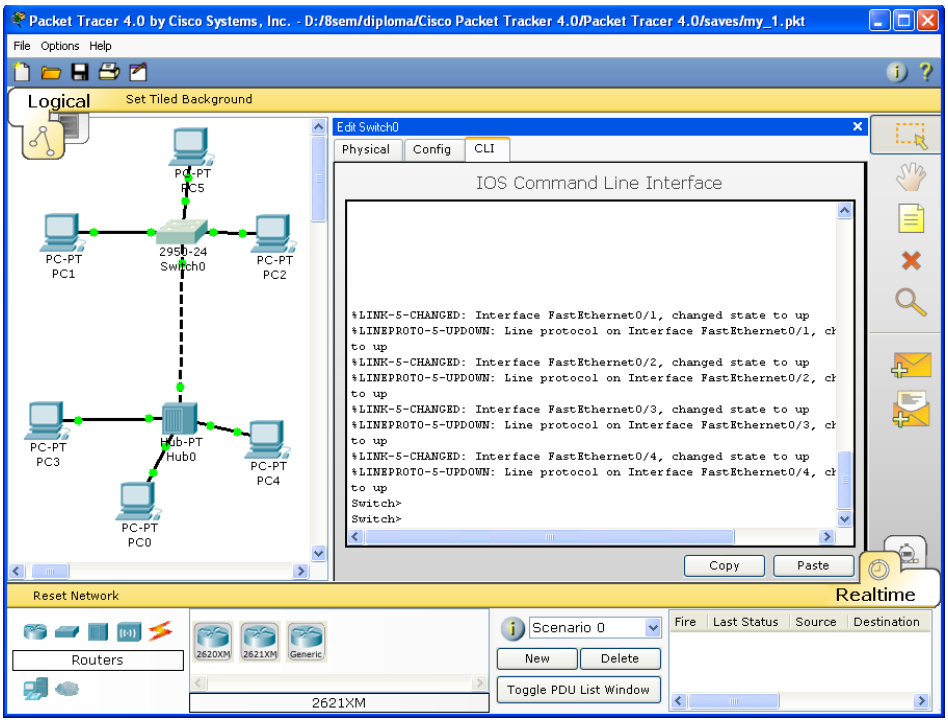
5. Бағдарламаның көптілді интерфейсі бағдарламаны ана тілінде оқуға мүмкіндік береді.

6. Әртүрлі компоненттерді қосу/жою мүмкіндігі бар желілік жабдықтың жетілдірілген кескіні.

7. Белсенділік шеберінің болуы желілік инженерлерге, студенттерге және мұғалімдерге желі үлгілерін жасауға және оларды болашақта пайдалануға мүмкіндік береді.

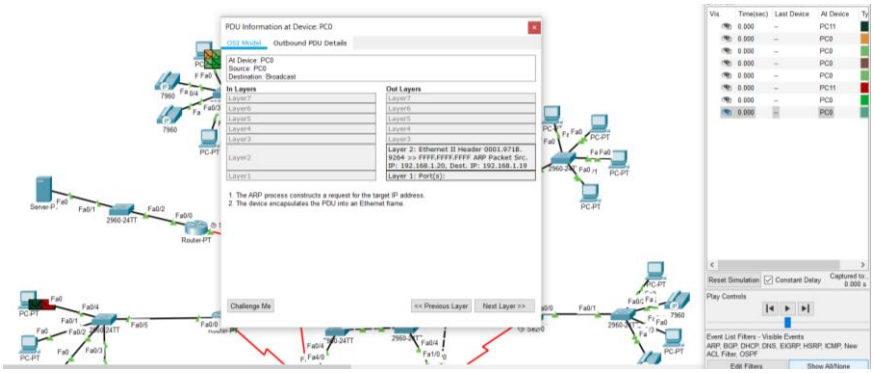
8. Физикалық топологияның дизайны: қала, ғимарат, тірек және т.б. ұғымдарды пайдалана отырып, физикалық құрылғылармен қол жетімді өзара әрекеттесу. [3]

Бұл өнімнің мүмкіндіктерінің кең ауқымы желі инженерлеріне компьютерлік желіні конфигурациялауға, жөндеуге және құруға мүмкіндік береді. Сондай-ақ, бұл өнім оқу процесінде таптырмас, өйткені ол желіні көрнекі түрде көрсетеді, бұл студенттердің материалды игеруін арттырады. Желілік эмулятор желі инженерлеріне әртүрлі деректер пакеттерін жасау және жіберу, сақтау және олардың жұмысына түсініктеме беру арқылы кез келген күрделіліктегі желілерді жобалауға мүмкіндік береді. Мамандар екінші және үшінші деңгейлі коммутаторлар, жұмыс станциялары сияқты желілік құрылғыларды зерттеп, пайдалана алады, олардың арасындағы байланыс түрлерін анықтап, сызықтарды қоса алады .



3.1-сурет — Cisco Packet Tracer

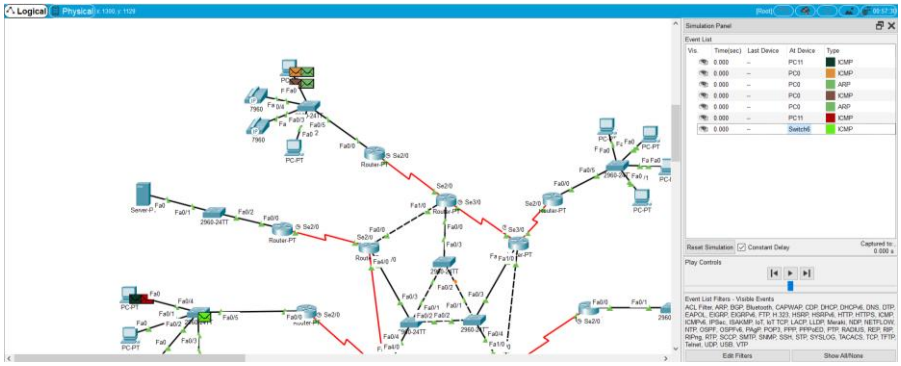
Бұл тренажердің маңызды ерекшеліктерінің бірі - онда «Симуляция режимінің» болуы (3.1-сурет). Бұл режимде желі ішінде жіберілген барлық пакеттер графикалық түрде көрсетіледі. Бұл мүмкіндік желі мамандарына пакеттің қазіргі уақытта қандай интерфейсте жүріп жатқанын, қандай протокол қолданылып жатқанын және т.б. көрнекі түрде көрсетуге мүмкіндік береді.



3.2-сурет — Cisco Packet Tracer бағдарламасындағы «Симуляция» режимі

«Симуляция режимінде» желілік инженерлер пайдаланылған хаттамаларды қадағалап қана қоймай, сонымен қатар берілген хаттама OSI моделінің жеті қабатының қайсысына қатысатынын көре алады (3.3-сурет). Бұл OSI моделінің жеті деңгейінің қайсысында қате жіберілгенін анықтауды және сәйкесінше оны дер кезінде түзетуді жеңілдетеді

.



3.3-сурет — Cisco Packet Tracer жүйесінде жеті деңгейлі OSI үлгісін талдау.

Cisco Packet Tracer әртүрлі мақсаттағы құрылғылардың үлкен санын, сондай-ақ көптеген әртүрлі қосылым түрлерін модельдеуге қабілетті, бұл күрделіліктің жоғары деңгейінде кез келген өлшемдегі желілерді жобалауға мүмкіндік береді.

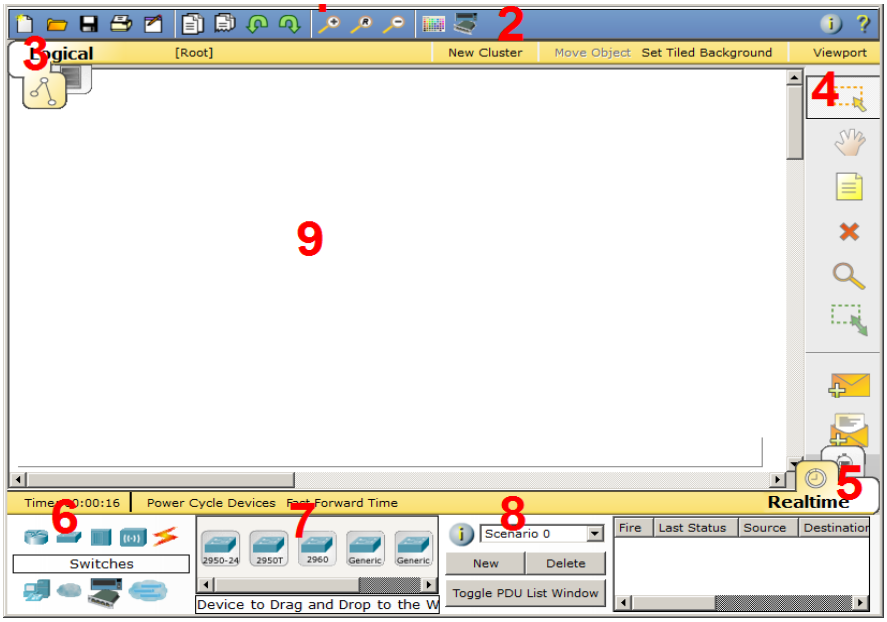
Үлгіленген құрылғылар: 2-деңгей және 3-деңгей коммутаторлары, желілік хабтар, соңғы құрылғылар, сымсыз құрылғылар.

Байланыс түрлері: консоль, тікелей кабель, айқас кабель, талшықты-оптикалық кабель, телефон желісі, SerialDCE, SerialDTE.

PacketTracer әртүрлі протоколдарды бақылай алады: ARP, CDP, DHCP, EIGRP, ICMP, RIP, TCP, UDP. [4]

Cisco Packet Tracer интерфейсі 3.4-суретте көрсетілген.

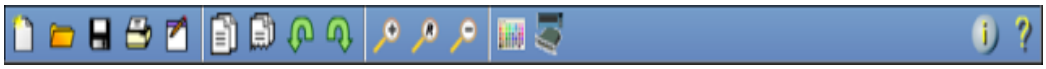
1. Бағдарламаның негізгі мәзірі.
2. Құралдар тақтасы – кейбір мәзір пункттерін қайталайды.
3. Логикалық және физикалық ұйым арасында ауысу.
4. Басқа құралдар тақтасында объектілерді таңдау, жою, жылжыту, масштабтау, сондай-ақ ерікті бумаларды қалыптастыру құралдары бар.
5. Нақты режим мен модельдеу режимі арасында ауысыңыз.
6. Соңғы құрылғылар топтары және байланыс желілері бар панель.
7. Соңғы құрылғылардың өзі, ол ажыратқыштардың, түйіндердің, кіру нүктелерінің, өткізгіштердің барлық түрлерін қамтиды.
8. Пайдаланушы сценарийлерін жасауға арналған панель.
9. Жұмыс кеңістігі.



