AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

Arif Mübariz oğlu Abdurahmanov

Abdulla İdrak oğlu Cəlilov

Sarvan Kənan oğlu Məmmədov

Nərmin Hikmət qızı Zəkiyeva

PROQRAMLA İDARƏ OLUNAN ŞƏBƏKƏLƏRİN KİBERTƏHLÜKƏSİZLİKDƏ TƏTBİQLƏRİ MÖVZUSUNDA MAGİSTRLİK DİSSERTASİYASI

İxtisas: **060632 – "İnformasiya texnologiyaları və sistemləri"**

İxtisaslaşma**: "Kibertəhlükəsizlik"**

Kafedra müdiri: **t.e.d., dos. Y. N. İmamverdiyev**

Elmi rəhbər: **H. S. Cəfərli**

BAKI-2024

MAGİSTRANTIN ANDI

Proqramla idarə olunan şəbəkələrin kibertəhlükəsizlikdə tətbiqləri mövzusunda təqdim etdiyimiz magistrlik dissertasiyasını elmi əxlaq normalarına və istinad qaydalarına tam riayətetməklə və istifadə etdiyimiz bütün mənbələri ədəbiyyat siyahısında əks etdirməklə yazdığımıza and içirik və magistrlik dissertasiyasının AzTU Kitabxana İnformasiya Mərkəzində saxlanılması, həmin mərkəz tərəfindən AzTU Rəqəmsal Repozitoriyasına daxil edilərək repozitoriyanın veb saytında yerləşdirilməsinə icazə veririk.

Arif Abdurahmanov	_____
(Adı, Soyadı)	(imza)
__Abdulla Cəlilov___	_____
(Adı, Soyadı)	(imza)
_Sarvan Məmmədov__	_____
(Adı, Soyadı)	(imza)
__Nərmin Zəkiyeva___	_____
(Adı, Soyadı)	(imza)

Tarix

MÜNDƏRİCAT

İxtisarların siyahısı

API - Application Programming Interface (Tətbiq proqramlaşdırma interfeysi)

ISA- International Student Assessment (Beynəlxalq Tələbə Qiymətləndirilməsi)

MitM – man-in-the-middle (Ortadakı adam)

NFV - Network Functions Virtualization (Şəbəkə Funksiyalarının virtuallaşdırılması)

VNF - Virtual Network Functions (Virtual şəbəkə funksiyaları)

Open SDN – Open Software Defined Networking (açıq roqram təminatı ilə müəyyən edilmiş şəbəkə)

SD-WAN – Software Defined Wide Area Network (Proqram təminatı ilə müəyyən edilmiş geniş sahə şəbəkəsi)

SIEM – Security information and event management (Təhlükəsizlik məlumatları və hadisələrin idarə edilməsi)

SDN - Software Defined Networking (Proqram təminatı ilə müəyyən edilmiş şəbəkə)

SDK - Software Development Kit (Proqram təminatının inkişafı dəsti)

WAN - Wide Area Network (Geniş sahəli şəbəkə)

VLA - Virtual Local Area (Virtual Yerli Ərazi)

VLAN - Virtual Local Area Network (Virtual Lokal Şəbəkə)

VXLAN – Virtual Extensible Local Area Network (Virtual Genişlənən Lokal Şəbəkə)

LAN - Local Area Network (Lokal Şəbəkə)

DoS - Denial of service (Xidmətdən imtina hücumu)

CPU – Central Processing Unit (Mərkəzi Prosessor Modulu)

HTTP – Hypertext Transfer Protocol (Hipermətnlərin nəqliyyat protokolu)

OF – OpenFlow (Açıq Axın)

PISA – Protocol Independent Switch Architecture (Protokoldan Asılı Olmayan Keçid Arxitekturası)

BGP – Border Gateway Protocol (Sərhəd Keçid Protokolu)

SNMP – Simple Network Management Protocol (Sadə Şəbəkə İdarəetmə Protokolu)

CLI – Command-Line Interface (Komanda xətti interfeysi)

IP – Internet Protocol (İnternet Protokolu)

APIC – Application Policy Infrastructure Controller (Tətbiq Siyasəti İnfrastruktur Nəzarətçisi)

PCE – Path Computation Element (Marşrut Hesablama Elementi)

IBN – Intent-Based Networking (Məqsədəsaslı Şəbəkələşmə)

AI – Artificial Intelligence (Süni İntellekt)

ML – Machine Learning (Maşın Öyrənməsi)

IPX – Internetwork Packet Exchange (Şəbəkəarası Paket Mübadiləsi)

OSI – Open Systems Interconnection (Açıq Sistemlərin Qarşılıqlı Əlaqəsi)

MAC – Media Access Control (Media Əlaqə Nəzarəti)

MAU – Media Attachment Unit (Çoxlu giriş vahidi)

SMAU - Smart Media Attachment Unit (Ağıllı çoxstansiya giriş vahidi)

MSAU - Multi-Station Access Unit (Çoxlu Stansiyaların Müraciət Vahidi)

IEEE – Institute of Electrical and Electronics Engineers (Elektrik və Elektronika Mühəndisləri İnstitutu)

AUI – Attachment Unit Interface (Qoşulma Bloku İnterfeysi)

QoS – Quality of Service (Xidmət Keyfiyyəti)

SYN-flood – Synchronize Flood (Sinxron Axın)

ISP – Internet Service Provider (İnternet Xidmət Təchizatçısı)

SSL – Secure Sockets Layer (Təhlükəsiz giriş qatı)

SNMP - Simple Network Management Protocol (Sadə Şəbəkə İdarəetmə Protokolu)

IoT - Internet of Things (Əşyaların İnterneti)

MANO - Management, Automation and Network Orchestration (İdarəetmə, avtomatlaşdırma və şəbəkə orkestrasiysı)

ETSİ - European Telecommunications Standards Institute (Avropa elekommunikasiya standartları instutu)

MEF - Metro Etherner Forumu (Metro Etherner Forumu)

Rİ - Ring İn (Giriş halqa)

RO - Ring Out (Çıxış halqa)

MHS - Message Handling System (Mesaj İdarəetmə Sistemi)

P2P - Peer to peer (Adamdan adama)

NOS - Network operation system (Şəbəkə İşlətmə Sistemi)

EMS - Element Management System (Element İdarəetmə Sistemi)

EDR - Endpoint detection and response (Nöqtə Nəzarət və Cavablandırma)

XDR - Extended detection and response (Genişləndirilmiş Aşkar Etmə və Cavablandırma)

SOAR - Security orchestration, automation and response (Təhlükəsizlik Orkestrasiyası, Avtomatlaşdırılması və Cavabı)

SaaS - Software as a Service (Xidmət Olaraq Proqram)

SOC - Securiry operation center (Təhlükəsiz əməliyyat mərkəzi)

İDS - Intrusion Detection System (Əlçatmaz İdarəetmə Sistemi)

İPS - Intrusion Prevention System (Əlçatmaz Qarşılama Sistemi)

GİRİŞ

Mövzunun aktuallığı. Bu gün müasir təşkilatlarda proqram təminatı ilə idarə olunan şəbəkələr getdikcə daha mühüm rol oynayır. Onlar şəbəkə resursları üzərində çeviklik və nəzarəti təmin edir, performansı yaxşılaşdırır və idarəetmə proseslərini sadələşdirir. Bununla belə, bu texnologiyanın inkişafı şəbəkə təhlükəsizliyi üçün riskləri də artırır.

Təcavüzkarlar şəbəkəyə icazəsiz giriş əldə etmək, korporativ resurslara nüfuz etmək və məxfi məlumatları oğurlamaq üçün proqram təminatının zəifliklərindən istifadə edə bilərlər. Buna görə də proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizliyi məsələsi getdikcə aktuallaşır. Proqram təminatı ilə idarə olunan şəbəkələri qorumaq üçün proqram təminatını mütəmadi olaraq yeniləmək, təhlükəsizlik siyasətlərini konfiqurasiya etmək, autentifikasiya və avtorizasiya mexanizmlərindən istifadə etmək, şəbəkə trafikinə nəzarət etmək və təhlükəsizlik insidentlərinə operativ reaksiya vermək lazımdır. Şəbəkənin təhlükəsiz istifadəsi və təhlükəsizlik auditinin aparılması ilə bağlı işçilərə təlim keçmək də vacibdir.

Beləliklə, proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizliyini təmin etmək müasir təşkilatlar üçün onların biznes proseslərinə və məlumatlarına təhlükə və riskləri minimuma endirmək üçün vacib vəzifədir.

Mövzunun işlənmə dərəcəsi. Tədqiqat işinin yazılması zamanı Azərbaycan, Rusiya və xarici alimlərin bu sahədəki əsərləri, yazılmış kitab və tezislərdən istifadə edilmişdir.

Tədqiqatın məqsədi. Dissertasiya işinin məqsədi proqramla idarə olunan şəbəkələrin təhlükəsizlyinin təhlilinin aparılmasıdır.

Bununla əlaqədar olaraq dissertasiya işinin qarşısında bilavasitə aşağıdakı vəzifələr durur:

- proqramla idarə olunan şəbəkələrin əsas prinsiplərinin müəyyən edilməsi;
- proqramla idarə olunan şəbəkələrin müasir dövrümüzdə tətbiqi və inkişaf predmeti araşdırılması;

- proqramla idarə olunan şəbəkələrdə istifadə olunan cihazların müəyyən edilməsi;

- proqramla idarə olunan şəbəkələrdə mümkün təhlükə və hücumlara qarşı effektiv müdafiə strategiyalarının təhlilinin aparılması;

- proqramla idarə olunan şəbəkələrdə mövcud təhlükələrin və potensial hücumların təhlilinin aparılması;

- proqramla idarə olunan şəbəkələrin modelləri və strukturlarının təhlili.

Tədqiqatın predmeti. Təqdiqatın predmeti proqramla idarə olunan şəbəkələrin təhlükəsizlyinin təhlili zamanı yaranan münasibətlərdir.

Tədqiqatın obyekti. Tədqiqatın obyekti proqramla idarə olunan şəbəkələrin təhlükəsizlyinin təhlilinin aparılmasıdır.

Tədqiqatın nəzəri əsasını yerli və xarici alimlərin bu mövzuda olan elmi əsərləri təşkil edir.

Tədqiqat işinin metodoloji əsası. İş prosesində elmi abstraksiya, təhlil və sintez, qruplaşdırma, müqayisə üsullarında istifadə olunub.

Tədqiqat işinin informasiya bazasını beynəlxalq saziş və konvensiyalar, AR-nın qanun və hüquqi aktları, AR Rəqəmsal və İnkişaf Nazirliyinin, digər rəsmi orqanların materialları, elmi araşdırmaların materialları və dövri nəşrlər təşkil edirdi.

Tədqiqatın yeniliyi: Proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizliyinə dair dissertasiyanın mövzusu ədəbiyyatda hələ kifayət qədər tədqiq edilməmiş və təsvir edilməmiş aktual problemdir. Bu dissertasiyanın əsas elmi yeniliyi ondan ibarətdir ki, o, proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizliyinin təmin edilməsinə yeni yanaşma təklif edir ki, bura zəifliklərin təhlili, hücumların aşkarlanması və qarşısının alınması vasitələrinin işlənib hazırlanması, eləcə də təhlükəsizlik insidentlərindən sonra bərpa üsulları daxildir.

Proqram təminatı ilə idarə olunan şəbəkələrin əsas problemləri və zəifliklərı müəyyən edilmiş, onlardan bəzilərini aşağıdakı təkliflərlə aradan qaldırmaq və ya azaltmaq olar:

- Monitoriq sistemlərinin (SİEM) Şəbəkə funksiyalarının virtuallaşdırılması (NFV) inteqrasiyası
- Suni intellekt və maşın öyrənilməsi metodları ilə dəstəklənmiş Avtomatlaşdırırlmış monitorinq (Soar) sistemlərinin şəbəkə funksiyalarının virtuallaşdıırlmasında tətbiqi
- Süni intellektin tətbiqi ilə virtullaşdırılmış şəbəkə funksiyalarında yaranan problemlərin həlli
- Proqram təminatı ilə idarə olunan şəbəkələr üçün təhlükəsizlik modellərinin hazırlanması.
- Proqram təminatı ilə idarə olunan şəbəkələrdə təhlükəsizlik üsullarının müqayisəli təhlili.
- Proqram təminatı ilə idarə olunan şəbəkələrə hücumların təsirinin və onların qarşısının alınması üsullarının öyrənilməsi.
- Proqram təminatı ilə idarə olunan şəbəkələri daxili və xarici təhlükələrdən qorumaq üçün strategiyalar hazırlanması.
- Proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizlik müstəvisinin qiymətləndirilməsi və mühafizənin yaxşılaşdırılması üçün tədbirlərin təklif edilməsi.
- Proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizliyində mövcud tendensiyalar və onların təcrübəyə təsirinin öyrənilməsi

Bu mövzuda aparılan tədqiqatlar proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizliyini yaxşılaşdıracaq və belə şəbəkələrdə ötürülən və saxlanılan məlumatların mühafizə müstəvisini yüksəldəcək. İşin nəticələri proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizliyinin təmin edilməsi üçün yeni standartların və tövsiyələrin hazırlanmasında istifadə oluna bilər və bu sahədə potensial təhlükə və hücumların qarşısını almağa kömək edəcəkdir.

Tədqiqat işinin elmi-təcrübi əhəmiyyəti: proqramla idarə olunan şəbəkələrin təhlükəsizlyi ilə əlaqədar Azərbaycan Respublikasının tərəfdar çıxdığı saziş və konvensiyaların təhlili ilə bağlı nəticə və təklifləri, müəllif rəylərini müəyyən edir.

Dissertasiyanın strukturu və həcmi. Magistr dissertasiyası 81 səhifədən ibarətdir və aşağıdakı struktura malikdir: giriş, 3 fəsil, nəticə, istifadə olunmuş ədəbiyyat siyahısı.

Girişdə tədqiqatın aktuallığı, məqsədi, vəzifələri, yeniliyi və praktiki əhəmiyyəti əsaslandırılır.

Birinci fəsildə - Proqramla idarə olunan şəbəkələr haqqinda ümumi məlumat təhlil edilmişdir – proqramla idarə olunan şəbəkələrin əsas prinsiplərinin öyrənilməsi; proqramla idarə olunan şəbəkələrin müasir dövrümüzdə tətbiqi və inkişaf predmetinin müəyyən edilməsi.

İkinci fəsildə - Proqramla idarə olunan şəbəkələrin işləmə prinsipinin təhlili aparılmışdır – proqramla idarə olunan şəbəkələrin modelləri və strukturların müəyyən edilməsi; proqramla idarə olunan şəbəkələrdə istifadə olunan cihazların təhlilinin aparılması.

Üçüncü fəsildə - Proqramla idarə olunan şəbəkələrin kibertəhlükəsizlik həlləri təhlil edilmişdir – proqramla idarə olunan şəbəkələrdə mövcud təhlükələrin və potensial hücumların təhlili; proqramla idarə olunan şəbəkələrdə mümkün təhlükə və hücumlara qarşı effektiv müdafiə strategiyalarının tətbiqi

İşin sonunda tədqiqatın nəticəsi verilmiş və ədəbiyyat siyahısı göstərilmişdir.

FƏSİL I. PROQRAMLA İDARƏ OLUNAN ŞƏBƏKƏLƏR HAQQINDA ÜMUMİ MƏLUMAT

1.1. Proqramla idarə olunan şəbəkələrin əsas prinsipləri.

Analitiklərin fikrincə, Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) və şəbəkə funksiyalarının virtuallaşdırılması (Network Functions Virtualization) ənənəvi şəbəkə məhsulları bazarına mənfi təsir edir və Cisco, Juniper Networks və Hewlett-Packard kimi şirkətlərin gəlirli aparat biznesini təhdid edir. proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) və şəbəkə funksiyalarının virtuallaşdırılması (Network Functions Virtualization) şəbəkə idarəetməsi və tapşırıq funksiyalarını bahalı aparatdan daha ucuz, əmtəə sistemlərində işləyə bilən proqram təminatına keçir. Məqsəd daha çevik, proqramlaşdırıla bilən və avtomatlaşdırılmış şəbəkələr yaratmaqdır. (Edelman J., Lowe S. S., Oswalt M., 2018)

Proqram təminatı ilə müəyyən edilmiş şəbəkələrin əsas prinsipləri məlumatların ötürülməsi və idarəetmə proseslərinin ayrılması, vahid proqram təminatından istifadə etməklə şəbəkənin idarə edilməsinin mərkəzləşdirilməsi, fiziki şəbəkə resurslarının virtuallaşdırılmasıdır. Məntiqi şəbəkə nəzarətçisi və şəbəkə nəqliyyatı arasında satıcıdan müstəqil interfeysi həyata keçirən OpenFlow protokolu proqram təminatı ilə müəyyən edilmiş şəbəkə konsepsiyasının tətbiqlərindən biridir və onun yayılması və populyarlaşmasının hərəkətverici qüvvəsi hesab olunur.

Mərkəzləşdirilmiş idarəetmə prinsipi. Böyük, paylanmış şəbəkə mühitləri çoxsaylı əllə toxunma tələb edir, nəticədə səmərəliliyi azaldır və təhlükəsizliyi riskə atır. Mərkəzləşdirilməmiş bir şəbəkədə, trafiki və ya performansı müqayisə etməkdən əlavə, yeniləmələri təkan vermək və ya hər şeyin baş verdiyini görmək daha çətindir. Bu, dəyişiklikləri idarə etmək üçün şəbəkələrlə qarşılıqlı əlaqənin daha effektiv yolunu təmin edir. Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) şəbəkə imkanlarının idarə edilməsini mərkəzləşdirməklə bu narahatlıqları aradan qaldırır. Eyni zamanda, o, şəbəkənin görünməsini birləşdirir, gücləndirir və istifadəçilərə mərkəzi əlaqə nöqtəsindən infrastruktura dəyişikliklər etməyə imkan verir.

Şəbəkə abstraksiyası prinsipi. Şəbəkə abstraksiyası şəbəkə avtomatlaşdırılması üzərində qurulur. Şəbəkə avtomatlaşdırılması bizə infrastruktur dəyişikliklərini daha effektiv, daha az səhvə meylli şəkildə aparmağa imkan versə də, şəbəkə abstraksiya eyni konsepsiya üzərində qurulur. Şəbəkə mücərrədliyi sizə şəbəkənin istənilən yerinə xidmətləri çatdırmağa imkan verir. Əslində, şəbəkə proqram təminatı ilə müəyyən edilmiş şəbəkə paradiqmasında ağıllı proqram təminatından istifadə etməklə mücərrədləşdirilir. Nəticədə, məqsədli şəbəkə funksiyaları əvəzinə, İT departamentləri infrastrukturun istənilən yerində vahid şəkildə xidmətləri daha mücərrəd şəkildə təqdim edə bilər.

Şəbəkə avtomatlaşdırılması. Şəbəkənin avtomatlaşdırılması üçün, ənənəvi olaraq, bir serveri (virtual maşın kimi) ayağa qaldırdığınız zaman mərkəzi prosessor (CPU), yaddaş və saxlama resursları ayılır, lakin bundan sonra təhlükəsizlik komandası cəlb etməli və firewall qaydaları yerinə yetirilməlidir. Şəbəkə komandasını cəlb edilməli və virtual maşın üçün tələb olunan Virtual Lokal Şəbəkə (Virtual Local Area Network) təyin edilməlidir. Lakin proqram təminatı ilə müəyyən edilmiş şəbəkə (software defined networking) virtual maşının qurulmasından tutmuş onun hansı virtual lokal şəbəkədə (Virtual Local Area Network) olması lazım olduğuna, onun tələb etdiyi təhlükəsizlik parametrlərinə və istifadəçi girişi üçün həmin virtual maşına qoşulmasına, məlumat mərkəzi daxilində serverlər arasında əlaqəyə qədər bütün bunları avtomatlaşdırma vasitəsilə birləşdirir. Bu virtual maşının əməliyyat baxımından əlçatan olması üçün bütün tələb olunan parametrləri konfiqurasiya etmək yükünü yüngülləşdirir.

Proqramlaşdırıla bilənlik prinsipi. Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) infrastrukturunu idarə edən intellektual proqram təminatının başqa bir xüsusiyyəti proqramlaşdırıla bilməsidir. Şəbəkə ilə daha çox proqramlı şəkildə əlaqə saxlayırıq. Bu, vəziyyəti, şəbəkələrin tələblərini və onların şəbəkədən ehtiyac duyduqlarını düzgün əks etdirən infrastruktur dəyişiklikləri etməyə imkan verir. Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) məhsulları açıq REST API-ləri (HTTP protokolları vasitəsilə hərəkətə, əlavələrə və dəyişikliklərə imkan verən ümumi funksiyalar dəsti)

vasitəsilə proqramlaşdırıla bilir. Bu API-lər iki təkmilləşdirməyə imkan verir. Birincisi, iş yükünün yerləşdirilməsini sürətləndirmək üçün Software Defined Networking (proqram təminatı ilə müəyyən edilmiş şəbəkə) funksiyaları skript edilə bilər. İkincisi, API-lərin açıqlığı eyni təchizatçıdan və ya həlli təkmilləşdirən üçüncü tərəf satıcıdan gəlməsindən asılı olmayaraq digər əlaqəli proqramlarla sıx inteqrasiyaya imkan verir. Bu, çoxlu təchizatçı həllinə imkan verən güclü imkanların yeni müstəvisini təmin edir. (Sandhya, 2017)

Proqram təminatı ilə müəyyən edilmiş şəbəkənin bir sıra üstünlükləri var:

• **Sadələşdirilmiş əməliyyatlar**: Daha böyük mürəkkəb şəbəkənin idarə edilməsi inanılmaz dərəcədə vaxt aparan və işçi qüvvəsi tələb edə bilər. Proqram təminatı ilə müəyyən edilmiş şəbəkə bu cür böyük, mürəkkəb şəbəkələri sadələşdirir və idarəçilərə şəbəkəni bir mərkəzdən asanlıqla izləməyə və idarə etməyə imkan verir. Administrator əlavə olaraq istənilən şəbəkə keçidi qaydalarına (daxil olan məlumat paketləri ilə necə davranmağı diktə edən) dəyişikliklər edə bilər. Bu şəkildə məlumat paketlərinə icazə verilə bilər, müəyyən paketlər digərlərindən üstün ola bilər və tələb olunduqda bəzi məlumat paketləri tamamilə bloklana bilər.

• **Şəbəkələr üzrə təkmil görünmə**: Şəbəkənin görünməsi təşkilatın öz şəbəkələrindəki trafik axınından və həmin şəbəkələrdəki trafikin davranışından nə dərəcədə xəbərdar olduğunu nəzərdə tutur. Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) administratorlara öz şəbəkə trafiki axınını real vaxtda görmək imkanı verir. Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) çoxlu fərdi cihazları idarə etmək əvəzinə, bütün şəbəkəni mərkəzləşdirilmiş şəkildə idarə etməyə imkan verir. Bu, monitorinqin asanlığını yaxşılaşdırır və administratorlara təhlükəsizlik siyasətlərini tez bir zamanda tətbiq etməyə imkan verir.

• **Azaldılmış avadanlıq izi (Reduced hardware footprint)**: Ənənəvi şəbəkələr yeni avadanlıq əlavə etməyi və şəbəkə tutumunu genişləndirmək istədikdə, daha çox resurs təmin etməyi tələb edirdi. Müqayisəli olaraq, proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) əlavə fiziki avadanlıqlara investisiya

qoymadan şəbəkələri genişləndirməyə imkan verir. Bu, təşkilatların aparat izlərini azaldır və həmçinin ümumi xərcləri azaldır. (Blial O., 2016)

İndi proqram təminatı ilə müəyyən edilmiş şəbəkənin bəzi çatışmazlıqlarına nəzər salaq:

• **Təhlükəsizlik riskləri:** Bir tərəfdən proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) texnologiyası təhlükəsizliyi təkmilləşdirə bilər, lakin digər tərəfdən bu, həm də yeni təhlükəsizlik narahatlıqlarına səbəb ola bilər. Unutmamaq lazımdır ki, proqram təminatı ilə müəyyən edilmiş şəbəkə (SDN) nəzarətçi tam mərkəzləşdirilmişdir. Bu o deməkdir ki, əgər haker mərkəzi nəzarətçini hədəfə alırsa, o, bütün şəbəkəyə daxil ola bilər.

