ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы
АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Компьютерлік технологиялар
кафедрасы

«Қорғауға жіберілді»
Кафедра меңгерушісі
Құрманбаев З.Қ., профессор ф.-м.ғ.д
(аты-жөні, ғылыми дәрежесі, атағы)
«_____» _____ **20___ ж.**
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Cisco Pix Firewall 515E желі аралық экранын қолдану арқылы компьютерлік желінің ақпараттық қауіпсіздік жүйесін жетілдіру

мамандығы бойынша

Орындаған Сахова Динара
(аты - жөні) (тобы)

Жетекші Аманбаев А.А доцент, ф.-м.ғ.к.
(аты-жөні, ғылыми дәрежесі, атағы)

Кеңесшілер :

Экономикалық бөлім бойынша : ЭЖ.К доцент Тузелбаев Б.Ш.
(ғылыми дәрежесі, атағы, аты-жөні)
«21» 05 2016 ж.
(қолы)

Өмір тіршілігі қауіпсіздігі бойынша: Лакишжанов Т.Е.
(ғылыми дәрежесі, атағы, аты-жөні)
«26» 05 2016 ж.
(қолы)

Есептеу техникасын қолдану бойынша : Аманбаев А.А доцент, ф.-м.ғ.к.
(ғылыми дәрежесі, атағы, аты-жөні)
«2» 06 2016 ж.
(қолы)

Мөлшер бақылаушы: Аманбаев А.А доцент, ф.-м.ғ.к.
(ғылыми дәрежесі, атағы, аты-жөні)
«2» 06 2016 ж.
(қолы)

Пікір жазушы : Нуркасымов Алибек Сарсенбаевич
(ғылыми дәрежесі, атағы, аты-жөні)
«03» 06 2016 ж.
(қолы)

Алматы 2016

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы
АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Ақпараттық және аэроғарыштық технологиялар факультеті
Есептеу техникасы және бағдарламалық қамтамасыз ету мамандығы
Компьютерлік технологиялар кафедрасы

жобаны орындауға берілген

ТАПСЫРМА

Студент Сахова Динара
(аты - жөні)

Жоба тақырыбы Cisco Pix Firewall 515E желі аралық экранын қолдану арқылы компьютерлік желінің ақпараттық қауіпсіздік түйінін зерттеу
ректордың **« 29 » қыркүйек №124** бұйрығы бойынша бекітілген.

Аяқталған жұмысты тапсыру мерзімі: «____»_____20___ ж.

Жобаға бастапқы деректер (талап етілетін жоба нәтижелерінің параметрлері және нысанның бастапқы деректері)
Жобаға желінің ақпараттық қауіпсіздігін қамтамасыз ету тағаптарынсын байланысты, қолдағы Қатар. Cisco Pix желіаралық экрандардың ақпараттық құралдары және бағдарламалық қамтамасыз ету мәселелері, Мемлекеттік бақылаушы комитетінің Шымкент қаласының бұқаралық ақпарат құралдарының компьютерлік желісінің ақпараттық қауіпсіздік түйінін жүзеге асыру бағыты қарастырылады.

Диплом жобасындағы әзірленуі тиіс сұрақтар тізімі немесе диплом жобасының қысқаша мазмұны:
Берілген дипломдық жоба Cisco Pix Firewall 515E желіаралық экранын қолданушымен „Шымкент қаласының құқықтық қызметі" компьютерлік желісінің ақпараттық қауіпсіздігін қамтамасыз ету түйінін құрастыруға арналған. Дипломдық жобада қазіргі кездегі желіні қорғау құралдары қарастырылған. Cisco Pix Firewall 515E табалығы негізінде AAA технологиясымен желіні қорғау түйіні, жабарлау, локалдық желіні қорғау ұйымдастырылады.

Сызба материалдарының (міндетті түрде дайындалатын сызуларды көрсету) тізімі

1. Кәсіпорын желісінің топологиясы

Негізгі ұсынылатын әдебиеттер

1. М. Чанстроме. Организация защиты сетей Cisco
2. Cisco Fundamental Network Security 1 курс материалдарое
3. Д. Темпен., Э. Фокс. Брандмауэрлар Cisco Secure Pix!

Жоба бойынша бөлімшелерге қатысты белгіленген кеңесшілер

бөлімшелер	кеңесші	мерзімі	қолы
Еңбек қорғау	Хакимжанов Т.Е	26.05.2016	
экономика	Тұзелбаев Б.	21.01-26.05.16	
Рецензия	Нұрқасымов А.С	03.06.2016	

диплом жобасын дайындау

КЕСТЕСІ

№ р/с	Тарау аттары, әзірленетін сұрақтардың тізімі	Жетекшіге ұсыну мерзімдері	Ескерту
1.	Жеңі қауіпсіздігін қамтамасыз ету тапсырмасы	25.01 - 03.02.	
2.	Жеңні зерттеу	03.02 - 16.02.	
3.	Басып кірулерді тоқтатады	16.02 - 1.03	
4.	Корпоративтік қауіпсіздік саясатының үлгісін жасау	1.03 - 18.03	
5.	PIX брандмауэрлерінің конфигурациясын және түрлерін талдау	18.03 - 25.03	
6.	ASA қауіпсіздігінің деңгейлерін зерттеу	25.03 - 16.04	
7.	AAA технологиясын анықтау	16.04 - 29.04.	
8.	Тіршілік қауіпсіздігін сақтау	29.04 - 07.05	
9.	Бизнес-жоспар құру	07.05 - 18.05.	

Тапсырманың берілген уақыты «_____»_____20___ж.

Кафедра меңгерушісі _____ _____
(қолы) (аты-жөні, ғылыми дәрежесі, атағы)

Жоба жетекшісі _____ Аманбаев А.А., доцент, ф.-м.ғ.к.
(қолы) (аты-жөні, ғылыми дәрежесі, атағы)

Орындалатын тапсырманы қабылдаған студент _____ Сахова Д.М.
(қолы) (аты -жөні)

Аннотация

Данный дипломный проект посвящен разработке системы информационной безопасности компьютерной сети Государственного казённого коммунального предприятия «Служба спасения города Шымкент» с использованием межсетевого экрана Cisco PIX Firewall 515 E.

В дипломном проекте произведено сравнение ныне существующих средств защиты сетей. На основе оборудования Cisco PIX Firewall 515 E разработана система защиты периметра сети, приведена настройка трансляции сетевых адресов в брандмауэре, настройка управления исходящим и входящим доступом через брандмауэр, защита локальной сети средствами AAA брандмауэра PIX Firewall.

Также рассмотрены вопросы безопасности жизнедеятельности. Выполнено создание оптимальных условий труда.

Annotation

This thesis project focuses on the development of computer network information security of the State treasury utility «Emergency Shymkent» using firewall Cisco PIX Firewall 515 E.

In comparison capstone project produced remedies now existing networks. Hardware-based Cisco PIX Firewall 515 E system developed perimeter, given setting NAT firewall, setting control outgoing and incoming access through the firewall, protection network means AAA Firewall PIX Firewall.

Also consider the safety. Achieved create optimal working conditions.

Аңдатпа

Берілген дипломдық жоба Cisco PIX Firewall 515 E желіаралық экранын қолдануымен «Шымкент қаласының құтқару қызметі» компьютерлік желісінің ақпараттық қауіпсіздігін қамтамасыз етуге жүйесін құрастыруға арналған.

Дипломдық жобада қазіргі кездегі желіні қорғау құралдары салыстырылған. Cisco PIX Firewall 515 E жабдығы негізінде AAA технологиясымен желіні қорғау жүйесі, хабарлауды, басқаруды құрастыру, локалдық жүйені қорғау ұйымдастырылды.

Соған қоса өмірқауіпсіздік сұрақтары қарастырылды. Оптималды жұмыс шарттары орындалды.

Мазмұны

Кіріспе

Бүгінгі күні компьютерлер, желілер және интернет біздің күнделікті тіршілігіміздің басым бөлігін қамтиды. Біздің технологиялармен және әлемге жылдам қадам басумен толықтырылған әр күніміз барған сайын компьютерге және желілерге тәуелді болуда. Алайда компьютерге және интернетке деген осы тәуелділік бірден пайда болған жоқ. Жыл өткен сайын компьютерлік технологиялар барынша қаржыландырылды, нәтижесінде бұл технологиялар адамның еңбекпен қамтылған барлық саласына енді. Адамдардың басым бөлігі компьютерлік технологиялардың даму кезеңінде осы технологиялар келешекте кеңінен қолданылады деп ойлағанда емес. Сондықтан адамдардың басым бөлігі оларды оқып білуге, үйренуге көп уақыт пен күш-жігер жұмсауға батылы жетпеді.

Егер сол кездегі технологиялар мен желілердің компьютерлік саласында жұмыс атқаратын адамдардың саны қазіргі таңдағы еңбек нарығының талаптарымен салыстырғанда өте кем болатын. Осы тығыз аймақта қызмет ететін адамдар бір-бірімен өте жақсы таныс және сенімді қарым-қатынасқа ие болатын. Сонымен қатар адамдардың осы аймағына тек бір-біріне сенімі бар адамдар ғана қабылданатын. Сондықтан ол уақытта компьютерлік технологиялар және желілер аясында қауіпсіздікпен байланысты мәселелер айтарлықтай болған емес.

Қазіргі таңда Internet көмегімен желілердің көлемді саны жалпы бір желіге бірігеді. Сондықтан осындай ауқымды желінің қауіпсіз жұмыс атқаруы үшін мекеме желісінің қауіпсіздік жүйесін қамтамасыз ету бойынша нақты шаралар қабылдау қажет екені түсінікті, себебі айтарлықтай әрбір компьютерден кез келген мекеменің, кәсіпорынның кез келген желісіне қолжеткізуге болады және компьютер желісін бұзу міндетті түрде физикалық күшпен кіруді талап етпейді, нәтижесінде қауіптілік деңгейі жоғарылайды.

Компьютерлік желі ұғымын байланыс желілерімен қосылған және арнайы белгіленген бағдарламалық қамтамасыз етулердің басқаруымен жұмыс атқаратын көптеген компьютерлер деп түсінуге болады.

Байланыс желісі – бұл дыбысты таратқыштан қабылдағышқа таратуды қамтамасыз ететін техникалық құрылғылардың және физикалық ортаның жиынтығы.

Күнделікті өмірде телефон желісінің коммутаторлары арасында дыбыстарды таратуды қамтамасыз ететін кәбіл учаскелері және күшейткіштер байланыс желісінің мысалы бола алады. Байланыс желілері негізінде байланыс арналары құрастырылады. Абоненттер арасында белгіленген ақпаратты таратуды қамтамасыз ететін байланыс желілерін және техникалық құрылғылар жүйесін байланыс арнасы деп санауға болады. Компьютерлерді біріктіру мақсаты пайдаланушыларға құжаттар, бағдарламалар және осы компьютерлер арқылы таратылған және жалпы пайдаланудағы деректер қоры тәрізді түрлі ақпараттық ресурстарға қолжеткізу мүмкіндігін ұсыну.

Кез келген компьютерлік желінің маңызды сипаттамасы ол қамтылған аймақтың аумағы болып табылады. Қамту ұзындығын желіні құрайтын

компьютерлердің орын алуының өзара үлкен қашықтығымен анықтайды және ол желіні салу кезінде таңдап алынатын технологиялық шешімдерге әсер етеді.

Әдетте желілер екі түрге бөлінеді. Бұл локалді желілер және ауқымды желілер. Локалді желілерге көбінесе салыстырмалы кішігірім аймақтарға, әдетте бұл кәсіпорын компьютерлерінен бастап бірнеше км (әдетте 2-3) дейінгі радиусқа топталған, компьютерлер желілерін жатқызады.

Бір немесе бірнеше жақын орналасқан ғимараттарда аталған кәсіпорынның желісі локалді желінің мысалы бола алады. Бұл желілердің ықшамды көлемі локалді желілерді салу үшін сапасы жоғары барынша қымбат, компьютерлер арасында деректер мен ақпараттардың жоғары жылдамдықпен алмасуын қамтамасыз ететін технологияларды қолдануға мүмкіндік береді.

Қазіргі сәтте желілердің қауіпсіздік мәселесі шешілмеген деп болжауға болады, себебі компаниялардың басым бөлігінде қауіпсіздікті қамтамасыз ету мәселесі шешілмеген, нәтижесінде олар желілік қауіп-қатердің салдарынан қаржылық шығынға тап болуда және ақпараттық құпиялығы мен бүтіндігі сақталмауда. Келешекте кәсіпорын желілік шабуылдардан зиянға ұшырамауы үшін ақпараттық қауіпсіздікті қамтамасыз ету шараларын қабылдау қажет.

1 Желі қауіпсіздігін қамтамасыз ету талаптары

1.1 Желі қауіпсіздігінің негізгі анықтамалары

Біріктірілген желі (internetwork) терминін көптеген бір біріне қосылған желі деп ұғынады. Біріктірілген желіде арнайы тараулар құрылады, олардың әрқайсысы белгіленген ақпаратты өңдеу және сақтау үшін тағайындалған.

Осы тарауларды бөліп, олардың қауіпсіздігін қамтамасыз ету үшін брандмауэр (firewall) немесе желіаралық экран деп аталатын арнайы құрылғылар қолданылады. Желіаралық экрандардың тағайындалуы туралы келесідей ұғым бар, яғни жабық ішкі желілер мен сыртқы жалпы қолдану желілерін бөлу, бірақ бұл ұғым үнемі осындай бола бермейді. Брандмауэрлер көбінесе жабық желінің сегменттерін шектеу үшін қолданылады.

Желіаралық экран ұғымы қолжетімділіктің (бір немесе бірнеше) бағдар сілтеуші немесе сервері ретінде анықталады, бұл ашық желілер мен жабық желілер арасында қорғаныс экраны рөлін атқарады. Бағдар сілтеуші – экран қолжетімділіктің тізімін және жабық желінің ақпараттарын қорғаудың басқа құралдарын қолданады. Бұл ұғым «Вильямс» баспа үйімен шығарылған CiscoSystems, Inc. ресми баспаның желілік терминдердің және қысқартылған атаулардың түсіндірме сөздігінде аталып өткен.

Көптеген жағдайда желіаралық экрандарда кемінде үш интерфейс қарастырылады, бірақ едәуір бұрын шыққандарда екеуі қолданылған. Сондықтан осы сәтте желіаралық экрандарда негізінен небәрі үшеуінің ішінен екі интерфейс қана қолданылады. Белгіленген үш интерфейспен бірге брандмауэр қолданылған жағдайда үш бөлінген желілік аймақты құру мүмкіндігі орын алады. Төменде осы аймақтардың әрқайсысына қысқаша сипаттама беріледі.

Аталған біріктірілген желінің ішкі аймағы сенімді аймақ болып саналады және жабық желі құрылғысының жұмыс атқаруы үшін тағайындалады. Бұл құрылғылар сыртқы желімен (мысалы, Internet) жұмыс атқару кезінде қауіпсіздік саясатын орындайды. Алайда, іс жүзінде желіаралық экран ішкі аймақта бөлімдердің сегменттерге бөлінуі үшін қолданылады. Мысалы, брандмауэр жалпы желіден кәсіпорынның қандай да бір саласын желіден бөлу үшін қолданылады.

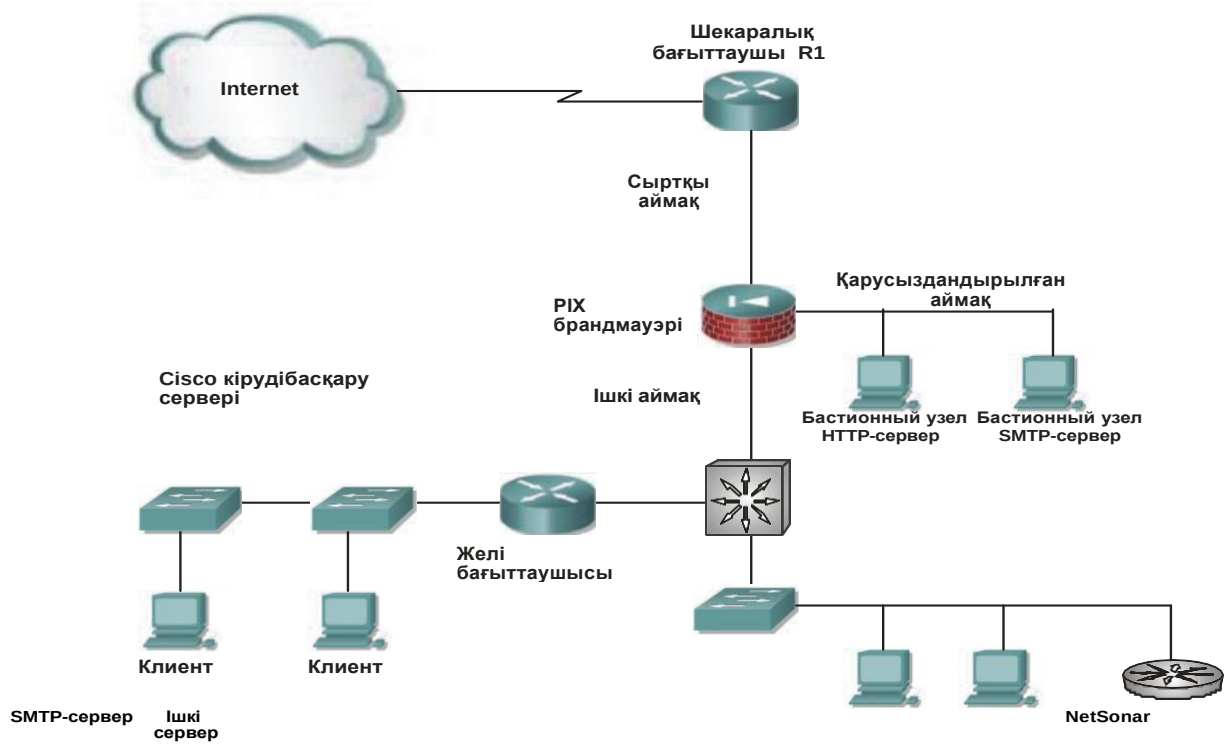
Біріктірілген желінің сыртқы аймағы сенімділігі төмен аймақ болып саналады. Желіаралық экранның негізгі қызметі - бұл сыртқы аймақта орналасқан құрылғылардан ішкі және қарусыздандырылған аймақтың құрылғыларын қорғау. Сонымен қатар, қажеттілігіне қарай желіаралық экран қарусыздандырылған аймақта орналасқан құрылғыларға сыртқы аймақтан қолжеткізудің қауіпсіз таңдау күйіне баптап келтіріледі. Егер брандмауэр өте қажет болса, онда ішкі аймақта сыртқы аймақтан қолжетімділікті қамтамасыз

ету күйін баптап келтіруге болады. Бірақ мұндай іс-әрекеттер тек ерекше жағдайларда ғана қолданылады, себебі ішкі аймаққа сыртқы аймақтан келетін қауіп оқшауланған қарусыздандырылған аймаққа қолжеткізумен салыстырғанда едәуір жоғары.

Қарусыздандырылған аймақ (DMZ) дегеніміз оқшауланған желі (немесе желілер), бұл пайдаланушыларға тек сыртқы желіден ғана қолжетімді. Желіаралық экран сыртқы аймақтан ішкі немесе қарусыздандырылған аймаққа қолжеткізуді қамтамасыз ету үшін кескінделенеді. Қарусыздандырылған аймаққа қолжеткізу үшін рұқсат жасау кәсіпорынға компаниямен ұсынылатын ақпараттарға және қызметтерге сыртқы пайдаланушылардың қауіпсіз қолжеткізуін ұйымдастыруға мүмкіндік береді. Осыған байланысты, аталған аймақ сыртқы пайдаланушылармен ішкі қауіпсіз аймаққа олардың қолжеткізуінсіз жұмыс атқаруға рұқсат береді.

Бастиондық тораптар дегеніміз қарусыздандырылған аймаққа кіретін тораптар немесе серверлер. Демек, бұл операциялық жүйелердің жаңа нұсқалары жұмыс атқаратын және жаңартудың барлық модулдері орнатылатын тораптар. Өндіруші қателіктерді жоя алады және қосымшаға толықтыру енгізе алады, сондықтан бастиондық тораптарды қолдану жүйені желілік шабуылдарға барынша тұрақты етеді. Бастиондық тораптар қосымшалар жұмысы үшін қажет қызметтер ғана орындалатындығымен ерекшеленеді. Қажет емес тораптарды ажыратып немесе тіпті жойып тастайды.

1.1 Суретте Брандмауэрді қолдану кезіндегі желінің жалпы құрылымы көрсетілген.



1.1 Сурет - Брандмауэрді қолдану кезіндегі желінің жалпы құрылымы

Брандмауэрдің негізгі қызметі мыналар:

- сыртқы аймақтан ішкі аймаққа қолжеткізуге тыйым салу;
- сыртқы аймақтан қарусыздандырылған аймаққа қолжеткізуді шектеу;
- ішкі аймақтан сыртқы аймаққа толық қолжеткізу;
- ішкі аймақтан қарусыздандырылған аймаққа қолжеткізуді шектеу.

Алайда кейбір жағдайда желіаралық экран қызметінің көрсетілген тізімінен жеке немесе барлық тармақтары алып тасталынуы мүмкін. Мысалы, егер бізге сыртқы аймақтан ішкі аймаққа SMTP-хабарламаны жеткізуді қамтамасыз ету қажет болса, егер қарусыздандырылған аймақта SMTP-хабарламаны тарату үшін SMTP-сервер немесе құралдар жоқ болса, онда желінің ішкі аймағында орналасқан SMTP-серверге тікелей SMTP-топтамасын жөнелтуді қамтамасыз ету қажет. Осы тәрізді тәсілді жүзеге асырудың нәтижесінде аталған аймақта жұмыс қауіпсіздігі едәуір төмендейді.

Немесе егер рұқсат жоқ болса, онда ішкі аймақтан сыртқы аймаққа шыққан ақпарат ағынына қолжеткізуге тыйым салынуы мүмкін. Белгіленген портты пайдалануға шектеу бөлінген IP-мекенжайлар, желіішілік немесе бүкіл ішкі желі деңгейінде орнатылуы мүмкін. Сонымен қатар ішкі желіден сыртқы желіге шыққан деректер ағынын бақылау әдісін бірі URL-мекенжайлары бойынша сүзгіден өткізу болып табылады. WebSense тәрізді HTTP-сүзгіштерін қолдануды және басқа да ерекшеліктерді төменде қарастырамыз.

1.2 Желі қауіпсіздігінің қауіп-қатер санаттары

Желі қауіпсіздігі қауіп-қатерінің төрт санаты бар:

1 Құрылымдық емес қауіп-қатерлер.

Мұндай қауіп-қатерлер Internet-те оңай орналасқан дайын құралдарды бұзу үшін қолданатын кейбір тұлғалардан шығады. Мұндай жағдайда олардың кейбірінде қаскүнемдік мақсат болуы мүмкін, бірақ олардың басым бөлігі қарапайым құмарлықтан бұзу әрекетіне баратын әдеттегі скриптомандар болып табылады. Бұл скриптомандар желі қауіпсіздігіне шын мәнінде қауіп төндіреді.

Кейбір жағдайда олар тіпті өз қимылдарының бүлдіретін әрекеттер екеніне күмән келтірмей-ақ түрлі вирустарды немесе «троян аттарын» белсенді таратады. Бүкіләлемдік өріс алған вирустың салдары бүлдіру әрекеті болуы мүмкін және бұл бағдарлама арқылы осындай жағдайға келтірілген залал миллиондаған доллармен есептеледі. Сонымен бірге, кейбір жағдайда вирус авторының өзі оның құрбаны болуы мүмкін.

Вирус пайдаланушының жұмыс станциясында оның қандайда бір жағымсыз іс-әрекеттерді жасағаны үшін пайдалы бағдарламаға (немесе шамамен пайдалы) қосылатын зиянды іс-әрекеттеріне қатысты жазылған бағдарламаны білдіреді. Мысалы, вирус command.com файлына тіркеледі, белгіленген атауы бар файлдарды жояды және command.com тауып ала алатын оның барлық файлдарына әсер етеді.

Әдеттегі вирустан троян атының айырмашылығы сырттай ол қарапайым бағдарлама тәрізді көрінеді, бірақ зиян келтіретін әрекеттер жасайды.

«Троян аты» пайдаланушы байланыстарынан табылған, барлық мекен-жайларға өзінің көшірмесін тарататын, қарапайым ойын бағдарламасы болуы мүмкін, ал ештемеден күмәнданбайтын пайдаланушы ойнауды жалғастыра береді. Өзге пайдаланушылар өзінің компьютерінен осы ойынды қабылдайды және ашады, сол сәтте олардың өзі бұл вирустарды таратушы болып шығады.

Құрылымдық емес қауіп-қатердің басым көлемі скриптомандардың тек тәжірибесін, шеберлігін сынау және тексеру мақсатында жүзеге асырылады, бірақ осындай іс-әрекеттер кәсіпорынға айтарлықтай залал келтіреді. Мысалы, компанияның сыртқы Web-торабын бұзған кезде оның қызметінің барлық бағыттары қауіп-қатерге ұшырайды. Тіпті, егер сыртқы Web-торап желіаралық экранды қолдану арқылы компанияның ішкі ақпараттық құрылымынан бөлінген жағдайда да, компания туралы ақпаратты алғысы келген пайдаланушылар мақсаттарына қолжеткізе алмайды. Осы пайдаланушылардың барлығы компанияның Web-торабының бұзылғанын көрген соң, олар, ең дұрысы бұл компания бизнес бойынша қауіпсіз серіктес болып табылмайды деп шешеді..

2 Құрамдастырылған қауіп-қатерлер.

Компьютерлік технология саласы бойынша барынша білікті және байыпты ниеті бар бүлдірушілер құрамдастырылған қауіп-қатерді алға тартады. Әдетте бұл адамдар желілік жүйелердің жұмыс қағидаларын түсінеді және олардың кемістіктерін жақсы біледі. Олар кәсіпорын желілерін немесе белгіленген Web-тораптарын алдын ала бүлдіру үшін тағайындалған сценарийді өз бетінше жаза алады. Көбінесе, осы тәрізді бүліну іс-әрекетіне айлакерлік немесе ұрлық жасау мақсатымен заң мекемелері ұшырайды. Кейбір кезде мұндай бүлдірушілердің қызметін ақпарат алу мақсатымен аталған кәсіпорынның өнеркәсіптік бәсекелестері немесе ұйымдасқан қылмыскерлері қолдануы мүмкін.

3 Сыртқы қауіп-қатерлер.

Сыртқы қауіп-қатерлер бөгде тұлғалардан немесе кәсіпорынның желілеріне немесе компьютерлік жүйелерге ресми қолжеткізу мүмкіндігі жоқ мекемелерден түседі. Олар компанияның желісіне Internet немесе қашықтан кіру сервері арқылы қолжеткізу мүмкіндігін алады.

4 Ішкі қауіп-қатерлер.

Ішкі қауіп-қатерлер компьютерлік желіге физикалық тұрғыда қолжеткізу немесе серверде есептік жазбаға қолжеткізу мүмкіндігі бар тұлғалардан түседі. Ішкі қауіп-қатерлер компанияда бұрын қызмет еткен ренжулі немесе тұрақты немесе уақытша жұмыс атқаратын қызметкерден шығуы мүмкін.

1.3 Желілердің қауіпсіздігі қалай бұзылады

Желілердің қауіпсіздігін бұзудың үш түрі бар.

Желіні зерттеу, яғни қаскүнем желіні зерттеуге және оның жүйелерінің, қызметтерінің және кемістіктерінің сұлбасын алуға талпынады.

Қолжеткізу жүйесін бүлдіру – жүйеде тұлғаның жеке дәрежесін білу

немесе қолжеткізу деректерін алу мақсатымен компьютерлік желілерді немесе жүйелерді бұзу.

1.3.1 Желіні зерттеу

Зерттеу желілері – бұл осы жүйеде авторизациясы жоқ пайдаланушымен желі құрылымын, жұмыс атқаратын қызметтерді анықтауға және ping- тындау технологиясын қолдану арқылы орын алуы мүмкін кемістіктерді айқындауға ұмтылу. Ping – тындау – бұл ping- сұраныстары (ICMP-сұраныс және ICMP-жауап) қолданылатын және желі құрылымын анықтау үшін тағайындалған арнайы технология. Сонымен бірге мұндай іс-әрекеттер ақпараттарды жинау процесі (information gathering) деп аталады және көп жағдайда бұл процесс жүйеге қолжеткізу мүмкіндігін бұзуды немесе DOS-бүлдірулерді (Denial of Service attack – қызмет көрсетуден бас тарту) алдын алады.

Бастапқыда қаскүнем желідегі белсенді IP-мекен-жайларын айқындау мақсатында өзін қызықтыратын желіні тексереді. Осындай деректерге қолжеткізген соң, ол айқындалған IP-мекен-жайлармен тораптарда жұмыс атқаратын қызметтерді және қолданылатын порттарды анықтайды. Сонан соң белсенді IP-мекен-жайларда жұмыс атқаратын қосымшалардың түрін анықтау үшін белгіленген порттарға сұраныс жіберіледі. Нәтижесінде, ол қосымша түрі туралы ақпарат алады, тіпті операциялық жүйенің түрі және нұсқасы туралы ақпарат алуы да мүмкін.

Желіні зерттеу төңіректегі үйлерді қарап шығатын және иесі жоқ, есіктері мен терезелері оңай ашылатын үйлерді анықтайтын тонаушының ақпарат жинауы тәрізді іс-әрекеті. Сонымен тонаушы ретінде, компьютер бүлдіруші қорғау жүйесінде айқындалған тесікті қолданады және сонан соң оны айқындау мүмкіндігі кеміген сәтте желіні бұза алады.

1.3.2 Қолжеткізу жүйесі бұзу

Қолжетімділік (access) термині едәуір көп мәнді қамтиды және әдетте, нақты қоркөзінің қасиетін білдіреді (бұл желісі Internet-ке қосылған пайдаланушының компьютері болуы мүмкін), белгіленген объектіге қосылады (бұл желіге қосылған, өз кезегінде Internet-ке қосылған компьютер). Бұзу объектісі орнатылған соң, арнайы бағдарламалық қамтамасыз етуді қолдану арқылы оған ену ұмтылысы орын алады.

Егер бұзу сәтті орындалса, онда бүлдіруші авторизациясыз деректерді сұрау және олармен қулық әрекеттер жасау, жүйеге қарым-қатынас жасау немесе өзінің өкілеттігін кеңейту мүмкіндігін алады. Қолжеткізу мүмкіндігін бұзу жүйеге бақылау жасау үшін қолданылуы да мүмкін, бұл бағдарламалық қамтамасыз етуді орнатуға және әрі қарай бүркенуге ықпал етеді, нәтижесінде бұзу үшін қолданылуы мүмкін.

Деректерді авторизациясыз алу (unauthorizeddataretrieval) ұғымы авторизация жасалмаған пайдаланушылар үшін қолжетімсіз болып табылатын, файлдардың орын алмасуы немесе көшірілуі, оқудың, жазбаның әдеттегі операциялары деп түсіндіріледі.

Кез келген пайдаланушы үшін оқу немесе жазу құқы берілген, UNIX-жүйелерінде NT немесе NFS-қолданбалы каталогтар немесе Windows 9 жүйелерінде жалпы қолжетімді папкілер айтарлықтай жиі кездеседі. Авторизация жасалмаған пайдаланушылар мұндай файлдарға ешбір қиындықсыз қолжеткізуі мүмкін және қолжетімділігі оңай ақпараттар көбінесе сырт көзге арналмаған, құпия болып табылады.

Авторизациясыз жүйеге қолжеткізу. Жүйені бұзып қолжеткізудің бұл түрі жүйеге авторизациясыз қолжеткізу мүмкіндігін алуға ықпал етеді. Жүйеге қолжеткізу мүмкіндігін бірнеше нұсқамен алуға болады. Кейбір жүйелерге кіру үшін сәйкестендіруді талап етпейді, яғни жүйеге кіру кезінде құпиясөз сұралмайды. Кейбір қорғаныс құралдары қолданылатын, жүйелерге қолжеткізу мүмкіндігін алу үшін, бүлдіруші жүйеде орындалатын, бағдарламалық қамтамасыз етулерде немесе сценарийлерде орын алған кемістіктерді қолдана алады.

Сонымен қатар, ол авторизациясы жоқ пайдаланушымен жүйеге қолжеткізу мүмкіндігін алу үшін операциялық жүйенің өзінде осал жерлерді қолдана алады. Кейбір операциялық жүйелер қауіпсіздік талаптары ескерілмей дайындалған Бұл кемшіліктер, соңында операциялық жүйелердің кезекті нұсқаларында түзетілуі мүмкін, бірақ жүйеде жаңарту орнатылғанға дейін кез келген бүлдіруші оларды қолдана алады.

Өкілеттілікті авторизациясыз кеңейту. Мұндай үлгідегі бұзылымды жүйеге қолжеткізу мүмкіндігі шектелген пайдаланушылар қолданады. Сонымен қатар жүйеге қолжеткізуге ерекшелігі жоқ авторизация жасалмаған пайдаланушылар осы тәрізді бүлдірулерді қолдана алады. Мұндай бүлдірулердің мақсаты - ақпарат алу немесе бұл деңгейде тыйым салынған рет-жосықтарды орындау.

Әдетте, мұндай сипатта бұзу кезінде олар жүйені супер пайдаланушы құқын (root) алады, деректердің бүкіл ағынын сараптайтын бағдарлама орнатады және осы пайдаланушылардың есептік жазбаларын және құпиясөздерін табады. Кейбір бүлдірушілер жүйені қандай да бір ақпаратты алу үшін емес, өзінің қабілетін тексеріп, нығайту үшін бұзған сәттері де болады.

1.3.3 DOS-бүлдірулер

Компьютер желісінің қызметін шектеу немесе растау үшін оған сыртқы пайдаланушылардың қызмет көрсетуіне кедергі жасау мақсатымен DOS-бүлдірулерді қолданады. Әдетте, бұл тәрізді бүлдірулер жүйенің күйреуіне немесе пайдаланушыларға әрі қарай қызмет көрсету мүлдем болмай бара жатқан деңгейге дейін оның жұмысының баяулауына жетелейді.

Бұл ретте DOS-бүлдірулер компания жұмысы үшін аса қажет маңызды

ақпараттардың жойылуымен немесе бүлінуімен тұжырымдалуы мүмкін. Мұндай бүлдірулерді орындау арнайы бағдарламаны немесе сценарийді орындаумен шектеледі, бұл ретте, қаскүнемге тіпті бұзылатын жүйеге қолжеткізу мүмкіндігінің болуы талап етілмейді, тек оған апаратын бағытты білсе жеткілікті.

Мұндай бағытты алу шын мәнінде DOS-бүлінуіне әкеп соғады. Себебі мұндай бүлдірулер өте оңай жүзеге асырылады және аты-жөнін көрсетпеу сақталады, сонымен бірге желіні бұзудың кеңінен тараған түрі болып табылады.

Қызмет көрсетуде бас тартуға жетелейтін бүлдірудің бөлінген ұғымы (DistributedDenialofService - DOS) компьютерлердің басым бөлігімен бірмезгілде жүзеге асырылатын көптеген DOS-бүлдірулер деп түсіндіріледі, яғни бұзудың бастапқы қоркөзін бұғаттауға және анықтауға мүлдем мүмкіндік бермейді.

Желілердің шабуылы, түрлері және қорғау

Вирусқа қарсы бағдарламаларды, брандмауэрлерді, криптографиялық құралдарды және т.б. тәрізді қауіпсіздікті қамтамасыз ету құралдарын мақсатты бағытта қолдану деректерге сырттан қолжеткізу мүмкіндіктерінен сақтауға көмектесетіндігі мәлім. Бірақ сонда да адами фактор туралы ұмытуға болмайды. Адам ақпараттық жүйе қауіпсіздігінің әлсіз факторы болып табылады, сондықтан мұны басқалардың ақпарат жүйесіне кіріп кететін компьютерлік бұзақылар әлеуметтік инженерия әдістерінің көмегімен қолданады.

Пайдаланушылар оңай бұзуға болатын қарапайым құпиясөздерді қолданған сәтте көп сатылы қорғаныс жүйесінен ешбір пайда болмайды. Бұл мәселені шешу үшін компания күрделі және өте сирек кездесетін құпиясөздерді орталықтандырылған жолмен алынған құпиясөздерді қолданады немесе қауіпсіздік шараларын сақтамағаны үшін қатаң жаза белгілейді.

