ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

ӘОЖ 004.056.5

ЖЕЛІЛІК ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДЕГІ SASE МОДЕЛІНІҢ МҮМКІНДІКТЕРІ

Барат Дана Даулетбекқызы
Barat.Danna@mail.ru
Л.Н.Гумиев атындағы Еуразия Ұлттық Университетінің 1-курс магистранты,
Астана, Қазақстан
Ғылыми жетекшісі – Ж.Ахметова, PhD доктор, «Ақпараттық қауіпсіздік жүйелері» кафедрасының доценті

Кілт сөздер: ақпараттық қауіпсіздік, шекаралық қауіпсіз қол жеткізу қызметі, желілік қауіпсіздік

Аңдатпа

Бұл жұмыста инфрақұрылымның ақпараттық қауіпсіздігін қамтамасыз ету үшін шекара қызметінің қауіпсіз қол жеткізу моделі қарастырылған. Мақалада үйден немесе басқа қашықтағы желіден жұмыс істегенде қауіпсіздікті қамтамасыз етудің тиімді стратегиясының қажеттілігін дәлелдейтін зерттеу нәтижелері келтірілген. Бұл модель жұмыс жүктемелерінің едәуір бөлігін бұлтқа ауыстыруды жоспарлайтын және ішкі ресурстарға қол жеткізу құқықтарын қатаң ажыратуды қажет ететін мобильді және қашықтағы қызметкерлері бар компанияға арналған. Бұл модельдің функционалды мүмкіндіктері корпоративтік қауіпсіздікті бұлтқа негізделген операциялық модельге көшіреді. Ол конвергентті, орталықтан басқарыланатын бұлттық қызмет құрылымын құру арқылы бұлтты, мобильді және шекаралық кәсіпорындардың қажеттіліктерін қанағаттандыра алады.

1. Кіріспе

Қазіргі цифрлық әлемде қауіпсіз және тиімді желілік байланысқа деген қажеттілік туындауда. Бұлтты қызметтер мен қашықтағы жұмыс күшін енгізу статикалық ортаға арналған дәстүрлі қауіпсіздік модельдеріне жаңа міндеттер қойды. Қауіпсіз қол жетімділіктің шекаралық қызметі (Secure Access service Edge – SASE) – бұл заманауи кәсіпорындар үшін қауіпсіздіктің бұлтты моделін ұсынатын желілік инфрақұрылымды қорғаудың жаңа тәсілі. SASE брандмауэр, басып кіруді анықтау және алдын алу, VPN, қауіпсіз веб-шлюздер және т.б. сияқты әртүрлі қауіпсіздік мүмкіндіктерін бұлт арқылы қамтамасыз етілген біртұтас интеграцияланған шешімге біріктіреді [1]. Бұл интеграция ұйымдарға желілік трафик пен пайдаланушылардың белсенділігін көбірек көруге және бақылауға мүмкіндік береді, бұл қауіпсіздік қатерлерін анықтауды және олардың әсерін азайтуды жеңілдетеді. Бұл мақалада ұйымдарға желілік қауіпсіздік қажеттіліктері туралы негізделген шешімдер қабылдауға көмектесу үшін SASE моделін пайдалану ерекшеліктері талқыланады.

Gartner зерттеу фирмасы 2019 жылдың соңында енгізген SASE термині бұлтқа негізделген, мобильді және шекаралық ұйымдардың қажеттіліктерін қанағаттандыруға бағытталған қызмет көрсету үлгісін білдіреді. SASE моделі қай жерде болса да, кәсіпорын деректеріне қауіпсіз қол жеткізуді қамтамасыз етеді. Бұл заманауи және салыстырмалы түрде жаңа модель, бірақ бұл Gartner-ге 2024 жылға қарай SASE енгізу жоспарлары ұйымдардың 40% болады деп болжауға кедергі болмады.

