SDN texnologiyalarının təhlükəsizliyi problemləri

Orxan Mənsimzadə
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
orxan@iit.science.az

Xülasə – **Son illərdə proqramla idarəolunan şəbəkə (Software Defined Network, SDN) texnologiyası əsas tədqiqat istiqamətindən biridir. Ümumiyyətlə, SDN şəbəkə proqram təminatı olaraq gələcək şəbəkə arxitekturasını ənənəvi şəbəkələrdə tətbiq edəcək, çünki SDN şəbəkə idarəçiliyi üçün sadəlik, proqramlaşdırma və elastiklik baxımından perspektiv imkanlar yaradır. SDN texnologiyasını tətbiq edərkən təhlükəsizliyə də diqqət yetirilməlidir. Bu məqalə SDN-nin təhlükəsizlik aspektlərinə yönəlmişdir, məqalədə SDN-nin xarakteristikaları, standartları və təhlükəsizlik problemləri və müvafiq müdafiə mexanizmləri müzakirə edilir.**

Açar sözlər – SDN, şəbəkə, DoS, təhlükəsizlik ekranı, OpenFlow

I. GİRİŞ

Bulud texnologiyasının inkişafi və tələbatın artması ilə bulud xidməti göstərən provayderlər şəbəkə arxitekturasının yüksək elastikliyə və rahatlığa malik olmasını tələb edən istifadəçilər üçün xidmət keyfiyyəti, təhlükəsizlik və ya etibarlılıq kimi müxtəlif şəbəkə xidməti tələblərini şəbəkə funksiyası virtualizasiyası vasitəsi ilə rahat istifadə ediləcəyini bildirir. Ancaq ənənəvi şəbəkələrdə ümumi olaraq istifadə edilən qapalı şəbəkə avadanlıqları aşağıdakı çatışmazlıqlara malikdir: a) proqram təminatı və avadanlıq sıx birləşdirilmişdir; b) çox mürəkkəb olan şəbəkə protokolları cihazlara inteqrasiya olunur; c) Demək olar ki, bütün qurğular istehsalçının mülkiyyətidir, yəni onların funksiyalarını dəyişdirmək və ya yeniləmək çətindir Bu isə istifadəçilərə bulud xidməti göstərən provayderlərə istifadəçinin tələblərinə uygun olan şəbəkə resurslarının effetkiv şəkildə optimallaşdırılmasına çətinlik törədir.

Proqramla idarə olunan şəbəkə (SDN) texnologiyası şəbəkə funksiyasını virtuallaşdırmaq üçün ən yaxşı texnologiya hesab edilən yeni və inqilabi şəbəkə arxitekturasına malikdir. Əsas məqsəd kompleks idarəetmə məntiqini bütün şəbəkə modellərindən ləğv etmək və paket ötürülməsinə rəhbərlik etmək üçün məntiqi nəzarət mərkəzi təşkil etməkdir; bu mövcud şəbəkə texnologiyasını dəyişdirmədən tətbiqi proqramlar vasitəsilə bütün şəbəkə trafikini sərbəst şəkildə idarə etmək məqsədi daşıyır. Ən perspektivli texnologiyalardan biri olan SDN ənənəvi şəbəkə arxitekturları ilə müqayisəsiz üstünlüklərə malikdir: a) SDN şəbəkə idarəetmə modelini asanlaşdırır ki, bu da operatorların şəbəkəni rahat idarə etməsinə imkan verir; b) Mərkəzləşdirilmiş idarəetmə məntiqi şəbəkənin qlobal bir görünüşünə malikdir ki, operator şəbəkə xidmətlərini optimallaşdırmaq və ya şəbəkənin işini yaxşılaşdırmaq üçün kifayət qədər məlumat verə bilər.

Son bir neçə ildə SDN-nin təhlükəsizlik problemləri və həllərinin öyrənilməsi üçün müvafiq işçi qrupları yaradılıb. Eyni zamanda, SDN-nin təhlükəsizliyi ilə bağlı təhdidlərə qarşı autentikasiya və avtorizasiya mexanizmləri, Denial of Service və ya Distributed Denial of Service (DoS / DDoS) hücumlarına qarşı idarəediciləri təmin etmək üçün sxemlər, trafikin monitorinqi və analizi və digərləri bir sıra həllər təklif edilmişdir [1] [2].