Желілік шабуылдар барынша алуан түрлі болса, олардың қарсы бағытталған жүйелері де алуан түрлі болып табылады. Желілік шабуылдардың басым бөлігі бастапқыдан TCP/IP хаттамасына тән бірқатар шектеулерді қолданады. IP жүзеге асыру алғашқы кезде әлсіз болған, себебі интернет-хаттаманың (IP) бұрынғы нұсқаларының өзіндік сипаттамаларында қауіпсіздік талаптары жоқ. Тек электронды коммерция қарқынды дамыған соң және басқалардың ақпарат жүйесіне кіріп кететін компьютерлік бұзақылардың қатысуымен айтарлықтай келеңсіз оқиғалар орын алған соң ғана интернет-хаттаманың қауіпсіздігін қамтамасыз ету құралдары кеңінен енгізіле басталды.

IP үшін алғашқы кезде қорғаныс құралдары жете зерттелген жоқ, сол себептен оны жүзеге асыру үшін ол осы хаттамаға тән қауіп дәрежесін төмендететін, түрлі желілік рет-жосықтармен, қызметтермен және өнімдермен толықтырыла басталды.

1.3.4 Пошталық бомбалау

Шабуылдардың ең көне және арзанқол түрлерінің бірі электронды поштаны бомбалау болып табылады. Бұл тіпті компьютерлік мұраларды орынсыз қирату деп аталады. Пошталық бомбалаудың мәні пошта жәшігі түрлі хат-хабарлармен ластанады, тіпті кейбір жағдайда интернет-провайдердің пошталық сервері істен шығып кетеді. Осы мақстатты жүзеге асыру үшін арнайы бағдарламалар – мэйлбомберлер қолданылады. Яғни бұл бағдарламалар белгіленген мекен-жайды жөнелтушінің мекен-жайы, кейде тіпті IP-мекен-жайлары туралы жалған деректер көрсетілген түрлі хаттармен толтырады. Бұл бағдарламада тек жөнелтілуі тиіс хаттардың көлемі және мазмұны, пошталық мекен-жайы көрсетілуі тиіс. Көбінесе тіл тигізетін бір нәрсе жазылады. Әрі қарай, егер бағдарлама мекен-жайды көрсетпесе, онда жөнелтушінің жалған деректерін жазу қажет және соңында жөнелту үшін «іске қосу» түймешігін басамыз.

Дегенмен, интернет-провайдерлердің басым бөлігінде пошталық шабуылдардан клиенттерді қорғау үшін өз жүйесі болады. Сондықтан пошталық бомбалаулардан уайымдамауға болады, себебі егер бір мекен-жайдан хаттардың белгіленген көлемі түссе, онда бұл хаттар жай ғана жойылады немесе спам ретінде белгіленеді.

1.3.5 Құпиясөзді таңдау шабуылдары

Басқалардың ақпарат жүйесіне кіріп кететін компьютерлік бұзақы жүйеге шабуыл жасаған сәтте, ол әдетте кәсіпорын әкімгерінің немесе қандай да бір қарапайым пайдаланушының құпиясөзін бұзуға ұмтылады. Құпиясөзді біліп алудың сан алуан тәсілі бар. Құпиясөзді бұзудың негізгі тәсілі пакеттердің IP-спуфингі және сниффингі болып табылады. Бұл тәсілдерді әрі қарай қарастырамыз. Жүйеге «троян атын» енгізу - басқалардың ақпарат жүйесіне кіріп кететін компьютерлік бұзақылардың іс жүзінде барынша кеңінен таралған тәсілдерінің бірі, біз бұл жөнінде әрі қарай толығырақ тоқтиаламыз.

«Маңдайға» іріктеп алу (bruteforceattack - «өрескел күшпен шабуылдау»). Құпиясөздің мүмкін болатын барлық амалдарын жай ғана теретін көптеген бағдарламалар бар. Бұл бағдарламалардың кейбірі белгіленген сөздік бойынша құпиясөзді іріктеп тере бастайды, ал басқалары рандом әдісімен таңбалардың түрлі кезектілігімен жай ғана кездейсоқ түрлендіріледі. (bruteforceattack - «атака грубой силой»).

Құпиясөздің логикалық іріктелуін пайдаланатын, басқалардың ақпарат жүйесіне кіріп кететін компьютерлік бұзақылар пайдаланушы құпиясөз ретінде қолдануы мүмкін түрлі таңбаларды жай ғана іріктеп береді. Бұл әдіс көбінесе өте тиімді болып табылады. Компьютерлердің тәжірибелі пайдаланушыларын адамдар құпиясөз ретінде qwerty123 үлгісін, өзінің атын қарапайым теруді немесе атын ақырғы жағынан жазуды қолданатындығы енді таң қалдырмайды.

Басқалардың ақпарат жүйесіне кіріп кететін компьютерлік бұзақылар құпиясөзді бұзу барысында адамды мұқият зерделейді. Мысалы, оның отбасы мүшелерінің және өзге де туыстарының есімдері, үй жануарларының лақап аттары; спорттың қандай түрімен айналысады және қай команданың жанкүйері,

сүйікті кітаптары және фильмдері, таңертең қандай газет оқиды. Осы деректерді ол құпиясөз ретінде қолдануы мүмкін. Осы тәрізді жағдайлардан алшақ болу үшін ешбір мәні жоқ кездейсоқ таңбаларды қолдануға немесе бағдарламаның арнайы түрленген құпиясөздерін қолдануға нұсқау беріледі.

Әрине, оқтын-оқтын құпиясөзді ауыстыру қажет - мұны жүйелік әкімгер бақылап отыруға міндетті. Әлеуметтік инженерия. Компьютерлік бұзақылар пайдаланушыларға психологиялық әдіс жұмысын қолданады. «Жүйелік әкімгер» ретінде қоңырау шалынып, «Мұнда біздің жүйемізде тоқтап қалу орын алды және пайдаланушылар туралы ақпарат жойылды. Сол үшін Сіз тағы да бір рет өз логиніңіз бен құпиясөзіңізді хабарлап жібересіз бе?» деген өтініш білдіруі әдеттегі және қарапайым мысал болып табылады. Мұндай жағдайда пайдаланушылар еш нәрсені күмәнға алмастан өздері компьютерлік бұзақыларға құпиясөзін береді. Қырағылықтан басқа, қорғаныс ретінде бірреттік құпиясөздер жүйесі қолданылады. Алайда бұл әдіс өз қолдануының күрделі болуына байланысты кеңінен таралмаған.

Вирустар, поштalық құрттар және «троян аттары»

Мұндай басып кірулер негізінен провайдерлердің немесе корпоративтік коммуникациялардың емес, соңғы пайдаланушылардың компьютерлерін зақымдайды. Ауқымды компьютерлік індет көптеген миллиардтаған залал келтіреді, себебі зақымдалу аясы жай ғана әсерлі болып табылады. Осындай ашу-ызалы бағдарламалардың авторлары қазіргі таңдағы вирустарға ең озық бағдарламалық және психологиялық технологияларды нақты енгізіп, барынша шектен шығып, мұнымен тоқтамайды.

Вирустар және «троян аттары» залалды бағдарламалық листингтің түрлі топтары болып табылады. Басқа бағдарламаларға вирустарды енгізу мақсаты оларға пайдаланушы жұмыс атқаратын, кәсіпорынның жұмыс стансасына зиян келтіретін қызметтерді енгізу болып табылады. Оған қатты дискіде белгіленген файлдарды ғана немесе бәрін жою, жабдықты жарамсыз ету немесе басқа да операциялар мысал бола алады. Кейде вирустар, осы уақытта әсер ете бастауы үшін белгіленген мерзімге бағдармаланады. Сонымен бірге электрондық поштаны қолдана отырып, пайдаланушының мекен-жай тізімінен табылған барлық мекен-жайлар бойынша өзінің көшірмесін жөнелтеді. Троян атының вирустан айырмашылығы вирустарға тән ақпаратты өрескел бұзуға бейімделмеген, өз бетінше жеке бағдарлама болып табылады. Көбінесе троян аты компьютерге қашықтан жасырын бақылау жүргізу, келешекте ондағы ақпаратты қулық әрекеттер үшін пайдалану мақсатында жүйеге енгізіледі.

Троян аттарын Интернетте орын алған түрлі ойындармен жасырады және тегін таратылады. Кейде, тіпті компьютерлік бұзақылар троян аттарын пайдаланушылар жиі қолданатын әдеттегі бағдарламаларға үндестіріп қояды. Енгізген соң олар компьютерде өздірінің бар екенін білдірмей, өз қызметтерін мүкіндігінше жасырын орындайды. Мысалы, троян аттары тәрізді мұндай бағдарламалар компьютерлік бұзақыға аталған нақты компьютерден Интернетке кіру үшін құпиясөз бен логинды жасырын жібере алады, сонымен бірге белгіленген файлдарды жасайды және оған енгізілген мекен-жай бойынша

жөнелтеді, пернетақтадан енгізілгеннің бәрін тексереді және т.б.

«Троян аттарының» барынша шектен шыққан нұсқалары белгіленген пайдаланушылардың нақты компьютерлерін шабуылдауға бейімделеді. Сонымен қатар олар компьютерлік бұзақылардың өкімі бойынша кейбір деректерді алдын ала дайындалған басқа деректерге ауыстыруы мүмкін. Компьютер иесін жаңылысуға жетелеп, олар файлдарда сақталған деректердің түрін өзгертеді. Яғни, өнеркәсіптік тыңшылық және арандатушылық тәсілдердің ішіндегі барынша кең таралған әдісі. Мұндай вирустармен және троян аттарымен арнайы мамандандырылған бағдарламалық қамтамасыз етулерді қолдану арқылы күресу қажет. Жақсы орнатылған қорғаныс нақты компьютер деңгейінде және локалді желі деңгейінде қосарлы бақылау жүргізуді қамтамасыз етеді.

Бүгінгі күні қауіпсіздікті қамтамасыз ету құралдары едәуір тиімді болып табылады және тәжірибе бойынша компьютерлік вирустардың үнемі таралуына пайдаланушылардың өздері кінәлі болып табылады. Пайдаланушылардың және жүйелік әкімгерлердің басым бөлігі вирусқа қарсы бағдарламалардың дерек қорын үнемі жаңартуға және электронды хатты оқудың алдында вирусқа тексеріп алуға (бірақ бүгінде бұл Интернет қызметтері провайдерлерінің міндетіне кіреді) ерінеді.

1.3.6 Желілік барлау

Желілік барлау барысында компьютерлік бұзақы ешқандай зиян келтіретін әрекеттер жасамайды және сол себептен желілік барлауды компьютерлік желіге басып кіру деп атай алмаймыз. Осыған қарамастан желілік барлауды кем бағалауға болмайды, себебі бұл үнемі шабуылды алдын алады және оған дайындық кезінде компьютерлік бұзақылар үнемі жүйе туралы барлық қолжетімді ақпаратты жинауы тиіс. Компьютерлік бұзақы мейлінше пайдалы ақпараттар жинауға тырысады және ақпараттар жалпы қолжетімді деректер мен қосымшалардың көлемді тізбегін қолдану арқылы жиналады. Ақпараттарды жинау үшін порттар көшіріп алынады, DNS сұраныстары жүргізіледі және DNS көмегімен ашық мекен-жайларды және т.б. жаңғыртып-тестілеу жүргізіледі. Осылайша, осы немесе басқа домен және осы доменге таңылған мекен-жайлар кімге тиесілі екенін анықтауға болады. DNS ашылатын, мекен-жайларды жаңғыртып-тестілеуді қолдану аталған желіде шын мәнінде қандай хост жұмыс атқаратынын көруге мүмкіндік береді, ал порттарды көшіріп алу құралдарының көмегімен осы хостармен қолдау көрсетілетін қызметтердің толық тізімін құрастыруға болады. Сонымен бірге желілік барлау және қосымшаларға сипаттама жүргізу кезінде ақпарат сарапталады, нәтижесінде оны бұзу немесе DOS- шабуылдар жүргізген сәтте қолдануға болады. Себебі желілік барлау кезінде зиян келтіретін әрекеттер жасалмайды, желілік шабуылдан толығымен арылу мүмкін болмайды. Мысалы, егер қашықтық бағыттаушыда ICMPжаңғырығы және жаңғырық-жауабы өшірілсе, онда жаңғыртып-тестілеуден арылуға болады, бірақ бұл ретте Желіде тоқтап қалуларды анықтау үшін қажет деректерді жоғалтып алуға болады. Оған қоса

компьютерлік бұзақы порттарды алдын ала жаңғыртып-тестілеусіз көшіріп ала алады.

Желі және хостар деңгейінде қорғаушы және бақылаушы жүйелер, әдетте, желілік барлаудың жүргізілуі жайында жүйелік әкімгерді хабардар ету тапсырмасын толық орындай алады. Жүйелік әкімгер өз міндеттерін жақсы орындаған кезде алдағы шабуылға дайындалады және шабуылға жол бермеу үшін мысалы, провайдерді желіден біреу шамадан тыс құмарлық танытып отырғаны жөнінде хабардар етіп, қауіпсіздік шараларын қабылдай алады.

1.3.7 Сниффинг пакеттер

Сниффер пакеттер promiscuous mode тәртібінде жұмыс атқаратын желілік картаны қолданатын қолданбалы бағдарлама болып табылады. Яғни, желілік адаптер осы тәртіпте өңдеуге арналған физикалық арналар, қосымша бойынша қолжеткізілген барлық пакеттерді жөнелтеді. Бұл ретте сниффер шабуыл жасайтын домен арқылы таратылатын барлық желілік пакеттерді қамтиды. Сниффферлердің ерекшелігі, олар тап осы кездегі көптеген жағдайда желілерде толық заң негізінде жұмыс атқарады, себебі трафикті сараптау және бұзылғанды анықтау үшін қолданылады. Осыған байланысты, бұл сниффер-бағдарламасы бұзақылармен қолданылды ма немесе қызметтері барынша «кеңейтілген» ұқсас бағдарламаға жай ғана ауыстырылды ма, міне осының бәрін үнемі толығымен сенімді анықтауға болады. Бұзақылар сниффердіқолданып, түрлі құпияларды біліп қоя алады. Мысалы, пайдаланушылардың аты және құпиясөздері. Бұл кеңінен қолданылатын бірқатар желілік қосымшалардың elnet, FTP, SMTP, POP3 және т.б. тәрізді мәтінді форматта деректер таратуымен байланысты. Ақпараттар дерегін тіпті бірреттік қолға түсірудің салдары кәсіпорынға айтарлықтай қауіп төндіреді, себебі пайдаланушылардың басым бөлігі басқа қосымшалар мен жүйелер үшін де сол бір ғана логин мен құпиясөзді қолданады. Бір қызметкердің логині және құпиясөзі туралы ақпаратты бір рет қолға түсіріп алған бұзақы жүйелік деңгейде пайдалану ресурсына қолжеткізу мүмкіндігін ала алады және кез келген сәтте Желіге және ақпараттық ресурстарға қолжеткізу үшін қолданатын, жаңа, жалған пайдаланушыны жарыққа шығарып алады. Алайда, құралдардың белгіленген жиынтығын қолдана отырып, пакеттердің сниффинг қаупін едәуір төмендетуге болады. Біріншіден, бұл тіпті адами факторларды қолдана отырып, айналып өтуі күрделі сәйкестендірудің едәуір құуатты құралдары. Мысалы, бірреттік құпиясөздер (One-TimePasswords).

Бұл екі факторлы сәйкестендіру технологиясы деп аталады, бұл ретте сіздегі бар зат сіз білетін нәрсемен уақыт жағынан сәйкес келтіріледі. Сонымен бірге аппараттық немесе бағдарламалық құрал кездейсоқтық қағидасымен бір сәттік бірреттік құпиясөзді түрлендіреді. Компьютерлік бұзақы сниффердің көмегімен осы құпиясөзді білген кезде, бұл ақпараттың пайдасы болмайды, себебі аталған сәтте құпиясөз қолданылып, пайдаланудан шығарылып тасталынады. Бірақ бұл тек құпиясөздерге ғана тән, ал электрондық поштадағы хабарламалар сонда да қорғаусыз қалады.

Сниффингпен күресудің тағы бір тәсілі бар ол сниффер-қарсыласын қолдану. Бұл Желіде жұмыс атқаратын снифферлерді танып білетін бағдарламалық құрал. Олар хостардың жауап қату уақытын өлшейді және хостардың артық трафикті өңдеген не өңдемегенін анықтайды. Мұндай құралдар сниффинг қаупін толығымен жояды, бірақ қорғаныстың кешенді жүйесін салуда қажет болады.

Тәжірибелі мамандардың пікірі бойынша сниффферлер жұмысын жай ғана пайдасыз ету барынша тиімді шара болып табылады. Мұны жүзеге асыру үшін байланыс арналары арқылы таратылатын деректерді криптографияның қазіргі таңдағы әдістерімен қорғау жеткілікті. Нәтижесінде, бұзақы хабарламаның орнына түсініксіз кезектілікпен жазылған ақпараттар мөлшерін, яғни шифрланған мәтінді қолға түсіреді. Барынша кең таралғаны Cisco корпорациясының IPSecot криптографиялық хаттамалары, сондай-ақ SSH (SecureShell) және SSL (SecureSocketLayer) хаттамалары.

1.3.8 IP-спуфинг

Спуфинг – шабуыл түрі, мұнда компьютерлік бұзақы өзін мекеме ішінде немесе оның сыртында рұқсат етілген пайдаланушы ретінде көрсетеді. Мұны жүзеге асыру үшін көптеген тәсілдер бар. Мысалы, компьютерлік бұзақы аталған кәсіпорын Желісінің аясында қолдануға рұқсат етілген аумақтың шегінде орналасқан IP-мекен-жайды немесе егер оның нақты белгіленген ресурстарға қолжеткізу мүмкіндігі болса авторизацияланған сыртқы мекен-жайды қолдана алады. Реті келгенде IP-спуфинг мейлінше күрделі, кешенді шабуылдардың құрамды бөлігі ретінде жиі қолданылады.

DOS шабуылын қарапайым мысал деп айтуға болады, мұнда компьютерлік бұзақы өзінің шынайы келбетін жасыру үшін қажетті бағдарламаны әдетте бөтен IP-мекен-жайға орналастырады. Жалған бұйрықтарды қолдану арқылы жүйені істен шығару және ұрлық жасау, қандай да бір өзге ақпаратты енгізу үшін IP-спуфинг қолданылады. Спуфинг қаупін жою мүмкін емес дерлік, бірақ қауіпті едәуір төмендетуге болады. Мысалы, қауіпсіздік жүйесін олар сыртқы желіден түсетін, ішкі желіде болуы тиіс кез келген трафикті бастапқы мекен-жаймен қоса жоя алатындай реттеп келтіруге болады. Бірақ бұл егер ішкі мекен-жайларға рұқсат етілсе ғана көмектеседі.

Аталған әдіс, егер кейбір сыртқы деректер осындай болса, онда жарамсыз болып табылады. Сонымен қатар қажет бола қалған жағдайда, сіздің желіңізге бөтен желінің пайдаланушылары спуфинг жасау ұмтылысын алдын ала тоқтату артық болмайды, себебі бұл іс-шара кәсіпорында бұзақы немесе әдеттегі компьютерлік бұзақы пайда болған сәтте көптеген келеңсіздіктерден арылуға мүмкіндік береді. Осы мақсатқа қолжеткізу үшін, егер бастапқы мекен-жай кәсіпорын IP-мекен-жайларының ішкі аумағы болмаса, онда кез келген шығыс трафигін қолдану қажет. Егер қажет болса, онда Интернет қызметтерінің провайдері аталған рет-жосықты орындай алады. Бұл сүзгішті RFC 2827 – деп атайды. Сонымен қатар сниффинг жағдайында қауіпсіздікті қамтамасыз ету

үшін спуффингтің пайдасыз болғаны тиімді болады. IP-мекен-жайлардың негізінде пайдаланушыларды сәйкестендіру орын алған жағдайда ғана IP-спуфингті пайдалануға болады. Осыған байланысты шабуылды сәйкестендіруді криптошифрлеу пайдасыз болады. Сонымен қатар мақсатқа қолжеткізу үшін кездейсоқ амалмен бірреттік құпиясөздерді түрлендіретін бағдарламаларды қолдануға болады.

1.3.9 Қызмет көрсетуден бас тартуға шабуыл

Бүгінгі күні желілік шабуылдардың барынша кеңінен тараған түрі қызмет көрсетуден бас тарту шабуылы (Denial of Service - DOS). Осымен бірге аталған әдіс жас технологиялардың бірі. Бұл тәсіл Интернеттің шын мәнінде жан-жақты таралуына байланысты қолданыла басталды. DOS-шабуылдар туралы осы техологияның көмегімен 1999 жылы желтоқсанда Amazon, Yahoo, CNN, eBay және E-Trade тәрізді әйгілі корпорациялардың web-тораптары «жүктелген» соң ғана кеңінен айтыла бастауы сәйкессіздік.

Алайда осыған ұқсас алғашқы хабарламалар 1999 жылы «рождественолық тосын сыйға» дейін 1996 жылы пайда болды, DOS-шабуылдар Желіде қауіпсіздіктің қатерлі қаупі ретінде қабылданбады. Жыл өткен соң, 2000 жылы желтоқсанда бәрі қайталанды: ірі корпорациялардың web-тораптарына DOS технологиясы бойынша шабуыл жасалды, ал олардың жүйелік әкімгерлері қайтадан бұзақыларға қарсы тұра алмады. Сонымен 2001 жылы DOS-шабуылдар әдеттегі іс болып қалды. Шынын айтқанда, DOS-шабуылдар ақпаратты ұрлау немесе онымен құлық әрекет жасау үшін жүргізілмейді, олардың негізгі мақсаты – шабуыл жасайтын web-тораптың жұмысын тоқтату. Шын мәнінде бұл жай ғана желілік терроризм. Американдық арнайы қызметтер ірі корпорациялардың серверлеріне жасалатын көптеген DOS-шабуылдардың артында аты шулы антиглобалистер тұрғанына күмән келтіруі кездейсоқ емес.

Шын мәнінде, қандай да бір жерде Мадридте немесе Прагада «Макдональдс» көрмесіне кірпіш лақтырған өз алдына бір іс болса, ал мүлдем басқасы – бұрыннан әлемдік экономиканы жаһандандырудың ерекше таңбасы болған, осы суперкорпорацияның сайтын – «күйрету».

DOS-шабуылдар, яғни оларды күшейту үшін кибертеррористерге қандай да бір ерекше білімді және ептілікті меңгерудің талап етілмеуімен қауіпті - барлық қажетті бағдарламалық қамтамасыз етулер технологияның өз сипаттамаларымен бірге Интернетке мүлдем еркін қолжеткізеді. Сонымен бірге осы тәрізді шабуылдардан қорғану өте қиын. Жалпы DOS-шабуылдар технологиясы келесідей бейнеде көрініс табады: нысана ретінде таңдап алынған web-торапқа бүкіл әлем бойынша көптеген компьютерлерден жалған сұраныстар борап түседі. Нәтижесінде, қызмет көрсететін сервер торабы тоқтатылып, әдеттегі пайдаланушылардың сұраныстарына да қызмет көрсете алмайды. Бұл ретте жалған сұраныстар жөнелтілетін компьютерлердің пайдаланушылары олардың компьютерлері бұзақылармен астыртын қолданылатынына күмән келтірмейді.

«Жұмыс жүктемесін» осылай бөлу тек шабуылдың бүлдіру әрекетін

күшейтіп қана қоймай, сонымен бірге шабуыл үйлестірушінің шынайы мекен-жайын анықтауға мүмкіндік бермей отырып, оны бейнелеу шараларын өте қиындатады. Шабуыл кезінде шабуыл жасайтын желінің шамадан тыс толып кетуі үшін тағайындалған трафикті Интернет қызметтерінің провайдерінде «кесіп тастау» қажет, себебі Желіге кіру жолында мұны жүзеге асрыу мүмкін емес болады – өткізудің барлық жолағы бос емес болады.

Осы үлгідегі шабуыл көптеген құрылғылар арқылы бірмезгілде жүргізілген жағдайда DOS (Distributed Denial of Service - DDOS) бөлінген шабуыл туралы сөз қозғалады. DOS-шабуылдарының қауіп-қатерін бірнеше тәсілмен төмендетуге болады. Біріншіден, желіаралық экрандарда және бағыттаушыларда анти-спуфинг қызметін дұрыс кескіндеу қажет. Бұл қызметтер кемінде RFC 2827 сүзгілеуді қамтуы тиіс. Егер компьютерлік бұзақы өзінің шынайы келбетін бүркеуге шамасы келмесе, ол шабуыл жасауға шешім қабылдауы екіталай. Екіншіден, желіаралық экрандарда және бағыттаушыларда анти- DOS қызметін қосу және дұрыс кескіндеу қажет. Бұл қызметтер жүйені шамадан тыс жүктеуге мүмкіндік бермей, жартылай ашық арналардың санын шектейді. Сонымен бірге DOS-шабуылдар қауіп-қатері төнген кезде сыналмайтын трафиктің Желі бойынша өту көлемін шектеуге нұсқау беріледі, бұл жөнінде өзінің интернет-провайдерімен келісу қажет. Әдетте, мұндай кезде ICMP трафигінің көлемі шектеледі, себебі ол тек қана диагностикалық мақсаттар үшін ғана қолданылады.

1.3.10 Man-in-the-Middle үлгісіндегі шабуылдар

Шабуылдардың осы түрі өнеркәсіптік бұзуға өте тән сипат.
Man-in-the-Middle үлгісіндегі шабуыл кезінде компьютерлік бұзақы Желі бойынша таратылатын пакеттерге қолжеткізу мүмкіндігін алады, сондықтан мұндай жағдайда мекеме қызметкерлерінің, провайдер-фирмасы қызметкерлерінің өзі қаскүнем болып табылуы жиі кездеседі. Man-in-the-Middle шабуылын қолдану үшін пакеттердің снифферлерін, тасымалдау хаттамаларын және бағыттаушы хаттамаларды қолдану қажет. Аталған шабуылдың мақсаты таратылатын ақпаратты ұрлау немесе бұрмалау, немесе желі ресурстарына қолжеткізу мүмкіндігін алу болып табылады. Бұл шабуылдар кәсіпорынның ішінде орын алғандықтан, шабуылдардың басқа түрлері тәрізді жүйені қорғау қиын. Сондықтан қауіпсіздікті қамтамасыз ету үшін таратылатын деректерді криптошифрлеу әдісін қолдану қажет. Мұндай жағдайда бұзақы өзіне қажет ақпараттың орнына, ұғып алатындай таңбалардың қандай да бір жиынтығына қолжеткізеді. Алайда, егер компьютерлік бұзақы жақсы жұмыс атқарса және оның жолы болып кетсе, онда оған криптографиялық сесси туралы деректерді қағып алу сәті түседі. Бұл жағдайда деректерді шифрлеудің түрлі мағынасы автоматты түрде жоғалады. Сондықтан аталған жағдайда күрестің «алдыңғы шебінде» техникалық мамандар емес, кәсіпорынның кадр бөлімі мен қауіпсіздік қызметі тұруы тиіс.

БҚ «тесіктерді» және «бактарды» қолдану

Компьютерлік бұзақы шабуылдарының мейлінше кеңінен тараған түрі

бағдарламалық қамтамасыз етуде, ең алдымен бүкіл серверлер үшін кеңінен қолданылатын әлсіз орындарды (ең дұрысы бүкіл ескірген, орындалып бітпеген) пайдалану болып табылады.

Microsoft жете зерттелген бағдарламалық қамтамасыз етулер ерекше сенімсіз және әлсіз қорғалған болып табылады. Әдетте, бұл жағдай келесідей өтеді: кім де кім сервер үшін бағдарламалық қамтамасыз етуде «тесік» немесе «бак» тауып алады және бұл ақпаратты тиісті конференцияның Интернетінде осы ақпаратты жариялайды.

Аталған БҚ өндірушісі осы түйінді мәселені жоятын және оны өзінің web-серверінде жариялайтын жамау шығарады. Мәселе мынада әкімгерлердің басым бөлігінің еріншектігінен патчелерді анықтауға және пайда болуына тұрақты тексеру жүргізілмейді және осал тұстарын анықтау және олардың түзету үшін қандай да бір уақыт өтеді. Компьютерлік бұзақылар қандай да бір кемшілікті жою бойынша жаңартуларды бақылайды және оны өз мақсаттары үшін қолданады. Ақпараттық қауіпсіздік жөніндегі жетістігі мол әлемнің жетекші мамандарының басым бөлігі бұрынғы компьютерлік бұзақылар екендігі кездейсоқтық емес.

Осы тәрізді шабуылдардың негізгі мақсаты - қосымшалармен, көбінесе жүйелік әкімгер құқымен және қолжеткізу мүмкіндігінің тиісті деңгейімен жұмыс атқарушы пайдаланушының атынан серверге қолжеткізу мүмкіндігін алу. Мұндай бұзып кіруден жүйені қорғау оңай іс емес. Осы тәрізді шабуылдарды жүргізу барысында қаскүнемдер сапасы төмен БҚ басқа себептердің бірі өту жолы технологиялық себептермен жабылмайтын және брандмауэр арқылы өту мүмкіндігі бар порттарды жиі қолданады. Жүйені қорғаудың үздік тәсілі бұл жақсы әрі жауапты әкімгер.

1.5 Желілердің қауіпсіздік саясаты және оны қамтамасыз ету

Компьютерлік желілердің қауіпсіздігін қамтамасыз ету жаңа компьютерлік технологияларды үнемі дамытумен және енгізумен шартталған, үздіксіз процесс. Сондықтан мекеменің компьютерлік жүйелерінде қауіпсіздікті қамтамасыз ету саясаты желілердің қауіпсіздігі аясында орын алған барлық ықтимал қауіп-қатерлерді ескеру арқылы жете зерттелуі тиіс.

RFC 2196 SiteSecurityHandbook құжатында: «Қауіпсіздік саясаты – мекеменің технологияларына және ақпараттық деректеріне қолжеткізу мүмкіндігі бар тұлғалар сақтауы тиіс қатаң белгіленген ережелер мен тұжырымдамалардың жиынтығы» деп айтылған.

Қауіпсіздік саясаты келесідей міндеттерді шешуі тиіс. Кәсіпорынның қорғалатын объектілерін сәйкестендіру. Сізге нені қорғау қажет екенін және оны Сіз қалай жүзеге асырасыз, міне осыларды анықтап алу қажет. Компьютерлік желідегі осал тұстарды айқындау және бұзып кіру үшін оларды қалай қолдану қажет екенін жете түсіну. Мұның бәрі аталған желіде жұмыс атқару барысында қауіпсіздік деңгейін арттыруға көмектеседі.

Қорғалатын ресурстарды қатаң есепке алуды ұйымдастыру. Қалыпты тәртіпте жүйенің қызмет етуін, қандай құрылғылаар қолданылатынын, желіде

деректердің қандай ағыны өтетіндігін зерделеңіз.

Желі құрылымдарын оның құрылғыларымен және сұлба деректерімен бірге анықтау. Желі қауіпсіздігін және оны қамтамасыз ету үшін қандай құралдарды қолдану қажет екенін ойлау қажет. Пайдаланушының құрылғыға физикалық тұрғыда қолжеткізу мүмкіндігі оған осы құрылғыға бақылау жүргізуге ықпал етеді.

Қауіпсіздікті қамтамасыз етудің барынша тиімді тәсілі қауіпсіздік саясатының үнемі жаңартып отыру, себебі ол жүйе қауіпсіздігін және жаңартылып отыратын қорғау тәсілдерін үздіксіз тексеруді қамтамасыз етеді. Қауіпсіздікті қамтамасыз ету процестерінің кезектілігін қауіпсіздікті қамтамасыз ету айналымы түрінде (SecurityWheel) бейнелеуге болады. Қауіпсіздік саясаты қауіпсіздікті қамтамасыз ету айналымын қамтитын төрт кезеңнің негізінде құрылуы тиіс.

1 Кезең.

Жүйені қорғау. Желілік жүйелерге құқықсыз қолжеткізу мүмкіндіктерін алдын алатын, келесі құрылғыларды және (немесе) жүйелерді қолданыңыз:

- One-TimePassword (OTP) тәрізді сәйкестендіру және бірегейлендіру жүйелері (IdentificationAuthenticationSystem), пайдаланушыларды сәйкестендіру және авторизациялау құралдарын қамтамасыз етеді, мұндай жүйелердің мысалы Cisco Secure Control Server (CSACS), Windows Dial-up Networking, S/Key, CryptoCard және SecurlD бола алады;

- шифрлеу авторизация жасалмаған пайдаланушылардың ақпарат ағынынан ақпаратты басып алуына жол бермеуге ықпал етеді. Internet-те жұмыс атқару кезінде шифрлеудің стандартты хаттамасы IPSecurity (IPSec) болып табылады. IPSec стандарты RFC2401 құжатымен белгіленген;

- желіаралық экрандар тек деректер ағынының белгіленген түрін ғана сүзгілеу арқылы деректер ағынын өткізуге немесе бұғаттауға мүмкіндік береді;

- желіде орын алған кемістіктерді жою оларды қолдануға негізделген бұзылымдарды алдын алу үшін қажет. Бұл процесс барлық жүйелерде қажет емес қызметтерді өшіруді көздейді. Жұмыс атқаратын қызметтер неғұрлым кем болса, бұзақыларға жүйеге кіру мүмкіндігі соғұрлым қиын;

- физикалық тұрғыдағы қауіпсіздікке өте кем назар аударылғанымен, ол компьютерлік желілердің қауіпсіздігін қамтамасыз етудің аса маңызды элементі болып саналады. Егер бұзақының желі жұмысын қамтамасыз ететін аппараттық құралдарды физикалық тұрғыда тонау мүмкіндігі болса, қауіпсіздікті қамтамасыз етудің барлық басқа мәселелерін шешу қажет емес болып қалады. Сонымен бірге маңызды деректерді тонау үшін қолдануы мүмкін түрлі құрылғыларды желіде рұқсатсыз орнатуға тыйым салу қажет.

2.Кезең

Қауіпсіздіктің корпоративтік саясатына қарсы бағытталған кемшіліктердің және бүлдірулердің орын алуы бойынша желіде орналасқан деректер ағынының жай-күйіне сараптама жүргізу. Қауіпсіздікті бұзудың бастапқы көзі желі ішінде тәрізді (мысалы, ренжулі қызметкерлер) оның шегінен тыс болуы да мүмкін (мысалы, компьютерлік бұзақылар).

Желінің қауіпсіздік саясатын бұзатын мұндай келеңсіздіктерден арылу үшін басып кіруді айқындауға тағайындалған арнайы жүйелерді қолдануға болады, мысалы, бұзып кірудің алуан түрін табуға және алдын алуға мүмкіндік беретін CiscoSecureInstructionDetectionSystem (CSIDS).

CSIDS жүйесін қолданумен бірге қауіпсіздікті қамтамасыз ету айналымының бірінші кезеңін сипаттауда ескерілген қауіпсіздікті қамтамасыз ететін, құрылғыларды ретке келтірудің дұрыстығы тексеріледі. Жүйеде орын алатын барлық оқиғаларды хаттамалау желіде деректер ағынының жай-күйін сараптаудың маңызды құрамы болып табылады. Желіден өтетін деректер ағынына хаттама жүргізу бұзақының желі туралы ақпарат жинау кезеңіндегі іс-әрекетін айқындауға және желінің бүкіл жұмысын бұғаттайтын бұзылымды алдын алуға көмектеседі.

3. Кезең

Қауіпсіздікті қамтамасыз ету әдісетерінің және құралдардың тиімділігін тексеру. Сізде желінің қауіпсіздігін қамтамасыз ету жүйесі өте қымбат және қиын боуы мүмкін, ал егер оның құралдары дұрыс баптап күйге келтірілмесе желі не дұрыс жұмыс істемейді, не оны бұзу оңай болады.

4. Кезең

Қауіпсіздіктің корпоративтік саясатын үздіксіз жетілдіру. Қауіпсіздіктің жалпы деңгейін арттыру мақсатында желідегі деректер ағынының жай-күйін сараптау нәтиежесінде қолжетікізілетін барлық ақпаратты жинау және сараптау қажет. Сонымен қатар желілердің қауіпсіздік қауіп-қатерлерінің және жаңа кемістіктерінің барлығы дерлік күн сайын айқындалады, мұны есте сақтау қажет.