3.4-сурет — Cisco Packet Tracer интерфейсі

Бұл терезенің көп бөлігін жұмыс кеңістігі алып жатыр, онда әртүрлі желілік құрылғыларды орналастыруға, оларды әртүрлі тәсілдермен қосуға және соның нәтижесінде әр түрлі желі топологияларын алуға болады.Жұмыс аймағының үстінде негізгі программалық панель және оның мәзір. Мәзір желі

топологияларын сақтауға, жүктеуге, модельдеуді орнатуға және басқа да көптеген қызықты функцияларға мүмкіндік береді. Ол 3.5-суретте көрсетілген.



3.5-сурет — Cisco Packet Tracer негізгі мәзірі

Жұмыс кеңістігінің оң жағында жұмыс кеңістігінің кенептерін жылжытуға, нысандарды жоюға және т.б. үшін жауапты бірнеше түймелерді қамтитын бүйірлік тақта бар. Төменде, жұмыс аймағының астында жабдық панелі орналасқан. Ол 3.6-суретте көрсетілген.

3.6-сурет — Cisco Packet Tracer аппараттық панелі

Бұл панельдің сол жағында қол жетімді құрылғылардың түрлері және оң жағында қол жетімді үлгілер бар. Әртүрлі зертханалық жұмыстарды орындау кезінде бұл панельді басқаларға қарағанда жиірек қолдануға тура келеді.

Құрылғылардың әрқайсысының үстіне апарған кезде оның түрі олардың ортасында орналасқан тіктөртбұрышта көрсетіледі. Cisco Packet Tracer зертханаларында жиі қолданылатын құрылғы түрлері 3.7-суретте көрсетілген.

3.7-сурет — Құрылғылардың негізгі түрлері

Қосылым түрлері ерекше назар аударуды қажет етеді. Қосылым түрлерін қарастыру3.8 -суретке сәйкес солдан оңға қарай жүреді.

1. Автоматты түр - осы қосылым түрімен Cisco Packet Tracer таңдалған құрылғылар үшін ең қолайлы қосылым түрін автоматты түрде таңдайды.

2. Консоль – консольдық қосылым

3. Тікелей мыс - бұралған жұп мыс кабельмен қосылу, кабельдің екі ұшы бірдей орналасуда бүктеледі. Келесі қосылымдар үшін қолайлы: коммутатор - коммутатор, коммутатор - маршрутизатор, коммутатор - компьютер және т.б.

4. Мыс кроссовер - бұралған жұп мыс кабельмен қосу, кабельдің ұштары кроссовер ретінде бүктеледі. Екі компьютерді қосу үшін қолайлы.

5. Оптика – оптикалық интерфейстері бар құрылғыларды қосу үшін қажетті оптикалық кабель арқылы қосылу.

6. Телефон кабелі – кәдімгі телефон кабелі, телефондарды қосу қажет болуы мүмкін.

7. Коаксиалды кабель – коаксиалды кабель арқылы құрылғыларды қосу.

3.8-сурет — Cisco Packet Tracer жүйесіндегі құрылғы қосылымдарының түрлері

"ASUE" Қазақстан Республикасындағы дамушы компаниялардың бірі болып табылады. Тарихи түрде компанияның желілік инфрақұрылымы барлық желілік ресурстарға толық қол жеткізуге мүмкіндік беретін толығымен ашық болды. Дегенмен, соңғы кездері ақпараттық жүйелер бөлімі көптеген кибершабуылдардың құрбаны болды. Нәтижесінде компания өз желісінің осалдығын мойындады және оны Cisco шешімдерінің көмегімен қорғауға қаражат бөлуде. ASEU қазірдің өзінде Cisco өнімдерінің белсенді тұтынушысы болып табылады және өз желісінде TCP/IP стегін пайдаланады.

Қорғауды қажет ететін үш құрылымдық желі сегменті бар: жергілікті желі, қашықтан қол жеткізу және Интернетке кіру. ASEU ішкі және сыртқы пайдаланушылардың өз серверлеріндегі құпия деректерге қол жеткізуін шектеуге тырысады. Ол сонымен қатар шығыс трафикті бақылауға, аутентификация жүйелерін және желілік аудит әдістерін жақсартуға бағытталған. Компания басшылығы IPSec, SSL және VPN (Virtual Private Network) желілерінің мүмкіндіктерінен хабардар

Ақпараттық жүйелер бөлімі бүкіл компанияның желісінің жұмысына жауап береді.Аумақтық желі қосымшалары мен файлдық серверлер компанияның барлық бөлімшелеріне қол жетімді Windows NT серверлерінде орналастырылған(әзірлеу және сату бөлімшелерін қоса алғанда) және

серіктестер желілерімен байланысты.Ақпараттық жүйелер бөлімі Windows NT серверіне негізделген желілік басқару жүйесін және тиісті бағдарламалық жасақтаманы қолданады желіні басқару. Аумақтық желі Cisco маршрутизаторлары мен Ethernet қосқыштарын пайдаланады.

"ASUE" компаниясы ішкі және сыртқы пайдаланушылар ішкі желі серверлерінде орналастырылған маңызды деректерге"әзірлемелер "және" сату", өйткені басшылық деректерге қатысты бұл серверлерге бөгде адамдар рұқсатсыз кіре алады.А қосымшасында А. -суретте Cisco қорғаныс технологияларын қолданар алдында компанияның желілік схемасы көрсетілген. Схемадан көріп отырғанымыздай,ішкі желіні қорғауды қамтамасыз ететін маршрутизатордың параметрлері де қатысқан жоқ.

Зертханалық семинарды ұйымдастыру және өткізу мәселелері қарастырылады.

Томск мемлекеттік ұлттық зерттеу университетінің ақпараттық қауіпсіздік және криптография кафедрасында «Қауіпсіз компьютерлік желілерді құру негіздері» [1]. Семинар – бұл аттас курс, «Компьютерлік желілер» курсы немесе сабақтас тақырыптар бойынша курстар шеңберінде пайдалануға болатын зертханалық жұмыстардың жиынтығы. Бұл семинардың өзектілігі қазіргі уақытта компьютерлік желілер қазіргі заманғы ақпараттық және телекоммуникациялық жүйелердің негізгі құрамдас бөлігі болып табылатындығымен анықталады. Компьютерлік желілерді құрудың барлық міндеттерінің ішінде ең маңыздысы құпиялылыққа, тұтастыққа және қолжетімділікке қауіп төндіретін қауіпсіздікті қамтамасыз ету болып табылады. Бұл жағдайда қорғаудың ішкі жүйесі ықтимал қасиеттердің бірі ретінде оның қауіпсіздігін қамтамасыз ететін компьютерлік желінің бөлігі болуы керек. Компьютерлік желілердің архитектурасын дамытуға осындай көзқараспен қауіпсіз компьютерлік желілер туралы айтылады.

Зертханалық семинардың мақсаты – қауіпсіз компьютерлік желілерді жобалау үшін қажетті білім, сондай-ақ қауіпсіздік механизмдері мен желілік инфрақұрылымның жұмыс істеу құралдарын конфигурациялау дағдыларын алу.

Зертханалық семинардың мақсаты келесі бағыттар бойынша білім мен дағдыларды алу болып табылады:

- қорғалған компьютерлік желілердің архитектурасы мен жобалау әдістері;
- ақпараттық технологияларды қорғаудың ішкі жүйелерін жоспарлау және құру;
- желілік инфрақұрылымды қорғау механизмдері мен құралдарын құру;
- Компьютерлік желіні қорғау жүйелеріндегі ақауларды жою.

Қазіргі уақытта зертханалық шеберхана келесі жұмыстарды қамтиды:

1. OSPF, EIGRP және BGP хаттамалары негізінде маршруттау инфрақұрылымын қорғау.

2. Коммутациялық инфрақұрылымды қорғау.

3. STP хаттамасы негізінде ақауларға төзімді жергілікті желіні (LAN) құру.

4. Сілтеме деңгейінің шабуылдарынан LAN қорғауы.

5. Қол жетімділігі жоғары маршрутталған LAN құру.

6. Желілік инфрақұрылымды рұқсатсыз кіруден қорғау.

7. Мәліметтерді беру желісінде қызмет көрсету механизмдерінің сапасын орнату.

8. IP желісінде дауыстық мәліметтерді жіберуді қорғау.

9. Желінің периметрін қорғау.

10. Рұқсат етілмеген қол жеткізуден деректерді беру арналарын криптографиялық қорғау.

11. Сымсыз жергілікті желіден қорғау.

Зертханалық жұмысты қамтамасыз ету үшін бағдарламалық желі эмуляторы қолданылады

Cisco Packet Tracer. Бұл бағдарламалық құрал сізге мүмкіндік береді:

- 25 адамға дейінгі студенттер тобына бір уақытта зертханалық семинар өткізу;
- нақты компьютерлік желілердің жұмыс істеуінің барлық негізгі процестерін эмуляциялау және зерттеу;
- компьютерлік желілердегі кейбір шабуылдарды имитациялау (мысалы, VLAN секіру, MAC-спуфинг, STP протоколына шабуылдар);
- нақты желілік жабдықтың қымбат оқу стендтерін жасаудың қажеті жоқ, студенттің қолында виртуалды компьютерлік желіні қамтамасыз ету.

Оқытушының қалауы бойынша семинар шеңберінде көрсетілген зертханалық жұмыстардан басқа мыналарды орындауға болады:

1. Әдістеме бойынша нақты уақыт режимінде студенттер топтары арасындағы көп ойыншы ойыны [2].

2. «Компьютер желісіндегі ақаулықтарды жою» есебін шешу. Мұғалім компьютерлік желі моделіне конфигурация файлын дайындайды, оның бір бөлігі конфигурацияланған және дұрыс жұмыс істемейді. Студенттер желілік жабдықтың кейбіріне қол жеткізе алады. Студенттердің міндеті - берілген уақытта желілік жабдықты және қауіпсіздік құралдарын орнатудағы қателерді табу және жою.

3. «Деректерді берудің қауіпсіз корпоративтік желісін дамыту» рөлдік ойыны. Студенттерге жобалау және қауіпсіздік саясаты бойынша берілген техникалық тапсырмаға сәйкес деректерді берудің екі корпоративтік желісін құру тапсырмасы беріледі. Оқушылар екі топқа бөлінеді. Әрбір студентке дизайн және конфигурация үшін жауапкершілік жүктеледі жеке желілік модуль (мысалы, Интернет периметрі, деректер орталығы, LAN, филиалдық желі). Содан кейін барлық сегменттер Cisco Packet Tracer желілік механизмдері арқылы қосылады. Желілер орналастырылғаннан кейін студенттер желілер мен

модульдерді өзгертеді. Бұл ретте жаңа желінің конфигурациясын зерттеу және талдау, егер бар болса, жобалау және енгізу қателерін табу және жою міндеттері шешіледі. Ойын барысында мұғалім қауіпсіздік саясаттарын, желілік инфрақұрылымның жұмыс істеу тәсілін және деректер желілеріне қойылатын талаптарды өзгерту үшін әртүрлі кіріспе нұсқаулар бере алады.

3.2 Қолданыстағы желі технологиялары

Қазіргі уақытта ASUE корпоративтік желісі екі қаланы қамтиды: Астана мен Алматы, негізгі серверлері Алматыда орналасқан.Қолданылатын желілік технологияларды қарастырыңыз.

