VLAN TEXNOLOGIYASI VA UNING TARMOQ XAVFSIZLIGIDAGI ROLI
VLAN TECHNOLOGY AND ITS ROLE IN NETWORK SECURITY

Ibragimov Sh.M.[1], Raxmonova U.B[2]
[1]FarDU dotsenti, shavkat19702008@gmail.com
[2]FarDU talabasi, raxmonovaumidaxon380@gmail.com

Annotatsiya: Zamonaviy korporativ tarmoqlarda turli xavfsizlik talablariga ega foydalanuvchilar va xizmatlarni bitta fizik infratuzilma doirasida mantiqiy ajratish dolzarb muammoga aylangan. Ushbu maqolada Virtual Local Area Network (VLAN) texnologiyasining nazariy asoslari, IEEE 802.1Q standarti asosidagi kadrlarni teglashtirish mexanizmi hamda uning tarmoq xavfsizligidagi ahamiyati IMRAD tuzilmasi asosida tadqiq etilgan. Tadqiqotda IEEE 802.1Q-2018 standarti, Cisco va Juniper Networks rasmiy hujjatlari, shuningdek Imperva, Akamai, Infosec Institute kabi xavfsizlik bo'yicha ilmiy-amaliy manbalar qiyosiy va tahliliy usullar yordamida o'rganildi. Tadqiqot natijalari shuni ko'rsatdiki, VLAN broadcast domenlarini kichraytirish, foydalanuvchi guruhlarini ajratish va Layer 2 darajasida xavfsizlik siyosatlarini joriy qilish nuqtai nazaridan samarali yechim hisoblanadi. Shu bilan birga, VLAN hopping, Switch Spoofing, Double Tagging va VTP zaifliklari kabi hujum vektorlari texnologiyaning cheklovlarini ochib beradi. Muhokamada VLAN ning mikrosegmentatsiya va Zero Trust modeli bilan qiyosiy tahlili keltirilgan. Xulosada VLAN ni DHCP Snooping, Dynamic ARP Inspection, Private VLAN va DTP ni o'chirish kabi qo'shimcha mexanizmlar bilan birgalikda qo'llash tavsiya etilgan.

Annotation: The logical separation of users and services with different security requirements within a single physical infrastructure has become a pressing challenge in modern enterprise networks. This article investigates the theoretical foundations of Virtual Local Area Network (VLAN) technology, the frame tagging mechanism based on the IEEE 802.1Q standard, and its significance for network security using the IMRAD structure. The study employs comparative and analytical methods to examine the IEEE 802.1Q-2018 standard, official Cisco and Juniper Networks documentation, as well as authoritative security sources such as Imperva, Akamai, and Infosec Institute. The findings demonstrate that VLAN technology effectively reduces broadcast domains, isolates user groups, and enforces Layer 2 security policies. However, attack vectors such as VLAN hopping, Switch Spoofing, Double Tagging, and VTP vulnerabilities reveal the inherent limitations of the technology. The discussion provides a comparative analysis of VLAN with microsegmentation and the Zero Trust model. The conclusion recommends combining VLAN with

complementary mechanisms such as DHCP Snooping, Dynamic ARP Inspection, Private VLAN, and disabling DTP to achieve a robust defense-in-depth strategy.

Kalit so'zlar: VLAN, IEEE 802.1Q, tarmoq xavfsizligi, kadrlarni teglashtirish, VLAN hopping, Switch Spoofing, Double Tagging, segmentatsiya, Private VLAN, mikrosegmentatsiya, Zero Trust, defense-in-depth.

Key words: VLAN, IEEE 802.1Q, network security, frame tagging, VLAN hopping, Switch Spoofing, Double Tagging, segmentation, Private VLAN, microsegmentation, Zero Trust, defense-in-depth.