Желінің қауіпсіздік деңгейін барынша арттыру үшін барлық төрт кезеңді орындау қажет – желіні қорғау, деректер ағынының жай-күйін сараптау, қауіпсіздік саясатын жетілдіру және сынақтан өткізу. Осы аталған кезеңдердің барлығы үнемі бірі біріне ауыстырылып отыруы тиіс. Әрбір жаңа кезекті айналым қауіпсіздіктің корпоративтік саясатына сапалы өзгерістер енгізуі тиіс.

Желінің қауіпсіздігін қамтамасыз ету тұрақты жұмыс атқаруды және бөлшектерге жіті назар аударуды талап етеді. Аталған жұмыс «Бағдадта бәрі тыныш кезде», бұзақылар тарапынан орын алуы мүмкін іс-әрекеттерді жорамалдаумен, қорғаныс шараларын жоспарлаумен және пайдаланушыларды үнемі оқытумен тұжырымдалады. Егер жүйеге басып кіру орын алған болса, онда қауісіздіктің жүйелік әкімгері қорғау жүйесіндегі бұзып кіру жолын, оның себептерін және басып кіру әдісін табуы тиіс.

Әкімгер қауіпсіздікті қамтамасыз ету саясатын қалыптастыра отырып, ең алдымен ресурстарға түгендеу жүргізеді, сәйкесінше оны қорғау жоспарланады, ресурстар дерегінен әрқайсысына қолжеткізу мүмкіндігін алу үшін талап етілген пайдаланушыларды сәйкестендіреді, ресурстар дерегінің ішінен әрқайсысы үшін қауіпсіздіктің барынша ықтимал көздерін анықтайды. Аталған ақпаратқа ие бола отырып, пайдаланушылар орындауға міндетті қауіпсіздікті қамтамасыз ету саясатын жобалауға кірісуге болады.

Қауіпсіздікті қамтамасыз ету саясаты – бұл онсыз да бәріне түсінікті қарапайым ережелер емес. Ол басылып шыққан қатаң құжат түрінде болуы тиіс.

Пайдаланушыларға қауіпсіздікті қамтамасыз ету маңызды екенін әрқашан естеріне салып отыру үшін аталған ереже барлық қызметкерлердің үнемі көз алдында болуы мақсатында осы құжаттың көшірмесін таратуға болады. Қауіпсіздікті қамтамасыз етудің жақсы саясаты бірнеше элементтерді қамтиды.

Қауіп-қатерді бағалау. Біз, дәлірек айтқанда, нені және кімнен қорғау қажет екенін бағалауымыз қажет. Желіде орналасқан құндылықтарды және әлеуеттік қоркөздерін бірегейлендіру қажет және жаңа есептік жазбаларды бекітуден бастап бұзылуларды зерттеуді аяқтаумен қауіпсіздікті қамтамасыз етудің осы немесе өзге шараларын және құралдарын қабылдауға кім жауапты екенін көрсету қажет.

Желілік ресурстарды пайдалану ережелері. Саясатта пайдаланушылар ақпаратты тағайындалусыз пайдаланбау, желіні өздерінің жеке мақсаты үшін қолданбау, сондай-ақ желіге немесе онда орналасқан ақпаратқа мақсатты бағытта зиян келтірмеу тікелей көрсетілуі тиіс.

Заң аспектілері. Сонымен қатар заңгерден кеңес алуға және деректер желісінде сақталған немесе түрлендірілген барлық мәселелерді анықтауға және бұл деректерді қауіпсіздікті қамтамасыз ету құжаттарына енгізуге нұсқау беріледі.

Қорғау жүйесін қалпына келтіру рет-жосықтары. Қорғау желісі бұзылған жағдайда не істелінуі қажет екенін және осындай бұзылымның орын алуына себеп болғандарға қандай іс-әрекеттер қолданылатындығын нақты көрсету қажет.

1.6 Басып кірулерді топтастыру

Әдеттегі басып кіру мақсаты болып табылатын ресурстар тізімін RFC 1244 құжатынан табуға болады.

Басып кіру мақсаттарының қандай екеніне байланысты, оларды бес тапқа топтастыруға болады.

Аппараттық құралдар – бұл жұмыс стансалары және серверлері, баспалық құрылғылар, дискілі жинақтаушылар және желілік кәбілдер, сонымен бірге көпірлер, бағыттаушылар және коммутаторлар тәрізді желілік құрылғылар.

Бағдарламалық қамтамасыз етулер. Кез келген бағдарламалық қамтамасыз ету желіде кез келген компьютермен жұмыс атқаратын бұзақылар үшін әлеуетті қоркөзі болып табылады. Сыртқы зерттеушілерден сатып алынған және меншігіндегі бағдарламашылар бөлімімен құрылған, ішкі қолдану үшін тағайындалған бағдарламалық қамтамасыз етулер осындай бағдарламалар ретінде қызмет етеді. Сол себептен операциялық жүйелер тұрақты түрде патчтардың орнатылуына мұқтаж.

Ақпарат. Желіде қолданылатын немесе құрылатын деректер өте маңызды болып табылады. Барлық бағдарламалық қамтамасыз етулерді және операциялық жүйелерді қайта орнатуға болады. Бірақ, егер мысалы, клиенттердің тізімі, сату туралы мәліметтер немесе корпоративтік құпиялар тәрізді маңызды деректер таралып кетсе, онда зор шығынға ұшырауы мүмкін.

Адамдар. Желіге немесе оған қосылған кез келген құрылғыға кіру

мүмкіндігі бар барлық пайдаланушылар қауіп-қатер тобына кіреді.

Құжаттар. Бұл ресурс компьютерлік бұзақылар үшін өте маңызды екенін есте сақтау қажет. Әдетте, көптеген жағдайда бұл қоқысқа тасталынған басып шығарылған құжаттар немесе блокнота жазылған құпиясөздер. Қаскүнемдердің қолына бұл деректер түспеу үшін қағаздарды ұсақ бөлшектерге майдалау немесе басқа тәсілмен оларды оқи алмайтындай етіп, тек сонан соң ғана тастау қажет. Компьютерлік қауіпсіздіктің үлкен қауіп-қатері жапсырмалы парақтарға жазылған белгілер. Адамдардың басым бөлігі өздерінің логиндері мен құпиясөздерін осындай жапсырма парақшаларға жазып, монитордың шетіне желіпдеп қояды. Бұл қауіпсіздік саясатын бұзу болып саналады.

Пайдаланушылардың бәріне түсінікті, жақсы ойлап табылған қауіпсіздікті қамтамасыз ету саясаты кейбір әлеуетті қауіп-қатерлерді алдын алудың қарапайым құралдарына анағұрлым берік. Пайдаланушыларды таңдап алынған саясатпен жүйелі түрде қайталап таныстыру рет-жосығы, жұмыс орнында техника қауіпсіздігі нұсқамасымен таныстыру тәрізді жақсы тәжірибе болып табылады. Бұл жай ғана формалділік болмауы тиіс, мұның бәрі іс жүзінде қолданылуы тиіс. Пайдаланушылар корпоративтік компьютер желісіне қолжеткізу құқымен қоса бірмезгілде, олар өздеріне алып отырған барлық жауапкершілікті сезінуі өте маңызды.

1.6.1 Физикалық сипаттағы қауіпсіздік

Желілік ресурстарға авторизациясыз кіру мүмкіндігін алдын алу ең алдымен, желінің құрамдас бөлігіне – жұмыс стансаларына, серверлеріне, желілік кәбілдерге және құрылғыларға және т.б. физикалық тұрғыда қолжеткізе алмау мүмкіндігін білдіреді. Желілік қосылулар мысалы, интернеттің сыртқы провайдеріне қосу нүктесінде әсер ету аясынан шығып кеткен кезде, желінің физикалық аспектілеріне бақылау жоғалады, сондықтан шифрлеу және туннелдеу тәрізді қорғаудың басқа әдістеріне жүгінуге тура келеді. Келеңсіздіктерге жол бермеу үшін мекеменің жайында қолданылатын жабдық жіті бақылауда болуы тиіс.

Қаншалықты дөрекі болса да, көбінесе рұқсатсыз кіруден әдеттегі есік құлпы құтқарады. Өте маңызды және осал деректердің барлығы серверде орын алады, сондықтан серверлер үстел үстінде ашық қалмауы тиіс немесе кез келген адам кіруге болатын бөлме жабық болуы тиіс. Бағыттаушылар, концентраторлар, коммутаторлар және басқа құрылғылар да осылай қорғалуы тиіс.

Серверлер сақталған бөлмелер қатаң түрде кілтпен жабылуы немесе қатаң бақылауда болуы тиіс. Біреу тәулік бойы жұмыс атқарған жағдайда және қызметкерлер бір бірден кезекшілік жасамайтын болса, онда бұл бөлмені кілтпен жабу міндетті емес. Дұрысы, мұндай жайларға кіру, мысалы журналға тіркеу арқылы бақылануы тиіс.

Таспалар, қайта жазылатын жинақы-дискілер, жалпы резервтік тасымалдаушылар да бастапқы деректер тәрізді қорғалуы тиіс. Резервтік көшірмелерді серверде немесе жұмыс стансасында сақтамау қажет, сонымен

бірге картридждерді және CD үстел үстінде немесе кілттелмеген жәшікте қалдырмау қажет.

Көне компьютерлерді пайдаға асыру

Желіні жаңартқан кезде және жаңа жұмыс стансалары мен серверлерін орнату кезінде, көне және қажет емес жабдық көбінесе компания қызметкерлеріне немесе басқа мекемелерге, мысалы мектептерге тапсырылады.

Бастапқыда қауіпсіздікті қамтамасыз ету саясатын таңдаған сәтте ережеге сәйкес есептен шығарылатын барлық қатты дискілерден, оған жазылған бүкіл деректердің жойылуы, қажеттілігіне қарай операциялық жүйенің ресми көшірмесінің қайта орнатылуы ескерілуі тиіс. Сонымен қатар саясатта қолданылған дискеттерді, жинақтау-дискілерін және резервтік көшірмелері бар картридждерді пайда асыру рет-жосығы сипатталуы тиіс.

Ең дұрысы, егер қайта қалпына келтіруге болатын маңызды ақпаратты сақтауға кішкене ғана күдік болса, ақпарат тасымалдаушыларды алдымен сындырып, тек сонан соң ғана тасттау қажет. Мұндай жағдайда «жаппай» өшірудің магниттік құрылғысы бұл тасымалдаушылардан ақпараттарды жоюдың жақсы құралы болып табылады.

Бағдарламалық кіру мүмкіндігі

Физикалық тұрғыда кіру мүмкіндігімен бірге желіге бағдарламалық кіру мүмкіндігін де шектеу қажет. Кіру мүмкіндігіне жіті бақылау қойылғанына қарамастан, бұл қорғанысты бұзатын адам әрқашан табылады. Сондықтан желілік оқиғаларды бақылау және олар арқылы әлдекімдер желіге басып кіруге ұмтылыс жасаған не жасамағанын, ал егер жасаған болса, қаншалықты орын алғанын анықтау мүмкіндігі болуы маңызды.

Желіге кіру мүмкіндігін бақылаудың бірнеше типтік тетіктері бар:

- пайдаланушылық есептік жазбалар және құпиясөздер;
- физикалық тұрғыдағы сәйкестендіргіштер;
- ресурстарды қорғау.

Көптеген операциялық жүйелерде ресурстарды меңгеру тұжырымы осы сұлбаның маңызды бөлігі болып табылады. Мысалы, OpenVMS және Windows 2000/Server 2003 ресурстар (файлдар тәрізді) құратын пайдаланушылар бақыланады. Мұндай ресурстардың иелерінде файлды қорғау тәртібін өзгеру және осы файлмен жұмыс атқару үшін қажет өкілеттілікті өзге пайдаланушыларға ұсыну құқы бар. Алайда шамалы дәрежеде болса да, Unix/Linux 7 операциялық жүйелер туралы да осындай тұжырым жасауға болады.

Пайдаланушыларды бірегейлендіру

Егер желіде аса құпиялы деректер сақталмаса, онда бұл ресурстарға қолжеткізу үшін логин мен құпиясөз жеткілікті. Мұндай жүйелерді басқару әдетте қиындық тудырмайды. Windows 2000/XP және Server 2003 домендер, яғни басқарудың ерекше қорғалған аймақтарын құруға болады.

Жүйелік әкімгер домен пайдаланушыларына кез келген компьютердің серверіне немесе жұмыс стансасына, яғни ресурстарына кіру құқын ұсына алады. Сонымен қатар, әкімгерлердің бірлескен қызметі барысында домендер арасында сенімді қарым-қатынас орнатылуы мүмкін, нәтижесінде пайдаланушылар сол есептік жазба және құпиясөз арқылы өзге доменнің

желілік ресурстарына қолжеткізу мүмкіндігін алады. Windows 2000 және өте көне нұсқаларда маңызды ресурстарға қолжеткізу мүмкіндігін шектеу үшін топтық саясат қолданылуы мүмкін.

Novell NetWare үшін пайдаланушыға тіркелген желілік есім ұсынатын Novel Directory Services қызмет қолданылады. Әрбір пайдаланушы қасиеттерінде оның құпиясөздері және қосылулар туралы ақпаратты қамтитын User объектісінің каталогында ұсынылады.

Unix операциялық жүйелерде домен тұжырымы жоқ. Оның орнына Unix әрбір хосты шифрленген құпиясөзбен қоса әрбір пайдаланушы туралы ақпарат сақталған құпиясөздер файлын қамтиды. Unix пайдаланушысы басқа желілік хостардың ресурстарына кіру үшін не осы компьютерде тіркелуі, не проксилерді қолдануы тиіс. FTP және Telnet тәрізді TCP/IP утилиттер желі бойынша пайдаланушылардың құпиясөздерін ашық мәтінмен жиі жібереді, сондықтан компьютерлік бұзақылар үшін оңай олжа болып табылады. Unix файлдарды көшіру немесе басып шығару, немесе қашықтағы жүйеде тіркелу тәрізді қарапайым желілік операцияларды орындау үшін әдетте r-бұйрықтары (олардың есімдеру r әрпінен басталады) деп аталатын қашықтағы жұмыстың утилиттері қолданылады. Мұндай утилиттер бірнеше компьютерде бір пайдаланушы жұмыс атқаратын желілік ортада өте пайдалы, бірақ көбінесе қауіпсіздікке қатысты мәселелерді туындатады: себебі қашықтағы хоста бұйрықты орындау үшін пайдаланушыға осы хостың шын мәніндегі есептік жазбасына қолжеткізу жеткілікті. Құпиясөздің орнына кіру мүмкіндігінің құқы /etc/hosts.equiv немесе rhosts файлындағы жазбамен анықталады. Қашықтағы компьютер r-бұйрықтарын орындайтын пайдаланушының компьютеріне, егер осы файлдардың бірінен тиісті жазбаны тапса сенім артады. Файлдың әрбір жазбасы /etc/hosts.equiv пайдаланушының есімін және хост есімін қамтиды, тиісті бұйрықтарды орындауға рұқсат етілген хосттарды және пайдаланушыларды бірегейлендіруге мүмкіндік береді. Сонымен қатар құпиясөзді енгізу талап етілмейді.

Егер пайдаланушы қашықтағы хостқа тіркелген болса, онда ол сәйкестендіруден өткен болып саналады. Файл.rhosts осы тәрізді жұмыс атқарады, бірақ пайдаланушының үй каталогында орын алады. Осы файлда көрсетілген қашықтағы пайдаланушылар өзінің есептік жазбалары негізінде іс-әрекеттерді орындай алады.

Unix және Linux операциялық жүйелердің басым бөлігінде негізгі r-бұйрықтарының сақтаулына қарамастан, енді оларда сәйкестендіруі және шифрлеуі бар r-бұйрықтары тәрізді деректерді таратуды қамтамасыз ететін қорғаныс қабыршағының (Secure Shell, SSH) балама – утилиттері пайда болады. SSH туралы барынша толық мәліметтерді мекен-жай бойынша, ал SSH-утилитінің тегін нұсқаларын веб-сайт арқылы алуға болады.

Мұның бәрі Windows NT/200/Server 2003/XP сенімді қарым-қатынастарының тетігін еске салады – бірақ қанша дегенмен бұл түрлі тетіктер. Қаскүнем өзін өзі қашықтағы торап ретінде таныту және Unix/Linux жүйесінде r-бұйрықтарының көмегімен жүйеге қолжеткізу мүмкіндігі жеңіл болады.

Жүйелік қызметтер

Windows серверлерінде түрлі қызметтерді орындайтын бедерсіз бір түсті процестер қызметтер деп аталады.

Сонымен қатар Unix операциялық жүйелерде демондар деп аталатын, бедерсіз бір түсті ұқсас процестер де бар. Осы және басқа процестер бедерсіз бір түсті болып табылады - пернетақтамен өзара әрекеттесуді талап етпейді және кейбір функцияларды іске қосуды күтетін компьютерде орындалады. Кейбір кезде олар жүйенің қорғалуының бұзылуына себеп болуы мүмкін.

Желінің барлық серверлерінде орындалатын бедерсіз бір түсті процестермен танысу және артығын өшіру қажет. Мысалы, Unix жүйесінде TCP/IP хаттамаларын жинаумен байланысты көптеген бедерсіз бір түсті демондар бар. Компьютерлердің біріне олар қажет, ал өзгелерінде олардың кейбірі ғана қолданылады. Төменде жиі өшіруге болатын кейбір демондар тізбектелген.

Кейбір кезде өшіруге болатын TCP/IP қызметтер:

- uucp - Unix бір компьютерінен басқаға көшіру;
- finger - пайдаланушылар туралы ақпарат алу;
- tftp – файлдарды таратудың қарапайым хаттамасы (Trivial File Transfer Protocol);
- talk – желі бойынша пайдаланушылар арасында деректермен алмасу мүмкіндігі;
- bootp – желі туралы ақпаратты клиенттерге ұсыну;
- systat – жүйе туралы ақпарат алу;
- netstat – ағымдағы қосылулар тәрізді желі туралы ақпарат алу;
- rusersd – осы сәтте тіркелген пайдаланушылар туралы ақпарат алу;
- rexd – жұмыс атқарып отырған утилиттерді жою.

Мысалы, tftp қызметі FTP жеңілдетілген нұсқасы болып табылады. Ол ықшамды және әдетте қайта бағдарламаланатын ПЗУ түрінде оңай жүзеге асырылады. Сондықтан бұл қызмет хостан бастап операциялық жүйені жүктеуді талап ететін кейбір құрылғыларда пайдалы. Бірақ FTP салыстырғанда tftp қызметі басқару тетіктеріне қолжеткізу мүмкіндігі жоқ екенін ескеру қажет, осыған байланысты ол үшін пайдаланушының есімі және құпиясөзі қолданылмайды. Сәйкестендіру жоқ, сол себептен дұрыс баптап күйге келтірудің тапшылығы – мысалы, белгіленген мақсаттар үшін ғана қолдану рұқсаты – жүйелердің қорғалуын елеулі дәрежеде бұзуға жетелеуі мүмкін.

Windows серверлерінде кез келген бағдарламаны немесе пакеттік файлды іс жүзінде қызмет тәртібіне сәйкес орнатуға және іске қосуға мүмкіндік беретін Resource Kit құрамынан екі утилит бар. Бұл орындалатын бағдарламаларды орнату үшін қолданылатын INSTRV.EXE және басқа файлдарды қызметке айналдыру үшін қолдануға болатын SRVANY.EXE.

Бірнеше пайдаланушылар жиі тіркелетін серверде тұрақты қызмет көрсету жоспарына жұмыс атқаратын қызметтерді қарау және операциялық жүйені бастапқыда орнату кезінде орнатылмаған немесе аталған компьютерде орнатылған өнімдермен жеткізілмейтін қызметтерді өшіру немесе жою барысын енгізу. Бұл үшін әрбір серверде жұмыс атқаратынның бәріне түгендеу

жұмысын тұрақты жүргізу қажет.

Мұндай түгендеудің нәтижесінде қолжеткізілген ақпарат басқа мақсаттар үшін де – мысалы, апаттық жағдайдан кейін серверді қайта орнату кезінде қолданылуы мүмкін.

1.7 Корпоративтік қауіпсіздік саясатының үлгісі

Қауіпсіздік саясатының мақсаты мекеменің телекоммуникациялық ресурстарын және компьютерлерін тағайындалуы бойынша қызметкерлердің, тәуелсіз мердігерлердің және басқа пайдаланушылардың кепілді пайдалануы болып табылады. Компьютерлердің барлық пайдаланушылары компьютерлік ресурстарды заң және этика нормативтерін сақтай отырып, білікті әрі тиімді қолдануы тиіс.

Компанияның компьютерлік және телекоммуникациялық ресурстарының, қызметтерінің барлық пайдаланушылары, өздерінің қайда болғанына қарамастан қабылданған саясатты және оның ережелерін, барлық пайдаланушыларға қатысты саясат шарттарын сақтауы тиіс. Саясаттың бұл ережелері сақталмаған жағдайда, тіпті жұмыстан босату және/немесе қылмыстық іс қозғауға дейін қатаң жазаға тартылады. Қажеттілігіне қарай қабылданған саясатты мезгіл-мезгіл ауыстыруға және қайта қарастыруға болады.

Мекеме басшылығы саясаттың сақталуына кепілдік беру үшін компьютерлік жүйенің барлық аспектілерін, қызметкерлер поштасын тексере алады, себебі оған өкілеттігі бар. Қызметкерлер өз жұмысын тиімді орындауы үшін оларға компьютерлер және бюджет беріледі.

Компьютерлік және телекоммуникациялық жүйелер жеке қажеттілік үшін емес тек жұмыс атқару мақсатында ғана қолданылады, себебі олар компанияға тиесілі Сондықтан қызметкерлердің Компанияға тиесілі компьютерлердің және телекоммуникациялық ресурстардың көмегімен жасаған, жөнелткен немесе қабылдаған ақпараттары құпия болып табылмайды.

Компьютер пайдаланушылары барлық компьютерлік және телекоммуникациялық ресурстар мен қызметтерге қатысты төменде көрсетілген сақтандыру шараларын басшылыққа алуы тиіс. Компьютерлік және телекоммуникациялық ресурстар мен қызметтер мыналарды қамтиды (бірақ шектелмейді): хост-компьютерлер, файл серверлері, жұмыс стансалары, автономдық компьютерлер, ұялы компьютерлер, бағдарламалық қамтамасыз етулер, сонымен бірге Компанияның компьютерлк құрылғыларына тікелей немесе жанама қатынас жасайтын ішкі және сыртқы байланыс желілері (интернет, коммерциялық интерактивті қызметтер және электронды пошта жүйелері).

Барлық пайдаланушылар бүкіл бағдарламалық рұқсатнамалардың шарттарын, авторлық құқықты және зияткерлік меншікке қатысты заңды сақтауға міндетті, басқаша айтқанда зардап әкеледі.

Электронды поштаның немесе электронды байланыстың басқа да құралдарының көмегімен құрамында жалған, жалықтыратын, әдепсіз, жала

жабатын, тіл тигізетін, қауіп төндіретін немесе заңға қарсы сөздері бар материалдарды қайта жөнелтуге, сонымен қатар оларды Компанияның компьютерлерінде бейнелеуге және сақтауға тыйым салынады. Егер қызметкерлердің бірі осындай материалды байқаған болса немесе қабылдаса, бұл жөнінде өзінің басшысына тез арада баяндауға міндетті.

Кәсіпорын басшылығы компьютерде жасалғанның бәрін, оның ішінде электронды поштадағы хабарламаларды және басқа да электронды құжаттарды сараптай алатындығын білу қажет. Сонымен қатар Компанияның желісіне және компьютерлеріне жүйелік әкімгердің рұқсатынсыз бағдарламалық өнімдерді орнатуға тыйым салынады.

Қызметкерлер жөнелтушінің рұқсатынсыз өзге тұлғаларға немесе мекемелерге аталған ақпаратты тарата, жөнелте алмайды.

Электрондық поштада компания заңгерінен немесе оның қорғаушысынан алынатын хабарламаның әр бетінің колонтитулында «қорғаушы құқымен қорғалған/рұқсатсыз жіберілмесін» деген жазба болуы тиіс. Сонымен қатар пайдаланушыларға, өзге пайдаланушыларға тиесілі файлдарды өзгертуге және көшіруге файл иелерінің рұқсаты болмаса да рұқсат беріледі.

Коммерциялық немесе жеке басына қатысты жарнамаларды, қолдаухаттарды, жарнамалық материалдарды, сондай ақ бүлдіру бағдарламаларын (вирустарды және/немесе өздігінен туындайтын кодты), саяси материалдарды және пайдаланушының өкілеттігі жоқ немесе жеке қажеттілікке тағайындалған жұмысқа қатысты кез келген қандай да бір ақпаратты Компанияның компьютерлік және телекоммуникациялық ресурстарына кіруге алдын ала жазбаша рұқсатсыз қолдануға тыйым салынады.

Пайдаланушы жүйеге кіруге арналған өз құпиясөздерінің сақталуына жауапты. Оған өзінің жеке құпиясөздерін басқа тұлғаларға беруіне немесе желіде сақтауына, басып шығаруына болмайды. Егер кімді кім олардың құпиясөздерінің көмегімен қандай да бір іс-әрекет жасаған болса, онда оған тек пайдаланушылар ғана жауапкершілік алады.

Тіпті, пайдаланушының желі арқылы басқа компьютерлік жүйелерге кіруге рұқсаты болғанымен, бұл оларға жүйе операторларының арнайы рұқсатынсыз осы жүйелерді қолдану және оған қосылу құқықын

1.2 Суретте кәсіпорын қауіпсіздігінің бірегейлендірілген жүйесі көрсетілген.

1.2- сурет. Кәсіпорын қауіпсіздігінің бірегейлендірілген жүйесі

2 CiscoPIX брандмауэрлерінің аппараттық құралдары және бағдарламалық қамтамасыз етулері

Құрылыс өнеркәсібінде желіаралық экран дегеніміз қызуға берік материалдан жасалған өртке қарсы қалқа, бұл өрт кезінде оттың бір жайдан өзге жайға өтуіне жол бермейді.

Компьютерлік желілерде брандмауэр(firewall) - екі немесе одан жоғары тордың өзара әрекеттесуін бақылайтын компьютер немесе компьютерлер тобы. Егер жеке компьютер брандмауэр болып саналса, оның қызметін желі шекарасына орнатылған арнайы құрылғы орындай алады, бұл алдын ала белгіленген өлшемдерді негізге ала отырып, деректер ағынының өтуін бұғаттайды немесе рұқсат береді. Әдетте брандмауэр желінің шекаралық қауіпсіздігі саясатының бөлігі болып табылады, бұл өз кезегінде қауіпсіздіктің желілік саясатының құрамына кіреді.

Қауіпсіздіктің барынша күрделі сұлбасында брандмауэр жеке компьютерді алға тартады, бірақ қауіпсіздіктің брандмауэрлік жүйесі жалпы компьютерлер тобын қамтиды, олар ішкі желіде немесе Интернетте жұмыс атқарған сәтте қауіпсіздікті қамтамасыз етеді. Аталған жағдайда брандмауэр желілік қауіпсіздік жүйесін жүзеге асырудың бөлігі болып табылады.

2.1 Cisco Secure Private Internet Exchange (PIX) Firewall желіаралық экран

Cisco Secure Private Internet Exchange (PIX) Firewall желіаралық экран корпоративтік желілерді өз дәрежесінде қорғауды жүзеге асырады, бұл ертеректе қолжетімсіз болған және қолданылуы қарапайым. PIXFirewall желіні сыртқы әлемнен жасырады, осылайша ішкі желінің қауіпсіздігін қамтамасыз

етеді.

Әрбір желілік пакетті орталық процессорды едәуір жүктеу арқылы жеке өңдеу жұмысын орындайтын, әдеттегі proxy-серверлерден айырмашылығы, PIXFirewall айтарлықтай жоғары өнімділікті қамтамасыз ететін, UNIX тәрізді нақты уақыттың операциялық емес жүйесін қолданады. PIX Firewall барндмауэрдің негізгі артықшылығы бұл қорғаныстың арнайы сұлбасы. Бұл сұлба бейімделме қауіпсіздіктің тәртібін (adaptive security algorithm - ASA) қолдануға негізделеді. Бұл тәртіп пайдаланушылардың мекен-жайын қаскүнемдерден тиімді жасырады.

Осы бейімделме тәртібі қосылу деңгейінде қауіпсіздікті қамтамасыз етеді, бұл ретте жөнелтушінің және қабылдаушының мекен-жайы туралы ақпаратқа, TCP пакеттері нөмірлерінің кезектілігіне, TCP қосымша жалауларының және порттарының нөмірлеріне жүргізілетін бақылауды қолданады. Аталған ақпарат арнайы кестеде сақталады және бұл деректер барлық кіріс пакеттері өтетін жазбаларға сәйкестігі тексеріледі. PIX арқылы кіру мүмкіндігі қосылу бірегейлендіруден сәтті өткен кезде ғана беріледі.

Бұл әдіс ішкі пайдаланушылар және авторизацияланған ішкі пайдаланушылар үшін айқын кіру мүмкіндігін қамтамасыз етеді, бұл ретте рұқсат етілмеген кіру мүмкіндігінен ішкі желіні толығымен қорғайды.

Кесіп өтетін делдалдың (Cut-Through Proxy) технологиясын пайдаланудың нәтижесінде Cisco PIX Firewall брандмауэрі UNIX ОЖ негізінде экрандармен-делдалдармен салыстырғанда өнімділікте едәуір артықшылықты қамтамасыз етеді. PIX әдеттегі proxy-серверлер тәрізді қосымшалар деңгейінде белгіленген қосылуларды бақылайды. Қабылданған қауіпсіздік ережелеріне сәйкес пайдаланушылар кіру мүмкіндігінің авторизациясынан сәтті өткен соң PIX сессия деңгейінде абоненттер арасында деректер ағынына бақылау қамтамасыз етіледі. Мұндай технология PIX желіаралық экранға әдеттегі proxy-экрандарға қарағанда едәуір жылдам жұмыс атқаруға мүмкіндік береді.

Өнімділікті арттырумен қатар, нақты уақыттың мамандандырылған кіріктірме операциялық жүйесін қолдану қауіпсіздік деңгейін арттыруды қамтамасыз етеді. Бастапқы мәтін кеңінен қолжетімді UNIX тән операциялық жүйелерден айырмашылығы Cisco PIX – қауіпсіздікті қамтамасыз ету тапсырмаларын шешу үшін арнайы құрылған, компанияның жекеменшік зерттеуі. PIX Firewal желіаралық экран тұрақтылықты арттыру үшін «отты резервтеу» тәртібінде қосарланған кескіндемеде орнату мүмкіндігін алдын ала қарастырады, соның есебінен тоқтап қалу мүмкіндігінің бірыңғай нүктесінің болуы желіде шығарылады. Егер екі PIX-экран қатар тәртіпте жұмыс атқарып, олардың бірі істен шығып қалса, онда екіншісі айқын тәртіпте қауіпсіздікті қамтамасыз етудің барлық функцияларын «қоса қамтып» орындайды.

2.1.1 Жоғары өнімділік

Cisco Secure PIX Firewall желіаралық экранның өнімділігі жоғары және 500 мыңнан аса бірмезгілдік байланыстарды қолдайды, демек өнімділікті төмендетусіз жүздеген және мыңдаған пайдаланушыларға қолдау көрсетеді.

Толығымен жүктелген PIX Firewall 1,0 Гбит/с дейін, яғни UNIX ОЖ немесе Microsoft Windows NT ОЖ негізінде кез келген желіаралық экранға қарағанда едәуір жоғары өткізу қабілетін қамтамасыз ете алады.

2.1.2 Қолдану қарапайымдылығы

Cisco Secure PIX Firewall брандмауэр пайдаланудың және сүйемелдеудің төмен құнын қамтамасыз етеді. Тіпті арнайы мамандығы жоқ пайдаланушылар да PIXDeviceManager (PDM) қарапайым графикалық қабықшаның арқасында оңай және жылдам баптап күйге келтіреді. Осы қабықшаға кіру мүмкіндігі әдеттегі web-браузердің көмегімен жүзеге асырылады. Брандмауэрді бастапқы баптап күйге келтіру үшін қажет командалардың негізгі жиынтығын қолдайтын және PIX кіріктірілген, http-серверді қолданатын PDM қосымша болып саналады. Сонымен бірге PDM айтарлықтай кез келген компьютерден PIXFirewall баптап күйге келтіруге мүмкіндік береді, пайдаланушы кескіндеме жасау кезінде «бұзып кіруден» қорғану құрылғысына SSL хаттамасын қолдана алады.

2.1.3 IP-мекен-жайлардың жетіспеу мәселелерін шешу

Cisco Secure PIX Firewall желіішілік экран IP-желілерін кеңейту және өзгерту барысында мекен-жайлардың жетіспеу мәселелерінен арылуға мүмкіндік береді. Network Address Translation (NAT) желілік мекен-жайларды трансляциялау технологиясы қолда бар мекен-жайлар тәрізді резервті мекен-жайлар кеңістігін де жекеменшік желісінде қолдануға мүмкіндік береді.

Қазіргі таңда Firewall пайдаланушыларына Cisco Secure PIX Firewall аппаратты-бағдарламалық желіаралық экрандардың келесідей - PIX 501, 506E, 515E, 525 және 535 моделдері ұсынылады. 2.1 Кестеде салыстырмалы сипаттамалары келтірілген.

2.1 Кесте - CiscoPIXFirewall салыстырмалы сипаттамалары

	Pix 501	Pix 506E	Pix 515	Pix 525	Pix 535
Өнімділік, Мбит/сек	60	100	190	330	1667
Қосылулардың ең жоғары саны	7500	25000	130000	280000	500000
Бірмезгілде қолдау көрсетілетін сессиялардың көлемі	19500	53000	176000	625000	1000000
Қолдау көрсетілетін физикалық интерфейстер	1x10/100	2x10/100	6x10/100	8x10/100	10x10/100
Қолдау көрсетілетін логикалық интерфейстер VLAN8o2.1q	0	0	8	10	24

VPN өнімділігі (Triple DES / AES-128), Мбит/сек	3/4,5	16/30	135/130	145/135	425/495
VPN-туннелдердің ең жоғары саны	10	25	2000	2000	2000

2.1.4 Негізгі мүмкіндіктер

Ішкі желі ресурстарының қауіпсіздігін қосылу деңгейінде рұқсатсыз кіру мүмкіндігінен қорғаудың қатаң жүйесі қамтамасыз етеді.

Cut Through Proxy технологиясы Terminal Access Controller Access Control System (TACACS немесе Remote Access Dial-In User Service (RADIUS) тәрізді қауіпсіздік хаттамаларының негізінде кіріс және шығыс қосылуларды, қорғаныстың кеңейтілген ережелерін қолдану үшін алтауға дейін желілік интерфейстерді бақылауға мүмкіндік береді.

SecurityManager әкімгерінің графикалық интерфейсі бірыңғай консолімен бірге PIXFirewall 100 желіаралық экранға дейін баптау күйге келтіру үшін тағайындалған.

Мекен-жайлардың динамикалық және статикалық трансляциясы. SNMP желілік басқару хаттамасына қолдау көрсету.

Жүйелік оқиғалардың (syslog) жұрналын жүргізуді қолдану арқылы есептік ақпарат.

WorldWideWeb (WWW), FileTransferProtocol (FTP), Telnet, Archie, Gopher тәрізді барлық негізгі желілік қызметтерге айқын қолдау көрсету.

Progressive Networks RealAudio & ReadVideo, Xing StreamWorks, White Pines CU-SeeMe, Vocal Tec Internet Phone, VDOnet VDOLive, Microsoft NetShow және VXtreme Web Theater қоса, мультимедиа қосымшаларына қолдау көрсету.

Microsoft Networking сервер - клиент, Oracle SQL Net сервер – клиент өзара әрекеттеріне қолдау көрсету.

Нақты уақыттың қауіпсіз кіріктірме операциялық жүйе.

Жұмыс стансаларында және бағытаушыларда бағдарламалық қамтамасыз етуді жаңарту қажеттілігі жоқ.

Ішкі желінің тіркелген пайдаланушылары үшін Интернет желісінің ресурстарына толық кіру мүмкіндігі.

Cisco IOS™ басқаруымен жұмыс атқаратын бағыттаушылармен үйлесімділігі.

Microsoft NetMeeting, Intel Internet Video Phone және White Pine Meeting Point қоса H.323 хаттамасы бойынша бейнеконференцияға қолдау көрсету.

