Дәріс 14. Қол жеткізуді басқару тізімдері (ACL)

ACL тізімі дегеніміз не?

ACL тізімі-бұл маршрутизатордың пакеттерді жіберетінін немесе оларды пакеттің тақырыбындағы ақпаратқа сүйене отырып қалпына келтіретінін анықтайтын бірқатар iOS командалары. ACL тізімдері-Cisco IOS операциялық жүйесінің ең көп қолданылатын ерекшеліктерінің бірі.

ACL конфигурациясына байланысты тізімдер келесі тапсырмаларды орындайды:

Желінің жұмысын жақсарту үшін желілік трафикті шектеңіз. Мысалы, егер корпоративті саясат желіде бейне жазуға тыйым салса, трафиктің осы түрін бұғаттайтын ACL тізімдерін конфигурациялау және қолдану қажет. Мұндай шаралар желіге жүктемені айтарлықтай азайтады және оның өнімділігін арттырады.

ACL тізімдерінің екінші міндеті-трафик ағынын басқару. Қол жеткізуді басқару тізімдерін (ACL) қолдана отырып, сіз осындай жаңартулар көздерінің сенімділігіне кепілдік беру үшін маршруттық жаңартуларды жеткізуді шектей аласыз.

Қол жеткізуді басқару тізімдері желіге кіруге қатысты қауіпсіздіктің негізгі деңгейін қамтамасыз етеді. ACL тізімдері желінің бір бөлігіне бір түйінге қол жеткізе алады және оны басқа түйіндер үшін жаба алады. Мысалы, кадрлар бөлімінің желісіне қол жетімділік шектеулі болуы мүмкін және тек уәкілетті пайдаланушыларға рұқсат етіледі.

ACL тізімдері трафик түріне негізделген трафикті сүзеді. Мысалы, ACL тізімі электрондық пошта трафигіне рұқсат бере алады, бірақ Telnet протоколының барлық трафигін бұғаттай алады.

Қол жеткізуді басқару тізімдері желілік қызметтерге қол жеткізуге рұқсат беру немесе тыйым салу мақсатында түйіндерді сұрыптайды. ACL тізімдерінің көмегімен FTP немесе HTTP сияқты белгілі бір файл түрлеріне кіруге рұқсат беруге немесе тыйым салуға болады.

Әдепкі бойынша, ACL тізімдері маршрутизаторда конфигурацияланбайды, сондықтан маршрутизатор трафикті сүзбейді. Маршрутизаторға кіретін Трафик тек бағыттау кестесінің ақпаратына негізделген. Алайда, егер ACL тізімі интерфейсте қолданылса, маршрутизатор пакеттің жіберілу рұқсатын

анықтау үшін интерфейс арқылы өтетін барлық желілік пакеттерді бағалау арқылы қосымша тапсырманы орындайды.

Трафикке рұқсат беруден немесе тыйым салудан басқа, ACL тізімдерін трафиктің жеке түрлерін талдау, бағыттау немесе өңдеу үшін пайдалануға болады. Мысалы, ACL тізімдерін қолдана отырып, басымдылыққа сәйкес деректерді өңдеуді қосу үшін трафикті жіктеуге болады. ACL тізімдерінің бұл мүмкіндігі концертке немесе спорттық іс-шараға VIP рұқсаттаманың болуына ұқсас. VIP-рұқсатнама таңдалған қонақтарға кіру басымдығы немесе жабық аймаққа кіру сияқты қарапайым билет иелеріне қол жетімді емес артықшылықтар береді.

Пакеттерді сүзу

ACL қол жеткізуді басқару тізімі-бұл қол жеткізуді басқару жазбалары (ACE) деп аталатын рұқсат беру немесе тыйым салу операторларының дәйекті тізімі. Қол жеткізуді басқару жазбалары көбінесе ACL тізім ережелері деп аталады. Желілік трафик кіруді бақылау тізімі (ACL) жұмыс істейтін интерфейс арқылы өткен кезде, маршрутизатор пакеттегі ақпаратты сәйкестікті бақылау тізіміндегі әр жазбамен дәйекті түрде салыстырады. Бұл процесс пакеттерді сүзу деп аталады.

Пакеттерді сүзу кіріс және шығыс пакеттерді талдау негізінде желіге кіруді бақылауды қамтамасыз етеді, содан кейін берілген өлшемдерге сәйкес осы пакеттерді қайта бағыттау немесе тастау. Суретте көрсетілгендей, пакеттерді сүзу 3 және 4 деңгейлерде жүруі мүмкін. Қол жеткізуді басқарудың стандартты тізімдері (ACL) тек 3 деңгейінде сүзуді қамтамасыз етеді. Қол жеткізуді басқарудың кеңейтілген тізімдері (ACL) 3 және 4 деңгейлерде сүзуді қамтамасыз етеді.

Ескерту. Қол жеткізуді басқарудың кеңейтілген тізімдері (ACL) осы курс аясында қарастырылмайды.