• **Konfiqurasiya:** Şəbəkədə proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) tipli arxitektura tətbiq etmək istədikdə, bütün şəbəkə infrastrukturunda dəyişikliklər edilməlidir. Şəbəkəni tam yenidən konfiqurasiyası inanılmaz dərəcədə mürəkkəb ola bilər və xərclərin artmasına səbəb ola bilər.

• **Yavaş qəbul (Slow adoption):** Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) inanılmaz dərəcədə faydalı ola bilər, lakin bütün biznes müəssisələri bu dəyişikliyə tez uyğunlaşmır. Məhdud resursları olan kiçik müəssisələr proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) konfiqurasiyasının və yerləşdirilməsinin dəyərini onun təklif etdiyi faydalara dəyər kimi görmürlər.

1.2. Proqramla idarə olunan şəbəkələrin müasir dövrümüzdə tətbiqi və inkişaf predmeti.

Son 30 ildə internet sosial inkişafa və texniki tərəqqiyə imkan verən həyati vacib infrastruktur kimi səciyyələndirilib və insanların iş, təhsil və həyat tərzinə köklü şəkildə təsir edib. Ənənəvi şəbəkə texnologiyası, əksinə, sərt quruluş və mürəkkəb quraşdırma kimi özünəməxsus çatışmazlıqlara malikdir və buna görə də şəbəkə innovasiyası tələbini ödəyə bilməz. Nəticədə, şəbəkəni dinamik və çevik şəkildə idarə edə bilən yeni şəbəkə arxitekturasının layihələndirilməsi və qurulması kritik hesab olunur. Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined

Networking) paradiqmasının tətbiqi şəbəkə sənayesində yeni eranın başlanğıcını qoydu. Proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) məqsədi xüsusi və daxili həlləri dəstəkləyən tam proqramlaşdırıla bilən proqram təminatı ilə idarə olunan şəbəkə təmin etməkdir. (Fu Y., 2015)

Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) idarəetmə müstəvisini, məsələn, şəbəkənin idarəetmə mexanizmlərini məlumat müstəvisindən, yəni şəbəkənin ötürmə mexanizmlərini ayırmaqla geniş spektrli yeni imkanlar verir. Proqram təminati ilə müəyyən edilmiş şəbəkə (SDN) nəzarətçisi inzibatçının siyasətlərinə uyğun olaraq bütün şəbəkənin idarə edilməsinə cavabdeh olan məntiqi mərkəzləşdirilmiş qurumdur. OpenFlow (Of) protokolu proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) memarlıq standartıdır. Bu protokol proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) nəzarətçisi ilə şəbəkə cihazı (switch, marşrutlaşdırıcılar və digərləri) arasında əlaqəni müəyyən edir. O, ənənəvi şəbəkələrə real vaxt rejimində trafik və biznes tələblərinə uyğunlaşmağa və onlara cavab verməyə kömək etmək üçün təqdim edilib. (Fei Hu, 2014)

Alternativ olaraq, başqa bir abstraksiya qatı əlavə edilməlidir ki, bu da işin nəzarətçi tərəfini daha mürəkkəb hala gətirəcək və daha çox kod tələb edəcəkdir. Bu protokol P4 inkişaf etdirilənə qədər proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) innovasiyasını irəli sürməyə davam etdi, sonra bu yeniliyi daha da artırdı. İnzibati və əməliyyat interfeyslərinin olmaması OpenFlow kimi protokolun başqa bir problemidir. OpenFlow ilə bağlı başqa bir problem yeni protokolları dəstəkləməyin nə qədər vaxt aparmasıdır. OpenFlow-nun başqa bir çatışmazlığı ondan ibarətdir ki, bütün funksiyalar həmişə tələb olunmasa da, İnternet xidmət provayderləri xüsusi funksiyaları seçə bilmirlər, bu da yüksək xərclərə və proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) inkişaf müstəvisinə çatmadığına görə hər yeni OpenFlow versiyası ilə yeni avadanlıq alınmasına səbəb olur. (Berde P., 2014)

Nəticədə, P4 dili OpenFlow -nun paket başlığında hər hansı bir sahəni təhlil və emal edə bilməməsini həll etmək üçün təqdim edildi. Proqramlaşdırıla bilən keçid arxitekturasına doğru hərəkət tamamilə yeni deyildi, əvvəlki mülahizələrdə sürət və vaxt problemləri var idi. Bununla belə, mikroelektromexanikadakı təkmilləşdirmələr sayəsində bu problem həll edildi. P4 istifadəçilərə şəbəkə aparat əməliyyatlarını idarə etməyə imkan verən açıq mənbəli proqramlaşdırma dili kimi qəbul edilir. O, switch, marşrutlaşdırıcılar və şəbəkə interfeys kartları kimi şəbəkə ötürücü qurğularda olan silikon prosessor çiplərinin idarə edilməsinə cavabdehdir. Proqramlaşdırıla bilən şəbəkələr, paketləri yalnız bir istiqamətə yönləndirən sabit funksiyalı switch "aşağıdan yuxarı" qurulan cari şəbəkə funksiyalarından fərqli olaraq, istifadəçinin tələb etdiyi hər hansı funksionallığı quraşdırmaq üçün "yuxarıdan aşağı" idarə oluna bilər. P4 switch-i proqramlaşdırılmamış protokolu başa düşmür və beləliklə o protokoldan müstəqildir.

P4, hər hansı bir keçid və ya marşrutlaşdırıcının davranışını proqramlaşdırma qabiliyyətinə görə Openflow protokolunu əvəz etmək üçün təqdim edildi. İndi P4-ə aparat və proqram switch, şəbəkə interfeysi kartları və marşrutlaşdırıcılar daxildir. P4 daha çox irəliləyişlərə imkan verən proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) təkamülünün növbəti addımıdır. O, P4 proqramlaşdırma dilindən istifadə edir və P4 Runtime interfeysini ehtiva edir. (Leconte M., 2018)

OpenFlow, şübhəsiz ki, OpenFlow protokolunu dəstəkləyən proqramlaşdırıla bilən switch-dən və köhnə sabit funksiyalı switch-dən ibarət şəbəkələr üçün faydalıdır. **PISA (Programme for International Student Assessment)** şəbəkə yanaşmasıdır ki, keçid daxil edilmiş ikili koddan daha çox məqsədə uyğun dildə yazılmış şərh edilmiş kodu icra edir. proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) texnologiyası təşkilatlara avtomatlaşdırılmış təminat və siyasətə əsaslanan idarəetmə vasitəsilə şəbəkə resurslarından istifadəni tez idarə etməyə və yenidən konfiqurasiya etməyə imkan verir. Şəbəkə sənayesi müəssisəni, məlumat mərkəzini, xidmət provayderini, daşıyıcını və kampus şəbəkələrini çevirmək üçün açıq proqram təminatı ilə müəyyən edilmiş şəbəkəni

(Software Defined Networking) geniş şəkildə qəbul etmişdir. Açıq proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking), şəbəkə administratorlarına məlumat müstəvisi müstəvisində fiziki və virtual switch-lərin hərəkətlərini idarə etmək üçün OpenFlow kimi bir protokoldan istifadə etməyə imkan verən bir yol kimi müəyyən edilə bilər. (Leconte M.,2018) Bu proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) keçidinin əsas məqsədi fərqliləşdirilmiş yeni xidmətlərin əvvəlkindən daha sürətli çatdırılmasını təmin etmək, şəbəkəni sadələşdirmək və ümumi sahiblik xərclərini azaltmaqdır. Proqram təminatı ilə müəyyən edilmiş şəbəkəni (Software Defined Networking) təmin edən şəbəkənin əsas xüsusiyyətləri proqramlaşdırıla bilmə, açıqlıq və davamlılıqdır.

Bundan əlavə, proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) dinamik əlaqənin yaratdığı artan tələbi ödəmək üçün şəbəkənin yenidən qurulmasını asanlaşdırır. Proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) qəbulu ənənəvi şəbəkə ilə müqayisədə bir çox üstünlüklərə malikdir, məsələn : aşağı xərclər, artan təhlükəsizlik, daha çox çeviklik, asan konfiqurasiya və istifadəçinin kilidlənməsinin qarşısının alınması. Proqram təminatı ilə müəyyən edilmiş şəbəkənin Software Defined Networking) qəbulu üzrə irəliləyiş bu günə qədər proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) geniş şəkildə mənimsənilməsi qorxuları səbəbindən ləngimişdir. Son araşdırmalara görə, bəzi şirkətlər proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) strategiyası olmayan İT mütəxəssisləri tərəfindən mənimsənilməyə mane olan mürəkkəblik və xərclər səbəbindən proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) qəbulunda dünyanın qalan hissəsindən geri qalırlar. Microsoft və Amazon kimi bir çox böyük korporasiyalar artıq Software Defined Networking (proqram təminatı ilə müəyyən edilmiş şəbəkə) -ni qəbul etsə də, kiçik müəssisələr, kampus şəbəkə operatorları və xidmət təminatçıları tərəddüd edir. Bu, proqram təminatı ilə müəyyən edilmiş şəbəkəsinə (Software Defined Networking) miqrasiya etmək üçün tələb olunan geniş planlaşdırma və tədqiqatla bağlıdır. Məhdud daxili

təcrübəyə malik müəssisələr texniki yerləşdirmə problemləri ilə üzləşirlər. Bu yolda xərc, performans, xidmətin əlçatanlığı, idarəetmə və təhlükəsizlik daxil olmaqla bir neçə problemin öhdəsindən gəlmək lazımdır. Təhlükəsizlik zəifliklərinin aradan qaldırılması şəbəkə operatorlarının əsas prioritetlərindən biridir. (Владыко, 2016)

Daha çox şəbəkə operatoru proqram təminatı ilə müəyyən edilmiş şəbəkəni (Software Defined Networking) qəbul etdikcə, mövcud şəbəkələri və xidmətləri SDN-ə köçürmək üçün ən yaxşı təcrübələrə ehtiyac var. Bu bölmə proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) miqrasiya strategiyaları ilə bağlı tövsiyələri qısa şəkildə ümumiləşdirir. O, aparıcı proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) qabaqcılları tərəfindən paylaşılan real dünyada istifadə halları vasitəsilə SDN miqrasiyasının ən yaxşı təcrübələrinə yeni perspektiv təqdim edir. Proqram təminatı ilə müəyyən edilmiş şəbəkəyə (Software Defined Networking) keçid çox çətin bir prosesdir. Aşağıdakılar proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) miqrasiyasında operatorlar tərəfindən izlənilməli olan əsas addımlardır: (Salman O., 2016)

- Hədəf şəbəkəsinin əsas tələblərini müəyyənləşdirmək və prioritetləşdirmək;
- Miqrasiya üçün ənənəvi şəbəkəni hazırlamaq;
- Mərhələli şəbəkə miqrasiyasını tətbiq etmək;
- Nəticələri təsdiq etmək.

Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking), müəssisələrin mövcud infrastrukturunu dəyişdirməsini diktə etmir. Proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) qəbuluna geniş marağa baxmayaraq, proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) həyata keçirilməsi bəzi problemləri özü ilə gətirir. Aşağıdakılar proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) təşəbbüslərini qəbul edərkən potensial problemlərin təhlilində proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) təşəbbüslərini dayandıran və ya gecikdirən ilk üç meyyar kimi müəyyən edilmişdir:

1) Mövcud şəbəkələrlə proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) inteqrasiyası ilə bağlı narahatlıqlar. Proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) maraqlı tərəfləri, xüsusən də şəbəkə mühəndisləri proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) köhnə istehsal şəbəkələri ilə inteqrasiyasını nəzərdə tutan proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) təşəbbüslərini həyata keçirməyə cəhd edərkən texniki problemlərlə üzləşirlər. SDN şəbəkə intellektini mərkəzi nəzarətçidə cəmlədiyi üçün fərdi köhnə şəbəkə qovşaqlarının intellektini silmək çox vaxt çətindir. Bu əməliyyat yüksək risklidir və şəbəkənin dayanmasına səbəb olmadan başa çatdırmaq çətin ola bilər; (Karakus M. A 2017)

2) Nəzarətçinin mövcudluğu ilə bağlı narahatlıqlar. Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) nəzarətçisi təhlükəsiz şəbəkənin saxlanması üçün çox vacibdir. Bu potensial zəiflik avtomatik uğursuzluqla şəbəkədə nəzarətçi ehtiyatının tətbiqi ilə azaldıla bilər;

3) Bu müəssisələr yeni proqram təminatı ilə müəyyən edilmiş şəbəkəsinə (Software Defined Networking) imkan verən xidmətlər təqdim etmək istəyirlər, lakin onlar həm də mövcud xidmətlərin pozulmayacağına dair təminata ehtiyac duyurlar. Bu, onları proqram təminatı ilə müəyyən edilmiş şəbəkəni (Software Defined Networking) qəbul etməkdən çəkindirir. (Владыко А.Г, Матвиенко Н.А, Новиков М.И., Киричек Р.В. 2016)

Müəssisələr adətən xərcləri əsas maneə kimi göstərirlər, lakin bu bəyanat SDN qurmaq üçün tələb olunan kapital xərclərindən daha çox azaldılmış əməliyyat xərclərinə istinad edir. Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) dizaynına əsasən, ənənəvi şəbəkələri idarə etmək üçün tələb olunan işçilərin sayı mövcud şəbəkə cihazlarından daha yaxşı istifadə etməklə azaldıla bilər. Bu, müəssisələr üçün əməliyyat xərclərinin azalmasına səbəb olur. Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) haqqında biliklərin olmamasıdır ki, bu da istifadəçilərin geniş miqyasda mənimsənilməsini təşviq etmək üçün aradan qaldırmalıdır. Bütün miqrasiya

mərhələlərinin tamamlanmasını təmin etmək üçün yoxlama siyahısından istifadə olunur. İkinci mərhələ üç hissədə həyata keçirilir: başlanğıc şəbəkə, mərhələli yerləşdirmə və hədəf şəbəkə. Mərhələli proqram təminatı ilə müəyyən edilmiş şəbəkə (SDN) miqrasiya strategiyası OpenFlow cihazları mövcud cihazlarla yanaşı yerləşdirilir. Həm mövcud idarəetmə maşını, həm də OpenFlow nəzarətçisi və konfiquratoru şəbəkənin işləməsini təmin edir. Miqrasiya başa çatdıqdan sonra idarəetmə maşını istismardan çıxarılır. (Бородин А.С., 2017) OpenFlow-un Border Gateway Protocol (BGP) ilə inteqrasiyası özəl Geniş Sahə Şəbəkələri üçün mərhələli miqrasiyanın başqa bir nümunəsidir. Mərhələli miqrasiya strategiyasını aşağıdakı kimi təsnif etmək olar:

a) Qarışıq yerləşdirmə. Bu modeldə köhnə cihazlarla yeni OpenFlow cihazları istifadə olunur. Bu yanaşma müəssisələrə mövcud şəbəkələrini pozmadan idarə etmək, konfiqurasiya etmək və yerləşdirmək daha asan olan proqram təminatı ilə müəyyən edilmiş şəbəkəyə (Software Defined Networking) imkan verən arxitekturadan faydalanmağa imkan verir. Texnologiya gündəlik iş əməliyyatlarına təsir etmədən hərtərəfli sınaqdan keçirilə bilər. O, həmçinin proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) yerləşdirmə prosesində problemlərin erkən aşkarlanmasına kömək edə bilər və problemlərin böyümədən həll edilməsinə imkan verir;

b) Hibrid yerləşdirmə. Bu modeldə köhnə cihazlar, OpenFlow cihazları və hibrid cihazlar var. Bu hibrid yanaşma çox vaxt maliyyə resursları olmayan, lakin proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) texnologiyasından maksimum yararlanmaq istəyən orta ölçülü müəssisələr üçün daha cəlbedici olur. Proqram təminatı ilə müəyyən edilmiş şəbəkəyə (Software Defined Networking) keçidin ən yaxşı yolu həm proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking), həm də ənənəvi şəbəkəni dəstəkləyən hibrid proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) həllindən istifadə etməkdir. (В. А. Лихачев. 2014) Sadəcə olaraq, keçidi ənənəvi şəbəkəyə qayıtmağa imkan verən rejimə çevirmək lazımdır. Bu, şəbəkəni xüsusi tətbiq və iş yükü tələblərinizə uyğunlaşdırmağa imkan verir.

Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) operatorlara kapital və əməliyyat xərclərinə qənaət, təkmilləşdirilmiş şəbəkə performansı, artan məhsuldarlıq və təkmilləşdirilmiş təhlükəsizlik baxımından fayda verə bilər. Proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) yerli tətbiqləri aşağıda daha ətraflı müzakirə olunur. Proqram təminatı ilə müəyyən edilmiş geniş sahə şəbəkəsi (Software-defined networking in a wide area network - SD-WAN) ardıcıl tətbiq performansını və dayanıqlığını təmin edir, biznes niyyətinə əsasən trafikin idarə edilməsini avtomatlaşdırır, şəbəkə təhlükəsizliyini yaxşılaşdırır və geniş sahə şəbəkəsi (WAN) arxitekturasını sadələşdirir. SD-WAN üzərindən trafiki təhlükəsiz və ağıllı şəkildə istiqamətləndirmək üçün mərkəzləşdirilmiş idarəetmə funksiyasından istifadə edir. Bu, proqram performansını yaxşılaşdırır və yüksək keyfiyyətli istifadəçi təcrübəsi təmin edir, biznes məhsuldarlığını və çevikliyi artırır, eyni zamanda İT xərclərini azaldır. SD-WAN, yerli və uzun məsafələrdə filiallar və məlumat mərkəzləri daxil olmaqla, müəssisə şəbəkələrini birləşdirmək üçün istifadə edilən WAN bağlantılarına tətbiq edilir. Vodacom şirkəti yalnız internet trafikindən istifadə etməyi və pula qənaət etməyi seçməyə imkan verən SD-WAN imkanlarına malikdir. Cellular Networks-də proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) 5G görmə üçün potensial katalizator kimi təklif edilmişdir. (Кадилов А.В., 2022) Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) ilə şəbəkə arxitekturası yeni 5G cihaz tələblərini dəstəkləmək üçün yenidən işlənib. Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) tərəfindən işə salınan gələcək 5G rabitəsi buna görə də müxtəlif cəmiyyətlər, istifadəçilər və operatorlar tərəfindən qoyulan əsas məsələləri və tələbləri kifayət qədər həll etməlidir ki, onlara şəbəkə dayanıqlığı, xidmətin səmərəliliyi və xidmət keyfiyyəti kimi əməliyyat standartlarına riayət etsinlər. MTN, Telkom, RAIN və Vodacom şirkətləri kimi telekommunikasiya nəhəngləri 5G-nin tətbiqinə başlayıb. Bu texnologiya şəbəkələr arasında yayılmağa başladıqda, operatorlar etibarlı əsas şəbəkə arxitekturasını inkişaf etdirmək üçün işləməyə davam edirlər. Daha çox fərdiləşdirmə, çeviklik və idarəetməni dəstəkləmək üçün

5G infrastrukturu operatorlara funksiyaları bir yerdən idarə etmək imkanı verən proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) arxitekturasını özündə birləşdirir.

Bulud hesablama xidmətlərini, mobil proqramları dəstəkləmək, öz cihazınızı gətirmək və böyük məlumat proqramları ilə bağlı İT işçilərinə yeni tələblər daha çox çeviklik, daha yaxşı performans və daha çox təhlükəsizlik təmin etmək üçün məlumat mərkəzinə yeni tələblər qoyur. Fiziki məlumat infrastrukturunu bu dəyişən tələblərə uyğunlaşdırmaq üçün davamlı olaraq uyğunlaşdırmaq əvəzinə, infrastruktur proqram təminatı ilə təchiz edilmiş bir xidmət kimi təqdim edilməlidir, yəni proqram təminatı ilə müəyyən edilmiş məlumat mərkəzi. Məlumatlara görə, Liquid Intelligent Technologies, hər bir biznes üçün ölçü və uyğunlaşdırıla bilən müştəri tərəfindən idarə olunan şəbəkə olan Data port kimi tanınan proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) xidmətini təqdim etmək üçün 350 milyondan çox sərmayə qoyub. (Лихачев В.А 2014) Liquid Data portu təmin etmək, xidmət təminatlarını təşkil etmək və müştəri xidməti tələblərini avtomatik konfiqurasiya etmək üçün sənayedə aparıcı proqram həllini tətbiq etmişdir. Müəssisə mühitlərində proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) faydaları tez görünsə də, kiçik və orta bizneslər də infrastruktura və işçi heyətinə böyük investisiyalardan qaçaraq və xərcləri azaltmaqla texnologiyadan qazana bilərlər. Proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) gələcəyi ilə əlaqədar olaraq, gecikmə, artıqlıq, etibarlılıq, təhlükəsizlik, xərc və əlçatanlıq kimi bütün tədqiqat sahələri üzrə ümumi amillər nəzərə alınmalıdır. Nəticə etibarilə, şəbəkə operatorları optimal imkanlar toplusunu həyata keçirməzdən əvvəl proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) arxitekturasına, interfeyslərinə və tətbiqlərinə bir neçə düzəliş gözləməlidirlər. Bu sənəd şəbəkə operatorlarının proqram təminatı ilə müəyyən edilmiş şəbəkəni (Software Defined Networking) qəbul etməsinə bəzi əsas maneələri müəyyən etmiş və müzakirə etmişdir. Onların bir çoxu yeni texnologiyanın təhlükəsizlik, qarşılıqlı fəaliyyət və performans kimi təqdim etdiyi risklərdən narahat olduqlarını dəfələrlə vurğulamışdırlar.

FƏSİL II. PROQRAMLA İDARƏ OLUNAN ŞƏBƏKƏLƏRİN İŞLƏMƏ PRİNSİPİ.

2.1. Proqramla idarə olunan şəbəkələrin modelləri və strukturları .

Proqram təminatı ilə müəyyən edilmiş şəbəkədə (Software Defined Networking) istifadə olunan bir neçə model var:

1. Open SDN;

2. API vasitəsilə SDN;

3. Hypervisor-based Overlay Network vasitəsilə SDN;

4. Hibrid SDN.

Open SDN: Open SDN OpenFlow keçidindən istifadə etməklə həyata keçirilir. Bu, proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) sadə tətbiqidir. Open SDN-də nəzarətçi OpenFlow protokolunun köməyi ilə southbound API istifadə edərək switch-lərlə əlaqə qurur.

Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) arxitekturada şəbəkə nəzarəti və yönləndirmə funksiyalarını ayırmaqla idarəetmə müstəvisinin proqramlaşdırılmasına və infrastrukturda tətbiq və şəbəkə xidmətlərinin abstraksiyasına imkan verir. Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking), fiziki və virtual qurğular arasında qeyri-operativliyə nail olmaq və satıcı üçün neytral olmaq, şəbəkə axınının daimi görünməsini təmin etmək, bütün cihazlar üçün vahid idarəetmə çərçivəsinə sahib olmaq, proqramlaşdırıla bilmək və avtomatlaşdırmaya imkan vermək kimi üstünlüklər təklif edərək şəbəkədə inqilab etdi. (Siamak Azodolmolky, 2013)

• **Açıq standartlar**: OpenFlow kimi ortaq bir proses vasitəsilə işlənib hazırlanmış və saxlanılan aparat və ya proqram təminatı üçün sərbəst və ümumiyyətlə mövcud spesifikasiyalar.