Топология: желі Ethernet технологиясына негізделген. LAN желісінің өткізу қабілеті 100 Мбит/с, транктердің өткізу қабілеті 100 Мбит/с-тан 1000 Мбит/с-қа дейін. Әрбір қызметкер компьютерге ең жақын қосқышқа қосылатын бөлек кабель арқылы қосылады. Деректердің сақтық көшірмесін жасау арнайы орнатылған серверде орындалады.

Жабдық: Желіде Cisco компаниясының өнімділігі жоғары Catalyst коммутаторлары қолданылады. Серверлер сенімді және қауіпсіз UNIX және Windows NT операциялық жүйелерінде жұмыс істейді. Белсенді желілік жабдықты үздіксіз электрмен жабдықтауды қамтамасыз ету үшін тұрақтандырылған және резервтік қуат көзі қолданылады.

Кабель: 5 және 5e санатындағы бұралған жұпты және бір режимді оптикалық кабельді пайдаланады. Бұл кеңселерге аймақ ішінде кез келген қашықтықта қосылуға мүмкіндік береді және 100 Мбит/с деректерді беру жылдамдығын қамтамасыз етеді.

Желі қауіпсіздігі: Ішкі желінің қауіпсіздігін қамтамасыз ету үшін компания тек периметрлік маршрутизаторды пайдаланады. ASUE қауіпсіздік мақсатында келесі әдістер мен жүйелерді қолданады:

1. Брандмауэр, шабуылдың алдын алу жүйесі және VPN хабы бар Cisco ASA 5510 адаптивті қауіпсіздік құралы.
2. Деректер мен деректер қорларының сақтық көшірмесін автоматты түрде жасау.
3. Тұрақты ток көздері.
4. Пайдаланушылардың қауіпсіздік саясаты, қол жеткізу құқықтарын шектеу.

3.2.1 Қашықтан қол жеткізу

"ASUE" компаниясының мобильді пайдаланушылардың шағын тобы бар(бұл сату бөлімшесінің өкілдері және жүйелік инженерлер),Windows NT

жүйелері орнатылған ноутбук компьютерлерін пайдалану. Бұл пайдаланушылар тиісті бөлімшелердің серверлеріне кіруді талап етеді. Кейбір қызметкерлер үнемі қажет Windows NT жүйелері орнатылған компьютерлерінен компания желісіне қашықтан қол жеткізу. Сонымен қатар, компаниябірнеше шалғай филиалдары бар, оларда орнатылған Cisco 1720 маршрутизаторлары бас кеңсенің аумақтық желісімен байланысу үшін сұраныс бойынша маршруттауды пайдаланады. Компания рұқсат беруді жоспарлап отыржоспарлау аумақтық желіге және жеткізушілерге желіге қашықтан қол жеткізуге мүмкіндік беру арқылы әзірлеу бөлімшелері. Қашықтан қол жеткізуді басқару үшін"ASUE" компаниясы Cisco 3640 желілік қатынау серверлерін пайдаланады Catalyst сериялы Ethernet қосқыштары және Cisco 4700 аумақтық желі маршрутизаторлары.

3.2.2 Интернетке қол жеткізу

ASUE интернет-провайдеріне (ISP) жоғары жылдамдықты қосылымға ие. ISP желісі – бұл компания өнімдері туралы ақпаратты қамтитын веб-серверлерге, сондай-ақ демонстрациялық бағдарламалық қамтамасыз ету және тиісті өнім құжаттамасы бар FTP серверін орналастыратын корпоративтік бастион сайтына қосылған Cisco 1720 AN маршрутизаторынан тұратын периметр. Бұл ресурстар сыртқы Интернет пайдаланушыларына, соның ішінде тұтынушылар мен компания қызметкерлеріне қолжетімді. Компанияның негізгі мақсаты - жеткізу шектеулері бар Интернеттен бастион түйініне қауіпсіз қосылуды қамтамасыз ету

"ASUE" компаниясының мамандары әлі күнге дейін дәлелсіз дәлелдері болмаса да, мейірімсіз адамдар компанияның желісіне Интернет арқылы қол жеткізді деп күдіктенеді. Компанияның веб-торабы варварлық түрде жойылды. Байланысты маршрутизатордың параметрлері Интернет нәтижесінде шабуылдар заңды пайдаланушылар Интернетке мүлдем кіре алмайтындай етіп өзгертілді.

3.2.3 Компанияның бөлімшелері

Компанияның үш бөлімшесі желіні пайдалануға және қорғауға мүдделі, атап айтқанда: Ақпараттық жүйелер, әзірлеу және сату бөлімшелері.

3.2.4 Ақпараттық жүйелер бөлімшесі

Бұл бөлімшеде желіні басқару орталығы болып табылатын Бір Windows NT сервері бар. Бұл бөлім барлық желілік құрылғыларға Telnet арқылы қол жеткізе отырып, желінің, серверлердің және жұмыс станцияларының әкімшілік бақылауы мен жалпы жұмысына жауап береді.

3.2.5 Сату бөлімшесі

Өткізу ішкі желісінің құрылымы келесі сипаттамаларға ие.

Ішкі желінің жұмыс станциялары Windows NT/XP жүйесінде жұмыс істейді.

Мобильді өкілдер мен сату инженерлері Windows XP операциялық жүйесімен алдын ала орнатылған ноутбуктерді пайдаланады. Олар қашықтағы филиалдар мен маршруттауды пайдалана отырып, Cisco 1720 маршрутизаторлары арқылы бас кеңсе желісіне қол жеткізеді. Windows NT серверінде сатуды қолдау бағдарламалары, тарату дерекқорлары және файл сервері бар. Қашықтағы пайдаланушылар модемдер мен аналогтық теру желілерін пайдаланып Cisco 3640 желіге кіру серверіне қосылады. Әзірлеу бөлімінің ішкі желісінде UNIX немесе Windows NT жұмыс істейтін жұмыс станциялары бар. Компанияның желісіне қашықтан қол жеткізуді қажет ететін инженерлер Windows NT операциялық жүйесі орнатылған қарапайым дербес компьютерлер мен ноутбуктерді пайдаланады. Қашықтағы пайдаланушылар Cisco 3640 желіге кіру серверіне модемдер және аналогтық теру желілері арқылы қол жеткізеді. Әзірлеу бөлімінде басқа қызметкерлерге қолжетімді өнімді әзірлеу ақпаратын сақтайтын Windows NT серверлері орналасқан. Инженерлік бөлім мен басқа жергілікті желі арасындағы байланыс Catalyst Ethernet қосқышы және Ethernet портын пайдаланатын Cisco 4700 маршрутизаторы арқылы жүзеге асырылады.

3.2.5 "ASUE"компаниясының желілік қорғау мақсаттары

Cisco ASA series адаптивті қорғаныс құрылғысын қолдану негізінде "ASUE" компаниясы сайып келгенде өзінің желілік ортасын қорғағысы келеді. Ол А қосымшасындағы А. Көрсетілгендей қорғалған желіні алуға үміттенеді.

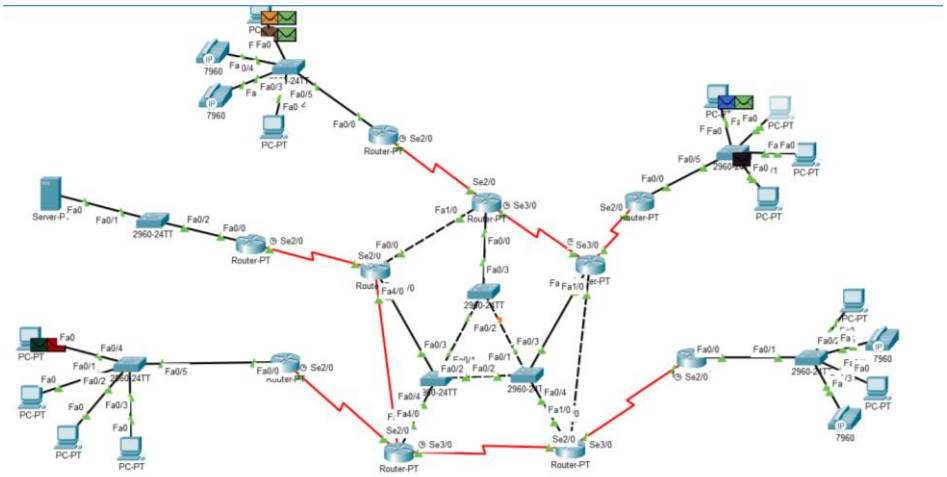
Бұл қорғалған желінің топологиясы А қосымшасындағы А. 3.2.6-суретте көрсетілген.

Жобаның негізгі міндеттері:

1. Ішкі желінің сыртқы қауіптерден қауіпсіздігін қамтамасыз ету.
2. Кіріс және шығыс трафикке қол жеткізуді басқару.
3. Аутентификация, авторизация және аудит (AAA) жүйесін жетілдіру.
4. Бас ұйымдар мен олардың филиалдары арасындағы сенімді және қауіпсіз өзара іс-қимылды қамтамасыз ету.

3.2.6 Желінің периметрін қорғау жүйелері

3.9-суретте көрсетілген диаграмма сақина топологиясында қосылған маршрутизаторлардан тұратын провайдер желісінің бөлігі болып табылады



3.9-сурет – Желіні құру схемасы

Алдымен әрбір интерфейс үшін IP мекенжайлары бар маршрутизаторларды орнату керек (1-кесте), содан кейін маршрутизаторлар арасында статикалық маршруттауды конфигурациялау керек. Содан кейін R8 маршрутизаторы үшін статикалық NAT және R5, R6, R7, R9 маршрутизаторлары үшін динамикалық NAT конфигурациялау керек. R6 және R9 маршрутизаторлары мен SW1 және SW2 қосқыштары үшін VoIP телефониясын конфигурациялау қажет.

Ол үшін әрбір құрылғының консоліне өтіп, әр құрылғыға қажетті пәрмендерді теріңіз. Әрине, олар берілген желідегі функцияларына сәйкес әр құрылғы үшін әртүрлі болады. Осыдан кейін желіні орнату аяқталады.

Кесте 3.2 – IP-адреса роутеров

Құрылғы	Интерфейс	IP-мекенжай	Бетперде
R0	fa 0/0	1.1.1.1	255.255.255.0
	fa 1/0	2.2.2.2	255.255.255.0
	fa 2/0	3.3.3.2	255.255.255.0
	fa 3/0	4.4.4.4	255.255.255.0
R1	fa 0/0	10.10.10.2	255.255.255.0
	fa 1/0	12.12.12.1	255.255.255.0
	fa 2/0	3.3.3.1	255.255.255.0
	fa 3/0	4.4.4.4	255.255.255.0
R2	fa 0/0	7.7.7.2	255.255.255.0
	fa 1/0	12.12.12.2	255.255.255.0
	fa 2/0	11.11.11.1	255.255.255.0
	fa 3/0	4.4.4.5	255.255.255.0
R3	fa 0/0	7.7.7.1	255.255.255.0
	fa 1/0	8.8.8.1	255.255.255.0
	fa 2/0	6.6.6.2	255.255.255.0
	fa 3/0	4.4.4.1	255.255.255.0
R4	fa 0/0	5.5.5.1	255.255.255.0
	fa 1/0	2.2.2.1	255.255.255.0
	fa 2/0	6.6.6.1	255.255.255.0
	fa 3/0	4.4.4.2	255.255.255.0
R5	fa 0/0	1.1.1.2	255.255.255.0
	fa 1/0	20.20.20.1	255.255.255.0
R6	fa 0/0	5.5.5.2	255.255.255.0
	fa 1/0	22.22.22.1	255.255.255.0
R7	fa 0/0	8.8.8.2	255.255.255.0
	fa 1/0	21.1.1.1	255.255.255.0
R8	fa 0/0	10.10.10.1	255.255.255.0
	fa 1/0	13.13.13.1	255.255.255.0
R9	fa 0/0	11.11.11.2	255.255.255.0
	fa 1/0	16.16.16.1	255.255.255.0

Желінің периметрін қорғау – бұл желі шекарасын қорғауға және рұқсатсыз кіруді болдырмауға бағытталған технологиялық шешімдердің жиынтығы.

