ISSN 2181-3187

TARMOQ HIMOYA VOSITALARI: FIREWALLAR

Toshkent Axborot Texnologiyalari Universiteti,

Kiber xavfsizlik fakulteti, Kriptologiya kafedrasi dotsent v.b.,

PhD-**Imamaliyev Aybek**

Talabalar:

Norbutayev Dilshodbek

Amanov Nodirbek

Sanjarov Ulug'bek

Annotatsiya: Tarmoq himoyasi zamonaviy axborot texnologiyalarining muhim jihatlaridan biridir. Internet va boshqa tarmoqlar orqali axborot almashinuvi kengaygani sayin, tarmoq xavfsizligi masalalari ham dolzarblashmoqda. Ushbu masalalarni hal qilishda eng asosiy vositalardan biri firewallar hisoblanadi. Firewall, ya'ni "devor", tarmoqni tashqi tahdidlardan himoya qilish uchun mo'ljallangan dasturiy yoki apparat tizimidir. Ushbu maqolada firewallarning turlari, funksiyalari, afzalliklari va kamchiliklari haqida ma'lumotlar berilgan.

Kalit so'zlar: tarmoq, internet, ma'lumotlar, kompyuter, dasturlar, funksiyalar, afzalliklar.

Firewallar ikki asosiy turga bo'linadi: apparat va dasturiy. Apparati firewallar odatda tarmoqning o'rtasida joylashadi va barcha kiruvchi va chiquvchi ma'lumotlarni nazorat qiladi. Dasturiy firewallar esa kompyuterda yoki serverda o'rnatiladi va faqat shu qurilmaga kiruvchi va chiquvchi ma'lumotlarni boshqaradi. Har ikkala tur ham o'zining afzalliklari va kamchiliklariga ega. Apparati firewallar ko'proq tarmoq darajasida himoya ta'minlaydi, lekin ularni o'rnatish va sozlash ko'proq vaqt va resurs talab qiladi. Dasturiy firewallar esa oson o'rnatiladi va sozlanadi, lekin ularning himoya

ISSN 2181-3187

darajasi apparat firewallariga nisbatan pastroq bo'lishi mumkin. Firewallning asosiy vazifasi - tarmoqdan o'tayotgan ma'lumotlarni nazorat qilish va tahdidlarni aniqlashdir. U kiruvchi va chiquvchi trafikni filtrlaydi, ya'ni ma'lum bir qoidalar asosida ma'lumotlarni qabul qiladi yoki rad etadi. Bu qoidalar foydalanuvchi tomonidan belgilanishi mumkin va ular tarmoq xavfsizligini ta'minlashda muhim rol o'ynaydi. Masalan, agar biror IP manzilidan kelayotgan trafik xavfli deb hisoblangan bo'lsa, firewall ushbu trafikni bloklaydi. Shuningdek, firewalllar tarmoqda mavjud bo'lgan resurslarga kirishni boshqarish imkonini beradi. Bu esa foydalanuvchilarning faqat ruxsat etilgan resurslarga kirishini ta'minlaydi va xavfsizlikni oshiradi.[1]

Firewalllarning yana bir muhim funksiyasi - tarmoq trafikining monitoringidir. Ular kiruvchi va chiquvchi ma'lumotlarni qayd etadi va tahlil qiladi. Bu esa tarmoqda yuzaga kelishi mumkin bo'lgan muammolarni aniqlashda yordam beradi. Misol uchun, agar tarmoqda nojo'ya trafik ko'payib ketsa, bu tahdidni aniqlash va unga qarshi choralar ko'rish imkonini beradi. Firewalllar shuningdek, tarmoqda mavjud bo'lgan xatolarni aniqlash va ularni tuzatish uchun zarur bo'lgan ma'lumotlarni taqdim etadi. Firewalllarning bir nechta afzalliklari mavjud. Birinchidan, ular tarmoqni tashqi tahdidlardan himoya qilishda muhim rol o'ynaydi. Bu, o'z navbatida, axborot xavfsizligini oshiradi va foydalanuvchilarning ma'lumotlarini himoya qiladi. Ikkinchidan, firewallar tarmoqda mavjud bo'lgan resurslarga kirishni boshqarish imkonini beradi, bu esa tarmoqning samaradorligini oshiradi. Uchinchi afzallik - tarmoq trafikining monitoringi. Bu foydalanuvchilarga tarmoqda yuzaga kelishi mumkin bo'lgan muammolarni tezda aniqlash va ularga qarshi choralar ko'rish imkonini beradi. Biroq, firewalllarning kamchiliklari ham mavjud. Masalan, ba'zi hollarda firewallar noto'g'ri konfiguratsiya qilinishi mumkin, bu esa tarmoq xavfsizligini pasaytiradi. Shuningdek, ba'zi firewallar tarmoqning ish faoliyatini sekinlashtirishi mumkin, chunki ular ma'lumotlarni filtrlaydi va tahlil qiladi. Bu esa foydalanuvchilarga noqulaylik tug'dirishi mumkin. Yana bir muhim kamchilik - firewallar faqat tashqi tahdidlarga qarshi himoya qiladi, ichki tahdidlar (masalan,

ISSN 2181-3187

xodimlar tomonidan sodir etilgan xato yoki qasddan zarar yetkazish) uchun yetarli darajada himoya ta'minlamaydi.[2]