KIRISH

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi va korporativ tarmoqlarga ulanuvchi qurilmalar sonining yildan-yilga ortib borishi natijasida zamonaviy tarmoq infratuzilmasi oldida ikki yo'nalishdagi murakkab vazifa paydo bo'ldi: bir tomondan tarmoq unumdorligini ta'minlash, ikkinchi tomondan turli xavfsizlik talablariga ega bo'lgan foydalanuvchi guruhlari, xizmatlar va qurilmalarni ishonchli ravishda ajratib turish. Moliya bo'limi xodimlari, marketing mutaxassislari, mehmonlar uchun mo'ljallangan Wi-Fi tarmog'i, IP-telefoniya, videokuzatuv tizimlari va Internet of Things (IoT) qurilmalari ko'pincha bitta fizik tarmoq infratuzilmasi orqali xizmat ko'rsatiladi. Bunday vaziyatda broadcast trafikning haddan tashqari ortishi tarmoq unumdorligini sezilarli darajada pasaytiradi, nosozliklarni aniqlash jarayonini murakkablashtiradi va eng asosiysi - xavfsizlik chegaralarini zaiflashtiradi [15].

Ushbu muammoga yechim sifatida 1990-yillar oxirida Virtual Local Area Network (VLAN) texnologiyasi taklif qilindi va keyinchalik IEEE (Institute of Electrical and Electronics Engineers) tomonidan 802.1Q standarti shaklida rasmiylashtirildi [1]. VLAN texnologiyasi bitta fizik kommutator yoki kommutatorlar majmuasining infratuzilmasini bir nechta mantiqiy broadcast domenlarga ajratish imkonini beradi va qurilmalarning fizik joylashuvidan qat'i nazar, ularni belgilangan mezonlar bo'yicha guruhlashga sharoit yaratadi. Vaqt o'tishi bilan VLAN faqatgina tarmoq unumdorligini oshirishga xizmat qiluvchi texnologiya darajasidan chiqib, tarmoq xavfsizligining muhim qatlamlaridan biriga aylandi [3].

Shu bilan birga, amaliyot shuni ko'rsatadiki, noto'g'ri konfiguratsiya qilingan yoki sukut bo'yicha sozlamalar saqlab qolingan VLAN tizimlari aksincha jiddiy xavfsizlik zaifliklariga olib kelishi mumkin. Switch Spoofing, Double Tagging va VLAN Trunking Protocol (VTP) zaifliklari kabi hujum vektorlari segmentatsiya chegaralarini chetlab o'tish imkonini beradi va shu sababli VLAN texnologiyasi atrofidagi xavfsizlik masalalari doimiy ravishda tadqiqot ob'ekti bo'lib qolmoqda [8, 11]. Bundan tashqari, bulutli hisoblash, konteynerlashtirish va mikroservis

arxitekturalarining keng tarqalishi an'anaviy VLAN-asosli segmentatsiyaning cheklovlarini yana ham yaqqolroq namoyon qildi, bu esa mikrosegmentatsiya va Zero Trust kabi yangi yondashuvlarning paydo bo'lishiga turtki bo'ldi [12, 13].

Tadqiqotning maqsadi VLAN texnologiyasining ishlash tamoyillarini, asosiy turlarini va tarmoq xavfsizligidagi rolini har tomonlama tahlil qilish, shuningdek, unga qaratilgan hujum vektorlari va himoya choralari bo'yicha asoslangan tavsiyalar ishlab chiqishdan iborat. Tadqiqotda quyidagi vazifalar bajariladi: IEEE 802.1Q standarti asosida VLAN ning texnik ishlash mexanizmini o'rganish; VLAN turlari va Inter-VLAN routing usullarini qiyosiy tahlil qilish; VLAN ga qaratilgan hujumlarni, jumladan VLAN hopping va VTP zaifliklarini batafsil tadqiq etish; VLAN ni mikrosegmentatsiya va Zero Trust modeli bilan taqqoslash hamda xavfsiz VLAN konfiguratsiyasi bo'yicha amaliy tavsiyalar shakllantirish. Tadqiqotning ilmiy yangiligi an'anaviy VLAN mexanizmlari va zamonaviy mikrosegmentatsiya yondashuvlarini birgalikda tahlil qilish, ularning bir-birini to'ldiruvchi jihatlarini aniqlash hamda defense-in-depth strategiyasi doirasida foydalanish bo'yicha tizimlashtirilgan tavsiyalar berishdir.