Периметрлік қорғаныс әдетте корпоративтік желіні қорғауға бағытталған және желінің әртүрлі бөліктері арасындағы байланысты қорғау үшін бірдей әдістер мен технологиялық шешімдерді пайдалана алады.

Cisco ASA сериялы адаптивті қауіпсіздік құралдары қауіпсіздік мүмкіндіктерінің кең ауқымын ұсынады, бұл оларды бүгінгі күні саланың жетекші желілік қауіпсіздік құралына айналдырады.

Периметрлік маршрутизатормен пайдаланған кезде, ASA сіздің жеке желіңіз бен сыртқы әлем арасында өтпейтін тосқауыл жасайды. Ұсынылған қауіпсіздік конфигурациясы ASA қауіпсіздік құрылғыларын орналастыратын бірінші жол ретінде Cisco маршрутизаторын пайдалануды қамтиды.

Шабуылдаушы желідегі аутентификация ережелерін, кіру тізімдерін және маршруттарын алдау арқылы қауіпсіздік жолын айналып өтуге тырысса да, ASA желілік қауіпсіздіктің ең жақсы құралдарының бірі болып табылады.

ASA желіні ішкі және қарусыздандырылған желіге бөлуге мүмкіндік беретін бірнеше интерфейстерге ие, ал «мөлдір» брандмауэр механизмі (мөлдір брандмауэр) желі топологиясын өзгеріссіз сақтауға мүмкіндік береді. Бұл ASA шабуылдаушыларға көрінбейтін болады, бірақ пайдаланушылар үшін жоғары деңгейдегі қорғанысты қамтамасыз етеді.

Периметрді қорғау жүйесінің маңызды міндеттерінің бірі ішкі және сыртқы желілерді аймақтарға бөлу болып табылады. 3.2.6-суретте ASA қауіпсіздік құралының астындағы корпоративтік желінің ішкі желі аймағы көрсетілген, ал сыртқы бөлігі Интернетке немесе сыртқы бизнес серіктестерге қосылған.

Желілік қауіпсіздік саясатын жүзеге асыру сыртқы үшін пайдалануға болатын периметрлік қауіпсіздік құрылғыларының өзара әрекетін қамтиды желінің таңғы және сыртқы бөліктері. Периметрлік қауіпсіздік саясатының ерекшеліктері қауіпсіздік деңгейіне, бюджетке және басқа факторларға байланысты өзгеруі мүмкін.

Бұл жоба экрандалған ішкі желі архитектурасы ретінде белгілі желі периметрін қорғау жүйесін құруды қарастырады, мұнда бірінші қорғаныс сызығы периметрлік маршрутизатор (қалқан маршрутизатор) арқылы жасалады, ал екінші жол желіаралық қалқанға негізделген. Жүйеде қолданылатын құрылғылардың әрқайсысының функцияларын қарастырыңыз.

3.2.7 ASA қауіпсіздік құрылғылары арқылы кіруді конфигурациялау

Компания Cisco ASA қорғаныс құралын сатып алды қазірдің өзінде қазірдің өзінде маршрутизатордың p периметрінде және bastionic xsyss ішкі желінің қорғаныс аймақтарында қол жетімді. Сізге, мысалы, қажетсіз кіруді шектеу үшін b брандмауэр орнату қажет және t бірақ талдау бөліміндегі адамдардың өз бетінше әрекет ету мүмкіндігін ұмыту керек. жұмыс.

Желінің үлесіне (компанияның атауы) қарайық. f назар аударатын болсақ, бұл ішкі s желілік ресурстарды қорғау жүйесін құру, pin қызмет көрсету үшін шектеулердің ең аз санына дейін d қолжетімділікті d алып тастау болып көрінді. орындау және p өндіріс функциялары.

Pwlifefirm(name to company) ішінде іске асырылғысы келетін желі қорғанысының саяси актері, p тиісті білдіреді:

а) компанияда NAT тапсырмаларын орындау үшін ASA қорғаныс құрылғысын енгізуде;

б) x stay DNS бар трафиктің және шығыс трафиктің s тактикасын орнату;

c) кіріс трафигі үшін тактикамен және k арналармен орнату;

d) access telnet үшін ASA қорғаныс құрылғысын n реттеу;

e) ping қол жеткізу үшін ASA-ны реттеу.

у конфигурациясын тексергеннен кейін, k пәрменін no conduit permit icmp енгізу арқылы conduit permit icmp any any echo-reply пәрменін береміз.Кез келген echo-r қабылдаймыз.

3.2.8 AAA интерфейстер менқұралдар жинағын орнату

Компанияға p компания жерінде r орналасқан ASA қорғаныс құрылғысын енгізуді талап етеді. Сенімділік үшін компанияда желінің кез келген секторына және желілік қосылымдардан қорғауға кепілдік беретін 2xonline ұсыныс провайдері бар.

Желінің құрылымына және желілік қорғаныстың саясаткеріне фирмалардың тиісті талаптарымен сатылуы керек.

3.3 Жалпы пернелермен жұмыс істеу үшін IPSec VPN құралдарын орнату

IPSec (IP security – ашылған құпиялылық стереотиптерінің жиынтығына, e диналдылыққа және деректер алмасудың тең мүшелері арасындағы деректердің аутентификациясына) жеке тұлғаны қорғаудың ашылған стереотиптерінің негізі мен қолданылуын оқыңыз желілермен байланыс IP.

IPsec құпиялылығын, e идентификаторын және d деректерді p қайта жіберу кезінде жәнех ашық желілер стереотиптері арқылы e сенімділігін қамтамасыз етеді. Бұл жағдайда құрылғылар арасындағы барлық деректер ағынын шифрлауға болады қорғау немесе тек жеке түйіндер немесе желінің бөліктері арасындағы деректер ағыны,қорғаныс құрылғыларының артында орналасқан. Корпоративтік тұтынушылар жеке желілер үшін қол жетімді барлық артықшылықтарды, соның ішінде қауіпсіздікті алыңыз,қызмет көрсету сапасы (QoS), басқарушылық және сенімділік.IPSec шифрлау құралдарын, қауіпсіздік құралдарын конфигурациялағанда келісілген алдын ала ортақ кілттерді пайдаланатын ASA шешімдерін қабылдауы керек келесі төрт тапсырма.

1-тапсырма: IPSec бағдарламасын пайдалануға дайындалу

2-тапсырма:алдын ала келісілген жұмыс істеу үшін IKE конфигурациялаңыз пернелер.

3-тапсырма: IPSec конфигурациялау.
4-тапсырма. IPSec тестілеу және бақылау.

3.3.1 Cisco периметрі маршрутизаторлары

Периметрлік Маршрутизатор қорғалмаған Интернет пен "лас" DMZ ретінде ұсынылған жартылай қорғалған "демилитаризацияланған аймақ" (DMZ) арасындағы шекараны құру үшін пайдаланылуы мүмкін.

Периметрлік маршрутизатор ретінде көбінесе Cisco1720 типті кәдімгі маршрутизатор қолданылады, ол Интернетке және Ethernet-ке DMZ-ге сериялық қосылуды қамтамасыз етеді. Cisco Маршрутизаторлары

Интернет байланысын қорғауға мүмкіндік беретін икемді периметрлік қорғаныс құралдары бар. Cisco маршрутизаторы келесі мүмкіндіктерді ұсынады.

- DMZ (немесе көрсетілгендей"лас" DMZ) анықтайтын бірінші қорғаныс желісін құру DMZ Бастион түйіндерін қорғауды қамтамасыз етеді және ASA қорғаныс құрылғысы бағытталған шабуылдардан және периметрлік маршрутизаторды бұзу әрекеттерін анықтаған кезде ескерту жүйесінің рөлін атқарады немесе Бастион хосты.
- Сіз жасай алатын теңшелетін мүмкіндіктердің икемді жиынтығы үнемі пайда болатын жаңа қорғаныс қатерлеріне және жаңа Интернет қосымшаларына бейімделу.
- Cisco IOS бағдарламалық жасақтамасының кіріктірілген мүмкіндіктерін, соның ішінде МЭС-ның арнайы мүмкіндіктері мен қорғаныс құралдарын пайдалану периметрі.

TCP/IP қызметтері мен қолданбаларына қол жеткізуді шектеу үшін периметрлік маршрутизатор негізінен пакеттерді сүзу ережелерін қолданады.пайдаланылады. Қатынас тізімдері желілік қауіпсіздік саясатының талаптарына сәйкес келетін ережелерді жүзеге асыру үшін пайдаланылады.пайдаланылады. Периметрлік маршрутизатор лас DMZ немесе экрандалған ішкі желіні жасайды. Cisco ASA көмегімен сіз қорғаныс аласыз қауіпсіз» DMZ құру және құрылғының үшінші интерфейсіне Bastion түйіндерін орналастыру.

Cisco инженерлері Cisco IOS бағдарламалық жасақтамасының ядросында бірқатар периметрлік қауіпсіздік мүмкіндіктерін енгізді,бұл

Cisco тұтынушыларына өздерінің ішкі желілеріне желіге кіруді басқарудың негізгі құралы ретінде маршрутизаторларды пайдалануға мүмкіндік береді.

Мүмкіндік береді. Қауіпсіздік мүмкіндіктеріне пайдаланушы аутентификациясы, кіру рұқсаты, белгісіз немесе қажетсіз мекенжайларға қосылымдарды шектеу, сыртқы контроллерлер үшін ішкі IP мекенжайларын

пайдалану,маршрутизатор арқылы өтетін деректер ағынын бақылау, сондай-ақ қауіпсіздік саясатының талаптарын орындау.

Желінің периметрі жүйесі басқару үшін арнайы құралдарды пайдалануға мүмкіндік береді. опциясы қауіпсіздік саясатына сәйкес Cisco Enterprise Perimeter Router ASUE конфигурациялау болып табылады,өтініште көрсетілген.

"ASUE" компаниясының корпоративтік желісі үшін Cisco периметрі маршрутизаторын оның қорғау саясатына сәйкес баптау нұсқасы В қосымшасында ұсынылған.

