ӘОЖ 004.75

ЖЕЛІЛІК ҚАУІПСІЗДІКТІ JUNOS ОЖ НЕГІЗІНДЕ БАСҚАРУ

Тоқтыбаев Иса Асхатұлы
isa.toktybaev@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің ақпараттық қауіпсіздік кафедрасының магистранты, Нұр-Сұлтан, Қазақстан
Ғылыми жетекші – аға оқытушы, PhD Ж.М. Ташенова

Қазіргі заманғы күрделі желілік архитектурада және үнемі өзгеріп отыратын ортада IT мамандарына қауіпсіздікті тиімді деңгейде сақтау қиынға соғады. Қауіпсіздікті қамтамасыз ету жөніндегі әкімшілік міндеттерге пайдаланушылардың, құрылғылардың, орналасу

орындары мен қолдану тәсілдерінің үнемі кеңейетін матрицасын қолдау; талаптарды сақтау; жаңа сервистерді, қол жеткізуді бақылау құралдарын және қауіпсіздік тетіктерін ұсыну; өнімділікті оңтайландыру; сұрау салу бойынша ақауларды жою кіреді. Конфигурациядағы кез келген қателер желіні күрделі қатерлерге осал етуі және нормативтік талаптардың бұзылуына әкелуі мүмкін. Бұл мәселелерді шешу үшін желі әкімшілері желідегі қауіпсіздік саясатын қолдануы керек.

Желінің қауіпсіздігін басқару әкімшіге физикалық және виртуалды брандмауэрлардан тұратын желіні бір орталық нүктеден басқаруға мүмкіндікбереді. Желінің әрекетін жоғары сапалы визуалды бақылау, құрылғы конфигурацияларын автоматтандыру, ғаламдық саясатты қолдану, брандмауэр трафигін қарау, есептер дайындау және физикалық және виртуалды жүйелер үшін бірыңғай басқару интерфейсін ұсыну үшін әкімшілерге желінің қауіпсіздігін басқару шешімдері қажет.

Зерттеу жұмысыың мақсаты. Мақала мақсатына байланысты келесі зерттеу міндеттері жүзеге асырылады:

1. Желілік инфрақұрылымдағы желілік саясат ережелерінің логикасын зерттеу;
2. Желінің қауіпсіздігін басқару желінің толық визуализациясын қамтамасыз ететін және ресурстарға (ресурстарды топтау және жіктеу), брандмауэрлерге, қосымшаларға, порттарға, хаттамаларға, VPN желілеріне, желілік мекен-жайларды түрлендіру механизмдеріне (NAT),
3. Қауіпсіздік саясатына және жеткізуші құрылғыларға тәжірибелік зерртеу жұмыстарын орындау;
4. Juniper Networks құрылғыларын енгізе отыр желілік қауіпсіздікті зерттеу.

Зерттеу нысаны мен әдістері.

Желілік қауіпсіздікті басқару желінің толық көрінуін қамтамасыз етеді және активтер (активтер топтары мен жіктелімдері), брандмауэрлер, қосымшалар, порттар, хаттамалар, VPN, NAT, қауіпсіздік саясаты және жеткізуші құрылғылар үшін мәліметтер жасайды. Бұл ақпарат жеке құрылғылар үшін егжей-тегжейлі және талданады. Деректер қауіпсіздік операцияларын саясатты құру түрінде басқарылатын, пайдалы ақпаратқа айналдыратын ақылды ақпаратқа айналады. Жаңартылған саясат желіні қорғауды қамтамасыз ететін мәжбүрлі қолдану нүктелеріне (брандмауэр) қолданылады.[1]

Junos Space Security Director-бұл интуитивті және кеңейтілген қауіпсіздік көрінуін автоматтандырылған саясатты басқарумен біріктіретін желілік қауіпсіздікті басқарудың толық шешімі. Security Director-де шебер басқаратын интерфейс, егжей-тегжейлі конфигурация опциялары және құрылғылар мен қауіпсіздік қызметтерін орналастыруға арналған алдын-ала анықталған профильдер бар.

Security Director әкімшілерге брандмауэр үшін қауіпсіздік саясатының өмірлік циклінің барлық кезеңдерін басқаруға, бірыңғай қауіптерді басқаруға (UTM), басып кіруді болдырмауға, қолданба брандмауэріне (AppFW), VPN және желілік мекен-жайларды түрлендіруге (NAT) барлық сайттардағы орталықтандырылған веб-интерфейс арқылы көмектеседі. Security Director бірнеше қауіпсіздік құрылғылары үшін саясатты тиімді басқаруды қамтамасыз етеді және кеңейтілетін құрылғыны басқаруды қамтамасыз етеді.

Нәтижелері мен талдау.

Juniper Networks компаниясының Network and Security Manager (NSM) басқару жүйесі –бұл желілік инфрақұрылымды орталықтандырылған басқарудың заманауи көп функциялы жүйесі[2] Онда кез-келген күрделіліктегі желілерді жылдам орналастыру, басқару және бақылау үшін барлық қажетті құралдар бар.

