ӘОЖ 004.01

SDN ЖЕЛІЛЕРІНДЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ

Қайрбекова Назгүл Ерланқызы
nazgul.kairbekova17@gmail.com
Л.Н.Гумилев атындағы ЕҰУ, «Радиотехника, электроника және телекоммуникация» кафедрасының магистранты, Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – Н.К. Набиев

Үздіксіз өсіп жатқан трафиктің сапасы мен қауіпсіздігіне қойылатын талаптардың жоғарылауы, заманауи желілік технологиялар дамуының негізгі қозғаушы себептерінің бірі болып табылады. Дәстүрлі желілер күрделі құрылымға ие және басқарылуы қиын, өйткені желілік баптамаларды жүзеге асыру үшін әр желілік құрылғыны бөлек конфигурациялау қажет, бұл өз кезегінде қате конфигурациямен байланысты қауіптерге әкеледі. Сонымен қатар, ірі желіні қайта автоматты түрде конфигурациялаудың дәстүрлі функциялары, егер ол өзгерсе немесе дұрыс жұмыс істемесе, желілік инфрақұрылымның жұмысын төмендететін механизмдерге сүйенеді, өйткені қайта конфигурацияны жүзеге асыратын хаттамалар желілік құрылғыларға жүктемені арттырады, бұл бағдарламалық және аппараттық жасақтама жұмысын қиындатады.

Software Defined Networking (SDN) немесе бағдарламалық-конфигурацияланатын желілер термині салыстырмалы түрде жаңа емес. Осы тақырып бойынша алғашқы жұмыстар мен зерттеулер 1995 жылдан бастап пайда болады [1].

Технология таратылатын есептеулердің, яғни бұлттарда желілік технологияларды қолдану (желілерде басқарылатын маршрутизаторлар саны бірнеше ондаған мыңға жетуі мүмкін), ірі деректер орталықтарының пайда болуы, интернетті виртуализациялаудың басталуы қажеттіліктеріне жауап ретінде пайда болды [2]. Негізінен, бұл дәстүрлі деректер желілерін ұйымдастыруды өзгертетін жаңа архитектура. SDN желілерінде коммутаторлар мен маршрутизаторлардың негізгі функциялары орталық желі контроллеріне беріледі, бұл желілік саясатты қолдануды және желінің күйін бақылауды жеңілдетеді. Бұл тәсілде таратушы құрылғылар өзара әрекеттесетін орталықтандырылған желілік контроллер құратын ағындар кестесіне сүйене отырып, деректерді жіберу үшін жауап береді [3].

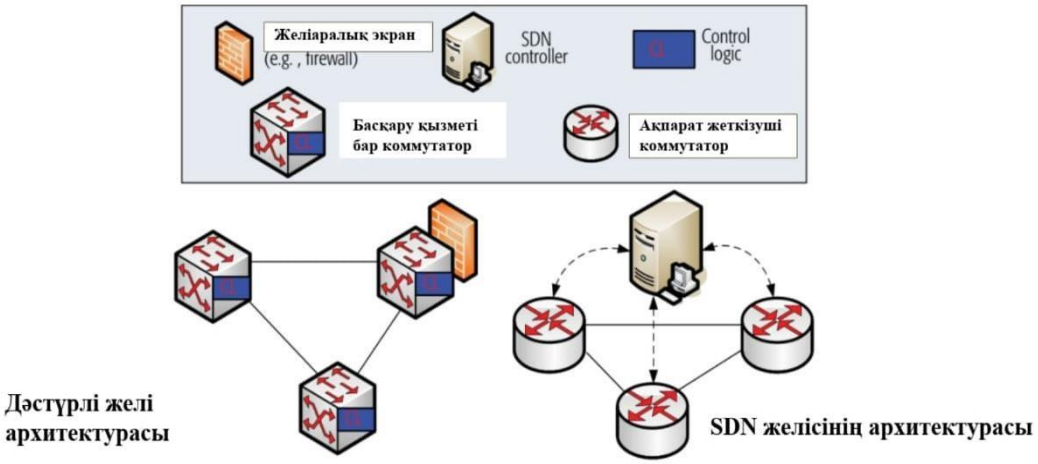
Software Defined Network архитектурасының негізгі принциптері келесі түрде көрсетіледі (Сурет 1).

- Басқару және акпаратты тасымалдау функциялары ажыратылған. Желілік құрылғы тасымалдаушы функциясын ғана орындайды.
- Контроллер тасымалдаушы құрылғы үшін сыртқы объект болып саналады.
- Контроллер желі жұмысын бағдарламалауға мүмкіндік береді.

