ISSN 2181-3187

KOMPYUTER TARMOQLARIDA ZARARKUNANDA TRAFIKNI FILTRLASH

Norbutayev Xurshid Alijon o‘g‘li
Toshkent axborot texnologiyalari universiteti
123norbutayev@gmail.com

Annotatsiya: Ushbu maqolada zararkunanda trafikni aniqlash va filtrlash usullari, shuningdek, ularning tarmoq xavfsizligini ta’minlashdagi roli ko‘rib chiqiladi. Zararkunanda trafik yani kompyuter tarmoqlarida xavfsizlikka tahdid soluvchi va foydalanuvchilarning ma’lumotlariga zarar yetkazishi mumkin bo‘lgan trafikdir.

Kalit so‘zlar: Tarmoq xavfsizligi, tarmoqlararo ekranlar, ips ,hips, trafikni filtrlash,
IP filtrlash,geografik filtrlash,so‘rov chastotasi orqali filtrlash.

ФИЛЬТРАЦИЯ ВРЕДОНОСНОГО ТРАФИКА В КОМПЬЮТЕРНЫХ СЕТЯХ

Норбутаев Хуршид Алижан оглы
Ташкентский университет информационных технологий
123norbutayev@gmail.com

Аннотация: В данной статье рассматриваются методы обнаружения и фильтрации вредоносного трафика, а также их роль в обеспечении безопасности сети. Вредоносный трафик – это трафик, который угрожает безопасности компьютерных сетей и может нанести ущерб данным пользователей.

Ключевые слова: сетевая безопасность, межсетевые экраны, IPS ,HIPS, фильтрация трафика, IP-фильтрация, географическая фильтрация, фильтрация по частоте запросов.

FILTERING PEST TRAFFIC IN COMPUTER NETWORKS

Norbutayev Khurshid Alijan Ogli
Tashkent University of Information Technology
123norbutayev@gmail.com

ISSN 2181-3187

Abstract: The following article analyzes methods for detecting and filtering pest traffic, as well as their role in ensuring network security. Pest traffic is traffic that threatens security in computer networks and can damage user data.

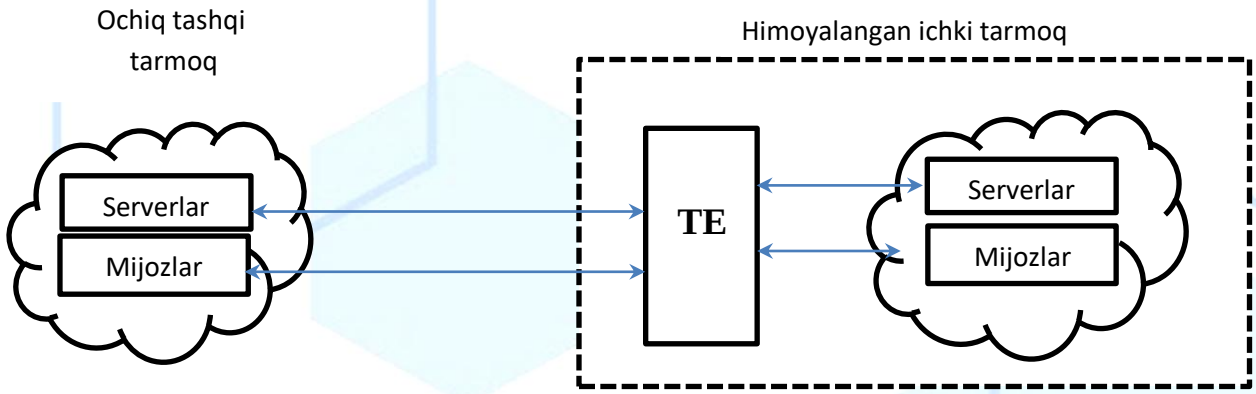
Hozirgi zamonaviy raqamlashgan internet olamida biz qabul qilayotgan har bir ma’lumot bizning foydamizga yoki bizga qarshi ishlashi mumkin.Shu boisdan hozirda kompyuter tarmoqlaridagi trafikni filtrlash undagi zararkunanda trafikni ajratib olish ka’bi dolzarb bo‘lgan muammo oldimizda turibdi. Tarmoq xavfsizligi bu tarmoqqa bo‘ladigan xujumlar va suqulib kirishlarni monitoringlash, bartaraf etish uchun mo’ljallangan xavfsizlik siyosati, taktikasi va instrumentlarini tavsiflovchi soha hisoblanadi. U hujumlarni aniqlab, buzg‘unchilarning hujumlarini bartaraf etish, tarmoqdagi faoliyatni aniqlay oladi va tarmoq o’tkazuvchanligi va blokirovkadan foydalanadi[2]. Bunday holatda yechimlardan biri xujumlarni bartarat etish tizimidan (IPS – Intrusion Prevention System) foydalanish, IPS – kirish trafiklarini tahlil qilish orqali buzg’unchilarning mavjudligini aniqlashga imkon beradigan himoya vositasi, bu vositalar zararkunanda trafiklar to‘plamiga ega bo’lgan holda, kirish trafiklar paketi namunalarini o’z ichiga olgan ma’lumotlar bazasidagi zararkunanda trafiklar bilan taqqoslash orqali tahlil qilinadi. Bunda agar tarmoq paketlari ma’lumotlar bazasidagi qoidalarga mos kelsa tarmoqda buzg‘unchilik holati haqida ogohlantirish yuboradi [1]. Tarmoqdagi zararli trafikni aniqlash masalasini o‘rganish, birinchi navbatda, anomal hodisalarning asosiy manbalarini aniqlashni talab qiladi.Har qanday korporativ tarmoq infratuzilmasi mustaqil ishlaydigan yoki bir-biri bilan o‘zaro ta’sir qiluvchi ko‘plab komponentlarni o‘z ichiga oladi va bu komponentlarning har biri tarmoq anomaliyalarining potensial manbai hisoblanadi. Tarmoq trafigi zararli harakatlarini barcha mumkin bo‘lgan birlamchi manbalarining to‘liq ro‘yxati murakkab vazifadir va shuning uchun korporativ tarmoqning ichki segmentidagi potensial zararli trafik manbalarining umumlashtirilgan tasnifi ishlab chiqilgan.