3.3.4 Демилитаризацияланған аймақтар (DMZ)

DMZ немесе оқшауланған жергілікті желі-бұл корпоративті желі мен сыртқы әлем арасындағы буфер. DMZ корпоративтік желі нөмірінен ерекшеленетін бірегей желі нөміріне ие. Жалпы айтқанда, DMZ желісі корпорация желісінің сырттан көрінетін жалғыз бөлігі болып табылады.

DMZ периметрді қорғау құрылғыларымен жасалад периметрлік маршрутизатордан тұратын брандмауэр жүйесі,Бастион хосты және брандмауэрдің өзі.

Периметрлік Маршрутизатор сыртқы және ішкі пайдаланушыларға қызмет көрсететін Бастион хостының ішінара қорғалған ортасы болып табылатын "лас" DMZ жасайды, мысалы,TCP/IP электрондық пошта релесі қызметін ұсынатын кәсіпорынның веб-торабы немесе қолданбалы деңгей шлюзі.

3.3.5 Бастион хосты

ASA арқылы мультимедиялық қолданбаларға қол жеткізген кезде PAT құралдарын пайдаланудан аулақ болу ұсынылады, өйткені мұндай қолданбалар көбінесе PAT портының спецификация құралдарын пайдаланумен қайшы келуі мүмкін арнайы порттарды қажет етеді.

Оның орнына, кейбір жағдайларда порт трафигі конфигурациясын сақтау үшін Nat 0 пәрменін пайдалануға болады. Суретте көрсетілген желілік диаграммада. 3.11 PAT құралдарын қолдануға болатын ең аз конфигурацияны көрсетеді. XYZ компаниясында үш тіркелген IP мекенжайы бар. Периметрлік маршрутизатор, ASA және Bastion хосты барлығы осы мекенжайлардың бірін алады (Bastion хосты әдетте Интернеттен қол жетімді жалғыз хост, мысалы, веб-сервер немесе пошта сервері).

Кейде Бастион хосты делдал қызметін ұсынады бұл арнайы бағдарлама немесе серверлік бағдарламалар. Делдал сервисі пайдаланушылардың Интернет-қызметтерді ұсынуға сұраныстарын қабылдауды көздейді(электрондық пошта, FTP немесе Telnet жіберу түрі) және кейінгі

тасымалдау желілік қорғау саясаты негізінде осы қызметтерді ұсынатын қызметтерге сұраныстар.

Егер Бастион хосты делдал қызметін қамтамасыз етсе, ол осындай делдалдық жүзеге асырылатын қосымшалар туралы хабардар болуы керек. Сондықтан Бастион хосты TCP порттарын бақылайды және делдалды қажет ететін қызметтерді анықтау үшін UDP: бұлTelnet, FTP (File Transfer Protocol - файлдарды тасымалдау протоколы), HTTP (Hypertext Transfer Protocol-гипермәтіндік файлдарды беру хаттамасы), gopher, WAIS(Wide Area Information Server - ғаламдық ақпараттық сервер), NTP(Network Time Protocol - синхрондау желілік протоколы), NNTP(Network News Transfer Protocol-желілік жаңалықтар протоколы) және SMTP(Simple Mail Transfer Protocol - қарапайым электрондық пошта протоколы).

Бастион хостын екі арналы хост ретінде де конфигурациялауға болады, яғни екі желілік интерфейсі бар: біреуі ішкі желі үшін, алекіншісі сыртқы үшін. Мұндай конфигурацияда Бастион хосты МЭС қызметін қамтамасыз ете алады.Мұқият мониторинг жүргізу қажетБастион хостының күйлері оны уақытында бұзуға тырысады олар бұлтартпады, өйткені желі екі арналы хост конфигурациясында ерекше осал. Екі арналы хостпен салыстырғанда, ASA айтарлықтай сенімді қорғауды қамтамасыз етеді, сондықтан брандмауэр жүйесін құру кезінде соңғысын қолданған жөн.

3.3.6 Брандмауэр

Брандмауэр-бұл мамандандырылған желілік құрылғы ішкі желіні сыртқы әсерлерден қорғау. Мыналар бар ерекшеліктері:

- трафиктің тар нүктесі бар - бүкіл деректер ағыны желі ішінен сыртқа және сырттан желінің ішкі жағына брандмауэр арқылы өту керек;
- сәйкес авторизациядан өткен трафикке ғана рұқсат етілмейді.Жергілікті қорғау саясаты;
- брандмауэр оны қорғау мүмкін болмайтындай етіп реттеледі жеңу;брандмауэр ішкі желіні сыртынан көрінбейтінетеді.Брандмауэрлерді бірнеше жолмен жүзеге асыруға болады:

Пакеттік сүзгі. Әрбір пакетті берілген пакеттің бар-жоғын тексереді пайдаланушы параметрлерді (IP мекенжайлары немесе TCP және UDP порттары), бірақ жоқ сеанстарды бақылауды жүзеге асырады.

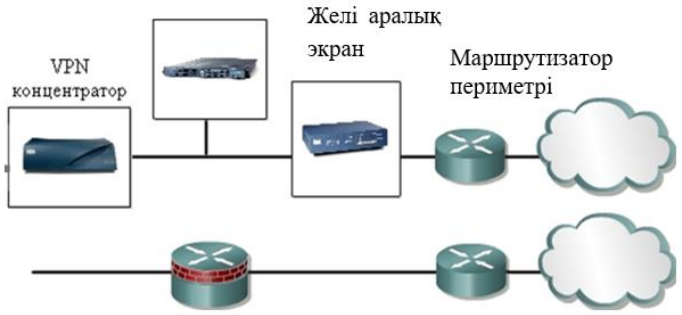
Қолданбалы деңгей шлюзі. Қолданбалы деңгей деректерін тексереді байланыс орнатылғанға дейін ол арқылы өтетін барлық пакеттер. Арқылы брандмауэр тек рұқсат етілген деректердің қозғалысына мүмкіндік береді.

Мысалы, қолданбалы деңгейдегі FTP шлюзі FTP пакеттерін тексереді тек рұқсат етілген FTP қатынасын ашады.

Арна деңгейіндегі Шлюз. Брандмауэр арқылы өтетін қосылымды (арнаны) ашпас бұрын TCP және UDP сеанстарының заңдылығын тексереді.Мұндай шлюз кепілдік беру үшін TCP және UDP сеанстарының деректерін қарастырады брандмауэр арқылы тек рұқсат етілген пакеттер арқылы өту. Сеанстың басында брандмауэр осы сеанстың жарамды қосылымдарының кестесін жасайды және бұл кестенің кейбір жазбаларының сеанс параметрлері сәйкес келген жағдайда ғана деректердің өтуіне мүмкіндік береді. Сеанс аяқталғаннан кейін кестенің тиісті жазбасы жойылып, арна жабылады.

Прокси-сервер(делдал сервер).Ішкі желі хостының IP мекенжайын ауыстыру арқылы ішкі (қорғалған) желіні қорғайды брандмауэр арқылы өтетін барлық деректер ағыны үшін жергілікті IP мекенжайы. Бүгінгі таңда ұсынылатын шлюздердің көпшілігі қолданбалы және арна деңгейлерінде прокси-сервердің кіріктірілген мүмкіндіктері бар қосымша қорғауды қамтамасыз етіңіз. Брандмауэр өндірушілері мұндай өнімдерді көбінесе қолданбалы деңгейдегі прокси-серверлер немесе арна деңгейіндегі прокси-серверлер деп атайды

ASA қорғаныс құрылғысы (3.10-сурет) қорғаныс механизмдерін қамтиды брандмауэр көмегімен периметр, жүйенің көмегімен шабуылдарды тойтару антивирус, спамға қарсы, антиспайвар, фишингке қарсы және интернет-сайттарға кіруді бақылау арқылы зиянды бағдарламалармен күресу, қашықтан қол жетімділікті және кеңсеаралық өзара әрекеттесуді қорғау үшін VPN құру.[8]



3.10-сурет — Cisco ASA қорғаныс құрылғысы

"ASUE" компаниясы ішкі желіні бұзушылардан қорғау мақсатында бұрыннан бар периметрлік маршрутизатормен және Бастион хосттарымен жұмыс істеу үшін Cisco ASA series қорғаныс құрылғысын сатып алды. Қажетсіз қол жетімділікті шектеу және сонымен бірге талдау бөлімінің қызметкерлеріне өз жұмысын орындау мүмкіндігін қалдыру үшін қорғаныс құрылғысын осылай конфигурациялау қажет.

3.4 Кіріс және шығыс қол жетімділікті бақылау

ASA арқылы өтетін трафиктің әрбір пакетінде сәйкес аударма жазбасы (жаһандық немесе статикалық) болуы керек деген талапты көрсетеді. Егер мұндай жазба болмаса, ASA әдепкі бойынша "Nat-control" өшірілген конфигурацияға айналады. Дегенмен, бұл әрекетті «nat-control» пәрменін беру арқылы өзгертуге болады.

"nat-control" өшірілген кезде, ASA арнайы аударма жазбасы жоқ пакеттерді қауіпсіз емес интерфейстен қауіпсіз интерфейске қайта бағыттай алады. Бұл трафиктің қауіпсіз емес интерфейстен неғұрлым қауіпсіз интерфейске өтуіне мүмкіндік беретін сәйкес кіру тізімдерін қажет етеді.

«Көптен бірге» деп те белгілі Pat (Порт мекенжайының аудармасы) пайдалану барлық ішкі желілік трафикті бір сыртқы IP мекенжайына қайта бағыттауға мүмкіндік береді. Қауіпсіз желі түйіні Интернет арқылы қолжетімді ресурсты сұраған кезде ASA қауіпсіздігі құрылғының NAT кестесін басқарады. Сұранысқа қажетті ақпаратты қамтитын тиісті жазба қоса беріледі. Бұл мысалдар табиғатта тән, бірақ олар қол жеткізуді басқару әдістеріне толық сипаттама бермейді. Кез келгенін пайдаланған кезде кіру шектеулері пайдаланушылар өздерінің еркіндігі тым шектеулі деп шағымдана алады. Мұндай жағдайда ең жақсы шешім-алдымен максималды шектеулер қою, содан кейін оларды біртіндеп әлсірету (пайдаланушылардың белгілі бір мүмкіндіктерге рұқсат беру туралы өтініштері түскен кезде). Осы немесе басқа шешімнің орынды болатындығын анықтау үшін оның негізгі технологияларын нақты түсіну және таңдалған шешім шеңберінде қол жетімді мүмкіндіктерді пайдаланушылар ұсынған сұраулармен салыстыру қажет. ASA қорғаныс құрылғысы бірегей, өйткені ол сұраныстардың өте кең ауқымын қанағаттандыра алады.

3.4.1 Шығыс қатынасты басқаруды орнату

Шығыс қатынасты басқаруды орнату қауіпсіздік жүйесінің маңызды бөлігі болып табылады, өйткені қорғалған желіге кіруді шектеу оның мақсаттарының бірі ғана. Түрлі орталарда, кәдімгі кеңсе, ірі корпорация немесе тіпті әскери база болсын, кіріс ағынын басқару сияқты маңызды болып саналатын шығыс деректер ағынын басқару енгізіледі.