ADABIYOTLAR TAHLILI VA USULLAR

VLAN texnologiyasi va uning xavfsizlik jihatlari bo'yicha ilmiy adabiyotlar tahlili shuni ko'rsatadiki, mavzu yuzasidan tadqiqotlar bir necha asosiy yo'nalishlarda olib borilgan. Birinchi yo'nalishni texnologiyaning rasmiy standartlari va vendor hujjatlari tashkil etadi. IEEE 802.1Q-2018 standarti VLAN-aware tarmoqlarda kadrlarni teglashtirish formatini, trunk porti orqali ko'p VLAN trafigini uzatish qoidalarini va native VLAN tushunchasini batafsil belgilaydi [1]. Cisco Systems korporatsiyasining tarmoq segmentatsiyasi va VLAN Trunking Protocol (VTP) bo'yicha texnik hujjatlari amaliy ahamiyatga ega bo'lib, ko'pchilik korxonalarda qo'llaniluvchi standart konfiguratsiya yondashuvlarini aks ettiradi [3, 4]. Juniper Networks tomonidan e'lon qilingan Private VLAN bo'yicha texnik materiallar bitta IP-subnet doirasida qo'shimcha izolyatsiya darajasini ta'minlash imkoniyatlarini ochib beradi [7].

Ikkinchi yo'nalish - VLAN xavfsizligi va hujum vektorlariga bag'ishlangan ilmiy-amaliy tadqiqotlar. Imperva ekspertlarining tahlillarida VLAN hopping hujumi, jumladan Switch Spoofing va Double Tagging usullarining texnik mexanizmi batafsil tavsiflangan [8]. JumpCloud platformasining materiallari Double Tagging hujumining bosqichma-bosqich amalga oshirilishini va native VLAN ni majburiy teglash orqali himoya choralarini yoritadi [9]. Infosec Institute mutaxassislari VTP zaifliklari, voice va data trafikni ajratish hamda ovozli VLAN konfiguratsiyasi bo'yicha amaliy maslahatlar bergan [11]. Cisco kompaniyasining Dynamic ARP Inspection (DAI)

konfiguratsiyasi bo'yicha rasmiy qo'llanmasi DHCP Snooping jadvali asosida ARP-spoofing hujumlariga qarshi qatlamli himoya qurish usulini tushuntiradi [6].

Uchinchi yo'nalishni VLAN va zamonaviy segmentatsiya yondashuvlarini taqqoslovchi tadqiqotlar tashkil etadi. Akamai Technologies tahlilchilari VLAN va mikrosegmentatsiya o'rtasidagi farqlarni granularlik, qatlam, konfiguratsiya murakkabligi va Zero Trust mosligi mezonlari bo'yicha solishtirgan [12]. Zero Networks tadqiqotchilari esa VLAN ni mustaqil mikrosegmentatsiya strategiyasi sifatida ko'rishning chekli ekanligini asoslab bergan va lateral movement hujumlariga qarshi himoyaning yetishmasligini ta'kidlagan [13]. NetworkAcademy.IO va Cisco Press platformalari Inter-VLAN routing uchun Layer 3 switch va Switched Virtual Interface (SVI) yordamida amalga oshiriladigan zamonaviy yondashuvlarni tavsiflagan [5, 14]. ITU Online va Lightyear.ai resurslari broadcast domen tushunchasi va uning tarmoq unumdorligiga ta'sirini sodda akademik tilda izohlagan [15, 16].

Tadqiqotda nazariy-analitik metodologiya qo'llanildi va u o'zaro bog'liq to'rt bosqichdan tashkil topdi. Birinchi bosqichda tavsifiy tahlil usulidan foydalanib, VLAN ning umumiy arxitekturasi, IEEE 802.1Q kadr formatining tarkibi va Tag Protocol Identifier, Priority Code Point, Drop Eligible Indicator hamda VLAN Identifier maydonlarining vazifalari o'rganildi. Ikkinchi bosqichda qiyosiy tahlil orqali VLAN turlari port-based, tag-based, MAC-based va Private VLAN ko'rinishida tasniflandi, shuningdek, an'anaviy VLAN segmentatsiyasi mikrosegmentatsiya bilan taqqoslandi. Uchinchi bosqichda xavf tahlili usuli qo'llanilib, VLAN hopping va VTP zaifliklarining ishlash mexanizmi hamda ularga qarshi himoya choralari batafsil ko'rib chiqildi. To'rtinchi bosqichda sintez metodi orqali olingan ma'lumotlar umumlashtirilib, xavfsiz VLAN konfiguratsiyasi bo'yicha tizimlashtirilgan amaliy tavsiyalar shakllantirildi.