II. SDN TARXİTEKTURASINA BAXIŞ

SDN texnologiyası məlumatların ötürülməsini tənzimləyən inkişaf edən şəbəkə arxitekturasının bir növüdür. Hal-hazırda, SDN komutatorlar və marşrutlaşdırıcılar kimi ənənəvi şəbəkə avadanlıqlarına sıx şəkildə inteqrasiya olunur. Ümumiyyətlə, SDN arxitekturasını 3 səviyyəyə ayırmaq olar: 1) tətbiqi səviyyə 2) idarəetmə səviyyəsi, 3) məlumat ötürmə səviyyəsi.

1. Tətbiqi səviyyə

Tətbiqi səviyyə şəbəkə operatorlarının müxtəlif tələblərinə sürətlə cavab verməyə imkan verir. İnnovativ tətbiqi proqram təminatı SDN idarəediciləri üzərində işləmək üçün qurulmuşdur və şəbəkə virtuallaşdırması, topologiyanın quruluşu, trafik monitorinqi, təhlükəsizlik təkmilləşdirilməsi, yük balansı və s. kimi müxtəlif tələbləri yerinə yetirir. Tətbiqi səviyyə REST API kimi şəffaf API ilə idarəetmə səviyyəsi ilə əlaqə saxlayır. İdarəetmə səviyyəsi şəbəkənin fiziki resurslarının tətbiqi səviyyəsinə fərdi çıxarılmasını təmin edir, yəni şəbəkə operatorları yalnız SDN idarəedicikəri üzərində proqram təminatı istifadə edərək paketlərin məlumat yollarını dəyişə bilər, məlumatın yolunda bütün fiziki kommutatorları bir-bir konfiqurasiya etmir.

2. İdarəetmə səviyyəsi

İdarəetmə səviyyəsi ümumi SDN funksiyalarını idarə edən bir idarəedicidən ibarətdir. Bu səviyyə tətbiqi və məlumat ötürmə səviyyələri arasında bir vasitəçidir. İdarəedici bütün traffik axınının idarə olunması üçün məsuliyyət daşıyır və proqramlaşdırma vasitəsilə marşrutlaşdırma, traffikin yönləndirilməsi, paketin göndərilməsi ilə bağlı qərar qəbul edir. Paylanmış mühitdəki idarəedicilər bir-biri ilə şərqə və qərbə bağlı interfeyslər vasitəsilə əlaqə qururlar. İdarəetmə səviyyəsi və məlumat ötürmə səviyyəsi bir-biri ilə OpenFLow, NetConf, və s. kimi APİ vasitəsilə əlaqə saxlayırlar.

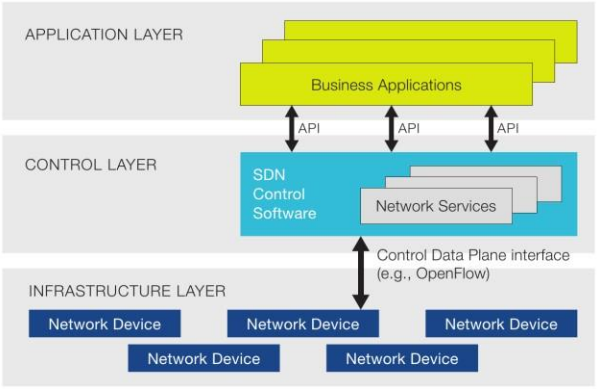
3. Məlumatötürmə səviyyəsi

Məlumat ötürmə səviyyəsi şəbəkə elementlərindən və paket ötürülməsini təmin edən qurğulardan ibarətdir [2] [3] [4].

DOI: 10.25045/NCInfoSec.2017.28

Ənənəvi şəbəkə arxitekturası ilə müqayisədə, SDN-nin təhlükəsizlik təhdidləri ənənəvi şəbəkələrin şəbəkə elementlərində görülən qarışıqlıqdan fərqli olaraq daha sıx olacaqdır. Buna görə, dizayn keyfiyyətinə görə SDN təhlükəsizlik üstünlüyünə və çatışmazlığına malikdir.

SDN texnologiyasının arxitekturası şəkil 1-də göstərilmişdir:



III. SDN ARXİTEKTURASININ TƏHLİLİ

Ənənəvi şəbəkə arxitekturası ilə müqayisədə, SDN-nin təhlükəsizlik təhdidləri ənənəvi şəbəkələrin şəbəkə elementlərində görülən qarışıqlıqdan fərqli olaraq daha sıx olacaqdır. Buna görə, dizayn keyfiyyətinə görə SDN təhlükəsizlik üstünlüyünə və çatışmazlığına malikdir.

