XAVFSIZLIK DEVORLARI UCHUN TARMOQ ARXITEKTURASI

A.G‘. Muhammadjonov
Muhammad Al-Xorazmiy nomidagi TATU Farg‘ona filiali
“Dasturiy inginiring” kafedrasi assistenti.

ANNOTATSIYA

Xavfsizlik devorining eng muhim jihati shundaki, u himoya qiladigan tarmoqqa ulangan tizimning kirish nuqtasida joylashgan. Bu shuni anglatadiki, xavfsizlik devori kiruvchi tarmoq trafigini qabul qiluvchi va boshqaradigan birinchi dastur va u chiquvchi trafikni boshqaradigan oxirgi dasturdir.

Kalit so‘zlar: firewall, tarmoq, axborot xavfsizlik, xavfsizlik devorlari.

Firewall (Xavfsiz devori)uchun tarmoq arxitekturasi. Xavfsizlik devori yordamida tashqi oqimlardan himoya qilish uchun tarmoq tuzilishining ba’zi namunalari mavjud:

1. Internetga ajratilgan ulanishdagi router xavfsizlik devori tizimiga ulanishi mumkin. Bu xavfsizlik devoridan tashqarida to‘liq kirish serverlari uchun markaz yordamida ham ta’minlanishi mumkin.

2. Routerni ba’zi filtrlash qoidalari bilan sozlash mumkin. Biroq, ushbu router ISPga tegishli bo‘lishi mumkin, shuning uchun ISPdan barcha kerakli boshqaruvni o‘rnatish so‘ralishi mumkin.

3. ISDN liniyasi kabi dialup xizmatida filtrlangan DMZni ta’minlash uchun uchinchi tarmoq kartasi ishlatiladi. Bu Internet xizmatlarini to‘liq nazorat qilish imkonini beradi va ularni oddiy tarmoqdan ajratib turadi.

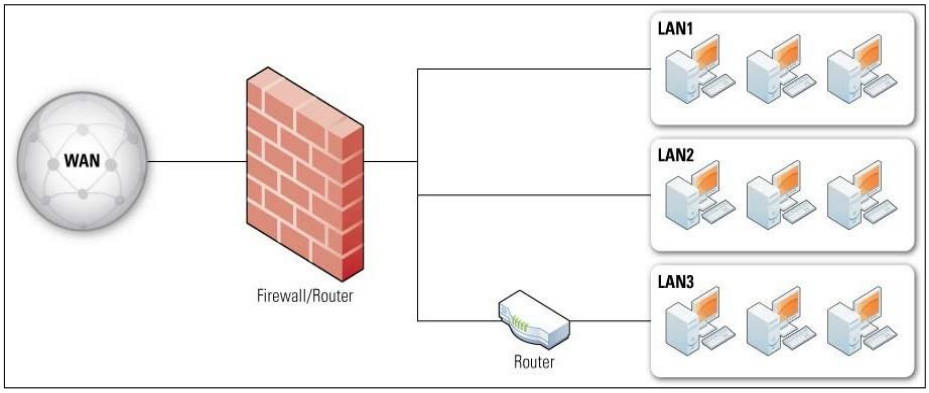
4. Proksi-server tarmoqdagi trafikni kuzatish va foydalanuvchilarga cheklangan miqdordagi xizmatlardan foydalanish imkonini berish yoki ba’zi kiruvchi xizmatlarni bloklash uchun ishlatilishi mumkin. Bu xavfsizlik devori bilan birlashtirilishi mumkin.

5. Xavfsizlik devoriga ulangan tashkilotning LAN tarmog‘idagi proksi-server faqat proksi-server taqdim etayotgan xizmatlar uchun Internetga ulanishiga ruxsat beruvchi qoidalarga ega bo‘lishi kerak. Shunday qilib, foydalanuvchilar Internetga faqat proksi-server orqali kirishlari mumkin.

1-rasmda router vazifasini bajaruvchi apparat xavfsizlik devori qurilmasi bilan odatiy tarmoq sxemasi ko‘rsatilgan. Xavfsizlik devorining himoyalanmagan tomoni “WAN” deb nomlangan yagona yo‘lga, himoyalangan tomoni esa “LAN1”, “LAN2” va “LAN3” etiketli uchta yo‘lga ulanadi. Xavfsizlik devori keng maydon tarmog‘i (WAN) yo‘li va LAN yo‘llari o‘rtasidagi trafik uchun marshrutizator vazifasini bajaradi. Rasmda LAN yo‘llaridan birida router ham mavjud; ba’zi tashkilotlar tarmoq ichidagi eski marshrutlash siyosati tufayli bir necha qatlamli marshrutizatorlardan foydalanishni afzal ko‘radi.