VLAN texnologiyasining xavfsizlik xususiyatlarini baholashda axborot xavfsizligining klassik to'rt mezonidan foydalanildi. Konfidensiallik mezoni segmentlar o'rtasidagi noqonuniy ma'lumot uzatishni cheklash imkoniyatini baholashga xizmat qiladi. Yaxlitlik mezoni tarmoq trafigini soxtalashtirish, spoofing va ARP poisoning kabi hujumlarga qarshilik darajasini o'lchaydi. Foydalanilishi mezoni broadcast yukini kamaytirish va tarmoq unumdorligiga umumiy ta'sirni qamrab oladi. Boshqaruv qulayligi mezoni esa masshtablanish imkoniyatlari, konfiguratsiya murakkabligi va inson omiliga bog'liq xato ehtimolini hisobga oladi. Ushbu mezonlar majmuasi VLAN texnologiyasining kuchli va zaif tomonlarini ob'ektiv baholash uchun asos bo'lib xizmat qildi.

MUHOKAMA

VLAN texnologiyasining tarmoq xavfsizligidagi o'rni haqida olib borilgan tahlil shuni ko'rsatadiki, ushbu yechim bir vaqtning o'zida ham kuchli, ham zaif tomonlarga

ega bo'lib, uning samaradorligi ko'p jihatdan konfiguratsiya sifati va qo'shimcha himoya mexanizmlari bilan birgalikda qo'llanilishiga bog'liq. VLAN ning kuchli tomonlari sifatida birinchi navbatda mantiqiy segmentatsiya imkoniyatini ko'rsatish mumkin, bu esa qurilmalarning fizik joylashuviga bog'liq bo'lmagan moslashuvchan guruhlash sxemalarini yaratishga imkon beradi. Bundan tashqari, har bir VLAN alohida broadcast domen sifatida ishlashi tufayli tarmoq trafigining sezilarli qismi cheklangan hududda saqlanadi va bu unumdorlikni oshiradi [16]. VLAN ning iqtisodiy jihatdan ham qulayligi muhim ahamiyatga ega: alohida fizik infratuzilma qurish o'rniga mavjud kommutatorlar resursidan samarali foydalanish imkonini beradi. Texnologiyaning IEEE 802.1Q standarti doirasida rasmiylashtirilganligi va deyarli barcha yetakchi vendorlar tomonidan qo'llab-quvvatlanishi esa uni keng joriy etish uchun universal asos yaratadi.

Shu bilan birga, Akamai Technologies va Zero Networks tomonidan o'tkazilgan tahlillar VLAN ning bir qator jiddiy cheklovlarini ochib bergan [12, 13]. Birinchi va eng muhim cheklov - granularlik darajasining yetarli emasligi. VLAN qurilmalarni keng kriteriyalar bo'yicha guruhlaydi, lekin individual ish yuki, ilova yoki jarayon darajasidagi nozik nazoratni ta'minlay olmaydi. Bu hujumchi tarmoq segmentiga muvaffaqiyatli kirib olgan vaziyatda u shu segment ichidagi barcha resurslarga deyarli erkin kirish imkoniga ega bo'lishini anglatadi va lateral movement deb ataluvchi yon yo'nalishdagi harakatlanishga sharoit yaratadi. Ikkinchi muhim cheklov bulutli hisoblash va konteyner muhitlarida namoyon bo'ladi: VLAN an'anaviy ravishda fizik kommutator porti bilan bog'langan tushuncha bo'lib, dinamik ravishda yaratiluvchi va o'chiriluvchi konteyner ish yuklariga osongina kengaytirilmaydi. Uchinchi cheklov - yirik tarmoqlarda boshqaruv murakkabligining keskin ortishi, bu esa konfiguratsiya xatolari ehtimolini oshiradi va xavfsizlik holatini zaiflashtiradi.