IPv4 қол жеткізуді басқарудың стандартты тізімінің (ACL) әр жазбасында сүзу критерийі бар, ол IPv4-бастапқы мекен-жайы болып табылады. Егер маршрутизатор стандартты бақылау тізімін теңшесе

IPv4 кіру (ACL), содан кейін пакетті алғаннан кейін, мұндай маршрутизатор пакеттің тақырыбынан IPv4-көздің мекенжайын алады. Әрі қарай, маршрутизатор бірінші жазбадан бастап қол жеткізуді басқару тізіміндегі (ACL) жазбалардың әрқайсысының мекен-жайымен дәйекті түрде салыстырады. Сәйкестікті анықтағаннан кейін маршрутизатор тиісті

нұсқауларды орындайды — пакеттің өтуіне рұқсат береді немесе тыйым салады. Бұл ретте кіруді бақылау тізіміндегі (ACL) қалған жазбалар талданбайды. Егер IPv4 көзінің Мекен-жайы қол жеткізуді басқару тізіміндегі (ACL) жазбаға сәйкес келмесе, мұндай пакет жойылады.

ACL тізіміндегі соңғы жазба әрқашан трафикке жанама тыйым салады. Бұл нұсқаулық физикалық түрде болмаса да, әр ACL тізімінің соңында автоматты түрде енгізіледі. Жасырын тыйым барлық трафикті бұғаттайды. Жанама тыйымға байланысты ACL-кем дегенде бір рұқсат беру ережесі жоқ тізім барлық трафикті бұғаттайды.

Қол жеткізуді басқару тізімдерінің жұмыс принципі

Қол жеткізуді басқару тізімдері мыналарды қамтамасыз ететін ережелер жиынтығын анықтайды Қол жеткізуді басқару тізімдері интерфейстер қабылдаған пакеттерге, маршрутизатор арқылы берілетін транзиттік пакеттерге, сондай-ақ маршрутизатор интерфейстерінен жіберілетін пакеттерге қосымша бақылауды қамтамасыз ететін ережелер жиынтығын анықтайды. Қол жеткізуді басқару тізімдері маршрутизатор жасаған пакеттерге қолданылмайды.

Кіріс және шығыс трафикке қол жеткізуді басқару тізімдерін (ACL) теңшеуге болады.

Кіріс ACL тізімдері-кіріс пакеттері Шығыс интерфейсіне жіберілмес бұрын өңделеді. Кіріс ACL тізімі тиімді, өйткені пакет қалпына келтірілсе, маршрутты іздеу үшін ресурстарды сақтайды. Егер кіруді бақылау тізіміне (ACL) сәйкес пакеттің өтуіне рұқсат етілсе, онда бұл пакет жіберіледі. Кіруді бақылау кірістері (ACL) тексерілетін пакеттердің жалғыз көзі кіріс интерфейсіне қосылған желі болған жағдайда жақсы жұмыс істейді.

Шығыс ACL тізімдері-кіріс пакеттері Шығыс интерфейсіне бағытталады, содан кейін Шығыс кіру тізімімен өңделеді. Шығыс ACL тізімдері бірдей Шығыс интерфейсіне кірмес бұрын көптеген кіріс интерфейстерден келетін пакеттерге бірдей сүзгілер қолданылған кезде жақсы қолданылады.

ACL-де шаблон маскаларын қолдану туралы негізгі ақпарат

Шаблон маскасын салу

IPv4 ACL тізімдері шаблон маскаларын қолданады. Үлгі маскасы-бұл маршрутизатор сәйкес келетін мекен-жай биттерін анықтау үшін пайдаланатын 32 екілік саннан тұратын жол.

Ішкі желі маскасы сияқты, шаблон маскасындағы "1" және "0" мәндері IPv4 мекен-жайының тиісті биттері қалай өңделетінін анықтайды. Алайда, шаблон маскасында бұл биттер басқа мақсаттарда қолданылады және басқа ережелерді ұстанады.

Ішкі желі маскасында екілік бірліктер мен нөлдер IPv4 мекенжайын бөліктерге бөлу үшін қолданылады-желі мекен — жайы, ішкі желі мекен-жайы және хост мекен-жайы. Үлгі маскасында екілік бірліктер мен нөлдер жеке IPv4 мекен-жайларын немесе IPv4 мекен-жай топтарын сүзу үшін қолданылады. Сүзу ресурстарға кіруге рұқсат береді немесе тыйым салады.

Шаблондық маскалар мен ішкі желі маскалары екілік бірліктер мен нөлдердің сәйкес келуімен ерекшеленеді. Екілік бірліктер мен нөлдерді сәйкестендіру үшін шаблон маскалары келесі ережелерді қолданады:

Үлгі маскасының 0 биті адрестегі биттің тиісті мәніне сәйкес келеді.

Үлгі маскасының 1 биті мекен-жайдағы биттің тиісті мәнін елемейді.

Жоғарыда келтірілген мысалды ескере отырып, екілік нөл сәйкес келуі керек битті, ал екілік бірлік ескерілмейтін битті білдіретінін ұмытпаңыз.

Үлгі маскасы көбінесе кері маска деп аталады. Себебі, ішкі желі маскасынан айырмашылығы, екілік бірлік сәйкестікке тең, ал екілік нөл сәйкестік емес, шаблон маскасында керісінше.