2. Тапсырманың қойылуы

Nemertes Research IT-консалтингтік компаниясының «2020-21 жылдарға арналған келесі буын желілері» зерттеуінің нәтижелері корпоративтік жаһандық желі трафигінің шамамен 39% ғана кәсіпорын ішінде бағытталғанын, яғни филиалдан басталып, деректер орталығында аяқталатынын көрсетті. Корпоративтік жаһандық желінің қалған трафигі ұйымнан тыс, яғни үй кеңсесінде немесе бұлттық қызметте бағытталады. Трафиктің 20%- дан сәл азы ұйымнан тыс жерде де, тоқтатылды[2].

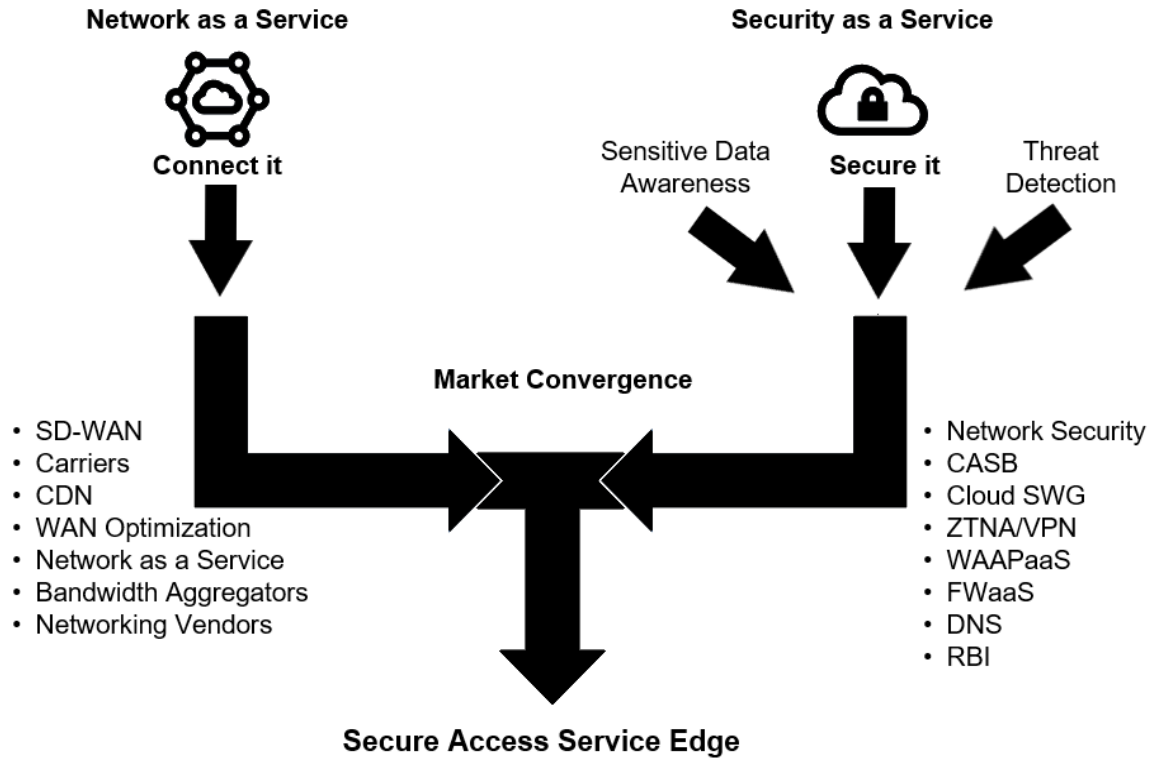
Осылайша, жүйеаралық трафикке негізделген бүкіл қауіпсіздік жүйесі кез келген жерден жұмыс істеуге арналған қауіпсіздік жүйесі ретінде қайта қаралуы керек. Кәсіпорындар дәстүрлі сценарийлер мен жаңа сыртқы өзара әрекеттесу сценарийлерінің қауіпсіздігін қамтамасыз етуді үздіксіз біріктіруі керек, олардың мысалы work from home (WFH) болуы мүмкін. Дәстүрлі VPN сеанстардың қажетті саны мен трафик көлеміне дейін масштабтау қиын және қымбат болуы мүмкін.