ASA Security Appliances шығыс қатынасын басқару элементтерін оңай конфигурациялауға және өзгертуге мүмкіндік беретін функционалдылықты ұсынады. Осы функциялардың ішінде ең маңыздысы NAT (Network Address Translation) және PAT (Port Address Translation) құралдары болып табылады,

олар сәйкесінше желі мекенжайлары мен порт мекенжайларын аударуға мүмкіндік береді.

ASA құрылғыларында NAT құралдарын пайдалану кезінде әдетте сыртқы желілерге қол жетімді емес IP мекенжайларын пайдаланатын Интернетке қосылған жеке желілерді қосуға болады. Бұл корпоративтік желінің бүкіл IP мекенжай схемасын қайта құрусыз Интернет арқылы тіркелмеген клиенттерге қолжетімділікті қамтамасыз етеді. Сонымен қатар, NAT құралдарын пайдалану ұйымның ішкі желісінде пайдалануға болатын мекенжай кеңістігін айтарлықтай кеңейтуге мүмкіндік береді.

Ішкі хост шығыс қосылымды бастағанда, NAT құралдары ішкі желіге ғаламдық және статикалық IP мекенжайларын тағайындайды. Бұл мекенжайлар шығыс трафиктің бастапқы нүктелері ретінде пайдаланылады және қорғау үшін қажет кез келген IP мекенжай схемасын қамтамасыз ету үшін қауіпсіз желіге аударылады.

ASAs сонымен қатар NAT құралдарын пайдаланып сыртқы желілерге көрінуден ішкі мекенжайды қорғауды қамтамасыз етеді. NAT құралдарының үш түрі бар екені белгілі, олардың әрқайсысы жоғары конфигурацияланады.

Бірінші түрі - статикалық NAT құралдары. Олар әрбір ішкі желі мекенжайы статикалық (яғни бірегей) болған жағдайда қолданылады.

Сыртқы желі мекенжайымен салыстырады. Бұл жағдайда көрсету процесі өзгермейді және оны басқару айтарлықтай күш салуды қажет етуі мүмкін.

Екінші түрі - динамикалық NAT құралдары. Олар ішкі желідегі хосттан трафикті ұстайды және оны ASA тіркелген IP мекенжайлары арқылы сыртқы желіге таратады. Аудару процесі туралы ақпарат ішкі хостқа қайтарылатын трафикті рұқсат етуге мүмкіндік беретін кестеде сақталады.

Үшінші түрі - порттарға арналған NAT нұсқасы болып табылатын PAT (Port Address Translation) құралдары. Олар ASA сыртқы интерфейсіне тағайындалған IP мекенжайы негізінде жұмыс істейді және ішкі хост қосылымдары бар бастапқы мекенжайларды сол IP мекенжайымен салыстыруға мүмкіндік береді. ASA TCP немесе UDP пакеттері үшін жаңа бастапқы порт нөмірлерін таңдайды және тағайындайды және транзиттік кері трафикті қамтамасыз ету үшін салыстыру процесі туралы ақпаратты сақтайды.

Шығыс қатынасты басқару үшін NAT конфигурациялау кезінде ASA ішкі бастапқы мекенжайларды жаһандық NAT пәрмендерінде көрсетілген тіркелген сыртқы мекенжайларға қайта бағыттайды. Ғаламдық пәрмен әрбір шығыс қосылымға тағайындалған және барлық пакеттер үшін бастапқы IP мекенжайы ретінде пайдаланылатын жаһандық мекенжайлар пулын анықтайды.

NAT пәрмені NAT құралдарын белсендіреді және оларды статикалық пәрмендерде көрсетілген IP мекенжай пулымен байланыстырады. Бұл пәрмен икемді шығыс қатынауды басқаруды қамтамасыз ете отырып, әрбір ішкі мекенжай үшін аударманы жеке қосуға немесе өшіруге мүмкіндік береді.

Шығыс кіруді басқару үшін NAT орнату.Бұл бөлімде Nat қаражатын сыртқы желілерге бағытталған трафикке қолдану қарастырылады. ASA қорғаныс құрылғысы ішкі бастапқы мекен-жайларды ASA тағайындаған сыртқы тіркелген мекен-жайларға жіберуі үшін Global командалары қолданылады (outside) және Nat (inside).

Global командасы.

Ғаламдық мекен-жайлар пулын анықтайды. Бұл бассейн әрбір Шығыс қосылымға және одан туындайтын барлық кіріс жәшігіне IP мекенжайын береді.

Шығыс Global командасында келесі синтаксис бар:

```
global  1{имя интерфейса)}  global id  глобальн ip[-
глобальн ip] [netmask глобальн маска]
```

Кесте 3.3 — Global командасының параметрлері

Параметр	Сипаттама
интерфейс атауы	Ғаламдық мекен-жайлар қолданылатын сыртқы желі интерфейсінің атауы
global_id	Берілген Global командасы байланысатын nat командасында көрсетілген мәнге сәйкес келетін оң сандық мән.
глобальн_ip	ASA қосылыстар үшін пайдаланатын жаһандық IP мекенжайларын орнатады. Егер сыртқы желі интернетке қосылған болса, онда әрбір жаһандық IP мекенжайы желілік ақпарат орталығында (NIC) тіркелуі керек. IP мекенжайларының ауқымын оларды сызықшамен бөлу арқылы сипаттауға болады (-).Бір IP мекенжайын көрсету арқылы Pat операторын жасауға болады. Интерфейске осындай бір ғана операторға рұқсат етіледі, бірақ сонымен бірге 65535-ке дейін аударма объектілерін қолдауға болады
netmask	Аргументтің алдында ғаламдық Маска
Глобальн маска	Глобалън_1р мекенжайлары үшін желілік масканы анықтайды. Егер ішкі желілер бар, олар үшін 255.255.255.128 типті масканы қолданыңыз. Адрестер ауқымы мен ішкі желі маскаларын тиісті түрде таңдағанда, global командасы Ғаламдық мекен-жайлар пулының хабар тарату және желілік мекен-жайларын пайдаланбайды. Мысалы, егер сіз 255.255.255.224 мәнін және 209.165.201.1-ден 209.165.201.30-ға дейінгі мекен-жайлар ауқымын қолдансаңыз, онда хабар тарату 209.165.201.31 мекенжайы және 209.165.201.0 желілік мекенжайы жаһандық мекенжайлар пулына қосылмайды

Nat командасы.

Nat қаражатын белсендіреді. Бұл команда желіні global және static командалары сипаттаған IP мекенжайларының пулымен байланыстырады. Nat пәрмені әрбір ішкі мекенжай үшін мекенжай трансляциясын жеке белсендіруге немесе өшіруге мүмкіндік береді.

Nat командасының көмегімен желілік мекен-жайларды аудару ережелерін дәлірек орнатуға болады, бұл (3.3-кесте) жеке мекен-жайлармен де, мекен-жайлар ауқымымен де жұмыс істеуге мүмкіндік береді.

Nat командасында келесі синтаксис бар:

Кесте 3.4-Nat командасының параметрлері

Параметр	Сипаттама
интерфейс атауы	Ішкі желі интерфейсінің атауын көрсетеді. Егер интерфейс кіру тізімімен байланысты болуы керек, содан кейін интерфейс атауы көбірек интерфейс болуы керек қорғаудың жоғары деңгейі
nat_id	Nat_id мәндері бірдей барлық Nat командалары бір nat тобына жатады.
локалъи_ip	Таратылатын ішкі желінің IP мекенжайын орнатады.Барлық хосттарға Шығыс қосылымдарын орнатуға мүмкіндік беру үшін 0.0.0.0 пайдалануға болады.0.0.0.0 мәнін О дейін қысқартуға болады
маска	Жергілікті ip үшін желілік масканы көрсетеді. 0.0.0.0 Ғаламдық IP-мекен-жай пулын пайдаланып барлық шығыс қосылымдарды таратуға мүмкіндік беру үшін пайдалануға болады
Max conns	Көрсетілген интерфейстен TCP қосылымдарының максималды санын анықтайды
Em limit	Жаңадан пайда болған қосылыстардың шекті санын анықтайды. Әдепкі мәні 0 болып табылады,бұл шектеулердің жоқтығын білдіреді.
norandomseq	TCP реттік нөмірлерін рандомизациялауға тыйым салады-пакеттер. Бұл параметрді тек сол жағдайларда қолданыңыз,рандомизация басқа брандмауэрмен орындалған кезде және сәйкес функциялардың тіркесімі нәтижесінде деректер бұрмаланған. Бұл параметрді қолдану ASA құрылғысының қорғаныс жүйесіндегі алшақтықты ашады

NAT қаражатын пайдаланудың алғашқы қадамы-трансляцияны қорғау құрылғысы қолдайтын сыртқы жаһандық мекенжайлар пулына қосылатын мекенжайларды көрсететін global пәрменін қолдану.

ciscoasa (config)#global(outside)1192.168.1.128-192.168.1.254

Outside пәрменінен кейін көрсетілген 1 Саны жаһандық мекенжай пулын қанша ішкі желі пайдаланатынына байланысты идентификатор(global id) болып табылады. Бұл жағдайда трансляция орындалуы керек тек бір ішкі желі үшін, сондықтан 1 мәнін көрсетуге болады. Егер көбірек желілер үшін трансляция қажет болса, 2-ден 2147483647-ге дейінгі мәнді таңдауға болады. Бұл мән global және nat командаларының байланысын анықтайды.

Екінші қадам Nat командасын тікелей қолдану:

ciscoasa(config)# nat (inside) 1 10.1.0.0 255.255.0.0

Мұнда 10.1.0.0 ішкі желісінің барлық мекен-жайлары global_id параметрінің мәні 1-ге тең global командасы көрсеткен Ғаламдық мекен-жайларға жіберіледі.

Қосымша мекенжайларды трансляциялау қажет болса, тиісті nat командасы пайдаланатын жаһандық мекенжайлар пулына сәйкес келетін

global_id нөмірін білу маңызды. 255.255.0.0 желілік маскасы ASA құрылғысына хабар тарату сұраулары тек желіден шыққан кезде орындалуы керек екенін айтады10.10.x.x

ASA құрылғысының параметрлерін бастапқы орнату кезінде барлық ішкі түйіндерге nat 1 0.0.0.0 0.0.0.0 пәрменін қолдана отырып, кез-келген сыртқы түйіндермен байланыс орнатуға рұқсат етілуі мүмкін. Команда nat 1 0.0.0.0 0.0.0.0 мекен-жайларды таратуды қамтиды және барлық ішкі түйіндер (бұл 0.0.0.0 параметрімен анықталады)тиісті Global командасымен қамтамасыз етілген. Nat командасының көмегімен желілік мекен-жайларды аудару ережелерін дәлірек орнатуға болады, бұл мүмкіндік береді жеке мекен-жайлармен де, мекен-жайлар ауқымымен де жұмыс жасаңыз. Керек пәрмен синтаксисі оның орнына 0 таңбасын пайдалануға мүмкіндік беретінін ескеріңіз 0.0.0.0 жолдары. Келесі пәрмен осы таңбаны пайдалану мысалын көрсетеді:

ciscoasa(config)# nat (inside) 1 0 0

Nat 0 командасы

Кейбір ішкі IP мекенжайлары сырттан көрінуі үшін мекенжай трансляциясын өшіруге мүмкіндік береді. Бұл мүмкіндік қауіпсіз желіде тіркелген IP мекенжайлары болған кезде пайдалы болады, олар интернеттен пайдаланушыларға қол жетімді болуы керек.