Топтық масканы қолдану

Кестеде 32 биттік IPv4 мекен-жайына 0.0.255.255 шаблон маскасын қолдану нәтижелері көрсетілген. Есіңізде болсын, екілік нөл сәйкес келетін мәнді көрсетеді.

Ескерту. IPv4 үшін ACL тізімдерінен айырмашылығы, IPv6 үшін ACL тізімдері шаблон маскаларын пайдаланбайды. IPv6 протоколында бастапқы немесе тағайындалған IPv6 мекен-жайының қай бөлігі сәйкес келетінін көрсету үшін префикс ұзындығы қолданылады.

Үлгі маскасының мысалдары

IPv4 ішкі желілеріне сәйкес келетін шаблондық маскаларды есептеу

Үлгі маскасын есептеу белгілі бір тәжірибені қажет етуі мүмкін. Үлгі маскаларының үш мысалы.

Үлгі маскасының бірінші мысалында 192.168.1.1 IPv4 мекен-жайындағы әр бит дәл сәйкес келуі керек.

Екінші мысалдағы шаблон маскасының шарты-сәйкестіктердің болмауы.

Үлгі маскасының үшінші мысалында 192.168.1.0/24 желісіндегі кез-келген түйін сәйкес келеді деп көрсетілген.

Полигондарға сәйкес келетін шаблондық маскаларды есептеу

1-мысалда бірінші екі октет және үшінші октеттің алғашқы төрт биті дәл сәйкес келуі керек. Үшінші октеттегі соңғы төрт бит және соңғы октет кез-келген рұқсат етілген сан болуы мүмкін. Нәтиже-192.168.16.0-ден 192.168.31.0-ге дейінгі желілердің ауқымын анықтайтын маска.

2-мысалда шаблон маскасы көрсетілген, оның алғашқы екі октеті мен үшінші октеттің соңғы биті сәйкес келеді. Үшінші октеттегі соңғы октет пен алғашқы жеті бит кез-келген рұқсат етілген сан болуы мүмкін. Нәтиже-192.168.0.0 негізгі желісінің тақ ішкі желілерінен барлық түйіндерге мүмкіндік беретін немесе тыйым салатын маска.

Үлгі маскасын есептеу

Шаблон маскаларын есептеу белгілі бір қиындықтарды тудыруы мүмкін. Қарапайым әдіс-ішкі желі маскасын 255.255.255.255-тен алу.

Үлгі маскасын есептеу. 1 мысал

Бірінші мысалда сіз 192.168.3.0 желісіндегі барлық пайдаланушыларға кіруге рұқсат бергіңіз келеді делік. Ішкі желі маскасы 255.255.255.0 болғандықтан, сіз 255.255.255.255 алып, 255.255.255.0 ішкі желі маскасын алып тастай аласыз. Нәтиже-0.0.0.255 шаблон маскасы.

Үлгі маскасын есептеу. Мысал 2

Екінші мысалда сіз 192.168.3.32/28 ішкі желісіндегі 14 пайдаланушыға желіге кіруге рұқсат бергіңіз келеді делік. IPv4-ішкі желіде 255.255.255.240 ішкі желі маскасы бар. Демек, 255.255.255.255-тен 255.255.255.240 ішкі желі маскасын алып тастау керек. Нәтиже-0.0.0.15 шаблон маскасы.

Үлгі маскасын есептеу. 3 мысал

Үшінші мысалда сіз 192.168.10.0 және 192.168.11.0 желілеріне сәйкес келетін шаблон маскасын есептегіңіз келеді делік. Тағы да 255.255.255.255 алыңыз

және ішкі желі маскасын алыңыз, бұл жағдайда 255.255.254.0 болады. Нәтиже-0.0.1.255.

Осындай нәтижені төмендегі командалардың көмегімен алуға болады:

R1(config)# access-list 10 permit 192.168.10.0 0.0.1.255

R1(config)# access-list 10 permit 192.168.11.0 0.0.1.255

Неғұрлым тиімді әдіс-шаблон маскасын келесідей конфигурациялау:

R1(config)# access-list 10 permit 192.168.10.0 0.0.1.255

Желілерді 192.168.16.0/24-тен 192.168.31.0/24-ке дейін сүзу керек делік. Осы желілерді қорытындылау кезінде біз 192.168.16.0/20 аламыз. Бұл жағдайда дұрыс шаблон маскасы 0.0.15.255 болады. Мұндай масканы қолдана отырып, сіз төменде көрсетілгендей қол жеткізуді басқару тізіміне (ACL) бір және ең тиімді жазба жасай аласыз.

R1(config)# access-list 10 permit 192.168.16.0 0.0.15.255

Үлгі маскасының кілт сөздері

Работа с десятичными ұсыныстары бар екілік шаблонной маскалар мүмкін энергияны. Хост және кез-келген кілт сөздер жиі қолданылатын шаблон маскасын анықтауға көмектесу арқылы тапсырманы жеңілдетеді. Бұл кілт сөздер белгілі бір түйінді немесе бүкіл желіні анықтаған кезде шаблон маскаларын енгізу қажеттілігін жояды. Бұл кілт сөздер ACL тізімін оқуды жеңілдетеді, бұл көзге немесе мақсатқа арналған өлшемдерге қатысты көрнекі кеңестер береді.