Желі құрылымының келесідей дейгейлері бар:

- Ақпарат беру деңгейі
- Басқару денгейі – контроллер
- Қосымшалар деңгейі – жоғары деңгейлі қосымшалар контроллер мен әрекеттесуі және нақты функцияларды жүзеге асырады.

SDN архитектурасы желілік инфрақұрылымды жүзеге асыруда айтарлықтай өзгеше көзқарасты жүзеге асырғандығымен, ақпараттық қауіпсіздік тұрғысынан қарастырылатын осалдықтары да бар. Контроллермен жұмыс істеу кезінде желілік қосымшаларға қол жетімділікті бөлу қажеттілігі, контроллермен жұмыс істеу кезінде аутентификация және авторизация мәселелері SDN желілерін жобалау кезінде ескерілуі керек бірнеше қауіпсіздік аспектілері ғана болып табылады.



Сурет 1 – SDN желісі архитектурасының ерекшелігі

Контроллер бүкіл SDN инфрақұрылымын басқарудағы негізгі компонент ретінде ең осал элемент, оған көзделген шабуыл бүкіл инфрақұрылым үшін маңызды салдарға әкелуі мүмкін [4].

SDN желісінің осал тұстары, шабуылдар

1. Жалған немесе алмастырылған трафик ағындары
2. Жіберу құрылғыларына шабуылдар
3. Басқару контроллерінің байланысына шабуылдар
4. Контроллерлерге шабуылдар
5. Контроллер және басқару қосымшалары арасында сенімділіктің болмауы
6. Әкімшілендіру құрылғыларына шабуылдар

Бағдарламалық-конфигурацияланатын желі принципі бойынша жұмыс істейтін желілік құрылғылар тарапынан туындайтын негізгі қауіптер «қызмет көрсетуден бас тарту», контроллерді ауыстыру және т. б. сияқты шабуылдардың вариациялары болып қала береді [5].

SDN желісінің тұтастығын бұзудың ең қарапайым және сонымен бірге тиімді әдісі – «қызмет көрсетуден бас тарту» түріндегі шабуылдар. Шабуылдың қауіптілігі белгісіз (яғни flow-кестеде бар ережелерге сәйкес келмейтін) пакетті алу кезінде SDN-коммутатордың жұмыс алгоритмінен туындайды. Мұндай жағдайда екі нұсқа мүмкін:

– Пакет толығымен талдау үшін контроллерге жіберіледі.

– Пакет коммутатордың жадында қалады, тек пакеттің тақырыптары контроллерге жіберіледі.

– Нәтижесінде шабуылды жүзеге асыру келесі салдарға әкелуі мүмкін:

– Коммутатор ресурстарының сарқылуы. Заңды пакеттер осы желілік түйінмен мүлдем өңделмейді немесе оларды өңдеу кідірістермен бірге жүреді.

– Контроллер мен коммутатор арасындағы байланыс арнасы деректер ағындарымен жүктелгендіктен басқару хабарламаларының жеткізілуін қамтамасыз етпейді.

- Контроллер кіріс сұрауларымен шамадан тыс жүктеліп, легитимді басқару хабарламаларын өңдей алмайды.
- SDN желілеріндегі ақпараттық қауіпсіздік қатерлеріне қарсы іс-қимыл.
- Орталықтандырылған желіні басқару тек желілік контроллерге ғана емес, сонымен бірге онымен біріктірілген қосымшаларға да қол жетімді болғандықтан, SDN архитектурасы қол жетімді және түбегейлі жаңа ақпаратты қорғау құралдарын құруға мүмкіндік береді. Openflow желілерін openflow-ға тән ақпараттық қауіпсіздік қатерлерінен қорғауды қамтамасыз ету әдістері бойынша зерттеулердің кең спектрі бар. Сонымен қатар, OpenFlow протоколының ерекшеліктерін қолдана отырып алдын алуға болатын дәстүрлі желілік қауіптерге қарсы тұру құралдары жетілдірілуде.
- Openflow – желілері үшін шабуылдардың алдын алудың тиімді әдісі, бұл верификация модельдерін қолдану арқылы желі конфигурациясындағы сәйкессіздіктерді алдын ала анықтау болып табылады.