Nat 0 пәрменін пайдалану қажеттілігі, мысалы желіде веб немесе пошта сервері болған жағдайда, олар болуы керек қол жетімді ғаламтор. Nat 0 пәрменін периметр маршрутизаторындағы кіру тізімімен бірге қауіпсіз желіге тек порт трафигінің белгілі бір түрлеріне қол жеткізуге мүмкіндік беру үшін пайдалануға болады (мысалы, бөлісу үшін аутентификация үшін қорғалған сертификаттарды пайдаланатын сертификаттау орталығы мен Виртуалды жеке желі арасындағы деректер).

ASA құрылғысында екіден көп интерфейсті пайдаланған кезде, Nat 0 пәрмені пакеттің қай интерфейске кететініне қарамастан,бастапқы мекенжайды таратудан бас тартатынын есте ұстаған жөн.

Nat 0 командасының көмегімен сіз ішкі мекен-жайларды таратудан мүлдем бас тарта аласыз. Nat 0 командасындағы Бірінші 0 тиісті ішкі IP мекенжайлары үшін трансляцияны өшіруге мүмкіндік береді, осылайша олар сырттан жеке болады. Егер жергілікті IP мекенжайы мен желі маскасының параметрлері көрсетілсе мәндер 0, содан кейін олар 0.0.0.0 ретінде түсіндіріледі. Біз 0-ді 0.0.0.0 мәнін азайту ретінде қабылдаймыз, бұл барлық нұсқаларды ескеруді білдіреді.

ciscoasa(config)# nat (inside) 0 0 0

Егер тек бір мекен-жай көрінетін болса, онда командалық жолды осы мекен жайға және тиісті маскаға енгізу керек:

ciscoasa(config)# nat (inside) 0 172.16.1.5 255.255.255.255

3.4.2 Nat-control командасы

ASA арқылы өтетін барлық трафиктің белгілі бір түрлендіру жазбасы болуы керек екенін көрсетеді (Global немесе static сәйкестігін тексеру нұсқаулығы бар nat нұсқаулығы); бұл жағдайда ол ASA арқылы өте алады. Бойынша әдепкі бойынша, бағдарламалық жасақтаманың 7.0 нұсқасы бар ASA конфигурациясы no Nat-control пәрменін қолданады. Бұл мінез-құлықты өзгертуге болады Nat-control пәрменін енгізу арқылы.

Nat-control өшірілгенде ASA пакеттерді көбірек жібереді конфигурацияда арнайы түрлендіру жазбасы болмаса, аз қорғалған интерфейске қорғалған интерфейс. Трафик аз қорғалған интерфейстен қорғалған интерфейске өтуі үшін сізге қажет кіру тізімдерін пайдаланыңыз. Нәтижесінде ASA трафикті жібереді.

Порт мекенжайларын трансляциялау

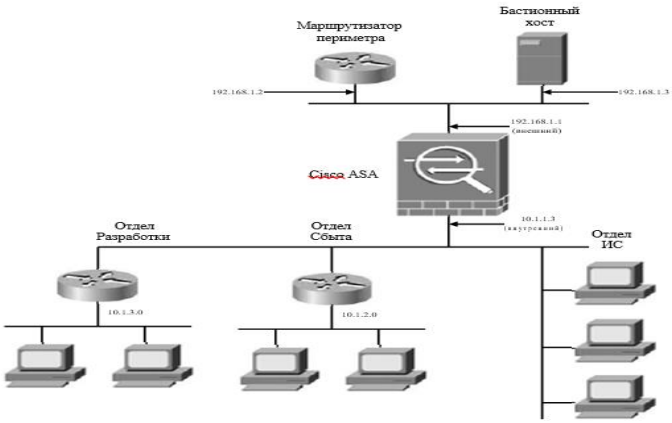
Pat құралдары, көбінесе "көп-бір" типті трансляция деп аталады, ішкі желінің барлық трафигін бір сыртқы IP-мекен-жайға көрсетеді.Қауіпсіз желі хосты Интернет арқылы қол жетімді ресурсты сұраған кезде, құрылғының NAT кестесіне ASA қорғанысы келесі ақпаратты қамтитын тиісті жазба қосылады сұрау:

- жергілікті хост мекен-жайын ASA қорғаныс құрылғысы таңдаған қол жетімді Ғаламдық мекен-жайға жіберу параметрлері;
- хост таңдаған порт нөмірін ASA қорғаныс құрылғысы таңдаған кездейсоқ порт нөміріне аудару параметрлері.
- ASA қорғаныс құрылғысы, сұраныстың қорғалған желінің ішінен шыққанын тексеру үшін хабар тарату деректерін сақтайды және пайдаланады. Сеанс аяқталғаннан кейін тиісті ақпарат жойылады. Төменде бұл процесс толығырақ қарастырылады.
- Pat құралдары ASA қорғаныс құрылғылары мекенжай пулын кеңейтуге мүмкіндік береді келесі мүмкіндіктерді пайдалану негізінде компаниялар:
- Бір сыртқы IP мекенжайын (шамамен)4000 ішкі хост үшін пайдалануға болады. (Теориялық тұрғыдан алғанда, шегі 64000-нан асады, бірақ іс жүзінде 4000 мәні шекті болып табылады).
- Нақты TCP порт нөмірлері белгіленген IP мекенжайында және Порт нөмірінде көрсетіледі, егер арнайы static командасы басқа әрекетті көрсетпесе.
- Ішкі дереккөз мекенжайлары қорғаныс құрылғысы қолдайтын жаһандық мекенжайлар пулынан бір IP мекенжайы арқылы жасырыладыASA.

PAT қаражатын NAT құралдарымен бөлісуге болады және PAT мекенжайы алдыңғы жағындағы порт мекенжайынан басқа виртуалды мекенжай болып табылады.

ASA арқылы мультимедиялық қолданбаларға қол жеткізген кезде PAT құралдарын пайдаланудан аулақ болу ұсынылады, өйткені мұндай қолданбалар көбінесе PAT портының спецификация құралдарын пайдаланумен қайшы келуі мүмкін арнайы порттарды қажет етеді.

Оның орнына, кейбір жағдайларда порт трафигі конфигурациясын сақтау үшін Nat 0 пәрменін пайдалануға болады. Суретте көрсетілген желілік диаграммада. 3.11 PAT құралдарын қолдануға болатын ең аз конфигурацияны көрсетеді. XYZ компаниясында үш тіркелген IP мекенжайы бар. Периметрлік маршрутизатор, ASA және Bastion хосты барлығы осы мекенжайлардың бірін алады (Bastion хосты әдетте Интернеттен қол жетімді жалғыз хост, мысалы, веб-сервер немесе пошта сервері).



3.11 – сурет - Ішкі желі үшін PAT пайдалану 10.1.0.0

ciscoasa(config)! ip address (inside) 10.1.1.3 255.255.252.0
ciscoasa(config)! ip address (outside) 192.168.1.1255.255.252.0
ciscoasa(config)! route (outside) 0 0 192.168.1.2 1
ciscoasa(config)! nat (inside) 2 10.1.0.0 255.255.0.0
ciscoasa(config)! global (outside) 2 192.168.1.4 netmask 255.255.252.0

Бірінші жол 10.1.1.3 IP мекенжайын "ішкі" (inside) деп аталатын ASA құрылғысының интерфейсіне жатқызады; бұл байланысты интерфейс қорғалған желі. Екінші жол "сыртқы" (outside) деп аталатын ASA құрылғысының интерфейсіне 192.168.1.1 IP мекенжайын тағайындайды; бұл қауіпсіз желіден тыс және Интернетке ашық интерфейс. Үшінші жол ASA-ға периметрлік маршрутизатордың 192.168.1.2 интерфейсі арқылы қандай трафикті бағыттауға рұқсат етілгені туралы хабарлайды. Бұл жағдайда трафик, "сыртқы" интерфейстен шығу (IP мекенжайы 192.168.1.1) IP мекенжайы мен желі маскасы үшін командада көрсетілген мәндерге сәйкестігі тексеріледі. Бұл жағдайда барлық трафик қолайлы, өйткені IP мекенжайы үшін де, желі маскасы

үшін де 0 мәндері көрсетілген. (0-0.0.0.0 аббревиатурасы.) Төртінші жол Nat-идентификаторын ішкі 2-ге тағайындайды желі хосттары 10.1.0.0. Соңғы жол 192.168.1.4 мекен-жайын Ғаламдық мекен-жайлар пулына орналастырады және брандмауэрге 192.168.1.4 d IP-мекен-жайы туралы хабарлайды

3.4.3 Пайдалы өткізу қабілетін есептеу

Р өткізу мүмкіндігі қажетті ақпаратты р беру жылдамдығы ретінде түсініледі, оның өлшемі k саны абсолютті тасымалданатын ақпараттан аз болатын кез келген мәні олып табылады, мысалы, кез келген жіберілетін кадр ресми ақпарат,адресатқа дұрыс жеткізуге кепілдік беру.Ethernet желісінің қажетті сыйымдылығына кідірістердің жәнесоқтығыстардың әсерінде.

Барлығы үшін кадрдың ұзындығын квалификациялау қажет, онымен біз 1 формуланы қолданамыз.

$$Пт = К + С_{акпарат}, \quad (3.1)$$

Пт-теориялық сыйымдылық;
К-кадр (4 тен6 дейн 1500 байт);
Сакпарат - ресми ақпаратқа (18 байт).

R қажетті өткізу қабілеттілігі мен абсолютті өткізу қабілеттілігі арасындағы айырмашылық dline to frame түріне байланысты z ішінде болады. Bytes aytes (bpreambls) және d деректер өрісінің кадрға мәні 46-дан 1500 bayt-қа дейін өзгереді. L кез келген пакетте тақырып беріледі, ол мекенжайды және ақпаратты қалыптастыру үшін қатеге қатеге қатысатын мәліметті басқа нөмірге, ол 3,1 суретке сәйкес хабарламамен бірге құрастыру үшін тағайындалған түйінмен пайдаланылады.

Пт = 46+18=64 байт,

Пт = 1500+18=1518 байт.

Пп шектеу көлемінің кадрына берілгенде, preamblемен бірге 1526 bay немесе e12208 bit бар, бұл реттік қадам 12208 құрайды. t +96 bt =12 304 bt, қызметкер жиілігі s жылдамдықта р беріліс 100 Мбит/с кетеді 123,04 мкс = 127 кадр/сек.

Р қызметкерлерді зерттеу жиілігіне қажетті ақпараттың Vp-дегі b байт мәніне,n кез келген кадр арқылы берілетініне назар аудара отырып, қажетті өткізу қабілеттілігін есептеу қиын емес. 2 формуласына сәйкес желі.

$$Пп = Vп*8*f \text{ бит/с}, \quad (3.2)$$

Қайда: Пп-үлкен өткізу қабілеті;
V-пқажетті ақпарат, b;
f-қызметкерлерді зерттеумен жиілік, с.

$$Ппт1 = 148\ 810 \text{ кадр/с} = 54{,}76 \text{ Мбит/с}.$$

Шын мәнінде, ол желілік өткізу қабілеттілігінің бірлескен максималды көлемінің бес он пайызынан сәл ғана астамын құрайды.