Tarmoqlararo ekran (TE) – *brandmauer* yoki *firewall sistema*si deb ham ataluvchi tarmoqlararo himoyaning ixtisoslashtirilgan kompleksi. Tarmoqlararo ekran umumiy tarmoqni ikki yoki undan ko‘p qismlarga ajratish va ma’lumot paketlarini chegara orqali umumiy tarmoqning bir qismidan ikkinchisiga o‘tish shartlarini belgilovchi qoidalar to‘plamini amalga oshirish imkonini beradi. Odatda, bu chegara korxonaning korporativ (lokal) tarmog‘i va Internet global tarmoq orasida o‘tkaziladi. Tarmoqlararo ekranlar garchi korxona lokal tarmog‘i ulangan korporativ intratarmog‘idan qilinuvchi hujumlardan himoyalashda ishlatilishlari mumkin bo‘lsada, odatda ular korxona ichki tarmog‘ini Internet global tarmoqdan suqilib kirishdan himoyalaydi. Aksariyat tijorat tashkilotlari

ISSN 2181-3187

uchun tarmoqlararo ekranlarning o‘rnatilishi ichki tarmoq xavfsizligini ta’minlashning zaruriy sharti hisoblanadi.

Ruxsat etilmagan tarmoqlararo trafikdan foydalanishga qarshi ta’sir ko‘rsatish uchun tarmoqlararo ekran ichki tarmoq hisoblanuvchi tashkilot tarmog‘i va tashqi tarmoq orasida joylanishi lozim (1-rasm).



1-rasm Tarmoqlararo ekrannni ulash sxemasi.

Ta’kidlash lozimki, tarmoqlararo ekran filtrlash funksiyasini vositachi-dastur ishtirokisiz amalga oshirib, tashqi va ichki tarmoq orasida o‘zaro aloqaning shaffofligini ta’minlashi mumkin.Ko‘pgina tarmoqlararo ekranlar statistikani qaydlovchi, yig‘uvchi va taxlillovchi quvvatli tizimga ega. Mijoz va server adresi, foydalanuvchilar identifikatori, seans vaqtlari, ulanish vaqtlari, uzatilgan va qabul qilingan ma’lumotlar soni, ma’mur va foydalanuvchilar harakatlari bo‘yicha hisob olib borilishi mumkin. Hisob tizimlari statistikani taxlillashga imkon beradi va ma’murlarga batafsil hisobotlami taqdim etadi. Tarmoqlararo ekranlar maxsus protokollardan foydalanib, ma’lum xodisalar to‘g‘risida real vaqt rejimida masofadan xabar berishni bajarishi mumkin[3].