VLAN va mikrosegmentatsiya o'rtasidagi qiyosiy tahlil ushbu ikki yondashuvning bir-birini istisno qiluvchi emas, balki to'ldiruvchi xarakterga ega ekanligini ko'rsatadi. VLAN asosan Layer 2 darajasida ishlaydi va kommutator portlari orqali konfiguratsiya qilinadi, mikrosegmentatsiya esa Layer 7 gacha bo'lgan barcha qatlamlarda dasturiy va dinamik tarzda amalga oshiriladi. VLAN ning granularligi guruh yoki subnet darajasi bilan cheklangan bo'lsa, mikrosegmentatsiya alohida ish yuki, ilova yoki hatto jarayon darajasida himoya yarata oladi. Zero Trust mosligi nuqtai nazaridan VLAN cheklangan imkoniyatlarga ega bo'lsa, mikrosegmentatsiya bu modelga to'liq mos keladi. Lateral movement hujumlariga qarshi himoyada VLAN zaif natija ko'rsatsa, mikrosegmentatsiya kuchli himoyani ta'minlaydi. Bulutli va konteyner muhitlariga qo'llab-quvvatlash masalasida VLAN ning imkoniyatlari deyarli yo'q yoki juda cheklangan, mikrosegmentatsiya esa bu muhitlarda to'liq ishlay oladi.

Zero Trust modeli kontekstida VLAN ning rolini alohida muhokama qilish zarur. Ushbu model hech qachon ishonma, har doim tekshir tamoyiliga asoslanadi va foydalanuvchining tarmoq ichida joylashganligi unga hech qanday avtomatik imtiyoz bermasligini taqozo etadi. VLAN ning an'anaviy ichki tarmoq ishonchli yondashuvi bu talabga to'liq mos kelmaydi va shu sababli ba'zi tadqiqotchilar VLAN ni eskirgan texnologiya sifatida baholashga moyildirlar. Biroq amaliyot shuni ko'rsatadiki, VLAN Zero Trust arxitekturasini qurishda birinchi qatlam segmentatsiyasi sifatida o'z ahamiyatini saqlab qoladi. Aniqrog'i, VLAN broadcast domenlarni ajratish va Layer 2 hujumlariga qarshi asosiy himoya chizig'ini yaratish vazifasini bajaradi, mikrosegmentatsiya va kimlikka asoslangan kirish nazorati esa undan yuqori qatlamlarda nozik granularlikni ta'minlaydi [12]. Shu tarzda VLAN va mikrosegmentatsiya bir-birini almashtirmaydi, balki defense-in-depth strategiyasi doirasida bir-birini to'ldiradi.

Amaliy nuqtai nazardan VLAN konfiguratsiyasining xavfsizligini ta'minlash uchun bir qator tavsiyalarni hisobga olish zarur. Ishlatilmaydigan alohida VLAN ni native VLAN sifatida belgilash va uni majburiy teglash Double Tagging hujumlarining oldini olishda hal qiluvchi ahamiyatga ega. Trunk bo'lmagan barcha portlarda Dynamic Trunking Protocol ni o'chirish va switchport mode access hamda switchport nonegotiate buyruqlari orqali portlarning avtomatik trunk holatiga o'tishini bloklash Switch Spoofing hujumiga qarshi samarali himoyani ta'minlaydi. VTP protokolidan foydalanishda ehtiyot bo'lish va imkoniyat mavjud bo'lsa transparent rejimda ishlatish yoki butunlay o'chirish katta tarmoq inqirozlarining oldini oladi. Har bir kirish kommutatorida DHCP Snooping va Dynamic ARP Inspection mexanizmlarini yoqish soxta DHCP serverlari va ARP-spoofing hujumlariga qarshi qatlamli himoya yaratadi. Umumiy infratuzilmali muhitlarda Private VLAN qo'llash bitta subnet ichidagi qurilmalarni bir-biridan ajratish imkonini beradi, bu mehmonxonalar Wi-Fi tarmog'i va kolokatsiya markazlarida ayniqsa muhimdir [11].

NATIJALAR

O'tkazilgan nazariy-analitik tadqiqot natijasida VLAN texnologiyasining texnik asoslari, xavfsizlik xususiyatlari va zamonaviy segmentatsiya yondashuvlari bilan o'zaro nisbati bo'yicha qator muhim xulosalar olindi. IEEE 802.1Q standartining batafsil tahlili shuni ko'rsatdiki, VLAN-aware tarmoq qismida har bir Ethernet kadriga 4 baytli teg qo'shiladi va u to'rt asosiy maydondan tashkil topadi. Tag Protocol Identifier maydoni 16 bitli bo'lib, 0x8100 qiymatiga ega va kadrning 802.1Q-tagged ekanligini bildiradi. Priority Code Point maydoni 3 bit hajmda IEEE 802.1p QoS prioritetini belgilaydi. Drop Eligible Indicator maydoni 1 bit hajmda tarmoq tiqilinchi sharoitida paketning tashlanish ehtimolini ifoda etadi. VLAN Identifier maydoni 12 bit hajmda VLAN raqamini saqlaydi va nazariy jihatdan 4094 ta VLAN ni qo'llab-