• **Açıq mənbə proqramı**: OpenStack və OpenDaylight kimi hər kəsin dəyişdirə və ya təkmilləşdirə biləcəyi mənbə kodu.

• **API (Application Programming Interface) və SDK (Software Development Kit):** API proqram təminatının yaradılması üçün alətlər kimi çıxış edir, çox vaxt proqram komponentlərinin bir-biri ilə necə əlaqə saxlamalı olduğunu diktə edir; software development kit (SDK) proqram təminatının işlənib hazırlanması dəstləri unikal kod tərtibatçılarının özləri yazmalı olan sayını

minimuma endirən əvvəlcədən yazılmış kod paketləridir; bir neçə SDK nəşr edilmiş API-lərdir və hər kəsin öz proqramlarına yaza bilməsi mümkündür

• **Açıq təchizat**: Açıq Hesablama Layihəsi kimi hesablama və şəbəkə məhsulları üçün açıq istinad ilə dizaynlar

API vasitəsilə SDN: API vasitəsilə SDN-də switch lar kimi uzaq cihazlardakı funksiyalar SNMP və ya CLI kimi ənənəvi metodlardan və ya Rest API kimi daha yeni metodlardan istifadə etməklə işə salınır.

Northbound API-lər proqramlar və SDN nəzarətçisi arasında əlaqədir. Tətbiqlər şəbəkəyə nəyə ehtiyacı olduğunu söyləyə bilər (məlumat, yaddaş, bant genişliyi və s.).

Bu API-lər müxtəlif proqramları dəstəkləyir. Bəlkə də buna görə proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) northbound API-lər SDN mühitində ən çox formalaşdırıla bilən komponentlərdən biridir. Şimal interfeysi vasitəsilə optimallaşdırıla bilən şəbəkə proqramlarının növlərinə yük balanslaşdırıcıları, firewalllar və ya digər proqram təminatı ilə müəyyən edilmiş təhlükəsizlik xidmətləri və ya bulud resursları üzrə orkestrasiya proqramları daxildir. (В. А. Лихачев, 2014)

Northbound API-lər həmçinin SDN Controller-i Kukla, Chef, SaltStack, Ansible və CFEngine kimi avtomatlaşdırma yığınları, həmçinin OpenStack, VMware-in vCloudDirector və ya Apache-nin açıq mənbəli CloudStack kimi orkestr platformaları ilə inteqrasiya etmək üçün istifadə olunur. Məqsəd şəbəkənin daxili işini mücərrəd etməkdir ki, proqram tərtibatçıları şəbəkəyə "qoşsunlar" və tətbiqin ehtiyaclarını ödəmək üçün dəyişikliklər edə bilsinlər. Northbound və REST API-lərini inkişaf etdirməyə həsr olunmuş bir neçə açıq mənbəli layihə və qruplar var.

Məsələn, Linux Açıq API Təşəbbüsü bir çox proqramlar, interfeyslər və əməliyyat sistemlərində istifadə oluna bilən açıq mənbə kodundan istifadə edərək proqramlaşdırıla bilən API-lərin yaradılmasına yönəlib.

Hypervisor-based Overlay Network vasitəsilə SDN: Hipervizor vasitəsilə SDN-də fiziki cihazların konfiqurasiyası dəyişməzdir. Bunun əvəzinə, fiziki

şəbəkə üzərindən Hypervisor əsaslı üst-üstə düşən şəbəkələr yaradılır. Yalnız fiziki şəbəkənin kənarındakı qurğular virtuallaşdırılmış şəbəkələrə qoşulur və bununla da fiziki şəbəkədəki digər cihazların məlumatlarını gizlədir. Üst qatı konseptuallaşdırmağın bir yolu onu telefon sistemi kimi identifikasiya etiketi və ya nömrə ilə təyin edilmiş son nöqtələr kimi düşünməkdir. Orijinal telefon sistemi kimi ənənəvi fiziki şəbəkədə telefon nömrəsi şəbəkəyə qoşulmuş xüsusi fiziki cihazı tapmaq üçün istifadə olunurdu. Bununla belə, müasir telefon sistemində telefon nömrəsi "virtuallaşdırıla" bilər - yəni cihazlara və ya proqram təminatına təyin edilə bilər və ya istifadəçini izləmək üçün proqramlaşdırıla bilər. Bu virtuallaşdırma və ya üst-üstə düşmə formasıdır.

Overlay şəbəkəsindəki son nöqtələr telefon paradiqmasına bənzər şəkildə fəaliyyət göstərə bilər. Onlar şəbəkə portu kimi faktiki fiziki yerlər ola bilər və ya şəbəkə buludunda proqram ünvanı ilə təyin edilmiş məntiqi yerlər ola bilər. (Панеш А. Х., 2016)

Overlay şəbəkələri peer-to-peer şəbəkələri, IP şəbəkələri və virtual Local Area Networks (VLAN) daxil olmaqla bir çox formada ola bilər. 3-cü müstəvi IP ünvanından istifadə edən İnternetin özü üst-üstə düşən şəbəkədir, çünki son nöqtələr onların IP ünvanları ilə təyin olunur. Bu üst-üstə düşmə üsulu tez-tez “Layer 3 şəbəkəsi” adlanır.

Şəbəkə Overlay texnologiyası üçün hazırlanmış bəzi protokollara IP, Virtual Genişlənən LAN (VXLAN — IETF RFC 7348), Virtual Şəxsi Şəbəkələr (VPN) və IP Multicast daxildir. Bu yaxınlarda, proqram təminatı ilə müəyyən edilmiş şəbəkənin (Software Defined Networking) gəlişi, ən çox tanınanı VMware-in NSX-i olan fərdi təchizatçılardan daha çox üst-üstə düşən texnologiyaları meydana gətirdi.

Cisco kimi satıcılar, öz müştərilərini mülkiyyət mühitindən proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) mühitinə köçürmək üçün nəzərdə tutulmuş öz hibrid həllərini təklif etdilər, eyni zamanda, tez-tez "alt örtük" olaraq adlandırılan öz keçid texnologiyasından istifadə edirlər. Cisco-nun Tətbiq Mərkəzli İnfrastruktur adlanan yanaşması ilə proqram nəzarətçisi, Cisco-nun

Tətbiq Siyasətinə Nəzarətçi İnfrastrukturu (APIC) SDN funksionallığına nail olmaq üçün şəbəkəyə əlavə edilə bilər. Bu yanaşmanın üstünlüyü ondan ibarətdir ki, APIC üst-üstə düşməsi əsas aparat infrastrukturu ilə "astar" inteqrasiya olunub. (Кадилов А.В., 2022)

Əksər üst-üstə düşmə formaları bir növ "kapsulyasiya"dan istifadə edir – mesaj təyinat yerinə aparılmazdan əvvəl onu əhatə edən proqram etiketi. Təyinat yerinə çatdıqda, bu əhatə olunmuş mesaj paketdən çıxarılır və nəzərdə tutulduğu təyinat yerinə çatdırılır. Mesajın inkapsulyasiyası və paketinin açılması prosesi hesablama gücü tələb edir. Proqram təminatının üst-üstə düşməsinin tənqidçiləri bunun miqyaslılıq problemləri olduğunu deyirlər. Bu da şəbəkəyə əlavə mürəkkəblik əlavə edir. (Лихачев В.А., 2014)

Şəbəkə örtüyü hətta marketinq müharibəsinə də məruz qalır, çünki Cisco kimi VMware rəqibləri ən yaxşı performansı təmin etmək üçün şəbəkə proqram təminatının hardware ilə sıx birləşməni tələb etdiyini söyləyərək xalis örtük həllərini tənqid edirlər. (Sandhya, 2017)

Overlay şəbəkəsinin necə qurulduğundan asılı olaraq, bu, bir çox insanlar üçün çox şey deməkdir, lakin üst-üstə düşmə texnologiyalarının İnternetin başlanğıcından bəri mövcud olduğunu nəzərə alsaq, çox güman ki, şəbəkələrin proqramlaşdırılmasını artırmaq üçün çevik üsullar kimi populyar olaraq qalacaqlar.

Hibrid SDN: Hibrid Şəbəkə şəbəkədə müxtəlif növ funksiyaları dəstəkləmək üçün bir şəbəkədə proqram təminatı ilə müəyyən edilmiş şəbəkə ilə Ənənəvi Şəbəkələrin birləşməsidir.

• **OpenFlow**. Şəbəkə avadanlığından bütün idarəetmə müstəvisini çıxarır, onu yalnız məlumat müstəvisi roluna endirir, beləliklə, məlumatların monitorinqini asan və daha sürətli edir. Şəbəkəyə nəzarətin yeni mexanizmləri hazırlanır və serverdə/buludda, onlayn yaddaş qurğusunda saxlanılır. (Логинов С.С., 2017)

• **Yol Hesablama Elementi (PCE).** SDN-nin PCE əsaslı yanaşmaya miqrasiyası müntəzəm və ya qismən ola bilər. OpenFlow-dan fərqli olaraq, hələ PCE-də təkmilləşdirilməmiş şəbəkə elementləri yollarda istifadə oluna bilər və həmçinin mövcud yol əlaqə funksiyasından istifadə edərək giriş qovşaqları kimi

fəaliyyət göstərməyə davam edə bilər. Bu yanaşma daha az xərcə, daha az riskə malikdir və OpenFlow-dan daha az pozucudur.

O, aparat əsaslı funksiyaları seçə, eyni zamanda proqram təminatının vaxt qrafiklərini inkişaf etdirə və təşkil edə bilər. SDN həm də qeyri-SDN mühitləri ilə müqayisədə onu daha səmərəli, xətaya dözümlü və deterministik edən məntiqi mərkəzləşdirilmiş idarəetməni təmin edir. Nəhayət, avtomatlaşdırma Google-a monitorinqi ayırmağa kömək edir, şirkətə öz sisteminin müxtəlif aspektlərini müəyyən etməyə və onu ayrı-ayrı qutulardan idarə etməyə imkan verir.

Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) arxitekturası 3 fərqli təbəqədən ibarətdir, yəni tətbiqlər təbəqəsi, idarəetmə təbəqəsi və infrastruktur təbəqəsi. Nəzarət təbəqəsi adətən tətbiq təbəqəsi ilə əsas infrastruktur təbəqəsi arasında sıxışdırılır. Buradan, bu təbəqələr hər bir təbəqə arasında əlaqə yaratmaq üçün southbound and northbound API-lərdən və ya tətbiq proqramlaşdırma interfeyslərindən istifadə edir.

Ənənəvi şəbəkələrdə, bunun əvəzinə bir cihaz və ya yük balanslaşdırıcısı kimi xüsusi bir firewall istifadə edərdiniz. Lakin SDN-də məlumat müstəvisini idarə etmək üçün tətbiq müstəvisindən istifadə edirik. (S. Ghorbani, C. Schlesinger, M. Monaco, 2014)

• **Nəzarət layeri**: Bundan sonra tətbiq təbəqəsi ilə infrastruktur qatını birləşdirən idarəetmə qatımız var. Bu təbəqə administratorun bütün şəbəkəyə nəzarət edə, siyasətləri idarə edə və trafik axınına nəzarət edə biləcəyi mərkəzləşdirilmiş SDN nəzarətçi proqramını təmsil edir.

• **İnfrastruktur təbəqəsi**: Nəhayət, biz infrastruktur qatına sahibik. Bu, şəbəkədəki fiziki switch və routerlərin əsas şəbəkəsidir. Bu cihazlar nəzarətçi tərəfindən təmin edilən qaydalar və siyasətlər əsasında şəbəkə trafikini təyinat məntəqələrinə yönləndirir.

SDN arxitekturaları şəbəkə davranışını proqramlı şəkildə tənzimləmək və idarəetməni mərkəzləşdirmək qabiliyyətinə görə şəbəkə texnologiyalarının istiqamətinə əhəmiyyətli dərəcədə təsir etmək potensialına malikdir.

• **IBN:** AI və ML şəbəkənin uyğunlaşdırılmasını və özünü idarəetməni gücləndirərək, arzu olunan nəticələr əsasında şəbəkə konfiqurasiyasını avtomatlaşdırır;

• **Şəbəkənin dilimlənməsi**: Fiziki şəbəkələrin bölünməsi performans, təhlükəsizlik və təcrid kimi tələblər əsasında xüsusi resursların bölüşdürülməsinə imkan verir;

• **Çoxdomenli SDN**: Mürəkkəb və paylanmış şəbəkələri idarə etmək üçün SDN yerləşdirmələri bulud, kənar və məlumat mərkəzləri daxil olmaqla müxtəlif domenlərdə təşkil edilir;

• **Süni intellekt şəbəkə əməliyyatlarını avtomatlaşdırması**: AI alqoritmləri və ML texnikaları proqram təminatı ilə müəyyən edilmiş şəbəkədə (Software Defined Networking) şəbəkənin qurulmasını, idarə edilməsini və problemlərin aradan qaldırılmasını avtomatlaşdırır; (Muhizi S., 2017)

• **Proqnozlaşdırılan analitika**: Süni intellekt effektiv optimallaşdırma və resurs bölgüsünə imkan verən performans problemlərini proqnozlaşdırmaq üçün şəbəkə məlumatlarını təhlil edir**.**

Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) arxitekturalarının misilsiz çeviklik və nəzarət təklif etməklə şəbəkənin gələcəyini formalaşdıracağı, ənənəvi yanaşmaları dəyişdirəcəyi və bağlantıda irəliləyişlərə təkan verəcəyi gözlənilir.

Ölçüləbilənlik, rahatlıq və iqtisadi səmərəliliyin artan ehtiyaclarını ödəyən proqram tərəfindən müəyyən edilmiş şəbəkə arxitekturası, təşkilatlara şəbəkə və rabitə sahəsində inqilab etməyə kömək edən inqilabi bir üsuldur.

• **Mərkəzləşdirilmiş şəbəkəyə nəzarət**: Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) şəbəkə nəzarətini tək nəzarətçidə mərkəzləşdirir, daha yaxşı təhlükəsizlik, performans və etibarlılıq üçün ətraflı siyasətin tətbiqinə imkan verir;

• **Proqramlaşdırıla bilən Şəbəkə:** Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) dəyişən trafik tələblərinə uyğunlaşmaq üçün

şəbəkə cihazlarının anında yenidən konfiqurasiyasına imkan verir, nəticədə performans və səmərəlilik yüksəlir;

• **Xərclərə qənaət**: Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) şəbəkələr qurmaq üçün əmtəə avadanlıqlarından istifadə edir, xüsusi avadanlıqların qiymətini azaldır və əmək və texniki xidmət xərclərinə qənaət edir;

• **Təkmilləşdirilmiş şəbəkə təhlükəsizliyi**: Proqram təminatı ilə müəyyən edilmiş şəbəkədə (Software Defined Networking) mərkəzləşdirilmiş nəzarət incə dənəli siyasətin həyata keçirilməsi vasitəsilə şəbəkə təhlükəsizliyi riskinin aşkarlanması və cavablandırılmasını asanlaşdırır; (Siamak Azodolmolky, 2013)

• **Ölçüləbilənlik**: Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) əl müdaxiləsi olmadan trafik tələblərini yerinə yetirmək üçün şəbəkəni səmərəli şəkildə miqyaslandırır;

• **Şəbəkə idarəetmə**: Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking), şəbəkə problemlərinin həllini asanlaşdıraraq, iş vaxtını və etibarlılığı artıraraq, aparat abstraksı vasitəsilə şəbəkə idarəsini sadələşdirir.

Proqram təminatı ilə müəyyən edilmiş şəbəkə (Software Defined Networking) arxitekturaları şəbəkə dizaynı, yerləşdirilməsi və idarə edilməsində inqilab edən, innovasiyalara təkan verən və biznesin rəqəmsal transformasiyasını asanlaşdıran çoxsaylı üstünlüklər təklif edir.

2.2. Proqramla idarə olunan şəbəkələrdə istifadə olunan cihazlar.

Şəbəkənin kabel seqmenti bir-birinə elektriklə bağlı olan kabel bölmələrinin zəncirid**ir.**

Məntiqi şəbəkə seqmenti və ya sadəcə bir seqment, keçid qatı paketləri müstəvisində bir-birinə birbaşa çıxışı olan şəbəkə qovşaqları qrupudur.

İnternet körpülər və ya routerlər vasitəsilə bir-birinə bağlanan kabel şəbəkələrinin məcmusudur.

IPX şəbəkəsi, İnternetdə unikal olan öz IPX nömrəsinə (4 bayt identifikatoru) malik, qəbul edilmiş çərçivə növü ilə birlikdə kabel şəbəkəsidir. Bir Ethernet kabel

şəbəkəsində istifadə olunan çərçivə tipinə görə (802.2 və 802.3) fərqlənən öz nömrələri olan iki müxtəlif IPX şəbəkəsi ola bilər.

Şəbəkə adapterləri. Şəbəkə adapteri kompüter və ya digər şəbəkə avadanlığı kimi bəzi şəbəkə cihazlarını şəbəkəyə qoşmaq üçün istifadə olunur. Şəbəkə adapterlərinin dizaynı şəbəkə siqnalının ötürülməsinin xüsusi üsullarına, kompüter şininin növünə və şəbəkə ötürmə mühitinə yönəldilmişdir. Şəbəkə bağlantısını həyata keçirmək üçün dörd komponent lazımdır:

1. Şəbəkə ötürmə mühitinə uyğun olan birləşdirici;
2. Ötürücü;
3. OSI məlumat keçid müstəvisinin MAC alt qatını dəstəkləyən nəzarətçi
4. Protokolun idarə edilməsi üçün proqram təminatı.

Bağlayıcılar və çərçivə sxemləri müəyyən bir rabitə mühiti növü üçün nəzərdə tutulmuşdur (məsələn, koaksial, bükülmüş cüt, fiber optik və ya simsiz texnologiyalar). Bəzi şəbəkə kartları çoxlu bağlayıcılarla istehsal olunur və buna görə də müxtəlif növ media ilə istifadə oluna bilər.

Simsiz şəbəkə adapterləri. Simsiz adapter iki rejimdən birində məlumat ötürülməsini təmin edir. Bir rejim digər simsiz adapterlə xüsusi, həmyaşıd qarşılıqlı əlaqədir. Başqa bir rejim giriş nöqtəsi ilə, məsələn, simsiz körpü ilə qarşılıqlı əlaqədir. Əgər siz simsiz giriş nöqtəsi ilə işləyirsinizsə, xüsusi simsiz rabitələrdən istifadə etmək də məqsədəuyğun deyil, çünki onlar giriş nöqtəsi olduqda etibarlı işləməyəcəklər.

802.11b standartına uyğun olan mövcud simsiz adapterlər adətən 1, 2, 10 və 11 Mbit/s sürətlə qiymətləndirilir. Bəzi istehsalçılar və ya həmçinin 802.11a standartına uyğun simsiz adapterlər istehsal edirlər. Simsiz adapterlər həmişə mümkün olan ən yüksək sürətlə işləmirlər, həmyaşıd kompüterlərdə və ya giriş nöqtəsində yükü nəzərə alaraq, mövcud şərtlər üçün ən uyğun olan sürəti "danışırlar".

Çoxlu giriş vahidi (MAU) token ring şəbəkəsində mərkəzi mərkəz rolunu oynayır. Ağıllı çoxstansiya giriş vahidi (SMAU) termini modulun iş stansiyalarına

qoşulmalarda nasazlıqları tapmaq və nasaz stansiyaları bütün şəbəkədən təcrid etmək qabiliyyətinə malik olduqda da istifadə olunur. (Leconte M., 2018)

MAU modulları yalnız aşağıdakı funksiyaları yerinə yetirə bilən token ring şəbəkələrində istifadə olunur:

- iş stansiyalarını fiziki ulduz topologiyası daxilində məntiqi halqaya birləşdirmək;
- halqa ətrafında marker və çərçivələri köçürmək;
- informasiya siqnallarını gücləndirmək;
- marker halqasını genişləndirmək üçün ardıcıl zəncirlərdə birləşdirmək;
- verilənlərin düzgün hərəkətini təmin etmək;
- nasaz qovşaqlarla əlaqəli portları söndürmək.

Çoxlu giriş vahidi şəbəkədəki stansiyaları işarə halqasına birləşdirən mərkəzdir. MSAU abbreviaturası bəzən onu təyin etmək üçün istifadə olunur.

Bütün şəbəkə cihazları tipik olaraq Tip 1, 2 (qoruyucu) və ya 3 (qoruyucusuz) burulmuş cüt kabeldən istifadə etməklə MAU modulu vasitəsilə işarə halqasına qoşulur. MAU modulu fiziki ulduz topologiyasını həyata keçirərək kadrları bir qovşaqdan digərinə ötürür, lakin məntiqi olaraq çərçivələr halqada olan kimi hərəkət edir. MAU modulu mərkəzi mərkəz rolunu oynayır və OSI Fiziki və Məlumat Bağlantısı müstəvilərində işləyir.

Ən sadə MAU modulu səkkizə qədər kabel seqmentini birləşdirir. Ən son modullarda qovşaqları birləşdirmək üçün 16 port var. MAU modulu passiv və ya aktiv mərkəz kimi çıxış edə bilər.

Aktiv qovşaq hər dəfə növbəti qovşaqda hərəkət etdikdə siqnalları bərpa edir, sinxronlaşdırır və gücləndirir. Nəticədə Uzaq qovşaqlar iki dəfədən çox güclü siqnal alır. Dəstəklənən qovşaqların sayını artırır; bu halda aktiv hub təkrarlayıcı kimi işləyir. Aktiv MAU-lardan istifadə edərkən Tip 3 kabel şəbəkəsində 150-yə qədər, Tip 1 və ya Tip 2 kabel şəbəkəsində isə 260-a qədər qovşaq ola bilər. 3-cü tip kabeldən istifadə edərkən qovşaqların maksimum sayı 1 və 2-ci növlərdən istifadə etdikdən daha azdır. Bu onunla izah olunur ki, 3-cü tip kabeldə titrəmə adlanan xeyli yüksək siqnal təhrifi olur. İstənilən MAU modulunda giriş portu - Ring In (RI) və

Ring Out (RO) portu olur. Bu portlar sizə MAU modullarını birləşdirməyə imkan verir. (В. А. Лихачев, 2014)

MALI modullarını birləşdirmək üçün istifadə olunan kabellər pat|H kabelləri, qovşağı MAU modulu ilə birləşdirən kabellər isə lob kabelləri adlanır. RI və RO portları arasındakı bağlantılar əlavə iş stansiyalarının şəbəkəyə qoşulmasına imkan verən işarə halqasının genişlənməsini təmin edir. Çoxlu MAU modullarından istifadə edərkən birinci modulun RI portu ikinci modulun RI portuna qoşulur və bütün modullar birləşdirilənə qədər belə davam edir.

Konsentrator - adətən müxtəlif arxitekturalı şəbəkələri birləşdirmək imkanı olan daha mürəkkəb mərkəz. Qovşaqlar və konsentratorlar arasında dəqiq sərhəd yoxdur; hər ikisi təkrarlayıcılar, körpülər və ya marşrutlaşdırıcılar ola bilər.

Ağıllı mərkəzlər şəbəkə cihazlarına şəbəkə performansı məlumatlarını toplamağa imkan verən Sadə Şəbəkə İdarəetmə Protokolunu (SNMP) dəstəkləyir.