Хост кілт сөзі 0.0.0.0 маскасы үшін қолданылады. Бұл маска IPv4 мекен - жайының барлық биттерін сәйкестендіруді білдіреді. Осылайша, жалғыз хост мекен-жайы сүзіледі.

Кез-келген кілт сөзді IPv4 мекен-жайы мен 255.255.255.255 маскасының орнына қолдануға болады. Бұл маска бүкіл IPv4 мекенжайын елемеуге немесе кез келген мекенжайды қабылдауға нұсқайды.

Мысал 1. Жалғыз IPv4 мекен-жайына сәйкес келетін шаблон маскасы.

Суретте көрсетілген 1-мысалда 192.168.10.10 0.0.0.0 енгізудің орнына host 192.168.10.10 жолын енгізуге болады.

Мысал 2. Кез-келген IPv4 мекен-жайына сәйкес келетін шаблон маскасы.

Суретте көрсетілген 2-мысалда 0.0.0.0 255.255.255.255 нұсқауларының орнына кез-келген кілт сөзді бөлек енгізуге болады.

ACL тізімдерін құру бойынша жалпы ұсыныстар

ACL тізімдерін жасау қиын болуы мүмкін. Әр интерфейс үшін осы интерфейске кіруге немесе шығуға рұқсат етілген трафик түрлерін басқаруға қажетті бірнеше ережелер болуы мүмкін. Суреттегі маршрутизаторда IPv4 және IPv6 үшін конфигурацияланған екі интерфейс бар. Егер екі протоколға да екі интерфейсте де, екі бағытта да ACL тізімдері қажет болса, онда сізге 8 бөлек ACL тізімін жасау керек. Әр интерфейсте төрт ACL тізімі болады: IPv4 протоколына арналған екі тізім және IPv6 протоколына арналған екі тізім. Әр протоколға кіріс трафигі үшін бір ACL тізімі және шығыс трафигі үшін біреуі қажет.

Ескерту. Қол жеткізуді басқару тізімдері екі бағытта да конфигурацияланудың қажеті жоқ. ACL тізімдерінің нөмірлері және олардың интерфейсте қолданылатын бағыттары мәлімделген талаптарға байланысты.

ACL тізімдерін пайдалану бойынша бірнеше ұсыныстар бар.

Интернет сияқты ішкі және сыртқы желілер арасында орналасқан маршрутизаторлардың желіаралық экрандарында ACL тізімдерін қолданыңыз.

Ішкі желінің белгілі бір бөлігіндегі кіріс немесе шығыс трафикті басқару үшін желінің екі сегменті арасында орналасқан маршрутизатордағы ACL тізімдерін қолданыңыз.

Қосымша ACL тізімдерін шекаралық маршрутизаторларда, яғни желілер шекарасында орналасқан маршрутизаторларда теңшеңіз. Бұл негізгі буферді сыртқы желіден немесе аз басқарылатын және сезімтал желі аймақтары арасында қамтамасыз етеді.

Немесе шекаралық маршрутизатор интерфейсінде конфигурацияланған әрбір желі протоколы үшін ACL тізімдерін теңшеңіз.

Қол жеткізуді басқару тізімдерін қолдану ережелері (ACL)

Протоколға, бағытқа, интерфейске қол жеткізуді басқарудың бір тізімін теңшеуге болады:

Бір ACL-бір протоколға арналған тізім-ACL интерфейсіндегі трафик ағынын басқару үшін-интерфейсте жұмыс істейтін әр хаттама үшін тізім анықталуы керек.

Бір бағытқа арналған бір ACL тізімі-ACL тізімдері бір интерфейстің бір бағытындағы трафикті бір уақытта басқарады. Шығыс және кіріс трафигін басқару үшін екі бөлек ACL тізімі жасалуы керек.

Бір интерфейске арналған бір ACL тізімі-ACL тізімдері бір интерфейстегі трафикті басқарады, мысалы GigabitEthernet 0/0.

ACL тізімдерін құру бойынша ұсыныстар

ACL тізімдерін жасау егжей-тегжейге назар аударуды және мұқият болуды қажет етеді. Қателер тоқтап қалуға, іздеуге және ақаулықтарды жоюға, сондай-ақ Желілік қызметтердің дұрыс жұмыс істемеуіне байланысты ауыр зардаптарға және қосымша шығындарға әкелуі мүмкін. ACL тізімін орнатпас бұрын негізгі жоспар құру керек.

ACL тізімдерін қайда орналастыру керек

ACL тізімін дұрыс орналастыру желінің тиімділігін арттыруы мүмкін. Артық трафикті азайту үшін ACL тізімін орналастыруға болады. Мысалы, қашықтағы тағайындалған орын қабылдамайтын трафикті осы бағытқа бағыт бойынша желілік ресурстар арқылы жібермеу керек.