quvvatlash imkonini beradi, chunki 0 va 4095 qiymatlari rezerv qilingan. 802.1Q teg qo'shilgandan so'ng Ethernet kadrining trayleri tarkibidagi Frame Check Sequence qayta hisoblanadi va bu kadrning yaxlitligini ta'minlaydi [1, 2].

VLAN ning broadcast domenlarini ajratish samarasi bo'yicha olib borilgan tahlil shuni tasdiqladiki, bitta fizik kommutator infratuzilmasini bir nechta mantiqiy broadcast domenlarga bo'lish tarmoq unumdorligini sezilarli darajada oshiradi. Qurilmalar faqat o'z VLAN i ichidagi broadcast trafikni qabul qiladi, bu esa keraksiz trafik hajmini kamaytiradi va xavfsizlik chegarasini mustahkamlaydi [15]. Inter-VLAN routing masalasi tahlilida aniqlandiki, VLAN lar o'rtasida aloqa o'rnatish uchun uchinchi qatlam qurilmasi zarur va eng samarali yechim Layer 3 switch va unda yaratilgan Switched Virtual Interface (SVI) dan foydalanishdir. SVI har bir VLAN uchun default gateway vazifasini bajaradi va ip routing buyrug'i orqali yoqiladi [5, 14]. Yuqori xavfsizlik talab qilinadigan muhitlarda esa Inter-VLAN trafikni firewall orqali o'tkazish tavsiya etiladi, chunki bu chuqurlashtirilgan trafik nazorati va qoidalarni qo'llash imkonini beradi.

VLAN texnologiyasiga qaratilgan hujum vektorlari tahlili uchta asosiy tahdid turini aniqlashga olib keldi. Birinchi tahdid - Switch Spoofing, ya'ni kommutatorni qalbakilashtirish hujumi bo'lib, unda hujumchi o'z qurilmasini trunk porti sifatida ko'rsatishga harakat qiladi. Cisco kommutatorlarida sukut bo'yicha Dynamic Trunking Protocol yoqilgan holatda port avtomatik tarzda trunk holatiga o'tishi mumkin va bu hujumchiga barcha VLAN trafigiga kirish imkoniyatini beradi [8]. Ikkinchi tahdid - Double Tagging hujumi bo'lib, unda hujumchi paketga ikkita 802.1Q teg qo'shadi: tashqi teg hujumchining o'z native VLAN ini, ichki teg esa nishon VLAN ni ko'rsatadi. Birinchi kommutator tashqi tegni olib tashlaydi va paketni native VLAN sifatida trunk orqali yo'naltiradi, ikkinchi kommutator esa ichki teg asosida paketni nishon VLAN ga yetkazadi, shu tariqa segmentatsiyani chetlab o'tadi [9]. Uchinchi tahdid VTP zaifliklari bilan bog'liq: yuqori revision raqamiga ega yangi kommutator tarmoqqa ulansa, butun VLAN ma'lumotlar bazasini bekor qilishi yoki o'zgartirishi mumkin va shuning uchun ekspertlar VTP dan ehtiyotkorlik bilan foydalanishni tavsiya etadilar [11].

Layer 2 darajasidagi qo'shimcha himoya mexanizmlari tahlili to'rt asosiy yechimni ajratib ko'rsatishga imkon berdi. DHCP Snooping mexanizmi DHCP trafikni nazorat qiladi, soxta DHCP serverlarini bloklaydi va IP-MAC bog'lanish jadvalini yaratadi. Dynamic ARP Inspection ushbu jadval asosida ARP paketlarni tekshiradi va ARP-spoofing hujumlariga qarshi himoya qiladi [6]. Port Security mexanizmi port orqali ulanadigan MAC manzillar sonini cheklash imkonini beradi. Private VLAN texnologiyasi esa VLAN ichidagi portlarni izolyatsiya qiladi va faqat ma'lum uplink yoki community guruhi bilan aloqa imkonini ta'minlaydi [7, 10]. Private VLAN bitta