Бағдарламалық және аппараттық жиынтықтың мүмкіндік берілген бірнеше нұсқасы.

Орталықтандырып басқару құралдары.

Пейджерге немесе электрондық поштаға маңызды оқиғалар туралы хабарлау. Ethernet, Fast Ethernet, Token Ring және FDDI интерфейстеріне қолдау көрсету.

IPSec стандартты технологияны қолдану арқылы виртуалды жекеменшік желілерге (Virtual Private Network) қолдау көрсету.

Жоғары өнімділік.

Cisco компаниясының өзге шешімдерімен, мысалы, Cisco Secure ACS пайдаланушыларының бірегейлендіру серверімен біріктіру.

2.2 Брандмауэр үлгілері

Брандмауэр технологиясы компьютерлік индустрияда қауіпсіздікті қамтамасыз ету қажеттілігі туындаған соң, бірден дами бастады. Бірінші брандмауэр пакеттер сараптамасына негізделген, өтетін деректер ағынын сүзетін әдеттегі компьютер болатын.

Бұл деректер ағынын сараптау мақсатымен жүргізілген салыстырмалы қарапайым курс болды. Деректерді сүзгіден өткізу деректер қайдан келгені және олар қайда түсуі тиіс туралы ақпаратқа ғана негізделген. Сонан соң деректердің осы пакеті алдын ала белгіленген ережелердің көмегімен бұғатталды немесе өтуіне рұқсат алған. Егер байланыс бойынша өтетін деректер ағынының түрі әйгілі болып, стандартты хаттаманы меңзейтін болса, онда деректердің сүзілуін орындауға болады. Бұл стандартизациялау қажеттілігін көрсететін мысалдардың бірі.

Деректер стандартты нұсқада (TCP/IP, IPX, AppleTalk, DECNET тәрізді) таратылған жағдайда, бұл тарату қатаң белгіленген қағидалар негізінде құрылады, осылайша деректер жөнелтушімен тәрізді қабылдаушымен де қабылдануы және түсіндірілуі мүмкін. Белгіленген стандарттарға негізделген байланыстарға деректерді тарату, деректер ағынын сүзгілеуді орындайтын құрылғыларды желілер деректерінде жақсы қолдануға мүмкіндік береді.

Аталған мысалда деректер ағынын сүзгілеу брандмауэрлерді қолдану бағыттарының бірін ғана көрсетеді. Брандмауэрлер үш санатқа бөлінеді:

- пакеттердің сүзгілері (packetfilter);
- прокси-сүзгілер (proxyfilter);
- деректердің жай-күйін ескеретін пакеттердің сүзгілері (stateful packet filter). Брандмауэр санаттарының дерегінен ішінен әрқайсысын толығымен қарастырамыз.

2.2.1 Пакеттердің сүзгілері

Пакеттердің сүзгілері – бұл TCP/IP хаттамалары ағынының желілік (Internet) немесе тасымалдау деңгейінде TCP/IP пакеттерін сүзгілейтін әдеттегі желіаралық экран. Егер ақпараттар TCP/IP хаттамаларының (немесе хаттамалардың кез келген басқа стандартты ағынында) стандартты ағынында шоғырланатын желі бойынша таратылатын болса, онда олар сүзгілеу ұшырауы мүмкін. Себебі құрамында ақпараты бар (мысалы, аталған пакетті жөнелтушінің IP-мекен-жайы, қабылдаушының IP-мекен-жайы және порт) жазықтардың пакетте орналасуы белгілі, осы деректердің негізінде пакеттер

сүзгіден өтеді. Сонымен қатар пакеттер сүзгілерімен тек пакеттер тақырыптарының статикалық ақпараты ғана сарапталатынын есте сақтау қажет.

Брандмауэрдің жұмыс атқаруы жеткілікті ережелер пакеттер жөнелтушілердің мекен-жайын және пакеттер қабылдаушылардың мекен-жайын қамтитын кейбір өлшемдердің негізінде құрылады. 2.1-суретте көрсетілгендей пакеттердің сүзгілері кезекті ақпараттарды негізге алып, деректердің өтуіне рұқсат беруі немесе бұғаттауы мүмкін:

- жөнелтушінің IP-мекен-жайы;
- қабылдаушының IP-мекен-жайы;
- хаттама;
- жөнелтушінің порты;
- қабылдаушының порты.

Cisco бағыттаушысы пакеттер сүзгілеуінің мысалы бола алады, деректер ағынын сүзгіден өткізу, ережелерді ретке келтіру кіру мүмкіндігін басқарудың арнайы тізімінің көмегімен (Access Control List - ACL) жүзеге асырылады.

Осы бағыттаушының мақсатымен жете зерттелген Cisco IOS бағдарламалық қамтамасыз ету кіру мүмкіндігін басқарудың тізімін құрастыруға, сондай ақ пакеттерге негізделген деректердің сүзілуін орындауға ықпал етеді.

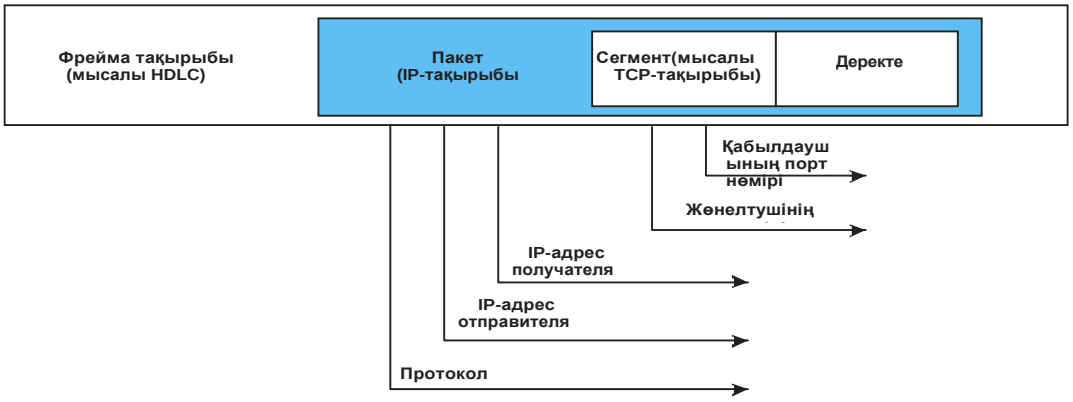
Сүзудің пакеттері динамикалық өзгеретін ақпаратты сақтау мүмкіндігін ешбір меңгере алмайтындығын атап өткен жөн. Пакеттер сүзгісі ACL-тізімінің негізінде деректер пакетін алған сәтте, аталған пакетті бұғаттау немесе оған рұқсат беру туралы шешім қабылданады. Пакет жеткілікті дәрежеде өңделе салысымен, деректер үнемі үнсіз жоғалады. Сонан соң сүзгіге деректердің кезекті пакеті түседі және өңделеді, осылайша өңдеудің бүкіл процесі қайталанады.

Брандмауэрлердің осы түрінің кейбір кемшіліктерін келтіреміз.

Еркін пакеттердегі деректер ACL-тізіміндегі деректермен сәйкес болса, онда олар сүзгі арқылы өтуге келуі мүмкін.

Пакеттер фрагменттеудің көмегімен сүзгіні басып озуы мүмкін. Кіру мүмкіндігін басқарудың сапалы және толық тізімінде ақпаратты құру, қолдану және жаңарту өте күрделі тапсырма болып табылады. Кейбір қызметтер сүзгіден өте алмайды (әдетте, әрбір қосымша үшін порт нөмірі белгілі). Пакеттерді кіру мүмкіндігінің басқару тізімі арқылы тексеру 2.1 суретте көрсетілген.

TCP/IP пакетінің мысалы



2.1 Сурет – Кіру мүмкіндігінің басқару тізімі арқылы пакеттерді тексеру

2.2.2 Прокси-сүзгілер

Желіаралық экрандардың қызметтерін орындайтын және жоғарыда қарастырылған пакеттер сүзгілеріне қарағанда, пакеттерді ашық жүйелердің өзара әрекеттесу моделінің (Open System Interconnection - OSI), әдетте, OSI моделінің жеті деңгейлі 4 деңгейі)) барынша жоғары дәрежесінде тексеретін құрылғылар прокси-сүзгілер деп аталады. Прокси-сүзгілердің осы ерекшелігін ескере отырып, олар қорғаныстың жоғары деңгейін ұсынады деп қорытынды жасауға болады, бірақ бұл бүкіл жүйенің өнімділігіне кері әсер етеді. Бұл құрылғылар пайдаланушы туралы маңызды деректерді соңғысының аралық сервері арқылы қосылуының көмегімен жасырады. Пайдаланушы сәйкестендірудің және авторизациялаудың белгіленген рет-жосықтары арқылы өту және сеанс ашу жолымен желіге кіру мүмкіндігін алады. Бұл пайдаланушының сыртқы қорғалмаған аймақта шлюз ретінде қолданатын арнайы қосымшаның (прокси-сервердің) көмегімен сыртқы серверлермен қосыла алатындығын білдіреді.

Брандмауэр жұмысының мүмкіндік берілген кестесінің бірі ішкі (сеніп тапсырылған) аймақтың пайдаланушыларына ең алдымен, тікелей брандмауэрмен (прокси-сервер сеанс жолданымының рөлін атқарады) өзара байланыс сеансын бастапқыдан жүктеуді талап етумен тұжырымдалады.

Сонан соң пайдаланушы пайдаланушылық идентификатды және құпиясөзді білу талап етілген, сәйкестендіруден өтуі тиіс. Пайдаланушы сәйкестендіруден сәтті өткен соң сыртқы интернетке кіру мүмкіндігін алады.

Осы тәрізді прокси-брандмауэрді қолданып, қосылуды құру кезінде өзара байланыстың екі түрлі сеансы құрылады (біріншісі, пайдаланушыдан брандмауэрге бағытталған, және екіншісі, брандмауэрден пайдаланушы сұрап отырған мекен-жайға бағытталған).

Брандмауэр жұмысының басқа кестесімен сеніп тапсырылған аймақта орын алған пайдаланушы, сыртқы аймақта орналасқан, сұраныс жасалған мекен-жай арқылы өзара байланыстың тікелей сеансын орнату кестесі ұсынылады. Анығырақ айтар болсақ, пайдаланушыда өзара байланыс тікелей орнатылғандай әсер қалдырады. Процесс барысында прокси-брандмауэр үнемі

пайдаланушының қосылуларын жолдан қағып әкетеді және кейбір ақпараттарды негізге ала отырып (мысалы, жөнелтушінің IP-мекен-жайында), сәйкестендіру жүргізеді және екі сирек кездесетін қосылуды құрады (біріншісі, пайдаланушыдан брандмауэрге бағытталған, және екіншісі, брандмауэрден пайдаланушы сұрап отырған мекен-жайға бағытталған).

Прокси-брандмауэрді қолданудың аталған тәсілі пайдаланушының мақсатымен сәйкес барынша айқын ұсынылады.

Прокси-брандмауэрді қолдану барысында кезекті түйінді мәселелер туындауы мүмкін.

Прокси-брандмауэрдің өзі осал жерді білдіреді, себебі оны бұзу кезінде компьютерлік бұзақы бүтін ішкі осал жерге кіру мүмкіндігін алады.

Брандмауэрге жаңа ортаны қосу қарапайым тапсырма болмауы мүмкін.

Жоғары жүктеме кезінже прокси-брандмауэрдің өнімділігі төмендейді.

Әдетте, прокси-брандмауэрлер жалпы тағайындалған мамандандырылмаған операциялық тәртіптердің негізінде құрылады, сондықтан брандмауэр кейбір қызметтерді ұйымдастыру арқылы орындайды.

2.2.3 Жай-күйді ескеретін, пакеттердің сүзгілері

Мұнда брандмауэрлердің түрлері әдеттегі пакеттер сүзгілерінің және прокси-сүзгілерінің ең үздік технологияларымен үйлеседі. Деректердің жай-күйін ескеретін пакеттер сүзгісі деректердің әрбір өңделген пакеті туралы ақпаратты сақтайды. IP-қосылуларды сыртқы немесе ішкі тораппен құру кезінде әр жолы бұл қосылулар туралы ақпарат деректер ағынының жай-күйін бақылаудың арнайы кестесінде сақталады (stateful session flow table). Cisco PIX брандмауэрінде пакеттерді сүзудің тап осы әдісі қолданылады.

Деректер ағынының жай-күйін бақылау кестесінде бастамашылар және қосылу нысаналары туралы ақпарат, порттар нөмірлері, өзара байланыстың қатаң белгіленген сеанстарына сәйкес келетін әрбір TCP/UDP-қосылулардың қосымша көрсеткіштері және TCP хаттамасының қызметтік ақпараты қамтылған. Себебі өзара байланыс сеансының бастамашысы ретінде брандмауэр ұсынылады, осылайша, клиенттің аталған тораппен өзара байланысының осал жері брандмауэер арқылы орын алады, сондықтан нәтиже ретінде кіріс және шығыс пакеттері үнемі жай-күйді бақылау кестесінде тексеруден өтеді.

Деректер брандмауэр арқылы егер олардың көрсеткіштері жай-күйді бақылау кестесінде сипатталған, қандай да бір қосылуларға сәйкес келгенде ғана өтуі мүмкін.

Аталған үлгідегі брандмауэрлерді қолдану ерекшеліктері төменде көрсетілген.

Әрбір пакетті жеке-жеке сараптау орындалады, оның барысында ол рұқсат етілген қосылулар туралы деректермен салыстырылады.

Пакеттер сүзгісімен немесе прокси-сүзгімен салыстырғанда жоғары өткізу қабілеті қамтамасыз етіледі.

Барлық қосылулар немесе транзакциялар барысында ешбір қосылуға

мүмкіндік болмаған деректер кестеге жазылады. Бұл кесте пакеттің қоркөзін анықтаудың бастапқы кезеңінде қолданылады.

2.2.4 PIX брандмауэрлердің логикасы және түрлері

Cisco Secure PIX Firewall желіаралық экраны Cisco қауіпсіздігін қамтамасыз етуді ұйымдастырудың негізгі элементін алға тартады. Аталған брандмауэр – бұл басқа желіаралық экрандармен салыстырғанда қауіпсіздіктің барынша жоғары деңгейін қамтамасыз ететін, бағдарламалық немесе ерекше назар аударылатын аппараттық сервер.

Cisco PIX брандмауэрі кезекті ерекшеліктермен сипатталады.

Нақты уақытта жұмыс атқаратын сенімді, кіріктірмелі операциялық орта. Деректердің әрбір пакетін өңдеген, әдеттегі прокси-сүзгілерден айырмашылығы, PIX брандмауэр жалпы мекеменің қауіпсіздік деңгейін арттыратын, нақты уақытта жұмыс атқаратын сенімді, кіріктірмелі ортаны қолданады. PIX патенттелген операциялық орта жақсы қорғалған, және онда үнемі жалпы тағайындалған операциялық жүйелерге тән ақаулар болмайды.

Қауіпсіздіктің бейімделген тәртібі (Adaptive Security Algorithm - ASA). Cisco PIX брандмауэрінде осы механизмнің көмегімен қосылуларды тексерудің көрсеткіштерін қатарластыру жүзеге асырылады. Пакеттерді қатарластырып сүзгіден өткізу сараптаудың қауіпсіз әдісі ретінде ұсынылады, бұл деректер пакеттері туралы маңызды ақпаратты кестеге орналастырады.

Тесіп өтетін прокси-сүзгі (cut-through proxy). Ішкі және сыртқы пайдаланушыларды сәйкестендіру әдісі тұжырымға жоғары емес жүктемені қамтамасыз етеді. Осылайша, әдеттегі прокси-сүзгілермен салыстырғанда жоғары өткізу қабілетіне қолжеткізіледі.

Бас тарту/отты резервтеу (stateful failover/hot standby) жағдайында жай-күйді толығымен қалпына келтіру. Cisco PIX брандмауэрлері тұрақсыздықтың жалпы деңгейін арттыру және осал жердің шамадан тыс топологиясын қамтамасыз ету мақсатында бірмезгілде 2 брандмауэрдің жұмысына қолдау көрсетеді.

PIX брандмауэрінің «жүрегі» патенттелген операциялық мекеменің құрамына кіретін ASA тәртібін алға тартады, бұл олардың жай-күйін ескеру арқылы пакеттердің тексерілуін қамтамасыз етеді, өзара байланыс сеансына қолдау көрсетеді, сонымен бірге брандмауэрмен бақыланатын, тор шекараларын қорғайды. Осы тәртіптің көмегімен қабылдаушы және жөнелтуші арасында өзара байланыс сеансы құрылады. PIX брандмауэрі біржақты қосылулар түзеуге (ішкі тораптан сыртқа) мүмкіндік береді, бұл ретте әрбір сыртқы қосылуды және әрбір қосымшаны баптап күйге келтіру ешқандай талап етілмейді.

Деректердің жай-күйін ескеру арқылы пакеттерді сүзгіден өткізу деректер пакеттерін сараптаудың қауіпсіз әдісімен жүзеге асырылады, бұл ретте пакеттер туралы маңызды ақпарат арнайы кестеге орналастырылады.

Әр ретте PIX брандмауэрінің көмегімен сыртқы немесе ішкі тораппен қосылу орнатылады, бұл қосылулар жөніндегі ақпарат деректер ағынының жай-күйін бақылау кестесінде сақталады.

Өзара байланыстың әрбір сеансының мақсаты қосылулар туралы ақпарат кестеде сақталған ақпаратқа сәйкес келуі тиіс. Осылайша, деректер ағынының жай-күйін ескеретін пакеттердің сүзгілерін, аталған технологияны қолдана отырып, пакеттердің емес, қосылулардың өзіне сараптама жүргізеді. Сондықтан аталған әдісті қолдану барысында қауіпсіздікті қамтамасыз етудің барынша жоғары деңгейіне қолжеткізіледі және нәтижесінде мекеменің бұзылу ықтималдығы барынша төмен болады.

ASA тәртібін қолдану арқылы PIX брандмауэрі деректер жай-күйін ескерумен пакеттерді сүзгіден өткізу кезінде кезекті операциялардың орындалуын қамтамасыз етеді.

Әрбір TCP-қосылулары үшін IP-мекен-жайлары және порттар тәрізді өзара байланыс сеансының бірегейлендірілген көрсеткіштерін алу.

Деректер ағынының жай-күйін бақылау кестесіне деректерді сақтау және сеансы объектісін құру.

Кіріс және шығыс пакеттерін қосылулар кестесінде сақталған сеанс объектілерімен салыстыру.

PIX брандмауэрі арқылы деректер пакеттері тек, егер тиісті қосылулар кестеде орын алған жағдайда ғана өтуі мүмкін және одан қосылуға рұқсат қабылданады.

Қосылу аяқталған соң қосылу және сеанс объектісі (объектілері) туралы ақпарат жойылады.

PIX брандмауэрдің тесіп өтетін прокси-сүзгісі пайдаланушының және оның TCP- немесе UDP-қосымшаларына кіру рұқсатының немесе оған тыйым салуының шынайылығын «айқын» тексерудің патенттелген технологиясында қолданылады.

Кіріс және шығыс қосылулардың осы тәрізді бірегейлендірілуін пайдаланушы бойынша бірегейлендіру (user-based identification) деп аталады. OSI моделінің қолданбалы деңгейінде әрбір пакетті сараптайтын қарапайым прокси-сүзгіден айырмашылығы, Cisco PIX брандмауэрі қолданбалы деңгейде ең алдымен, пайдаланушыға тексеру жүргізеді. Әрі қарай, өңдеу жылдамдығын едәуір арттыру мақсатында Cisco PIX брандмауэрі OSI моделінің ең төмен деңгейінде (3 деңгей) тексеру жүргізеді. Брандмауэр ерекшеліктерінің деректері пайдаланушының бірегейлендірілген деректері негізінде қауіпсіздік саясатын құруға мүмкіндік береді.

Cisco PIX брандмауэрін қолдану арқылы қосылуларды орнатудың алдында сәйкестендірулер пайдаланушының тегін және құпиясөзін қолданумен сәйкестендіруден өтуі тиіс. Пайдаланушының тегі және құпиясөзі туралы деректер HTTP, Telnet немесе FTP хаттамаларының көмегімен таратылуы мүмкін. Деректерді тексеру терминалды кіру мүмкіндігінің бақылаушысына (Terminal Access Controller Access Control System - TACACS) кіруді басқаруды немесе коммутаторлық кіру мүмкіндігі кезінде (Remote Authentication Dial-In User Service - RADIUS) пайдаланушыны қашықтан сәйкестендіру жұмысын ұйымдастыру арқылы жүзеге асырылады. Сонан соң брандмауэр деректер ағынын жолдан қағып әкетеді, осылайша, өзара байланыс сеансының процесіне 2 нүкте арасындағы деректерді жылдам және тұрақты таратуды қамтамасыз

етеді.

PIX брандмауэрлеріндегі тесіп өтетін прокси-сүзгі әдісі сәйкестендіруді, авторизацияны, сонымен бірге CiscoSecure Access ControlServer серверіне кіру мүмкіндігінің жұмысын қамтамасыз етеді.

Бүгінде PIX брандмауэрлердің 5 моделі қолжетімді.

Cisco Secure PIX 506 брандмауэрі. Аталған жиынтықтың ең жас моделі шағын немесе үй кеңсесіне (SOHO-класс) тағайындалған және ондаған Мбит/с өткізу қабілетін құрайды.

Cisco Secure PIX 515E брандмауэрі. Шағын және орта коммерцияда қолдану, сонымен бірге қызметтерді қашықтан басқару мақсатына тағайындалған. Өткізу қабілеті 188 Мбит/с құрайды, сонымен қатар өзара байланыстың 130000 дейінгі сеансына бірмезгілде қызмет көрсетуге мүмкіндік береді.

Cisco Secure PIX 520 брандмауэрі. Ірі мекемелерде қолдану, деректердің қуатты ағынына қызмет көрсету мақсатына тағайындалған, өткізу қабілеті - 120 Мбит/с, бірмезгілде қолдау көрсетілетін қосылулар көлемі - 250000.

Cisco Secure PIX 525 брандмауэрі. Ірі мекемелерде қолдану, сонымен қатар жеткізушілерге желілік қызмет көрсету мақсатына тағайындалған. Өткізу қабілеті 370 Мбит/с құрайды және бірмезгілде өзара байланыстың 280000 дейінгі сеансына қызмет көрсетуге қабілетті.

Cisco Secure PIX 535 брандмауэрі. PIX жиынтығының соңғы және ең қуатты брандмауэрімен ұсынылады. Ірі мекемелерде қолдану, сонымен қатар жеткізушілерге желілік қызмет көрсету мақсатына тағайындалған. Өткізу қабілеті 1 Гбит/с құрайды және өзара байланыстың бірмезгілде қолдау көрсетілетін сеанс көлемі - 500000 дейін.

PIX брандмауэрлерінің түрлі моделдерінде ажырайтын қосылыстардың және басқару элементтерінің орналасуы мен көлемі біркелкі емес. Әрине, брандмауэрлер деректерінде кейбір ұқсас блоктар бар, бірақ конструктивтік шешімдер құрылғылардың түрлі күрделілігімен шартталған, айырмашылықтарға ие.

2.2 Кестеде PIX сериясы брандмауэрлерінің қасиеттері және ерекшеліктері келтірілген

2.2 Кесте - PIX брандмауэрлерінің қасиеттері және ерекшеліктері

Сипаттамалар	Cisco Secure PIX	Cisco Secure PIX 515E	Cisco Secure PIX 520	Cisco Secure PIX 525	Cisco Secure PIX 535
Көлемі (бағанда 1 модуль = 1,75 дюйма)	1	1	3	2	3
Intel Pentium (Mhz) процессорының жиілігі	200	433	350	600	1000

Интерфейстердің ең жоғары көлемі	2	6	6	8	10
Тоқтап қалулардан кейін толық қалпына келтіру мүмкіндігі	жоқ	иә	иә	иә	иә

Cisco PIX Firewall 506 моделі шағын немесе үй кеңсесінде қолдану үшін зерттелді. Локалді басқару мақсатында 10BaseT екі интерфейс және консолдер порты бар. Әрі қарай USB-порт жақындайды, бірақ ол әдетте ешбір қолданылмайды. Сонымен бірге бұл моделде пайдаланушының құрылғы ішіне кіру мүмкіндігі ешқандай қарастырылмаған.

PIX 5о6 брандмауэрінің моделі оперативтік жадтың 32 Мбайтын және 8 Мбайт флэш-жадын құрайды. Бұл моделде жадты кеңейту ешбір қарастырылимаған.

Аталған моделдің алдыңғы панелінде кезекті жарықдиодты индикаторлар бар.

POWER. Брандмауэрдің қуат көзін қосқан сәтте аталған индикатор жанады.

ACT. Белсенділік индикаторы. Бағдарламалық қамтамасыз ету үлгісін құрылғыға жүктеген кезде жанады.

NETWORK. Деректер ең болмаса торлы интерфейстердің біреуі арқылы қабылданған жағдайда, бұл индикатор жанады.

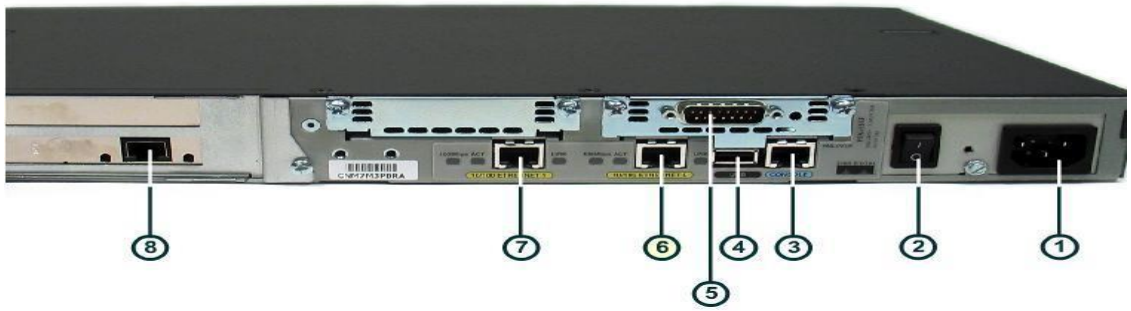
Брандмауэрдің артқы панелінде кезекті индикаторлар орналасқан.

ACT. Желілік белсенділіктің индикаторы.

LINK. Тиісті ажыратқышқа қосылған интернет арқылы деректердің өтуін индукциялау.

Сонымен қатар, PIX 506 брандмауэр DES стандарты бойынша 56-битті, сондай ақ 3DES стандарты бойынша 168-битті шифрлеуге қолдау көрсетеді, бірақ аталған брандмауэр жұмыстағы тоқтап қалулардан кейін толық қалпына келтіру мүмкіндігіне ешбір қолдау жасамайды.

Аталған Cisco PIX Firewall 515 брандмауэрінің артқы панелінде EthernetRJ-45 ажыратқыштары, консолдің порты, резервті брандмауэрді қосуға арналған ажыратқыш, жарықдиодты индикаторлар және қуатты айырғыш орналасқан (2.2 Сурет).



2.2 Сурет - Cisco PIX 515 брандмауэрінің артқы панелі

Ethernet (6, 7, 8) ажыратқыштары. Ethernet1 ажыратқыш ішкі торапты қосу мақсатына тағайындалған. Etherneto ажыратқышына сыртқы интернет қосылады.

(3) консолдің порттары. Терминалды консолді операцияларды орындау нысанасымен брандмауэрге қосу мақсатында қолданылады (мысалы, құрамында HyperTerm қосымшасы жұмыс атқаратын Windows жүйесі терминал ретінде орын алуы мүмкін).

Резервті брандмауэрдің (5) ажыратқышы. Резерв ретінде қолданылатын, PIX брандмауэрімен қосу мақсатында жұмыс атқарады.

CTO Mbps индикаторы. 100BaseTX стандартына сәйкес 100 Мбит/с жылдамдығымен өзара байланыс орнатылғанын растау мақсатында жұмыс атқарады. Егер индикатор ешқандай жанбаса, онда өзара байланыс 200Мбит/с жылдамдықпен орнатылғанын білдіреді.

LINK индикаторы. Ажыратқыш арқылы деректер ағыны өтетіндігін көрсетеді.

FDX индикаторы. Толық дуплексті өзара байланыстың индикаторы, яғни деректер бірмезгілде қабылдануы және таратылуы мүмкін. Егер аталған индикатор ешқандай жанбаса, бұл жартылай дуплексті өзара байланыс орнатылғанын білдіреді.

Қуатты айырғыш. Электр қоректендіруді басқару мақсатына тағайындалған.

Осы брандмауэрге қызмет көрсететін бағдарламалық қамтамасыз етудің 5.2 X нұсқасынан бастап ішкі интерфейсті қосу мақсатымен Ethernet 1 ажыратқышын және сыртқы интерфейсті қосу мақсатымен Ethernet 0 ажыратқышын қолдану ешқандай міндетті емес.

Енді кез келген стандартты немесе қосымша порт ішкі торларды тәрізді сыртқы торларды да қосу мақсатында қолданылуы мүмкін, алайда бағдарламалық қамтамасыз етулердің алдыңғы нұсқаларымен үйлестіру мақсатында, ішкі қосылулар мақсатымен Etherneto порты және сыртқы қосылулар мақсатымен Ethernet1 порты үнсіз келісім бойынша қолданылады.

Консол портының сол жағында орналасқан USB-порт және Ethernet1 портына жоғары орналасқан алынбалы панелі брандмауэрді кезекті кеңейту мақсатына тағайындалған.

PIX 515 брандмауэрдің алдыңғы панелінде әрі қарай тізбектелген индикаторлар орналасқан. Олардың тағайындалуы ACT индикаторын алып тастаумен PIX 606 брандмауэрінде қолданылатын индикаторларға ұқсас.

POWER. Брандмауэрді қуатқа қосқан сәтте аталған индикатор жанады.

ACT. Бұл индикатор егер брандмауэр қосымша брандмауэрсіз қолдылса ғана жанады.

PIX-брандмауэр басқа брандмауэрмен жұмыс атқару мақсатында баптап күйге келтірілген жағдайда аталған индикатор белсенді емес брандмауэрде жанады. ACT тек белсенді құрылғыларды тоқтап қалулар кезінде қалпына

келтіру тәртібіндегі мақсатпен орнатылады.

NETWORK. Бұл индикатор егер деректер ең болмаса бір торлы интерфейстер арқылы қабылданған жағдайда белсенді болады.

PIX 515 брандмауэрдің функционалдық мүмкіндіктерін кеңейту үшін бірмезгілде 6 дейін өзара байланыс интерфейсін орнатуға мүмкіндік беретін, кеңейтудің екі ажыратқышы алдын ала қарастырылған. Аталған брандмауэрге порттардың барынша жоғары көлемін орнату мақсатымен төрт қосымша портын құрайтын бір платаны кеңейтудің жоғарғы ажыратқышына орнату қажет. PIX қосымша порттармен жинақталған соң бағдарламалық қамтамасыз етуді жаңарту қажет. Брандмауэреді сату барысында жеткізу жиынтығына тек үш интерфейсі бар брандмауэрді (PIX- 515E) қолдануға мүмкіндік беретін рұқсат беру кіреді.

Брандмауэрдің қызметін 6 портқа дейін кеңейту барысында жаңа 515E кеңейтуді немесе шексіз кеңейтуді сатып алу талап етіледі. Осы платаға торлы кәбілдерді қосу барысында келесі ережелерді сақтау қажет: олар солдан оңға қарай қосылуы тиіс. Мысалы, Ethernet2 екінші порт сол жақтағы бірінші ажыратқышқа, Ethernet3 порты – екінші ажыратқышқа және т.с.с. қосылуы тиіс. Аталған брандмауэрдің архитектурасымен тек 6 интерфейске ғана қолдау көрсетіледі, сол себептен кеңейтудің қосымша платалары ешқандай іске қосыла алмайды.

Кеңейту ажыратқыштарының көлемі екеуден бастап үшке дейін немесе үштен төртке дейін ұлғайтылуы мүмкін. Егер сіздің брандмауэріңізде артқы панелдің сол жағына қосымша ажыратқыштардағы Ethernet жеке дара порттармен бірге 2 қосымша карта орнатылған болса, онда порттарды жоғарыдан ішкі жағына қарай нөмірлеу қажет (басқаша айтқанда, жоғарғы плата – бұл Ethernet2, ал ішкі – Ethernet3).

PIX брандмауэрін локалді баптап күйге келтіру үшін консолдің порты қолданылады, оның көмегімен брандмауэр компьютерге қосылады. Брандмауэрді консолді компьютерге қосу мақсатында брандмауэрмен бірге жеткізілетін кәбілді қолдану қажет. RJ-45 ажыратқыштармен бірге нөл-модемдік кәбілден басқа жиынтыққа сонымен бірге DB-9 екі ажыратқыш және 225 бір ажыратқыш кіреді (2.3 Сурет).

2.3 Сурет – Төрт порты бар кеңейтуге жаңа платаны қосу

Cisco PIX Firewall 520 брандмауэрлерінің моделінде торлы кәбілдердің ажыратқыштары панелдің бет жағында орналасқан. Сонымен қатар бұл модель 3,5-дюймдік эластикалы дискілер мақсатымен дисководпен жабдықталады. Қуатты айырғыш құрылғының артқы панелінде орналасады. Бұл брандмауэрдің биіктігі 5,21 дюймді құрайды. PIX 520 брандмауэріне қосымша құрылғылар орнату мақсатында қосымша модулдерді орнату үшін орындар алдын ала қарастырылған (бағанда бір модулдің биіктігі 1,75 дюймді құрайды).

Сонымен бірге аталған брандмауэрдің құрылымында кеңейтудің қосымша платаларын орнату мақсатымен төрт ажыратқыш алдын ала қарастырылған. PIX 520 брандмауэрінің төрт бірпортты интерфейстік платаларына торлы кәбілдерді қосу кезінде интерфейстік платалар нөлдік ажыратқышқа (сол жақтағы шеткі бос ажыратқыш) орнатылуы тиіс екенін ескеру қажет.

PIX брандмауэрінің оң жақтағы бірінші сыртқы интерфейстік платасын ішкі торларды қосу мақсатымен қолдану қажет. Бұл сыртқы платаға Ethernet 1 атауы беріледі. Егер Ethernet төрттен аса интерфейсін қолдану қажет болса, онда интерфейстің реттік нөмірі төрт порты платаның орналасуымен анықталады.

525 моделінің PIX брандмауэрі ірі корпоративтік торларды қорғау мақсатымен қуатты, сенімді шешіммен ұсынылады. Аталған модель клиенттердің басым көлемін қорғау мақсатында кешенді тұжырымды қамтамасыз етеді.

525 моделі кезекті хаттамалардың интерфейстік платаларына қолдау көрсетеді: 200-MB, 100-MB және GigabitEthernet. Сонымен қатар деректерді шифрлеудің кезекті стандарттарына да қолдау көрсетіледі: 56-битті кілті бар DES тәртібі және 168-битті кілті бар 3DES тәртібі.

Аталған брандмауэрдің алдыңғы панелінде екі кезекті индикатор орналасқан.

POWER. Құрылғының қуатқа қосылған индикаторы.

ACT. Құрылғы басқа брандмауэрмен бірге белсенді тәртіпте жұмыс атқарған жағдайда, аталған индикатор жанады. Егер құрылғы аталған тәртіпте жұмыс атқарса және негізгі ретінде ұсынылса, онда индикатор жанады, егер құрылғы күту тәртібінде (standby mode) болса, онда индикатор ешқандай да жанбайды.

100BaseTX стандартына сәйкес жұмыс атқаратын әрбір ажыратқыштың жанында, брандмауэрдің артқы панелінде кезекті индикаторлары орналасқан.

100 Mbps. Индикаторлардың деректері брандмауэрдің әрбір портының жанында орналасқан. Егер деректермен алмасу 100 Мбит/с жылдамдықпен жүргізілетін болса, онда индикатор жанады. Егер деректермен алмасу кезінде индикатор ешқандай да жанбаса, бұл өзара байланыс 10 Мбит/с жылдамдықпен жүзеге асырылып отырғанын білдіреді.

ACT. Индикаторлардың деректері брандмауэрдің әрбір портының

жанында орналасқан және желі белсенді екенін білдіреді.

LINK. Бұл индикатор аталған порт арқылы деректермен алмасу орын алып отырғанын білдіреді. Индикаторлардың деректері брандмауэрдің әрбір портының жанында орналасқан.