Жаңа технологиялардың коммерциялық құндылығын талдайтын Nemertes Research компаниясының цифрлық жұмыс орнындағы зерттеулері көптеген компаниялар кеңсе кеңістігін және онымен байланысты барлық жылжымайтын мүлік пен кеңсе шығындарын жою мүмкіндігі бар екендігін көрсетті. Дегенмен, мұны қауіпсіз орындау үшін ұйым инфрақұрылымның ақпараттық қауіпсіздігіне басқаша қарауы керек.

Нәтижесінде, ұйым қашықтағы желіден жұмыс істегенде қауіпсіздікті қамтамасыз етудің тиімді стратегиясын қажет етеді және Secure Access Service Edge (SASE) моделі бұл тапсырманы орындай алады.

3. Негізгі бөлім

Эндрю Лернер, Gartner вице-президенті 2019 жылдың желтоқсан айының соңында SASE моделін бағдарламалық жасақтамамен анықталған жаһандық желіні, қорғалған веб-шлюздерді, бұлтқа қол жеткізу қауіпсіздігі брокерлерін, нөлдік сенімді желіге қол жеткізуді және брандмауэрді қамтитын «жаңа технологиялар пакеті» деп анықтады. Негізгі қасиеттері – құпия деректерді , зиянды бағдарламаларды сәйкестендіру және деректерді беру жылдамдығында мазмұнды шифрын ашу, сеанстарды тәуекел мен сенім деңгейіне үздіксіз мониторинг жүргізу [4]. SASE моделінің негізгі компоненттері 1-суретте көрсетілген.



Сур.1 – SASE моделінің компоненттері.

Жылдам дамып келе жатқан SASE қауіпсіз қол жетімділік моделі корпоративті қауіпсіздікті бұлтқа негізделген операциялық модельге ауыстыруға бағытталған. Компанияның деректер орталықтарында орналасқан VPN қосылымдарының аз санының орнына SASE құралдары кең таралған қатысу нүктелерінің жиынтығын (POP – points of presence) қамтамасыз етеді және пайдаланушылар деректер орталығындағы кәсіпорын ресурстарына қосылу немесе бұлттың қандай да бір ұқсастығы үшін жақын жерде аутентификациядан өтеді.

SASE моделінің артықшылықтарының бірі – бұлттағы немесе кәсіпорынның деректер орталығындағы кіру нүктесіне және одан ресурстарға барлық трафик шифрланған және жүйені пайдалануды бақылау және қорғау үшін қауіпсіз веб-шлюздер мен бұлтты брандмауэрлерді қоса алғанда, қауіпсіздік технологияларының басқа да түрлері қолданылады. Ең бастысы, SASE жүйелері cloud access security brokers (CASB) компаниясымен деректер орталығынан тыс корпоративтік жүйелерге, әсіресе трафикті бұлтқа тікелей бағыттауға және деректер орталықтарын айналып өтуге мүмкіндік беретін SaaS құралдарына қол жеткізу үшін корпоративтік қол жеткізу саясатын қолдану үшін қамтамасыз етеді немесе біріктіреді [5].

Бұл мақалада SASE моделінің маңыздылығы және неге ол қазіргі қауіпсіздік стратегияларының маңызды құрамдас бөлігі болып табылатындығы талқыланады.

Осы жұмыста ұсынылған SASE моделі ұйымдарға цифрлық технологияларды қауіпсіз енгізуге және цифрлық трансформация мақсаттарына қол жеткізуге мүмкіндік береді. Бұл ұйымдарға инновацияларды енгізуге, икемділікті арттыруға және тұтынушыларға қызмет көрсетуді жақсартуға көмектеседі.