Ağıllı, stackable və rack-mountable qovşaqları, işçi qrup mərkəzləri ilə birlikdə, şəbəkə avadanlığının yerini birləşdirmək və nəzarət nöqtələrində şəbəkəni idarə etmək üçün ümumi strategiyanı həyata keçirmək üçün istifadə edilə bilər. Bu yanaşma şəbəkə administratoruna şəbəkənin istənilən yerindən performans məlumatlarını müəyyən etməyə imkan verəcək. Üstəlik, zərurət yaranarsa, şəbəkəni asanlıqla təkmilləşdirmək və səmərəliliyini artırmaq olar. Əgər, məsələn, binanın müəyyən qanadında yeni Ethernet seqmenti quraşdırmaq lazımdırsa, onda sizə lazım olan tək şey hub rafına bir kart əlavə etmək və ya bir və ya daha çox yığıla bilən qovşaqları birləşdirməkdir.

Təkrarlayıcı (Repeater) - bir şəbəkənin seqmentlərini birləşdirən, aralıq gücləndirmə və siqnal formalaşmasını təmin edən cihazdır. (Лапонина О.Р., Сухомлин В. А. 2015) OSI modelinin fiziki qatında işləyir. Məsafə və bağlı qovşaqların sayı ilə şəbəkəni genişləndirməyə imkan verir. Təkrarlayıcı aşağıdakı funksiyalarını yerinə yetirə bilər:

- radio və ya elektromaqnit müdaxiləsi nəticəsində yaranan süzgəc siqnalının təhrifi və ya səs-küyü;

- daxil olan siqnalı gücləndirmək və daha dəqiq ötürmə üçün onun formasını bərpa etmək;
- siqnalın sinxronizasiyası (Ethernet şəbəkələrində);
- siqnalı bütün kabel seqmentlərində təkrarlamaq.

Sinxronizasiya kabelə siqnal ötürüldükdə Ethernet şəbəkəsində siqnal toqquşmasının qarşısını alır. Təkrarlayıcılar aşağıdakı vəzifələri yerinə yetirməyə imkan verir:

- kabel sistemini uzatmaq (məsələn, 10Base2 seqmenti üçün 185 m-dən və 10Base5 üçün 500 m-dən çox məsafəyə);
- qoşulmuş qovşaqların sayını artırmaq seqmentə qoyulan məhdudiyyətləri keçmək;
- şəbəkə xətasını tanımaq və kabel seqmentini ayırmaq;
- hublar və açarlar kimi digər şəbəkə cihazlarının komponentlərinə qoşulmaq və siqnalları gücləndirmək və sinxronlaşdırmaq;
- müxtəlif ötürmə vasitələri ilə işləyən seqmentləri birləşdirin (məsələn, 10BaseT seqmentini 10Base2 seqmentinə və ya 10Base2 seqmentini 10Base5 seqmentinə qoşun);
- yerli və qlobal şəbəkələrdə magistral kabel seqmentlərinin genişləndirilməsi;
- fiber optik kabel seqmentlərini genişləndirmək;
- T xətləri üçün iş məsafəsini artırmaq.

Təkrarlayıcı siqnalı iki və ya daha çox kabel seqmentinə ötürürsə, ona çoxportlu təkrarlayıcı deyilir. Məsələn, təkrarlayıcıda 2-8 əlavə seqment üçün portlar ola bilər. Müəyyən bir portdan uzanan kabel normal kabel seqmenti hesab olunur. Yəni, çoxportlu 10Base2 şəbəkə təkrarlayıcısı 185 m uzunluğunda bir neçə kabelə siqnal ötürə bilər.

IEEE spesifikasiyasına əsasən, qalın koaksial kabelin uzunluğunu 2500 m-ə, nazik koaksial kabelin uzunluğunu isə 1000 m-ə qədər artırmaq üçün dörd təkrarlayıcı istifadə edilə bilər, şəbəkə topologiyasından və istifadə olunan ötürücü mühitdən asılı olaraq, bir məlumat paketi dörddən çox təkrarlayıcıdan keçə bilər. İki

qovşaq arasında dörd təkrarlayıcı varsa, ən azı iki birləşdirən seqmentdə heç bir kompüter qoşulmamalıdır.

Təkrarlayıcılar həm yerli, həm regional şəbəkələrdə, həm də qlobal şəbəkələrdə istifadə olunur. Məsələn, T-1 xəttinə əsaslanan qlobal şəbəkə hər 2,2 km-də təkrarlayıcılar yerləşdirməklə genişləndirilə bilər. (Владыко, А.Г. 2016)

Bir çox təkrarlayıcılarda müxtəlif növ daxil olan kabel birləşmələri üçün nəzərdə tutulmuş portlar var (məsələn, qalın və nazik Ethernet kabeli). Müvafiq ötürücüdən istifadə edərkən bir çox təkrarlayıcılarda koaksial və ya fiber optik magistrala qoşulmaq üçün AUI portu da var. Çıxış portları adətən nazik koaksial kabel üçün nəzərdə tutulub, lakin digər variantlar da mövcuddur.

Təkrarlayıcılar hər bir çıxış kabeli seqmentinin sağlamlığını davamlı olaraq izləyir. Səhv baş verərsə, təkrarlayıcı məlumatların səhv seqmentə ötürülməsini dayandırır. Seqmenti ayırmağın bu üsulu izolyasiya və ya bölmə adlanır. Seqment təcrid edildikdə, həmin seqmentdəki heç bir qovşaq məlumatları ötürə bilməz. Şəbəkə problemi həll edildikdən sonra təkrarlayıcı seqmenti yenidən işə sala və məlumatın ötürülməsini davam etdirə bilər.

Sadə təkrarlayıcılar koaksial şəbəkələrdə köhnə avtobus topologiyalarını genişləndirmək üçün ucuz həll yolu təqdim edir. Yeni şəbəkənin layihələndirilməsi zamanı əvvəldən daxili təkrarlayıcı imkanlarına (məsələn, mərkəzləşdirilmiş açarlar) malik olan müasir avadanlıqlardan istifadə edir.

Çoxportlu təkrarlayıcıdan istifadə edərkən şəbəkəni elə dizayn edin ki, bir seqmentdə minimum sayda qovşaq olsun. Məsələn, 40 iş stansiyası olan bir şəbəkə üçün hər biri 10 stansiyadan ibarət dörd seqment yaradın (12 və 28 qovşaqlı iki seqmentdən daha çox), bu halda müəyyən bir seqmentin təcrid edilməsi kompüterlərin minimum sayına təsir edəcəkdir. (Олифер Н. А., Олифер В. Г. 2017)

Təkrarlayıcıların üstünlüklərindən biri də odur ki, onlar şəbəkəni genişləndirmək üçün ucuz üsuldur. Dezavantaj odur ki, onlar məşğul şəbəkədə əlavə trafik yarada bilirlər, çünki onlar gələn siqnalı bütün gedən seqmentlərə yenidən yayımlayırlar. Bu trafikin əksəriyyəti faydasızdır, çünki hədəf nodu olmayan seqmentlərə məlumat göndərməyin mənası yoxdur.

Switch. Switch və onun səmərəliliyini (çox sayda port daha az trafik deməkdir) və performansını artıra bilən dizaynı olan çoxportlu körpüdür. Keçid məlumatları ötürməzdən əvvəl səhv yoxlamasını həyata keçirə bilər ki, bu da onu çox səmərəli edir, çünki səhvləri olan paketləri yönləndirmir və yaxşı paketləri seçərək yalnız düzgün porta yönləndirmir. Başqa sözlə, keçid hostların toqquşma domenini bölür, lakin yayım domeni eyni qalır.

Unmanaged switches: Bu switch-lər sadə plug-and-play dizaynına malikdir və qabaqcıl konfiqurasiya variantları təklif etmir. Onlar kiçik şəbəkələr üçün və ya daha böyük bir şəbəkənin genişləndirilməsi kimi istifadə üçün uyğundur.

Managed switches: Bu switch-lər VLAN, QoS və link aqreqasiyası kimi qabaqcıl konfiqurasiya seçimlərini təklif edir. Onlar daha böyük, daha mürəkkəb şəbəkələr üçün uyğundur və mərkəzləşdirilmiş idarəetməyə imkan verir.

Smart switches: Bu switch-lər idarə olunan açarlara bənzər xüsusiyyətlərə malikdir, lakin adətən qurmaq və idarə etmək daha asandır. Onlar kiçik və orta ölçülü şəbəkələr üçün uyğundur.

Layer 2 switches: Bu switch-lər OSI modelinin Data Link qatında işləyir və eyni şəbəkə seqmentindəki cihazlar arasında məlumatların ötürülməsinə cavabdehdirlər.

Layer 3 switches: Bu switch-lər OSI modelinin Şəbəkə müstəvisində işləyir və müxtəlif şəbəkə seqmentləri arasında məlumatları yönləndirə bilir. Onlar Layer 2 açarlarından daha təkmildir və tez-tez daha böyük, daha mürəkkəb şəbəkələrdə istifadə olunur.

PoE switches: Bu switch-lər Ethernet üzərindən güc imkanlarına malikdir ki, bu da onlara məlumat daşıyan eyni kabel vasitəsilə şəbəkə cihazlarına enerji verməyə imkan verir.

Gigabit switches: Bu switch-lər ənənəvi Ethernet sürətlərindən daha sürətli olan Gigabit Ethernet sürətlərini dəstəkləyir.

Rack-mounted switches: Bu switch-lər server rafına quraşdırılmaq üçün nəzərdə tutulmuşdur və məlumat mərkəzlərində və ya digər böyük şəbəkələrdə istifadə üçün uyğundur.

Desktop switches: Bu switch-lər masa üstü və ya kiçik ofis mühitində istifadə üçün nəzərdə tutulmuşdur və adətən rəfdə quraşdırılmış açarlardan daha kiçik ölçülüdür.

Modular switches: Bu switch-lər asan genişləndirməyə və ya fərdiləşdirməyə imkan verən modul dizayna malikdir. Onlar böyük şəbəkələr və məlumat mərkəzləri üçün uyğundur.

Proxy server. Proxy server istifadəçilər və internet arasında şlüz təmin edən sistem və ya marşrutlaşdırıcıdır. Buna görə də, kiber hücumçuların şəxsi şəbəkəyə daxil olmasının qarşısını alır. Bu, son istifadəçilər və onlayn ziyarət etdikləri veb səhifələr arasında keçdiyi üçün "vasitəçi" adlandırılan bir serverdir. Kompüter internetə qoşulduqda bir IP ünvanından istifadə edir. Bu, evinizin küçə ünvanına bənzəyir, daxil olan məlumatları hara gedəcəyini söyləyir və digər cihazların autentifikasiyası üçün gedən məlumatları qaytarma ünvanı ilə qeyd edir. Proksi server əslində internetdə özünəməxsus IP ünvanına malik kompüterdir. Proksilər kompüteriniz üçün qiymətli təhlükəsizlik qatını təmin edir. Onlar kompüterinizi zərərli proqram kimi internet təhdidlərindən qoruyan veb filtrlər və ya firewall kimi quraşdırıla bilər. Bu əlavə təhlükəsizlik təhlükəsiz veb şlüz və ya digər e-poçt təhlükəsizliyi məhsulları ilə birləşdirildikdə də dəyərlidir. Bu yolla siz trafiki onun təhlükəsizlik müstəvisinə və ya şəbəkənizin və ya fərdi kompüterlərin nə qədər trafiki idarə edə biləcəyinə görə filtrləyə bilərsiniz. Bəzi insanlar, məsələn, onlayn filmlərə baxarkən yerlərini gizlətmək kimi şəxsi məqsədlər üçün proksilərdən istifadə edirlər. Bununla belə, bir şirkət üçün bunlar bir neçə əsas vəzifəni yerinə yetirmək üçün istifadə edilə bilər, məsələn:

İşçilərin internet fəaliyyətini onlara göz yummağa çalışan insanlardan qorumaq, qəzaların qarşısını almaq üçün internet trafikini balanslaşdırmaq

Veb saytların işçilərinə və ofisdəki işçilərin girişinə nəzarət etmək. Faylları keşləmək və ya daxil olan trafiki sıxaraq bant genişliyinə qənaət etmək.

Proksi serverin öz IP ünvanı olduğu üçün o, kompüter və internet arasında keçid rolunu oynayır. Kompüteriniz bu ünvanı bilir və siz internetdə sorğu göndərdiyiniz zaman o, proksiyə yönləndirilir, sonra o, veb serverdən cavab alır və məlumatları

səhifədən Chrome, Safari, Firefox kimi kompüterinizin brauzerinə ötürür. və ya Microsoft Edge. Aparat və proqram təminatı versiyaları var. Avadanlıq əlaqələri şəbəkəniz və internet arasında oturur, burada internetdən məlumatları alır, göndərir və yönləndirir. Proqram təminatı proksiləri adətən provayder tərəfindən yerləşdirilir və ya buludda yerləşir. Siz kompüterinizə proksi ilə qarşılıqlı əlaqəni asanlaşdıran proqramı yükləyib quraşdırırsınız.

Çox vaxt proqram proksisini aylıq ödəniş üçün əldə etmək olar. Bəzən pulsuzdurlar. Pulsuz versiyalar istifadəçilərə daha az ünvan təklif etməyə meyllidir və yalnız bir neçə cihazı əhatə edə bilər, pullu proksilər isə bir çox cihazla biznesin tələblərinə cavab verə bilər. Proksi serverlə işə başlamaq üçün onu kompüterinizdə, cihazınızda və ya şəbəkənizdə konfiqurasiya etməlisiniz. Hər bir əməliyyat sisteminin öz quraşdırma prosedurları var, ona görə də kompüteriniz və ya şəbəkəniz üçün tələb olunan addımları yoxlayın.

Əksər hallarda quraşdırma avtomatik konfiqurasiya skriptindən istifadə deməkdir. Bunu əl ilə etmək istəyirsinizsə, IP ünvanını və müvafiq portu daxil etmək üçün seçimlər olacaq.

Proksi server firewall və filtr funksiyasını yerinə yetirir. Son istifadəçi və ya şəbəkə administratoru məlumat və məxfiliyi qorumaq üçün nəzərdə tutulmuş proksi seçə bilər. Bu, kompüterinizə və ya şəbəkənizə daxil olan və çıxan məlumatları yoxlayır. Daha sonra rəqəmsal ünvanınızı dünyaya göstərməyin qarşısını almaq üçün qaydalar tətbiq edir. Yalnız proksinin IP ünvanı hakerlər və ya digər pis aktyorlar tərəfindən görülür. Şəxsi IP ünvanınız olmadan internetdəki insanların şəxsi məlumatlarınıza, cədvəllərinizə, proqramlarınıza və ya fayllarınıza birbaşa çıxışı yoxdur.

Onun yerində olduğu halda, veb sorğuları proksiyə gedir, sonra o, uzanır və internetdən istədiyinizi alır. Əgər serverin şifrələmə imkanları varsa, parollar və digər şəxsi məlumatlar əlavə qorunma müstəvisi əldə edir.

Proksilər biznesinizə üstünlük verə biləcək bir sıra üstünlüklərə malikdir:

Enhanced security: Sistemləriniz və internet arasında təhlükəsizlik divarı kimi fəaliyyət göstərə bilər. Onlar olmadan, hakerlər kompüterinizə və ya şəbəkənizə

sızmaq üçün istifadə edə biləcəkləri IP ünvanınıza asanlıqla daxil olurlar. Şəxsi gözdən keçirmə, izləmə, dinləmə və alış-veriş, istənməyən reklamlar və ya IP-xüsusi məlumatların toplanması ilə su altında qalmamağınıza kömək etmək üçün müxtəlif proksilərdən istifadə edin. Proksi ilə sayta baxış yaxşı qorunur və izləmək mümkün deyil.

Məkanla bağlı xüsusi məzmuna giriş: Siz başqa ölkə ilə əlaqəli ünvanı olan bir proxy server təyin edə bilərsiniz. Siz faktiki olaraq, özünüzü həmin ölkədə olduğunuz kimi göstərə və həmin ölkədə əlaqə saxlamağa icazə verilən bütün məzmun kompüterlərinə tam giriş əldə edə bilərsiniz. Məsələn, texnologiya sizə görünmək istədiyiniz məkanın yerli IP ünvanlarından istifadə etməklə məkan məhdudiyyəti olan veb-saytları açmağa imkan verə bilər. İşçilərin qeyri-münasib və ya diqqəti yayındıran saytlara baxmasının qarşısını alın: Ondan işləyən veb-saytlara girişi bloklamaq üçün istifadə edə bilərsiniz. təşkilatınızın prinsiplərinə zidd. Həmçinin, adətən işçilərin diqqətini vacib işlərdən yayındıran saytları bloklaya bilərsiniz. Bəzi təşkilatlar vaxt itkisini aradan qaldırmaq üçün Facebook və digərləri kimi sosial media saytlarını bloklayır.

Bütün proksi serverlər istifadəçilərə internetdən istifadə etmək üçün alternativ ünvan versə də, hər birinin öz xüsusiyyətləri olan bir neçə müxtəlif növ var. Proksi növlərinin siyahısının arxasındakı təfərrüatları başa düşmək istifadə vəziyyətinizə və xüsusi ehtiyaclarınıza əsaslanaraq seçim etməyə kömək edəcək.

Forward Proxy. Müştərilərin qarşısında oturur yerləşir və məlumatları daxili şəbəkədəki istifadəçi qruplarına ötürmək üçün istifadə olunur. Sorğu göndərildikdə, proksi server əlaqə yaratmağa davam edib-etməməsinə qərar vermək üçün onu yoxlayır. Forward Proxy tək bir giriş nöqtəsi tələb edən daxili şəbəkələr üçün ən yaxşısıdır. O, şəbəkədəkilər üçün IP ünvan təhlükəsizliyini təmin edir və birbaşa inzibati nəzarətə imkan verir. Bununla belə, Forward Proxy təşkilatın fərdi son istifadəçilərin ehtiyaclarını ödəmək qabiliyyətini məhdudlaşdıra bilər.

Transparent Proxy. İstifadəçilər ev kompüterlərindən istifadə etsəydilər, eyni təcrübəni yaşaya bilərdilər. Şəffaf proksilər, işçilərə proksidən istifadə etdiklərini bildirmədən istifadə etmək istəyən şirkətlər üçün çox uyğundur. Problemsiz

istifadəçi təcrübəsi təmin etmək üstünlüyünü daşıyır. Digər tərəfdən, şəffaf proksi-serverlər SYN-flood xidmətdən imtina hücumları kimi müəyyən təhlükəsizlik təhdidlərinə daha çox həssasdırlar.

Anonymous Proxy. İnternet fəaliyyətini izlənilməz hala gətirməyə diqqət yetirir. O, şəxsiyyətini və kompüter məlumatlarını gizlədərkən istifadəçi adından internetə daxil olaraq işləyir. Anonim proxy internetə daxil olarkən tam anonimlik əldə etmək istəyən istifadəçilər üçün ən uyğundur. Anonim proksilər mümkün olan ən yaxşı şəxsiyyət qorunmasını təmin etsə də, çatışmazlıqları da yoxdur. Bir çoxları anonim proksilərin istifadəsinə əlçatanlıq kimi baxır və istifadəçilər bəzən bunun nəticəsində geri çəkilmə və ya ayrı-seçkiliklə üzləşirlər.

High Anonymity Proxy. Anonimliyi bir addım irəli aparan anonim bir proxydir. Proksi hədəf sayta qoşulmağa cəhd etməzdən əvvəl məlumatlarınızı silməklə işləyir. Server anonimliyin mütləq zərurət olduğu istifadəçilər üçün, məsələn, fəaliyyətinin təşkilata qədər izlənilməsini istəməyən işçilər üçün ən uyğundur. İşin mənfi tərəfi, onlardan bəziləri, xüsusən də pulsuz olanlar, şəxsi məlumatlarına və ya məlumatlarına daxil olmaq üçün istifadəçiləri tələyə salmaq üçün qurulmuş hiylələrdir.

Distorting Proxy. Özünü veb-saytın proksisi kimi tanıdır, lakin öz şəxsiyyətini gizlədir. O, bunu öz IP ünvanını səhv birinə dəyişdirməklə edir. Proksilərin təhrif edilməsi internetə daxil olarkən yerlərini gizlətmək istəyən insanlar üçün yaxşı seçimdir. Bu proksi növü onu müəyyən bir ölkədən baxdığınız kimi göstərə bilər və sizə təkcə şəxsiyyətinizi deyil, həm də proksinin kimliyini gizlətmək üstünlüyü verə bilər. Bu o deməkdir ki, hətta proksi ilə əlaqəli olsanız belə, şəxsiyyətiniz hələ də təhlükəsizdir. Bununla belə, bəzi veb-saytlar təhrif edən proksiləri avtomatik bloklayır ki, bu da son istifadəçinin ehtiyac duyduğu saytlara daxil olmasına mane ola bilər.

Data Center Proxy. İnternet xidmət provayderi (ISP) ilə əlaqəli deyil, lakin məlumat mərkəzi vasitəsilə başqa korporasiya tərəfindən təmin edilir. Proksi server fiziki məlumat mərkəzində mövcuddur və istifadəçinin sorğuları həmin server vasitəsilə yönləndirilir. Məlumat mərkəzi proksiləri sürətli cavab müddətinə və ucuz

həllə ehtiyacı olan insanlar üçün yaxşı seçimdir. Buna görə də, onlar bir şəxs və ya təşkilat haqqında çox tez kəşfiyyat toplamalı olan insanlar üçün yaxşı seçimdir. Onlar istifadəçilərə məlumatları tez və ucuz qiymətə toplamaq səlahiyyəti vermək üstünlüyünü daşıyırlar. Digər tərəfdən, onlar istifadəçilərin məlumatlarını və ya şəxsiyyətlərini riskə ata biləcək ən yüksək müstəvidə anonimlik təklif etmirlər.

Residential Proxy. İstifadəçiyə müəyyən, fiziki cihaza aid bir IP ünvanı verir. Bütün sorğular daha sonra həmin cihaz vasitəsilə ötürülür. Yaşayış etibarnamələri veb-saytlarına daxil olan reklamları yoxlamalı olan istifadəçilər üçün çox uyğundur, beləliklə, siz rəqiblərin və ya pis aktyorların kukiləri, şübhəli və ya arzuolunmaz reklamlarını bloklaya bilərsiniz. Yaşayış etibarnamələri digər proxy seçimlərindən daha etibarlıdır. Bununla belə, onlardan istifadə etmək çox vaxt daha çox pula başa gəlir, buna görə də istifadəçilər faydaların əlavə investisiyaya dəyər olub olmadığını diqqətlə təhlil etməlidirlər.

Public Proxy. Hər kəs tərəfindən pulsuz istifadə edilə bilər. Bu, istifadəçilərə IP ünvanlarına giriş imkanı verməklə, saytları ziyarət edərkən şəxsiyyətlərini gizlətməklə işləyir. İctimai proksilər, qiymətin böyük narahatlıq doğurduğu, təhlükəsizliyin və sürətin olmadığı istifadəçilər üçün ən uyğundur. Onlar pulsuz və asanlıqla əldə edilə bilsələr də, çox vaxt yavaş olurlar, çünki pulsuz istifadəçilərlə sıxılırlar. İctimai bir proksidən istifadə etdiyiniz zaman sizin məlumatınızın internetdə başqaları tərəfindən əldə edilməsi riski də artır.

Shared Proxy. Eyni anda birdən çox istifadəçi tərəfindən istifadə olunur. Onlar sizə başqa insanlar tərəfindən paylaşıla bilən IP ünvanına giriş imkanı verir və sonra siz seçdiyiniz yerdən gözdən keçirdiyiniz zaman internetdə gəzə bilərsiniz. Paylaşılan proksilər xərcləmək üçün çox pulu olmayan və mütləq sürətli əlaqəyə ehtiyacı olmayan insanlar üçün möhkəm seçimdir. Paylaşılan proxy-nin əsas üstünlüyü onun aşağı qiymətidir. Onlar başqaları tərəfindən paylaşıldığı üçün başqasının səhv qərarlarına görə günahlandırıla bilərsiniz və bu da sizi saytdan kənarlaşdıra bilər.