525 моделінің PIX брандмауэрінің артқы панелінде Ethernet о интерфейсінің RJ- 45 ажыратқышы, Ethernet 1 интерфейсінің RJ-45 ажыратқышы, консолдің RJ-45 ажыратқышы, DB-15 ажыратқышы резервті брандмауэрді және қолданылмайтын USB-портты қосу мақсатымен орналасқан.

Cisco PIX 535 бүгінгі күні PIX сериялы брандмауэрлердің ең қуатты моделі. Бұл өнімділігі жоғары модель көлемді корпоративтік тармақтардың қажеттіліктерін қанағаттандыруға қабілетті және мысалы, тармақты қызметтердің жеткізушілерімен қолданылуы мүмкін.

535 моделі 10-MB, 100- MB және Gigabit Ethernet хаттамаларының интерфейстік платаларына, сонымен бірге деректерді шифрлеудің кезекті стандарттарына да қолдау көрсетеді: 56-битті кілті бар DES тәртібіне және 168-битті кілті бар 3DES тәртібіне.

Брандмауэрдің аталған моделінің алдыңғы панелінде тағайындалуы Cisco PIX Secure 525 брандмауэрінің индикаторына ұқсас екі индикатор, POWER және LED орналасқан.

PIX брандмауэрінің аталған моделінде сегіз ажыратқышпен кеңейту мақсатында қолданылатын үш жеке қақпақ орнатылған.

0 және 1 ажыратқыштары – 64 бит/66 МГц (шина 0).

2 және 3 ажыратқыштары - 64 бит/66 МГц (шина 1).

4 – 8 ажыратқыштары - 32 бит/33 МГц (шина 2).

Аталған брандмауэрді қолдану барысында өнімділіктің және өткізу қабілетінің барынша жоғары деңгейін қамтамасыз ету үшін келесі ережелерді басшылыққа алу қажет.

6 интерфейстік әдістемелерді қолдану үшін шектелген рұқсатнама жеткілікті, бірақ сегіз интерфейсті қолдану мақсатында шексіз рұқсат алу қажет.

PIX-1 GE-66 (66 МГц) плата кез келген жалғағышқа орнатылуы мүмкін, бірақ платаның деректерін 66 МГц жиілігінде жұмыс атқаратын, 64-битті шиналарға қосылған ажыратқыштарға орнатуға нұсқау беріледі. Аталған брандмауэрде барлығы сегізге дейін осындай плата бірмезгілде орнатылуы мүмкін.

Қосымша FE-платалары (33 МГц) кез келген қақпаққа немесе кез келген жалғағышқа орнатылуы мүмкін (32 бит/33 МГц немесе 64 бит/66 МГц). Брандмауэрге сегізге дейін бірпортты немесе екі төрт порттық FE-плата орнатылуы мүмкін.

Жұмыс жиілігі әртүрлі платаны қақпаққа бірмезгілде орнатпаңыз (33 МГц және 66 МГц). Мұндай ұйымдастырудың жұмыс жылдамдығы ең баяу платаның жұмыс жылдамдығымен жеткілікті шектелген.

VPN Accelerator құрылғысын 32 бит/33 МГц қақпаққа орнату қажет. 100BaseTX стандартына сәйкес жұмыс атқаратын әрбір ажыратқыштың жанында, брандмауэрдің артқы панелінде кезекті индикаторлары орналасқан.

100 Mbps. Индикаторлардың деректері брандмауэрдің әрбір портының

жанында орналасқан. Егер деректермен алмасу 100 Мбит/с жылдамдықпен жүргізілетін болса, онда индикатор жанады. Егер деректермен алмасу кезінде индикатор ешқандай да жанбаса, бұл PIX брандмауэрлері моделінің өзара байланысы 10 Мбит/с жылдамдықпен жүзеге асырылып отырғанын білдіреді.

ACT. Индикаторлардың деректері брандмауэрдің әрбір портының жанында орналасқан және желі белсенді екенін білдіреді.

LINK. Бұл индикатор аталған порт арқылы деректермен алмасу орын алып отырғанын білдіреді. Индикаторлардың деректері брандмауэрдің әрбір портының жанында орналасқан.

525 моделінің PIX брандмауэрінің артқы панелінде Ethernet о интерфейсінің RJ- 45 ажыратқышы, Ethernet 1 интерфейсінің RJ-45 ажыратқышы, консолдің RJ-45 ажыратқышы, 25 ажыратқышы резервті брандмауэрді және қолданылмайтын USB-портты қосу мақсатымен орналасқан.

3 Мемлекеттік қазыналық коммуналды кәсіпорынның «Шымкент қаласының құтқару Қызметі» компьютерлік желісінің ақпараттық қауіпсіздік жүйесін жүзеге асыру

3.1 Жобаны жүзеге асыру орны

Қазақстан Республикасы Президентінің 1997 жылғы шілденің 20-күнгі 3358 Жарғысының 44 тармағына, Шымкент қаласы әкімиатының 2001 жылғы қазанның 3-і күнгі 3/229 қаулысына сәйкес, Шымкент қаласының тұрғындарына, олардың өміріне, денсаулығына және қауіпсіздігіне қауіп төнетін төтенше жағдайларға тап болған сәтте қосымша жедел жәрдем көрсету мақсатында Мемлекеттік қазыналық коммуналды кәсіпорынның «Шымкент қаласының құтқару Қызметі» құрылды (3.1 суретте құтқару қызметі көрсетілген).

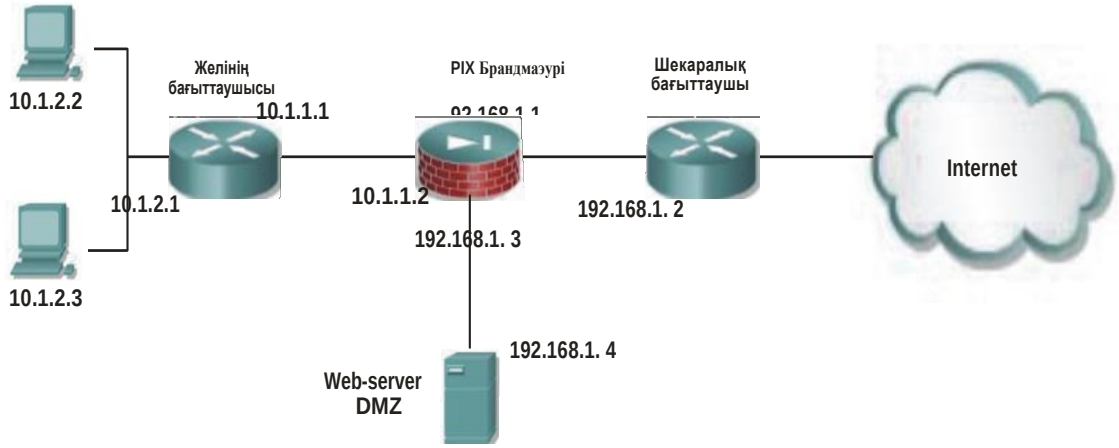
3.1 Сурет – МҚКК «Шымкент қаласының құтқару қызметі» белгісі

Қызметтің міндетіне мыналар кіреді:

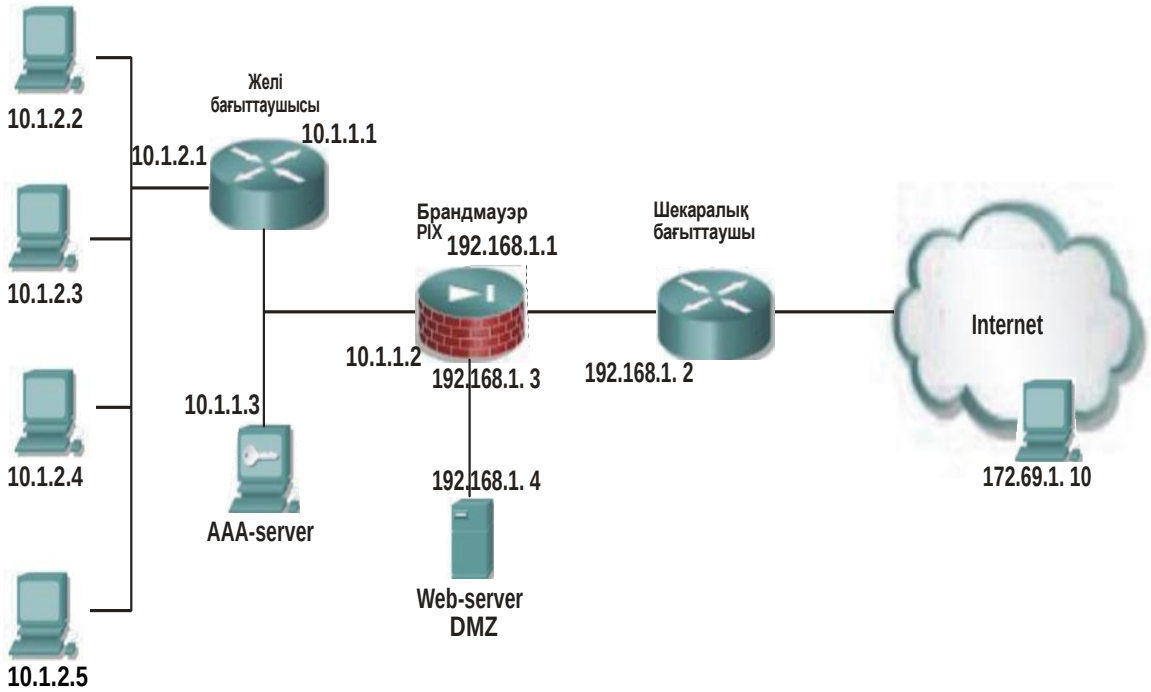
- зардап шеккендерге жедел жәрдем көрсетуді талап ететін тұрмыстық бақытсыздық жағдайлар және оқиғалар туралы ақпараттар жинау және өңдеу;
- түрлі төтенше жағдайларға тап болған азаматтарға көмек көрсету, тұрғындардың өмір сүру әрекетін қамтамасыз ету мәселелері бойынша тиісті қалалық жедел жәрдем қызметтерімен және басқа да мекемелермен өзара қарым-қатынас жасауды ұйымдастыру;
- аттестациядан өткен апаттық-құтқару жұмыстарының жиынтығын ұйымдастыру және жүргізу;
- төтенше жағдайлар және оқиғалар орын алған кезде қалалық жедел жәрдем және апаттық қызметтердің ақпараттануын қамтамасыз ету;
- түрлі төтенше жағдайларға жедел назар аудару үшін өзінің барлық құрылымдық бөлімшелерінің үнемі дайындығын қамтамасыз ету.

3.2 Жобаның құрылымдық сұлбасын зерттеу

3.2 және 3.3. суреттерде ақпараттық желінің сұлбалары көрсетілген



3.2 Сурет - Cisco Secure PIX Firewall қосу сұлбасы



3.3 Сурет - AAA технологиясымен желі топологиясы

3.3 Cisco Secure PIX Firewall брандмауэрін баптап күйге келтіру

Cisco Secure PIX Firewall брандмауэрлерін баптап күйге келтіру кезінде 2 интерфейсі бар PIX брандмауэрлерін баптап күйге келтіру қағидаларын есте сақтау қажет, себебі олардың 6 интерфейсті брандмауэрлерді баптап күйге

келтіру қағидаларынан ешбір айырмасы жоқ. Бұл қауіпсіздіктің бейімделген тәртібі (Adaptive Security Algorithm) қауіпсіздік деңгейлерінің (security levels) тұжырымын негізге алумен шартталған.

Аталған тұжырым, түрлі 2 интерфейсті қолдану барысында бір интерфейсті қауіпсіздіктің деңгейі өзге қауіпсіздік деңгейіне қарағанда айтарлықтай жоғары болуын меңзейді. Осылайша, PIX брандмауэрінің барлық мүмкіндік берілген екі интерфейсі виртуалды (virtual) брандмауэр қалыптастырады.

3.3.1 ASA қауіпсіздігінің деңгейлері

Ішкі (қауіпсіз) немесе сыртқы (қауіпсіз емес) қауіпсіздік деңгейі өзге интерфейстің қауіпсіздік деңгейін ескеру арқылы анықталады. Егер қауіпсіздік деңгейі өзге интерфейске қарағанда жоғары болса, онда интерфейс ішкі болып саналады және егер қауіпсіздік деңгейі өзге интерфейске қарағанда одан жоғары болса, онда интерфейс сыртқы болып саналады.

Қауіпсіздік деңгейлерін анықтау барысында келесі ережелерді басшылыққа алу қажет.

PIX брандмауэрін баптап күйге келтіру 6 команданың көмегімен жүргізіледі. Деректер қауіпсіздіктің ең жоғары деңгейімен интерфейс арқылы брандмауэрге түсуі мүмкін, брандмауэр арқылы өтіп, қауіпсіздіктің ең төмен деңгейімен интерфейске түсуі мүмкін. Әрине, қауіпсіздіктің ең төмен деңгейімен интерфейске түскен деректер, ешқандай да брандмауэрді тесіп өте алмайды және деректерді таратудың арнайы арнасы болмай немесе кіру мүмкіндігінің тізімінсіз (аталған мәселелер алдағы уақытта қарастырылады) қауіпсіздіктің жоғары деңгейімен интерфейске түсе алмайды.

Интерфейстің қауіпсіздік деңгейі 0-ден бастап 100-ге дейінгі мәнді қабылдай алады. Әрі қарай қауіпсіздік деңгейінің деректері толығырақ сипатталады.

Қауіпсіздік деңгейі 100. Бұл – интерфейс қауіпсіздігінің ең жоғары деңгейі. Аталған деңгей PIX брандмауэрінің ішкі интерфейстері үшін қолданылады. Сонымен қатар, ол PIX брандмауэрлерінде үнсіз келісім бойынша орнатылады және ешқандай өзгертілмейді. Қауіпсіздік деңгейі СТО мәнімен барынша қауіпсіз деңгейді алға тартады, демек ұйымның ішкі тармағына қауіпсіздіктің тап осы деңгейін меншіктеу қажет. Бұл кіруге арнайы рұқсат алғанға дейін ешкім, ешқандай жолмен ұйымның тармағына кіре ала алмайтындығын білдіреді.

Аталған рұқсаттарды ретке келтіру PIX брандмауэрін баптап күйге келтіру арқылы жүргізіледі. Сонымен бірге кез келген құрылығыны ішкі тармақтан сыртқы интернетке кіруін баптап күйге келтіру мүмкіндігі бар (егер бұл кіру мүмкіндігі тиісті тораптың қауіпсіздік саясатымен рұқсат берілген болса).

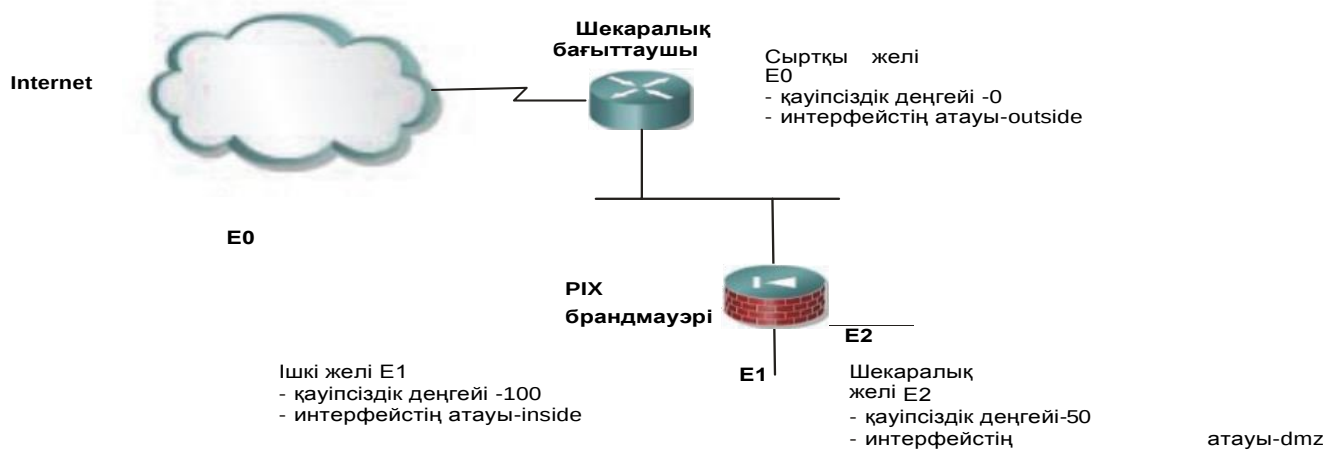
5.2 нұсқасының Cisco OS операциялық тұжырымында интерфейстерді қолдану мүмкіндігі жоғары, Etherneti ерекше ішкі тармақтар үшін және Ethernet1 ерекше сыртқы тармақтар үшін интерфейстерді қолдану. Алайда кез

келген жағдайда интерфейс деректері 100 мәнімен қауіпсіздік деңгейін қолдануы тиіс. Үнсіз келісім бойынша қабылданған баптап күйге келтіру өзгерісі, егер 6.0 нұсқасының PIX OS және одан жоғары ұйым брандмауэрінің ішкі және сыртқы тармақтары үшін жоғары жылдамдықты интерфейсті қолдануы тиіс болған жағдайда, мәнді құрайды.

Қауіпсіздік деңгейі 0. Бұл – қауіпсіздіктің ең шамалы деңгейі. PIX брандмауэрлерінде бұл деңгей сыртқы интерфейстер мақсатында қолданылады. Аталған мән PIX брандмауэрлерінде үнсіз келісім бойынша орнатылады және ешқандай өзгертілмейді. 0 деңгейі ең қауіпсіз түрде ұсынылады, сондықтан қауіпті тармақтардың басым бөлігі осы деңгейге жатқызылуы тиіс. Сыртқы желілерде орналасқан құрылғыларға брандмауэр арқылы кіру мүмкіндігі тек арнайы рұқсаттарды ретке келтірген жағдайда ғана ұсынылады. Аталған интерфейс әдетте Internet тармағына қосылған кезде қолданылады.

Қауіпсіздік деңгейі 1-99. Қауіпсіздік деңгейінің деректері PIX брандмауэрмен қызмет көрсетілетін, шекаралық интерфейстерге таңылуы мүмкін. Қауіпсіздік деңгейінің деректері қарусыздандырылған аймақтың (DMZ) интерфейстері тәрізді шекаралық интерфейстерді қосу мақсатында қолданылуы мүмкін. Қарусыздандырылған аймақ – бұл әдетте құрылғы немесе пайдаланушыларға сыртқы аймақтан қолжетімді интернет. Қарусыздандырылған аймақ ішкі (сеніп тапсырылған) аймақтан толығымен бөлінген, оқшауланған саламен ұсынылады.

3.4 суретте үш интерфейсі бар PIX брандмауэрінің мысалы көрсетілген.



PIX брандмауэрінің қауіпсіздік деңгейі

PIX брандмауэрі интерфейстердің жалпы көлемі 6-ға тең болғанда төртке дейін шекаралық торларға қызмет көрсетуге мүмкіндік береді.

Төменде PIX брандмауэрі және басқа шекаралық құрылғылар арасындағы интерфейстерді қосу мысалдары келтірілген.

Деректер қауіпсіздігі барынша жоғары интерфейстен (қауіпсіздік деңгейінің барынша жоғары мәнімен) қауіпсіздігі төменге (қауіпсіздік деңгейінің барынша төмен мәнімен) таратылады. Деректер таратудың мұндай бағыты кезінде деректер ағынының қауіпсіздігі барынша жоғары интерфейстен қауіпсіздігі барынша төменге өтуіне рұқсат қажет.

Мұндай шарт кезінде деректер ағынының ішкі тармақтан қауіпсіздіктің 100 деңгейімен сыртқы интернетке, ал егер кіру мүмкіндігіне басқарудың тізімімен (access control list), сәйкестендірумен (authentication) немесе авторзациямен (authorization) тыйым жасалмаған болса қауіпсіздіктің 0 деңгейімен өтуіне рұқсат беріледі.

Деректер қауіпсізді төмен интерфейстен (қауіпсіздік деңгейінің барынша жоғарыдан төмен мәнмен) қауіпсіздігі барынша жоғарығае (қауіпсіздік деңгейінің барынша жоғары мәнімен) таратылады. Деректерді таратудың осындай мақсатымен 2 шартты орындау қажет: қажетті деректер қорының өтуі мақсатымен кіру мүмкіндігін басқару тізімі және деректер қорының арнасы және статикалық трансляция. PIX брандмауэрінің деректер қорына қауіпсіздіктің 0 деңгейі арқылы сыртқы интерфейстен ішкі интерфейске қауіпсіздіктің 100 деңгейі арқылы өтуіне access-list бұйрығымен арнайы жеткілікті рұқсат берілмейінше тыйым салынады. Пайдаланушы access-list бұйрығын қолдану барысында сәйкестендіру (authentication) және авторизация (authorization) арқылы деректер қорын шектеуі мүмкін.

Деректер қауіпсіздік деңгейі бірдей 2 интерфейс арасында таратылады. Қауіпсіздік деңгейі бірдей 2 интерфейстің арасымен ешқандай деректер қоры өте алмайды. Егер брандмауэр екі немесе одан жоғары интерфейстің ASA қауіпсіздік деңгейі бірдей күйге келтірілген болса, онда мұндай кескіндемеге Cisco компаниясының техникалық қолдау (TAC) орталығы арқылы ешбір қолдау көрсетілмейді.

3.3.2 Cisco PIX брандмаэурін баптап күйге келтірудің негізгі алты командасы

PIX брандмауэрін баптап күйге келтіру барысында негізінен алты негізгі алты командасы қолданылады. Брандмауэрді басқару үшін келесі командалар қолданылады: nameif, interface и IP address. Nat, global және route командалары жиі қолданылады, бірақ брандмауэрмен жұмыс атқару кезінде оларды қолдану міндетті емес. Бұл командалар брандмауэр арқылы деректер қорын басқару үшін қолданылады. Nat және global командалары қауіпсіздігі барынша жоғары желіден (қауіпсіздік деңгейі барынша жоғары интерфейспен) қауіпсіздігі

барынша төмен желілерге (қауіпсіздік деңгейі барынша төмен интерфейспен) кіруін қамтамасыз етеді.

Nameif командасы

Nameif командасы PIX брандмауэрінің әр интерфейсіне есім беру және осы интерфейстің қауіпсіздік деңгейін анықтау үшін тағайындалған (есімдері үнсіз келісім бойынша берілген ішкі және сыртқы брандмауэр интерфейстерінен басқа).

Баптап күйге келтіруде сыртқы интерфейске үнсіз келісім бойынша Etherneto есімі және қауіпсіздік деңгейі 0 берілген, ал сыртқы интерфейске Etherneti есімі және қауіпсіздік деңгейі 100 берілген.

3.1 Кестеде nameif командасының міндетті және міндетті емес көрсеткіштері келтірілген, олардың синтаксисі келесідей көрініс табады: nameif сәйкестендіргіш деңгей есімі.

3.1 Кесте – Nameif командасының көрсеткіштері

Көрсеткіш	Сипаттама
Сәйкестендіргіш	PIX брандмауэрінде шекаралық интерфейсті және оның физикалық орналасуын анықтайды. Интерфейстердің үш түріне қолдау көрсетіледі: Ethernet, FDDI және Token Ring. Әрбір интерфейс интерфейстің физикалық орналасуына және түріне негізделген әріпті-санды сәйкестендіргішпен ұсынылады. Мысалы, Ethernet интерфейстерінің есімдері келесідей ethernet1, ethernet2, ethernet3 және т.с.с. Gigabit Ethernet интерфейстері келесідей сәйкестендіріледі: gb-ethernet1, gb-ethernet2, gb-ethernet3 және т.с.с.
Есім	Аталған көрсеткіш есім және физикалық тұрғыдағы шекаралық интерфейс арасында сәйкестік орнатады. Аталған есім пайдаланушымен анықталады және интерфейске қатысты келесі қатынастардың барлығында қолданылуы тиіс. Үнсіз келісім бойынша ішкі интерфейске E1, ал сыртқы интерфейске Eo есімі берілген.
Деңгей	Сыртқы интерфейстің қауіпсіздік деңгейін анықтайды. 1 бастап 99 дейін мәндер қабылдануы мүмкін.

Interface командасы

3.2. Кестеде interface командасының міндетті және міндетті емес көрсеткіштері келтірілген, олардың синтаксисі келесідей көрініс табады: interface сәйкестендіргіш жылдамдық [shutdown].

3.2 Кесте -IP address командасының көрсеткіштері

Көрсеткіш	Сипаттама

Есім	Интерфейсті сипаттау үшін тағайындалған. Интерфейстің есімі пайдаланушымен анықталады және осы интерфейске қатысты келесі қатынастардың барлығында қолданылады.
Маска	Егер желі ішінің маскасына тапсырыс берілмесе, онда желі ішіндегі үлгілік маскалардың бірі қолданылады А тобының желісі - 255.0.0.0 В тобының желісі - 255.255.0.0 С тобының желісі - 255.255.255.0

IP address командасы

PIX брандмауэр интерфейсінің әрқайсысы белгіленген қандай да бір IP-мекен-жаймен жұмыс атқару үшін баптап күйге келтіріледі. Жүйенің IP-мекен-жайын және желі ішіндегі маскаларды баптап күйге келтірген соң желілік интерфейстермен байланысты IP-мекен-жайлардың тізімдерін show IP командасының көмегімен қарап шығуға болады.

Қате болған жағдайда дұрыс көрсеткіштермен қайталап аталған команданы енгізу қажет. 3.3 Кестесінде команданың міндетті және міндетті емес көрсеткіштері келтірілген.

3.3 Кесте - Nat командасының көрсеткіштері

Көрсеткіш	Сипаттама
(есім)	Ғаламдық мекен-жайларды қолданатын желілік интерфейстердің есімдерін сипаттайды. Деректер global командасымен белгіленген интерфейстердің көмегімен таратылатын болады.
Сәйкестендіргіш	Ғаламдық пулды (p00l) анықтайды және global командасымен оның сәйкестігін белгілейді.
Локалді IP	Ішкі желінің құрылғыларымен тағайындалған IP-мекен-жай. 0.0.0.0 мекен-жайы барлық шығыс қосылуларға сәйкес ғаламдық пулдағы IP-мекен-жайларын трансляциялауға рұқсат беру үшін қолданылуы мүмкін.
Маска	Локалді IP-мекен-жайлар үшін желі ішіндегі маска

Nat командасы

Желілік мекен-жайларды трансляциялау (Network Address Translation - NAT) пайдаланушыға сыртқы желілерге қатынау кезінде ішкі желілік мекен-жайларды ашпауға мүмкіндік береді. Мысалы, пайдаланушы Internet-ке немесе кез келген сыртқы желіге қатынау кезінде ішкі ғаламдық желіге деректер пакеттерін таратудың алдында, ғаламдық желідегі IP-мекен-жайлары қолданылатын, тіркелген IP-мекен-жайларға, ғаламдық желіге қатысы жоқ ішкі трансляциялауды жүзеге асыру үшін nat командасы қолданылады.

Nat командасы осы команданың nat 0 түрін қолдану кезінен басқа жағдайда, үнемі global командасымен бірге қолданылады, бұл екі команда әрі

қарай толығымен қарастырылады.

PIX брандмауэрінің көрсеткіштерін бастапқыда баптап күйге келтіру кезінде барлық ішкі тораптарға 1 0.0.0.0 0.0.0.0. nat командасын қолдану арқылы 1 0.0.0.0 0.0.0.0. кез келген сыртқы тораптармен қосылу орнатуға рұқсат беруге болады.

1 0.0.0.0 0.0.0.0. nat командасы мекен-жайлар трансляциясын қамтиды және барлық ішкі тораптарға (0.0.0.0 көрсеткішімен анықталатын), тиісті global командасымен алдын ала қарастырылған қосылулар орнатуға мүмкіндік береді. Nat командасының көмегімен желілік мекен-жайлар трансляциясының ережелерін барынша нақты белгілеуге болады, бұл жеке мекен-жайлармен тәрізді мекен-жайлар аумағымен де жұмыс атқаруға ықпал етеді. Команданың синтаксисі 0.0.0.0 қатарының орнына 0 таңбасын қолдануға мүмкіндік береді.

Route командасы

Route командасы интерфейс үшін статикалық бағыт белгілейді. Бұл команданы қолдану белгіленген бағытқа тапсырыс беруді меңзейді. Егер бағыт белгіленбесе, онда үнсіз келісім бойынша белгіленген бағыт қолданылады.

3.4 кестеде route командасының міндетті және міндетті емес көрсеткіштері келтірілген. Аталған команданың синтаксисі келесідей көрініс табады: route есім IP_мекен-жайы маска шлюз [метрика]

3.4 Кесте - Route комадасының көрсеткіштері

Көрсеткіш	Сипаттама
Есім	Ішкі немесе сыртқы интерфейстің есімін сипаттайды. Бұл интерфейс брандмауэрден деректерді шығару үшін қолданылады.
IP-мекен-жай	Тағайындалудың ішкі немесе сыртқы мекен-жайын сипаттайды. Үнсіз келісім бойынша белгіленген бағытқа тапсырыс беру үшін 0.0.0.0.мекен-жайын қолданыңыз (барлық желі). 0.0.0.0.мекен-жайы о таңбасымен ауыстырылуы мүмкін.
Маска	IP-мекен-жайы көрсеткішінде белгіленген мекен-жай үшін желі маскасына тапсырыс береді. Үнсіз келісім бойынша белгіленген бағытқа тапсырыс беру үшін 0.0.0.0.мекен-жайын қолданыңыз (барлық желі). 0.0.0.0.мекен-жайы о таңбасымен ауыстырылуы мүмкін. Аталған масканы қолдану бір ғана желінің бар екенін білдіреді.
Шлюз	Шлюзді бағыттаушының IP-мекен-жайына тапсырыс береді (бұл бағыт үшін келесі ең жоғары мекен-жай)
Метрика	Шлюзді бағыттаушының мекен-жайына дейін өткелдер көлемін белгілейді. Егер сіз аталған көрсеткіштің дұрыс таңдалғанына сенімсіз болсаңыз, оны 1-ге тең деп белгілеңіз.

Route командасының көмегімен енгізілген барлық бағыттар бағыттаушы

кескіндемесінде сақталады.

Global командасы

Деректерді сенімді ішкі желіден сыртқы желіге тарату кезінде көбінесе дерек жөнелтушінің IP-мекен-жайы трансляциялауға ұшырайды. Брандмауэр екі команданың көмегімен мекен-жайларды трансляция жасауға ықпал етеді. Олардың ішінде біріншісі nat командасы болып табылады, бұл сеніп тапсырылған деректер көзінің трансляцияланатын мекен-жайларын анықтайды. 3.5 Кестеде global командасының міндеті жіне міндетті емес көрсеткіштері көрсетілген, оның синтаксисі келесідей көрініс табады: global (есім) сәйкестендіргіш interface|ғаламдық IP [- ғаламдық_IP] [netmask ғаламдық_маска]

Трансляциялау кестесінен жазбаны жою үшін global командасын қолдану қажет.

3.5 Кесте - Global командасының көрсеткіштері

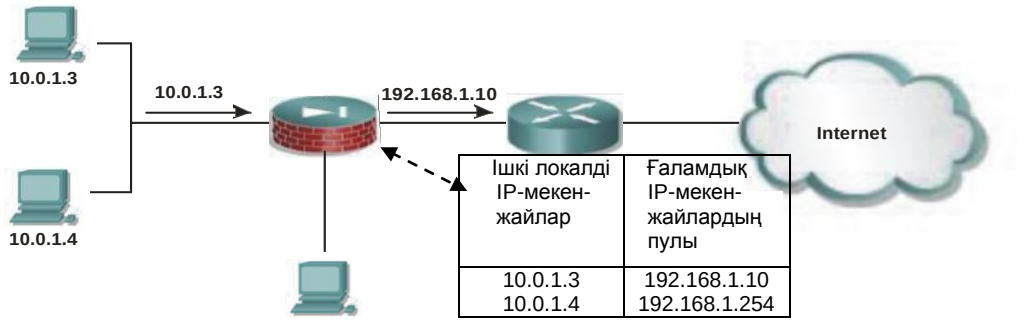
Көрсеткіш	Сипаттама
(есім)	Сыртқы мекен-жайлар үшін қолданылатын сыртқы желі интерфейстерінің есімдерін сипаттайды.
Сәйкестендіргіш	Ғаламдық пулды анықтайды және оның global командасымен сәйкестігін белгілейді.
Interface	Аталған көрсеткіш интерфейс портының мекен-жайын трансляциялау атауымен белгілі (Port Address Translation – PAT). Интерфейс портының мекен-жайын трансляциялау төменде қарастырылатын болады.
Ғаламдық IP	IP-мекен-жайлар диапазонының жеке IP-мекен-жайы немесе бастапқы мекен-жай
Netmask ғаламдық маска	Ғаламдық IP-мекен-жайлар үшін желі маскасына тапсырыс береді. Егер желі іші қолданылса, онда бұл көрсеткіште желі ішінің маскасын қолдану қажет (мысалы, 255.255.255.128). Егер сіз netmask командасында белгіленген желі ішімен түйісетін мекен-жайлар диапазонын көрсететін болсаңыз, онда бұл команда желілік немесе кең таралымды мекен-жайларды қолданбайды.

Ішкі желіде орналасқан құрылғыдан деректер пакеті PIX брандмауэрімен бөлінген ішкі желіге түскен сәтте деректер пакетінен жөнелтушінің IP мекен-жайы алынады және трансляциялау кестесінде орналасқан мәнмен салыстырылады. Егер бұл кестеде аталған құрылғының мекен-жайы жоқ болса, онда мекен-жай трансляцияланады. Бұл құрылғы үшін кестеде жаңа жазба жазылады, осы жазба аталған құрылғыға сәйкес мекен-жайлардың ғаламдық пулынан алынған IP мекен-жайын қамтиды. Аталған жазба трансляциялаудың слоты (translation slot) деп аталады. Мекен-жай трансляцияланған соң кесте жаңаланады және трансляцияланған IP-пакет әрі қарай бағытталады. Пайдаланушы белгілеген уақыт мерзімінен соң (бұл көрсеткіш timeout xlate

hh:ram:ss командасымен баптап күйге келтіріледі) немесе деректер пакеті белгіленген IP-мекен-жай үшін трансляцияланбайтын, үнсіз келісім бойынша қабылданған уақыт ішінде, үш сағат уақыт аралығынан кейін жазба кестеден жойылады және ғаламдық мекен-жай басқа сыртқы құрылғылар үшін қолданылуы мүмкін.

PIX брандмауэр ішкі NAT-мекен-жайларына виртуалды IP-мекен-жайларын тағайындау үшін ғаламдық мекен-жайларды қолданады. Global өрнегін қосқан, өзгерткен немесе жойған соң IP-мекен-жайларын трансляциялау үшін бос трансляцияның барлық слотттарын тазарту және құру мақсатында clear xlate командасын қолданыңыз.

3.5 Суретте Порт мекен-жайын трансляциялау мысалы көрсетілген.



3.5 Сурет- PIX брандмауэрінде мекен-жайларды трансляциялау

3.3.3 IP-мекен-жайларды трансляциялау

PIX брандмауэрі деректерді ішкі желіден тарату кезінде барлық ішкі IP мекен-жайларды трансляциялауға мүмкіндік береді. Деректердің тек шығыс ағындарына рұқсат беретін, қауіпсіздік саясатын енгізу қауіпсіздіктің айтарлықтай жеткілікті шешімі болып табылады. Егер ішкі желіге тиесілі тораптарды дербестендіру үшін жекеменшік дербестендіру (RFC 1918 қар.) қолданылса, Internet-те қолданылатын трансляцияланған мекен-жайлар үшін (қосылулардың бастапқы көзі) нақты тіркелген мекен-жайлар қолданылады.

Сыртқы желіден ішкі желіге қосылуға талпыныс жасаған пайдаланушы сәтсіздікке ұшырайды. Байланыс сеансы жекеменшік мекен-жайы бар пайдаланушыға Internet-тен орнатылмайды, себебі PIX брандауэрінің баптап күйге келтіруінде мұндай қосылуға рұқсат беруші арнайы ереже құрылуы тиіс.