broadcast domenni ikkilamchi VLAN larga ajratadi: isolated VLAN dagi portlar faqat promiscuous uplink port bilan, community VLAN dagi portlar esa bir-biri va uplink bilan aloqa o'rnatadi. Bu IP-manzillarni tejash va bitta subnet ichidagi qurilmalarni bir-biridan ajratish imkonini beradi, bu xususiyat mehmonxonalar Wi-Fi tarmog'i va ma'lumotlar markazlaridagi serverlar uchun ayniqsa muhim hisoblanadi.

Tadqiqotning yakuniy natijalaridan biri sifatida VLAN va mikrosegmentatsiyaning bir-birini istisno qiluvchi emas, balki to'ldiruvchi yechimlar ekanligi asoslandi. VLAN Layer 2 darajasida keng segmentatsiyani ta'minlaydi, mikrosegmentatsiya esa undan yuqori qatlamlarda nozik granularli himoyani amalga oshiradi. Defense-in-depth strategiyasi doirasida bu ikki yondashuvni birgalikda qo'llash zamonaviy tarmoq tahdidlariga qarshi eng samarali himoyani ta'minlaydi. Tadqiqot shuningdek shuni ko'rsatdiki, VLAN ning samaradorligi to'g'ridan-to'g'ri konfiguratsiya sifatiga bog'liq va sukut bo'yicha sozlamalarni o'zgartirmasdan qoldirish texnologiyaning eng katta zaifligi hisoblanadi.

XULOSA

O'tkazilgan tadqiqot natijalari shuni ko'rsatdiki, VLAN texnologiyasi IEEE 802.1Q standarti asosida ishlab chiqilgan va bugungi kungacha korporativ tarmoqlarda mantiqiy segmentatsiyaning asosiy vositasi bo'lib qolmoqda. VLAN broadcast domenlarni kichraytirish, foydalanuvchi guruhlarini izolyatsiya qilish va Layer 2 darajasida xavfsizlik siyosatlarini joriy qilish nuqtai nazaridan samarali yechim hisoblanadi. Texnologiyaning standartlashtirilganligi, vendorlar tomonidan keng qo'llab-quvvatlanishi va iqtisodiy jihatdan qulayligi uni zamonaviy tarmoq infratuzilmasining ajralmas qismiga aylantirgan.

Shu bilan birga, tadqiqot VLAN texnologiyasining bir qator jiddiy cheklovlarini ham aniqladi. VLAN hopping hujumlari, jumladan Switch Spoofing va Double Tagging, VTP protokolining zaifliklari, granularlikning yetishmasligi va bulutli muhitlarda kengaytirilishining cheklanganligi VLAN ni mustaqil xavfsizlik yechimi sifatida qabul qilishga to'sqinlik qiladi. Zamonaviy kiberhujumlarning, ayniqsa lateral movement va ichki tahdidlarning ortib borishi VLAN ni mustaqil himoya vositasi sifatida emas, balki defense-in-depth strategiyasining bir qismi sifatida ko'rishni taqozo etadi.

Tadqiqot natijalariga asoslangan holda quyidagi amaliy tavsiyalar ishlab chiqildi. Birinchidan, korporativ tarmoqlarda VLAN konfiguratsiyasi xavfsizlik nuqtai nazaridan sinchkovlik bilan ishlab chiqilishi va sukut bo'yicha sozlamalar majburiy ravishda o'zgartirilishi zarur. Bunda native VLAN sifatida ishlatilmaydigan alohida VLAN tayinlanishi va majburiy teglash yoqilishi, trunk bo'lmagan barcha portlarda Dynamic Trunking Protocol o'chirilishi, VTP transparent rejimda ishlatilishi yoki butunlay o'chirilishi tavsiya etiladi. Ikkinchidan, har bir kirish kommutatorida DHCP

Snooping va Dynamic ARP Inspection mexanizmlari yoqilishi, umumiy infratuzilmali muhitlarda Private VLAN qo'llanilishi va Inter-VLAN trafik muhim segmentlar uchun firewall orqali o'tkazilishi maqsadga muvofiqdir. Uchinchidan, zamonaviy tarmoq xavfsizligi konsepsiyalari talablariga javob berish uchun VLAN mikrosegmentatsiya va Zero Trust tamoyillari bilan birgalikda qo'llanilishi tavsiya etiladi.

