CISCO PACKET TRACER DASTURI YORDAMIDA TARMOQ ISHINI MODELLASHTIRISH

Farg'ona davlat universiteti, magistratura bo'limi
amaliy matematika yo'nalishi 1-bosqich magistranti
Mamazoidova Guliruxsor

Annotatsiya. *Ushbu maqola amaliy ahamiyatga ega bo‘lib, maqolada cisco packet tracer yordamida hususiy korxonalar uchun maxsus himoyalangan tarmoq kanali ishi loyihalash bosqichma bosqich ko‘rsatib o‘tilgan. Hususiy korxonalar va ularni hududiy filiallarini maxsus himoyalangan kanal orqali ma’lumotlar uzatishni ta’minlash maqsadida mahsus tarmoq qurishda foydalaniladigan qurilmalar va ularni xavfsizlik parametrlarini sozlash batafsil tushuntirib o‘tilgan. Natijada amaliy ahamiyatga ega mahsus tarmoq loyihasi bajarilishiga erishilgan.*

Kalit so‘zlar: *cisco packet tracer, kanal, Lan, UTP, MAN, ASA, server, router, svitch, Host.*

Marshrutizatorlar maxsus marshrutlash algoritmlari asosida ma'lumotlarni uzatishning optimal marshrutini izlash uchun ishlatiladi, masalan, transit tugunlarining eng kam soniga ega marshrutni (yo'lni) tanlash. Ushbu bo‘limda tadqiqot natijalariga ko‘ra Cisco Packet Tracer simulatori yordamida hususiy korxona bosh ofisi ham ularni hududiy filiallari o‘rtasida kompyuter tarmoqlari yordamida maxsus aloqa kanalini yaratish loyihasi taqdim etilgan. Buning uchun bizga Cisco Packet Traser dasturini 8.2.1 versiyani kompyuterimizga o‘rnatish talab etiladi. Loyihani amalga oshirishda reallikga urg‘u bergan holda Farg‘ona viloyatida Oltiariq tumani “Taraqqiyot omad eksport” MCHJ korxonasi uchun Oltiariq tumani bosh ofisi, Farg‘ona shahar, Rishton tumani, Qo‘qon shahar, hududiy filiallari o‘rtasida o‘zaro malumot almashish uchun maxsus kanali loyihasini ishlab chiqish maqsad qilib olingan. Oraliq tarmoqlardan foydalanishda

“O‘zbektelekom” AK ATClaridan foydalanilgan. Maxsus kanal hosil qilishda Mesh topologiyasidan foydalangan holda MAN tarmog‘i va ichki LAN tarmog‘i qurishda chiziqli, yulduz topologiyalaridan foydalanamiz. Umumiy tarmog‘da Routerlar, ASA firewallar, switchlar, server kompyuterlar, shaxsiy kompyuterlar, WiFi routerlar kabi qurilmalardan hamda serial koaksial, UTP kabellaridan foydalanilgan. Adabiyotlar tahlili va metodologiya. Maqolani yozishda Mulayam Singh. CISCO PACKET TRACER LABS kitobidagi laboratoriya ishlaridan, Наполова Е.И. Кожевников С.В. Защита компьютерных сетей на основе технологии virtual private network mavzusidagi va D.Tojimatovning “Kiberxavfsizlik: tahdilar, muammolar, yechimlar” mavzusidagi hamda D.Tojimatovning “Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems” mavzusidagi maqolalari o‘rganib chiqilib, tahlil qilingan. Yuqorida nomi keltirilgan tadqiqotchilarning ilmiy maqolalaridan foydalanib iqtiboslar keltirilgan. Huddi shu amallarni “Create New Building” bo‘limi yordamida yangi binolarni yaratgan holda korxona va ATC larni fizik ko‘rinishlarini keltiramiz. Endi korxonamizning ichki xonalari va tarmoq qurilmalari joylashuvini fizik ko‘rinishlarini rasmda ko‘rsatilganidek tayyorlab olamiz. Buning uchun bino ko‘rinishidagi raimni ichiga “Create New Building” orqali xona sxemasi rasmini yuklab olamiz. Tarmog‘imizni fizik ko‘rinishini yaratib olgandan so‘ng, server xona uchun “Create New Closet” uskunasi orqali server xonani ishchi shkafi va stolini serverxona sifatida keltirilgan xonamizga joylashtiramiz. Oraliq tashqi tarmoq routerlariga RIP (Routing Information Protocol) protokoli yordamida marshrutizatsiya rejimini sozlab qo‘yamiz. Buning uchun routerni barcha ulangan portlariga alohida ip manzillar berib chiqish va portlarni yoqish hamda turli ip manzillarga ega portlarda paketlar marshrutizatsiya bo‘lishi uchun RIP buyrug‘larini kiritishtalab qilinadi. Buning uchun xar bir routerni CLI (Command Line) bo‘limiga o‘ziga beriladigan ip manzilni tanib olgan holda quyidagicha buyruqlarni berib chiqamiz. Birinchi navbatda tashkil etilgan korxona tarmog‘ining ichki tarmog‘iga ichki axborotlarni sizib chiqishidan himoyalash uchun korxona tuzilmasidan kelib chiqib Vlan