RFC 1918 Address Allocation for Private Internets құжаты локалді желілер үшін мекен-жайларды таратудың келесідей ережелерін белгілейді:

Жекеменшік желілерде қолдану үшін Internet (Internet Assigned Numbers Authority – IANA) хаттамаларының нөмірлерін және есімдерін бөлу Агенттігі IP мекен-жайлардың үш блогын бөлді:

- 10.0.0.0. - 10.255.255.255 (префикс 10/8);
- 172.16.0.0 - 172.31.255.255 (префикс 172.16/12);
- 192.168.0.0 - 192.168.255.255 (префикс 192.168/16).

PIX брандмауэрі мекен-жайларды трансляциялау ережелерін орнату кезінде екі әдісті алдын ала қарастырады. Алғашқыда трансляция статикалық (static translation) түрде жүзеге асырылады, мұндай жағдайда ішкі мекен-жай

белгіленген ішкі ғаламдық мекен-жай бойынша трансляцияланады. Ішкі мекен-жайдан сыртқы мекен-жаймен қосылуға сұраныс түскен кезде ішкі мекен-жайды мекен-жайлардың ғаламдық пулында трансляциялау басқа әдіс болып табылады. Мұндай әдіс мекен-жайларды динамикалық трансляциялау деп аталады (dynamic addresstranslation).

PIX брандмауэрі NetBIOS хаттамасының кіріктірілген қолдауымен жабдықталған. Ішкі тораппен шығыс NetBIOS-байланыс сеансын құру барысында PIX брандмауэрімен IP-мекен-жайы пакеттердің IP-тақырыбындағы тәрізді NetBIOS-тақырыбында трансляцияланады.

3.3.4 Мекен-жайларды динамикалық трансляциялау

Мекен-жайларды динамикалық трансляциялау локалді IP-мекен-жайлардың белгіленген диапазондарын ғаламдық мекен-жайлардың тапсырыс берілген диапазонында немесе бір ғаламдық мекен-жайда трансляциялау үшін қолданылады. Локалді IP-мекен-жайлардың диапазондарын ғаламдық мекен-жайларда трансляциялауды желілік мекен-жайларды трансляциялау (Network Address Translation - NAT) деп атайды. Локалді мекен-жайлардың диапазонын бір ғаламдық мекен-жайда трансляциялауды порттың мекен-жайын трансляциялау деп атайды.

Желілік мекен-жайларды трансляциялау (Network Address Translation)

Динамикалық трансляциялауда NAT әдісін қолдану кезінде локалді тораптардың IP-мекен-жайлары (яғни, трансляцияланатын мекен-жайлар) nat командасының көмегімен анықталуы тиіс. Сонымен бірге global командасының көмегімен мекен-жайлардың пулы анықталуы тиіс. Сыртқы интерфейстермен жұмыс атқару үшін IP-мекен-жайлардың пулы nat_id көрсеткішінде nat командасымен бөлінеді. Пайдаланушының ғаламдық IP-мекен-жайлардың 256 пулын анықтау мүмкіндігі болады. Бұл үшін келесі командаларды қолдануға болады:

```
pixfirewall(config)# nat (inside) 1 0.0.0.0. 0.0.0.0. 0 0
pixfirewall(config)# global (outside) 1 192.168.1.10-192.168.1.254
netmask 255.255.255.0
```

Егер IP-мекен-жайы 10.0.1.10 торап бірінші болып PIX брандмауэрі арқылы Internet-пен байланыс сеансын орнақтан болса, онда бұл мекен-жай 192.168.1.10. трансляцияланады. 3.6 суретте 254 дейін жеке ғаламдық IP-мекен-жайларды қамтамасыз ететін, диапазоны 192.168.1.10-192.168.1.254, global командасымен анықталған ғаламдық мекен-жайлардың пулы бейнеленген. Барлық локалді мекен-жайлар nat командасында 0.0.0.0. маскасын қолдану арқылы трансляцияланады.

3.6 Сурет – Желілік мекен-жайларды трансляциялау

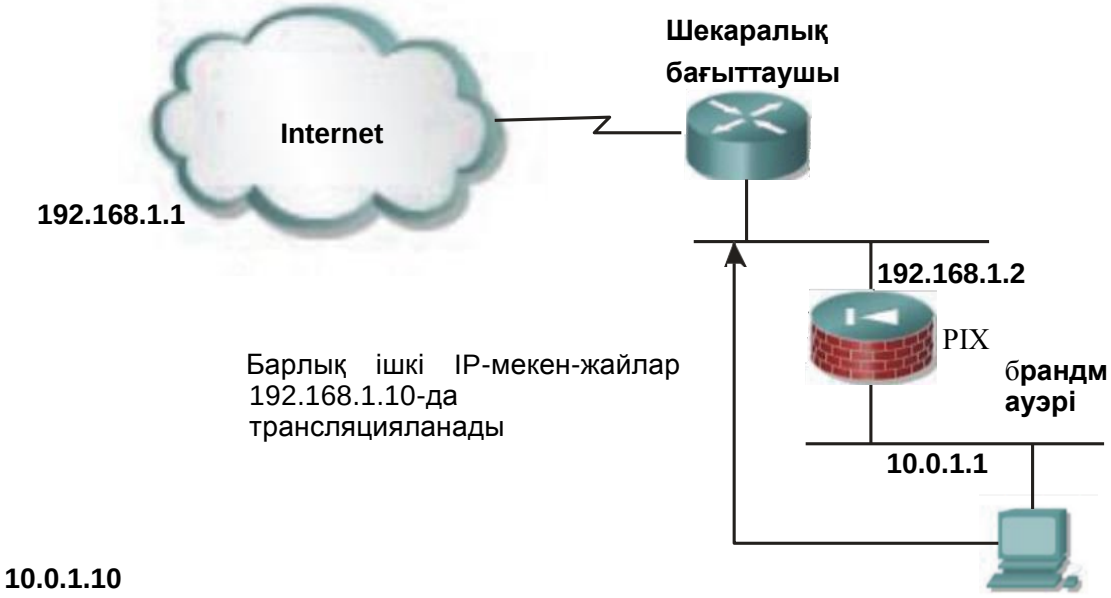
Static және global/nat командалары бірдей көрсеткіштермен өте жиі қолданылады. Static командасын қодану барысында global командасымен анықталатын, ғаламдық мекен-жайлар диапазонына кірмейтін ғаламдық IP-мекен-жайларды қолдану қажет. Мысалы, келесі мысалда static командасының 192.168.1.10 дұрыс емес көрсеткіштері берілген, себебі аталған мекен-жай global командасымен 192.168.1.10-192.168.1.254 берілген, IP-мекен-жайлардың диапазонына кіреді:

```
     pixfirewall(conf)#   nat (inside) 1 0.0.0.0. 0.0.0.0. 00
     pixfirewall(conf)#   global (outside) 1 192.168.1.10-192.168.1.254
netmask 255.255.255.0
     pixfirewall(conf)#   static    (inside,    outside)    192.168.1.10
10.1.1.10
     Төменде    көрсеткіштері    дұрыс    мысал    келтірілген
     pixfirewall(conf)#   nat(inside) 1 0.0.0.0. 0.0.0.0.00
     pixfirewall(conf)#   global (outside) 1 192.168.1.11-192.168.1.254
netmask 255.255.255.0
     pixfirewall(conf)#   static (inside,outside) 192.168.1.1010.1.1.10
```

Порт мекен-жайларын трансляциялау

Порт мекен-жайларын трансляциялау (Port Address Translation – PAT) әдісін қолдану кезінде барлық локалді IP-мекен-жайлар бір ғаламдық мекен-жайда трансляцияланады. PAT әдісін қолдану арқылы брандмауэрді баптап күйге келтіру барысы NAT әдісін қолдану кезіндегі баптап күйге келтіруге ұқсас. Айырмашылығы тек global командасында мекен-жайлар диапазонының орнына бір IP-мекен-жай қолданылады. 3.7 суретте келесі команданың сипаттамасы көрсетілген:

```
pixfirewall(conf)# nat (inside) 1 0.0.0.0. 0.0.0.0. 00
pixfirewall(conf)#   global   (outside)   1   192.168.1.10   netmask
255.255.255.255
```



3.7 Сурет – Порт мекен-жайларын трансляциялау

Бұл мысалда Internet-пен қосылу кезінде барлық сыртқы IP-мекен-жайлар бір IP-мекен-жайда 192.168.1.10. трансляцияланады.

PAT әдісін қолдану барысында мыналарды ескеру қажет:

PAT әдісін қолдану бір ғана IP-мекен-жаймен бірнеше шығыс байланыс сеанстарын құруға мүмкіндік береді. PAT технологиясын қолдану кезінде брандмауэр шығыс қосылуды трансляциялаудың әрбір слоты үшін бірегей нөмір таңдайды. Бұл технологияның осы қасиеті Internet (ISP) қызметтерін жеткізуші пайдаланушыларға ұсыну үшін бос сыртқы IP-мекен-жайлар жетіспеген жағдайда пайдалы болуы мүмкін.

PAT-та қолдану үшін белгіленген IP-мекен-жай ғаламдық мекен-жайлардың өзге пулдарында қолданылмайды.

Ғаламдық мекен-жайлардың пулын кеңейту кезінде ең бірінші ғаламдық пулдан алынған мекен-жайлар қолданылады, ал сонан соң келесі қосылу үшін IP-мекен-жай PAT- мекен-жайларынан таңдап алынады. Егер ғаламдық пулдың мекен-жайлары босатылса, онда келесі қосылулар үшін осылардың өзі қолданылады. Ғаламдық мекен-жайлардың пулын PAT-мекен-жайларымен кеңейту ғаламдық пул және PAT құрайтын global командаларында бірдей сәйкестендіргіштерді қолдану арқылы жүзеге асырылады.

PAT әдісі H.23 стандартының қосымшаларымен, сондай ақ есімдерді кэштеу серверлерімен жұмыс атқармайды. PAT әдісін PIX брандмауэрі арқылы мультимедиа-қосымшаларымен жұмыс атқаруға қолданбаңыз. Бұл қосымшалар PIX брандмауэрімен ұсынылатын порттардың тағайындалу механизмімен қақтығысуы мүмкін.

3.3.5 Static және access-list командаларын сипаттау

Қосылулардың басым бөлігі қауіпсіздік деңгейі барынша жоғары интерфейстен қауіпсіздік деңгейі барынша төмен интерфейске орнатылуына қарамастан, көптеген қосымшалармен жұмыс атқару үшін қауіпсіздік деңгейі барынша төмен интерфейстен қауіпсіздік деңгейі барынша жоғары интерфейске қосылу орнату қажет. Ол үшін access-list бағдарламасын қолдану қажет.

Мысалы, access-list командасын ICMP-хабарламаларының көмегімен PIX брандмауэр арқылы орнатылған қосылуларға тексеру жүргізу үшін қолдануға болады. PIX брандмауэр арқылы сыртқы желілерден жаңғырық-жауаптарын (ping) алу үшін access-list командасының көмегімен брандмауэрді баптап күйге келтіру қажет. Сонымен бірге сыртқы желінің пайдаланушысында деректерді қабылдаушының IP-мекен-жайы болуы тиіс. Аталған ақпаратты static командасының көмегімен брандмауэрді баптап күйге келтіру үшін қолдануға болады.

Static командасы локалді (ішкі) IP-мекен-жайды және ғаламдық (сыртқы) IP-мекен-жайды біріктіретін трансляция слотын құрады. Static командасы ғаламдық IP-мекен-жай мен белгіленген ішкі IP-мекен-жай арасында қатаң сәйкестік орнатуға, сондай ақ қауіпсіздік деңгейі барынша төмен интерфейстің қауіпсіздік деңгейі барынша жоғары интерфейске деректер таратуына мүмкіндік береді.

Static командасының көмегімен лоакалді және ғаламдық IP-мекен-жайлар арасында статикалық сәйкестің құрған соң ішкі жіне сыртқы интерфейстер арасындағы қосылу қауіпсіздіктің бейімделген тәртібімен (Adaptive Security Algorithm – ASA) бұғатталып қалады. Деректер ағынының қауіпсіздік деңгейі барынша төмен интерфейстен қауіпсіздік деңгейі барынша жоғары интерфейске өтуіне рұқсат беру үшін access-list командасын қолдану қажет. Осы команданың көмегімен PIX брандауэрінің бейімделген қауіпсіздік тәртібі үшін мүмкіндіктер құрылады.

Static командасы локалді және ғаламдық IP-мекен-жайлардың статикалық сәйкестігін (статикалық трансляцияның слоты (static translation slot) немесе xlate деп аталатын) құрады. Шығыс қосылулары үшін static командасын үнемі локалді торапты трансляциялауда қолданылатын ғаламдық мекен-жайларды анықтау мақсатында қолдану қажет. Кіріс қосылулары үшін сыртқы желіде көрінетін мекен-жайларды сәйкестендіру мақсатында static және access-list командаларын қолдану қажет. Келесі ережелерді есте сақтау өте маңызды:

Access-list командасы қауіпсіздік деңгейі барынша жоғары интерфейстен

қауіпсіздік деңгейі барынша төмен интерфейске қосылуын орнатуға мүмкіндік береді. Бұл команда аталған торап үшін бейімделген қауіпсіздіктің тәртібін қолдануды қамтамасыз ететін, кіріс қосылуларының қауіпсіздік саясатына мүмкіндіктер енгізуге ықпал етеді.

Static командасы локалді және ғаламдық IP-мекен-жайлардың статикалық сәйкестігін құру үшін қолданылады.

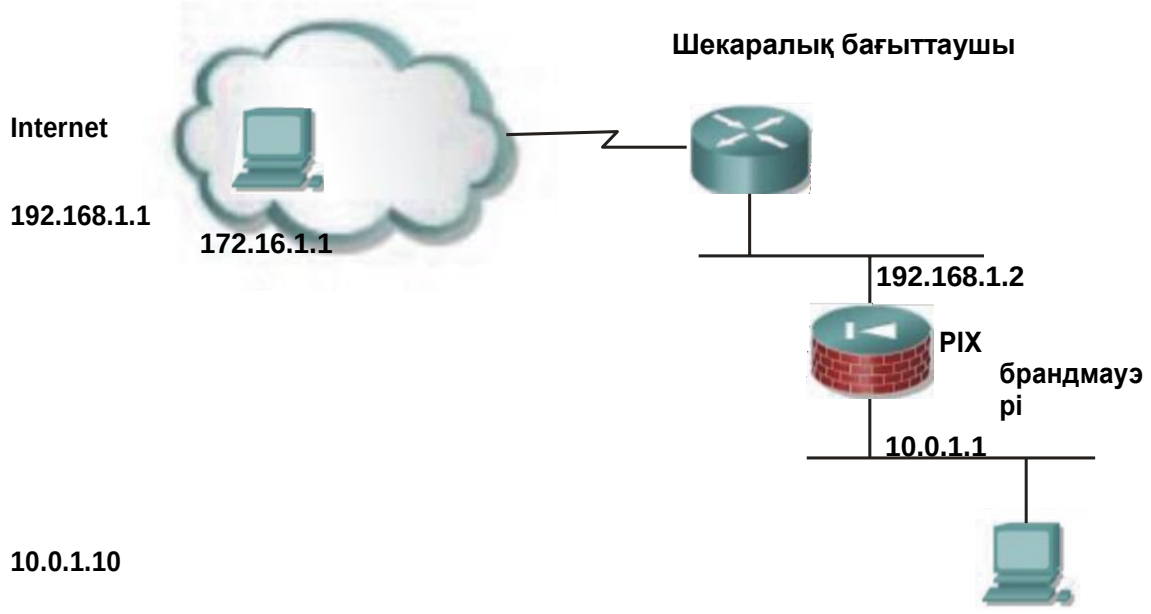
Static командасы локалді IP-мекен-жайларды белгіленген ғаламдық IP-мекен-жайларға статикалық түйістіруді (статикалық трансляция деп аталатын) қамтамасыз етеді. Егер сыртқы желі ретінде Internet қолданылатын болса, онда ғаламдық IP-мекен-жай домендік есімдер қызметінде тіркелген болуы тиіс. Static командасының синтаксисі жоғарыда сипатталды. Static командасының nat және global командаларымен салыстырғанда артықшылығы барынша жоғары. Брандмауэрдің ағымдағы кескіндемесінде static өрнегін қарап шығу үшін show static командасын қолдануға болады.

Әрбір интерфейс үшін қауіпсіздік деңгейі nameif командасының көмегімен белгіленеді. PIX брандмауэр арқылы қауіпсіздік деңгейі барынша төмен интерфейстен қауіпсіздік деңгейі барынша жоғары интерфейске бағытталған байланыс сеансын қамтамасыз ету, сонымен бірге деректер ағынын тарату үшін осы екі интерфейстің арасында access-list және static командаларын қолдану қажет. Мысалы, байланыстың кіріс сеансына сыртқы аймақтан қарусыздандырылған аймаққа немесе сыртқы аймақтан – ішкі аймаққа өтуіне рұқсат беру үшін access-list және static командаларын қолдану қажет.

Access-list командасы

Access-list командасы TCP, UDP хаттамалары және ішкі желінің тораптарымен қолдау көрсетілетін басқа хаттамалар бойынша сыртқы желіден қосылулар орнатуға рұқсат береді немесе тыйым салады. Сонымен бірге аталған команда ғаламдық ережелер үшін де, қандай да бір нақты көрсеткіштерді орнату үшін де қолданылуы мүмкін. Мысалы, access-list командасы нақты торапқа HTTP-кіруге рұқсат беруге ықпал етеді.

3.8 суретте access-list командасы қалай қолданылатындығы көрсетілген.



3.8 Сурет - Access-list командасын қолдану

Access-list командасын қолдану барысында баптап күйге келтірудің барлық бөлшектерін ескеру қажет, себебі пайдаланушыларға сыртқы желіден ішкі желіге telnet-кіру мүмкіндігін кездейсоқ ұсыну желінің бүкіл қауіпсіздік саясатына қауіп-қатер төндіруі мүмкін.

3.9 суретте бір локалді торапқа тек бір ғана ғаламдық торапқа кіру мүмкіндігін ұсыну бейнеленген.

10.0.1.10

3.9 Сурет - Static және access-list командаларын қолдану

3.9 суретте IP-мекен-жайы 172.16.1.1 бар сыртқы желінің пайдаланушысы қабылдаушының 192.168.1.101. IP-мекен-жайын қолданады.

PIX брандмауэрі осы мекен-жайды трансляциялайды және static командасының көмегімен құрылған ережеге сәйкес ішкі мекен-жайға 10.0.1.10 сұраныс жөнелтеді. PIX брандмауэрінде access-list командасының көмегімен 8000 дейін байланыс арнасын анықтауға болады. Құрылған байланыс арналары туралы, сондай ақ олардың көлемі туралы ақпаратты қарау үшін show access-list командасын қолдануға болады. Байланыс арнасын жою үшін noaccess-list командасы тағайындалған. Егер ішкі желінің пайдаланушыларына сыртқы тораптардан жаңғырық-сұраныстарын (ping) жүргізу мүмкіндігін ұсыну қажеттілігі туындаса, жаңғырық-жауаптарын тарату үшін тағайындалған арнайы байланыс арнасын құру қажет.

3.3.6 Cisco PIX брандмауэрлерінде сәйкестендіру, авторизациялау және есепке алу барысын баптап күйге келтіру

Қауіпсіздік саясатын жүзеге асырудың басым бөлігі пайдаланушылардың түрлі ресурстарға кіру деңгейін бөлу санасына негізделген. Басқаша айтқанда, қауіпсіздік саясаты ұғымы оны қамтамасыз етуге арналған шараларды ғана емес, сонымен бірге басқа да аспектілерді қамтиды. Қорғаныс құралдарының басым көлемін қолдануды қамтамасыз ететін, тәсілдерді қолдану кезінде қауіпсіздік саясаты барынша жетілдірілген, қауіпсіздікті бұзуы мүмкін барлық қауіп-қатерлерді ескерген болып қалыптасады.

Қауіпсіздік саясатына қатысты аспектілердің бірі белгіленген қызметтерге кіру мүмкіндігін алу үшін пайдаланушыларға нақты идентификаторды және құпиясөзді енгізу талабы қойылуы мүмкін. Аталған әдіс пайдаланушыға негізделген сәйкестендіру (user-based authentication) деп аталады. Бұл ретте сәйкестендіру қандай да бір нақты пайдаланушының жұмысына ешбір әсер етпейді – көбінесе ол бір желілік құрылғыны басқамен сәйкестендіруге жинақталады.

3.3.7 AAA технологиясын анықтау

Сәйкестендіру (authentication) ұғымы дегеніміз пайдаланушыны бірегейлендіру және осы ақпаратты тексеру. Дәстүр бойынша пайдаланушыны бірегейлендіру үшін пайдаланушының есімі (немесе бірегей сәйкестендіргіш) қолданылады. Белгіленген сәйкестендіргіш арқылы желіге немесе құрылғыға кіру мүмкіндігі пайдаланушыны анықтайды.

Авторизациядан кейін пайдаланушы жүйеде пайдаланушының бірегей сәйкестендіргішіне және оған тиесілі құпиясөзге негізделген авторизациядан (authorization) өтуі тиіс. Авторизация процесі жүйеде пайдаланушының құқын анықтайды. Пайдаланушының жүйедегі барлық іс-әрекеттеріне хаттама жүргізіледі. Осылайша, пайдаланушының жүйеге кірген соң қызметке, торапқа немесе желіге кіруі туралы жазбалар сақталады. Жүйеде пайдаланушының іс-әрекеттерін хаттамалау процесі есепке алу (accounting) деп аталады.

Пайдаланушының іс-әрекетіне қатысты толық мәліметті жұрнал жүргізудің кейбір кезде пайдасы өте зор, себебі жүйе жұмысында қандай да бір түйінді мәселе туындаған сәтте, пайдаланушының іс-әрекеті тіркелетін жұрналдың болуы жүйенің жұмыс қабілетін қалпына келтіру процесін едәуір жеңілдетуге және жылдамдатуға мүмкіндік береді. Сонымен қатар пайдаланушылардың есептік жазбалары пайдаланушыларға шот жазып берген сәтте, сот талқылаулары жағдайында, сондай ақ автоматтандырылған жүйелердің архитектурасын жоспарлау барысында қолданылуы мүмкін.

PIX брандмауэрінде пайдаланушымен жасалған іс-әрекеттерге хаттама жүргізу және жүйеде пайдаланушының құқын анықтау, бірегейлендіру үшін сәйкестендіру, авторизациялау және есепке алу (Authentication, Authorization, Accounting - AAA) технологиясы қолданылады. Кіруді бақылаудың қарапайым әдісі порттар және IP-мекен-жайлары туралы ақпаратты тексеруге негізделген. Бақылаудың бұл әдісі кейбір пайдаланушыларды бірегейлендіру механизмін ұсынбайды және кейбір пайдаланушының деректер ағынын бақылауға мүмкіндік бермейді. Пайдаланушы авторизациясыз сәйкестендіруден өте алады, бірақ алдын ала сәйкестендірусіз авторизациядан өте алмайды. PIX брандмауэрлерінде AAA технологиясын қолдану кезінде сәйкестендіру және авторизациялау келесідей өтеді:

Клиент кейбір қызметке сұраныс жөнелтеді. Клиент пен сервер қызметі арасында бағыттаушы қызметін атқаратын PIX брандмауэрі орын алады. Брандмауэр клиенттерден жеке индентификатор мен құпиясөз сұрайды (сұраныс түріне және брандмауэр кескіндемесіне сәйкес).

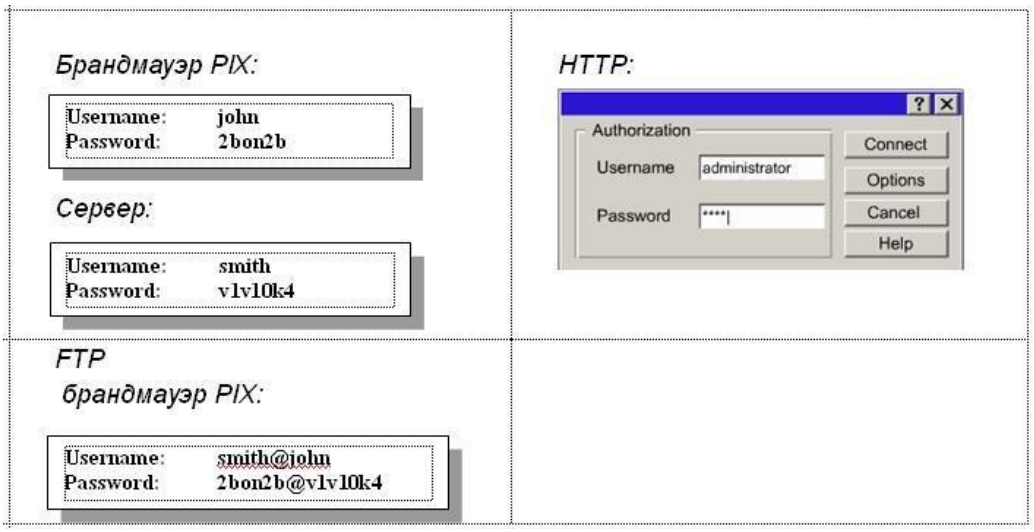
Пайдаланушыдан жеке идентификатор және құпиясөз алған соң, брандмауэр бұл деректерді AAA-серверіне жөнелтеді, мұнда олар тексерілген соң клиенттің сұранысына рұқсат беру немесе тыйым салу туралы шешім қабылданады. AAA үш қызметінің кез келгенін ұсынатын қандай да бір логикалық объект осындай сервер болып табылады. Аталған серверде пайдаланушылардың осы немесе өзге қызметке кіру құқын анықтау үшін пайдаланушылардың әмбебап индентификаторлары және құпиясөздері қамтылған деректер қоры сақталады.

Жеке брандмауэрмен жұмыс жүргізу үшін бөлінген AAA-серверінің орын алуы брандмауэрді басқару және баптап күйге келтіру жұмысын жеңілдетеді, сондай ақ жүйені кеңейтуді барынша қарапайым етеді.

Желіге кіру мүмкіндігі сәйкестендіруден өткен пайдаланушыларға ғана ұсынылуы мүмкін. Мысалы, ішкі желіден Internet-ке кіру мүмкіндігін «идентификатор-құпиясөз» дұрыс амалын енгізген пайдаланушылар ғана алады. Сонымен бірге сәйкестендіруден өткен пайдаланушылардың авторизациясын

(қосымшаларға кіру мүмкіндігі) шектеу мүмкіндігі. Әкімгер брандмауэрді баптап күйге келтіру арқылы FTP, HTTP, Telnet қызметтеріне және басқа да қосымшаларға (немесе қосымшаның кез келген амалдарына) кіру мүмкіндігін шектей алады. Сәйкестендіруге бақылау жүргізу үшін AAA-серверін баптап күйге келтіру Cisco Secure Access Control Server (CSACS) бағдарламалық жүйесінің көмегімен жүргізілуі мүмкін, бұл пайдаланушыларды сәйкестендіруге және авторизациялауға мүмкіндік береді. Сонымен бірге, AAA-сервері пайдаланушылардың есептік жазбаларының жұрналын жүргізуге ықпал етеді. Басқа жағдайда PIX брандмауэрі арқылы пайдаланушыға тек FTP-қызметіне кіруге рұқсат берілуі мүмкін. Пайдаланушының жөнелткен сұранысы брандмауэрмен қағып алынады, мұнда сұраныстың өтуіне рұқсат алу үшін пайдаланушылық есімді және құпиясөзді енгізу талап етіледі. Пайдаланушымен енгізілген ақпарат AAA-серверіне таратылады. Пайдаланушы ретінде AAA-серверінде сәйкестендірілген соң, ол қосымша сұраныстарды орындай алады. Пайдаланушының әрбір сұранысы брандмауэрмен қағып алынады және AAA-серверіне авторизациялану үшін жөнелтіледі.

Пайдаланушы FTP, Telnet немесе HTTP үш қызметтің бірін қолдана отырып, брандмауэрде сәйкестендіруден өтуі мүмкін. Осы қызметтердің әрқайсысында сәйкестендірудің өз механизмдері бар, бірақ брандмауэрмен жұмыс атқара алатын қосымшалардың көлемі осы үш хаттамамен шектелмейді. Басқа қосымшалар үшін сәйкестендіру сұлбасы осы немесе өзге қызметтерді жүзеге асыруға байланысты. 3.10 суретте қолданылатын қызметтің түріне байланысты пайдаланушыдан талап етілетін түрлі ақпарат көрсетілген.



3.10 Сурет - Telnet пайдаланушыдан талап етілетін ақпарат.

Сұраныс брандауэрмен түрленеді. Әрбір пайдаланушының жүйеге кіру үшін төрт мүмкіндігі болады. Төрт мүмкіндік сәтсіз аяқталған жағдайда брандмауэр тез арада қосылуды аяқтайды. Егер сәйкестендіру және авторизациялау процесі сәтті өтсе, онда пайдаланушыға кіру мүмкіндігі берілген сервер, өз кезегінде пайдаланушыдан пайдаланушылық есімді және құпиясөзді енгізуді сұрауы мүмкін.

FTP. Сұраныс FTP-бағдарламасымен түрленеді. Құпиясөз дұрыс емес енгізілген жағдайда қосылу тез арада мәжбүрлі ажырайды. Егер қосымшалардың деректер қорындағы пайдаланушының есімі немесе құпиясөзі FTP-кіру мүмкіндігі берілген қашықтағы тораптың құпиясөзінен немесе пайдаланушының есімінен айырмашылық тапса, онда пайдаланушының есімін және құпиясөзін келесідей үлгіде енгізу қажет:

- есім_ааа@ _үшін есім_қашықтан_кіру_үшін;
- құпиясөз_ааа@ _үшін құпиясөз_ қашықтан_кіру_үшін.

PIX брандмауэрі есім_ааа_үшін және құпиясөз_ааа_үшін мәндерін AAA-серверіне жөнелтеді. Егер сәйкестендіру және авторизация сәтті өтсе, онда FTP-серверіне есім _қашықтан_кіру_үшін құпиясөз_ қашықтан_кіру_үшін мәндерін жібереді.

HTTP. Пайдаланушының браузері пайдаланушылық есімді және құпиясөзді енгізу үшін терезе ашады. Пайдаланушы ұқпиясөзді дұрыс емес енгізген жағдайда құпиясөзді қайталап енгізе алады. Құпиясөзді сәтсіз енгізу мүмкіндігінің белгіленген санынан соң (кез келген мән белгіленуі мүмкін) есептік жазба шектелуі мүмкін.

Егер қосымшалардың деректер қорындағы пайдаланушының есімі немесе құпиясөзі HTTP-кіру мүмкіндігі берілген қашықтағы тораптың құпиясөзінен немесе пайдаланушының есімінен айырмашылық тапса, онда пайдаланушының есімін және құпиясөзін келесідей үлгіде енгізу қажет:

- есім_ ааа@_үшін есім _қашықтан_кіру_үшін;
- құпиясөз_ ааа@ _үшін құпиясөз _қашықтан_кіру_үшін.

PIX брандмауэрі есім_ааа_үшін және құпиясөз_ааа_үшін мәндерін AAA-серверіне жөнелтеді. Егер сәйкестендіру және авторизация сәтті өтсе, онда HTTP-серверіне есім _қашықтан_кіру_үшін және құпиясөз_ қашықтан_кіру_үшін мәндерін жібереді.

PIX брандмауэрі сәйкестендіру үшін пайдаланушының 127 дейінгі таңба құрайтын есімді және 63 жоғары емес таңба қамтитын құпиясөзді қолдайды. FTP және HTTP хаттамаларын қолдану барасында пайдаланушылардың есімдерін және құпиясөздерін тарату үшін арнайы үлгі қолданылады, сондықтан пайдаланушылардың есімдерінде және олардың құпиясөздерінде @ таңбасын қолдануға жол берілмейді.

HTTP хаттамасы бойынша сәйкестендіру өткен соң пайдаланушыға timeout uauth (осы көрсеткішпен берілген уақыт шегінен асып кеткен соң, пайдаланушыға сәйкестендіру рет-жосығынан қайтадан өтуіне тура келеді) көрсеткішімен берілген уақыт ішінде қайталап сәйкестендіруден өту талап етілмейді. Пайдаланушы браузері осы Web-торап арқылы барлық кезекті қосылулар үшін авторизация туралы ақпаратты кэштейді, бұл қызмет сол үшін қажет. Бұл деректерді жою үшін Internet Explorer және Netscape Navigator қосымшаларының барлық данасын жабу және жүйені қайта жүктеу қажет. Оған дейін кэшті тазартудың пайдасы болмайды.

3.3.8 Айқын прокси-серверінің тәртібіндегі жұмыс

PIX брандмаэурінде сәйкестендіру және авторизациялау құралдарын баптап күйге келтіру айқын прокси-сервер тәртібін баптап күйге келтіру деп аталады (cut-through proxy). Пайдаланушылардың сәйкестендірілуін айқын тексерудің (яғни пайдаланушыға көрінбейтін) бұл технологиясын қолдану кезінде брандмауэрдің өнімділігі бірден артады. Осы тексерудің нәтижесінде белгіленген TCP- және UDP-қосымшаларына кіруге рұқсат беру немесе бұғаттау туралы шешім қабылданады.

Аталған әдісте UNIX және басқа да операциялық жүйелердің негізінде жүзеге асырылған, басқа брандмауэрлердегі ұқсас кескіндемеде байқалатын кемшіліктер жоқ. Сонымен қатар аталған әдіс CSACS серверлерінде сәйкестендіру және авторизациялау қызметтерін қолдануға мүмкіндік береді.

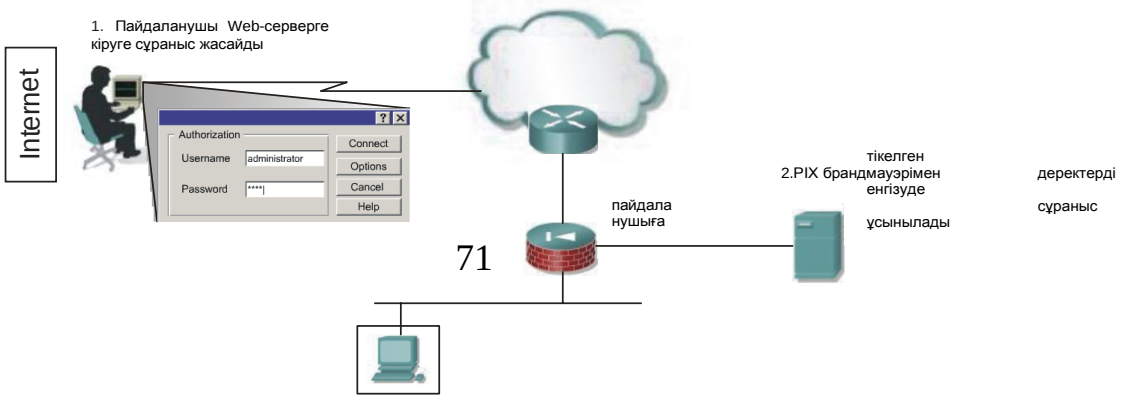
Бірінші кемшілігі осы сервер және брандмауэрдің өз қосымшасы үшін операциялық жүйенің, сервердің аппараттық құралдарын сатып алу қажеттілігінде. Екінші кемшілік – бұл брандмауэр басқаратын операциялық жүйенің өзіне қызмет көрсету қажеттілігіне байланысты брандмауэр жұмыс атқаратын сервердің өнімділігін төмендету.

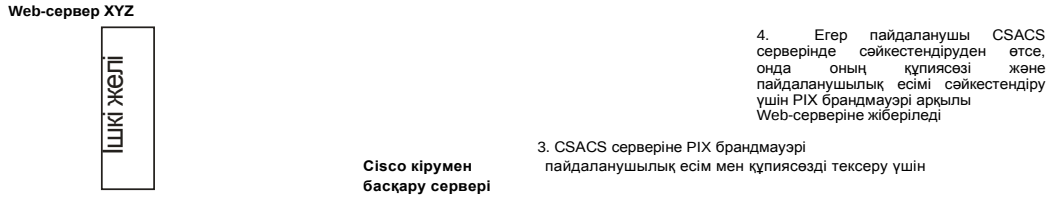
Айқын прокси-сервер тәртібінде жұмыс атқару барысында PIX брандмауэр пайдаланушыны негізге ала отырып, байланыс сеансын сәйкестендіру қажеттілігін анықтайды, пайдаланушылық есімді және құпиясөзді сұраудың тиісті механизмін ұсынады, сонымен бірге TACACS+ және RADIUS жүйелерінің стандартты дерек қорларының көмегімен пайдаланушыларды сәйкестендіреді. Пайдаланушы сәйкестендіруден сәтті өткен соң PIX брандмауэр осы деректер ағынымен жұмыс атқаруды тоқтатады және әрі қарай ақпарат алмасу тікелей клиент пен сервер арасында жүзеге асырылады. Брандмауэр тек сеанстың жай-күйі туралы ақпаратты ғана тексеріп отырады.