Anomaly-based Detection bu ayni damda ishlab turgan va sozlangan tizimda tarmoq trafigini kuzatib turib, vaqti-vaqti bilan uni tahlil qiladi va agar oldingi misol bilan taqqoslaganda g’ayritabiiy statistika yuzaga kelsa, u ushbu g‘ayritabiiy vaziyatga aralashadi. Misol uchun, biz uni ichkaridan tashqariga g'ayritabiiy tarzda yaratilgan va ma'lumotlarni tashqariga chiqarishga urinayotgan xaker tomonidan yaratilgan trafik misolida ko'rishimiz mumkin. Bu yerda, standart baza davom etar ekan, ichkaridan tashqariga yoki tashqaridan ichkariga trafik ma’lum vaqt oralig‘ida g‘ayritabiiy ravishda o‘zgarishi yoki hujum sodir etuvchisi e’tiborga tushmaslik uchun ma’lum bir manbadan muntazam buyruqlar bilan ma’lumotlarni turli nuqtalarga yubirishga harakat qilishi mumkin. Bu kabi holatlar IPS dagi sensorlar tomonidan aniqlanishi mumkin.

ISSN 2181-3187

HIPS (Host-based Intrusion Prevention System) xostga asoslangan IPS tizimi bitta tizim ichidagi serverlar (Jismoniy Xost yoki VM Xost) kabi mahsulotlarda internet-trafikdan kelib chiqishi mumkin bo‘lgan viruslar va tahdidlarga qarshi himoya mexanizmini yaratadi. U xostda 3-sathdan 7-sathgacha, yani Network sathdan Application sathgacha xavfsizlik mexanizmini ta’minlaydi. HIPS o‘rnatilgan xost muntazam ravishda voqealarni, ma’lumotlarni uzatishni, unda ishlaydigan ilovalar xizmatlarini va xost xususiyatlarini tekshiradi. HIPS tizimdagi trafiklar, ilova va log jurnallari va fayl tizimi o‘zgarishlari ma’lumotlar bazasini tahlil qiladi va o‘zgarishlar va ruxsatsiz kirish ustidan nazorat qiladi. HIPS ma’lumotlar bazasidagi har bir obyektni solishtirar ekan, u obyekt xususiyatlaridan foydalangan holda o‘z-o‘zini nazorat qiladi va kontentdagi o‘zgarishlarni muntazam ravishda tekshirib, kerakli choralarini ko‘radi. HIPS shuningdek, xotiraga biron bir o'zgartirish kiritilgan yoki yo‘qligini bilish uchun xotira bo‘limlarini tekshiradi.Agar HIPS ning afzalliklari haqida gapiradigan bo‘lsak, u korporativ va davlat muassasalariga topshiriladigan tizimlarda taqdim etgan xavfsizlik siyosati bilan xavfsizlik darajasini yanada yuqori darajaga olib chiqadi. Xostda ishlash orqali u lokal tarmoqdan kelishi mumkin zararkunanda trafik va tahdidlarni ehtimoliy hujumlarini oldini oladi[4].

Trafikni filtrlash sizga zararli so‘rovlarni filtrlash imkonini beradi va shu bilan birga serverni qonuniy foydalanuvchilar uchun mavjud bo‘ladi. Trafikni filtrlash-ning bir necha usullari mavjud bo’lib, ularning har biri o‘ziga xos xususiyatlarga va afzalliklarga ega. Shuni ta'kidlash kerakki, DdoS hujumlaridan samarali himoya qilish odatda bir vaqtning o‘zida bir nechta filtrlash usullaridan foydalanishni talab qiladi.

IP manzillar bo‘yicha filtrlash - bu usul shubhali yoki zararli so‘rovlar keladigan IP manzillarni bloklashni o‘z ichiga oladi. IP bloklari ro‘yxatlari statik yoki dinamik bo‘ishi mumkin. Statik ro‘yxatlar qo‘lda yaratiladi va muntazam yangilashni talab qiladi, dinamik ro'yxatlar esa trafik tahlili asosida avtomatik ravishda yangilanishi mumkin. IP-manzilni filtrlash eng oddiy va samarali xavfsizlik usullaridan biridir, ammo uning cheklovlari mavjud. Masalan, hujumchi o‘zlarining haqiqiy IP manzillarini yashir- ish uchun proksi-serverlar yoki VPN-lardan foydalanishlari mumkin.Bu jarayonda hujumchi boshqa ip manzil orqali tizimga kirib olishi hamda zararkunanda trafikni serverga yuklashi mumkin.