texnologiyasi asosida maxsus kanallar hosil qilib olamiz. Bizni holatda korxona tarkibi “Server xona”, “ATM bo‘limi”, “Boshliq xonasi”, “Qabulxona”, “Bug‘alteriya”, “Marketing bo‘limi”, “Hodimlar xonasi”dan iborat. Korxona uchun quyidagi ko‘rinishda va nomlar bilan alohida ajratilgan maxsus kanal hosil qilishni tavsiya etamiz. •Administrator kanali; •Boshqaruvchilar kanali; •Hodimlar kanali. Administratorlar kanali bog‘lanuvchilari tarmoqda to‘liq boshqaruv huquqi bo‘lganligi bois server xona va ATM bo‘limini kompyuterlariga barcha qurulmalarga ulanish huquqini beramiz. Boshqaruv kanaliga boshliq xonasi, bug‘alteriya, marketing bo‘limini bog‘laymiz va boshliq uchun bu kanaldan tashqari boshqa kanallar bilan ham bog‘lanish huquqini beramiz. Hodimlar kanaliga qabulxona va hodimlar bo‘limidagi kompyuterlarni bog‘laymiz. Bularni barchasini markaziy boshqariladigan SWITCH qurulmasida amalga oshiramiz. SWITCH orqali yuqorida nomi keltirilgan kanallarni hosil qilib, ulangan portlarni statusiga qarab kanallarga biriktirib chiqamiz. Bu SWITCH qurilmasiga quyidagi ketmaketlikda buyruqlarni kiritish orqali amalga oshiriladi. 1. Telnet yoki SSH protokoli yoki SWITCHni konsol portiga admin kompyuterini ulagan holda CLI oynasida SWITCHni Confugratsiyasiga (sozlamalari) kirib olamiz. Agar masofadan bog‘lanish uchun telnet yoqilgan bo‘lmasa avvaliga konsol port orqali ulanib telnetni yoqib olish tavsiya etiladi. Yuqorida berilgan loyiha ma’lumotlari asosida hususiy korxonalar va ularning hududiy filiallari uchun xavfsiz ma’lumot almashishga asoslangan mahsus tarmoq qurish mumkun. Mahsus tarmoqning avzalliklari sifatida birinchi navbatda o‘rtadagi odam hujumi, DDos hujumi, tarmoq uzulish xatoliklari kabi xavf-xatarlarini ko‘rsatishimiz mumkun. Ishning amaliy yangiligi sifatida mesh texnologiyasi, stp protokoli, vpn texnologiyalarini birgalikda qo‘llash avfzalliklarini keltirishimiz mumkun. Berilgan loyihani model sifatida har qanday korxona va tashkilotlarda qo‘llash va natijaga erishish real tarmoqqa qo‘llagan holda tekshirib ko‘rilgan va ijobiy xulosa olingan.

Adabiyotlar ro‘yxati

[1]. Mulayam Singh. CISCO PACKET TRACER LABS/ BookRix, 2019.

[2]. Наполова Е.И. Кожевников С.В. Защита компьютерных сетей на основе технологии virtual private network/ Экономика и качество систем связи. 2018

[3]. Dostonbek T., Jamshid M. Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems //Central Asian Journal of Theoretical and Applied Science. – 2023. – Т. 4. – №. 4. – С. 93-98.

[4].Tojimatov D. X. Kiberxavfsizlik: tahdilar, muammolar, yechimlar, "//Axborotkommunikatsiya texnologiyalari va telekommunikatsiyalari sohasida zamonaviy muammolar va yechimlar"