Халықаралық жеткізушілердің SASE құралдары мен қызметтері, соның ішінде Cato Networks, Cisco, Fortinet және Palo Alto Networks, кәсіпорындарда интеграцияланған соңғы нүктелерді қорғауды енгізу тереңдеген сайын және мінез-құлық қауіп-қатерін талдауды тереңірек біріктірген сайын SCAPE бағытында дамып келеді.

SASE – ге сұраныс артып келе жатқандықтан, осы жаңа қауіпсіздік архитектурасының бүкіл әлемдегі ұйымдарға әсерін түсіну үшін халықаралық зерттеулер жүргізілді.

Бұл зерттеулердің негізгі қорытындыларының бірі – SASE моделі ұйымдарға қауіпсіздік шығындарын азайтуға және қауіпсіздік жүйесін жақсартуға көмектеседі. Себебі SASE моделі әртүрлі қауіпсіздік мүмкіндіктерін бір платформаға біріктіреді, бірнеше қауіпсіздік шешімдерінің қажеттілігін жояды және қауіпсіздікті басқарудың күрделілігін төмендетеді [6]. Сонымен қатар, SASE моделі қашықтан жұмыс істеуді қажет ететін ұйымдар үшін үнемді шешім ұсынады, өйткені ол ұйымдарға қауіпсіздік периметрін өз желісінің шекараларына дейін кеңейтуге және кез келген жерден бұлттық қызметтерге қауіпсіз қол жеткізуге мүмкіндік береді. Бұл технология ұйымдарды брандмауэр, VPN және нөлдік сенімділік қорғанысы сияқты әртүрлі мүмкіндіктер үшін жеке қауіпсіздік шешімдеріне инвестициялау қажеттілігінен құтқарады. Бұл шығындардың төмендеуіне және тиімділіктің жоғарылауына әкеледі, өйткені ұйымдар өздерінің барлық қауіпсіздік мүмкіндіктерін бір платформадан басқара алады.

Осы халықаралық зерттеулердің тағы бір маңызды қорытындысы – SASE моделі ұйымдарға деректердің бұзылу қаупін азайту арқылы қауіпсіздік жүйесін жақсартуға көмектеседі. Себебі SASE моделі барлық трафиктің зиянды болуы мүмкін екенін және желіге кіруге рұқсат бермес бұрын аутентификация мен авторизацияны қажет ететін нөлдік сенімділік қауіпсіздік моделін жүзеге асырады. Бұл киберқауіптерден қорғауға көмектеседі және тек уәкілетті пайдаланушылар құпия ақпаратқа қол жеткізе алады.

Зерттеулер, сонымен қатар, SASE моделі ұйымдарға нақты уақыт режимінде қауіп-қатерді анықтауға мүмкіндік беру арқылы қауіпсіздік жүйесін жақсартуға көмектесетінін көрсетті [7]. Бұл ұйымдарға қауіпсіздік оқиғаларына тез жауап беруге және киберқауіптерден қорғануға мүмкіндік береді, бұл деректердің бұзылу қаупін азайтады және олардың құпия ақпаратының қауіпсіздігін қамтамасыз етеді.

SASE моделі барлық өлшемдегі ұйымдар үшін маңызды бола түсуде. Бұл қашықтан жұмыс істеудің өсуіне және бүкіл әлемдегі ұйымдар үшін жаңа қауіпсіздік мәселелерін тудырған цифрлық трансформация қажеттілігіне байланысты. SASE моделі ұйымдарға бұлттық қызметтерге қол жеткізудің және қашықтағы қызметкерлеріне қолдау көрсетудің үнемді және қауіпсіз әдісін ұсына отырып, осы мәселелерді шешуді ұсынады.

Кәсіпорындар өздерінің қажеттіліктері мен қалауларын бағалауы керек, өйткені олар өз нұсқаларын бағалайды, әсіресе жергілікті пайдаланушылар мен жеке бұлт ресурстары үшін қауіпсіздікті басқаруды кеңседен басқа кез келген жерден қауіпсіздікті басқарумен қалай біріктіргісі келетініне қатысты.