Geografik joylashuv bo‘yicha filtrlash muayyan mintaqalar yoki mamlakatlardan kelgan zararkunanda trafikni blokirovka qilish imkonini beradi. Hujum ma’lum bir geografik mintaqa- dan kelayotgan zararkunanda trafik mavjud bulsa, bu usul foydalidir. Misol uchun, agar sizning kompaniyangiz ma’lum bir mamlakatda biznes yuritmasa, siz ushbu mamlakatdan barcha trafikni bloklashingiz mumkin. Biroq, bu usul ham o'z cheklovlariga ega. Hujumchilar hujumni amalga

oshirish uchun boshqa mamlakatlardagi serverlardan foydalanishi mumkin, buning natijasida geografik filtrlashni samarasiz qiladi.

So‘rov chastotasi bo‘yicha filtrlash ma’lum vaqt oralig‘ida bir manbadan so‘rovlar sonini cheklash imkonini beradi yani tizimdagi trafikni bir saytga yoki so‘rovga bo‘lgan murojatlar soniga qarab cheklaydi.Buning natijasida hujumchining yubor- ishi mumkin bo‘lgan ko‘p sonli so‘rovlarini bloklaydi.Bu server yuklanishining oldini olishga yordam beradi. Misol uchun, agar bitta IP manzil qisqa vaqt ichida juda ko‘p so‘rov yuborayotgan bo'lsa, u vaqtincha bloklanishi mumkin. Bu usul, ayniqsa, tajovuzkorlar serverni juda ko'p so'rovlar bilan yuklashga harakat qiladigan zararkunanda trafik hujumlariga qarshi samarali usul hisoblanadi[5].

Xulosa

Zararkunada tarmoq trafikni aniqlash muammosini o‘rganish va uning usullari yo‘llari har qanday axborot-kommunikatsiya tarmog‘ining barqaror va xavfsiz ishlashini tashkil etishning muhim elementidir. Zararkunanda tarmoq trafigini tavsiflangan manbalari va sabablari, shuningdek ularni aniqlashning mavjud usullarini tahlil qilish tarmoqdagi zararli trafikni aniqlash nazariyasi bo‘yicha mavjud tadqiqotlarni to‘ldirishga imkon beradi.

Trafikni filtrlash DDoS hujumlaridan himoya qilishning muhim elementidir. IP-manzil, geo-joylashuv va so‘rov tezligini filtrlash kabi turli xil filtrlash usullaridan foydalanish serverlaringiz va tarmoqlaringizni zararakunanda trafikdan samarali himoya qilishga yordam beradi. Bundan tashqari, apparat va dasturiy ta'minot tarmoqlararo ekran, CDN va WAF kabi zamonaviy texnologiyalar va vositalardan foydalanish samarali hisoblnadi.Tarmoqni muntazam zararkunanda trafikdan monitoring va filtrlash qoidalarini yangilash, shuningdek, avtomatik vositalardan foydalanish hujumchilardan bir qadam oldinda turishga yordam beradi va DDoS hujumlaridan ishonchli himoyani ta'minlaydi. Shuni unutmangki, samarali himoya qilish har tomonlama yondashuvni va yangi tahdidlar va zaifliklarga doimiy e'tibor berishni talab qiladi.

Foydalanilgan adabiyotlar:

1. Qurbonaliyeva D. Tarmoq xujumlarini aniqlash vositalari tahlili,maqola Информатика и инженерные технологии,1(2) 2023, 44–48 bet. (https://inlibrary.uz/index.php/computer-engineering/article/view/24979)
2. F.Q Tojiyeva Tarmoq trafigini sinflashtirish va filtrlash uchun boshqaruv dasturini ishlab chiqish,maqola,Raqamli iqtisodiyot 8-son, 2024,869-875-bet;(https://cyberleninka.ru/article/n/tarmoq-trafigini-sinflashtirish-va-filtrlash-uchun-boshqaruv-dasturini-ishlab-chiqish)

ISSN 2181-3187

3. G.S. Karimovich, K.M. Malikovich,T.K. Axmatovich axborot xavfsizligi,darslik,toshkent -2016,206-215 bet.
4. Ips tizimlari arxitekturasi haqida, Netcom Bilgisayar A.Ş, (https://www.netcom.com.tr/uz/ips_tizimlari_arxitekturasi_haqida_aytilmaganlar-139).
5. Фильтрация трафика как метод защиты от DDoS атак, Skypro, (https://sky.pro/wiki/python/ponimaem-funktsiyu-enumerate-v-python-na-primere-koda/)