Kelajakdagi tadqiqot yo'nalishlari sifatida bir qator dolzarb masalalarni ajratib ko'rsatish mumkin. SDN muhitida VLAN va VXLAN texnologiyalarining qiyosiy tahlili dasturiy-aniqlangan tarmoqlar sharoitida segmentatsiyani amalga oshirishning eng samarali usullarini aniqlashga xizmat qilishi mumkin. Cisco ACI, VMware NSX, Illumio va Zero Networks kabi mikrosegmentatsiya yechimlarining amaliy taqqoslamasi korxonalarga texnologiyani tanlashda asoslangan qaror qabul qilishga yordam beradi. IoT tarmoqlarida VLAN segmentatsiyasini avtomatlashtirish bo'yicha izlanishlar ulanuvchi qurilmalar sonining keskin ortishi sharoitida boshqaruv murakkabligini kamaytirish imkonini yaratadi. 5G va edge computing muhitida VLAN ning rolini chuqur o'rganish esa keyingi avlod telekommunikatsiya infratuzilmasida segmentatsiya yondashuvlarini takomillashtirishga ko'maklashadi.

ADABIYOTLAR RO'YXATI

1. IEEE Standards Association. IEEE 802.1Q-2018 - Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks // IEEE. – 2018. – 1993 p.
2. Wikipedia. IEEE 802.1Q // Wikimedia Foundation. – 2024. – URL: https://en.wikipedia.org/wiki/IEEE_802.1Q
3. Cisco Systems. What Is Network Segmentation? // Cisco Learn Center. – 2023. – URL: https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-segmentation.html
4. Cisco Systems. Understand VLAN Trunk Protocol (VTP) // Cisco Technical Documentation. – 2022. – URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html
5. Cisco Press. Inter-VLAN Routing using Layer 3 Switches // Cisco Press Articles. – 2021. – URL: https://www.ciscopress.com/articles/article.asp?p=3089357
6. Cisco Systems. Configuring Dynamic ARP Inspection (DAI) // Cisco Catalyst 3850 Configuration Guide. – 2020. – 24 p.
7. Juniper Networks. Understanding Private VLANs (Junos OS) // Juniper TechLibrary. – 2023. – URL: https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/topic-map/private-vlans-qfx-series.html

8. Imperva. What is VLAN Hopping: Risks, Attacks & Prevention // Imperva Learning Center. – 2023. – URL: https://www.imperva.com/learn/availability/vlan-hopping/
9. JumpCloud. What Is a Double-Tagging Attack? // JumpCloud IT Index. – 2023. – URL: https://jumpcloud.com/it-index/what-is-a-double-tagging-attack
10. JumpCloud. What Is a Private VLAN? // JumpCloud IT Index. – 2023. – URL: https://jumpcloud.com/it-index/what-is-private-vlan
11. Infosec Institute. VLAN Network Segmentation and Security - Chapter Five // Infosec Resources. – 2022. – URL: https://www.infosecinstitute.com/resources/management-compliance-auditing/vlan-network-chapter-5/
12. Akamai Technologies. Comparing the Benefits of Microsegmentation vs. VLANs // Akamai Security Blog. – 2023. – URL: https://www.akamai.com/blog/security/comparing-the-benefits-of-microsegmentation-versus-vlans
13. Zero Networks. VLANs Are Not a Microsegmentation Strategy // Zero Networks Blog. – 2023. – URL: https://zeronetworks.com/blog/vlans-are-not-a-microsegmentation-strategy
14. NetworkAcademy.IO. InterVLAN Routing using Layer 3 Switch // CCNA Course Materials. – 2023. – URL: https://www.networkacademy.io/ccna/ethernet/intervlan-routing
15. ITU Online. Broadcast Domain: What It Is And Why It Matters // ITU Online Tech Definitions. – 2023. – URL: https://www.ituonline.com/tech-definitions/what-is-a-broadcast-domain/
16. Lightyear.ai. What are Broadcast Domains? // Lightyear Networking Tips. – 2023. – URL: https://lightyear.ai/tips/what-are-broadcast-domains