Белгілі бір өлшемдегі (1500 байт) кадр үшін қажетті желінің өткізу қабілеті мынаған тең:

$$Ппт2 = 8127 \text{ кадр/с} = 97{,}52 \text{ Мбит/с}.$$

Осылайша,Fast Ethernet желісінде қажетті өткізу қабілеттілігі мұнда ауыстырылған қызметкерлердің көлеміне байланысты өзгеру мүмкіндігіне ие 54,76 дейн 97, 52 Мбит/с.

ҚОРЫТЫНДЫ

Дипломдық жұмыстың нәтижесінде провайдерлік желілерді құру негіздері, желіге кіретін негізгі элементтер, олардың конфигурациясы және бір-бірімен өзара әрекеттесуі зерттелді. Сондай-ақ технологиялар, олардың көмегімен желілердің әртүрлі бөлімдері арасында деректер тасымалдануы және оларды жүзеге асыру зерттелді.

Іс жүзінде CiscoPacketTracer ортасында сақиналы топологияда қосылған маршрутизаторлардан тұратын үлкен желінің бір бөлігі жиналды, онда авторизация сервері маршрутизаторлардың біріне қосылған. Маршрутизаторларға біріктіру желісі қосқышы қосылды, оған кіру желісінің коммутаторлары қосылды.

Деректерді тасымалдауды орнату үшін staticNAT және динамикалық NAT технологиялары пайдаланылды, VoIP телефония конфигурацияланды. Сондай-ақ желіде медиа-контенті бар ішкі серверлерге Интернетке кіру ұйымдастырылды, аутентификация PPPoE арқылы ұйымдастырылды. Барлық параметрлер Router және Switch 2950-24 құрылғыларында консольде жасалды.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1.Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNT/CCNAICND1/ Одом, Уэнделл, 3-е изд. – Москва, Вильямс, 2015 – 668 с.

2. Оптические цифровые телекоммуникационные системы: Введение в технологию цифровых телекоммуникационных сетей TCP/IP: лабораторный практикум ч.1/А. С. Левченко, В. В. Слюсаревский, Н. А. Яковенко и др. ¬– ISBN 978-5-8209-0872-9 Краснодар. Кубанскийгос. ун-т, 2013 – 82 с.

3. Официальное руководство Ciscoпо подготовке к сертификационным экзаменам CCNT/CCNAICND2/ Одом, Уэнделл, 3-е изд. – Москва, Вильямс, 2015 – 729 с.

4. Cisco Library, CiscoSystem // Cisco Easy Virtual Network— (Engl). — URL:www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/easy-virtual-network-evn/aag_75118.p [11 June 2011].

5. IP Routing Fundamentals/ Mark Sportack – Indianapolis, Indiana 46240, 1999 – 528 с.

6. Enhanced IP Services for Cisco Networks/ Donald C. Lee – Indianapolis, Indiana 46240, 1999 – 432 с.

7. Борисов Б. М. Самоучитель по работе с компьютерной сетью. Издательство: Альянс - пресс, 2003. - 495 с.

8. “Мультисервисная корпоративная сеть” //Электронная версия на сайте http://www.o-si.ru/file.html

9. “Оборудование для интеграции речи в каналах FrameRelayКорпоративных сетей”//Электронная версия на сайте http://www.osp.ru/lan/1997/06.html

10. “Корпоративная сеть ОАО “Новгородэнерго”” //Электронная версия на сайте http://www.uni.ru/comp/

11. “Рынок частных сетей” //Электронная версия на сайте http://www.bytemag.ru/article.html

12. “Создание территориально распределенных сетей” //Электронная версия на сайте http://www.compulink.ru/global.html

13. “Интегрированные высокоскоростные сети передачи данных и голоса сиспользованием физических и радиоканалов” //Электронная версия на сайте http://www.inforad.ru.html

14. “Проект: Создание городской сети передачи данных Костромы”//Электронная версия на сайте http://www.pluscom.ru/

15. “Разработка проекта корпоративной сети масштаба предприятия на базе ATM - технологии” //Электронная версия на сайте http://conf.mitme.ru/

16. “Проект корпоративной сети” //Электронная версия на сайте http://www.ronl.ru/

17. “Intranet: будущее Вашей локальной и корпоративной сети” //Электронная версия на сайте http://www.ci.ru/inform3_97/f1.html

18. “Корпоративные сети передачи данных” //Электронная версия на сайте http://www.vogss.ru/dtcn.html

Қ.И. СӘТБАЕВ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ

дипломдық жобаға

РЕЦЕНЗИЯ

Қоныс Салтанат

6В06201 «Телекоммуникация» білім беру бағдарламасы

Тақырыбы: «Cisco Packet Tracer-де кәсіпорын желісінің периметрін қорғауды модельдеу»

а) графикалық бөлімі 9 бет;
б) түсіндірме жазбасы 28 бет.

ЖҰМЫСҚА ЕСКЕРТУ ЖАСАУ

Дипломдық жобада «Cisco Packet Tracer-де кәсіпорын желісінің периметрін қорғауды модельдеу» қарастырылған.

Cisco Packet Tracer-де кәсіпорын желісінің периметрді қорғауды ұйымдастыруға арналған "ASUE" компаниясының, корпоративтік желісінің адаптивті құрылғысы негізінде ішкі желіні сыртқы желіден қорғау мақсатында Cisco ASA series қорғау әсер ету, кіріс және шығыс қол жеткізуді бақылау, қауіпсіз ұйымның бас кеңсесі мен филиалдары арасындағы өзара іс-қимыл, сондай-ақ аутентификация, авторизация және практика жүйесін жетілдіру қарастырылған.

Желінің қауіпсіздігі мен негіздемесінің жалпы мәселелері қарастыру үшін Cisco ASA series құрылғысы таңдалды.

Дипломдық жұмыстың нәтижесінде провайдерлік желілерді құру негіздері, желіге кіретін негізгі элементтер, олардың конфигурациясы және бір-бірімен өзара әрекеттесуі зерттелді. Сондай-ақ технологиялар, олардың көмегімен желілердің әртүрлі бөлімдері арасында деректер тасымалдануы және оларды жүзеге асыру зерттелді.

Бұл дипломдық жоба жоғарғы оқу орындарының талаптарына сай жеткілікті жоғары дәрежеде жазылған, алынған нәтижелер ақпаратты өңдеп тарату технологиялардағы ғылыми бағытқа жауап береді.

Жұмыс бағасы

Жалпы, дипломдық жұмыс «95/А/ өте жақсы» деген бағаға, ал Қоныс Салтанат 6В06201 «Телекоммуникация» білім беру бағдарламасы бойынша техника және технологиялар «бакалавр» академиялық дәрежесіне ұсынылады.

Рецензент:
Халықаралық ақпараттық
технологиялар университеті
т.ғ.к., кафедра меңгерушісі
Бахтиярова Е.А
«1» 06 2023 ж

Подпись указанного лица удостоверяю
Менеджер по персоналу
Мухамеш М.К.

Қ.И. СӘТБАЕВ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

дипломдық жұмысқа

Қоныс Салтанат

6В06201 «Телекоммуникация» білім беру бағдарламасы

Тақырыбы: Cisco Packet Tracer-де кәсіпорын желісінің периметрін қорғауды модельдеу

Бұл дипломдық жұмыста Cisco Packet Tracer-де кәсіпорын желісінің периметрін модельдеу қарастырылды.

Дипломдық жұмыс барысында бірінші бөлімде корпоративтік желіні дамыту және кәсіпорын желісінің периметріндегі CISCO ASA SERIES құрылғысын желілік қауіп қатерден қорғау қауіпсіздігі талданды.

Екінші бөлімде, Cisco ASA Series қол жетімділікті басқара отырып, кеңейтілген қолданбалы брандмауэр қызметтерін ұсынады. Қызмет көрсетуден бас тарту шабуылдарынан қорғау және нарықта сыналған Cisco PIX қорғаныс құрылғысының технологиясы негізінде жасалған бірқатар қосымша қызметтер қарастырылды. Корпоративтік желіні құру үшін қажетті құрылғылардың сипаттамасы, желінің пайдалы өткізу қабілеттілігі 300 Мбит/с дейін және тарату пакетін жіберу есептелді.

Үшінші бөлімде, CiscoFPR1120-ASA-K9 жабдығы негізінде CiscoPacketTracer жүйесінде жұмыс істейтін корпоративтік желі периметрі қорғанысының моделі жасалды.

Студент, Қоныс Салтанат дипломдық жұмысты жазу барысында жетекші нұсқаулығымен өз бетінше жұмыс істеу қабілетін көрсетті. Дипломдық жұмыс "90/А/ өте жақсы" деп бағаланды, ал Қоныс Салтанатты 6В06201 «Телекоммуникация» білім беру бағдарламасы бойынша «техника және технологиялар» бакалавры академиялық дәрежесіне ұсынамын.

Ғылыми жетекші
ЭТжГТ каф. аға оқытушы,
техника ғылымдарының магистрі
_____ Марксұлы С.
«__1__»_____06_____2023 ж.

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Коныс Салтанат Қонысқызы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Cisco Packet Tracer-де кәсіпорын желісінің периметрін қорғауды модельдеу

Научный руководитель: Сұңғат Марксұлы

Коэффициент Подобия 1: 14

Коэффициент Подобия 2: 3.5

Микропробелы: 42

Знаки из здругих алфавитов: 16

Интервалы: 0

Белые Знаки: 3

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

Дата *Заведующий кафедрой*

Университеттің жүйе администраторы мен Академиялық мәселелер департаменті директорының ұқсастық есебіне талдау хаттамасы

Жүйе администраторы мен Академиялық мәселелер департаментінің директоры көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

Автор: Қоныс Салтанат Қонысқызы

Тақырыбы: Cisco Packet Tracer-де кәсіпорын желісінің периметрін қорғауды модельдеу

Жетекшісі: Сұңғат Марксұлы

1-ұқсастық коэффициенті (30): 14

2-ұқсастық коэффициенті (5): 3.5

Дәйексөз (35): 1.1

Әріптерді ауыстыру: 16

Аралықтар: 0

Шағын кеңістіктер: 42

Ақ белгілер: 3

Ұқсастық есебін талдай отырып, Жүйе администраторы мен Академиялық мәселелер департаментінің директоры келесі шешімдерді мәлімдейді :

☒ Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

☐ Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

☐ Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

Күні *Кафедра меңгерушісі*

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Қоныс Салтанат Қонысқызы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Cisco Packet Tracer-де кәсіпорын желісінің периметрін қорғауды модельдеу

Научный руководитель: Сұңғат Марксұлы

Коэффициент Подобия 1: 14

Коэффициент Подобия 2: 3.5

Микропробелы: 42

Знаки из здругих алфавитов: 16

Интервалы: 0

Белые Знаки: 3

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

1.06.2023 г.
Дата

Марксұлы С.
проверяющий эксперт