Бұл басқару жүйесінің ерекшелігі:

- Жоғары масштабталу-бір NSM сервері алты мың құрылғыны басқара алады, егер бұл жеткіліксіз болса, яғни орталық басқару серверін қолдана отырып, онға дейін осындай NSM серверлерін біріктіру мүмкіндігі, жүйеде басқарылатын құрылғылардың жалпы саны 60 мың болуы мүмкін.
- Өнімділікті арттыру үшін Juniper NSM екі серверге орнатуға болады. Бұл

конфигурацияда серверлердің бірі (Device Server) құрылғылармен жұмыс істеу үшін жауап береді (статистиканы жинау және сақтау), ал екіншісі (GUI Server) пайдаланушылармен жұмыс істеу үшін (конфигурацияларды сақтау және өзгерту).

Device және GUI серверлерін резервтеумен ақауларға төзімді конфигурацияны қолдау қарастырылған.

NSM құрылғылардың келесі түрлерін қолдайды:

- J, M және MX сериялы маршрутизаторлар
- EX сериялы коммутаторлар
- SSG, ISG, NS және SRX сериялы қауіпсіздік шлюздері
- IDP сериялы шабуылдарды анықтау және алдын-алу құрылғылары
- SSL VPN кіру платформалары
- Infranet IC сериялы контроллерлерNSM келесі функцияны қамтамасыз етеді[3]:
- Әр түрлі сериялы құрылғыларға арналған бірыңғай басқару интерфейсі барлық желілік құрылғылар үшін бірыңғай қауіпсіздік саясатын жылдам ұйымдастыруға және тағайындауға мүмкіндік береді
- Vpn қосылымдарын орнатуды және ұйымдастыруды жеңілдетеді.
- Әр түрлі критерийлер негізінде есептерді жылдам құруды қамтамасыз етеді.
- Барлық құрылғылар үшін БҚ орталықтандырылған басқаруды және орнатуды қамтамасыз етеді.
- Нақты уақыт режимінде VPN қосылымдарының, қауіпсіздік шлюздерінің және IDP құрылғыларының күйін бақылауға мүмкіндік береді.
- Бір уақытта бірнеше әкімшіге құрылғы конфигурациясын өзгертуге мүмкіндік береді
- Орталықтандырылған жаңартуды және қауіпсіздік сигнатураларын қолдануды қамтамасыз етеді.
- Автоматты Backup, сондай-ақ ақауларға төзімді конфигурацияларды қолдауды қамтамасыз етеді.

Қорытынды

Мақала жұмысының қорытындысында Juniper NSM шешімдерінің осы уақытқа дейінгі желілік шешімдерден артылықшылықтары келтіріледі. Қосымша өзгертулерді жадыда сақтаудан бастап желілік қауіпсіздікті басқару протоколдарымен Linux базасында жұмыс жасаудағы тиімділіктерді зерттеу болып табылады.

Пайдаланылған әдебиеттер тізімі

1. Start here at the Security Director product page on the Juniper Networks website: http://www.juniper.net/us/en/products-services/security/security-director/
2. Security Director is an application that leverages the Junos Space Network Management http://www.juniper.net/us/en/products-services/network-management/junos-space-platform/
3. Security Director technical documentation: http://www.juniper.net/techpubs/en_US/release-independent/junos-space-apps/junos-space-security-director.html
4. “WikiLeaks Supporters Tear down VISA in DDoS At-tack,” December 9, 2010. http://www.digitaltrends.com/ computing/wikileaks-supporters-tear-down-visa-in-ddos- attack/.
5. Cnet news, “Twitter Crippled by Denial-of-Service At-tack”, 15 October 2010.http://news.cnet.com/8301-1357 7_3-10304633-36. html
6. R. Richardson, “2008 CSI Computer Crime & Security Survey,” CSI, 2008.
7. “US Suspects N Korea Launched Internet Attack on July 4,” 15 October 2010. http://ibnlive.in.com/news/us-sus-pects-n-korea-laun-ched-internettack-on-%20%20%20% 20%20july-4/96715 -2.html
8. S. Kumar, “Smurf Based Denial of Service Attack Am-plification in Internet,” IEEE Computer Society, ICIMP, 2007.
9. M. R. Lyu and L. K. Y. Lau, “Firewall Security: Policies, Testing and Performance Evaluation,”

The 24th Annual International Computer Software and Applications Conference, Taipe, 25-27 October 2000, pp. 116-121.
10.S. Kumar, M. Azad, O. Gomez and R. Valdez, “Can Mi-crosoft’s Service Pack-2 (SP2) Security Software Pre-vents Smurf Attacks?” Advanced International Confer-ence on Telecommunications, Guadeloupe, September 2006, pp. 89-93