Әрбір ACL тізімін максималды тиімділікті көрсететін жерге орналастыру керек. Мұнда ACL тізімдерін орналастырудың негізгі ережелерінің тізімі берілген:

Кеңейтілген ACL-тізімдер - кеңейтілген ACL-тізімдер сүзілетін трафик көзіне мүмкіндігінше жақын орналасуы керек. Осылайша, қалаусыз трафик желі инфрақұрылымынан өтпей - ақ, бастапқы желіге жақын орналасады.

Стандартты ACL тізімдері-қол жеткізуді басқарудың стандартты тізімдері тағайындалған мекен-жайларды анықтамайтындықтан, олар тағайындалған жерге мүмкіндігінше жақын орналастырылады. Стандартты ACL тізімін трафик көзіне орналастыру осы трафиктің басқа желілерге ACL тізімі қолданылатын интерфейс арқылы жетуіне жол бермейді.

Қол жеткізуді басқару тізімін (ACL) орналастыру және соның салдарынан тізім түрі келесі факторларға да байланысты болуы мүмкін.

Желілік әкімшінің басқару саласы-ACL тізімін орналастыру желілік әкімшінің бастапқы желіні де, тағайындалған желіні де басқаратындығына байланысты болуы мүмкін.

Қосылған желілердің өткізу қабілеті-көзден қалаусыз трафикті сүзу трафиктің тағайындалған жерге барар жолда желінің өткізу қабілетін төмендеткенге дейін берілуіне жол бермейді. Бұл әсіресе өткізу қабілеті төмен желілерде өте маңызды.

Конфигурацияның қарапайымдылығы-желілік әкімшінің бірнеше желілерден келетін трафикке тыйым салуы үшін, бір әдіс тағайындалған жерге жақын маршрутизаторда бір стандартты ACL тізімін пайдалану болуы мүмкін. Бұл әдістің кемшілігі - бұл желілерден алынған трафик өткізу қабілетін пайдаланады. Кеңейтілген ACL тізімін трафик жүретін әр маршрутизаторда қолдануға болады. Бұл трафик көзін сүзу арқылы өткізу қабілетін сақтайды, бірақ бұл бірнеше маршрутизаторларда кеңейтілген ACL тізімдерін жасауды қажет етеді.

Ескерту. ICND1/CCENT емтихан бағдарламасында қол жеткізуді басқарудың кеңейтілген тізімдерімен (ACL) жұмыс істеу туралы сұрақтар жоқ. Дегенмен, сіз стандартты ғана емес, сонымен қатар кеңейтілген қол жеткізу тізімдерін (ACL) орналастырудың жалпы принциптерін түсінуіңіз керек. CCNA-ны сәтті сертификаттау үшін келесі жалпы ережені есте ұстаған жөн: қол жеткізуді басқарудың кеңейтілген тізімдері (ACL) көзге мүмкіндігінше жақын орналастырылады; қол жеткізуді басқарудың стандартты тізімдері (ACL) межелі жерге мүмкіндігінше жақын орналастырылады.

Стандартты ACL тізімін орналастыру

Суретте көрсетілген топология қол жеткізуді басқарудың стандартты тізімін (ACL) орналастыру принциптерін көрсетеді. Әкімші трафиктің 192.168.10.0/24 желісінен 192.168.30.0/24 желісіне өтуіне тыйым салғысы келеді.

Суретте стандартты ACL тізімін тағайындалған жерге мүмкіндігінше жақын орналастыруға арналған негізгі нұсқауларға сәйкес стандартты ACL тізімін пайдалануды реттеуге болатын екі R3 маршрутизатор интерфейсі көрсетілген:

R3 маршрутизаторының S0/0/1 интерфейсі-192.168.10.0/24 желісінен S0/0/1 интерфейсіне трафиктің алдын алу үшін стандартты ACL тізімін пайдалану, сонымен қатар 192.168.30.0/24 желісіне және 192.168.31.0/24 желісін қоса

алғанда, R3 маршрутизаторы қол жеткізе алатын басқа желілерге бұл трафикке жол бермейді. ACL тізімінің мақсаты тек 192.168.30.0/24-ке арналған трафикті сүзу болғандықтан, стандартты ACL тізімін бұл интерфейсте қолдануға болмайды.

 G0 / 0 R3 интерфейсі-G0/0 Шығыс интерфейсінің трафигін басқарудың стандартты тізімін қолдану 192.168.10.0/24-тен 192.168.30.0/24-ке дейінгі желілерден пакеттерді сүзуге әкеледі. Бұл тізімді қолдану R3 қол жетімді басқа желілерге әсер етпейді. 192.168.10.0/24 желісіндегі пакеттер әлі де 192.168.31.0/24 желісіне қосылуы керек.

IPv4 стандартты нөмірленген кіруді басқару тізімінің (ACL) синтаксисі

Cisco маршрутизаторында стандартты нөмірленген ACL тізімдерін пайдалану үшін алдымен стандартты ACL тізімін жасап, содан кейін оны интерфейсте іске қосу керек.