SSL Proxy. Təhlükəsiz yuva təbəqəsi (SSL) proksi müştəri və server arasında şifrənin açılmasını təmin edir. Məlumatlar hər iki istiqamətdə şifrələndiyi üçün proksi öz mövcudluğunu həm müştəridən, həm də serverdən gizlədir.

Bu proksilər SSL protokolunun aşkar etdiyi və dayandırdığı təhdidlərə qarşı gücləndirilmiş qorunmaya ehtiyacı olan təşkilatlar üçün ən uyğundur. Google SSL-dən istifadə edən serverlərə üstünlük verdiyi üçün, vebsaytla əlaqəli istifadə edildikdə SSL proxy-si onun axtarış sisteminin sıralamasına kömək edə bilər. İşin mənfi tərəfi, SSL proxy-də şifrələnmiş məzmunu keşdə saxlamaq mümkün deyil, buna görə də veb-saytlara dəfələrlə daxil olanda, başqa cür olduğundan daha yavaş performansla qarşılaşa bilərsiniz.

Rotating Proxy. Ona qoşulan hər bir istifadəçiyə fərqli bir IP ünvanı təyin edir. İstifadəçilər qoşulduqca, onlara ondan əvvəl qoşulmuş cihazdan unikal olan ünvan verilir. Fırlanan proksilər çoxlu yüksək həcmli, davamlı veb kazıma etməli olan istifadəçilər üçün idealdır. Onlar sizə anonim olaraq təkrar-təkrar eyni vebsayta qayıtmağa imkan verir. Bununla belə, fırlanan proxy xidmətləri seçərkən diqqətli olmalısınız. Onların bəzilərində məlumatlarınızı ifşa edə biləcək ictimai və ya paylaşılan proksilər var.

Reverse Proxy. Müştərilərin qarşısında oturan irəli proksidən fərqli olaraq, əks proksi veb serverlərin qarşısında yerləşdirilir və sorğuları brauzerdən veb serverlərə yönləndirir. O, veb serverin şəbəkə kənarında istifadəçidən gələn sorğuları ələ keçirməklə işləyir. Daha sonra sorğuları mənbə serverinə göndərir və ondan cavablar alır.

Reverse Proxy. bir çox daxil olan sorğuların yükünü tarazlaşdırmağa ehtiyacı olan məşhur veb saytlar üçün güclü seçimdir. Onlar təşkilata bant genişliyi yükünü azaltmağa kömək edə bilər, çünki onlar daxil olan sorğuları idarə edən başqa bir veb server kimi fəaliyyət göstərirlər. İşin mənfi tərəfi odur ki, əks proksilər, təcavüzkar ona nüfuz edə bilsə, HTTP server arxitekturasını potensial olaraq ifşa edə bilər. Bu o deməkdir ki, şəbəkə administratorları əks proksi istifadə etdikdə təhlükəsizlik divarını gücləndirməli və ya yerini dəyişdirməli ola bilər.

SDN, şəbəkə arxitekturası yanaşması olan Software Defined Network deməkdir. Proqram proqramlarından istifadə edərək şəbəkəni idarə etməyə və idarə etməyə imkan verir. Proqram təminatı ilə müəyyən edilmiş Şəbəkə (SDN) vasitəsilə bütün şəbəkənin və onun cihazlarının şəbəkə davranışı açıq API-lərdən istifadə edən proqram proqramları vasitəsilə mərkəzdən idarə olunan şəkildə proqramlaşdırılır. Proqram təminatı ilə müəyyən edilmiş şəbəkələri başa düşmək üçün biz şəbəkədə iştirak edən müxtəlif müstəvilər başa düşülməlidir:

- Məlumat müstəvisi;
- İdarəetmə müstəvisi.

Məlumat müstəvisi: Son istifadəçi tərəfindən göndərilən məlumat paketləri ilə bağlı bütün fəaliyyətlər bu müstəviyə aiddir. Bura daxildir:

- Paketlərin yönləndirilməsi;
- Məlumatların seqmentasiyası və yenidən yığılması;
- Multicasting üçün paketlərin təkrarlanması.

İdarəetmə müstəvisi: Məlumat müstəvisi fəaliyyətlərini yerinə yetirmək üçün lazım olan, lakin son istifadəçi məlumat paketlərini əhatə etməyən bütün fəaliyyətlər bu müstəviyə aiddir. Başqa sözlə, bu şəbəkənin beynidir. İdarəetmə müstəvisiinin fəaliyyətlərinə aşağıdakılar daxildir:

Marşrut cədvəllərinin hazırlanması.

Paketlə işləmə siyasətinin qurulması.

Daha yaxşı Şəbəkə Bağlantısı: SDN satış, xidmətlər və daxili kommunikasiyalar üçün çox yaxşı şəbəkə bağlantısı təmin edir. SDN həmçinin daha sürətli məlumat mübadiləsinə kömək edir.

Tətbiqlərin Daha Yaxşı Yerləşdirilməsi: Yeni proqramların, xidmətlərin və bir çox biznes modellərinin yerləşdirilməsi Proqram Təminatlı Şəbəkədən istifadə etməklə sürətləndirilə bilər.

Daha yaxşı təhlükəsizlik: Proqram təminatı ilə müəyyən edilmiş şəbəkə bütün şəbəkədə daha yaxşı görünürlük təmin edir. Operatorlar müxtəlif müstəvili təhlükəsizlik tələb edən cihazlar üçün ayrıca zonalar yarada bilərlər. SDN şəbəkələri operatorlara daha çox azadlıq verir.

Yüksək Sürətlə Daha Yaxşı İdarəetmə: Proqram təminatı ilə müəyyən edilmiş şəbəkə açıq standart proqram əsaslı nəzarətçi tətbiq etməklə digər şəbəkə növlərinə nisbətən daha yaxşı sürət təmin edir.

• Müəssisələr ümumi yerləşdirmə və əməliyyat xərclərini azaltmaqla yanaşı, tətbiqləri daha sürətli yerləşdirmək üçün proqramların yerləşdirilməsi üçün ən çox istifadə edilən metod olan SDN-dən istifadə edirlər. SDN İT administratorlarına şəbəkə xidmətlərini bir yerdən idarə etməyə və təmin etməyə imkan verir;

• Bulud şəbəkəsi proqram təminatı ilə müəyyən edilmiş ağ qutu sistemlərindən istifadə edir. Bulud provayderləri tez-tez ümumi avadanlıqdan istifadə edirlər ki, Bulud məlumat mərkəzi dəyişdirilə bilsin və CAPEX və OPEX xərclərinə qənaət edilsin.

Proqram təminatının müəyyənləşdirilməsi şəbəkəsinin (SDN) komponentləri

SDN-i yaradan üç əsas komponent bunlardır:

1. SDN Tətbiqləri: SDN Tətbiqləri sorğuları və ya şəbəkələri API istifadə edərək SDN Controller vasitəsilə ötürür;

2. SDN nəzarətçisi: SDN Controller aparatdan şəbəkə məlumatlarını toplayır və bu məlumatı proqramlara göndərir;

3. SDN şəbəkə cihazları: SDN Şəbəkə cihazları məlumatların ötürülməsi və emalı tapşırıqlarında kömək edir.

SDN arxitekturası

Ənənəvi şəbəkədə hər bir keçidin öz məlumat müstəvisi, eləcə də idarəetmə müstəvisi var. Müxtəlif açarların idarəetmə müstəvisi topologiya məlumatlarını mübadilə edir və beləliklə, daxil olan məlumat paketinin məlumat müstəvisi vasitəsilə hara yönləndiriləcəyinə qərar verən yönləndirmə cədvəli qurur. Proqram təminatı ilə müəyyən edilmiş şəbəkə (SDN) idarəetmə müstəvisini keçiddən ayırdığımız və onu SDN nəzarətçisi adlanan mərkəzləşdirilmiş bölməyə təyin etdiyimiz bir yanaşmadır. Beləliklə, şəbəkə administratoru fərdi açarlara toxunmadan mərkəzləşdirilmiş konsol vasitəsilə trafiki formalaşdıra bilər. Məlumat müstəvisi hələ də kommutatorda yerləşir və paket keçidə daxil olduqda, onun ötürülməsi fəaliyyəti nəzarətçi tərəfindən əvvəlcədən təyin edilmiş axın

cədvəllərinin qeydləri əsasında qərarlaşdırılır. Axın cədvəli uyğunluq sahələrindən (giriş port nömrəsi və paket başlığı kimi) və təlimatlardan ibarətdir. Paket əvvəlcə axın cədvəli girişlərinin uyğunluq sahələrinə uyğunlaşdırılır. Sonra müvafiq axın girişinin göstərişləri yerinə yetirilir. Təlimatlar paketi bir və ya bir neçə port vasitəsilə yönləndirmək, paketi atmaq və ya paketə başlıqlar əlavə etmək ola bilər. Paket axın cədvəlində müvafiq uyğunluq tapmazsa, keçid keçidə yeni axın girişi göndərən nəzarətçini sorğulayır. Keçid bu axın girişinə əsasən paketi irəli aparır və ya buraxır.

Tipik bir SDN arxitekturası üç qatdan ibarətdir:

• Tətbiq müstəvisi: O, müdaxilənin aşkarlanması, firewall və yük balansı kimi tipik şəbəkə proqramlarını ehtiva edir;

• İdarəetmə təbəqəsi: Şəbəkənin beyni rolunu oynayan SDN nəzarətçisindən ibarətdir. O, həmçinin üzərində yazılmış proqramlara aparat abstraksiyasına imkan verir;

• İnfrastruktur təbəqəsi: Bu, məlumat müstəvisini təşkil edən və məlumat paketlərinin faktiki hərəkətini həyata keçirən fiziki keçidlərdən ibarətdir.

SDN-də istifadə olunan bir neçə model var:

1. Open SDN
2. API vasitəsilə SDN
3. Hypervisor-based Overlay Network vasitəsilə SDN
4. Hibrid SDN

Open SDN: Open SDN OpenFlow keçidindən istifadə etməklə həyata keçirilir. Bu, SDN-nin sadə tətbiqidir. Open SDN-də nəzarətçi OpenFlow protokolunun köməyi ilə cənuba bağlı API istifadə edərək açarlarla əlaqə qurur.

API vasitəsilə SDN: API vasitəsilə SDN-də açarlar kimi uzaq cihazlardakı funksiyalar SNMP və ya CLI kimi ənənəvi metodlardan və ya Rest API kimi daha yeni metodlardan istifadə etməklə işə salınır. Burada cihazlar nəzarətçiyə API-lərdən istifadə edərək uzaq cihazları manipulyasiya etməyə imkan verən idarəetmə nöqtələri ilə təmin edilir.

Hypervisor-based Overlay Network vasitəsilə SDN: Hipervisor vasitəsilə SDN-də fiziki cihazların konfiqurasiyası dəyişməzdir. Bunun əvəzinə fiziki şəbəkə üzərindən Hypervisor əsaslı üst-üstə düşən şəbəkələr yaradılır. Yalnız fiziki şəbəkənin kənarındakı qurğular virtuallaşdırılmış şəbəkələrə qoşulur və bununla da fiziki şəbəkədəki digər cihazların məlumatlarını gizlədir.

Hibrid SDN: Hibrid Şəbəkə şəbəkədə müxtəlif növ funksiyaları dəstəkləmək üçün bir şəbəkədə proqram təminatı ilə müəyyən edilmiş şəbəkə ilə Ənənəvi Şəbəkələrin birləşməsidir.

SDN-nin üstünlükləri:

• Şəbəkə proqramlaşdırıla bilir və buna görə də fərdi açarlardan çox nəzarətçi vasitəsilə asanlıqla dəyişdirilə bilər;

• Hər keçid yalnız məlumat müstəvisinə ehtiyac duyduğundan, keçid aparatı ucuzlaşır;

• Aparat mücərrəddir, ona görə də proqramlar keçid satıcısından asılı olmayaraq nəzarətçinin üstünə yazıla bilər;

• Nəzarətçi trafikə nəzarət edə və təhlükəsizlik siyasətlərini yerləşdirə bildiyi üçün daha yaxşı təhlükəsizlik təmin edir. Məsələn, nəzarətçi şəbəkə trafikində şübhəli fəaliyyət aşkar edərsə, o, paketlərin marşrutunu dəyişdirə və ya buraxa bilər.

SDN-nin çatışmazlıqları:

• Şəbəkənin mərkəzdən asılılığı tək bir uğursuzluq nöqtəsi deməkdir, yəni nəzarətçi xarab olarsa, bütün şəbəkə təsirlənəcək;

• SDN-nin geniş miqyasda istifadəsi düzgün müəyyən edilməmiş və tədqiq edilməmişdir.

SD-WAN şəbəkələri təşkilatlar üçün şəbəkə infrastrukturunu genişləndirmək, təhlükəsizliyi təkmilləşdirmək və məhsuldarlığı artırmaq yolu kimi getdikcə populyarlaşır. SD-WAN vasitəsilə təşkilatlar geniş ərazi şəbəkələrini (WAN) təkmilləşdirə, işçilərinə və sistemlərinə daha yaxşı və daha etibarlı bağlantı təmin edə bilər – lakin bu, düzgün SD-WAN cihazları vasitəsilə dəstəklənməlidir. Bundan əlavə, SD-WAN texnologiyası ənənəvi WAN texnologiyası üzərində

işləyir, fərdi WAN kənar cihazlarının aparatını mücərrədləşdirir, mərkəzləşdirilmiş konfiqurasiya və idarəetməyə imkan verir.

Qeyd edildiyi kimi, SD-WAN WAN-ın aparat cihazlarını idarə edən proqram sistemidir. Təşkilat hələ də SD-WAN nəzarətçisi ilə şəbəkə qurmaq üçün sxemləri və WAN kənar cihazlarını dizayn etməli və satın almalıdır.

Ənənəvi WAN sistemləri altında hər bir cihaz öz şəbəkə bağlantısını və təhlükəsizliyini idarə etməli və saxlamalıdır; xüsusiyyətlər və funksionallıq hardware ilə məhdudlaşır və proqram təminatı ilə idarə olunur və təşkilatdan öz sisteminin təhlükəsizliyini və sabitliyini konfiqurasiya etmək və saxlamaq üçün hər bir cihazda xeyli təkrarlanan iş görmək tələb olunur.

Sürətlə sənaye standartına çevrilən SD-WAN sistemi ilə təşkilatlar öz şəbəkələrini aparat deyil, proqram təminatı vasitəsilə mərkəzləşdirilmiş şəkildə idarə edə və genişləndirə bilərlər. SD-WAN nəzarətçisi fiziki cihazları idarə edir və eyni anda bütün şəbəkənin konfiqurasiyasına, performansına və təhlükəsizliyinə nəzarət edir.

SD-WAN texnologiyası buna görə də sistemi daha geniş, daha təhlükəsiz, saxlanması asan və istifadəsini asanlaşdırır. Təşkilatlar SD-WAN texnologiyasının sadələşdirilmiş idarəçiliyindən, eləcə də gücləndirilmiş təhlükəsizlik və gələcəyə nəzarətdən istifadə edə bilirlər. Həmçinin, SD-WAN, VPN-lərin mərkəzləşdirilməsi, idarə olunması və optimallaşdırılması üçün daha yüksək səviyyədə müdaxilə və avtomatlaşdırma imkanı təmin edir. (Zəkiyeva N., Məmmədov S., 2024)

Lakin SD-WAN nəzarətçisinin işləmək üçün hələ də etibarlı WAN texnologiyasına ehtiyacı var, onun təkmilləşdirilməsi və ya peşəkar komanda tərəfindən inteqrasiyası tələb oluna bilər.

SD-WAN cihazı kimi tanınan SD-WAN marşrutlaşdırıcısı təşkilatların WAN bağlantılarına nəzarət etməyi asanlaşdırır. Çox vaxt SD-WAN marşrutlaşdırıcısı birbaşa WAN-a qoşulacaq, lakin SD-WAN marşrutlaşdırıcısı WAN infrastrukturuna tək son nöqtə bağlantısını təmin edir. SD-WAN sisteminin işləməsini asanlaşdırmaq üçün bu cihazları təmin edən satıcılar var.

SD-WAN marşrutlaşdırıcısına sahib olmaq təşkilatın WAN sistemi üzərində daha birbaşa nəzarətə malik olması deməkdir və onu yenidən daha sabit və təhlükəsiz edir. SD-WAN əsas WAN aparatının və bağlantılarının sabitliyinə güvənsə də, Proqram təminatı ilə müəyyən edilmiş WAN təşkilata eyni və ya daha çox bant genişliyinə, sürətə, sabitliyə və daha aşağı qiymətə təhlükəsizliyə nail olmaqla daha çox müxtəlif WAN əlaqə növlərindən istifadə etməyə imkan verir. Daha az idarəetmə mürəkkəbliyi ilə.

SD-WAN yerləşdirilməsinin qurulmasının çətin olması lazım deyil, xüsusən də artıq möhkəm və etibarlı WAN yerləşdirməsi varsa. Təşkilat İdarəetmə/Nəzarətçi dəstini yerləşdirməklə başlaya və sonra SD-WAN Edge cihazlarını yerləşdirə bilər. Bir çox SD-WAN təchizatçıları idarəetmə-nəzarətçi dəstini xidmət kimi təklif edir, ona görə də heç bir yerli server yerləşdirməyə ehtiyac yoxdur.

SD-WAN yerləşdirməsinin üstünlüklərinə aşağıdakılar daxildir:

• Təşkilatlar öz şəbəkələrinin ən adi və təkrarlanan tapşırıqlarını avtomatlaşdıra bilir, bununla da inzibati yükü azaldır və sistemlərinin idarə edilməsini sadələşdirir;

• Təşkilatlar öz sistemlərinin sabitliyini təkmilləşdirə bilər, xüsusilə çoxlu və ya çoxlu işçilərin uzaqdan işlədiyi ofislər üçün vacibdir;

• Təşkilatlar, IoT və uzaq cihazların ələ keçirdiyi dünya üçün həyati əhəmiyyət kəsb edən daha effektiv son nöqtə idarəetməsinə malik ola bilər;

• Təşkilatlar daha sərfəli və idarə olunması asan olan filial və uzaq ofislər üçün çoxlu WAN son nöqtələrini yerləşdirə bilər;

• Təşkilatlar öz təhlükəsizliklərini təkmilləşdirə bilərlər, bu, Bulud ilə daha bağlı dünyada kritik əhəmiyyət kəsb edir.

Ancaq hələlik alış-veriş siyahılarını pozmayın. SD-WAN texnologiyasını təşkilatınızda uğurla yerləşdirməyin ən yaxşı yolu SD-WAN təcrübəsi olan təcrübəli İdarə olunan Xidmətlər Provayderi ilə əməkdaşlıq etməkdir. Əksər şəbəkə infrastrukturlarında olduğu kimi, SD-WAN yerləşdirilməsi bütün texnologiya və cihazların "birlikdə yaxşı işləməsini" tələb edir; onlar yaxşı inteqrasiya edilmiş,

konfiqurasiya edilmiş və uyğun olmalıdır və bunun üçün bir mütəxəssisin biliyi tələb olunur.

MSP sizə SD-WAN-ı uğurla yerləşdirməyə və onu təşkilatınızın ehtiyaclarına uyğunlaşdırmağa kömək edə bilər. Şirkətinizin hal-hazırda nəyə sahib olduğunu, eləcə də böyümək və inkişaf etmək üçün nəyə ehtiyacınız olduğunu ciddi qiymətləndirmədən başlayın. SD-WAN yerləşdirməniz şəbəkə infrastrukturunuzun əsasını təşkil edir, ona görə də təkcə bu gün etibarlı və təhlükəsiz deyil, həm də sabahın ehtiyaclarına uyğunlaşa biləcək bir sistemin təmin edilməsi çox vacibdir.
İndi hərəkət etmək vaxtıdır. Ətrafınızda SD-WAN-ın yerləşdirilməsinin bütün üstünlüklərini, sizə lazım olacaq cihazları, hətta SD-WAN quraşdırıldıqdan sonra idarə olunan xidmətləri və növbəti addımı necə atacağınızı kəşf etmək üçün Red River mütəxəssisləri ilə əlaqə saxlayın. Heç bir öhdəlik yoxdur; sadəcə görüş təyin etmək üçün zəng edin.

Şəbəkə funksiyalarının virtuallaşdırılması (NFV) şəbəkə cihazının avadanlığının virtual maşınlarla əvəz edilməsidir. Virtual maşınlar şəbəkə proqramlarını və marşrutlaşdırma və yük balansı kimi prosesləri idarə etmək üçün hipervizordan istifadə edir. NFV rabitə xidmətlərini marşrutlaşdırıcılar və təhlükəsizlik divarları kimi xüsusi avadanlıqlardan ayırmağa imkan verir. Bu ayırma o deməkdir ki, şəbəkə əməliyyatları dinamik şəkildə və yeni avadanlıq quraşdırmadan yeni xidmətləri təmin edə bilər. Şəbəkə komponentlərinin şəbəkə funksiyalarının virtuallaşdırılması ilə yerləşdirilməsi ənənəvi şəbəkələrdə olduğu kimi aylar əvəzinə saatlar çəkir. Həmçinin, virtuallaşdırılmış xidmətlər xüsusi avadanlıq əvəzinə daha ucuz, ümumi serverlərdə işləyə bilər. Günümüzdə böyük ofislər və şirkətlərdə hazırlanan virtual sistemlər, yəni programla idarə olunan şəbəkəkərdə təhlükəsizlik əsasən Active Directory funksiyası sayəsində qorunur. (Cəlilov A., 2024)
Şəbəkə funksiyalarının virtuallaşdırılmasından istifadə üçün əlavə səbəblərə aşağıdakılar daxildir:

• Daha az cihaz: NFV fiziki maşınlar əvəzinə virtual maşınlarda işlədiyi üçün daha az cihaz tələb olunur və əməliyyat xərcləri daha azdır.

• Ölçüləbilənlik: Şəbəkə arxitekturasını virtual maşınlarla miqyaslaşdırmaq daha sürətli və asandır və bu, əlavə avadanlıqların alınmasını tələb etmir.

Əslində, şəbəkə funksiyalarının virtuallaşdırılması fərdi aparat şəbəkə komponentləri tərəfindən təmin edilən funksionallığı əvəz edir. Bu o deməkdir ki, virtual maşınlar ənənəvi avadanlıqla eyni şəbəkə funksiyalarını yerinə yetirən proqram təminatını işlədirlər. Yük balansı, marşrutlaşdırma və təhlükəsizlik divarının təhlükəsizliyi bütün avadanlıq komponentləri əvəzinə proqram təminatı ilə həyata keçirilir. Hipervisor və ya proqram təminatı ilə müəyyən edilmiş şəbəkə nəzarətçisi şəbəkə mühəndislərinə virtual şəbəkənin bütün müxtəlif seqmentlərini proqramlaşdırmağa və hətta şəbəkənin təmin edilməsini avtomatlaşdırmağa imkan verir. İT menecerləri bir neçə dəqiqə ərzində bir şüşə panel vasitəsilə şəbəkə funksionallığının müxtəlif aspektlərini konfiqurasiya edə bilərlər.

Bir çox xidmət təminatçıları hesab edirlər ki, şəbəkə funksiyalarının virtuallaşdırılmasının faydaları risklərdən üstündür. Ənənəvi aparat əsaslı şəbəkələrlə şəbəkə menecerləri xüsusi aparat cihazları almalı və şəbəkə qurmaq üçün onları əl ilə konfiqurasiya etməli və birləşdirməlidir. Bu çox vaxt aparır və xüsusi şəbəkə təcrübəsi tələb edir.