4. Қорытынды

Қорытындылай келе, SASE шекара қызметінің қауіпсіз қол жеткізу моделі қазіргі заманғы қауіпсіздік стратегияларының маңызды құрамдас бөлігі болып табылады. Бұл ұйымдарға желіні және соңғы нүктелерді киберқауіптерден қорғай отырып, әртүрлі қауіпсіздік мүмкіндіктерін басқару үшін үнемді, бірыңғай платформаны ұсынады. Қашықтан жұмыс істеудің жоғарылауымен және цифрлық трансформация қажеттілігімен SASE моделі кез-келген көлемдегі ұйымдар үшін маңызды бола түсуде.

Ұсынылған модельдің артықшылықтары бар брандмауэр, басып кіруді анықтау және алдын алу, VPN және т.б. сияқты желілік қауіпсіздік мүмкіндіктерін қауіпсіз веб-шлюздер және нөлдік сенімді желіге қол жеткізу сияқты бұлттық қызметтермен біріктіретін желілік қауіпсіздікке кешенді тәсілді қамтамасыз ету сияқты. Бұл қауіпсіздікке төнетін қатерлерді анықтауды және олардың әсерін азайтуды жеңілдететін желілік трафик пен пайдаланушылардың белсенділігін көбірек көруге және бақылауға мүмкіндік беретін тиімдірек және үнемді қауіпсіздік стратегиясына әкеледі.

Алайда, SASE моделін енгізу инфрақұрылымға және сараптамалық білімге қомақты инвестицияларды талап етуі мүмкін, өйткені бұл көптеген технологиялар мен қауіпсіздік қызметтерін біріктіруді және шоғырландыруды көздейді. Жалпы, SASE желілік қауіпсіздік тұрғысынан айтарлықтай артықшылықтар бере алады.

Пайдаланылған әдебиеттер тізімі

1. Gartner. (2019). The Future of Network Security Is in the Cloud. https://www.gartner.com/smarterwithgartner/the-future-of-network-security-is-in-the-cloud/
2. Mather T., Kumaraswamy S., Latif S., «Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance», 2009, O'Reilly Media, Inc 292.
3. Cobb C., «Network Security for Dummies», 2011, For Dummies, 499.
4. Hines C., «SASE: Cloud Native Security for the Enterprise», 2022, O'Reilly Media, 515.
5. Adkins H., Beyer B., Blankinship P., «Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems», 2020, O'Reilly Media, 558.
6. Lowe D., «Networking All-in-One For Dummies», 2021, For Dummies, 1056.
7. Arundel J., «Cloud Native DevOps with Kubernetes: Building, Deploying, and Scaling Modern Applications in the Cloud», 2019, O'Reilly Media, 344.
8. Erl T., Puttini R., Mahmood Z., «Cloud Computing: Concepts, Technology & Architecture», 2013, Pearson, 528.
9. Nagendra P., Gupta R., Zacharia M., «Cloud Security Automation: Get to Cloud Securely Using DevOps Practices», 2018, Manning, 384.
10. Zscaler. (2021). What is SASE? https://www.zscaler.com/SASE/what-is-SASE
11. AT&T Business. (2021). Secure Access Service Edge (SASE). https://www.business.att.com/solutions/secure-access-service-edge-SASE.html

УДК 004.056

ИСПОЛЬЗОВАНИЕ УЯЗВИМЫХ КОНТЕЙНЕРОВ DOCKER В ПРОЦЕССЕ ОБУЧЕНИИ БАКАЛАВРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Боранбай Жандос Асылханұлы
boranbay.zhandos@gmail.com
магистрант 1 курса (7М06306 – Системы информационной безопасности), ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Д.Ж.Сатыбалдина

Введение. Контейнеры Docker становятся все более популярной технологией упаковки и развертывания приложений. Для студентов, изучающих информационную безопасность, важно понимать как нужно эксплуатировать уязвимости и как их устранять. В этой статье