Access-list Ғаламдық конфигурация командасы 1-ден 99-ға дейінгі нөмірі бар стандартты ACL тізімін анықтайды. Cisco IOS 12.0.1 нұсқасында бұл ауқым кеңейтілді; стандартты ACL тізімдері үшін 1300-ден 1999-ға дейінгі нөмірлерді пайдалануға болады. Бұл 798 мүмкін стандартты ACL тізімдерін жасауға мүмкіндік береді. Осы қосымша нөмірлері бар тізімдер IPv4 қол жеткізуді басқарудың қосымша тізімдері (ACL) деп аталады.

Стандартты ACL тізімінің толық синтаксисі:

Router (config)# access-list кіру тізімінің нөмірі { deny | permit / remark } көзі [source-wildcard] [log]

Кіруді бақылау тізіміндегі жазбалар белгілі бір хост мекен-жайына немесе осындай мекен-жайлар ауқымына қатысты трафикке рұқсат береді немесе тыйым салады. 10 нөмірлі кіруді басқару тізімінде (ACL) 192.168.10.10 IP мекен-жайы бар хост үшін трафикті қамтамасыз ететін host кілт сөзіне негізделген жазба жасау үшін келесі пәрменді енгізу керек:

R1(config)# access-list 10 permit host 192.168.10.10

10 / 192.168.10.0 / 24 желісіндегі барлық IPv4 мекенжайларына рұқсат беретін нөмірленген ACL тізімінде IPv4 мекенжайларының ауқымын шешетін жазбаны жасау үшін келесі пәрменді енгізу қажет:

R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255

ACL тізімін жою үшін no access-list Ғаламдық конфигурация пәрмені қолданылады. Show access-list пәрменін енгізу ACL тізімінің 10 жойылғанын растайды.

Әдетте, әкімші қол жеткізуді басқару тізімін жасаған кезде әр жазбаның қолданылуы белгілі және айқын болады. Алайда, әкімші мен басқа пайдаланушылар кездесуді еске түсіруі үшін

бір немесе басқа жазба, тиісті пікірлерді қосу керек. ACL тізімдерін құжаттау және оқуды жеңілдету үшін remark кілт сөзі қолданылады. Пікірдің ұзындығы 100 таңбамен шектелген. Show running-config пәрменін пайдаланып ACL тізімінің конфигурациясын қарау кезінде тиісті түсініктеме көрсетіледі.

Интерфейстерге қол жеткізуді басқарудың стандартты тізімдерін (ACL) қолдану

Қол жеткізуді басқарудың стандартты тізімін (ACL) жасағаннан кейін оны интерфейс параметрлері режимінде енгізілген ip access-group пәрменін қолдана отырып интерфейспен байланыстыру керек:

Router(config-if)# ip access-group { access-list-number | access-list-name } { in | out }

Интерфейстен барлық ACL тізімін жою үшін алдымен интерфейске no ip access-group пәрменін енгізу керек, содан кейін ғаламдық no access-list пәрменін енгізу керек.

Бұл ACL тізімі трафикті тек 192.168.10.0 бастапқы желісінен S0 / 0 / 0 интерфейсінен жіберуге мүмкіндік береді. 192.168.10.0-тен басқа желілерден Трафик бұғатталған.

Бірінші жол кіруді бақылау тізімін 1 кіру тізімі ретінде көрсетеді. Осылайша, берілген параметрлерге сәйкес трафикке рұқсат етіледі. Бұл жағдайда IPv4 мекен-жайы және бастапқы желіні анықтайтын шаблон маскасы-192.168.10.0 0.0.0.255. Қол жеткізуді басқару тізімінің (ACL) соңында access-list 1 deny 0.0.0.0 255.255.255.255 немесе access-list deny any жолына тең deny all жасырын тыйым салынғанын есте ұстаған жөн.

Ip access-group 1 out интерфейсінің конфигурация командасы ACL 1-ді Serial 0/0/0 интерфейсіне Шығыс сүзгі ретінде байланыстырады және байланыстырады.

Сондықтан, ACL тізімі 1 R1 маршрутизаторы арқылы 192.168.10.0/24 желісіндегі түйіндерге ғана шығуға мүмкіндік береді. Сонымен қатар, ол кез-келген басқа желіге тыйым салады, соның ішінде 192.168.11.0.

IPv4 стандартты нөмірленген кіруді басқару тізімінің (ACL) мысалдары

Бірінші пәрмен 1-тізімнің ACL алдыңғы нұсқасын жояды. Кіруді бақылау тізімінің келесі жазбасы желіде орналасқан PC1 Түйініне тыйым салады 192.168.10.10. 192.168.10.0 / 24 желісіндегі барлық басқа хосттарға рұқсат етіледі. Тағы да, бас тартудың жанама жазбасы әр басқа желіге сәйкес келеді.

ACL тізімі S0/0 / 0 интерфейсінің шығыс бағытында қайта қолданылады.

белгілі бір түйінге тыйым салатын қол жеткізуді басқару тізімі (ACL) көрсетілген. Бұл ACL тізімі алдыңғы мысалды алмастырады. Бұл мысалда PC1 түйінінен трафик әлі де бұғатталған, бірақ қалған трафик рұқсат етілген.