NFV virtual şəbəkə funksiyasının hipervizor tərəfindən idarə olunan standart ümumi serverdə işləməsinə imkan verir ki, bu da xüsusi avadanlıq cihazlarının alınmasından daha ucuzdur. Şəbəkə konfiqurasiyası və idarə edilməsi virtuallaşdırılmış şəbəkə ilə daha sadədir. Ən yaxşısı, şəbəkə funksionallığı dəyişdirilə və ya əlavə edilə bilər, çünki şəbəkə asanlıqla təmin edilən və idarə olunan virtual maşınlarda işləyir.

NFV şəbəkəni daha həssas və çevik edir və asanlıqla genişlənə bilir. O, bazara çıxma müddətini sürətləndirə və avadanlıq xərclərini əhəmiyyətli dərəcədə azalda bilər. Bununla belə, təhlükəsizlik riskləri var və şəbəkə funksiyalarının virtualizasiyası ilə bağlı təhlükəsizlik narahatlıqları telekommunikasiya provayderləri arasında geniş tətbiq üçün maneə olduğunu sübut etdi. Şəbəkə funksiyalarının virtuallaşdırılmasının həyata keçirilməsində xidmət təminatçılarının nəzərə almalı olduğu bəzi risklər bunlardır:

Fiziki təhlükəsizlik nəzarətləri effektiv deyil: Şəbəkə komponentlərinin virtuallaşdırılması məlumat mərkəzində kilidlənmiş fiziki avadanlıqla müqayisədə onların yeni hücum növlərinə qarşı həssaslığını artırır.

Zərərli proqramı təcrid etmək və ehtiva etmək çətindir: Zərərli proqram təminatının hamısı bir virtual maşında işləyən virtual komponentlər arasında hərəkət etməsi, təcrid oluna və ya fiziki olaraq ayrıla bilən aparat komponentləri arasından daha asandır.

• **Şəbəkə trafiki daha az şəffafdır**: Ənənəvi trafik monitorinqi alətləri virtual maşınlar arasında şərqdən qərbə doğru hərəkət edən şəbəkə trafikində potensial zərərli anomaliyaları aşkar etməkdə çətinlik çəkir, buna görə də NFV daha incə təhlükəsizlik həlləri tələb edir.

• **Mürəkkəb təbəqələr bir çox təhlükəsizlik formalarını tələb edir**: Şəbəkə funksiyalarının virtualizasiya mühitləri mahiyyət etibarı ilə mürəkkəbdir, çoxlu təbəqələri əhatəli təhlükəsizlik siyasətləri ilə təmin etmək çətindir.

Ənənəvi şəbəkə arxitekturasında, marşrutlaşdırıcılar, açarlar, şlüzlər, təhlükəsizlik duvarları, yük balanslaşdırıcıları və müdaxilənin aşkarlanması sistemləri kimi fərdi mülkiyyətli aparat cihazları hamısı müxtəlif şəbəkə tapşırıqlarını yerinə yetirir. Virtuallaşdırılmış şəbəkə bu avadanlıq hissələrini şəbəkə tapşırıqlarını yerinə yetirmək üçün virtual maşınlarda işləyən proqram təminatı ilə əvəz edir.

NFV arxitekturası üç hissədən ibarətdir:

- **Centralized virtual network infrastructure**: NFV infrastrukturu ya konteyner idarəetmə platformasına, ya da hesablama, saxlama və şəbəkə resurslarını mücərrəd edən hipervizora əsaslana bilər;
- **Software applications**: Proqram təminatı müxtəlif növ şəbəkə funksionallığını (virtuallaşdırılmış şəbəkə funksiyaları) təmin etmək üçün ənənəvi şəbəkə arxitekturasının aparat komponentlərini əvəz edir;
- **Framework:** İnfrastrukturun idarə edilməsi və şəbəkə funksionallığının təmin edilməsi üçün çərçivə (çox vaxt MANO kimi tanınır – idarəetmə, avtomatlaşdırma və şəbəkə orkestrasiyası) lazımdır.

AT&T, China Mobile, BT Group, Deutsche Telekom və bir çox başqa şirkətlər daxil olmaqla xidmət təminatçıları konsorsiumu olan Avropa Telekommunikasiya Standartları İnstitutu (ETSI) şəbəkə funksiyalarının virtualizasiya standartı ideyasını ilk dəfə 2012-ci ildə OpenFlow Dünya Konqresində təqdim etmişdi. Bu xidmət təminatçıları şəbəkə xidmətlərinin yerləşdirilməsini sürətləndirmək üçün bir yol axtarırdı.

Yeni şəbəkə xidmətlərinin işə salınması əlavə aparat qutuları üçün yer və güc tələb edən çətin proses idi. Enerji və məkan xərcləri artdıqca və bacarıqlı şəbəkə aparat mühəndislərinin sayı azaldıqca, ETSI komitəsi bu problemlərin hər ikisini həll etmək üçün şəbəkə funksiyalarının virtuallaşdırılmasına müraciət etdi. NFV hardware cihazları üçün fiziki məkan ehtiyacını aradan qaldırır və konfiqurasiya və idarə etmək üçün intensiv şəbəkə təcrübəsi tələb etmir.

Bu gün ETSI, NFV üçün Açıq Platforma, Açıq Şəbəkə Avtomatlaşdırma Platforması, Açıq Mənbə MANO və MEF (əvvəllər Metro Ethernet Forumu) daxil olmaqla bir neçə açıq mənbəli layihə NFV standartlarının hazırlanması üzərində işləyir. Standartlar üçün rəqabətli təklifləri olan bir çox müxtəlif təşkilatlar xidmət təminatçılarının şəbəkə funksiyalarının virtuallaşdırılması ilə rahat olmasını çətinləşdirdi. Bununla belə, bu gün müəssisə şəbəkələrinin sürətlə genişlənən mürəkkəbliyi və tələbləri səbəbindən populyarlığı artır.

NFV şəbəkə xidmətlərini xüsusi aparat cihazlarından, proqram təminatı ilə müəyyən edilmiş şəbəkələşmədən və ya SDN-dən ayırsa da, marşrutlaşdırma, siyasətin müəyyən edilməsi və proqramlar kimi şəbəkəyə nəzarət funksiyalarını şəbəkə yönləndirmə funksiyalarından ayırır. SDN ilə virtual şəbəkə idarəetmə müstəvisi trafikin hara göndəriləcəyinə qərar verir və bütün şəbəkələri bir şüşə panel vasitəsilə proqramlaşdırmağa imkan verir. SDN şəbəkəyə nəzarət funksiyalarını avtomatlaşdırmağa imkan verir ki, bu da şəbəkənin dinamik iş yüklərinə tez cavab verməsini mümkün edir. Proqram təminatı ilə müəyyən edilmiş şəbəkə ya virtual şəbəkənin, ya da fiziki şəbəkənin üstündə otura bilər, lakin virtual şəbəkənin işləməsi üçün SDN tələb olunmur. Həm SDN, həm də NFV işləmək üçün virtuallaşdırma texnologiyasına əsaslanır.

Çoxsaylı giriş modulları. Çoxlu giriş vahidi (MAU) token ring şəbəkəsində mərkəzi mərkəz rolunu oynayır. Ağıllı çoxstansiyalı giriş vahidi (SMAU) termini modulun iş stansiyalarına qoşulmalarda nasazlıqları tapmaq və nasaz stansiyaları bütün şəbəkədən təcrid etmək qabiliyyətinə malik olduqda da istifadə olunur.

MAU modulları yalnız aşağıdakı funksiyaları yerinə yetirə bilən token ring şəbəkələrində istifadə olunur:

- •iş stansiyalarını fiziki ulduz topologiyası daxilində məntiqi halqaya birləşdirmək;
- • halqa ətrafında marker və çərçivələri köçürmək;
- •informasiya siqnallarını gücləndirmək;
- • marker halqasını genişləndirmək üçün ardıcıl zəncirlərdə birləşdirin;
- • verilənlərin düzgün hərəkətini təmin etmək;
- • nasaz qovşaqlarla əlaqəli portları söndürün.

Çoxlu giriş modulu şəbəkədəki stansiyaları işarə halqasına birləşdirən mərkəzdir. MSAU abbreviaturası bəzən onu təyin etmək üçün istifadə olunur.

Bütün şəbəkə cihazları tipik olaraq Tip 1, 2 (qoruyucu) və ya 3 (qoruyucusuz) burulmuş cüt kabeldən istifadə etməklə MAU modulu vasitəsilə işarə halqasına qoşulur. MAU modulu fiziki ulduz topologiyasını həyata keçirərək kadrları bir qovşaqdan digərinə ötürür, lakin məntiqi olaraq çərçivələr halqada olan kimi hərəkət edir. MAU modulu mərkəzi mərkəz rolunu oynayır və OSI Fiziki və Məlumat Bağlantısı müstəvilərində işləyir.

Ən sadə MAU modulu səkkizə qədər kabel seqmentini birləşdirir. Ən son modullarda qovşaqları birləşdirmək üçün 16 port var. MAU modulu passiv və ya aktiv mərkəz kimi çıxış edə bilər. Passiv hub yalnız stansiyadan stansiyaya siqnal ötürür. Siqnal hər dəfə MAU-dan keçəndə qismən zəifləyir və maksimum şəbəkə ötürmə qabiliyyətini azaldır. Məsələn, passiv qovşaqları və Tip 3 (UTP) kabelləri olan bir şəbəkə real olaraq 72-dən çox qovşağı birləşdirə bilməz. (Leconte M., 2018)

Aktiv qovşaq (active hub) hər dəfə növbəti qovşaqda hərəkət etdikdə siqnalları bərpa edir, sinxronlaşdırır və gücləndirir. Nəticədə Uzaq qovşaqlar iki dəfədən çox güclü siqnal alır. Dəstəklənən qovşaqların sayını artırır; bu halda aktiv hub

təkrarlayıcı kimi işləyir. Aktiv MAU-lardan istifadə edərkən Tip 3 kabel şəbəkəsində 150-yə qədər, Tip 1 və ya Tip 2 kabel şəbəkəsində isə 260-a qədər qovşaq ola bilər. 3-cü tip kabeldən istifadə edərkən qovşaqların maksimum sayı 1 və 2-ci növlərdən istifadə etdikdən daha azdır. Bu onunla izah olunur ki, 3-cü tip kabeldə titrəmə adlanan xeyli yüksək siqnal təhrifi olur.) və istənilən MAU modulunda giriş portu - Ring In (RI) və Ring Out (RO) portu. Bu portlar sizə MAU modullarını birləşdirməyə imkan verir. MALI modullarını birləşdirmək üçün istifadə olunan kabellər pat|H kabelləri, qovşağı MAU modulu ilə birləşdirən kabellər isə lob kabelləri adlanır. RI və RO portları arasındakı bağlantılar əlavə iş stansiyalarının şəbəkəyə qoşulmasına imkan verən işarə halqasının genişlənməsini təmin edir. Çoxlu MAU modullarından istifadə edərkən, birinci modulun RI portu ikinci modulun RI portuna qoşulur və bütün modullar birləşdirilənə qədər belə davam edir.

Körpü (Bridge) — şəbəkələr arasında paketlərin ötürülməsi vasitəsi (lokal), OSI modelinin iki aşağı müstəvisində işləyir və şəbəkə müstəvili protokollar üçün şəffafdır. Paket filtrasiyasını, şəbəkə daxilində yerləşən alıcılar üçün paketləri şəbəkədən buraxmamağı, həmçinin marşrutlaşdırma cədvəlinə uyğun olaraq paketləri başqa şəbəkəyə və ya cədvəldə ünvançı olmadıqda bütün digər şəbəkələrə yönləndirməyi həyata keçirir. Marşrutlaşdırma cədvəli adətən daxil olan paketin mənbə ünvanı əsasında öz-özünə öyrənmə prosesində tərtib edilir. Körpülər bir neçə meyarlara görə təsnif edilir:

Protokol müstəvisinə görə:

• MAC Layer Körpüləri media girişinə nəzarət alt qatında işləyir və eyni arxitekturaya malik (eyni paket formatları ilə) şəbəkələri birləşdirməyə imkan verir;

• MMC-Layer Körpüləri müxtəlif arxitekturalı (Ethernet - Token Ring - Arcnet) şəbəkələri birləşdirməyə imkan verən məntiqi keçid idarəetmə alt müstəvisində işləyir. (Лихачев В.А, 2014)

İzləmə alqoritminə görə:

• Şəffaf marşrutlaşdırma (şəffaf) - körpünün özü bütün qovşaqların yerini xatırlayaraq hər bir paket üçün marşrutu müəyyən edir. Ethernet şəbəkələrində istifadə olunur;

• Source Routing – paket izi paket mənbəyinin özü tərəfindən ünvan hissəsinə daxil edilir. Tokeng Ring-də istifadə olunur;

Serverə münasibətdə:

• daxili körpü (Internal Bridge) - müxtəlif şəbəkə adapterlərinə qoşulmuş seqmentlər arasında paketlərin yönləndirilməsini təmin edən server proqram təminatının bir hissəsi;

• xarici körpü (External, Stand-alone Bridge) - ayrıca qurğu.

Qoşulmuş şəbəkələr arasındakı məsafəyə görə:

• yerli körpü yaxınlıqdakı yerli şəbəkələri birləşdirir;

• uzaqdan Körpü coğrafi cəhətdən səpələnmiş yerli şəbəkələri telekommunikasiya vasitələri (xüsusi və ya dial-up telefon xətləri və s.) vasitəsilə birləşdirir.

Router — müxtəlif şəbəkələrin qovşaqları arasında əlaqəni təmin edən vasitə, OSI modelinin şəbəkə müstəvisində fəaliyyət göstərir, şəbəkə (məntiqi) ünvanlardan istifadə edir. Şəbəkələr xeyli məsafədə yerləşə bilər və paketin ötürüldüyü yol bir neçə marşrutlaşdırıcıdan keçə bilər. Şəbəkə ünvanı qovşağın yerinin iyerarxik təsviri kimi şərh olunur. Routerlər şəbəkə müstəvili protokolları dəstəkləyir: IP, IPX, X.25, IDP. Routerin əsas xüsusiyyətləri:

• növü: tək və ya çox protokol, LAN və ya WAN, Brouter;

• dəstəklənən protokollar;

• ötürmə qabiliyyəti;

• qoşulmuş şəbəkələrin növləri;

• dəstəklənən interfeyslər (LAN və WAN);

• portların sayı;

• şəbəkəni idarə etmək və monitorinq etmək bacarığı. (Kirichek R., 2016)

Şlyuz (Gateway) — İstifadəçi üçün şəffaf olan təkrarlayıcılardan, körpülərdən və routerlərdən fərqli olaraq, şlüzün olması görünür. Şlüz paket formatının və

ölçüsünün dəyişdirilməsini, protokolun konvertasiyasını, məlumatların konvertasiyasını həyata keçirir. Adətən böyük yaddaşa malik kompüterdə həyata keçirilir. Şlüzlərə nümunələr:

E-mail serverlər: yerli şəbəkələr arasında poçt rabitəsini təmin edir. Şlüz adətən şəbəkə əməliyyat sistemi üçün xüsusi MHS-ni X.400 poçt xidməti ilə əlaqələndirir;

Internet: qlobal internetə çıxışı təmin edir;

Node - şəbəkə interfeysi olan kompüter (iş stansiyası, server və ya hər ikisi kimi fəaliyyət göstərir), printer və ya şəbəkə interfeysi olan digər paylaşılan cihaz.

Fiziki şəbəkə topologiyası - qovşaqların və birləşmələrin təşkili: Avtobus(Bus), Üzük (Ring), Ulduz (Star), (Mesh), Ağac (Tree) və s.

Məntiqi topologiya məlumat axınlarını müəyyən edir. Məntiqi avtobusda məlumat eyni seqmentə qoşulmuş bütün qovşaqlar üçün eyni vaxtda mövcuddur. Məntiqi halqada məlumat qovşaqdan düyünə ardıcıl olaraq ötürülür. Düyün bütün paketləri yayımlayır və ona ünvanlananları emal edir. Qovşaqda daxili halqa ilə halqa və ya ulduz fiziki topologiyasında həyata keçirilir. (Букатов А.А., 2019)

FƏSİL III. PROQRAMLA İDARƏ OLUNAN ŞƏBƏKƏLƏRİN KİBERTƏHLÜKƏSİZLİK HƏLLƏRİ

3.1. Proqramla idarə olunan şəbəkələrdə mövcud təhlükələrin və potensial hücumların təhlili.

Ənənəvi şəbəkələrin hələ də istifadəsinə baxmayaraq, Secuirty Define Network (Proqram Təminatı ilə Müəyyən edilmiş Şəbəkələr) və ya Network Function Virtualization (Şəbəkə Funksiyasının Virtuallaşdırılması) kimi

konsepsiyalar onları əvəz etməyə başlayır. Bugünkü xidmət və proqramların bir çoxu, xüsusən də buludla əlaqəli olduqda, SDN olmadan işləyə bilməz. SDN (Software-Defined Networking) məlumatların paylanmış yerlər arasında asanlıqla hərəkət etməsinə imkan verir ki, bu da bulud proqramları üçün vacibdir. SDN-nin təklif etdiyi sürət və çeviklik sayəsində o, uzaq saytlar arasında məlumatların tez və asanlıqla ötürülməsini tələb edən kənar hesablama və Əşyaların İnterneti kimi inkişaf etməkdə olan tendensiyaları və texnologiyaları dəstəkləyə bilir.

Proqram təminatı ilə müəyyən edilmiş şəbəkə məlumat müstəvisini (data layer) və idarəetmə müstəvisini (control layer) ayırmaqla şəbəkə infrastrukturunu əsaslı şəkildə dəyişdi. Bu memarlıq dəyişikliyi maraqlı problemlərə səbəb olan şəbəkələrin yenidən proqramlaşdırılması və mərkəzləşdirilmiş idarə edilməsini təmin etməklə şəbəkə qatını möhkəmləndirdi. Adi şəbəkələrlə müqayisədə Secuirty Define Network (Proqram Təminatı ilə Müəyyən edilmiş Şəbəkələr) təhlükəsiz şəbəkə kimi görünsə də, o, hələ də həssasdır və yerləşdirmə ilə bağlı ciddi problemlərlə üzləşir. Üstəlik, Məlumat müstəvisini (Data layer) və İdarəetmə müstəvisinin (Control layer) ikiyə bölünməsi yeni təhlükəsizlik problemləri açır.

Security Define Network (Proqram Təminatı ilə Müəyyən edilmiş Şəbəkələr) ənənəvi şəbəkələrdə çeviklik və proqramlaşdırma problemlərini aradan qaldırmaq üçün şəbəkəyə müasir proqramlaşdırıla bilən funksiyalar əlavə etmək üçün standartlaşdırılmış və ya ardıcıl tətbiq proqramlaşdırma interfeysi API (Application Programming Interface) təklif edir. Bundan əlavə, Secuirty Define Network (Proqram Təminatı ilə Müəyyən edilmiş Şəbəkələr) şəbəkə xidməti itifadəçilərə daha çevik, idarə oluna bilən və proqramlaşdırıla bilən şəbəkə arxitekturası əldə etməyə kömək edir. SDN-lərin bu xüsusiyyətləri İdarəetmə müstəvisinin (Control layer) gücləndirməyə kömək edir və şəbəkənin funksiyalarını dinamik şəkildə dəyişdirmək üçün şəbəkə topologiyasının qlobal görünüşünü həyata keçirir. Secuirty Define Network (Proqram Təminatı ilə Müəyyən edilmiş Şəbəkələr) daha mərkəzləşdirilmiş şəkildə idarə etsə də, indi həm akademik, həm də sənaye mütəxəssisləri tərəfindən yeni təsdiqini tapmışdır. Bunun səbəbi, təhlükəsizliyin bütün müstəvilərdə, xüsusən də bulud şəbəkələri və peer-to-peer (Peer-to-peer və

ya P2P kimi müəyyən edilir. Peer bərabər deməkdir. Bu, iki və ya daha çox müştəri arasında məlumat mübadiləsi üçün istifadə olunan şəbəkə protokoludur) şəbəkələri kimi yeni dizayn edilmiş şəbəkə sistemlərində böyük narahatlıq doğurmasıdır. Buna görə də, üstünlüklərin sayına baxmayaraq, Secuirty Define Network (Proqram Təminatı ilə Müəyyən edilmiş Şəbəkələr)-lər genişlənmə, etibarlılıq, nəzarətçilərin yerləşdirilməsi və gecikmə də daxil olmaqla bir çox özünəməxsus şəbəkə təhlükəsizliyi problemlərinə malikdir. Bundan əlavə, bir sıra təhlükəsizlik hücumları digər tədqiqatçılar tərəfindən də araşdırılmış. Mənfi tərəfi, Secuirty Define Network (Proqram Təminatı ilə Müəyyən edilmiş Şəbəkələr) müstəvilərinə təhlükəsizlik hücumlarının artması potensialı əsas narahatlıq doğurur. Axın qaydalarının ardıcıllığı, nəzarətçi zəifliyi, qanunilik, zərərli proqramlar, standartlaşdırılmış və şimala və cənuba istiqamətli kommunikasiyalar daxil olmaqla təhlükəsizlik təhdidlərinin artan potensialı Secuirty Define Network (Proqram Təminatı ilə Müəyyən edilmiş Şəbəkələr) funksiyaları, komponentləri və şəbəkələrin açıq proqramlaşdırıla bilməsi ilə bağlı ən yaxşı təcrübələrin olmaması səbəbindən baş verir. Secuirty Define Network (Proqram Təminatı ilə Müəyyən edilmiş Şəbəkələr) -nin çox qatlı arxitekturasına görə müxtəlif müstəvilərə təhlükəsizlik təhdidləri fərqlidir:

Tətbiqi müstəvi (Application layer) idarəetmə müstəvisi kimi də tanınır və SDN arxitekturasında ən üst müstəvisidir. Tərtibatçılar tərəfindən hazırlanmış bütün biznes və təhlükəsizlik proqramları bu müstəvidə icra olunur. Bu müstəvi tərəfindən idarə olunan proqramlar firewall tətbiqi, girişə nəzarət, yük balanslaşdırıcısı, müdaxilənin qarşısının alınması sistemi (Intrusion prevention systems), müdaxilənin aşkarlanması sistemi (Intrusion detection systems) və şəbəkə virtualizasiyasından ibarətdir.

Tətbiqi müstəvisi şimala bağlı APİ (Application Programming Interface) istifadə edərək İdarəetmə müstəvisi (Control Layer) ilə əlaqə qurur. SDN tətəbiqi müstəvisində çoxsaylı şəbəkə xidmətləri yerləşir ki, bu da xakerlərin hədəf mənbəyidir. Bu müstəvidə ən çox yayılmış təhlükəsizlik təhdidləri autentifikasiya, avtorizasiya, girişə nəzarət və hesabatlılıqdır.

Control müstəvisi SDN nəzarətçisindən və ya şəbəkə əməliyyat sistemindən NOS (Network operating system) (Şəbəkə əməliyyat sistemi əsasən iş stansiyalarını, fərdi kompüterləri və bəzi hallarda yerli şəbəkəyə qoşulmuş köhnə terminalları dəstəkləmək üçün nəzərdə tutulmuş kompüter əməliyyat sistemidir) ibarət olan Application müstəvisi ilə Data müstəvisi arasında vasitəçidir. Bu müstəvinin ümumi məsuliyyəti paketlərin yönləndirilməsi və routing ilə bağlı qərarlar qəbul etməklə bütün şəbəkənin funksionallığını idarə etməkdən ibarətdir. İdarəetmə müstəvisi cənuba gedən API-dən istifadə edərək aşağı müstəvisi (Data) ilə əlaqə qurur. Bu müstəvi məntiqi mərkəzləşdirilmiş nəzarətçi sayəsində yalnız qərar qəbul etmək üçün məsuliyyət daşıyır. Buna görə də bütün şəbəkədə zərərli tapşırıqları yerinə yetirmək üçün asanlıqla hədəflənir. Bu müstəvidəki əsas təhlükəsizlik problemləri icazəsiz tətbiqlər, axın qaydasının dəyişdirilməsi, siyasətin tətbiqi və yönləndirmə siyasətinin kəşfidir. Məlumat müstəvisi fiziki açarlar və virtual açarlar kimi yönləndirici cihazların təyin edilmiş siyasətlərinə uyğun olaraq paket yönləndirilməsi üçün cavabdehdir.