Кесте 1. Шабуылдар салдары

1. Жалған немесе алмастырылған трафик ағындары	DoS шабуылдарының есігі болуы мүмкін.
2. Жіберу құрылғыларына шабуылдар	Әсер етуі ықтималы күшеюде.
3. Басқару контроллерінің байланысына шабуылдар	Логикалық орталықтандырылған контроллермен өзара әрекеттесу мүмкіндігін жоюға болады.
4. Контроллерлерге шабуылдар	Контроллерді басқару бүкіл желіге қауіп төндіруі мүмкін.
5. Контроллер және басқару қосымшалары арасында сенімділіктің болмауы	Зиянды қосымшаларды енді контроллерлерде оңай орналастыруға болады.
6. Әкімшілендіру құрылғыларына шабуылдар	Осалдықты желі ішіне тарату

Желілік ресурстарды қабаттарға бөлу әдісін қолдана отырып, екілік анықтау диаграммаларын қолданатын Flow Checker желі қауіпсіздігі үшін қолданылады.

S. Son және т.б. [6] модульдік теорияны қолдана отырып, трафик ағындарын өңдеу саясатын тексеруді ұсынады. Overflow жобасы нақты уақыт режимінде ағын ережелерін тексеру саясатын жүзеге асырады. Осы ағындарды одан әрі талдау үшін желі контроллері openflow қосқышына жіберген ағындардың ережелерін ұстап тұратын қызметтік бағдарлама жасалды.

Контроллердің ықтимал қауіп-қатерлері мен қауіпсіздік тәжірибесіне сүйене отырып, контроллердің дизайнымен, дамуымен тікелей байланысты болмауы мүмкін, бірақ олар оның ортасы, жұмысы немесе басқаруы үшін маңызды болып табылатын жалпы қауіпсіздік «функционалдық талаптарын» тұжырымдауға болады.

Кесте 2 – Жалпы функционалдық талаптар

Талаптар	Талаптың қосымша компоненті
IP тексеру	
Пайдаланушының аутентификациясы	
Есептік жазбаларды басқару	
Жабдықтың тұтастығы мен келісімділігі	
Гипервизордың қауіпсіздігі	
Журналды модификациядан қорғау	
Берілетін деректердің тұтастығы	
Журналдарға кіруді қорғау	Тіркеу журналының қауірсіздігі Функциялардың тұрақтылығы
Деректер құпиялылығын қорғау	
Құпия сөз бен кілттердің көрсетілуін жасыру	
Трафиктің әртүрлі түрлерін бөлу	
Виртуалды машиналардың қауіпсіздігі	
Пайдаланылмаған қызметтерді жабу	
Anti-DoS функциясы:	Есептеу қуаты мен ресурстардың сарқылуынан анти-DoS,

Физикалық хосттың қауіпсіздігі	
Жүйелік пайдалануға рұқсат функциялар	Үшінші тұлғалардың интерфейке рұқсаты
Хост ОЖ қауіпсіздігі	

SDN архитектурасы желі құрылымына айтарлықтай өзгерту енгізетіндіктен, инфрақұрылымның жаңа компоненттері осалдықтарынан туындаған қауіптер пайда болады. Сонымен қатар, дәстүрлі деректер желілерімен байланысты қауіптердің көпшілігі SDN желілері тұрғысынан да маңызды. Екінші жағынан, SDN архитектурасы қауіпсіздік құралдарын дамытуда инновациялық мүмкіндіктерін ашады. Желіні орталықтандырылған басқару мен бағдарламалаудың үйлесуі желінің қауіпсіздігін қамтамасыз ету тиімділігін арттырады.

Мақалада SDN архитектурасына және OpenFlow хаттамасына шолу, SDN архитектурасы мен OpenFlow хаттамасына қауіп-қатерлерді талдау және оларды бейтараптандыру технологиялары, сондай-ақ осы қауіптерге қарсы тұру талаптары ұсынылған.

Қолданылған әдебиеттер тізімі

1. K. Calvert, S. Bhattacharjee, E. Zegura, and J. Sterbenz, Directions in Active Networks IEEE Communications magazine. October 1998. P.72–78
2. Diego Kreutz, Fernando MV Ramos, P Esteves Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky, and Steve Uhlig. Software-defined networking: A comprehensive survey. proceedings of the IEEE, 103.2015.P.14–76
3. Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. Openflow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38. 2008. P. 69–74.
4. Kevin Benton, L Jean Camp, and Chris Small. Openflow vulnerability assessment. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. 2013. P. 151–152.
5. Seungwon Shin and Guofei Gu. Attacking software-defined networks: A first feasibility study. In Proceedings of the second ACM SIGCOMM work- shop on Hot topics in software defined networking. 2013.P. 165–166.
6. Seuk Son, Seungwon Shin, Vinod Yegneswaran, Phillip Porras, and Guofei Gu. Model checking invariant security properties in openflow. In Communications (ICC), 2013 IEEE International Conference on 2013. P. 1974–1979.