Алғашқы екі команда алдыңғы мысалдағы командаларға ұқсас. Бірінші команда ACL 1-дің алдыңғы нұсқасын жояды, ал келесі кіру тізімінің командасы желіде орналасқан PC1 Түйініне тыйым салады 192.168.10.10.

Үшінші команда қайтадан енгізілді-оған барлық басқа түйіндер рұқсат етіледі. Бұл алдыңғы жолда тыйым салынған PC1 компьютерін қоспағанда, 192.168.10.0/24 желісіндегі барлық хосттарға рұқсат етілгенін білдіреді.

Қарастырылған ACL тізімі G0 / 0 интерфейсінің кіріс бағытында қолданылады. Сүзгі тек Lan 192.168.10.0/24 G0/0-ге әсер ететіндіктен, ACL тізімін кіріс интерфейсінде қолдану тиімдірек болады. Қол жеткізуді басқару тізімін (ACL) шығыс бағытта s0/0/0-ге қолдануға болады, алайда R1 маршрутизаторы барлық желілердің пакеттерін, соның ішінде 192.168.11.0/24-ті тексеруге мәжбүр болады.

IPv4 стандартты қол жеткізуді басқару тізімінің (ACL) синтаксисі

ACL тізімдеріне атау беру белгілі бір тізімнің функциясын түсінуді жеңілдетеді. Нөмірдің орнына ACL тізіміне атау берген кезде конфигурация режимі мен пәрмен синтаксисі аздап өзгереді.

Қадам 1. Аталған ACL тізімін жасау үшін IP access-list Ғаламдық конфигурация режимінің пәрменін іске қосыңыз. ACL тізімдерінің атаулары әріптік-сандық таңбалардан тұрады, олар регистрге сезімтал және ерекше болуы керек. IP access-list standard атауы пәрмені стандартты қол жеткізуді басқару тізімін (ACL) жасау үшін қолданылады. Осы пәрменді енгізгеннен кейін маршрутизатор стандартты (std) деп аталатын (NaCl) қол жеткізуді

басқару тізімінің (ACL) конфигурация режимінде болады, бұл екінші пәрмен жолының шақыруымен дәлелденеді (1-сурет).

Ескерту. Нөмірленген қол жеткізуді басқару тізімдері (ACL) үшін ғаламдық access-list конфигурация пәрмені қолданылады, ал IPv4 қол жеткізуді басқару тізімдері (ACL) үшін IP access-list пәрменін пайдалану керек.

Қадам 2. ACL деп аталатын тізімдерді конфигурациялау режимінде пакеттің жіберілуін немесе қабылданбауын анықтау үшін permit немесе deny пәрмендерін қолданыңыз. Қол жеткізуді басқару тізіміне (ACL) remark кілт сөзін қолдана отырып түсініктеме қосуға болады.

Қадам 3. Ip access - group name командасын қолдана отырып, интерфейске кіруді бақылау тізімін (ACL) қолданыңыз. Пакеттерге кіруді бақылау тізімін (ACL) қашан қолдану керектігін көрсетіңіз — пакеттерді интерфейске (in) алған кезде немесе пакеттерді интерфейстен (out) жіберген кезде.

ACL тізімдерінің аттарын бас әріптермен көрсету қажет емес, бірақ бұл ағымдағы конфигурацияның шығуын қарау кезінде оларды көрнекі етеді. Сондай-ақ, бірдей атаулармен, бірақ бас әріптер мен кіші әріптердің қолданылуымен ерекшеленетін екі түрлі ACL тізімдерін кездейсоқ құру мүмкіндігін азайтады.

Стандартты ACL тізімдерін өңдеу

Реттік жазба нөмірлерін қолдана отырып, жеке жазбаларды оңай енгізуге немесе жоюға болады. Бұл әдісті стандартты деп аталатын ACL тізімдерін өңдеу кезінде де қолдануға болады.

 Show командасының шығуында ACL тізіміне "NO_ACCESS" атауы берілгенін көруге болады, онда IPv4 мекен-жайы 192.168.11.10 бар жұмыс станциясына кіру ережелерін көрсететін екі нөмірленген жол бар.

Қол жеткізуді басқару тізімінің (ACL) конфигурация режимінде жазбаларды енгізуге және жоюға болады.

Басқа жұмыс станциясына тыйым салынған жазбаны қосу үшін нөмірленген жолды қосу қажет. Бұл мысалда IPv4 мекен-жайы 192.168.11.11 жаңа реттік нөмірі 15 бар жұмыс станциясы қосылады.

Show командасының қорытынды нәтижелері жаңа жұмыс станциясына кіруге тыйым салынғанын растайды.

Ескерту. Қол жеткізуді басқарудың аталған тізімін (ACL) конфигурациялау режимінде жеке жазбаларды тез жоюға мүмкіндік беретін no sequence-number пәрменін пайдалануға болады.

Кіруді бақылау тізімдерін тексеру

Show IP interface пәрмені интерфейстегі ACL тізімін тексеру үшін қолданылады. Бұл команданың шығысына кіру тізімінің нөмірі немесе атауы және ACL тізімі қосылған бағыт кіреді. Шығарылған деректер R1 маршрутизаторында S0/0/0 Шығыс интерфейсіне қолданылатын 1 қатынауды басқару тізімі (ACL), сондай-ақ G0/0 интерфейсіне қолданылатын NO_ACCESS тізімі бар екенін көрсетеді.