İnfrastruktur müstəvisi (məlumat müstəvisi) Ethernet keçidləri və marşrutlaşdırıcılar daxil olmaqla bir neçə fiziki və virtual şəbəkə qurğularından ibarətdir. Data layer kimi tanınır. Məlumatların ötürülməsi bu müstəvinin əsas məsuliyyətidir. Onların istifadə etdiyi interfeys, idarəetmə qatında yerləşən nəzarətçi ilə qarşılıqlı əlaqə yaratmaq üçün Southbound API adlanır. OpenFlow Protokolu ən çox yayılmış Southbound API protokoludur.

Yeni şəbəkə texnologiyaları əvvəllər mövcud olmayan təhlükələri təqdim edə bilər və ya hətta vəziyyəti daha da pisləşdirə bilər. Ənənəvi şəbəkələrdə mövcud hücum vektorları ilə yanaşı, nəzarətçilər və Control müstəvisinə qoşulmalar SDN üçün unikal olan yeni təhlükəsizlik problemləri gətirir. Tək zəiflik çoxlu ziyana səbəb ola bilər, ona görə də təhlükəsizlik SDN-də quraşdırılmış əsas komponent olmalıdır. SDN nəzarətçisi vasitəsilə, xakker şəbəkəyə tam nəzarət edilə bilər.

Xakkerlər yüksək dəyərli hədəfə doğru gedirlər, ona görə də nəzarətçini tək uğursuzluq nöqtəsi kimi tərk etmək o qədər də yaxşı fikir deyil. Control müstəvisini mərkəzləşdirməklə, SDN bütün şəbəkə üzərində mükəmməl nəzarəti təmin edə bilər,

lakin o, həm də idarəçinin iş yükünü artıra bilər, çünki təhlükəsizlik əl ilə yerləşdirilməlidir.

Proqramlaşdırıla bilənlik: Avtomatlaşdırma və çevikliyi artırmaq üçün mərkəzləşdirmə şəbəkələri asanlıqla proqramlaşdırmağa imkan verir. Bu şəbəkənin proqramlaşdırılması SDN-lərin xarakteridir. Bununla belə, əsas əməliyyatlarının proqramlaşdırıla bilən proqram təminatına həvalə edildiyi bir-biri ilə əlaqəli sistem təqdim edildikdə, daima yeni zəifliklər təqdim olunur. SDN istifadəçilərə proqramlı giriş təklif etdikdə daha çox riskə məruz qalır. İstifadəçilərin "güvənməyə" məcbur olduğu və şəbəkənin açarları ilə üçüncü tərəf proqramlarından və ya standart əsaslı həllərdən asılı olduğu halı nəzərdən keçirək. Başqa bir hal, izolyasiya düzgün həyata keçirilmədikdə, nəzarət məlumatı və şəbəkə elementlərinin idarə edilməsindən istifadə oluna bilər.

Şəbəkələrin təkamülü yeni hücum növləri, müəyyən edilmiş və naməlum risklər yaradır. Hələlik faktiki SDN hücumları ilə bağlı heç bir tarixçə yoxdur, ona görə də mövcud zəifliklərı müəyyən etmək və onlardan qorunmaq çətindi. SDN arxitekturasını və onun mümkün hücum vektorlarına aşağıdakıları misal göstərmək olar:

Network Manipulation*:* Control müstəvisində baş verən kritik hücum. Təcavüzkar SDN nəzarətçisini pozur, yalançı şəbəkə məlumatları istehsal edir və bütün şəbəkəyə digər hücumlara başlayır.

Traffic diversion*:* Bu hücum Data müstəvisində şəbəkə elementlərinə baş verir. Təcavüzkar SDN nəzarətçisini pozur, yalançı şəbəkə məlumatları istehsal edir və bütün şəbəkəyə digər hücumlara başlayır.

App manipulation*:* Bu hücum Aplication müstəvisində baş verir. Application zəifliyindən istifadə nasazlığa, xidmətin dayandırılmasına və ya məlumatların dinlənməsinə səbəb ola bilər. Təcavüzkar SDN tətbiqinə yüksək imtiyazla giriş əldə edə və qeyri-qanuni əməliyyatlar həyata keçirə bilər.

API istismarı*:* Proqram komponentinin API-lərində xakkerrə məlumatın icazəsiz açıqlanmasına icazə verə biləcək zəifliklər ola bilər. API istismarı şimala gedən interfeysdə də baş verə bilər və şəbəkə axınlarının məhvinə səbəb ola bilər.

Traffic sniffing*:* Sniffing hücumları xakkerrlər tərəfindən şəbəkə kommunikasiya məlumatlarını ələ keçirmək və təhlil etmək üçün istifadə edilən məşhur üsuldur. Sniffing ilə xakkerr həmçinin şəbəkə elementlərindən və ya keçidlərdən məlumatları dinləyə və vacib məlumatları oğurlaya bilir. Sürətli trafikin olduğu hər yerdə sniffing baş verə bilər. SDN-də xakkerr mərkəzi nəzarətçidən gələn və ona gedən trafikin qarşısını almaq üçün şifrələnməmiş rabitədən istifadə edə bilər. Əldə edilmiş məlumatlara şəbəkədə icazə verilən axınlar və ya trafik haqqında kritik məlumatlar daxil ola bilər.

Parolun təxmin edilməsi və ya kobud güc*:* Bu hücum SDN olmayan elementdə baş verə bilər. Parolun təxmin edilməsi və ya kobud güc tətbiqi ilə icazəsiz istifadəçi SDN-ə giriş əldə edə bilər.

Hardware Trojan Attack*:* Trojan zərərli aparat modifikasiyasıdır ki, bu da təcavüzkarın yoluxmuş IoT cihazından istifadə edərək cihazda işləyən həssas məlumatlara və ya proqram təminatına daxil olmasına imkan verir. Bu mərhələdə təcavüzkar dizayn və ya inkişaf zamanı ilkin sxemləri dəyişir və Trojan-ın zərərli hərəkətlərini aktivləşdirmək üçün tetikleyici mexanizm daxil edir.

Zərərli kod hücumları*:* Zərərli kod hücumları, zərərli proqramlar, qurdlar, casus proqramlar və Trojan atları daxil olmaqla həm əməliyyat sistemini, həm də istifadəçi proqramını hədəfləyə bilər.

Dinləmə hücumu*:* Bu, məxfiliyə edilən ən çox yayılmış hücumdur. Məlumatları gözdən keçirərək, təcavüzkar qarşılıqlı əlaqənin məzmununu asanlıqla kəşf edə bilər. Trafik sensor şəbəkəsi konfiqurasiyası haqqında nəzarət məlumatını ötürəndə, hansı ki, məkan serveri vasitəsilə əldə edilə biləndən daha spesifik məlumatları ehtiva edə bilər, dinləmə məxfiliyin qorunmasının qarşısını effektiv şəkildə ala bilər.

Spoofing Attack*:* Təcavüzkar bir saxtakarlıq hücumunda şəbəkədəki başqa bir nodeun şəxsiyyətini qəbul edir, buna görə də həmin qovşaq üçün nəzərdə tutulmuş mesajları alır. Normalda bu tip hücumlar şəbəkəyə ciddi ziyan vura biləcək əlavə hücumlara başlamaq üçün şəbəkəyə daxil olmaq üçün həyata keçirilirdi.

Denial of Service Attack (DoS)*:* Təcavüzkar bu hücumda şəbəkənin səmərəliliyini ciddi şəkildə aşağı sala biləcək bütün şəbəkə aktivlərini manipulyasiya etməyə çalışır. DoS hücumu da kompüter resurs hücumudur. Bu hücumlar iki qrupa bölünür: fərdi (tək) DoS və DDoS (Paylanılmış DoS) Tək DoS: Təcavüzkar tək bir qurum olaraq göstərilən obyektin resurslarını bir DoS hücumunda tükətməyə çalışır. Paylanmış DoS: Çoxlu təcavüzkarlar DDoS hücumunda tək obyektdən və ya tək bir təcavüzkardan istifadə edir, hədəf maşını çoxlu tələblərlə aşmaq üçün müxtəlif istifadəçilərə güzəştə gedirlər. Bu daim dəyişən təhlükə mənzərəsinə cavab olaraq kibertəhlükəsizlik üzrə ekspertlər və texnoloqlar bir sıra qabaqlayıcı tədbirlər və əks tədbirlər hazırlayıblar. (Abdurahmanov A., 2024).

Man-in-the-middle (MitM) hücumu*:* MitM hücumunun arxasında duran əsas fərziyyə ondan ibarətdir ki, üçüncü tərəf özünün və ya özünün iki son nöqtə arasında, adətən müştəri ilə həmin müştərinin şlüzü arasında şəbəkəyə daxil olmasıdır. Bu o deməkdir ki, İnternet üçün nəzərdə tutulan bütün müştəri trafiki artıq üçüncü tərəf vasitəsilə ötürülməlidir. MITM hücumu, digər hostlarla təmasda olan hədəf hostdan alınan məlumatları manipulyasiya etmək üçün istifadə edilən bir əməliyyatdır. SDN şəbəkəsinin yönləndirmə-nəzarət keçidində baş verir.

Şəbəkə Funksiyalarının Virtuallaşdırılması (Network Functions Virtualization), aparat resursları əvəzinə proqram təminatı tətbiq etməklə şəbəkə funksiyalarını təmin etməklə şəbəkə sistemlərinin faktiki fiziki komponentlərində əsaslı dəyişikliklərin qarşısını almaq üçün vacib texnologiyadır. Virtuallaşdırma mühitində avadanlığı təqlid etmək mümkündür və multi-virtual funksiyalar virtuallaşdırma vasitəsilə mövcud resursları bölüşdürmək və eyni zamanda infrastruktura daxil olmaq qabiliyyətinə malikdir. Son zamanlar NFV əsas aparıcı qüvvələrdən biri kimi yaranaraq kompüter və rabitə şəbəkələrinin müasir inkişafını əhəmiyyətli dərəcədə sürətləndirir. Baxmayaraq ki, NFV bir çox üstünlüklərə malikdir, buraya: resursların istehlakını optimallaşdırmaq, investisiya xərclərinə qənaət etmək, əməliyyat səmərəliliyini artırmaq və şəbəkə xidmətinin həyat dövrünün idarə edilməsini asanlaşdırmaq üçün bir sıra zəifliklər və təhlükəsizlik

təhdidləri təqdim ediləcək, bununla da onların genişlənməsinə və praktikada istifadəsinə mane olacaq.

Filtirləmə texnologiyaları, proqramla idarə olunan şəbəkələrdə zərərli məzmunun, spam mesajların və təhlükəli veb səhifələrin qarşısını alaraq kibertəhlükəsizliyi və şəbəkənin bütövlüyünü təmin edir. (Zəkiyeva N., Məmmədov S., 2024)

Avropa Telekommunikasiya Standartları İnstitutu (ETSI) tərəfindən təqdim edilən nəticəyə əsasən, NFVis dörd əsas komponentdən ibarətdir:

Birinci komponent yerləşdirilmiş Virtual Şəbəkə Funksiyalarında (VNF) virtuallaşdırma mühitini təmin edən bütün proqram və aparat resurslarını göstərən NFV İnfrastrukturudur (NFVI). Məsələn, fiziki hesablama, şəbəkə və yaddaş müxtəlif şəbəkə funksiyaları arasında paylaşılmaq üçün virtuallaşdırıla bilər.

İkinci komponentə Virtual Şəbəkə Funksiyaları (Virtual Network Functions) və Element İdarəetmə Sistemləri (Element Management System) daxildir. VNF-lər virtuallaşdırılmış mühitlərdə işləyən firewall və yük balanslaşdırıcıları kimi proqram əsaslı şəbəkə funksiyalarıdır. EMS-lər VNF-ləri konfiqurasiya edir və idarə edir. Üçüncü komponent NFV İdarəetmə və Orkestrasiyanı (MANO - Management and Orchestration) göstərir. Bu komponent hesablama, şəbəkə və saxlama daxil olmaqla NFV mühitində bütün resursları idarə etmək və təşkil etmək üzərində işləyir. Son komponent Əməliyyat Dəstəyi Sistemi/Biznes Dəstək Sistemini (Operating Support System/Business Support System) göstərir. Bunlar faturalandırma prosesi kimi müxtəlif biznes məqsədlərinə cavab vermək üçün VNF xidmət təminatçıları vasitəsilə həyata keçirilir. NFV İnfrastrukturunda baş verə biləcək hücumlar:

1. Əməliyyat müdaxiləsi: İnfrastrukturun razılaşdırılmış əlçatanlığı sayəsində, təhlükəsi olan provayder və ya VNF-nin zərərli istifadəçisi şəbəkə trafikini dəyişdirməklə və ya zərərli proqram daxil etməklə infrastruktur əməliyyatlarına müdaxilə edə bilər;

2. Zərərli provayderlərlə əməkdaşlıq şansı: Şəbəkə infrastrukturu resurslarına çıxış vasitəsilə VNF provayderləri şəbəkənin əməliyyatlarında iştirak edə bilirlər;
3. Paylaşılan resurslardan sui-istifadə: İnfrastrukturun paylaşılan resurslarından elə sui-istifadə. Paylaşılan qaynaqlar, bu təhdidlərin prinsipidir. Bu hücumların həlli yollarını tapmaq üçün istifadəçilər üçün xüsusi instansiyalar yaradıla və İP ünvanlarının qara siyahısı ilə bağlı zərərli tələblər yoxlana bilər.

3.2. Proqramla idarə olunan şəbəkələrdə mümkün təhlükə və hücumlara qarşı effektiv müdafiə strategiyalarının tətbiqi.

Bəzi təşkilatlar üçün daha çox işçi işə götürmək mümkün ola bilər, lakin bunun xərclərə təsiri var və nəzərə alınmalı olan mövcud və ixtisaslı bacarıqların olmaması var. Avtomatlaşdırma bir seçimdir. Beləliklə, SIEM, EDR, XDR və SOAR-ın yüksəlişi. Onların hər birinə ayrıca nzərə salaq:

SIEM (Security Information and Event Management) uzun müddətdir mövcuddur. SIEM bir çox mənbədən məlumatları qəbul edir, hadisələri əlaqələndirməyə kömək edir və insan operatorunun nəticəni təhlil etməsi və növbəti qərarı qəbul etməsi üçün hesabatları avtomatlaşdırır.

EDR (Endpoint Detection and Response) bu gün XDR və SOAR-da gördüyünüz avtomatlaşdırılmış "cavab" dövrünün ilk təkrarlamalarından biridir. Son nöqtələr təhdidlər üçün izlənilir, təhdidlər uyğunlaşdırılır və təhlükə avtomatik olaraq cavablandırılır, bu da problemlərin aradan qaldırılması addımlarını əhatə edə bilər.

XDR (Extended Detection and Response), vəziyyəti aşkar etmək, cavab vermək və düzəltmək üçün yalnız son nöqtələrdən daha çox məlumat mənbəyinin izlənildiyi və istifadə edildiyi bir uzantı və ya "extended" aşkarlama və cavab mexanizmi olaraq görürük. Bu məlumat mənbələrinə SİEM, yeni nəsil təhlükəsizlik divarları, son nöqtələr və daha çox şey daxil ola bilər.

SOAR (Security Orchestration, Automation and Response) XDR funksionallığının çoxuna malikdir, lakin təhlükəsizlik qruplarına yükü azaltmaq

üçün həllə zəifliyin idarə edilməsi və oyun kitabları kimi digər təhlükəsizlik idarəetmə proseslərinin avtomatlaşdırılmasını əlavə edir.

Bu həlləri araşdırarkən bir çox ziddiyyətli təriflər var. Bir çox təchizatçı bu həlləri (xidmət olaraq proqram təminatı) və ya SaaS adlandırmağı xoşlayır və bu, bir çox hallarda doğru ola bilər, lakin müqayisəli yerli həllər quraşdırmaq və ya xidməti idarə olunan xidmət təminatçısından əldə etmək mümkündür. Təşkilatınızın tələblərindən asılı olaraq nəzərə alınmalı olan müsbət və mənfi cəhətlər var.

Təşkilatlar hansı yanaşmanın seçiləcəyini diqqətlə araşdırmalıdırlar. Aşağıdakıları nəzərə almağa dəyər:

Hər bir həll üçün əhəmiyyətli bir xərc olacaq, buna görə də uzun müddət ərzində yerli, SaaS və ya idarə olunan xidmət arasındakı fərqləri diqqətlə araşdırın.

Bunlar “configure and leave” həlləri deyil. Bu həlləri idarə etmək üçün davamlı təkmilləşdirmə tələb olunur.

Bu həlləri idarə etmək, onları işə götürməkdən və ya onlarla müqavilə bağlamaqdan asılı olmayaraq hələ də ixtisaslı mütəxəssislər tələb edir.

Biznes nöqteyi-nəzərindən həllər nasazlıqlar və ya fasilələr olmadan hücumların və ya hacklərin qarşısını almalıdır.

Məqsəd kritik tətbiqlərin, aktivlərin, Şəxsi məlumatların (PII) və təşkilatın nüfuzunun qorunmasını və saxlanmasını təmin etməkdir.

Extended Detection and Response (XDR) təşkilatın bütün İT mühitində təhlükəsizliyin vahid görünüşünü təmin edən yeni nəsil kibertəhlükəsizlik həlləridir. XDR həlləri həm EDR-in imkanlarını ehtiva edir, həm də əhatə dairəsini təşkilatın digər sahələrinə genişləndirir:

Son nöqtələr: Noutbuklar, masaüstü kompüterlər və serverlər kimi cihazları şübhəli fəaliyyətə görə izləyir və qoruyur.

Şəbəkə: Zərərli fəaliyyət əlamətləri üçün şəbəkə trafikini izləyir və təhlil edir.

Bulud: Bulud infrastrukturunu və təhdidlər üçün tətbiqləri izləyir və təhlil edir.

E-poçt: Fişinq və zərərli proqramlar üçün e-poçt trafikinə nəzarət edir və təhlil edir.

XDR son nöqtələr, şəbəkələr və proqramlar daxil olmaqla bir çox təhlükəsizlik təbəqələri üzrə məlumatları birləşdirir. Müxtəlif təbəqələrin bir-birinə bağlı olduğu SDN-də XDR hərtərəfli təhlükənin aşkarlanması və cavab vermə imkanlarını təmin edə bilər. XDR SDN infrastrukturu üzrə təhlükəsizlik hadisələrini əlaqələndirə bilər, potensial təhdidlərin vahid görünüşünü təmin edir və insidentlərə daha effektiv cavab verməyə imkan verir.

SOAR təşkilatlara insidentlərə cavab proseslərini avtomatlaşdırmağa və sadələşdirməyə kömək edən kibertəhlükəsizlik həllinin bir növüdür. SOAR həlləri iş axınının avtomatlaşdırılması (Hadisəyə cavab verən qruplara triaj, təhlil və məhdudlaşdırma kimi insidentlərə cavab iş axınlarını müəyyən etməyə və avtomatlaşdırmağa imkan verir), təhdid kəşfiyyatının inteqrasiyası (İnsident reaksiyasını təkmilləşdirmək üçün təhdid kəşfiyyatı məlumatlarına daxil olmaq və istifadə etmək üçün insidentlərə cavab verən qruplara imkan verir), işin idarə edilməsixüsusiyyətləri (İnsidentə cavab hallarını idarə etmək və izləmək üçün mərkəzləşdirilmiş platforma ilə insidentlərə cavab verən qrupları təmin edir), hesabat və analitika ehtiva edir (Hadisəyə cavab verən qruplara insidentin həcmi və cavab müddəti kimi insidentlə bağlı cavab məlumatlarını izləməyə və təhlil etməyə imkan verir).

SOAR platformaları Software Defined Networking (proqram təminatı ilə müəyyən edilmiş şəbəkə)-nin dinamik mühitində çox vacib olan təhlükəsizlik proseslərini avtomatlaşdırır və sadələşdirir. SOAR SDN nəzarətçi ilə inteqrasiya oluna bilər ki, təhlükələrə məruz qalan son nöqtələri təcrid etmək və ya təhlükələri azaltmaq üçün şəbəkə siyasətlərini tənzimləmək kimi insidentlərə cavab tədbirləri avtomatlaşdırıla bilər. Təhlükəsizlik iş axınlarını təşkil etməklə və təkrarlanan tapşırıqları avtomatlaşdırmaqla SOAR SDN-nin ümumi təhlükəsizlik vəziyyətini artırır.

Ümumilikdə, EDR, XDR, SOAR və DID metodunun SDN təhlükəsizlik strategiyalarına inteqrasiyası təhdidlərin aşkarlanması, insidentlərə reaksiya və giriş nəzarətini təkmilləşdirərək şəbəkəni inkişaf edən kibertəhlükələrə qarşı daha davamlı edir.

3.3. Proqramla idarə olunan şəbəkələrdə monitorinq sistemlərinin tətbiqi.

Ənənəvi şəbəkə infrastrukturunda SIEM çoxsaylı şəbəkə təhlükəsizlik cihazlarının və digər aktiv şəbəkə elementlərinin konfiqurasiyasında ziddiyyətlər nəticəsində yarana biləcək mürəkkəb problemlər səbəbindən təhlükəsizlik təhdidlərinə effektiv şəkildə avtomatlaşdırılmış reaksiya verə bilmir. SDN (Software Defined Networks) texnologiyasının yüksəlişi bu problemin həllində yeni imkanlar açıb.

SIEM (Təhlükəsizlik Məlumatı və Hadisələrin İdarə Edilməsi) real vaxt rejimində bir çox mənbədən daxil olan məlumatları birləşdirən, təhlil edən və əlaqələndirən təhlükəsizlik idarəetmə sistemidir. SIEM sistemləri şəbəkə cihazları, serverlər, proqramlar və son nöqtələr kimi müxtəlif mənbələrdən log məlumatlarını toplayır və təhlil edir. SİEM məlumat qəbulu, məlumatların təhlili, məlumatların normallaşdırılması, korrelyasiya və təhlil, qaydaya əsaslanan xəbərdarlıq, insident cavabı, məlumatların saxlanması, hesabat, davamlı monitorinq sistemindən istifadə edərək məlumatı emal edir.

Təhlükəsizlik Məlumatı və Hadisə İdarəetmə (SIEM) inteqrasiyaları hər hansı bir təşkilatın təhlükəsizlik arsenalının vacib hissəsidir. SIEM-i digər sistemlərə qoşmaqla, təşkilatlar bütün mövcud giriş məlumatlarının potensial təhdidlər üçün izlənilməsini təmin edə və pozuntu baş verdikdə daha səmərəli cavab verə bilər. SIEM inteqrasiyaları həmçinin təşkilatlara zərərli fəaliyyəti tez aşkarlamağa kömək edir və zərər dəyməzdən əvvəl tədbir görməyə imkan verir. SIEM-in təşkilatınız boyu nəzarətdə saxlamağa kömək edə biləcəyi bəzi təhlükələr zərərli proqram, fidyə proqramı, fişinq, DoS (Xidmətdən imtina) və sairdir. Rəqəmsal əsr inkişaf etdikcə, daha çox kiberhücumlar təhlükə aktorları tərəfindən təqdim edilir.