Zamonaviy firewallar ko'plab qo'shimcha funksiyalarni ham taqdim etadi. Masalan, ko'plab firewallar virtual xususiy tarmoqlar (VPN) yaratish imkonini beradi. Bu esa foydalanuvchilarga xavfsiz va shifrlangan aloqa o'rnatishga yordam beradi. Shuningdek, ba'zi firewallar zararli dasturlardan himoya qilish, spam filtratsiyasi va boshqa xavfsizlik funksiyalarini ham o'z ichiga oladi. Bu esa tarmoq xavfsizligini yanada oshiradi va foydalanuvchilarga qo'shimcha himoya ta'minlaydi. Firewallar tarmoq xavfsizligi strategiyasining ajralmas qismi hisoblanadi. Ular tarmoqni himoya qilishda muhim rol o'ynaydi va foydalanuvchilarga xavfsiz va samarali ishlash imkonini beradi. Biroq, firewallar o'z-o'zidan barcha tahdidlardan himoya qilmaydi. Ular boshqa xavfsizlik vositalari bilan birgalikda ishlatilishi kerak. Masalan, antivirus dasturlari, tarmoq monitoring tizimlari va boshqa xavfsizlik vositalari bilan birgalikda foydalanish tarmoq xavfsizligini yanada oshiradi. Umuman olganda, firewallar zamonaviy tarmoq xavfsizligi uchun zarur vositalardan biridir. Ular tarmoqni tashqi tahdidlardan himoya qiladi, trafikni nazorat qiladi va foydalanuvchilarga xavfsiz va samarali ishlash imkonini beradi. Biroq, firewallar o'z-o'zidan barcha tahdidlardan himoya qilmaydi, shuning uchun ularni boshqa xavfsizlik vositalari bilan birgalikda ishlatish muhimdir. Tarmoq xavfsizligini ta'minlashda kompleks yondashuv kerak bo'ladi, bu esa foydalanuvchilarning ma'lumotlarini himoya qilishda samarali natijalar beradi.[3]

Firewallar haqida gapirganda, ularning konfiguratsiyasi va boshqaruvi ham muhim ahamiyatga ega. Firewallni to'g'ri sozlash va boshqarish tarmoq xavfsizligini ta'minlashda muhim rol o'ynaydi. Foydalanuvchilar va tarmoq administratorlari firewallning qoidalarini va sozlamalarini doimiy ravishda yangilab turishlari zarur. Bu esa yangi tahdidlarga qarshi himoya ta'minlaydi va tarmoq xavfsizligini oshiradi.Shuningdek, firewallar tarmoqni himoya qilishda qiyinchiliklarga ham duch kelishi mumkin. Masalan, ba'zi hollarda foydalanuvchilar kerakli resurslarga kira

ISSN 2181-3187

olmaydilar, chunki firewall ularni bloklaydi. Bunday hollarda tarmoq administratorlari foydalanuvchilarning ehtiyojlarini inobatga olgan holda firewallning qoidalarini o'zgartirishlari zarur. Bu esa tarmoqning samaradorligini oshirishga yordam beradi.[4]

Xulosa:

Xulosa qilib aytganda, firewallar zamonaviy tarmoq xavfsizligi uchun muhim vositalardir. Ular tarmoqni tashqi tahdidlardan himoya qiladi, trafikni nazorat qiladi va foydalanuvchilarga xavfsiz ishlash imkonini beradi. Biroq, ularni to'g'ri sozlash va boshqarish muhimdir. Tarmoq xavfsizligini ta'minlash uchun kompleks yondashuv zarur, bu esa foydalanuvchilarning ma'lumotlarini himoya qilishda samarali natijalar beradi. Firewallar tarmoq xavfsizligi strategiyasining ajralmas qismi bo'lib, ularni boshqa xavfsizlik vositalari bilan birgalikda ishlatish zaruriyati mavjud. Tarmoq xavfsizligini ta'minlashda har bir foydalanuvchi va administratorning mas'uliyati katta bo'lib, ular o'zlarining ma'lumotlarini va resurslarini himoya qilishda faol ishtirok etishlari lozim.

Foydalanilgan adabiyotlar:

1. Abdullayev, A. (2021). Tarmoq xavfsizligi: nazariya va amaliyot. Toshkent: O'zbekiston Milliy Universiteti.

2. Qodirov, S. (2020). Axborot xavfsizligi tizimlari. Samarqand: Samarqand Davlat Universiteti.

3. Tashkentov, M. (2022). Tarmoq himoyasi va firewallar. Buxoro: Buxoro Davlat Universiteti.

4. Karimov, R. (2019). Zamonaviy tarmoq texnologiyalari. Nukus: Qoraqalpoq Davlat Universiteti.

5. Ismoilov, D. (2023). Firewall va tarmoq xavfsizligi. Toshkent: Toshkent Axborot Texnologiyalari Universiteti.

ISSN 2181-3187

6. Rahmonov, E. (2021). Tarmoq infratuzilmasi va xavfsizlik. Andijon: Andijon Davlat Universiteti.

7. Xolov, U. (2022). Tarmoq himoyasi: nazariy va amaliy jihatlar. Farg'ona: Farg'ona Davlat Universiteti.