Access-class командасы

Әкімшілік желілердің қауіпсіздігін арттыру үшін VTY-ге кіруді шектеуге болады. Маршрутизаторда exec процесіне қашықтан кіруге рұқсат етілген IP мекенжайларының тізімін нақты көрсете отырып, сіз

VTY қатынасын шектеңіз. Маршрутизаторға қашықтан кіруге рұқсат етілген IP мекенжайларының тізімін кіруді бақылау тізімі (ACL) және VTY желілерінде access-class жазбасы арқылы орнатуға болады. Бұл әдісті әкімшілік қол жетімділікті қосымша қорғау үшін SSH протоколымен қолдануға болады.

Желіні конфигурациялау режимінде орнатылған access-class пәрмені көрсетілген VTY (Cisco құрылғысында) мен кіру тізіміндегі мекен-жайлар арасындағы кіріс және шығыс қосылымдарды шектейді.

Access-class командасының синтаксисі келесідей:

Router (config-line)# access-class кіру тізімінің нөмірі { in [vrf-also] | out }

In параметрі кіру тізіміндегі мекенжайлар мен Cisco құрылғысы арасындағы кіріс қосылымдарды шектейді, ал out параметрі жеке Cisco құрылғысы мен кіру тізіміндегі мекенжайлар арасындағы Шығыс қосылымдарды шектейді.

мекенжай ауқымы VTY 0-4 жолдарына қол жетімді. Суреттегі ACL тізімі 192.168.10.0 желісі үшін VTY 0-4 желілеріне кіруге және барлық басқа желілерге кіруге тыйым салуға арналған.

VTY арналарына кіру тізімін орнату кезінде келесі ережелерді ескеру қажет:

VTY сызықтарына сілтеме жасалған және нөмірленген қол жеткізу тізімдерін (ACL) қолдануға болады.

Бірдей шектеулер барлық VTY арналарына орнатылуы керек, өйткені пайдаланушы олардың кез-келгеніне қосылуға тырысуы мүмкін.

Ескерту. Қол жеткізуді басқару тізімдері (ACL) маршрутизатор арқылы өтетін пакеттерге қолданылады. Олар маршрутизатордың ішінде жасалған пакеттерді бұғаттауға арналмаған. Әдепкі бойынша, қол жеткізуді басқару тізімі (ACL) маршрутизатордан басталған Қашықтан қатынау қосылымдарын бұғаттамайды.

VTY портының қауіпсіздігін тексеру

ACL тізімін орнатқаннан кейін, VTY желілеріне кіруді шектеу үшін оның дұрыс жұмыс істейтініне көз жеткізу керек. Суретте SSH протоколы арқылы R1-ге қосылуға тырысатын екі құрылғы көрсетілген. 21 кіру тізімі R1 маршрутизаторының VTY жолында конфигурацияланған. PC1 SSH қосылымын сәтті орнатты, ал PC2 мұны істей алмады. Бұл болжамды мінез-құлық, өйткені теңшелген кіру тізімі VTY-ге 192.168.10.0/24 желісінен кіруге мүмкіндік береді, бұл барлық басқа құрылғыларға кіруге тыйым салады.

R1 шығысы PC1 және PC2 SSH қосылымын орнатуға тырысқаннан кейін show access-lists командасының нәтижесін көрсетеді. Шығару ажыратымдылығы жолындағы сәйкестік PC1 сәтті SSH қосылымының нәтижесі болып табылады. Тыйым салу жолындағы сәйкестік 192.168.11.0 / 24 желісіндегі құрылғымен PC2 SSH қосылымын орнатудың сәтсіз әрекетінің нәтижесі болып табылады.

Жасырын өрнек deny any

Егер ACL тізімі бір тыйым салу командасынан тұрса, барлық трафик қабылданбайды. Осылайша, тізімде кем дегенде бір рұқсат командасы болуы керек, өйткені әйтпесе барлық трафик бұғатталады.

Желі үшін R1 маршрутизаторының S0/0/0 интерфейсінде 1 ACL немесе 2 ACL тізімін шығыс бағытта қолдану бірдей нәтиже береді. 192.168.10.0 желісі үшін бұл желілерге S0 / 0 / 0 интерфейсі арқылы кіруге рұқсат етіледі. 192.168.11.0 желісі үшін бұл желілерге кіруге

тыйым салынады. 1 кіруді бақылау тізімін (ACL) пайдаланған кезде permit жазу шартына сәйкес келмейтін кез келген пакет тасталады.

Қол жеткізуді басқару тізіміндегі жазбалар тәртібі (ACL)

Cisco IOS стандартты ACE жазбаларын қабылдау және өңдеу процесінде ішкі алгоритмді қолданады. Жоғарыда айтылғандай, қол жеткізуді басқару тізіміндегі жазбалар (ACL) рет-ретімен өңделеді. Сондықтан бұл жазбалардың орналасу тәртібі үлкен мәнге ие.

Мысалы