Üstünlükləri:

- Anomal trafikin effektiv monitorinqi.

SDN idarəedicisinin eyni zamanda bütün şəbəkə trafikini qəbul etdiyinə görə hücumun şəbəkə trafikində anomal davranışı aşkarlamaq daha asandır.

- Şəbəkədə olan boşluqları görmək və vaxtında aradan qaldırmaq.

Bir təhlükə aşkar edildikdən sonra, operatorlar əməliyyat sisteminə və ya istehsalçıya aid olan proqram təminatına inteqrasiya edən proqram təminatını gözləyən zaman həmin zaman ərzində təhlükəsizliyi dərhal təhlil etmək və idarə etmək üçün yeni proqramları işə sala bilərlər. Bundan əlavə, SDN idarəedici Open Systems Interconnection (OSI) arxitekturasının 2-7 qatını əhatə edən təhlükəsizlik siyasəti konfiqurasiyasını əldə edə və daha zəngin nəzarət təmin edə bilər.

Çatışmazlıqları:

- Kənar təsirlərə həssas idarəedici.

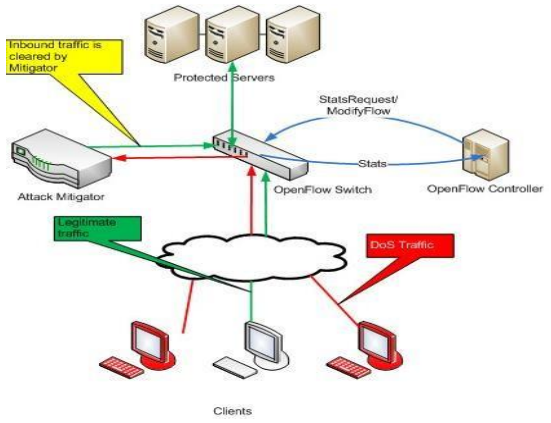
Şəbəkə məlumatlarının toplanması, şəbəkə konfiqurasiyası və marşrutlama hesablamaları kimi funksiyaların əksəriyyəti SDN idarəediciləri tərəfindən aparılır. Təcavüzkarlar bulud hesablama platformalarının dəstəyi ilə hücumları asanlıqla həyata keçirə bilərlər.Təcavüzkarlar müvəffəqiyyətlə bir SDN idarəedicisini ələ keçirsələr, idarəçilər tərəfindən əhatə olunan bütün şəbəkəyə təsir edə bilərlər.

- Hücum etmək üçün nöqtələr daha coxdur.

SDN üç qata ayrıldığı üçün, hər bir təbəqənin obyekti şəbəkənin müxtəlif hissələrinə yayıla bilir və bu obyektlər arasında əlaqə tez-tez baü verə bilər. Beləliklə, SDN ənənəvi şəbəkələrlə müqayisədə həmin nöqtələrə təcavüzkarların daha cox hücum etməsinə şərait yaradır [1] [5].

IV. SDN TEXNOLOGİYASINDA TƏHLÜKƏSİZLİK VƏ MÜVAFİQ MÜDAFİƏ TƏDBİRLƏRİ

İndi isə SDN-də təhlükəsizlik məsələlərinə baxaq. Məlumatötürmə səviyyəsi SDN arxitekturasının alt səviyyəsində yerləşir və bir-birinə qoşulan minlərlə komutatordan ibarətdir. Bu komutatorların əsas işi paketlərin ötürülməsidir. Bir komutator təhlükəyə girərsə, göndərilən paketlər düzgün ötürülmür. Komutatorlar istifadəçilərin şəbəkəyə qoşulması üçün birbaşa giriş nöqtəsidir və təcavüzkarlar giriş portuna sadəcə keçid edərək hücum edə bilərlər. Bunun üçün də komutatorlarda təhlükəsizlik tədbirlərini göcləndirmək lazımdır. Ümumiyyətlə OpenFLow SDN texnologiyasının ən məşhur standartıdır ki, həmin standartla işləyən SDN komutatorları şəkil 2-də göstərilmışdır. Əsas təhlükə məqamları idarəedici və komutator arasında verilən qaydaların dəyişdirilməsi və komutatorlar və istifadəçilər arasında ötürülən paketlərə DoS hücumlardır.