Аталған технологияны үлгі түрінде қолдану Internet-тен DMZ-аймағына кіруді жүзеге асыратын пайдаланушыларды тексеру болып табылады.

8.2 суретте пайдаланушының XYZ Web-серверіне кіру үшін белгіленген URL-мекен-жайға кіруі көрсетілген

Бұл үшін пайдаланушы сәйкестендіруден және авторизациядан өтуі тиіс, мұнда пайдаланушылық идентификаторды және құпиясөзді енгізу талап етіледі. Пайдаланушы аталған ақпаратты енгізеді, сонан соң ол шифрленбеген түрде брандмауэрге тапсырылады, брандмауэр оны CSACS орындалатын AAA-серверіне жібереді. Пайдаланушы сәйкестендіруден сәтті өткен жағдайда сұраныс жасалып отырған сервермен өзара әрекеттесуге рұқсат алады. Егер қосылу үшін Web-серверге кіру құпиясөзі талап етілсе, онда пайдаланушы осы деректерді енгізуі тиіс (3.11 Сурет).





3.11 Сурет - Айқын прокси-сервер тәртібінде жұмыс атқару

Сәйкестендіруді баптап күйге келтіру

CSACS бағдарламасын PIX брандмауэрінің кескіндемесінде баптап күйге келтірген соң AAA-серверіне қатысты тиісті баптап күйге келтірулерді енгізу қажет.

AAA-сервері мен брандмауэр көрсеткіштерінің едәуір жеткілікті көлемі бар, оларды әкімгер баптап күйге келтіре алады. Ең алдымен, AAA-сервері үшін сәйкестендіру хаттамасы анықталуы тиіс. Сонан соң AAA-серверін құру және оны AAA-тобына қосу қажет. Бір топқа бірнеше AAA-сервері тиесілі бола алады. AAA-серверлерін топқа біріктіру жалпы жүйе жұмысының барынша жоғары сенімділігіне қолжеткізуге мүмкіндік береді. Сонымен, мысалы егер бір серверге қолжеткізу мүмкін емес болса (сұраныстарға жауап бермейтін серверге кіру уақытының аралығы қолжетімсіз деп саналады, арнайы таймермен анықталады, бұл келешекте қарастырылады), онда сұраныс келесі AAA-серверіне тапсырылады.

AAA-тобын құру үшін aaa-server командасы қолданылады. PIX брандмауэрін қолданған жағдайда, әкімгердің түрлі деректер ағынымен жұмыс атқару үшін TACACS+ немесе RADIUS серверлерінің түрлі топтарына сұраныс жасау мүмкіндігі бар. Мысалы, кіріс және шығыс деректер қоры үшін TACACS+ жүйесінің екі түрлі сервері қолданылуы мүмкін. AAA командасы сәйкестендіруді, авторизацияны жүзеге асыруға, сондай ақ тапсырыс берілген AAA-сервері арқылы нақты есептік жазбадан шығатын деректер қорын сараптауға ықпал етеді.

Әкімгердің 16 топты басқару мүмкіндігі бар, оның әрқайсысына 16 дейін AAA-серверлері кіруі мүмкін. Осылайша, әкімгер TACACS+ немесе RADIUS жүйесінің 256 серверін басқара алады. Сонымен бірге, бірнеше AAA-серверін қолдану кезінде олар жүйе жұмысын бұзбай, резерв жасау арқылы тоқтап қалулардан қорғау тәртібінде жұмыс атқара алады. Пайдаланушы жүйеге кірген сәтте топта белгіленген біріншіден бастап, серверден бірінші жауап келгенге дейін барлық серверден сұраныс жүргізіледі.

Үнсіз келісім бойынша AAA-серверлерінің екі түрлі хаттамасымен жұмыс қамтамасыз етіледі. Аталған хаттамаларға қолдау көрсету келесі командалармен қосылады:

```
aaa-server tacacs+ protocol tacacs+
aaa-server radius protocol radius
```

Cisco OS операциялық жүйесінің ескі нұсқаларымен жұмыс атқару кезінде әкімгерден AAA-тобын құру талап етілмейді. Осы екі хаттаманы үнсіз келісім бойынша қолдану екі топ құруды алға тартады. Бұл өте ескі операциялық жүйені барынша жаңасына жаңарту (онда AAA-топтарын қолдану қажет болатын) барысында барлық басқа AAA-командалары қолжетімді болатындығын білдіреді.

RADUIS хаттамасы бойынша жұмыс атқару үшін PIX брандмауэр 1645 және 1646 порттарын қолданады. Егер RADUIS-сервері жұмыс атқару үшін 1812 және 1813 порттарын қолданса, онда оның баптап күйге келтіруін 1645 және 1646 порттарын қолдануға өзгерту қажет.

Ааа-server командасының синтаксисі келесідей:

```
ааа-server топ (есім) host IP_мекен-жай кілт timeout
секундтар ааа-server топ protocol хаттама_сәйк
```

3.6 Кестеде ааа-server командасының көрсеткіштері сипатталады.

3.6 Кесте - AAA-server командасының көрсеткіштері

Көрсеткіш	Сипаттама
Топ	Кез келген әріпті-санды таңбаларды қамтуы мүмкін серверлердің топ есімі. Аталған көрсеткіш AAA authentication және AAA accounting өрнегінің байланысы үшін AM-командасында қолданылады.
Есім	Сервермен қолданылатын интерфейстің атауы
hostIP-мекен-жай	TACACS+ немесе RADIUS серверінің IP-мекен-жайы
Кілт	TACACS+серверімен қолданылатын негізгі сөз 127 – жоғары емес таңба құрауы мүмкін; таңбалар регистріне сезімтал. 127-ден соң енгізілген кез келген таңба қабылданбайды. Аталған кілт клиент пен сервер арасында таратылатын деректерді шифрлеу үшін қолданылады. Клиент пен серверде key көрсеткішінің мәні бірдей болуы тиіс. Кілтте бос орын таңбасын қолдануға жол берілмейді, бірақ басқа арнайы таңбалар қолданыла береді.
timeout-секундтары	PIX брандмауэрінің AAA-серверіне қосылудың төрт талпынысының арасында, келесі серверге қосылу талпынысын бастамас бұрын қайталап тарату таймері (retransmit timer) тоқтап қалуды анықтайды. Үнсіз келісім бойынша уақыт аралығы 5 с. болып қабылданған. Аталған көрсеткіштің барынша жоғары шамасы 30 с. құрайды. Мысалы, егер тоқтап қалу уақыты 10 с тең болса, қосылуды орнату мүмкін болса, онда PIX брандауэрі әрбір 10 с сайын деректерді таратудың қайталанған талпыныстарын жүзеге асырады. Осылайша, келесі AAA-серверіне қосылардың алдында 40 с ішінде бірінші AAA-серверімен қосылудың 4 талпынысы жүзеге асырылатын болады.
Protocol	AAA-серверінің түрі. Tacacs+ немесе radius мәнін қабылдай алады.

Топтың есімі - MYTACACS, қолданылатын хаттама - TACAS+. Екінші өрнекте MYTACACS тобындағы сервер анықталады, PIX брандмауэр (inside) арқылы жұмыс атқару үшін AAA-серверінің интерфейсі орнатылады, AAA-серверінің (10.0.0.2) IP-мекен-жайы белгіленеді, кілт (secretkey) орнатылады және сұраныстар арасындағы тоқтап қалу уақыты анықталады

```
pixfirewall(config)#  aaa-server  MYTACACS  protocol  tacacs+
pixfirewall(config)#  aaa-server  MYTACACS  (inside)  host  10.0.0.2
secretkey timeout 10
```

AAA-server командасының көмегімен жүргізілген баптап күйге келтірулерден соң әкімгер authentication командасының көмегімен сәйкестендіруді баптап күйге келтіруі тиіс. Пайдаланушыларды сәйкестендіру қызметі AAA authentication командасы арқылы қосылады немесе өшіріледі. Сәйкестендіру қызметі жұмыс атқарып тұрған кезде Telnet, FTP немесе HTTP қосылуларын құру үшін пайдаланушы өз есімін және құпиясөзін енгізуі тиіс. Енгізілген пайдаланушылық есім және құпиясөз алдыңғы командада анықталған AAA-серверінің көмегімен тексеруден өтеді.

Алайда AAA authentication командасы қауіпсіздік саясатын қамтамасыз ету үшін тағайындалмаған. Пайдаланушының кіру мүмкіндігі бар немесе жоқ объектілерді, сондай ақ қызметтерді және рұқсат етілген IP-мекен-жайларды анықтау үшін AAA-серверлері қолданылады. Telnet, FTP және HTTP хаттамаларымен жұмыс жүргізу кезінде PIX брандмауэрі жүйелік оқиғалардың хаттамаларын белсендіруге немесе белсендірмеуге сұраныс ұсынады. PIX брандмауэрі сәйкестендіру үшін бір қызмет жеткілікті болып баптап күйге келтірілуі мүмкін, бірақ аталған күйге келтірулер сәйкестендіру серверінің баптап күйге келтірулерімен келісімделуі тиіс.

PIX брандмауэрімен жұмыс жүргізу кезінде сәйкестендіру үшін бір желіге тек бір ғана хаттаманы қолдануға мүмкіндік беріледі. Мысалы, егер брандауэр TACACS+ хаттамасының көмегімен, ішкі интерфейске қосылған желімен жұмыс жүргізетін болса, онда тап осы желімен жұмыс жүргізу үшін RADIUS хаттамасы қолданылмайды. Алайда, егер бір желімен жұмыс жүргізу үшін TACACS+ хаттамасы қолданылса, онда PIX брандмауэрі арқылы басқа желімен жұмыс жүргізу үшін RADIUS хаттамасы қолданылады. Кіруді тексеру кезіндегі әдістер келесідей болады:

- tacacs+ -TACACS серверін қолдану;
- none – тексерусіз жеке тұлғаны растау;
- enable – жеке тұлғаны тексеру үшін әкімгердің құпиясөзін (enable password) қолдану;
- krb5 - Kerberos5 серверін қолдану;
- krb5-telnet - Kerberos серверін, оған telnet арқылы қосылып, қолдану;
- line – желіге тіркелген құпиясөзді қолдану;
- local - есімдердің локальді ДҚ қолдану;
- radius - RADIUS серверін қолдану.

3.7 Кестеде AAA authentication командасының көрсеткіштері келтірілген.

3.7 Кесте - AAA authentication командасының көрсеткіштері

Көрсеткіш	Сипаттама
Authentication	Пайдаланушылардың сәйкестендірілуін белсендіруге немесе белсендірмеуге мүмкіндік береді, пайдаланушылық есімді және құпиясөзді сұрайды, сонымен бірге сәйкестендіру серверінің көмегімен енгізілген ақпаратты тексереді. Console көрсеткішімен бірге қолданған жағдайда PIX брандмауэрінің консолді кәбілі арқылы немесе Telnet хаттамасы бойынша брандмауэрдің консоліне кіру үшін сәйкестендіру қызметін қосуға немесе өшіруге мүмкіндік береді. AAA authentication командасын қолданудың алдында сәйкестендіру серверін анықтау үшін aaa-server командасын қолдану қажет.
Include	Белгіленген қызметпен қоса жаңа ереже құрады
Exclude	Белгіленген торап үшін сәйкестендіруден нақты қызметтерді алып тастап, алдыңғы ереже үшін мүмкіндіктер құрады. Мысалы, exclude пайдаланушыға белгіленген тораптармен жұмыс жүргізуді алып тастау үшін порттарды анықтауға мүмкіндік бере отырып, функциялардың алып тастауды қамтамасыз етеді.
Қызмет	Пайдаланушының желіге кіру мүмкіндігін алатын қосымша түрі. Келесі мәндерді қабылдай алады: any, ftp, http немесе telnet. Any мәні барлық TCP-қызметтерінің сәйкестендірілуін қамтамасыз етеді. Пайдаланушы есімді және құпиясөзді енгізуге сұраныс алу үшін келесі хаттамалармен жұмыс жүргізетін қосымшаларды қолдануы тиіс: FTP, HTTP немесе Telnet. (HTTP хаттамасын пайдаланушыдан есімді және құпиясөзді енгізуін сұрау мүмкіндігі бар браузерлермен ғана қолдануға болады).
Inbound	Кіріс қосылуларын сәйкестендіреді. Сыртқы интерфейстерден ішкіге бағытталған қосылулар кіріс қосылулары деп аталады.
Outbound	Шығыс қосылуларын сәйкестендіреді. Ішкі интерфейстерден сыртқыға бағытталған қосылулар шығыс қосылулары деп аталады.
Есім	Пайдаланушының сәйкестендірілуін сұрау үшін қолданылатын интерфейс есімі. Кіру құқын анықтау үшін есім көрсеткішін IP_лок және IP_внеш көрсеткіштерімен бірге қолдану қажет. IP_лок көрсеткіші үнемі қауіпсіздік деңгейі барынша жоғары тораптың IP-мекен-жайын сұрайды, IP_внеш көрсеткіші қауіпсіздік деңгейі барынша төмен тораптырң IP-мекен-жайын анықтайды.

Консолге кіру үшін сәйкестендіру

Арнайы кәбіл арқылы PIX брандмауэрінің консоліне немесе Telnet-консоліне кіру мүмкіндігін алатын пайдаланушылардың сәйкестендірілуін қамтамасыз ету үшін AAA authentication console командасы қолданылады. Сонымен бірге, аталған команданың кейбір көрсеткіштері консолдердің көмегімен жүргізілген PIX брандмауэрінің кенкіндемесіндегі барлық өзгерістерді syslog-серверінде жұрналға енгізуге мүмкіндік береді.

3.8 Кестеде AAA authentication console командасының көрсеткіштері көрсетілген.

3.8 Кесте - AAA authentication console командасының көрсеткіштері

Көрсеткіш	Сипаттама
Serial	Бірінші хабарламаны шығару алдында, кәбілді қолдану арқылы қосылған брандмауэрдің консоліне кіру кезіндегі пайдаланушылық есімді және құпиясөзді сұрау
Enable	Кәбілдің көмегімен немесе Telnet хаттамасы бойынша қосылған консоль арқылы артықшылығы басым тәртіпке кірудің алдында пайдаланушылық есімді және құпиясөзді сұрау
telnet	Бірінші хабарламаны шығару алдында брандмауэрдің Telnet-консоліне кіру кезіндегі пайдаланушылық есімді және құпиясөзді сұрау
Console	Брандмауэр консоліне кіру сәйкестендіруді талап етуін және жүйелік оқиғалар журналы syslog-серверінде сақталатындығын анықтау
Топ	AAA-server командасының көмегімен орнатылатын топ идентификаторы

PIX брандмауэрінің консоліне кіру үшін пайдаланушыларды сәйкестендіру процесі сәйкестендірудің таңдап алынған тәртібіне байланысты. Егер брандмауэрдің enable-құпиясөзі қолданылса, онда қателердің мүмкіндік берілген көлемі үшпен шекетеледі. Егер кәбілді немесе Telnet қолдану арқылы сәйкестендіру тәртібі қолданылса, онда пайдаланушы тіркелу деректерін енгізуді жүйеге кіргенше қайталай алады.

Брандмауэрдің консолі арқылы кіруді сәйкестендіру кезінде, егер сәйкестендіру сервері сәйкестендіру сұранысына жауап алмаған болса, ал диагностика жасау үшін брандмауэр консоліне кіру қажет болса, бұғатталу (deadlock) туындауы мүмкін екенін ескеру қажет. Егер консолден жүйеге кіруге берілген уақыт өтіп кетсе, пайдаланушы пайдаланушылық есімді және брандмауэрдің enable-ұкпиясөзін енгізе отырып, кәбілдің көмегімен қосылған консоль арқылы брандмауэрге кіру мүмкіндігін алады.

Егер TACACS+ немесе RADIUS серверлері қолжетімсіз болса, онда брандмауэрге кіру үшін пайдаланушылық ріх есімін қолдану қажет.

Консолден енгізуге болатын құпиясөз 16 таңбадан аспауы тиіс.

AAA authentication console командасының синтаксисі келесідей:

```
aaa authentication [serial | enable | telnet] console топ
```

Мысалда консолден PIX брандмауэріне кіруді сәйкестендіру тәртіптерін баптап күйге келтіру үшін authentication командасын қолдану бейнеленген:

```
pixfirewall(config)# aaa authentication serial console MYTACACS
pixfirewall(config)# aaa authentication enable console MYTACACS
pixfirewall(config)# aaa authentication telnet console MYTACACS
```

Telnet тобы әкімгерге Telnet хаттамасына сәйкес PIX брандмауэрінің рентасына кіруге қолжеткізудің барлық мүмкіндіктері бар аспаптардың тізімін жоғары қоюға мүмкіндік береді. Операторлық мекеменің нұсқаларында әрі қарай Telnet арқылы PIX брандмауэрінің рентасына 5.0 кіру мүмкіндігі тек ішкі интерфейс арқылы ғана жүзеге асырылған, ал сыртқы интерфейстен рентаға кіруге ешқандай мүмкіндік болмаған. Cisco PIX OS операторлық мекеменің нұсқаларында сыртқы интерфейс арқылы PIX брандмауэрінің рентасына кіру мүмкіндігі туындады. Дегенмен, PIX файерволы IPSec хаттамасының қолдауымен сыртқы интерфейстен келіп түсетін Telnet-ақпаратының ағынын қорғауға кепілдік береді. Осы тәрізді әдіспен, сыртқы сокет арқылы өтетін өзара байланыстың Telnet-сеансын орындау мақсатында, IPSec жүйесін сыртқы интерфейстің PIX брандмауэрімен IP-ақпаратының ағынын құруға мүмкіндік беру арқылы және сыртқы интерфейс үшін telnet жүйесін енгізу арқылы баптап күйге келтіру қажет.

Уәкілеттілігі төмен құралмен (деректерді PIX файерволына қорғаныс деңгейі барынша төмен сокет арқылы тарататын) PIX файервол арқылы уәкілеттілігі барынша жоғарыға (деректерді PIX брандмауэрінен қорғаныс деңгейі барынша жоғары сокет арқылы қабылдайтын) кіру мүмкіндігін беру үшін 2 тәсіл бар.

Дұрыс сұраққа жауап (response to valid request). Құрамның ішкі торабынан юзердің жанына орнатылған сыртқы торапқа келіп түсетін, құрал арқылы файервол үнсіз келісімге сәйкес сұраққа тұжырымды тапсыруға мүмкіндік береді. Шығыс қосылулар туралы деректер үнемі PIX брандмауэрінің трансляциялау кестесінен (translation table) орын алады. Сұраққа тұжырым берудің сыртқы құрал сұранысының жанында PIX файерволы аталған сұрақтың мақсатымен трансляциия слотының (translation slot) орын алуы бойынша трансляция кестесіне тексеру жүргізеді. Егер осы тәрізді жалғағыш бар болса, онда PIX файерволы сұраққа келесі тұжырымды тапсыруға мүмкіндік береді. Өзара байланыстың сеансы аяқталған соң аталған слотты трансляциялау мақсатында ештеме жасамау уақытын (idle timer) сақтаудың арнайы тағайындалған реттегіші орын алады. Cisco OS (5.1 нұсқасының) операторлық мекемесінің рольтаймерін қолдану жағдайында үнсіз келісімге сәйкес 3 сағат шамасына тең.

Ақпаратты таратуды жалғап қоюды баптап күйге келтіру (configure a access-list).

Ақпаратты сыртқы интерфейстен ішкіге таратуды қолдану. Бастапқыда global және nat командаларының қолдауымен динамикалық трансляцияның немесе тұрақты трансляцияның (static тобы) сипаттамаларын баптап күйге келтіру қажет (мұндай жағдайда nat/global нұсқаулары синтездермен еңбек етуге мүмкіндік беретініне, жөнелтушімен қандай табиғи сокет ұсынылатына қарамастан, егер юзерге PIX файервол арқылы осы немесе өзге құралмен жауап-нәтиже қажет болса, ақпараттарды тарату арналарын access-list нұсқауларын қолдаумен баптап күйге келтіру қажет). Ақпаратты тарату арналарын белгілеу мақсатында жөнелтушінің IP-мекен-жайларын немесе IP-мекен-жайларының санаттарын және (немесе) PIX файервол арқылы ақпарат ағынын жөнелтуге мүмкіндік берілген порттар аралығын белгілеу қажет.

Cisco PIX OS операторлық мекемесінің жаңа нұсқалары юзерге қауіпсіздігі төмен тордан барынша зиянсызға кіруді алып тастау мақсатымен 2 қосымша тәсіл береді. Олардың бір ерекшелігі access-list нұсқауын қолдану, өзгесі – кодтау сеансында қабылдаушының немесе жөнелтушінің PIX брандмауэрін қолдану және кодтауды қолдану. Аталған екі тәсіл ақпараттың таралуын жалғауды қалыптастыруды ешбір бұлтартпай орындауды талап етпейді.

PIX брандмауэрі AAA серверлерінің және хаттамаларының келесі түрлерін ұстап қалады:

- контроллерге ақырғы кіру мүмкіндігін басқару тұжырымы (Terminal Access Controller Access Control System Plus - TACACS+);
- Windows NT(CSACS-NT) мақсатымен Cisco қауіпсіз жүрісті басқару компьютері (Cisco Secure Access Control Server (CSACS));
- UNIX(CSACS-UNIX) мақсатымен Cisco қауіпсіз жүрісті басқару компьютері (Cisco Secure Access Control Server (CSACS));
- қашық юзерлерді сәйкестендіру бөлімі (Remote Authentication Dial-In User Service-RADIUS);
- Windows NT (CSACS-NT) мақсатымен Cisco қауіпсіз жүрісті басқару компьютері;
- Windows NT(CSACS-NT) мақсатымен UNIX қауіпсіз жүрісті басқару компьютері;
- Livingston (қазір - LucentTechnologies);
- InterlinkNetwork фирмасының Merit;
- FunkSoftware фирмасының Steel Belted Radius.

Юзердің тіркелген ақпараттарын кэштеу ұзақтығының тапсырмасы үшін олармен өзара байланыс сеансы аяқталған timeout uauth тобы қолданылады. Timeout көрсеткішінің рөлі 2 минут шамасына тең ең төмен өлшемге сәйкес келуі тиіс. Айтарлықтай барлық юзерлердің тіркелген ақпарат кэшін тазарту мақсатында clear uauth тобы қолданылады. Clear uauth нұсқауын қолданудың нәтижесінде юзерлер үнемі келесі қосылулардың жанынан сәйкестендіруден өтіп кететін болады. Юзерлердің тіркелген ақпараттарын кэштеуге тыйым салу мақсатымен timeout uauth0 тобын қолдануға мүмкіндік беріледі.

Timeout uauth командасының кезекті синтаксисі мынаны қамтиды:

```
timeout uauth [чч:мм:сс] [absolute | inactivity]
```

4 Тіршілік қауіпсіздігі

4.1 Оңтайлы еңбек жағдайын құру

Пайдаланушы компьютерлік техникамен жұмыс атқару барысында келесідей қауіпті және зиянды өндірістік факторларға тап болуы мүмкін: электромагниттік сәулелену, статикалық кернеу, электр тогымен жарақаттану, жұмыс орнының жеткіліксіз жарықтануы, ауаның иондануының төмендеуі және т.б. Аталған зиянды өндірістік факторлар компьютерлік техниканы (аталған жағдайда дербес компьютердің) пайдаланушының денсаулығына кері әсер етуі мүмкін.

Компьютерлік техника электр тогымен және өрт қаупімен жарақат алудың әлеуетті қоркөзі болып табылады. Дербес компьютермен жұмыс атқару кезінде өрт қауіпсіздігін қамтамасыз ету шараларына мыналар жатады: жабдықты және электрлік кәбілдерді дұрыс орналастыру. Профилактикалық іс-шаралар ретінде жабық электр желісін, сенімді розеткаларды қолдану, желіге тиесілі жүктемені есептеу және өрт қауіпсіздігі ережелерін сақтау қажет. Сонымен бірге жабдықтың ішкі бөлігін тұрақты түрде шаңнан тазарту қажет. Ұшқын шығып кетуіне жол бермеу үшін розеткалардағы штепсель айырларына жиі тиіспеу қажет.

Жұмыс барысында компьютерлер электростатикалық өріс шығарады, олардың әрекет ету аймағына түрлі заттар енеді. Жүйелік блоктарында ауа айдайтын желдеткіштер жұмыс атқарған кезде электрленбеген тозаңдар сыртқа шығарылады, олар біздің терімізге қонып қана қоймай, сонымен бірге тыныс алу жолдарымызға да өтеді. Монитор экраны да статикалық электр зарядтарының жинақтаушысы болып табылады.

Бүгінгі күні статикалық электрдің адам организміне әсер ету аясы өте кем зерттелген. Зерттеушілердің басым бөлігі адамға статикалық электр әсер еткен сәтте терінің жүйке жасушалары тітіркенеді, сонымен бірге тіндердің иондық құрамында өзгерістер орын алады деп санайды. Мұндай өзгерістердің барлығы ұйқының бұзылуына, шаршаудың жиілеуіне және ашуланшақтыққа жетелейді.

Статикалық электрден қорғау шараларына мыналарды енгізген жөн: ылғалды жинау, жұмыс жайында ауаны қосымша ылғалдандыру (салыстырмалы ылғалдылық 50% жоғары болуы тиіс), жайды желдету, техниканы жерге тұйықтау.

Статикалық электр ауаның ионсыздануының себебі болып табылатындығын атап өткен жөн. Ауаны ионсыздандыру монитор экранына кері зарядты иондардың тартлуымен түсіндіріледі. Ионизация деңгейі төмендесе жұмыс атқару қабілеті кемиді, бас ауру көлемі артады, күш-қуат төмендейді, ойлау және физикалық белсенділік нашарлайды. Жасанды ионизация жүйесін енгізу және ауаны тазарту жағдайды тұрақтандыруға ықпал етеді. Электрлік қауіппен қоса ДК пайдаланушысына электромагниттік әсер

етулер де бар. Компьютердің электромагниттік сәулелену шығаратын екі қоркөзі бар (монитор және жүйелік блок).

Ноутбук пайдаланушылардың басым бөлігі сұйық кристалды мониторлардың есебінен электромагниттік сәулеленумен байланысты мәселенің қаупі мейлінше төмен деп есептеуі дұрыс емес. Алайда жүргізілген зерттеулердің нәтижесінде сұйық кристалды мониторлар да ЭЛТ-мониторлар тәрізді денсаулыққа зиян электромагниттік сәулелену шығаратын, қауіпті қоркөзі болып табылатындығы, бірақ кемдеу көлемде екені анықталды. ДК-мен ауасы тазартылмағанғ яғни желдетілмеген жайда тығыз жұмыс атқару кезінде жағдай күрделене түседі.

Электромагниттік сәулемен жарақаттануға көбінесе көз және ми, ішек-қарын жолы және несеп-жыныстық жүйе, қан алмасу органдары және иммунитет жүйесі бейім болады. Жалпы организмнің жай-күйі нашарлайды. Компьютердің электромагниттік сәулеленуінен қорғану шараларының бірі жиі-жиі таза ауада серуендеу, жайды желдету, дене шынықтыру сабақтары, компьютермен жұмыс атқару ережелерін сақтау, қауіпсіздік стандарттарына және санитарлық нормаларға жауап беретін жақсы техниканы таңдау және қолдану.

ДК шуылөндірісінің деңгейі оның қуаттылығына байланысты. Шуылдың акустикалық тітіркенуді туындату қасиеті бар. Үнемі шуылдың әсеріне ұшырайтын адам, тез шаршайды, ұмытшақ және ашуланшақ болады. ДК шуылдың бастапқы көзі жүйелік блок, құрылғыны салқындатудың желдеткіш жүйелері, процесссор, сонымен бірге CD немесе DVD-жетектері болуы мүмкін. Қажеттілігіне қарай компьютермен ұзақ уақыт бойы жұмыс атқарған кезде санитарлық нормаларды және ережелерді сақтау және шуылдың деңгейін бақылау қажет. Сондай ақ үзілістер жасап отыру қажет.

Компьютермен жұмыс атқару кезінде жарық ерекше маңызды рөл атқарады. Жарық аса жарқыраған болмауы тиіс, қазіргі кездегі ДК жұмыс атқарған сәтте жарығы бәсеңдетілген жарықты қолданған дұрыс. Компьютердің терезеге қатысты орналасуының да маңызы кем емес. Компьютерді терезеден түскен жарық пайдаланушыға тікелей түспейтіндей орналастырған жөн. Себебі бұл жұмыс атқару кезінде көздің шамадан тыс шаршауына жетелеуі мүмкін. Бұдан сақтану үшін тікелей күн сәулесінен қорғайтын желбезек перделерді немесе тығыз матадан жасалған перделерді сатып алуға болады.

Жұмыс атқару барысында ДК пайдаланушысына тікелей әсер ететін жоғарыда көрсетілген зиянды және қауіпті факторлармен қоса компьютермен жұмыс атқаруды дұрыс емес ұйымдастырудан туындайтын басқа да зиянды факторларды атап өткен жөн. Жұмыс орнын ұйымдастыруға барынша назар аудару қажет, себебі пайдаланушының денсаулығы соған байланысты. Егер жақында жүргізілген зерттеулерге сенер болсақ, компьютермен жұмыс атқарудың, онымен жұмыс жасаудың негізгі ережелерін білмеудің, сондай ақ жұмыс орнын дұрыс емес ұйымдастырудың салдары денсаулықтың бұзылуына шамамен 20% ықпал еткен. Жалпы отырып жұмыс атқарудың өзі адамға зиян болып саналады. Ұзақ уақыт бойы бір қалыпта болу бұлшықетті үздіксіз демалмай жұмыс атқаруға мәжбүрлейді. Кем қозғалу ДК пайдаланушыларының

және бағдарламашылардың негізгі күрделі мәселесі. Ұзақ уақыт отырумен туындаған физикалық белсенділіктің төмендеуі салдарынан семіру, көтеу, остеохондроз тәрізді сырқаттардың асқындауы жоғарылайды. Егер компьютермен жұмыс атқару кезінде адам дұрыс емес қалыпта отырса, бүкірейіп немесе алға қарай еңкейіп отырса, оның омыртқасы зақымданады және дискілері жарақаттанады. Жұмыс орнын дұрыс ұйымдастыру, үнемі мүсінді бақылап отыру және демалуға үзілістер жасау және дене шынықтыру жаттығуларын жасау қажет.

Мағынасы ашылған барлық зиянды факторларды ескере отырып, компьютермен жұмыс атқаруды ұйымдастырудың келесідей талаптарын ерекше атап өткен дұрыс:

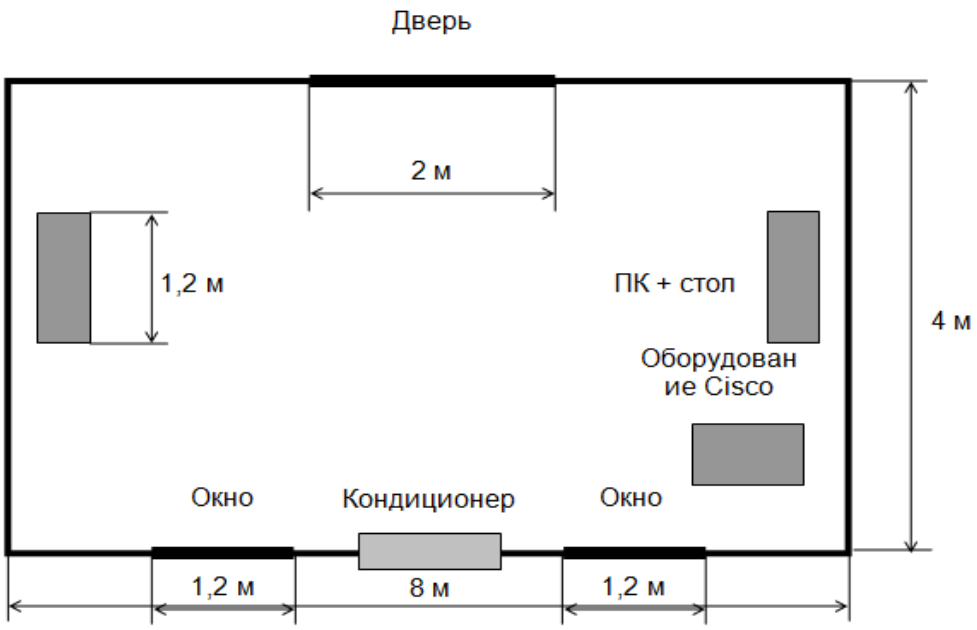
- жұмыс жайында табиғи тәрізді жасанды жарық та болуы тиіс;

жайды ауаны тазарту жүйесімен немесе тиімді желдеткішпен жабдықтау қажет;

- жай сағат сайын желдетілуі тиіс;
- жайда күн сайын ылғалды тазарту жүргізілуі тиіс;
- күн сәулесі тікелей түспеуі терезелерді перделермен немесе желбезек перделермен жапқан дұрыс;
- жасанды жарық жалпы біркелкі болуы тиіс;
- жұмыс үстелінің үстіне монитор, пернетақта, тышқан, сондай ақ құжаттар, кітаптар, қағаздар еркін жайғасуы тиіс;
- орындық биіктігі және арқасының, отырғышының еңкею бұрыштары бойынша қалыпты күйге келтірілуі тиіс;
- монитор экраны көзден кемінде 55-60 см арақашықтықта орналасуы тиіс, сондай ақ ол бөгде жарықты бейнелемейтіндей орнатылуы тиіс. Экранның жарығын дұрыс таңдау қажет;
- күніне кем дегенде бір-екі рет көзге арналған жаттығуларды орындауға нұсқау беріледі;
- пернетақтамен және тышқанмен жұмыс атқарған кезде қолдың дұрыс орналасуы: білектер үстелдің үстіне қатарласып, иыққа тік бұрышпен орналасады;
- жұмыс барысында дененің орналасу күйін, яғни мүсінді үнемі бақылау қажет;
- компьютермен тікелей жұмыс атқару уақыты ауысым ішінде алты сағаттан аспауы тиіс. Жұмыс күнінің ішінде ұзақтығы 10-20 минуттық үзілістер жасап, дене шынықтыру жаттығуларын орындау қажет.

Жұмыс жайының сипаттамалары.

Жұмыс жайы бір жұмыс орнына жабдықталған. Жұмыс жайы жұмыс процесіне әсер етуі мүмкін шуылдың бастапқы көзінен, теміржол бағыттарынан, ірі автомагистралдерден, ұшақ жайынан қашық жайда орналасқан. Жоғарыда баяндалып өткендей, жұмыс орнын ұйымдастырудың маңызды сәті жұмыскердің алып отырған алаңын анықтау болып табылады. Жайды жобалау мысалы 4.1.суретте көрсетілген.



4.1 Сурет – Жайды жоспарлау

Біз келесі сипаттамалары бар жабдықты қолданамыз:

1) Дербес компьютер Intel® Pentium® 4 630 CPU 3.00 GHz / Intel Corporation D945PVS (i945P+SB) / 1024MB DDR2 PC4300 (266MHz) / 160GB SATA Seagate / FDD / k / m / p / SP / LCD 17” Samsung193P.

2) Cisco PIX Firewall 515 E жабдығы.

Процессор - Intel Pentium, 350 MHz.

Оперативтік жад көлемі - 64MB.

Габариттері 24 ×21,1×5,7 .

Электрқоректендіру - ауыспалы кернеу 110/220±10%*B*, 50/ 60 *Гц* жиілігімен. Қуаты 23 *Вт* .

3) Cisco жабдығы.

ADSL router 1E,1ADSL.

Процессор - 1 x Motorola, 50 MHz, RISC.

Оперативтік жад көлемі - 16 MB, Flash 12 MB.

Габариттері 24×21,1×5,1.

Электрқоректендіру - ауыспалы кернеу 110/220±10%*B*, 50 / 60 *Гц* жиілігімен. Қуат 23 *Вт* .

4) Шамдар ЛД64-4 (10 дана), әр шырағданның қуаты 64 *Вт*.