Bugünkü müasir dünyada hərtərəfli təhlükəsizlik sisteminə malik olmaq bütün ölçülü müəssisələr üçün vacibdir. Düzgün təhlükəsizlik sistemi ilə təşkilatlar öz aktivlərini və məlumatlarını xakkerrlik və ya oğurluq kimi zərərli fəaliyyətlərdən qoruya bilər. Üstəlik, SIEM inteqrasiyaları kimi ən son texnologiyanı inteqrasiya etməklə, müəssisələr təhlükəsizlik sistemlərinin effektivliyini artıra və əməliyyatlarını rəvan davam etdirə bilərlər. SIEM inteqrasiyası ilə təhlükəsizlik sistemlərinin niyə bu qədər vacib olduğuna daha yaxından nəzər salaq. SIEM-in

təşkilatınız boyu nəzarətdə saxlamağa kömək edə biləcəyi bəzi təhdidlər zərərli proqram, fidyə proqramı, fişinq, DoS (Xidmətdən imtina) və sairdir. Rəqəmsal əsr inkişaf etdikcə, daha çox kiberhücumlar təhlükə aktorları tərəfindən təqdim edilir. Bugünkü müasir dünyada hərtərəfli təhlükəsizlik sisteminə malik olmaq bütün ölçülü müəssisələr üçün vacibdir. Düzgün təhlükəsizlik sistemi ilə təşkilatlar öz aktivlərini və məlumatlarını xakkerrlik və ya oğurluq kimi zərərli fəaliyyətlərdən qoruya bilər. Üstəlik, SIEM inteqrasiyaları kimi ən son texnologiyanı inteqrasiya etməklə, müəssisələr təhlükəsizlik sistemlərinin effektivliyini artıra və əməliyyatlarını rəvan davam etdirə bilərlər. SIEM inteqrasiyası ilə təhlükəsizlik sistemlərinin niyə bu qədər vacib olduğuna daha yaxından nəzər salaq.

SIEM inteqrasiyaları müəssisələrə öz məlumatları üçün əlavə qorunma səviyyəsi təqdim edir. Real vaxt rejimində müxtəlif proqramlar arasında məlumat paylaşmaq üçün sistemləri birləşdirərək, xakkerrlər və ya cinayətkarlar kimi icazəsiz qurumların həssas məlumatlara daxil olması və ya manipulyasiyası xeyli çətinləşir. Bundan əlavə, süni intellekt (AI) və maşın öyrənməsi (ML) kimi ən son texnologiyalardan istifadə etməklə, təşkilatlar təhlükəsizlik sistemlərini daha da gücləndirə və hər zaman ən son təhlükələrdən xəbərdar olmalarını təmin edə bilərlər.

Qabaqcıl Aşkarlama İmkanları SIEM inteqrasiyaları ilə hərtərəfli təhlükəsizlik sisteminin tətbiqinin digər faydası onun təmin etdiyi qabaqcıl aşkarlama imkanlarıdır. Mövcud sistemləri bir platformada birləşdirərək, biznes potensial təhlükələri problemə çevrilməzdən əvvəl aşkar etmək üçün güclü analitik vasitələrdən istifadə edə bilər. Məsələn, bir sistemdə və ya proqramda şübhəli fəaliyyət varsa, təhlükəsizlik əməliyyat mərkəzindəki (SOC) cavabdehlər dərhal xəbərdar oluna bilər ki, hər hansı bir zərərin qarşısını almaq üçün lazımi addımlar atılsın. Bu, zərərli hücumlar və ya digər gözlənilməz hallar səbəbindən dayanma müddəti və ya məlumat itkisi riskini xeyli azaldır. Nəticə olaraq, SIEM inteqrasiyası ilə hərtərəfli təhlükəsizlik sisteminə sərmayə qoymaq təşkilatlar üçün öz məlumatlarını qorumaq və eyni zamanda zamanla digər faydaları həyata keçirmək üçün əla yoldur. Bu həllər potensial təhlükələrə qarşı əlavə qorunma qatını təmin etməklə yanaşı, şübhəli fəaliyyəti problemə çevrilməzdən əvvəl aşkarlamağı asanlaşdırır. İndi hərtərəfli təhlükəsizlik sisteminə investisiya qoymaq

biznesinizin gələcək illər üçün təhlükəsiz və təhlükəsiz qalmasını təmin etməyə kömək edəcək.

SIEM İnteqrasiyaları nə edə bilər? SIEM kibertəhlükələri aşkar etmək və sistemlərin əməliyyat sağlamlığını qorumaq üçün ətraf mühitdə görünməni təmin etmək üçün istifadə edilən proqram həllidir. O, ətrafınızda zərərli fəaliyyət göstərə biləcək anomaliyaları aşkar etmək üçün log idarəetmə imkanlarından və üsullarından istifadə edir.

Log Management Login idarə edilməsi potensial təhlükəsizlik risklərini və ya insidentlərini müəyyən etmək üçün sistem daxilində müxtəlif mənbələrdən jurnala əsaslanan məlumatların toplanması prosesidir. Bu, SIEM-in əsas qabiliyyətidir və sisteminizdə baş verənləri real vaxt rejimində izləməyə imkan verir ki, problem yaranarsa tez tədbir görə biləsiniz.

Şəbəkə Monitorinqi və təhlili SIEM inteqrasiyasının əsas tərkib hissəsidir və sisteminizdə şəbəkə fəaliyyətini izləməyə imkan verir. Beləliklə, siz real vaxt rejimində şəbəkə trafikinizin fəaliyyətini görə bilərsiniz.

Son nöqtənin aşkarlanması Bu xüsusiyyət sizə bütün son nöqtələrinizdə fəaliyyətinizə baxmaq imkanı verir; bu məlumatların SIEM inteqrasiyası vasitəsilə gətirilməsi ətrafınıza daha yaxşı baxış imkanı verir. Son nöqtələrinizə nəzarət edə bildiyiniz üçün təhlükəni aşkar etmək və buna uyğun cavab vermək üçün lazım olan vaxtı azalda bilərsiniz.

Hadisə korrelyasiyası Hadisə korrelyasiyası sonrakı təhlil üçün müxtəlif mənbələrdən gələn hadisələri bir-biri ilə əlaqələndirməklə bir çox sistem və ya şəbəkələrdə şübhəli fəaliyyəti aşkar etmək üçün istifadə edilən xüsusiyyətdir. Bu, bir çox SIEM üçün mərkəzi xüsusiyyətdir, ona görə də ətrafınızdakı digər cihazlarla nə qədər çox SIEM inteqrasiya nöqtəsi olarsa, bir o qədər yaxşıdır. Korrelyasiya zərərli niyyəti göstərə bilən hadisələr arasında gizli əlaqələri və ya əks halda aşkarlanmayan digər təhlükəsizlik problemlərini aşkar etməyə kömək edir.

Hücumun aşkarlanması və qarşısının alınması Hücumun aşkarlanması və qarşısının alınması sistemləri (IDS və IPS) şəbəkə daxilində icazəsiz giriş cəhdlərini

aşkar etmək və ya xəbərdar etmək, ya da onların uğurlu olmasının qarşısını almaq üçün nəzərdə tutulmuşdur.

SIEM inteqrasiyaları logların idarə edilməsi, şəbəkə monitorinqi və təhlili, hadisələrin korrelyasiyası və müdaxilənin aşkarlanması və qarşısının alınması həlləri ilə əlaqələrdən istifadə etməklə şəbəkələri potensial kibertəhlükələrdən qorumaq üçün vacibdir. Hər bir inteqrasiya növünün birlikdə necə işlədiyini başa düşməklə, təhlükəsizlik mütəxəssisləri, İT administratorları və texnoloji startaplar öz sistemlərini icazəsiz giriş əldə etmək və ya başqa vasitələrlə zərər vurmaq istəyən zərərli aktorlardan daha yaxşı qoruya biləcəklər.

SIEM İnteqrasiyalarının üstünlükləri İstənilən biznesin rəqəmsal əsrdə uğur qazanması üçün onun möhkəm təhlükəsizlik infrastrukturu olmalıdır. Buna nail olmaq üçün ən vacib vasitələrdən biri SIEM-dir. Təhlükəsizlik arsenalınızdakı digər alətlərlə SIEM inteqrasiyası təşkilatların ümumi təhlükəsizlik vəziyyətinə daha çox görünməsini, eləcə də insidentlərə cavab vaxtlarının təkmilləşdirilməsini təmin etmək üçün nəzərdə tutulub.

Təkmilləşdirilmiş Hadisələrə Cavab Vaxtı SIEM inteqrasiyasının əsas üstünlüklərindən biri insidentlərə cavab müddətini artırmaqdır. Potensial təhdidləri tez aşkarlaya və onlara cavab verə bilən inteqrasiya edilmiş platformaya malik olmaqla, təşkilatlar insidentləri aşkar etmək və onlara reaksiya vermək və onların vurduğu zərəri minimuma endirmək üçün lazım olan vaxtı kəskin şəkildə azalda bilər.

Təhlükəsizlik Hadisələrinə Artan Görünmə SIEM inteqrasiyasının başqa bir üstünlüyü təhlükəsizlik hadisələrinə artan görünürlükdür. Sistemlərdən, proqramlardan, verilənlər bazalarından və digər mənbələrdən log faylları kimi çoxsaylı məlumat mənbələrini inteqrasiya etməklə, təşkilatlar potensial təhlükələri daha tez və dəqiq müəyyən etməyə kömək edən ətraf mühitin hərtərəfli görüntüsünü əldə edirlər. Bu səviyyəli görünürlük həm də təşkilatlara təhlükəsizlik insidentlərini onların şiddətinə görə prioritetləşdirməyə imkan verir ki, onlar ilk növbədə ən təcili olanları həll etsinlər.

Qısaca desək, SIEM inteqrasiyaları müəssisələrə insidentlərə cavab müddətini yaxşılaşdırır, təhlükəsizlik hadisələrinin daha çox görünməsini və müxtəlif təhlükəsizlik proseslərinin və məsuliyyətlərinin avtomatlaşdırılmasını təmin edir ki, bu da son nəticədə təşkilatınız üçün daha təhlükəsiz mühitə gətirib çıxarır. Əgər siz təşkilatınızın kibertəhlükəsizlik mövqeyini gücləndirməyin yollarını axtarırsınızsa, inteqrasiya olunmuş SIEM həllinə sərmayə qoymağı düşünün. Bu, sadəcə sizə lazım olan şey ola bilər.

Nəticə

Yekun olaraq qeyd etmək olar ki, proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizliyi müasir informasiya texnologiyaları dünyasında son dərəcə vacibdir. Tədqiqatın təhlili göstərdi ki, bu cür şəbəkələrin müxtəlif təhdidlərdən, o cümlədən kiberhücumlardan, zərərli proqramlardan və digər növ təhlükələrdən qorunması üsullarının daim işlənib hazırlanmasına və təkmilləşdirilməsinə ehtiyac var. Ümumiyyətlə, bu dissertasiya işinin nəticələri proqram təminatı ilə idarə olunan şəbəkələrin praktiki mühafizəsinin təkmilləşdirilməsi və şəbəkə texnologiyaları sahəsində təhlükəsizlik müstəvisinin yüksəldilməsi üçün istifadə oluna bilər.

Artıq qeyd edildiyi kimi, proqram təminatı ilə idarə olunan şəbəkələrdə təhlükəsizlik məsələsi aktual olaraq qalır və əlavə tədqiqat və inkişaf tələb edir. Proqram təminatı ilə idarə olunan şəbəkələrin əsas problemləri və zəiflikləri

müəyyən edilmiş, onlardan bəzilərini aşağıdakı təkliflərlə aradan qaldırmaq və ya azaltmaq olar:

- Monitoriq sistemlərinin (SİEM) Şəbəkə funksiyalarının virtuallaşdırılması (NFV) inteqrasiyası;
- Suni intellekt və maşın öyrənilməsi metodları ilə dəstəklənmiş Avtomatlaşdırırlmış monitorinq (Soar) sistemlərinin şəbəkə funksiyalarının virtuallaşdıırlmasında tətbiqi;
- Süni intellektin tətbiqi ilə virtullaşdırılmış şəbəkə funksiyalarında yaranan problemlərin həlli;
- Proqram təminatı ilə idarə olunan şəbəkələr üçün təhlükəsizlik modellərinin hazırlanması;
- Proqram təminatı ilə idarə olunan şəbəkələrdə təhlükəsizlik üsullarının müqayisəli təhlili;
- Proqram təminatı ilə idarə olunan şəbəkələrə hücumların təsirinin və onların qarşısının alınması üsullarının öyrənilməsi;
- Proqram təminatı ilə idarə olunan şəbəkələri daxili və xarici təhlükələrdən qorumaq üçün strategiyalar hazırlanması;
- Proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizlik müstəvisinin qiymətləndirilməsi və mühafizənin yaxşılaşdırılması üçün tədbirlərin təklif edilməsi;
- Proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizliyində mövcud tendensiyalar və onların təcrübəyə təsirinin öyrənilməsi.

İstifadə edilmiş ədəbiyyat

Abuarqoub A., Behaviour Profiling in Healthcare Applications Using the Internet of Things Technology / A. Abuarqoub, MH. Hammoudeh // Proceedings of Fourth International Conference on Advances in Information Processing and Communication Technology, 2016.

Benzekki K., Software-defined networking (SDN): a survey / K. Benzekki, A. El Fergougui, A. Elbelrhiti Elalaoui // Security and Communication Networks. - 2016. - Vol. 9(18). - pp.5803-5833.

Berde P., ONOS: Towards an open, distributed SDN OS / P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, W. Snow, and G. Parulkar, // SIGCOMM HotSDN. New York, NY, USA: ACM, 2014, pp. 1-6.

Blial O., An Overview on SDN Architectures with Multiple Controllers / O. Blial, M. Ben Mamoun, R. Benaini // Journal of Computer Networks and Communications. - 2016. - Vol.2016.

Blokdyk G. Network Functions Virtualization NFV Complete Self-Assessment Guide. CreateSpace Independent Publishing Platform, 2017, 122 p.

Bugnion E., Nieh J., Tsafrir D. Hardware and Software Support for Virtualization (Synthesis Lectures on Computer Architecture). Morgan & Claypool Publishers, 2017, 208 p.

Edelman J., Lowe S. S., Oswalt M. Network Programmability and Automation: Skills for the Next-Generation Network Engineer. O'Reilly Media, 2018, 584 p.

Fei Hu. Network Innovation through OpenFlow and SDN. Principles and Design. CRC Press. 1st edition. February 2014. – 520 p.

Fu Y., A hybrid hierarchical control plane for flow-based large-scale software-defined networks / Fu Y, J. Bi, Z. Chen, K. Gao, B. Zhang, G. Chen, and J. Wu // IEEE Trans. Netw. Service Manag., vol. 12, no. 2, pp. 117-131, June 2015.

Jararweh Y., SDIoT: A Software Defined Based Internet of Things Framework / Jararweh Y., Al-Ayyoub M., Darabseh A., Benkhelifa E., Vouk M., Rindos A // Journal of Ambient Intelligence and Humanized Computing, pp. 453-461. 2015.

Karakus M. A survey: Control plane scalability issues and approaches in Software-Defined Networking (SDN) / M. Karakus, A. Durresi // Computer Networks. - 2017. - Vol. 112. - C. 279-293.

Kirichek R., Model Networks for Internet of Things and SDN / Kirichek R., Vladyko A. Zakharov M., Koucheryavy A. // ICACT, pp. 76-79. IEEE 2016.

Leconte M., A Resource Allocation Framework for Network Slicing / M. Leconte, G. Paschos, P. Mertikopoulos, U. Kozat // IEEE International Conference on Computer Communications (INFOCOM 2018), Apr. 2018.

Muhizi S., Analysis and performance evaluation of SDN queue model / Muhizi S., Shamshin G., Muthanna A. S., Kirichek R. V., Vladyko A. G, Koucheryavy A. E. // WWIC 2017. Lecture Notes in Computer Science, vol 10372. pp 37-48. Springer, Cham.

Ross K. W., Kurose J. F. Computer Networking: A Top-Down Approach, 6Th Edn. Pearson India, 2017, 888 p.

Salman O., SDN controllers: A comparative study / O. Salman, I. H. Elhajj, A. Kayssi, A. Chehab // MELECON 2016. pp. 1 - 6. 2016.

Sandhya, A survey: Hybrid SDN / Sandhya, Yash Sinha, K. Haribabu // Journal of Network and Computer Applications Volume 100, 15 December 2017, pp. 35-55.

Siamak Azodolmolky. Software Defined Networking with OpenFlow. Packt Publishing. October 25, 2013. – 152 p.

S. Ghorbani, C. Schlesinger, M. Monaco “Transparent, live migration of a software-defined network” in Proceedings of the ACM Symposium, ACM, Seattle, November 2014.

X. Pan, W. Sun. Address Resolution Delay Metric in Software-Defined Networking (SDN). April 22, 2015

Бородин А.С., Сети связи пятого поколения как основа цифровой экономики / А.С. Бородин, А.Е. Кучерявый // Электросвязь. - 2017. - No 5. - С. 45-49.

Букатов А.А., Гуда С.А. Компьютерные сети. Расширенный начальный курс. - СПб.: Питер. - 2019. - С. 496.

В. А. Лихачев. Программно-конфигурируемые сети на основе протокола OpenFlow. Вестник ВГУ, серия: Системный Анализ и информационные технологии, 2014, №1.

Владыко А.Г, Матвиенко Н.А, Новиков М.И., Киричек Р.В. Тестирование контроллеров программно-конфигурируемой сети на базе модельной сети // Информационные технологии и телекоммуникации. 2016. Том 4. №1. С. 17-28.

Владыко, А.Г.Тестирование SDN контроллеров на базе модельной сети / А.Г. Владыко, Н.А. Матвиенко, М.И. Новиков, Р.В. Киричек // Информационные технологии и телекоммуникации. - 2016. - Т. 4. - No 1. - С. 17-28.

Кадилов А.В., Оценка надежности программно-конфигурируемых сетей с использованием виртуального моделирования // Universum: технические науки. 2022. № 1 (94) С. 73-77.

Лапонина О.Р., Сухомлин В. А. Способы трансформации сетей к SDN-архитектуре // International Journal of Open Information Technologies. 2015. №4.

Лихачев В.А. Программно-конфигурируемые сети на основе протокола OpenFLOW // Приволжский научный вестник. 2014. № 3-1 (31).

Логинов С.С. Об уровнях управления в программноконфигурируемой сети (SDN)/ T-Comm: Телекоммуникации и транспорт. 2017. Том 11. №3. С. 50-55.

Мухизи С., Анализ возможностей применения SDN/NFV в мобильных сетях 5G / Мухизи С., Киричёк Р.В. // Молодежная научная школа по прикладной теории вероятностей и телекоммуникационным технологиям (ÄPTCT). 2017. С. 166174.

Мухизи с., Исследование моделей балансировки нагрузки в программно-конфигурируемых сетях / Мухизи с., Мутханна А.С.; Киричёк Р.В, Кучерявый А.Е. // Электросвязь. 2019, No 01. С. 23-29

Олифер Н. А., Олифер В. Г. Принципы, технологии, протоколы. Учебник.- СПб: Питер. - 2017. - С. 992.

Панеш А. Х. Достоинства и недостатки программно-конфигурируемых компьютерных сетей // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2016. №3 (186).

Панеш А. Х. Содержание и перспективы технологий программно-конфигурируемых сетей и виртуализации сетевых функций // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2014. №2 (137).

Перепелкин Д.А., Цыганов И.Ю. Концепция и задачи сетевого слайсинга в программно-конфигурируемых сетях // Вестник Рязанского государственного радиотехнического университета. - 2020. - № 72. - С. 13-24.

Перепелкин Д. А. Концептуальный подход динамического формирования трафика программно-конфигурируемых телекоммуникационных сетей с балансировкой нагрузки // Информационные технологии. 2015. Т. 21. № 8. С. 602-610.

Смелянский Р.Л. Настоящее и будущее SDN&NFV // Первая миля, издательство АО "Рекламно-издательский центр «Техносфера» (Москва).- 2016. - № 3. - С. 78-85.

Смелянский Р.Л., Васин В.В., Беззубцев С.О. Разработка отечественного коммутатора для программно-конфинурируемых сетей // Электронная техника. Серия 3: Микроэлектроника, издательство Акционерное общество

"Научно-исследовательский институт молекулярной электроники" (Москва). - 2016. - Т 1. - № 161. - С. 9-17.

Ушаков Ю.А., Коннов А.Л., Полежаев П.Н. Моделирование корпоративной сети, построенной на основе принципов программно-конфигурируемой инфраструктуры и виртуализации сетевых функций // Интеллект. Инновации. Инвестиции. - 2017. - № 12. - С. 90-96.

Ю. Ю. Коляденко, Е. Э. Белоусова. Программно-конфигурируемые сети на базе протокола OpenFlow и их характеристики. Scientific Journal «ScienceRise» №3/2(20)2016 г.

Abdurahmanov A., DDOS hücumlarından müdafiə vasitələri. Academics and Science Reviews Materials, 2024, pp. 79-81.

Cəlilov A., Active Directory. Academics and Science Reviews Materials, 2024, pp. 75-78.

Zəkiyeva N., Məmmədov S., Filterləmə texnologiyaları. Scientific Research and Experimental Development, 2024, pp. 259-264.

Zəkiyeva N., Məmmədov S., Təhlükəsiz şəbəkə əlaqəsinin qurulmasi : virtual şəxsi şəbəkələrin istifadəsi (vpn). Scientific Research and Experimental Development, 2024, pp. 265-268.

Xülasə

Müasir dünyada proqram təminatı ilə idarə olunan şəbəkələr təşkilat və müəssisələrin ayrılmaz hissəsinə çevrilib. Bununla belə, onların istifadəsi artdıqca, şirkətin sistemi və məlumatları üçün ciddi nəticələrə səbəb ola biləcək yeni təhlükələr və zəifliklər yaranır. Bu dissertasiya işinin məqsədi proqram təminatı ilə idarə olunan şəbəkələrin təhlükəsizliyinin təmin edilməsi üsul və vasitələrini öyrənməkdir. İş mövcud təhlükə və riskləri təhlil edir və onları minimuma endirmək üçün həll yolları təklif edir. Hücumların aşkarlanması və qarşısının alınması üçün alətlər, həmçinin məlumat sızması və icazəsiz girişdən qorunma mexanizmləri də öyrənilir. Bu tədqiqatda aparılan nəzəri və praktiki tədqiqatlar əsasında da nəticələr əldə edilmişdir. Bu nəticələr əsasında elmi və praktiki təkliflər irəli sürülüb.

Резюме

В современном мире программно-управляемые сети стали неотъемлемой частью организаций и предприятий. Однако, с увеличением их использования, возникают новые угрозы и уязвимости, которые могут привести к серьезным последствиям для системы и данных компании. Целью данной диссертации является исследование методов и средств обеспечения безопасности программно-управляемых сетей. В работе проводится анализ существующих угроз и рисков, и предложены решения для их минимизации. Также изучаются средства обнаружения и предотвращения атак, а также механизмы защиты от утечек данных и несанкционированного доступа. Также были получены результаты на основе теоретических и практических исследований, проведенных в настоящем исследовании. На основе этих результатов были выдвинуты научно-практические предложения.

Summary

In the modern world, software-controlled networks have become an integral part of organizations and enterprises. However, as their use increases, new threats and vulnerabilities arise that can lead to serious consequences for a company's system and data. The purpose of this dissertation is to study methods and means of ensuring the security of software-controlled networks. The work analyzes existing threats and risks, and proposes solutions to minimize them. Tools for detecting and preventing attacks, as well as mechanisms for protecting against data leaks and unauthorized access are also being studied. Results were also obtained on the basis of theoretical and practical studies conducted in this study. Based on these results, scientific and practical proposals were put forward.