Şəkil 2. OpenFLow standartının təsviri

DoS hücumları ən ciddi təhdidlərdəndir, çünki şəbəkə fəaliyyətinə təsir göstərir və gecikməni artırır. Onlar hətta bütün şəbəkəni işə sala və ya fəaliyyətini dayandıra bilərlər. OpenFlow şəbəkələrində DoS hücumları idarəedici və komutatorlar arasında davamlı bir axın olduğundan daha dağıdıcı ola bilərlər. Bu hucumların qarşısını almaq üçün şəbəkələrarası ekran sistemindən istifadə etmək daha məqsədə uyğundur.

Şəbəkələrarası ekran ən məşhur təhlükəsizlik mexanizmlərindən biridir. Şəbəkələrarası ekranlar şəbəkə trafikini izləmək və istifadəçilər və ya şəbəkə administratorları tərəfindən müəyyən edilmiş hər hansı meyarlara əsasən onların keçidini və ya müdaxiləsini təmin etmək üçün məsuliyyət daşıyırlar. Xüsusilə, onlar OSİ modelinin 2 və 3-cü qatında işləyirlər. Ənənəvi şəbəkələrarası ekranlar yaxşı öyrənilmiş olsa da, SDN şəbəkələri üzrə tədqiqatlar hələ də inkişaf edir. SDN idarəedici özü adətən ənənəvi şəbəkələrarası ekranlar tərəfindən yerinə yetirilən bəzi vəzifələri yerinə yetirir.

Məsələn, SDN-nin idarəeiciləri axınların taleyi ilə bağlı qərarlar qəbul edir və komutatorların axın tablolarında müvafiq axın qaydaları yazırlar. SDN–də idarəedicilər bütün şəbəkə avadanlıqları üçün yazılan qaydaları saxlayır. Lakin ənənəvi şəbəkələrdə şəbəkələrarası ekran və komutator arasında belə bir əlaqə yoxdur. Bu qaydalar şəbəkə administratorları tərəfindən əlavə edilir [6] [7].

NƏTİCƏ

Məqalədə SDN texnologiyasının təhlükəsizlik sistemləri haqqında geniş məlumat verilmişdir. SDN texnologiyasının arxitekturası və standartları araşdırılmışdır. SDN texnologiyasının arxitekturasının təhlükəsizliyi, üstün və çatışmayan cəhətləri ilə bağlı araşdırma aparılmıdır. SDN texnologiyasında təhlükəsizlikla bağlı tədbirlərdə təhlükəsizlik ekranların prinsipi araşdırılmışdır.

ƏDƏBİYYAT

[1] Z. Shu, J. Wan, Di Li, “Security in Software-Defined Networking: Threats and Countermeasures,” “Mobile Network and Applications”, Vol. 21, No. 8, October 2016, pp 764-776.

[2] A. Nunes, M. Mendonca, X. Nyugen, K. Obraczka, T. Turletti “A Survey of Software Defined Networking: Past, Present and Future of Programmable Networks”, “IEEE Communications Surverys & Tutorials”, Vol. 16, No. 3, 2014, pp 1617-1634.

[3] R. Masoudi, A. Ghaffari, “Software defined networks: A survey”, “Journal of Network and Computer Applications”, Vol. 67, May 2016, pp 1-25.

[4] D. Nadeau, K. Gray, “SDN: Software Defined Networks”, O’Reilly Media, 2013. 360 p.

[5] B. Rawat, “Software Defined Networking Architecture, Security and Energy Efficiency: A Survey”, Vol. 19, No. 1, 2017, pp 325-346.

[6] N. McKeown, T. Anderson, “OpenFlow: enabling innovation in campus networks”, ACM SIGCOMM, 2008.

[7] I. Alsamadi, D. Xu, “Security of Software Defined Networks: A survey”, “Computers and Security”, Vol. 53, September 2015, pp 79-108.

SECURITY ISSUES OF SOFTWARE DEFINED NEWORKS

Orkhan Mansimzade
Institute of Information Tecnology of ANAS, Baku, Azerbaijan
orxan@iit.science.az

Abstract – Software defined networks (SDN) is one of the key research areas in recent years. Generally, the SDN will use network architecture as the next network architecture in traditional networks, because SDN provides network administrators with simplicity, programming and flexibility. When applying SDN technology, safety also should be considered. This article focuses on the SDN security aspects. The article discusses SDN's characteristics, standards, and overall security features.

Keywords – SDN, network, DoS, firewall, OpenFlow