4.2 Өмір сүру әрекетіне төнген қауіп-қатерді сараптау

Барлық электротехникалық жабдықтар өрт қаупінің туындауына әлеуетті қоркөзі болып табылады. Шуылы кем жабдық – мұнда шуылы жоғары түріндегі зиян орын алмайды. Бизнес орталығының ғимаратында орналасқан жұмыс жайы теміржолға немесе ірі автомагистралге, ұшақ жайына тікелей жақын орналаспаған, сондықтан жұмыс процесіне әсер ететін шуылдың сыртқы қоркөзі – жоқ. Электромагниттік сәуле шығарудың жоғары деңгейі жоқ (себебі біз LCD үлгісіндегі мониторларды қолдандық).

Электр тогымен жарақаттану қысқа тұйықталу кезінде, компьютермен епсіз жұмыс атқарғанда, ток өткізу бөліктеріне су тиіп кеткенде орын алуы мүмкін. Қызметкерлерді электр тогымен жарақаттанудан қорғау үшін ток өткізу бөліктері тұйықталған сәтте аппараттың жылдам өшуін қамтамасыз ететін нөлдену қолданылады.

Орындалатын жұмыс жеңіл жұмыстар санатына жатады (физикалық тұрғыда жеңіл, Іа санатты, кемінде

$\frac{Дж}{с}$,

жұмыс отырған күйде, физикалық күшті талап етпей жүргізіледі).

Жұмыс қабатының биіктігі: 725 *мм* , орындық биіктігі: 420 *мм,* МемСТ деректері 4.1.кестеде көрсетілген

4.1 Кесте – Жұмыс түрлері

Жұмыс атауы	Жұмыс тобы	Жұмыс орнын ұйымдастыру кезіндегі жұмыс қабатының биіктігі	Орындық биіктігі
Жеңіл жұмыстар	Іа тобы (отырған күйде орындалатын жұмыс)	725 *мм*	420 *мм*

Жұмыскерлер саны: 2.

Ғимарат: **Шымкент қаласының аумағында** орналасқан мемлекеттік мекеме. Ғимарат бір қабатты.

Жұмыс жайының көлемдері (бөлмелер): ұзындығы $l = 8$ *м* , ені $s = 4$ *м,* биіктігі $h = 3$ *м* .

Жарық өткізу материалының түрі – жалпақ бетті оюлы әйнек. Қабат түрі – болаттан жасалған екіжақты ашылмалы. Салмақ түсетін құрылым жабынының түрі – темірбетоннан жасалған берік фермалар және қақпалар. Күн сәулесінен қорғау құрылғылары – жиналып реттелетін желбезек және қалың перделер.

Әрқайсысының көлемі $1{,}2 \times 1{,}5\ м^2$ екі терезе.

Жасанды жарық - шырағдандар: люминесцентті шамдар ЛД64- 4 (10 дана).

Қабырғаның ішкі әрлеуі - аппақ.

Жұмыс кестесі (жұмыс күнінің ұзақтығы) сағат 09.00 бастап сағат 18.00 дейін. Түскі үзіліс сағат 13.00 бастап 14.00. дейін.

Ғимарат I дәрежелі өрт өзімділігіне жатады (ҚР СНжЕ 2.02-05-2002) [6].

Жайдың жалпы алаңы 32 $м^2$. Жабдықпен және жиһазбен алынып жатқан алаң 1,8 $м^2$.

4.3 Ауаны тазарту жүйесі

Таза ауа - біздің өміріміздің ең міндетті шарттарының бірі. Адам күніне 20 000 литр ауа жұтады. Бізге көңіл-күйіміз бен жұмыс атқару қабілетіміз бірқалыпты болуы үшін озонмен, иондармен және фитонцидтермен байытылған табиғи ауа қажет. Жұмыс жайын желдету үшін ғимараттың құрылысын салу кезінде қарастырылған табиғи желдету арналары және жазда ашық терезелер қолданылады. Алайда мұндай желдеткіш **Шымкент қаласының** климатында жұмыс жайының климаттық көрсеткіштерін нормалар шегінде (4.2 Кесте) ұстап тұруға мүмкіндік бермейді.

4.2 Кесте – Тұрмыстық, қоғамдық және әкімшілік-тұрмыстық жайлардың аумағында қызмет көрсетілетін ауа температурасының оңтайлы нормалары, салыстырмалы ылғалдығы және қозғалыс жылдамдығы (ҚР СНжЕ 2.04.05-91) [7]

Жыл мезгілі	Ауа температурасы, Ос	Ауаның салыстырмалы ылғалдығы, %, жоғары емес	Ауа қозғалысының жылдамдығы, $\overline{м}$, $с$ жоғары емес
Жылы	20 –22	60 –40	0,1
Суық	20 –22	45 – 30	0,1

Жұмыс жайында орнатылған компьютерлер жылу бөлетін қоркөзі болып табылмайды (аппаратурамен өыте шамалы ғана бөлінетін жылу жұмыс жайының микроклиматына ешқандай да әсер етпейді).

Жабдықты пайдаланудың климаттық шарттары толығымен жұмысшы қызметкер үшін нормаланған климаттық шарттарға сәйкес келеді.

Жұмыс жайының климаты қабылданған нормативтерге сәйкес келмейді, сондықтан жайда микроклиматтың бірқалыпты жағдайын қамтамасыз ету үшін оны қосымша желдеткіш жүйесімен жабдықтау қажет.

Жайда желдеткіш орнатылған: Samsung MH18ZC2 (4.2 Сурет).

4.2 Сурет - Samsung MH18ZC2 желдеткіші

Техникалық сипаттамалары:
- қуаты (салқындату) 5260 *Вт*;
- қуаты (қыздыру) 5560 *Вт*;
- пайдаланылатын қуат (салқындату) 890 /1780 *Вт*;
- пайдаланылатын қуат (қыздыру) 870 /1740 *Вт*;
- қоректендіру көзі 220 – 240 / 50(*В* , *Гц*);
- габариттер (ішкі блок)815·298·182*мм*;
- габариттер (сыртқы блок)787·620·320*мм*;
- басқару құрылғысы - бар;
- орнату үлгісі – қабырғаға ілу;
- шуыл деңгейі - 37 / 54 *Дб*;

3

- ауа шығыны - 7,5 $\frac{м}{мин}$ дейін
- 40 $м\,м^2$ дейінгі жайға есептелген.

4.4 Жұмыс жайының жарықтануы

Жұмыс жайының көлемі 1,2 ×1,5 $м^2$ екі терезе түрінде табиғи жарығы бар. Жалпы жарықтандыру жүйесі қолданылады (жасанды жарықтандыру): люминесцентті шамдар ЛД64-4 (10 дана).

4.3 Кестеде жарық қоркөзіне қатысты нормативтер келтірілген.

4.3 Кесте – Жалпы жарықтандыру жүйесі кезіндегі нұсқау берілген жарықтың қоркөздері (ҚР СНжЕ 2.04.-05-2002)

Түсті ажыратуға қойылған талаптар бойынша қарап орындау жұмысының сипаттамасы	Жарық дәрежесі, лк	Жарық қоркөзі температурасының түстер диапазоны T_C, ^0K	Жарық қоркөзінің қолданылатын түрі
Түсті ажыратуға жоғары емес талаптар қойылған кезде түрлі түсті объектілерді ажырату	500 және жоғары	3500 – 6000	ЛБ, (ЛХБ), МГЛ
	300 , 400	3500 – 5500	ЛБ,
	150 , 200	3000 – 4500	ЛБ,(ЛХБ), НЛВД+МТ Л, ДРЛ

Аталған жайда жұмыстарды бірқалыпты орындау үшін қажет жарық дәрежесі 300 *лк*.

4.5 Табиғи жарықты есептеу

Жұмыс орнында бірқалыпты жарықтылықты құру үшін қажет жайдың бүйірлі жарық ойықтарының алаңын есептейміз.

Жайдың көлемі: ұзындығы L=8*м*, ені $B = 4$ *м*, биіктігі H=3*м*. Жұмыс қабатының еден деңгейінен биіктігі $h_{рп}$ $h_{рп} = 0{,}725$ *м*, терезе биіктіктен басталады $h_{но}$, $h_{но}$=0,8*м*, терезе биіктігі $h_о$, $h_о$=1,5*м*.

Жұмыс жайы IV сағаттық белдеуде - Шымкент қаласында орналасқан (жарық климатының белдеуі - IV 50^0 солтүстік енінен және оңтүстікке қарай (**Шымкент, Қарағанды**)).

Жұмыс жайы терезе ойықтарын жобалайтын, жайдың сыртқы қабырғасынан $l_{рт}$, $l_{рт}$ =0,5*м* қашықтықта орналасқан.

Терезе ойығынан 4 *м* қашықтықтағы нүктеде ең төмен жарықтылық болады. Терезенің жалпы алаңын S_0 $м^2$, мына формуламен анықтаймыз:

$$S_0 = \frac{S_п \cdot e_н \cdot \eta_0 \cdot k_з}{100 \cdot \tau \cdot r_1} \qquad (4.1)$$

$S_п$- жай алаңы.

$S_п = 32\ м^2$;

$e_н$- КЕО нормаланған мәні.

Жайда бейненің орташа коэффициенті $\rho_{СР}$ =0,5, біржақты бүйірлі жарықты келесідей қабылдаймыз

$$\frac{L_{рт}}{B} = \frac{0{,}5}{4} = 0{,}125$$

$$r_1 = 1{,}05$$

Жақын маңда көлеңкелейтін ғимарат жоқ, сондықтан есептейміз терезелердің жалпы алаңын 4.1 формула бойынша $k_{зд} = 1$.

$$S_0 = \frac{32 \cdot 1{,}35 \cdot 9{,}6 \cdot 1 \cdot 1{,}2}{100 \cdot 0{,}24 \cdot 1{,}05} = 19{,}75\ м^2.$$

Жарық ойықтарының алаңы $S_{сп}$ = 19,75 $м^2$ тең. Терезе ойықтарының биіктігі 1,5 $м$ тең, сондықтан ұзындығы $S_{сп}$ $h_{сп}$= 13,17 $м$ құрайды.

5 Бизнес жоспар

5.1 Компания және сала

Мемлекеттік қазыналық коммуналды кәсіпорнына қарасты «Шымкент қаласының құтқару Қызметінің» Шымкент қаласының тұрғындарына олардың өміріне, денсаулығына және қауіпсіздігіне қауіп төнетін төтенше жағдайларға тап болған сәтте қосымша жедел жәрдем көрсету мақсатында құрылған.

Қызметтің міндетіне мыналар кіреді:

- зардап шеккендерге жедел жәрдем көрсетуді талап ететін тұрмыстық бақытсыздық жағдайлар және оқиғалар туралы ақпараттар жинау және өңдеу;
- түрлі төтенше жағдайларға тап болған азаматтарға көмек көрсету, тұрғындардың өмір сүру әрекетін қамтамасыз ету мәселелері бойынша тиісті қалалық жедел жәрдем қызметтерімен және басқа да мекемелермен өзара қарым-қатынас жасауды ұйымдастыру;
- аттестациядан өткен апаттық-құтқару жұмыстарының жиынтығын ұйымдастыру және жүргізу;
- төтенше жағдайлар және оқиғалар орын алған кезде қалалық жедел жәрдем және апаттық қызметтердің ақпараттануын қамтамасыз ету;
- түрлі төтенше жағдайларға жедел назар аудару үшін өзінің барлық құрылымдық бөлімшелерінің үнемі дайындығын қамтамасыз ету;
- тұрғындарды қорғау аясында білімді насихаттау, төтенше жағдайлар кезіндегі іс-әрекеттерге тұрғындарды және мекемелерді даярлауға қатысу. Кез келген компанияның ұялы телефондарынан, қалалық таксофондардан Құтқару Қызметінің телефонына қоңырау шалу тегін жүргізіледі.

5.2 Өнімді сипаттау

Дипломдық жұмыстың тақырыбына сәйкес Cisco PIX Firewall 515 E қорғау құрылғысының негізінде корпоративтік периметрді қорғау жүзеге асырылады.

Жобаның негізгі міндеттері:

- ішкі желіні сыртқы әсер етулерден қорғау;
- шығыс және кіріс мүмкіндіктерін бақылау;
- мекеменің бас кеңсесі және филиалдар арасында өзара әрекеттесудің қауіпсіздігі.

Қорғаныс мәселесінің шешімін дұрыс таңдау желінің әлсіздігін кемітеді және осылайша компания қаражатын үнемдейді. Дұрыс шешім желілік

қорғаныс құралдарын енгізу және пайдалану бойынша компанияның жалпы шығындарын кемітуі тиіс.

Cisco PIX Firewall құрылғысы желілерді кең көлемді қауіп-қатерден бастап барлық көлемде қорғау үшін тағайындалған. Ең алдымен, Cisco PIX Firewall буыны біріктірілген сервистердің көлемділігін және тапсырыс берушіге қауіпсіздіктің көптеген механизмдерінің бірмезгілді жұмысына, сонымен бірге желілік инфрақұрылымды пайдалану процесін күрделендірместен, олардың жоғары өнімділігіне және тиімділігіне кепілдік бере отырып, оларды жүйелі басқаруды қамтамасыз етуге жұмылдырылған.

5.3 Өтім нарығын сараптау. Қызметтер нарығын зерделеу

Қазіргі таңда желілердің басым көлемі Internet арқылы біріктірілген. Сондықтан мұндай ауқымды жүйенің қауіпсіз жұмыс атқаруы үшін қауіпсіздіктің нақты шараларын қолдану қажет екені мәлім, себебі айтарлықтай кез келген компьютерден кез келген мекеменің кез келген желісіне кіру мүмкіндігін алуға болады, бұл ретте қауіптілік жоғарылайды өйткені компьютерді бұзу үшін оған физикалық күшпен кіру талап етілмейді.

Желілердің қауіпсіздік мәселесі бүгінгі күні шешілмеген ашық мәселе екенін сенімділікпен айтуға болады, себебі компаниялардың басым бөлігінде қауіпсіздікті қамтамасыз ету мәселесі шешілмеген, дұрыс жолға қойылмаған, нәтижесінде олар қаржылық шығынға ұшырауда.

Аталған жобада Cisco PIX Firewall 515 E желіаралық экранды қолдану арқылы Мемлекеттік қазыналық коммуналды кәсіпорнына қарасты «Шымкент қаласының құтқару Қызметінің» компьютерлік желісінің ақпараттық қауіпсіздік жүйесі зерттеледі.

Желілерді қорғаудың қазіргі қолданыстағы құралдарын салыстыру жүргізілді. Cisco PIX Firewall 515 E жабдығының негізінде желі периметрін қорғау жүйесі зерттелді, брандмауэрде желілік мекен-жайларды трансляциялауды қалыпты күйге келтіру, брандмауэр арқылы шығыс және кіріс мүмкіндіктерін басқаруды қалыпты күйге келтіру жүргізілді.

5.4 Жабдық құрамын және оны таңдауды негіздеу

Cisco PIX Firewall жүйесінің функционалдық ерекшеліктерімен қоса экономикалық және пайдалану басымдылықтары бар. Олардың қатары бағдарламалық қамтамасыз етулер және аппараттық модульдер көмегімен сервистерді күшейту мүмкіндігін, түрлі объектілерде платформаларды стандартизациялауды, қауіпсіздіктің көптеген сервистері үшін басқарудың және мониторингтің жалпы қызметін қолдану арқылы пайдаланудың жеңілдетілген процесін, сондай ақ бұзылымдарды іздеудің және жоюдың жеңілдетілген процесін қамтиды.

Құрылғы сервистерінің бағыты олардың нақты функцияларын және оларды белгіленген инфрақұрылымның ішінде оңтайландыруға мүмкіндік

береді, сол себептен тапсырыс берушілерде Cisco PIX Firewall жүйесінің қорғау құрылғысын желіде қолданылатын көптеген салалар үшін стандарттау мүмкіндігі бар. Басқа жағдайда сол бір ғана тапсырмаларды шешу үшін көптеген түрлі платформалар және басқару жүйелері қажет болар еді.

Мұндай бейімделген тәсіл - «тағайындалуы көп бір құрылғы» - орнатылуы және басқарылуы тиіс платформалардың санын қысқартады, сонымен бірге барлық осы құрылғылар үшін пайдаланудың және басқарудың жалпы ортасын құрады. Құрылғыларды пайдалану мерзімін ұлғайтуға мүмкіндік беретін тиімді басқару осылайша инвестицияларды қорғаудың жоғары деңгейін қамтамасыз етеді.

Нарықпен тексерілген, тиімді VPN құрылысын салу және қорғау механизмдерін біріктірудің, сонымен қатар Gigabit Ethernet-тің және дискісіз (яғни, барынша сенімді) құрылымның флэш-жадпен қосылуларына кіріктірілген қолдау көрсетудің нәтижесінде, Cisco PIX Firewall буынының құрылғысы жоғары өнімділікті, күрделі салымның икемділігін, сенімділігін және қорғанысын қамтамасыз ететін үйлесімді шешімдердің ең үздігі қажет компанияларға мінсіз сәйкес келеді.

5.5 Қаржы салымдарының есебі

Жобаны жүзеге асыру үшін қаржы салымының шығындары негізгі жабдықты сатып алуға, жабдықты құрастыруға, жобалауға және тасымалдауға жұмсалатын шығындарды қамтиды, мына формуламен есептеледі:

$$K_L = K_O + K_M + K_{TP} + K_{ПР} \qquad (5.1)$$

мұнда $К_о$ – негізгі жабдықты сатып алуға жұмсалатын қаржы салым;

$К_{М.}$ – жабдықтықұрастыруға жұмсалатын шығындар;

$К_{ТР}$ - тасымалдау шығындары;

$К_{ПР}$ - жобалау шығындары.

5.1. Кестеде қажетті негізгі жабдықтың жалпы тізімі және оның құны көрсетілген.

5.1 Кесте – Негізгі жабдықты сатып алуға жұмсалатын шығындар сметасы

Жабдықтың аталуы	Бір бірлік үшін баға, теңге (ҚҚС-сыз)	Көлемі	Сомасы, теңге
Intel® Pentium® 4 630 CPU 3.ooGHz / Intel Corporation D945PVS (i945P+SB) / 1024MB DDR2 компьютері	174000	1	174000
Cisco PIX Firewall 515 E Брандмауэрі	688000	1	688000
Cisco 3755/3600 коммутаторы	307400	1	307400
Лазерлі басып шығару құрылғысы: HP LaserJet 1000 Series	34000	1	34000

Тасымалдау шығындары бүкіл жабдық құнының 3% құрайды және мына формуламен есептеледі:

$$Ктр = 0{,}03 \cdot Ко \quad (5.2)$$

$$Ктр = 0{,}03 \cdot 1203400 = 36102 \text{ теңге}$$

Жабдықты жөндеу, іске қосу-күйге келтіру жұмыстарын инженер-монтаждаушылар жүзеге асырады, шығындары бүкіл жабдық құнының 1% құрайды және мына формуламен есептеледі:

$$Км = 0{,}01 \cdot Ко \quad (5.3)$$

$$Км = 0{,}01 \cdot 1203400 = 12034 \text{ теңге}$$

Жобаның жобалау және жете зерттеу шығындары бүкіл жабдық құнының 0,5% құрайды және мына формуламен есептеледі:

$$Кпр = 0{,}005 \cdot Ко \quad (5.4)$$

$$Кпр = 0{,}005 \cdot 1203400 = 6017 \text{ теңге}$$

Жобаны жүзеге асыру бойынша қаржы салымының жалпы сомасы 5.1 формуласына сәйкес 1257553 теңгені құрайды.

5.6 Пайдалану шығындары

Аталған жүйені пайдалануға жұмсалатын ағымдағы шығындар мына формуламен анықталады:

$$С = ФОТ + Сн + А + М + Э + Н \quad (5.5)$$

мұнда ФОТ – еңбекақы төлеу қоры (негізгі және қосымша еңбекақы); Сн әлеуметтік салық;

А – амортизациялық аударымдар;

М – материалдық шығындар;

Э – өндірістік қажеттіліктер үшін электр қуаты.

Еңбекақы төлеу қоры

Желіаралық экранға күтім жасауүшін жүйелік әкімгер мамандығы бар екі қызметкер талап етіледі. Қызметкерлердің еңбекақысы 5.2.кестеде көрсетілген.

5.2 Кесте - Қызметкерлердің еңбекақысы

Лауазымы	Көлемі	Айлық еңбекақы, теңге	Жылдық еңбекақы, теңге
Жүйелік әкімгер	2	150000	1800000

Еңбекақыны төлеу шығындары негізгі және қосымша еңбекақыларды қамтиды және мына формуламен есептеледі:

$$ЕТҚ=Зосн+Здоп \qquad (5.6)$$

мұнда Зосн – негізгі еңбекақы;
Здоп – қосымша еңбекақы.

Негізгі еңбекақы жылына 1800000 теңгені құрайды.

Қосымша еңбекақы негізгі еңбекақының 10% қамтиды және 180000 теңге құрайды.

Осылайша, еңбекақы төлеудің жалпы қоры жылына мынаны құрайды

ФОТ=1800000 +180000 =1980000 теңге

Әлеуметтік салыққа жұмсалатын шығындарды есептеу

ҚР Салық кодексінің 385 бабына сәйкес есептелген кірістің 11% құрайды және мына формуламен есептеледі

$$Сн=0{,}11\cdot(ЕТҚ-ЗҚА) \qquad (5.7)$$

мұнда ЗҚА – зейнетақы қорына жіберілетін аударымдар;
ЕТҚ – еңбекақыны төлеу қоры;
0,11 – әлеуметтік қажеттіліктерге мөлшерлеме.

Зейнетақы қорына жіберілетін аударымдар ЕТҚ-ның 10% құрайды, әлеуметтік салық салынбайды және мына формуламен есептеледі:

$$ЗҚА = 0{,}1\cdot ЕТҚ \qquad (5.8)$$

$$ЗҚА = 0{,}1\cdot 1980000 = 198000$$

Осылайша, әлеуметтік салық 196020 теңгені құрайды.

Амортизацияға жұмсалатын шығындарды есептеу

Байланыс жабдығына қатысты амортизация нормасы 25% құрайды, осыған байланысты амортизациялық аударымдар алынып, келесі формула арқылы есептеледі:

$$A_0 = \frac{H_A \cdot \sum K}{100}$$

мұнда $Н_А$- амортизация нормасы;

∑К – жабдық құны.

Осылайша, амортизациялық аударымдар

A_0= 0.25·1203400=300850 теңге құрайды

Электр қуатына жұмсалатын шығындарды есептеу

Жыл бойы өндірістік қажеттіліктер үшін электр қуатына жұмсалатын шығындар жабдыққа жұмсалатын электр қуатының шығындарын және қосымша қажеттіліктерді қамтиды және мына формуламен есептеледі

$$Э = З_{ЭЛ.ОБОР.} + З_{ДОП.НУЖ.} \quad (5.10)$$

мұнда $З_{ЭЛ.оБоР.}$—жабдық үшін жұмсалатын электр қуатының шығындары; $З_{ДоП.НУЖ.}$ – қосымша қажеттіліктер шығыны.

Жабдыққа жұмсалатын электр қуатының шығындары мына формуламен есептеледі

$$З_{ЭЛ.ОБОР.} = W \cdot T \cdot S \cdot K_{ИСП} \quad (5.11)$$

мұнда W – қолданылатын қуат, W=1,075кВт;

Т – жұмыс уақыты (жылына 1983 сағат);

S - 1 кВтч=14,36 теңгеге тең тариф (ҚҚС-сыз);

$К_{ИСП}$ - пайдалану коэффициенті ($К_{ИСП}$ = 0,9).

$З_{ЭЛ.ОБОР.}$=1,075·1983·14,36·0,9=27550,4 теңге

Қосымша қажеттіліктер шығындары жабдыққа жұмсалатын электр қуаты шығынының 5% құрайды және мына формуламен есептеледі:

$$З_{ДОП.НУЖ.} = 0,05 \cdot З_{ЭЛ.ОБОР.} \quad (5.12)$$

мұнда $З_{ЭЛ.оБоР}$ - жабдыққа жұмсалатын электр қуатының шығыны.

Қосымша қажеттіліктер үшін жұмсалатын электр қуатының

шығындары

$З_{ДОП.НУЖ.}$ =0,05·27550,4=1377,5 теңге

Онда электр қуаты шығындарының сомасы мынаған тең болады

$Э = 27550,4 + 1377,5 = 28927,9$ теңге

Үстеме шығындарды есептеу

Үстеме шығындар барлық шығындардың 50 % қамтиды және мына формуламен есептеледі

$$H = 0,5 \cdot (ФОТ + C_н + A_о + Э) \quad (5.13)$$

Осылайша үстеме шығындар мынаны құрайды

$H = 0,5 \cdot (1980000 + 196020 + 300850 + 28927,9) = 1252899$ теңге

Жылдық пайдалану шығындары есебінің нәтижелері 5.3. кестеде ұсынылған.

5.3 Кесте – Пайдалану шығындары

Көрсеткіш	Сома, теңге
ЕТҚ	1 980 000
Әлеуметтік қажеттіліктер үшін аударымдар (Сн)	196 020
Амортизациялық аударымдар($А_о$)	300850
Электр қуатына жұмсалатын шығындар (Э)	127791
Үстеме шығындар (Н)	1252899
БАРЛЫҒЫ	3857560

5.7 Инвестициялық жобаны жүзеге асыру нәтижесіндегі экономикалық тиімділікті бағалау

Инвестициялық жобаның экономикалық тиімділігін бағалау жобаның экономикалық тиімділік коэффициенті көрсеткішінің негізінде жүргізіледі, бұл мына формуламен есептеледі:

$$_{Р} E \frac{ТК}{Қс} \quad (5.14)$$

мұнда ТТ – таза кіріс;

Қс – күрделі қаржы салымы.

Кәсіпорынның таза кірісі мына формуламен анықталады

$$КТК=Т–ККС \qquad (5.15)$$

мұнда Т – қызметтерді жүзеге асырудан түскен табыс;

ККС – заңды тұлғалардан алынатын корпоративтік кіріс салығы.

Қызметтерді жүзеге асырудан түсетін табыс мына формуламен есептеледі:

$$Т=К –\sum Э \qquad (5.16)$$

мұнда К – бір жылда қызметтерді енгізуден түсетін кіріс;

∑Э – пайдалану шығындары.

2015 - 2016 жылдары Мемлекеттік қазыналық коммуналды кәсіпорнына қарасты «Шымкент қаласының құтқару Қызметінің» корпоративтік желісіне 3 желілік шабуыл ұйымдастырылды, оның ішінде бірінші шабуыл 10000 доллар сомасына (3330000 теңге), екіншісі - 14000 доллар сомасына (4662000 теңге) залал келтірді. Келтірілген залалдың қосындысы 24000 доллар (7992000теңге) құрады.

Cisco компаниясының PIX Firewall желіаралық экранын қорғау құрылғысын енгізген соң қолжеткізілген шартты жылдық кіріс ретінде аталған соманы қабылдаймыз, сонда табыс мынаны құрайды

$$Т =7992000–3857560=4134440 \text{ теңге}$$

Заңды тұлғалардан алынатын корпоративтік кіріс салығы мына формуламен есептеледі

$$ККС =Т·0,2 \qquad (5.17)$$

$$ККС = 4134440· 0,2 =826888 \text{ теңге}$$

Осылайша, салық салудан соң таза табыс 5.12 формуласына сәйкес мынаны құрайды

$$ТТ = 4134440 –826888 = 3307552 \text{ теңге}$$

5.12 формуласына сәйкес жобаның экономикалық тиімділік коэффициент мынаны құрайды

$$Ер = \frac{3307552}{1252899} = 2,64$$

Мына формуламен жобаның өтелу мерзімін есептейміз

$$T = \frac{1}{Ep}$$

мұнда Т – өтелу мерзімі.

$$T = \frac{1}{2,64} = 0,4$$

Жоба 4 ай ішінде өтеледі, келесі жылдары қорғау құрылғысының Cisco PIX Firewall 515 E желіаралық экраны желінің әлсіздігін кемітеді, осылайша компанияның қаражатын үнемдейді.

Мемлекеттік қазыналық коммуналды кәсіпорнына қарасты «Шымкент қаласының құтқару Қызметінің» компьютерлік желісінің ақпараттық қауіпсіздік жүйесін Cisco PIX Firewall 515 E желіаралық экранды қолдану арқылы өңдеу» жобасын жүзеге асырудың экономикалық тиімділігін бағалаудың жиынтық нәтижелері 5.4 кестеде ұсынылған.

5.4 Кесте - Мемлекеттік қазыналық коммуналды кәсіпорнына қарасты «Шымкент қаласының құтқару Қызметінің» компьютерлік желісінің ақпараттық қауіпсіздік жүйесін Cisco/PIX Firewall 515 E желіаралық экранды қолдану арқылы өңдеу» жобасын жүзеге асыру нәтижесіндегі экономикалық тиімділік көрсеткіштері.

Көрсеткіштердің атаулары	Сома, теңге
1. Қаржы салымдары	1257553
2. Табыс (желілік шабуылдардан келетін залал)	7992000
3. Пайдалану шығындары	3857560
5.Өтелі мерзімі	0,4

Қорытынды

Менің дипломдық жобамда Cisco PIX Firewall 515 E желіаралық экранды қолдану арқылы Мемлекеттік қазыналық коммуналды кәсіпорнына қарасты «Шымкент қаласының құтқару Қызметінің» компьютерлік желісінің ақпараттық қауіпсіздік жүйесін зерттеу барысына сипаттама жүргізіледі.

Жобада желінің ақпараттық қауіпсіздігін қамтамасыз ету талаптарымен байланысты, сонымен қатар Cisco PIX желіаралық экрандардың аппараттық құралдары және бағдарламалық қамтамасыз ету мәселелері, Мемлекеттік қазыналық коммуналды кәсіпорнына қарасты «Шымкент қаласының құтқару Қызметінің» компьютерлік желісінің ақпараттық қауіпсіздік жүйесін жүзеге асыру бағыты қарастырылды.

Графикалық бөлігінде бейімделме алгоритміне негізделген Cisco Secure PIX Firewall қосудың құрылымдық сұлбасы, AAA технологиясын қолдану

арқылы желі топологиясы, PIX желіаралық экрандарға тағайындалған қауіпсіздік деңгейлері, PIX желіаралық экрандарда кіріс және шығыс мекен-жайларды трансляциялау, желілік мекен-жайларды трансляциялау, айқын прокси-сервер тәртібінде жұмыс атқару, сонымен бірге брандмауэрді қолдану арқылы желінің құрылымы көрсетілген.

Технико-экономикалық есептеулерде жобаны жүзеге асыруға жұмсалатын шығындар, кәсіпорынның күрделі қаржы салымы анықталды және жобаны енгізу нәтижесіндегі тиімділікке экономикалық баға берілді.

Жобада қызметкерлердің компьютермен жұмыс атқару кезіндегі техника қауіпсіздігіне және еңбекті қорғауға қатысты мәселелері қарастырылды. Жайды жасанды жарықтандыру нормалары, компьютермен жұмыс атқару кезіндегі электр қауіпсіздігі нормалары ұсынылды.

Желінің қауіпсіздік жүйесі қазіргі таңдағы жаңа желілік ортаның интегралды бөлігі болып табылады. Кәсіпорын желісінің қауіпсіздік саясатын жете зерттеу қажеттілігі ең маңызды мәселе болып табылады, мұнда осы зерттелген саясатты орындау үшін қажет, сәйкес келетін бағдарламалық қамтамасыз етулер және құрамдастар анықталуы мүмкін.

Болашақта қауіпсіздікті қамтамасыз ету технологияларының өте күрделі алгоритмдер табылған сәттен бастап жаңаруы және жақсаруы жалғасады.

Cisco пайда болған жаңа технологияларды бақылап отыруға және жаңа бағдарламалық құрамдастарды және функционалдық қасиеттерді, олардың қолжетімділігіне қарай өз өнімдерінің қатарына қосуға талпынады.

Қолданылған әдебиеттер тізімі

1 М.Уэнстром. организация защиты сетей Cisco®. - М.: Издательскийдом «Вильямс», 2005.

2 Д.Чэмпен-мл., Э.Фокс. Брандмауэры Cisco® Secure PIX®. - М.: Издательский дом «Вильямс»,2003.

3 А.Вито. основы организации сетей Cisco. - М.: Издательский дом «Вильямс», 2004.

4 Материалы курса Cisco Fundamental Network Security1.

5 СНиП РК 2.04 - 05 - 2002. Естественное и искусственноеосвещение. Общие требования.

6 Н.И. Баклашов, Н.Ж. Китаева, Б.Д. Терехов. охрана труда на предприятиях связи и охрана окружающей среды. Учебник для высших учебных заведений. - М.: Радио и связь,1989.

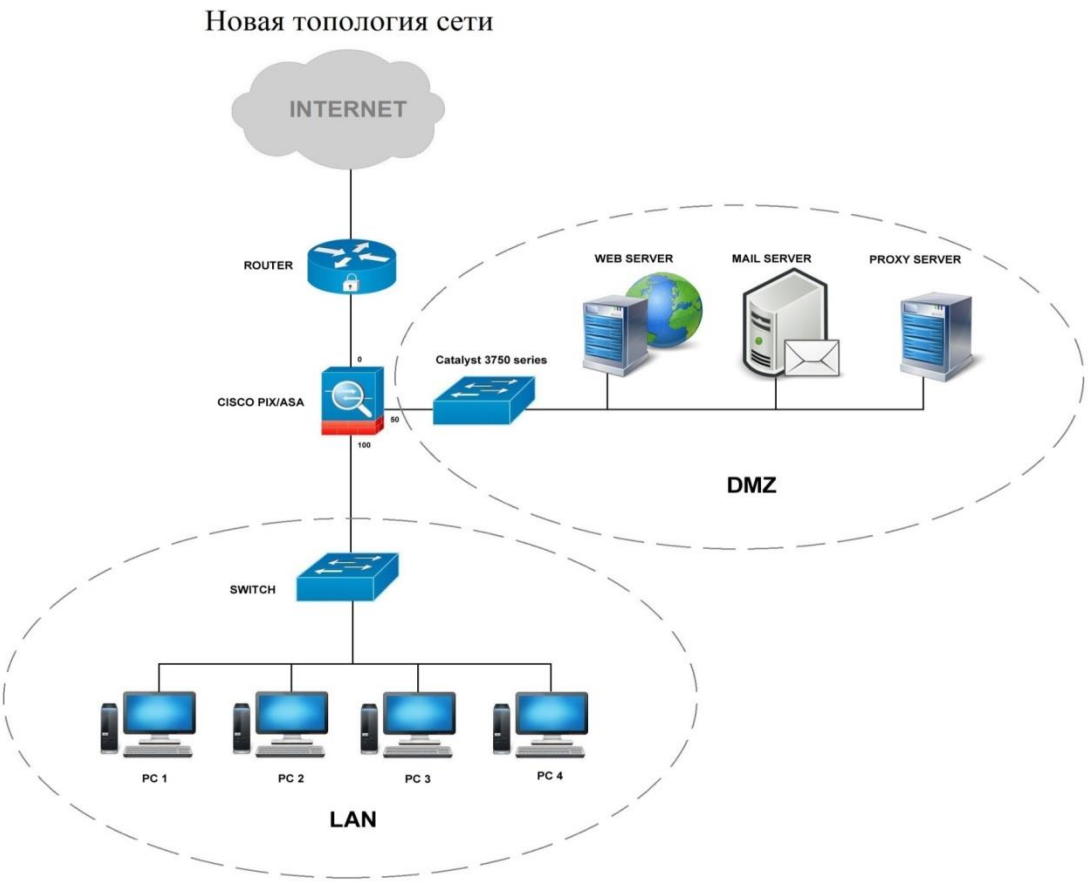
7 Т.Е. Хакимжанова. Безопасность жизнедеятельности. Расчет аспирационных систем: Методические указания к выполнению раздела в дипломных проектах (для студентов всех форм обучения всехспециальностей). - Алматы: АИЭС,2002.

8 СниП РК 3.02 - 04 - 2009. Административные и бытовые здания раздел Противопожарнаябезопасность.

9 С.А. Алибаева. Дипломное проектирование: Методические указания (для студентов всех форм обучения направления. - 652400 - Радиоэлектроника и телекоммуникации). - Алматы: АИЭС,2001.

10 Фирменный стандарт. Работы учебные. общие требования к построению, изложению, оформлению и содержанию. СТ НАО 56023-1910-01-2009. - Алматы: АИЭС,2014.

А Қосымшасы



А.1 Сурет – Кәсіпорын желісінің топологиясы