1-rasm. Xavfsizlik devori qurilmasi bilan oddiy marshrutlangan tarmoq.

Ko‘pgina apparat xavfsizlik devori qurilmalari DMZ(demilitarizatsiya zonalari) deb nomlangan xususiyatga ega. Kompyuter xavfsizligi sohasida DMZ tarmog‘i



(ba’zan “demilitarizatsiya zonasi” deb ataladi) tashkilotning ochiq, tashqi ko‘rinishdagi xizmatlarini o‘z ichiga olgan kichik tarmoq sifatida ishlaydi. U ishonchsiz tarmoqlarga, odatda Internetga ta’sir qiladigan nuqta sifatida ishlaydi. DMZning maqsadi tashkilotning mahalliy tarmog‘iga qo‘shimcha xavfsizlik qatlamini qo‘shishdir. Ichki tarmoqdan tashqarida joylashgan himoyalangan va nazorat qilinadigan tarmoq tugunlari DMZda ko‘rinadigan narsalarga kirishlari mumkin, tashkilot tarmog‘ining qolgan qismi esa xavfsizlik devori orqasida xavfsiz hisoblanadi. To‘g‘ri amalga oshirilganda, DMZ tarmog‘i tashkilotlarga qimmatli aktivlar saqlanadigan ichki tarmoqqa yetib borgunga qadar xavfsizlik buzilishlarini aniqlash va yumshatishda qo‘shimcha himoya beradi.

Xavfsiz masofaviy kirish: VPN kabi xavfsiz masofaviy kirish mexanizmlari vakolatli foydalanuvchilarga tashqi joylardan xavfsiz tarzda tarmoqqa kirish imkonini beradi. Ular umumiy tarmoqlar orqali uzatiladigan ma’lumotlarning maxfiyligi va yaxlitligini ta’minlash uchun shifrlash va autentifikatsiyadan foydalanadilar. Tarmoq monitoringi vositalari tarmoq trafigini va tizim jurnallarini doimiy ravishda kuzatib boradi, bu esa ma’murlarga potentsial xavfsizlik muammolarini ko‘rish imkonini beradi. Bu anomaliyalar va shubhali harakatlarni aniqlashga yordam beradi va o‘z vaqtida javob berish va tekshirish imkonini beradi. Umuman olganda, xavfsizlik

devorlari uchun yaxshi mo‘ljallangan tarmoq arxitekturasi turli tahdidlardan himoyalanish uchun bir nechta himoya qatlamlarini yaratishga qaratilgan, shu bilan birga tarmoq ichida xavfsiz va samarali aloqani osonlashtiradi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)

1. Muhammadjonov, A., & TURLARI, T. S. Y. T. ICHKI VA TASHQI YARIMO ‘TKAZGICHLAR. Research and implementation.–2023.
2. Tojiboev, I., Rayimjonova, O. S., Iskandarov, U. U., Makhammadjonov, A. G., & Tokhirova, S. G. (2022). ANALYSIS OF THE FLOW OF INFORMATION OF THE PHYSICAL LEVEL OF INTERNET SERVICES IN MULTISERVICE NETWORKS OF TELECOMMUNICATIONS. Мировая наука, (3 (60)), 26-29.
3. O. S. Rayimdjanova, M. Akbarova, & B. Ibrokhimova. (2022). THERMAL CONVERTER FOR HORIZONTAL WIND SPEED AND TEMPERATURE CONTROL. Oriental Journal of Technology and Engineering, 2(02), 14–20. https://doi.org/10.37547/supsci-ojte-02-02-03
4. Rayimjonova, O. S., Tillaboyev, M. G., & Xusanova, S. S. (2022). Underground water desalination device. International Journal of Advance Scientific Research, 2(12), 59-63.
5. Abdikhalikovna, N. R., Sodikovna, R. O., Umarali, E. S., & G‘anijonovich, T. M. (2022). Anomalous photovoltaic effect in dielectrics. International Journal of Advance Scientific Research, 2(06), 84-90.
6. Хусанова, М. К., & Сотволдиева, Д. Б. (2020). ИСПОЛЬЗОВАНИЕ ДЕЦИМАЦИИ И ИНТЕРПОЛЯЦИИ ПРИ ОБРАБОТКЕ СИГНАЛОВ В ПРОГРАММЕ MATLAB. In ЦИФРОВОЙ РЕГИОН: ОПЫТ, КОМПЕТЕНЦИИ, ПРОЕКТЫ (pp. 970-975).
7. Обухов, В. (2023). 5 СПОСОБОВ, КОТОРЫМИ БЛОКЧЕЙН ПОВЛИЯЕТ НА ИНДУСТРИЮ ОБРАЗОВАНИЯ. Engineering problems and innovations.